International Technology Alliance
in
Distributed Analytics
& Information Sciences

Biennial Program Plan, 2018

Applicable Period: January 15th, 2018 - January 14th, 2020

Revised November 18, 2018 to correct the TA2 budget moving UCLA & BAE budgets listed against project 6 in error to project 5 where they belong. The overall program budget and partner budget remain unchanged.

Revised December 5, 2018 to revise project 3.2 milestones to replace the topology inference work with the coreset work from quarter four through eight of BPP18

Table of Contents

Introduction

DAIS-ITA (International Technology Alliance in Distributed Analytics and Information Sciences) is a collaborative partnership between the U.S. Army and the UK Ministry of Defence which brings together researchers from U.S. Army Research Laboratories (ARL) and UK Defence Science & Technology Laboratory (Dstl) to work alongside a consortium of universities and industrial research laboratories in U.S. and UK. The goal of the alliance is to foster collaborative fundamental research in both nations that will to enable secure dynamic semantically aware distributed analytics for situational understanding in coalition operations. The members of the alliance seek to break down barriers, build relationships, develop mutual understanding and work in partnership to develop technology for the U.S. and UK military.

The consortium is led by IBM, which has major research and development operations in both nations. U.S. members of the consortium are University of California at Los Angeles, University of Massachusetts at Amherst, Pennsylvania State University, Purdue University, Stanford University, Yale University and Raytheon BBN Technologies. UK members of the consortium are Cardiff University, Imperial College London, University of Southampton, University College London, Airbus Group and BAE Systems.

DAIS-ITA consists of three components: The Basic Research Component and two Technology Transition Components, one each for U.S. or UK-led efforts. The Basic Research Component provides for fundamental research, the results of which will be in the public domain. The Technology Transition Components will provide for the application of the fundamental-research results to military, security and commercial applications to foster the best technologies for future defense and security needs.

This document describes the first biennial program plan (BPP) for the DAIS-ITA Basic Research Component, and provides an overview of the research work to be undertaken from January 15th, 2018 to January 14th, 2020.

The scope of basic research in the program spans two technical areas: Dynamic Secure Coalition Information Infrastructures (TA-1) and Coalition Distributed Analytics and Situational Understanding (TA-2). TA-1 will perform fundamental underpinning research for enabling distributed, dynamic, secure coalition communication/information infrastructures that support distributed analytics to derive situational understanding. Coalition operations at the tactical edge encounter severe resource constraints and rapid changes in the environment. The research in TA-1 seeks to develop techniques for dynamic, self-configuring services that build services "on-demand," taking into account changing mission needs, context and resource constraints, while seeking to protect coalition information and assets. TA-2 will explore the principles underlying distributed analytics and situational understanding, taking into account the fact that coalition operations involve complex multi-actor situations, have information with a high degree of complexity, needs to be processed in a time-sensitive manner at a high tempo, and are required to align itself with human needs and capabilities.

The outputs of the basic research component of the program will advance the state-of-the-art, develop fundamental knowledge, and provide generalizable results. This fundamental science will be manifested in scientific publications in peer reviewed conferences and journals, books covering subjects in scope of the program, as well as trained researchers. Experimental validation of the research is critical and any experimentation software will be made available across the Alliance (ideally as open source) and may be integrated into an experimental framework to enable wide-scale experiments to validate inter-disciplinary research.

The research is split into 6 projects, each with two research tasks, and with the 6 projects spanning two technical areas (TAs):

- Technical Area 1: Dynamic, Secure Coalition Information Infrastructures
  Research is needed to provide the fundamental underpinning research for enabling distributed, dynamic, secure coalition communication/information infrastructures that support distributed analytics to derive situational understanding.
- Technical Area 2: Coalition Distributed Analytics & Situational Understanding
  Multidisciplinary research is needed to provide the fundamental underpinnings for future coalition distributed analytics and situational understanding in the context of ad-hoc coalition operations at the tactical-edge.

These technical areas have associated Technical Area Leader (TAL) roles identified, with Government TALs (GTALs) from both government organisations (ARL and Dstl) as well as Industry TALs (ITALs) and Academic TALs (ATALs). These roles are:

- TA1
  - US GTAL – Ananthram Swami (ARL)
  - UK GTAL – Chris Williams (Dstl)
  - ITAL – Bongjun Ko (IBM US)
  - ATAL – Don Towsley (UMass)
- TA2
  - US GTAL – Tien Pham (ARL)
  - UK GTAL – Gavin Pearson (Dstl)
  - ITAL – Dave Braines (IBM UK)
  - ATAL – Alun Preece (Cardiff)

This biennial program plan consists of six projects, each of which address issues that cut across both technical areas. From an organizational perspective, the first three projects address more issues in TA-1, while the last three projects address more issues in TA-2. The six projects are:

- P1: *Software Defined Coalitions*: will explore the principles by which different elements across a coalition could be composed via control plane interactions to form a virtualized larger element.
- P2: *Generative Policy Models for Coalitions*: will investigate approaches for policy based management in a coalition environment with sufficient autonomy to its constituent elements.
- P3: *Agile Composition for Coalition Environments*: will explore new architectures in which analytics code and data of various types (ISR, HUMINT etc) are mobile and composed together optimally.
- P4[1]: *Instinctive Analytics in a Coalition Environment*: Information system adapts to user-context and exploits future heterogeneous edge compute paradigm.
- P5: *Anticipatory Situational Understanding for Coalitions*: Verifiable predictive analytics operating synergistically between users and machine learning/reasoning.
- P6: *Evolution of Complex Adaptive Human Systems*: Understanding complex adaptive human groups, their mutability and evolution.

After describing the overall research vision, this BPP describes each of the projects in more detail.

[1] Note that projects P4, P5 and P6 were reordered between IPP and BPP 2018.

Research Vision

With the explosion in low cost phones, wearables and the Internet of Things, most coalition operations will take place in an environment with a diverse set of small elements capable of computation, storage and communication. We propose leveraging the various devices available across the coalition members to create a system with distributed collaborative and cooperative capabilities. This interconnected system will provide an infrastructure for performing analytics required for coalition operations. It will leverage all the services offered by a wired backend infrastructure (e.g. a backend cloud system, data center or available cellular network infrastructure) but it will not be critically dependent on a continuous connectivity to the backend.

We envision a future where the interconnected system operates seamlessly across networks and systems belonging to different organizations (i.e. coalition members or sub-groups within a single coalition member). This system is frequently charged with performing tasks that require creating dynamic groups on a short notice. Such dynamic groups may be short-lived (days or hours), but could also last for a longer period (months). Differences in the pedigree of disparate systems belonging to different organizations necessitate the development of approaches that work with partial visibility, partial trust, and cultural differences, while simultaneously dealing with the challenges of a dynamically changing situation in which power, computation and connectivity may be severely constrained.

We want the ability to create an intelligent interconnected system, i.e. a system that can analyze the situation on the ground in real-time, anticipate the situation likely to happen in the future, and determine whether the situation requires human involvement. If the situation does not require human involvement, the system would undertake the most appropriate automatic action to the situation. When the situation needs human involvement, the system will recommend alternative courses of actions, along with their pros and cons. We refer to this capability that coordinates different elements, with opportunistic assistance from a fixed infrastructure with interrupted connectivity, as the *distributed coalition intelligence*.

2,5 and 10 Year Goals

The goal of our basic research is to discover and formulate the scientific principles that enable the physical realization of *distributed coalition intelligence* at the conclusion of our 10-year research agenda. This physical realization will require the transition of our basic research into the appropriate systems and solution development. We use the metaphor of a *distributed brain* to describe the end-vision. Just as the human brain is made of two parts, a left hemisphere and a right hemisphere, the distributed coalition intelligence will be an aggregation of several smaller sub-brains, each sub-brain belonging to a coalition member. All of the sub-brains work in a coordinated manner to perform analytics, and leverage the assets and knowledge available across the entire system. Just like the left hemisphere and right hemisphere of the human brain react differently to different stimuli, we expect different sub-brains to react differently in any situation, but the overall distributed system coordinates the different reactions in a seamless manner as needed. A pictorial representation of the concept is shown in Figure RP-1.

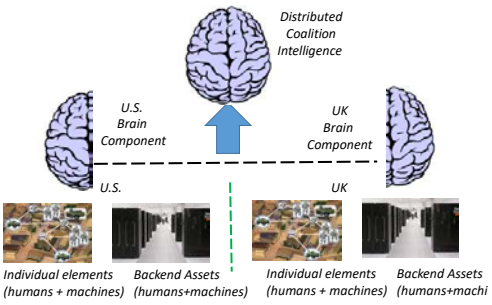

Figure RP-1

To attain the 10-year goal outlined above, we need to understand the fundamental principles underlying some of the key properties of the distributed coalition intelligence when applied to analytics. Our 5-year goal is to understand those principles underlying those properties.

In order to achieve our strategic vision, we must get an insight into the following properties by the end of 5-years.

- *Composability*: How do we compose smaller elements into a larger aggregate that works like a seamless whole? What are the principles that link the attributes of a component to the larger whole, and how can we compose components belonging to different organizations with partial visibility and control in an environment with limited resources?

- *Interactivity*: How do different computing elements and people interact with each other, both with other members of the groups and to external stimulus from the environment? How should we model and understand the interactions between different elements and information sources? How do different sub-brains work together as a larger aggregate brain under?
- *Optimality*: How can elements work together to obtain the optimal results in an environment with constrained resources? How can analytics be performed so that optimal performance is obtained automatically, instead of requiring complex manual optimization?
- *Autonomy*: How can elements work together in a proactive manner understanding future situations sufficiently well to operate with a degree of autonomous behavior? How can a system determine that autonomous operation is inappropriate and human intervention is needed? How can different elements simplify the cognitive burden involved to best assist humans in the loop when intervention is needed?

Understanding the principles behind these four attributes will allow us to attain significant capabilities for military defense as articulated in the UK MoD Technology Roadmap and in the U.S. third offset strategy.

Our six projects are defined so that the insights we obtain from them can be combined to help us understand the underpinnings of the four attributes. Our current view on how the different projects can be linked together to obtain the understanding of the four properties at the 5-year point is shown in Figure RP-2. Specifically, we plan on combining the results from projects P1, P2, P3 and P6 to understand the principles underlying composability, the results from projects P2, P6 and P5 to understand the principles that explain interactions among groups, the results from projects P1, P3 and P4 to understand how to self-optimize a system under limited resources, and the results from projects P2, P4 and P5 to understand the principles of autonomy. The results from the 5 years will be combined to get insights into principles governing the distributed coalition intelligence, which will enable us to physically realize such a system in 10 years by combining these scientific insights with appropriate systems building efforts.

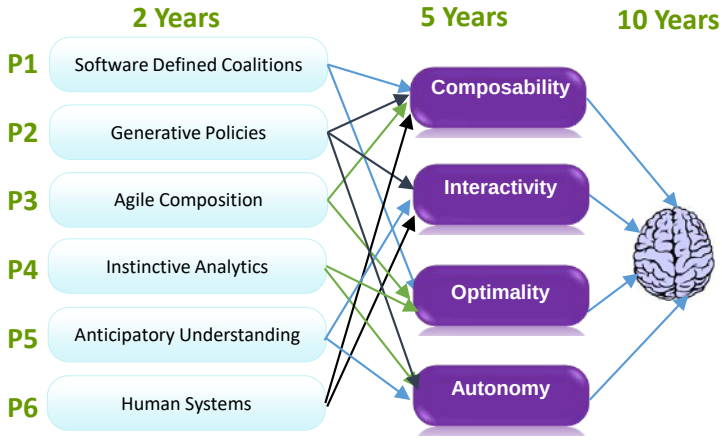

Figure RP-2

Project 1: Software Defined Coalitions

Project Champion: Kin Leung, Imperial College

Email: kin.leung@imperial.ac.uk **Phone: +44-207-594-6238**

Primary Research Staff	Collaborators
Frank Le, IBM US	Christian Makaya, IBM US
Kin Leung, Imperial	Andreas Martens, IBM UK
Liang Ma, IBM US	Vinod Mishra, ARL
Miguel Rio, UCL	Jeremy Tucker, Dstl
Leandros Tassiulas, Yale	Dinesh Verma, IBM US
Y. Richard Yang, Yale	Chris Williams, Dstl
Dave Conway-Jones, IBM UK	Sastry Kompella, NRL
Kelvin Marcus, ARL	Ali Hasan, IBM US
Unnamed PGR, Imperial	
Unnamed PGR, Yale	
Unnamed PGR, Yale	
Unnamed PDR, Yale	
Unnamed PGR, UCL	
Unnamed PDR, Yale	

Project Summary/Research Issues Addressed

To attain the vision of a distributed brain, we need to understand how different elements in a coalition can be composed together to form an efficient, unified, agile infrastructure, despite substantial resource constraints, high levels of dynamicity and local policies restricting coalition participation. The focus of P1 is to discover the fundamental principles and techniques by which we can obtain such composition. Extending Software Defined Networking (SDN) concept of separating the control and data plane to all coalition resources, including communication, storage and computation, to enable a new level of agility and dynamism, P1 has introduced the new architecture called Software Defined Coalitions (SDC), to realize many benefits including programmable coalition management, easy reconfiguration, on-demand resource allocation, and rapid response to network anomaly/failures.

Realizing an SDC infrastructure can lead to major advancements to support the overall DAIS-ITA project goal, for diverse settings from combat operations to intelligent operations to humanity operations.

Specifically, as illustrated as an example in Figure P1-1, an SDC is composed of multiple *domains (or enclaves)*, where each enclave represents a connected sub-network of a coalition partner. Each enclave contains one logical enclave controller (which may correspond to multiple physical controllers) and connects to the controller (which is also a logical entity where its functionalities can be distributed and co-located at the enclave controllers) associated with the given SDC slice. These controllers, which are collectively referred as the SDC controllers below, coordinate to utilize all infrastructure resources to achieve mission objectives and satisfy coalition policies for the given SDC. Note that multiple SDC slices can be defined in the same coalition physical infrastructure.

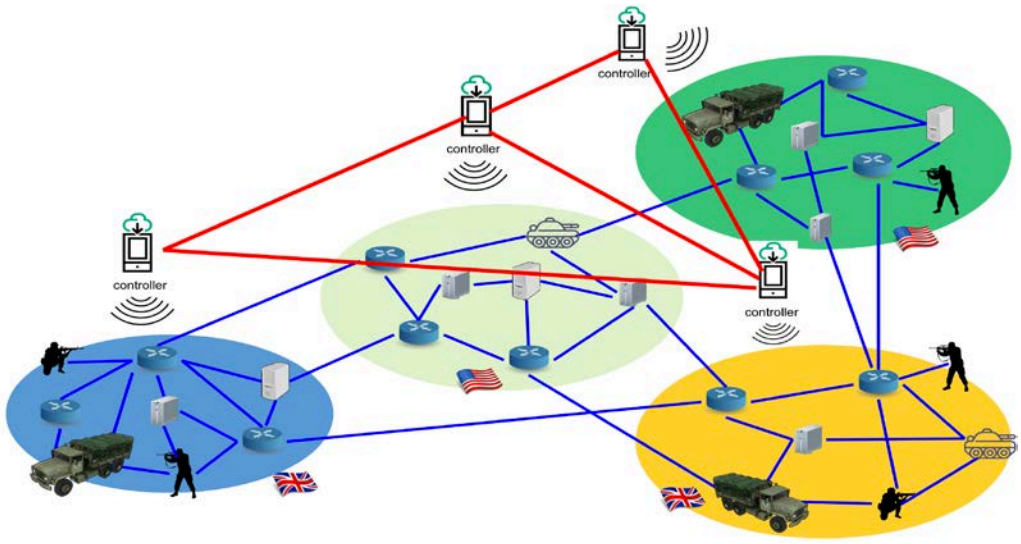

Figure P1-1. SDC-based coalition networks.

Realizing SDCs, however, needs to address substantial technical challenges and the goals of P1 in BPP18 are to address these challenges to make technical advancements in three key areas: (1) fundamental understanding of key factors affecting the overall performance of interconnected controllers; (2) fundamental understanding and design of programming abstractions of individual controllers; and (3) development of efficient designs of abstractions to interconnect controllers for SDC.

First, consider the fundamental understanding of key factors affecting the overall performance of interconnected controllers for SDC. Existing work on SDN architecture mostly emphasizes on advanced strategies for task-flow constructions within a domain. While for inter-domain task requests, the controllers need to rely on the knowledge of status information of other domains, obtained via control-plane synchronizations. However, due to wireless communications of fluctuating quality or fragmentations in the control plane, such synchronized information is generally limited and out of date, thus resulting in suboptimal decisions. Although these issues are known, there is a *lack* of *fundamental understanding* of how the network structural properties (e.g., topology, computation, storage, etc.) and the synchronization level (to what extent one domain has knowledge of other domains' information) may affect the overall performance of flow construction strategies in SDC settings. By significantly extending the preliminary work on the topic in the IPP, we will conduct a fundamental investigation to quantify the performance gains of the SDC control architecture in terms of network structural parameters and inter-domain synchronization levels in the BPP18. Furthermore, we will apply *insights* from the quantification to design techniques for the placement of functionalities, synchronization scheme design, as well as infrastructure fragmentation/re-joining issues.

Second, consider the configuration of the control-plane of individual coalition members. An efficient, agile SDC control-plane of each member must be highly programmable, to allow extensibility, composability, and reactivity, to handle ever evolving, diverse, dynamic mission requirements. Although SDN control-plane

programming progressed significantly lately[2], the state of the art, driven largely by commercial data center settings, focuses on handling complexities such as low-level device models or achieving extremely high throughput. Key SDC challenges, including high-levels of state dynamicity and weakly-connected data and control planes, are not addressed. During BPP18, we will conduct a systematic study by introducing SDC-Intensive Control-Plane Programming Abstractions.

Third, we plan to apply the insights of the first two advancements to guide our design of interconnection abstractions. The dominant and de facto interconnection abstraction (called inter-domain protocol in the general setting) is BGP[3], a possible candidate for SDC interconnection (and as a form of minimal inter-domain synchronization). Unfortunately, besides its potentially poor performance, BGP can encounter severe scalability and capability difficulties. Designed with limited programmability, BGP is a *full instantiation* protocol in that program decisions at each coalition member should be fully instantiated as data (i.e., routing information base) and then exchanged. The highly dynamic, resource constrained, policy constrained, and programmable SDC settings make full instantiation unfeasible. Further, focusing almost exclusively on single-destination connectivity, BGP cannot provide fundamental information such as resource contention of multi-flows to achieve optimal, coordinated resource composition. Based on the hierarchical path-vector abstraction, BGP enforces hierarchical routing, disallowing flexible composition of resources (e.g., the same network cannot appear twice in a network path). Such restrictions can severely reduce resource usage efficiency in tactical coalition settings, where resources from different coalition members can scatter and interleave at the same location. During BPP18, we will conduct a fundamental investigation on general abstractions, to provide mechanisms to allow trade-offs in autonomy and coordination, to go beyond networking resources to include other resources such as computation and storage. These new abstractions will facilitate highly efficient interconnection, coordination and synchronization among controllers to achieve the desirable performance, programmability and robustness of the SDCs.

Technical Approach

Our overall technical approach is to integrate fundamental analysis with design principles, where Task 1 focuses more on the analysis to acquire the basic understanding of performance tradeoffs for controller synchronization and Task 2 on the programming design and abstractions for interconnected controllers. Together, the two tasks form a right balance and synergy.

The goal of Task 1 is to reveal the fundamental principles that govern the performance of the SDC architecture, and our approach to achieve the goal is to introduce fundamental analysis under abstracted network parameters (e.g., topologies, computation/storage status, synchronization levels/costs). Specifically, in tactical networks, due to hostile environments, some SDC controllers can only synchronize with neighbors in their vicinity; in the extreme case, some SDC controllers have to act independently and resort to primitive inter-domain flow construction protocols (e.g., BGP-like protocol as studied in our recent work[4] - *Infocom'17 Best Paper Award*). It remains unknown how various degrees of synchronizations (e.g., caused by fragmentation, synchronization cost as shown in Figure P1-2) may affect the performance of the overall SDC architecture. Without such fundamental understanding, it is impossible to justify the necessity of developing complicated operational strategies. To understand the performance of distributed SDC architecture, we propose to establish a generic network model that captures major network parameters, e.g., intra-/inter-domain connections, node degree distributions (where the node degree is defined as the number of neighbors of the node), traffic status, resource utilization, etc. Based on this model, we study the performance of the constructed task flows, measured by the associated total cost, under various network parameters.

---

[2] e.g. Sushant Jain, Alok Kumar, Subhasree Mandal, Joon Ong, Leon Poutievski, Arjun Singh, Subbaiah Venkata, Jim Wanderer, Junlan Zhou, Min Zhu, Jon Zolla, Urs Hölzle, Stephen Stuart, and Amin Vahdat, "B4: Experience with a Globally-Deployed Software Defined WAN," In *Proceedings of the ACM SIGCOMM 2013 conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '13)*, pp. 3-14, Hong Kong, China, Aug. 12-16, 2013. Proceedings published as *Computer Communication Review (CCR)*, vol. 43, no. 4, pp. 3-14, Oct. 2013.

[3] Yakov Rekhter, Tony Li, and Susan Hares, "A border gateway protocol 4 (BGP-4)," *No. RFC 4271*, 2005.

[4] K. Poularakis, G. Iosifidis, G. Smaragdakis and L. Tassiulas, "One Step at a Time: Optimizing Incremental SDN Upgrades in ISP Networks," IEEE INFOCOM, 2017 (Best Paper Award).

As a further step, the details of resource status information of a given domain can be varied in a way that details from a distant domain can be coarse, while full details of close-by domains can be available to neighboring domains. We plan to study to what extent such resource-specific partial synchronizations can affect the overall performance and under what conditions satisfactory performance can be maintained in the distributed SDC environment. This aspect of the work will be carried out jointly with Task 1 in P3 where mathematical models to represent resource availability (status) in the multi-domain SDC will be developed.

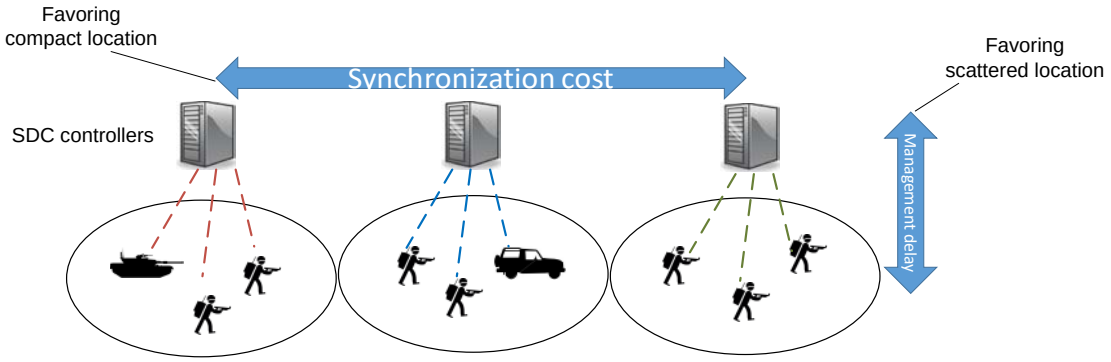

Figure P1-2. Controller placement and interplay among different objectives.

Based on the above theoretical foundations, we then study how to strategically enhance the distributed SDC control architecture for the maximal performance gain. Specifically, we explore how to place network functionalities to achieve the high-performance conditions in Subtask 1 (via gateway placement), increase the overall synchronization levels (via controller placement and management structure design under different objectives), and enforce synchronization policies.

The goal of Task 2 is to conduct a systematic design and analysis on programming and composition of an efficient, agile, and optimal SDC infrastructure, where programming means the specification of the control and resource planes of coalition members, and composition means the interconnection of coalition members. To achieve the goal, we follow a technical approach that *abstractions based on decomposition (modularity) are the way problems are solved*[5]. In particular, Task 2 follows a *problem-decomposition* approach and organize the research into four subtasks: (1) developing high-level, SDC-intensive programming, because we focus on key SDC challenges; (2) developing a unified model-views framework and an SDC abstraction calculus technique to understand and design how control-planes of SDC communicate and achieve interconnection; (3) developing constraints and composition techniques, which we refer to as an SDC composition algebra, to achieve global properties from local members, whenever possible; and (4) extending from abstractions to SDC architecture modelling, formalization and integration of all infrastructure components and applications.

Beyond analysis and designs, we will also integrate experimentation and validation from the beginning as a key technical approach. Specifically, we will develop a repository of key SDC use cases, including services to be supported by the infrastructure, operational environments (in particular, the size, dynamicity and resource constraints), and performance metrics and their implications on the overall mission effectiveness. We refer to this repository as the SDCbench, and will start with operational environments including NATO IST-124 RTG Emulated Scenario for cases such as the Anglova emulation, and use cases including moving target defense and anticipatory QoI[6]. To increase the utility of SDCbench, we will ensure use cases in SDCbench are composable.

Using the SDCbench and considering the specific need of each research thrust, we plan to develop a set of analysis tools to achieve initial problem space understanding and then solution validation. To avoid solo efforts, we will make the tools composable, forming an overall validation and experimentation tool chain which we call SDCsim. SDCsim and SDCbench will be used consistently to validate and experiment on the impacts of factors such

[5] Barbara Liskov, "The Power of Abstraction," In *Proceedings of International Symposium on DIStributed Computing (DISC '10)*, p. 3, Cambridge, MA, USA, Sep. 13-15, 2010.

[6] Kelvin Marcus, "An Environment for Tactical SDN Experimentation. P1 Workshop", London, U.K., Jun. 16, 2017.

as dynamicity and resource constraints, collecting key quantitative performance metrics including overhead, responsiveness, and scalability. Whether the designs can handle the operational environments (e.g., the level of dynamicity) under the given constraints (e.g., data-control-plane bottleneck and computational availability) will provide key validation decisions.

Task 1: Distributed SDC Control Plane with Limited Inter-Domain Synchronizations

Primary Research Staff	Collaborators
Liang Ma, IBM US	Sastry Kompella, NRL
Kin Leung, Imperial	Jeremy Tucker, Dstl
Leandros Tassiulas, Yale	Dinesh Verma, IBM US
Dave Conway-Jones, IBM UK	Ali Hasan, IBM US
Unnamed PGR, Yale	
Unnamed PGR, Imperial	

We plan to address the problem of control-plane synchronization in two related subtasks: (1) fundamental performance quantification, and (2) network architecture enhancement. The goal of the first subtask is to reveal fundamental principles that govern the performance of the SDC architecture under abstracted network parameters (e.g., topologies, computation/storage status, synchronization levels), whereas the second subtask is to enhance the network architecture based on (1) so that the corresponding network parameters jointly enable the best infrastructure performance.

Subtask 1.1: Fundamental Performance Quantification

We propose to formulate the SDC network as a two-tier hierarchical model. As illustrated in Figure P1-3, tier-1 consists of all domains, each modeled as a weighted random graph with nodes interconnected following a specific degree distribution[7] extracted from real coalition networks. Then abstracting each domain as a single vertex, we connect these vertices in tier-2 via the inter-domain degree distribution, and map each edge to several weighted links connecting the gateways in tier-1. The significance of this two-tier hierarchical model is its generality (with *no* reliance on specific graph models, such as Erdos-Renyi[8] or Barabasi-Albert[9,10] graphs), which can capture any distributed (wired/wireless) SDC networks. Here the weight of a link is the abstraction of the corresponding cost, e.g., computation, storage, and/or communication cost, when the link is used for flow constructions.

[7] M. Newman, S. Strogatz and D. Watts, "Random graphs with arbitrary degree distributions and their applications," Physical Review E, vol. 64, no. 2, 2001.

[8] P. Erdos and A. Renyi, "On the evolution of random graphs," Publ. Math. Inst. Hung. Acad. Sci 5.1 (1960): 17-60, 1960.

[9] R. Albert and A.L. Barabási, "Statistical mechanics of complex networks," Statistical mechanics of complex networks. Reviews of modern physics, 74(1), 47, 2002.

[10] A. L. Barabási and R. Albert, "Emergence of scaling in random networks," Science, 286(5439), 509-512, 1999.

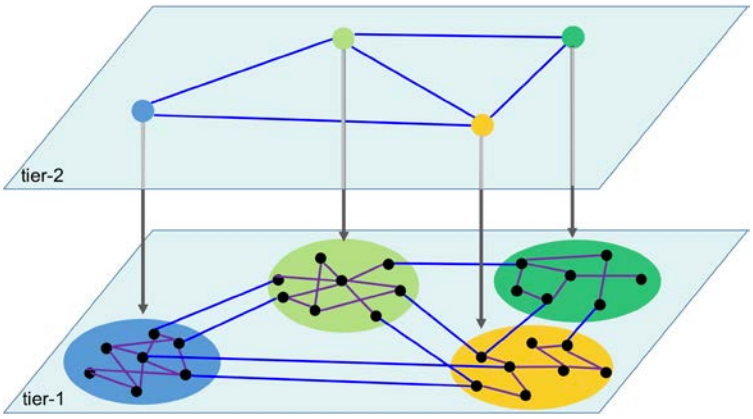

Figure P1-3. Two-tier hierarchical network model

As discussed above, due to fragmentation, the worst-case scenario happens when every domain is fragmented from the SDC architecture, i.e., no synchronization until new information is available upon re-joining the SDC architecture. By contrast, if all controllers are fully synchronized with each other, then they can jointly make the *globally* optimal decision for any task requests as all domains form a single infrastructure, i.e., the best-case scenario. Since the performance of any flow construction strategy lies between these two extreme cases, we first quantify their performance gap, where a big gap indicates a large SDC design space. For this goal, we first study the network with all edge weights being 1 (i.e., the total cost of the constructed flow is the corresponding number of hops) and homogeneous network parameters in each domain. Under this setting, our initial theoretical results[11] show that the average performance gap is a *logarithmic function* of the network size, node degree distribution, and the number of gateways, i.e., demonstrating *small-world* phenomenon[12,13]. Evaluation results also confirm the high accuracy of the derived performance gap. Based on these results, we next propose to extend them to heterogeneous domain settings. We then investigate the performance gap in a more challenging case where edge weights are different (i.e., to capture various construction costs). To address this issue, we propose to convert the original network into an augmented graph where all properties in the original network are retained but edge weights in this new graph are 1, and thus the above analytical methods can be re-applied. Assuming all edge weights are integers, one possible method for achieving this graph conversion is to replace each original edge with weight k by a tandem of $k-1$ nodes. Then the objective becomes computing the performance metric among nodes contained in the original network.

Our next step is to quantify the benefit achievable by SDC under limited inter-domain synchronizations (i.e., only partial inter-domain knowledge is available). To begin, we plan to explore this issue under two controller-synchronization models for communication resources (i.e., routing purposes). (1) Deterministic model: each controller knows the information of the nearest h domains; (2) Probabilistic model: a controller knows the information of a domain that is d-domain-hop away with the probability proportional to d^{-r} ($r \geq 0$, $r=0$: fully synchronized, $r=+\infty$: completely fragmented). Our further step is to extend these models to capture the degree of synchronization for other resources including computation and storage in various domains. To this end, we start with a basic strategy, where each controller is prepared to share its detailed status information with certain neighboring domains according to the synchronization models.

Finally, in tactical environments, networks may experience dynamics, e.g., mobility, node entering/leaving, and edge weights may be time-variant for different coalition partners. Moreover, in the distributed SDC environment, there may exist untruthful domains, i.e., some domains underreport its network status for saving resources. In this regard, we investigate how such dynamics affect the network performance. Intuitively, network dynamics directly affect tier-1 node degree/distance distribution and synchronization difficulties. However,

[11] Z. Zhang, L. Ma and K.K. Leung, "On SDC-Based Inter-Domain Routing Efficiency and Network Architecture Design," Technical Presentation, June 2017. [Online]. Available: https://dais-ita.org/node/1300

[12] J. Travers and S. Milgram, "The small world problem," Psychology Today, 1, 61-67, 1967.

[13] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," Nature, 393(6684), 440-442, 1998.

depending on where changes happen, tier-2 node degree distribution may remain the same (see Figure P1-3), and thus the decision-making policies may or may not be affected. Leveraging these observations, we aim to quantify performance variations of SDC-based strategies in terms of network dynamics.

Subtask 1.2: Network Architecture Enhancement

Placement of Gateways: By carefully placing gateways in each domain and leveraging the flexibility of SDC, we consider how to minimize the total number of gateways while satisfying the performance requirement. Furthermore, we also explore the gateway placement problem under network dynamics, based on the fundamental understanding in Subtask 1. We target to explore how to place the minimum number of gateways under coalition constraints (e.g., computation, delay, etc.) such that the network performance averaged over the time horizon satisfies coalition needs.

Placement of SDC Controllers: In the simplest scenario, each domain acquires only one controller. To enable efficient management, each domain may elect to place its controller at the most central location (i.e., minimizing the average distance to nodes). However, this placement strategy can result in high synchronization cost, especially when the controllers of partners' domains are *scattered* all over the coalition network. On the other hand, a more *compact* location, where the controllers are closer to each other, can achieve faster synchronization at a low cost. Hence, an interesting question is to explore the interplay between different objectives to find the controller placement that achieves the right tradeoff between these factors (Figure P1-2). This is a new problem, with unknown analytical solutions, since most of previous works[14] neglected the impact of synchronization cost among controllers.

After addressing the above problem, we next consider a more complex case where a domain can have *multiple controllers* (effectively one logical controller per domain). The nodes in a domain can be partitioned across the available controllers. Compared to the simpler scenario, the delay-cost tradeoff in this case is more challenging to analyze for the following reasons. First, there are two types of synchronization costs, *inter-domain* and *intra-domain* communications, which may have different priorities depending on coalition partners' requirements. Second, as indicated by recent measurement studies[15], the rate at which a controller sends control messages to the rest of controllers depends on its load (e.g., the number of nodes assigned to it). This requires us explicitly consider the assignment of nodes to the controllers in the same domain when deciding the controller placement strategy. Hence, the respective joint controller placement and node assignment problem needs to be addressed.

Besides the delay–cost tradeoff, we will explicitly model and study the dynamicity of the tactical environments where the topology changes. In this case, even a small change to the topology could deteriorate the performance of the "optimal" controller placement, which motivates us to study dynamic schemes where the placed controllers can physically move to adapt to topological changes.

Controller Structure Design: Another major challenge in facilitating management in an SDC network is to decide *how to organize the controllers*. Specifically, there are two main ways to organize controllers: (i) *flat organization* where all controllers are treated equally and responsible for the same network applications[16] (ii) *hierarchical organization* where different controllers can handle different network applications[17]. For example, organize controllers in a coalition network based on a hierarchy of two layers, where only one controller per domain is elected as a top-layer controller while the rest controllers belong to the bottom-layer. The top-layer controllers try to synchronize their states to convey the information for inter-domain flow construction, while the bottom-layer controllers communicate at different timescales with the respective top-layer controller and each other to perform different network applications. We will optimally design the controller structure, going beyond the above two special cases, to maximize performance gain, cost, control delay, and responses to fragmentations.

Enforcement of Synchronization Policies: Motivated by the above fundamental understanding, we finally revisit the synchronization policies for a given SDC network. Intuitively, domains with high *betweenness centrality* are more important to flow constructions; therefore, enabling higher synchronization levels on these domains can be

[14] B. Heller, R. Sherwood and N. McKeown, "The Controller Placement Problem," ACM HotSDN, 2012.

[15] A. Muqaddas, A. Bianco, P. Giaccone and G. Maier, "Inter-controller Traffic in ONOS Clusters for SDN Networks," IEEE ICC, 2016.

[16] A. Tootoonchian and Y. Ganjali, "Hyperflow: A Distributed Control Plane for Openflow," INM, 2010.

[17] S. Hassas Yeganeh and Y. Ganjali, "Kandoo: A framework for efficient and scalable offloading of control applications," ACM HotSDN, 2012.

beneficial. On the other hand, coalition partners may incur various synchronization costs. By considering such tradeoff, we target to strategically force the formation of certain fragmentations, so that domains within the same fragmented component can synchronize with small cost. We study how the frequency of synchronizations and details of status information among controllers will affect efficient synchronization policies adaptive to current resource conditions. Such enforcement of synchronization policies will in turn lead to state-of-the-art gateway/controller placement algorithms as discussed above.

Task 2: Programming and Interconnection (East-West) Abstractions and Formalization for Software-Defined Coalitions

Primary Research Staff	Collaborators
Frank Le, IBM US	Kin Leung, Imperial
Miguel Rio, UCL	Christian Makaya, IBM US
Y. Richard Yang, Yale	Andreas Martens, IBM UK
Kelvin Marcus, ARL	Vinod Mishra, ARL
Unnamed PGR, UCL	Jeremy Tucker, Dstl
Unnamed PDR, UCL	Dinesh Verma, IBM US
Unnamed PGR, Yale	Chris Williams, Dstl
Unnamed PDR, Yale	

Subtask 2.1: High-Level SDC-Intensive Control-Plane Programming Abstractions

A basic property of a *real* SDC control-plane is *substantial complexity*, as it integrates functionalities spanning resource allocation, measurements, security, policy enforcement, fault tolerance, scaling, among others. High-level abstractions are essential in handling complexities, but few control abstractions are developed for SDC, as traditional research focuses on data centers, not on SDC settings. Formally, the problem that Subtask 2.1 addresses is: *What are the fundamental programming abstractions to control an SDC*? Since we focus intensively on abstractions for SDC settings, we refer to Subtask 2.1 as **SDC-intensive programming**. We plan to investigate Subtask 2.1 in the following three aspects during BPP18.

S2.1 Dynamicity: High-level, Dynamicity-oblivious, Weakly-connected Programming: Existing abstractions tend to be event driven and hence expose, instead of automate, substantial complexities of handling dynamicity. As a result, SDN programming using existing abstractions are low level, complex, and often without formal correctness consistency guarantee. In this step, we formulate the following simple, but fundamental question: *Is it possible to define and system-enforce consistent SDC programming, for high-level, dynamicity-oblivious, weakly-connected SDN programs?* System-enforced consistent SDN programming offers many benefits including formal correctness, simplicity of programming, and ease of understanding. At the same time, system-enforced SDC programming can be challenging, in particular, due to substantial inefficiency due to *limited automation capabilities*.

We plan to address the system-enforced consistency problem by leveraging our initial progress during IPP[18]. During IPP, we have introduced FAST Magellan, a simple, high-level SDN programming model based on a model-view abstraction to achieve system-enforced consistency for programming general network services, by introducing a set of basic, efficiency-oriented data structures (e.g., fast-forwarding tree and micro request graph), optimization techniques (e.g., automatic data-dependency tracing, snapshot and transaction management, and selective, incremental, speculative execution), and well-defined, stable, consistency models (e.g., snapshot consistency). During BPP18, we plan to systematically define and evaluate the aforementioned techniques, and further introduce, scalable, *fast local adaptation* techniques (e.g., based on our Resilient Routing Reconfiguration framework[19]), to automate weakly or even disconnected SDC programming.

S2.1 Datapath: Diverse Resource Path Programming. Existing high-level abstractions and the above topic S2.1 Dynamicity focus on wireline networking. As a next step, we formulate the following problem: *What are high-level programming abstractions to achieve integrated resource (data) path programming to support both wireless and wireline control-plane programming, as well as networking, computation and storage programming?*

Our plan to address this problem is to substantially extend our previous work[20], which has defined the first high-level, *algorithmic, general-purpose, oracle* control-plane programming model, to include diverse data-control models, in particular, wireless coding based datapath programming. The problems that we plan to investigate are: (1) Is coding based programming a generic model to include both wireless and wireline networking? (2) If not, what are the additional, minimal abstractions for diverse resource path programming?

S2.1 Crosslayer: High-level, Cross-packet, Cross-Resource Programming. The existing programming abstractions are based on per packet. Although highly flexible, they leave substantial complexities in SDC orchestration (e.g., HTTP URL may span multiple packets). Given substantial need to integrate security, for example to integrate resource orchestration and security inspection, which depends on programming across packets, it is essential to address this issue and hence we formulate the following problem: *What are fundamental programming models to support cross-packet programming?*

We plan to address this problem by extending SDC programming from single packets to high-level packet streams, by introducing a simple, but basic abstraction, flow based programming, so that control-plane programmers can retrieve attributes from across layers; we also plan to integrate both networking resources and computation/storage resources, leveraging our initial work in IPP[21]. Introducing the preceding abstractions, however, can lead to substantial complexity, in particular, they require finite-state machine management to collect cross-layer attributes, but traditional programming models can be stateless in the datapath. Distributed state machine creation and management will be the key focus of this step.

Subtask 2.2: SDC Control-Plane Interconnection Abstractions

The interconnection of fundamentally programmable, complex, multi-function SDC control-planes, as we develop in Subtask 2.1, can pose severe scalability and capability difficulties for traditional interconnection. Subtask 2.2 aims to develop scalable, complete communication abstractions for composition of complex SDC control planes. Formally, the problem that Subtask 2.2 addresses is: *What are the fundamental abstractions to allow efficient*

---

[18] Kai Gao, Chen Gu, Qiao Xiang, Y. Richard Yang, and Jun Bi, "FAST: A Simple Programming Abstraction for Complex State-Dependent SDN Programming," In *Proceedings of the ACM SIGCOMM 2016 conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '16)*, pp. 579-580, Florianopolis, Brazil, Aug. 22-26, 2016.

[19] Ye Wang, Hao Wang, Ajay Mahimkar, Richard Alimi, Yin Zhang, Lili Qiu, and Yang Richard Yang, "R3: resilient routing reconfiguration," In *Proceedings of the ACM SIGCOMM 2010 conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '10)*, pp. 291-302, New Delhi, India, Aug. 30-Sep. 3, 2010. Proceedings published as *Computer Communication Review (CCR)*, vol. 40, no. 4, pp. 291-302, Oct. 2010.

[20] Andreas Voellmy, Junchang Wang, Yang Richard Yang, Bryan Ford, and Paul Hudak, "Maple: Simplifying SDN programming using algorithmic policies," In *Proceedings of the ACM SIGCOMM 2013 conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '13)*, pp. 87-98, Hong Kong, August 12-15, 2013. Proceedings published as *Computer Communication Review (CCR)*, volume 43, number 4, pp.87-98, Oct. 2013.

[21] Qiao Xiang, Shenshen Chen, Kai Gao, Harvey Newman, Ian Taylor, Jingxuan Zhang, and Yang Richard Yang, "Unicorn: Unified Resource Orchestration for Multi-Domain, Geo-Distributed Data Analytics," To appear in *Workshop on Distributed Analytics InfraStructure and Algorithms for Multi-Organization Federations (DAIS '17)*, San Francisco, CA, USA, Aug 6-7, 2017.

interconnection of software-defined coalitions? We say that the abstractions define the important *East-West interface*.

Our technical approach for Subtask 2.2 will be based on the SFP (SDN Federation Protocol) framework[22], which we have developed in the IPP. Specifically, SFP provides two features: (1) need-to-know only communications replacing request-oblivious communications; (2) model-views abstractions replacing ad hoc information exchange. Specifically, considering the logically centralized control-plane program PA of coalition member A as the unifying core, referred to as the model, SFP considers all information transfers, from the control plane of A to peers (East-West interface), to applications (Northbound), and to devices (Southbound) as computing on-demand views of the same PA. We believe that this unified framework leads to substantial intellectual simplicity and many potential benefits, including automation, modularity, and consistency.

During the BPP18, we plan to make significant progress to fully develop SFP. Since a key insight of the framework is that it considers each view as a (mathematical) derivative of the control-plane of each autonomous network, we refer to our approach as developing an **SDC abstraction calculus**, and plan to realize the approach with the following steps.

S2.2 Abstraction Complexity: Theoretical Complexity Analysis of Programming Abstraction. We will start with defining the theoretical-foundation problem: *What are the fundamental complexities of converting a general SDC control plane into data to be communicated during interconnection?* One can better appreciate this problem by comparing it to information capacity analysis in information theory.

Our plan to investigate the problem is to leverage the insight that although SDC control-plane programs can be complex for general algorithmic programs, they have a specific domain (e.g., limited to handle packet headers in SDN) and hence can have domain-specific compact representations. Hence, our strategy is to develop the fundamental capacity theorems for SDC communications, similar to information theory capacity theorems for data. Our initial approach is that we consider each control-plane program *f* as a point in a functional space, and map each *f* to a point in a unifying, abstraction functional space consisting of *characterization functions*. Information transmission structure defines the constraints (upper bounds) on *f*'s that can go through. During the IPP, we made initial progress in an Infocom'18 submission, and our goal during the BPP18 is to complete the study, by investigating both sufficient and necessary conditions.

S2.2 Abstraction Calculus: Development of SDC Abstraction Calculus. The fundamental abstraction that we plan to introduce for interconnection abstractions is that each coalition transmits the derivative *dP/dx*, where *P* is the control-plane program of the coalition and *x* a set of points in a general space. In our IPP work[23], we have investigated the case where *x* is a single point representing a single packet, and hence shown that BGP is a special case; in[24], we have investigated the case where *x* is a single point representing a set of flows, solving the issue of providing resource constraints. A main issue of our initial work, however, is that computing the derivative *dP/dx* is a tedious and complex process. Hence, the problem we formulate for this step is: What is a basic framework to allow systematic computation of *dP/dx*?

Our plan to investigate this problem is to focus on composition. A basic software reuse technique is composition: the behavior of an SDC is defined by composing two programs *f* and *g*. In traditional calculus, $(fg)' = f'g + fg'$, where ' denotes the derivative, and hence the derivative computation can be reusable. The key goal of this step is to develop a similar framework to allow systematic calculus for SDC composition.

<u>*Subtask 2.3: SDC Control-Plane Composition with Global Properties*</u>

---

[22] Franck Le, Christopher Leet, Christian Makaya, Miguel Rio, Xin Wang, and Yang Richard Yang, "SFP: Toward a Scalable, Efficient, Stable Protocol for Federation of Software Defined Networks," to appear in *Workshop on Distributed Analytics InfraStructure and Algorithms for Multi-Organization Federations (DAIS '17)*, San Francisco, CA, USA, Aug 6-7, 2017.

[23] Andreas Voellmy, Shenshen Chen, Xin Wang, and Yang Richard Yang, "Magellan: Generating Multi-Table Datapath from Datapath Oblivious Algorithmic SDN Policies," In *Proceedings of the ACM SIGCOMM 2016 conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '16)*, pp. 593-594, Florianopolis, Brazil, Aug. 22-26, 2016.

[24] Kai Gao, Qiao Xiang, Xin Wang, Yang Richard Yang, and Jun Bi, "NOVA: Towards On-Demand Equivalent Network View Abstraction for Network Optimization," In *Proceedings of 2017 IEEE/ACM International Symposium on Quality of Service (IWQoS '17)*, pp. 1-10, Vilanova i la Geltrú, Spain, Jun. 14-16, 2017.

Subtask 2.2 considers control-plane programs as fully given (hence the focus on analysis). The objective of Subtask 2.3 is to enforce global properties and hence guide the design of control-plane programs. In the absence of existing inter-SDC deployment, and the unique clean state opportunity, we propose a top-down approach to compose global properties, and refer to our approach as developing *an* **SDC composition "algebra"**.

To illustrate the objective and the challenges, let's assume that shortest path routing is the desired global network-wide property. Distributed algorithms such as Bellman-Ford allow shortest paths between every pairs of source and destination to be computed without any node having a global view of the network. However, such distributed algorithms require every participating node to select and advertise routes in the same defined way. Such an approach to guarantee global network wide properties is too restrictive for tactical military networks. Each coalition network may have different policies, and prefer to select/advertise routes differently. As a more desirable way to address the problem, researchers have more recently demonstrated that through minimal local constraints, global network-wide properties can still be achieved (while still allowing each domain to implement their own specific policies)[25]: researchers have modeled routing using algebraic structures (e.g., semi ring), and proved that when routes are propagated in a vector (versus link state) manner, and the operations (to select and transform routes as they traverse networks) are monotonic, then routing is guaranteed to be loop free. When routes are advertised in a link state (versus vector) manner, and the operations (to select and transform routes as they traverse networks) are isotone, then routing is guaranteed to be optimal across the entire network. Following the same philosophy, we formulate the following problem: what are the minimal local constraints (e.g., monotonic operations, isotone operations) to achieve global, tactical network wide properties for not only network (i.e., routing) but also compute and storage resources? We plan to address the problem in the following three steps.

S2.3 Global Properties: Identification of SDC Global Properties. We formulate the following basic problem for this basic step: What are the basic global properties for tactical military networks? For example, while loop free forwarding paths are a common goal in routing systems, given the intermittent and often capability restrained characteristic of wireless links in military coalition networks, SDCs may also want to route along highest available bandwidth paths, or most stable paths across the networks. Further, SDCs are responsible not only for networking but also storage and compute resources. The goal of this first step consists in identifying desirable global properties not only for networking resources, but also compute and storage resources. To achieve it, we will get input from Task 2.1, derive specific use-cases, and seek feedback from our government partners.

S2.3 Global Model: Modeling of SDC Resources through Algebraic Structures. We will explore the feasibility to model SDCs' resources (e.g., compute, storage) using algebraic structures. Researchers have recently showed that routing can be modeled as follows: each route has a signature ($\sigma \in \Sigma$) to model its relative precedence, and the notion of link weights is generalized to policy labels. When a route with signature σ is extended over a link (e.g., u - v), with policy label $\lambda \in L$, the route's new signature becomes $(\lambda \oplus \sigma) \in \Sigma$. In other words, a signature represents the set of a route's attributes, a label represents the set of routing policies when a route is propagated over a given link, and $\oplus$ symbolizes the application of the routing policies to a route. A relation $<$ is called a preference relation and creates a total pre-order over Σ. It allows routers to rank routes.

Properties of routing policies can then be defined and reasoned about. For example, strict monotonicity (SM) is defined as $\forall l \in L, \forall \sigma \in \Sigma, \sigma < (l \oplus \sigma)$. Similarly, can we model resources (e.g., compute, storage) and associated operations as algebraic structures, and identify sufficient and/or necessary conditions for global network wide properties? We first will review abstractions that have been suggested to advertise and exchange different resources (e.g., storage, compute) across different fields (e.g., grid computing, federated clouds), and identify relevant operations for each type of resource (e.g., how to advertise and aggregate storage resources). We will then model them using algebraic structures, and sufficient local conditions for different properties.

S2.3 Global Negotiation: Integration of Negotiation. We plan to incorporate a negotiation component into inter-SDC communications to allow coalition members to agree on the desired global properties, and we will design mechanisms (e.g., local constraints) to ensure that the corresponding sufficient conditions are met. We will build upon our previous work which presented a theoretical framework to provide various properties in the

[25] Timothy G. Griffin, and João Luís Sobrinho, "Metarouting," In *Proceedings of the ACM SIGCOMM 2005 conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '05)*, pp. 1-12, Philadelphia, PA, USA, Aug. 22-26, 2005. Proceedings published as *Computer Communication Review (CCR)*, vol. 35, no. 4, pp. 1-12, Aug. 2005.

interconnection of autonomous entities[26,27]. We will also investigate the possibility of previous work on distributed algorithmic mechanism design (DAMD) and look into basic impossibility results in composition (e.g., Arrow' Impossibility Theorem[28])).

Subtask 2.4: SDC Architecture Modelling, Formalization and Integration

Subtasks 2.1-2.3 are based on abstractions and decomposition. Subtask 2.4 investigates instantiation and integration. Since there are few studies focused on the mathematical modeling and formalization of SDC architectures, our technical approach is to use the tools of queuing theory, graph analysis, mixed integer nonlinear programming, and other needed formalisms to rigorously investigate instantiation and integration, with simulation and system implementation also playing a crucial role. Subtask 2.4 consists of the following steps:

S2.4 Arch Modelling: Multi-domain SDC Architecture Modelling. Current SDC architecture comparisons are ad-hoc and not based on a rigorous understanding of their operations. In particular, there is no rigorous modeling in various use case scenarios, e.g., disaster relief, warfighting, etc. Neither is there a thorough analysis and comparison on realization architectures, including (i) single controller, (ii) hierarchical controllers, or (iii) peer level controllers. Although our preliminary studies[29] have compared these 3 architectures with regard to the metric of coalition formation success, we plan to refine this initial approach to evaluate and discover other topologies with potentially better capabilities and also augment the East-West Interface among domain controllers. This step will also model how a distributed controller architecture will interact with neighboring domains via the East-West interface.

S2.4 Formal Analysis: SDC Security, Privacy, and Correctness Formal Analysis. SDC increases flexibility but may also increase risks. Informal or experimental analysis on security, privacy, and correctness of complex SDC control planes can leave serious issues uncovered. Hence, a key challenge is whether there are effective, formal methods to rigorously ensure security, privacy and correctness. In particular, a coalition member may require that minimum or bounded information be exposed, and we plan to utilize rigorous methods, in particular, *differential privacy,* to conduct formal analysis and definitions. We also plan to integrate formal specification methods recently developed in program verification, in particular[30], to verify the security and correctness of SDC programming and interconnection.

S2.4 Cross Paradigm: Cross-Paradigm and Technology Integration. A key complementing technique to SDC is content or information centric networking (CCN/ICN), which is a desired capability in SDC for warfighters' needs to access secure name-based contents in dynamic situations. Hence, the impacts of such networks on SDC, particularly their integration, should be investigated. We plan to develop an integrated interconnection and replication for CCN and SDC. We also plan to go beyond infrastructure to investigate the integration with slices and applications.

Military and DAIS ITA Relevance

In tactical networks, coalition partners may deploy network devices with heterogeneous computing, storage, and communication capabilities. To enable flexible, effective, and robust services in coalition networks, SDN-based network architecture has been proposed to address these coalition needs with dynamic configurability. Existing SDN

---

[26] Franck Le, Geoffrey Xie, and Hui Zhang, "Theory and New Primitives for Safely Connecting Routing Protocol Instances," In *Proceedings of the ACM SIGCOMM 2005 conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '10)*, pp. 219-230, New Delhi, India, Aug. 30-Sep. 3, 2010. Proceedings published as *Computer Communication Review (CCR)*, vol. 40, no. 4, pp. 219-230, Oct. 2010.

[27] Franck Le, and Joao Luis Sobrinho, "Interconnecting Routing Instances," In *IEEE/ACM Transactions on Networking (ToN)*, vol. 22, no. 2, pp. 540-553, Apr. 2014.

[28] Kenneth J. Arrow, "A Difficulty in the Concept of Social Welfare," Journal of Political Economy, vol. 58, no. 4, pp. 328–346, 1950.

[29] Vinod Mishra, Dinesh Verma, Chris Williams, and Kelvin Marcus, "Comparing Software Defined Architectures for Coalition Operations," In *Proceedings of the 2017 IEEE International Conference on Military Communications and Information Science (ICMCIS '17)*, pp. 1-7, Oulu, Finland, May. 15-16, 2017.

[30] Ronghui Gu, Jérémie Koenig, Tahina Ramananandro, Zhong Shao, Xiongnan (Newman) Wu, Shu-Chun Weng, Haozhong Zhang, and Yu Guo, "Deep Specifications and Certified Abstraction Layers," In *Proceedings of the 42nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL '15)*, pp. 595-608, Mumbai, India, Jan. 15-17, 2015. Proceedings published as *ACM SIGPLAN Notices*, vol. 50, no. 1, pp. 595-608, Jan. 2015.

techniques rely on centralized control and synchronization protocol design. However, constructing task flows between two coalition enclaves (domains) using the synchronized information in a distributed manner is of paramount importance. Unfortunately, complete inter-enclave synchronization is almost impossible in hostile environments. For instance, the coalition infrastructure could be fragmented, and thus the synchronized information from coalition partners is only limited, or even out of date. With such constrained information and potential network dynamics, it remains unknown how they affect the performance of SDC-based coalition networks. The main objective of Task 1 is to investigate and acquire the fundamental understanding of how the SDC management architecture can support various operational scenarios and dynamics in a distributed way, while achieving the performance required by network commanders, and then shedding new insights into future tactical network design and architecture enhancement.

Military coalition operations can benefit from the efficient, agile, optimal software-defined coalition (SDC) infrastructure. Toward this end, the high-level, SDC-intensive programming abstractions, as to be investigated in Task 2, can automate many aspects of war fighters' tasks in setting up and operating an SDC infrastructure, improving agility, reducing misconfigurations, and avoiding security risks, in complex, contested settings, when making relevant information, data, and resources available at the point of need. The SDC abstraction calculus and composition algebra will result in better integration of resources from highly agile SDC members. The modeling, formal methods and integration efforts can lead to higher levels of assured security, privacy and correctness. These issues will be investigated in Task 2.

Demonstrations of technology: We plan to conduct multiple demonstrations, ranging from for individual components to for the overall project. To demonstrate the benefits (e.g., simplicity and automation) of SDC-intensive programming, we plan to implement multiple control-plane use cases in real settings[6]. To demonstrate the benefits of the SDC abstraction calculus and composition algebra, we will demonstrate the substantial reduction in overhead and effectiveness of utilizing the aggregated resources in real settings[6]. We also plan to demonstrate provable correctness for SDC configurations.

Transition possibilities: From our research in Task 1 of controller synchronization, we shall provide in-depth understanding of the effect of potential network fragmentations and deployable distributed algorithms in military scenarios, e.g., CERDEC. In the UK, these aspects of research in Task 1 could feed into the existing Dstl research AI2 area, and hence Morpheus program under BATCIS, as well as related programs in Joint Force Command (JFC).

As far as the controller abstractions and formal methods in Task 2 are concerned, we envisage several potential transitions both within and outside ITA. Within ITA, our Task 2 research is of particular interest to IBM, in federated clouds where resources (e.g., compute, network, storage) from several sources are composed together to perform a common action (e.g., deploy and manage a cloud computing service); we plan to explore the transition of the SDC-intensive programming models and the SDC formalization tools to ARL. Outside ITA, we will take advantage of IETF to define Internet standards (e.g., SDC calculus as a new inter-domain protocol framework, for example in IETF working groups), OpenDaylight and ONOS to make our systems available, and our collaborators (Brocade and Broadcom) to make the software into commercial products.

Collaborations, Staff Rotations, and Linkages

Intra-Alliance Collaborations and Linkages

In terms of intra-Alliance collaboration, both Tasks 1 and 2 of P1 are highly related to Task 1 "Control of SDC for Distributed Analytics" of P3. Specifically, the latter will develop distributed mechanisms to allocate resources, the effectiveness of which is affected by the controller placement; the degree of controller synchronization includes the details of resource status information to be shared among domains (e.g., only coarse information from a distant domain, while full details available from a neighboring domain). Task 2 of this project provides programming and communications abstractions to realize their resource control with high-level abstractions (e.g., automated mapping to heterogeneous datapath), in a larger context (e.g., effectively composed with security policies), and with the ability of formalization (e.g., on correctness); their demand can help us identify abstractions. As we plan to study to what extent such resource-specific partial synchronizations can affect the overall performance, this aspect of the work will be carried out jointly with Task 1 of P3 where mathematical models to represent resource status will be developed.

Both Tasks 1 and 2 here are also related to TA2-P4 Task entitled "Resource Allocation for Dynamically Formed Distributed Analytics Services," which will study models representing availability of various resources, while the synchronization and abstractions of such model parameters among SDC controllers will be investigated here. We plan to maintain close contacts and exchange latest results with P4 colleagues in order to explore synergies between the efforts.

Task 2, in particular S2.1 and S2.3, can have a strong policy component, and there is a potential to design a unifying framework integrating both SDC control and SDC policy in a coherent, unified framework. We plan to maintain close contacts and exchange latest results with P2 colleagues in order to explore synergies between the efforts.

Staff Rotations

Investigators and students of P1 will participate in periodical conference calls and have mutual visits to ensure steady progress of our research. In particular, members from the Imperial and UCL teams plan to visit colleagues at IBM U.S., Yale and ARL during the summers of 2018 and 2019 for technical exchanges and collaborations. Members of the academic team are planning to visit ARL during the summers of the BPP.

Research Milestones		
Due	**Task**	**Description**
Q1	**Task 1**	Report, conference or journal submission(s): Generic closed-form expression of the performance metric of the constructed flows in synchronized sub-networks under constrained source/destination locations (Imperial, IBM U.S.); Models to capture different types of synchronizations or fragmentations (IBM U.S.).
Q1	**Task 2**	Report: dynamicity, weakly-connected programming design (S2.1 Dynamicity; Yale, IBM, ARL); Design of SDC intensive programming supporting cross-packet streams, (S2.1 Crosslayer; Yale, IBM); Report: formulation of abstraction complexity (S2.2-Abstraction Complexity; Yale, IBM); Report: routing state abstraction (S2.2 Abstraction Calculus; Yale, IBM, Dstl).
Q2	**Task 1**	Reports: Performance bound of the most basic SDC-based flow construction strategy under the simple synchronization model (Imperial, IBM U.S.); Emulating various commercial controller implementations to quantify and analyze costs of synchronization among controllers (Yale).
Q2	**Task 2**	Report: SDC-intensive programming including control-plane spec for computation and storage (S2.1 Crosslayer; Yale, IBM); Report: initial set of identified global properties (S2.3 Global Properties; IBM); Survey of current abstractions for different resources (S2.3; IBM); Validation and experimentation: initial version of SDCbench (ARL, IBM, Yale);
Q3	**Task 1**	Conference or journal paper(s):

Research Milestones		
Due	**Task**	**Description**
		Performance bound of different SDC-based flow construction strategies under various synchronization models and network dynamics (Imperial/IBM U.S.); Algorithms for controller placement and node assignment under various cost constraints and dynamic coalition network requirements (Yale).
Q3	**Task 2**	Validation and experimentation: Design and evaluation of dynamicity-oblivious model using SDCbench (Yale); Paper: results on SDC architecture modeling (S2.4 Arch Model; ARL/Vinod, UCL).
Q4	**Task 1**	Powerpoint slides: Extending the above results to weighted graphs (Imperial, IBM U.S.); Software: Developing simulation frameworks for validating the accuracy of the above analytical results (Imperial, Yale, IBM UK).
Q4	**Task 2**	Report: wireless datapath design (S2.1 Datapath; Yale); Report: global property modelling and analysis (S2.3 Global Model; IBM); Report: formal specification on formal methods (e.g., Coq) for verification of correctness (S2.4 Formal Method; ARL/Vinod); Validation and experimentation: Finalization of initial version of SDCbench (Yale, ARL/Kelvin).
Q5	**Task 1**	Conference or journal submission(s): Performance quantification of SDC-based flow construction strategy under heterogeneous per-domain synchronization policies; revealing how synchronization policies and network graphical properties affect the overall performance (IBM U.S.); Comparison between flat and hierarchical controller structures with respect to military-relevant performance metrics (Yale)
Q5	**Task 2**	Report: final set of global properties (S2.3 Global Properties; IBM); Paper: SDC interconnection with adaptive programs (S2.2 Abstraction Calculus; Yale, IBM, Dstl); Validation and experimentation: Initial release of SDCsim (Yale, ARL, UCL).
Q6	**Task 1**	Report(s): Algorithms for placing gateway nodes in each domain under various cost constraints and network conditions (Imperial/IBM UK); Controller structure design for various coalition network requirements (Yale, IBM U.S.)
Q6	**Task 2**	Paper: automated weakly- or disconnected- programming (S2.1 Dynamicity; Yale, ARL); Report: results of composition algebra condition (S2.3 Global Model; IBM, Dstl);

Research Milestones		
Due	**Task**	**Description**
		Report: initial integration with CCN (S2.4 Cross Paradigm; ARL/Vinod, UCL).
Q7	**Task 1**	Conference or journal submission(s), or slides: Algorithms for forced fragmentation and improved synchronization policies (IBM U.S., Imperial); Extensions for gateway/controller placement under enforced synchronization policies (Yale, IBM U.S.)
Q7	**Task 2**	Paper: diverse datapath design and validation (S2.1; Yale); Report: design of negotiation with secure computation and DAMD (S2.3 Negotiation; Yale, IBM, Dstl); Validation and experimentation: Formalization of both correctness and security (S2.4 Formal Analysis; ARL/Vinod, UCL).
Q8	**Task 1**	Report and demo: Evaluations of the developed analytical results and algorithms based on ITA experimental facilities, SDN devices, and real military network traces (Imperial, Yale, IBM U.S., IBM UK)
Q8	**Task 2**	Paper: overall paper on SDC-intensive programming for dynamicity and cross-resources (S2.1; Yale); Paper: overall communication abstraction calculus (S2.2; Yale, IBM); Report: global properties with negotiation mechanism design (S2.3 Global Model; IBM, UCL); Report on feasibility of integration of CCN and policies (S2.4 Cross Paradigm; ARL/Vinod, UCL).

Project 2: Generative Policy Models for Coalitions

Project Champion: Elisa Bertino, Purdue

Email: bertino@cs.purdue.edu **Phone: 765-496-2399**

Primary Research Staff	Collaborators
Alessandra Russo, Imperial	Chris Williams, Dstl
Amani Abu Jabal (PGR), Purdue	Geeth de Mel, IBM UK
Anand Mudgerikar (PGR), Purdue	Irene Manotas, IBM US
Dinesh Verma, IBM US	John Ingham, Dstl
Elisa Bertino, Purdue	Maryam Davari, Purdue
Emil Lupu, Imperial	Seraphin Calo, IBM US
Maroun Touma, IBM US	Supriyo Chakraborty, IBM US
Nigel Wheadon, BAE Systems	
Alan Pilgrim, BAE Systems	
Saritha Arunkumar, IBM UK	
Shahi Shahrokh (PGR), Imperial	
Brian Rivera, ARL	
Greg Cirincione, ARL	
Unnamed PDR, Imperial	

Project Summary/Research Issues Addressed

Different parts of a coalition are governed by their own sets of policies defined as directives used to guide their actions. The vision of a distributed coalition intelligence requires a dynamic, secure and resilient information infrastructure that needs to conform to the policies of each coalition member. The appropriate policy based management framework will help to attain key attributes such as autonomous operation, composing systems together, and controlling interaction among elements.

Policy technologies have been used successfully in management of IT systems and networks, but prevalent approaches tend to rely on rule-based systems that rely on centralized services. Coalition environments are highly dynamic, distributed, and heterogeneous, frequently without access to a centralized infrastructure. Although

advances have been made for policy enforcement in coalition operations[31], many challenges remain in addressing the high degree of dynamism and mobility encountered in coalition operations.

In coalition environments, policy issues need to address characteristics of the humans involved in the missions as well as the computer systems involved. Current policy approaches are computer-centric and do not take such considerations into account. New policy models that can adequately capture human aspects, both cultural and sociological are needed.

The current state of the art in policy management infrastructures focuses on automated enforcement of directives. However, in a dynamic coalition environment, blind enforcement of predefined policies may prevent the delivery of a critical piece of information from a coalition partner that may be important for mission effectiveness. Policy infrastructures for coalitions must provide for the ability to trade-off mission effectiveness against policy relaxation, and support policy adjustment and negotiation to maximize mission effectiveness while minimizing risk. Current infrastructures for policy fail to live up to this challenge. It is also important to notice that generative policy techniques can be instrumental in enhancing the security management to make it possible to better support context- and mission-based security. However it is also critical that generative policy management do not introduce vulnerabilities that can be exploited by adversaries.

In the IPP phase of the program, researchers working on the program have designed an architecture for generative policies[32]. Also, an initial set of policy quality requirements has been devised for role-based access control policies[33]. This proposed project will substantially expand these preliminary results by undertaking two tasks:

- *Generative Policy Analytics: Theory, Method and Tools*: We will undertake research in the areas of 1) developing formal foundations for policy analytics, 2) identifying a comprehensive set of policy quality metrics, and 3) designing methods for metrics evaluation and automatic policy evolution.

- *Dynamic Policy-Based Autonomous Management of Security in Coalition Environments using Generative Security Policies:* We will undertake research in 1) exploring security metrics to characterize security of systems using generative policies 2) using machine learning techniques to automatically generate security policies for future coalition systems, and 3) expanding and customizing the algorithms in the first task to take into account the special nature of security applications.

Task 1: Generative Policies Analytics – Theory, Method and Tools

Primary Research Staff	Collaborators
Alessandra Russo, Imperial	Christopher Williams, Dstl
Amani Abu Jabal (PGR), Purdue	Dinesh Verma, IBM US
Elisa Bertino, Purdue	Geeth de Mel, IBM UK

[31] Calo, S. B., Karat, C. M., Karat, J., Lobo, J., Craven, R., Lupu, E., … & Bandara, A. (2010). Policy Technologies for Security Management in Coalition Networks. Network Science for Military Coalition Operations: Information Exchange and Interaction, 146.

[32] D. Verma, S. Calo, S. Chakraborty, E. Bertino, C. Williams, J. Tucker, B. Rivera. Generative Policy Model for Autonomic Management. IEEE SmartWorld Congre– -- International Workshop on Distributed Analytics Infrastructure and Algorithms for Multi-Organization Federations, August 2017.

[33] E. Bertino, A. A. Jabal, S. Calo, C. Makaya, M. Touma, D. Verma, C. Williams. Provenance-based Analytics Services for Access Control Policies. IEEE Service Congress, 2017.

Primary Research Staff	Collaborators
Maroun Touma, IBM US	Irene Manotas, IBM US
Saritha Arunkumar, IBM UK	Maryam Davari, Purdue
Shahi Shahrokh (PGR), Imperial	Nigel Wheadon, BAE Systems
Brian Rivera, ARL	Seraphin Calo, IBM US

Future coalition military activities and missions will be carried out by autonomous groups of devices with a large variety of cognitive capabilities. These devices will operate in environments characterized by uncertainty, insecurity (both physical and cyber), and instability. In such environments, communications may be fragmented. Proper policy-based management of such autonomous device groups is thus critical. However current policy management systems (PBMSs) have limitations, including lack of flexibility, autonomy, and manual policy definition. Generative policies have emerged as the key approach to address such limitations for the self-autonomous management of parties in next-generation coalition settings. In such a setting, the managed parties (devices, agents, etc.) are provided an initial policy specification, referred to as *generative policy*. Each party can then (dynamically) refine and adapt the generative policy, and generate its own "customized" policy, referred to as *instantiated policy*. Such an approach has several advantages, including reduced cognitive/manpower burden, response timeliness, and adaptation capabilities.

A critical requirement in the above setting, as well as in conventional settings, is the specification of suitable policies. Policies are the main input for management decisions made by different parties in a PBMS. A critical requirement is to ensure that such policies are of "good quality". The deployment of a PBMS in the context of activities carried out by autonomous parties increases the difficulty of assuring the quality of policies. Such parties have often to operate in volatile, uncertain, complex and ambiguous environments. Parties may have to dynamically join different coalition operations characterized by different missions. In such contexts devising in advance all possible needed policies and making sure that they are of good quality is difficult, if not impossible. We need a different approach by which the policies may have to dynamically evolve based on situations encountered by the parties. An important motivation for policy evolution is the need of policy de-confliction as in the generative policy setting, a device may locally generate a policy that may conflict with the policies of the other devices, or a device may join a new coalition operation and its policies be in conflict with the policies for the new operation. Determining when and how to evolve policies (generative and/or instantiated) requires suitable metrics for assessing policies' quality. We also need mechanisms for collecting the data for policies assessment and criteria and methods for automatically evolving the policies. All such issues have to be addressed for both generative policies and instantiated policies.

In summary, this project aims to address the following key scientific questions:

i) how to dynamically compute instantiated policies from (incomplete) generative policies in a context-aware manner;
ii) how to evaluate the quality of policies statically, for generative policies, and at run-time for instantiated policies;
iii) how to automatically evolve policies and guarantee their quality in the presence of uncertain and volatile environments.

This project aims at addressing the above challenges by developing a comprehensive analytical data-based framework for generative policies. The framework will include different policy quality analysis techniques and will exploit data collected from the managed systems and parties to assess the quality metrics and identify policy changes. A key distinguishing aspect of our approach is the recognition that initial policy specifications will often be incomplete or inadequate to manage a given set of parties and thus the actions taken by the managed parties may diverge with respect to the policies. Therefore, we need to identify such divergences in order to execute proper management actions to reduce these divergences.

The technical approach underlying the development of our policy quality framework combines different research building blocks discussed in what follows. For each building block, we emphasize research challenges and expected novel results.

(i) *Formal models for generative policies.* To date there is no mechanism for devices to automatically generate policies that meet their own policy requirements and that take into account information of the entities in the domain with which the devices have to operate. Many policy languages[34], based predominantly on "event-condition-action" paradigm, relay upon administrators to manually handcraft the policies needed to manage a system, and assume a central administration point that defines in a prescriptive way the actions to be taken under various conditions by the managed devices. Work carried out by DAIS ITA IPP has proposed the notion of generative policies. But no formal models of this new notion of generative policies have been developed. The definition of such models is critical to support formal reasoning methods on policies. Such models must provide constructs for specifying the generative policies structures, the instantiated policies, that are locally generated, and the relationships between the two.

We thus plan to develop a formal model for generative policies. This will include a formal language for specifying the structures of generative policies, a semantic underpinning that defines the properties that structures of the generative policies have to satisfy, and efficient algorithms for the inference of instantiated policies from given structures of generative policies. The language will allow the specification of production rules, whose "terminal" constructs will be declarative primitives of the low-level policies needed by the devices, whereas the intermediate constructs will capture structure operators for composing the primitive constructs into full declarative policies.

Different classes of generative policies will be defined to allow for the production of different types of network and security policies (e.g. obligation, authorization and access control policies). Each such class will be labeled by the type of devices it targets, and such label will provide the start symbol of the grammar rules. General properties will be defined over the grammar (e.g. circular dependencies, stratification) to verify the well-formedness of the generative policies that the grammars are able to infer. Efficient (top-down) algorithms will be developed for automatically generating instantiated policies from specific grammars. These algorithms will take into account not only the grammars but also contextual/domain information, to appropriately ground the instantiated policies in different parts of the networks, and constraints over the generative policies to help preserve consistency across policies instantiated in different devices.

We expect different instantiated policies to be derivable from the same generative policy when contexts are different. Depending on the algorithm used to derive the instantiated policies, techniques might be required for verifying that formal properties specified at the level of the generative policies also hold for the instantiated policies. Similarly, analysis techniques will be developed for checking that existing instantiated policies "conform" or are "recognized" by a new given grammar. Such a situation may occur when a managed party is given a new generative policy in the context of a new collaborative mission and may already have policies that may be used for the new mission.

(ii) *Policy quality metrics.* To date there is no comprehensive set of policy quality metrics. Past work mainly focused on consistency of policy sets, notably in the area of access control policies. Previous work by the DAIS ITA IPP Project P2 has identified several quality metrics for policy sets, namely: consistency, minimality, completeness, relevance. Some of these metrics, e.g. consistency and minimality, can be evaluated by only inspecting the policy sets. Others, e.g. completeness and relevance, must be evaluated by comparing the policies with respect to the actions executed by the managed parties. We plan to expand this initial set of metrics with additional formally defined metrics. We will analyze the requirements identified in the field of data quality[35] to understand what their meaning and applicability are for policy systems. In addition, we will investigate two additional metrics: enforceability and risk. "Enforceability" indicates whether a policy can actually be enforced by a managed party in a certain context and at which cost. For example, a policy may require contextual information be acquired in real time and it is crucial to provide indicators about the feasibility of the policy enforcement. The risk metric quantifies possible risks that may result from the application of a policy (or set of policies). For example, a restrictive access

[34] H. Weili, and L. Chang. A survey on policy languages in network and security management. Computer Networks 56.1 (2012): 477-489.

[35] As an example, 15 different data quality requirements are identified in "Data and Information Quality" (by Batini and Scannapieco, Springer 2016).

control policy may prevent the delivery of relevant information needed by a party. All the metrics apply to both the generative policies and the instantiated ones; however their definitions may differ depending on the formal models adopted for the generative policies and the instantiated policies. Thus, we will develop different definitions for different formal models.

(iii) *Methods for assessing policy quality*. Several policy analysis methods have been proposed[36] including methods based on model checking, SAM and SAT solvers, abductive reasoning. However these previous methods have been defined only for "conventional" policy settings and do not cover generative policies. In addition, they suffer from one or more drawbacks: (i) are tailored towards specific requirements (typically, consistency), and (ii) require advanced knowledge of all possible actions executed by the managed parties.

We will develop methods for overcoming those drawbacks. We will develop two complementary categories of methods: static methods, which require to only analyze policies, and dynamic methods, which require analyzing the behavior of the system and comparing it with the policies. The static methods will be defined for both generative and instantiated policies. Analysis of generative policies will include equivalence, subsumption, compositionality of generative policies, whereas methods for instantiates policies will include enforceability, lack of coverage, risk assessment in given domains, and modality conflicts, for which existing analysis tools will be appropriately extended[37]. Dynamic methods for assessing policy qualities are particularly critical in our setting as the high dynamicity and non-deterministic nature of the heterogeneous coalition environments can make instantiated policies perform unexpectedly. This may be because policies are incomplete, or because changes in the environment make existing policies no longer enforceable. These methods will evaluate the execution traces of the system with respect to the policy quality metrics (Task 1.ii) and in case of divergence (e.g. violation, failure) they will diagnose the causes, e.g. parts of the policies that are not enforced, or that lead to unwanted behaviors. We expect these dynamic methods to work on both complete and incomplete execution traces. In the latter case, the quality of the policies will be conditional to properties over possible extensions of the traces. Dynamic methods will need to be supported by data collection tools[38] for gathering execution traces and other information from the monitored devices. By using these tools, we can observe whether the actions executed by the managed parties differ with respect to the policies. We plan to use the SimP provenance system designed by the Purdue University team as such system collects not only the actions executed by the parties, but also which policies (if any) were enforced. The current design of SimP only focuses on access control policies. However we will extend it to support other policies, such as policies for software defined coalitions (SDC), and to also capture the policy generation, and policy checking and enforcement actions executed in the system. By using such logs, we will be able to determine whether some policies were checked and the managed parties complied with the policies, or whether the parties did not comply with the policies, or even if no policies were checked at all. Thus our SimP system will be extended with the inclusion of a component specialized on monitoring all activities related to policies from generation to enforcement and modification.

Finally, analysis of policy quality will be executed at two different levels: locally at each device and globally at the policy management party (e.g. the party that specifies the generative policies). This is because instantiated policies may result to be optimal with respect to the device local conditions, however they may be less optimal at a global level. Such lack of optimality can only be detected by carrying out policy analysis at the global level by combining analytic results obtained locally from the various devices. The analysis results will then be used to automatically revise existing instantiated policies and drive the evolution of generative policies (Task 1.iv) by achieving the optimal trade-off between locally-driven vs globally-driven policy instantiation.

(iv) *Methods for automatic policy evolution*. The ability to automatically evolve policies is key to the autonomous management of parties in next-generation coalition settings. Existing approaches are based on predefines changes, e.g., run-time modification of policy parameters or dynamic selection of policies from

[36] D. Lin, P. Rao, E. Bertino, N. Li, and J. Lobo. EXAM: a comprehensive environment for the analysis of access control policies. International Journal of Information Security 9, no. 4 (2010): 253-273.

[37] Robert Craven, Jorge Lobo, Jiefei Ma, Alessandra Russo, Emil C. Lupu, Arosha K. Bandara. Expressive policy analysis with enhanced system dynamicity. ASIACCS 2009: 239-250.

[38] A. Abu Jabal, and E. Bertino. SimP: Secure interoperable multi-granular provenance framework. Proceedings of the 2016 IEEE 12th International Conference on e-Science, Baltimore, MD, USA, October 23 – 27, 2016.

predetermined sets of policies[39]. These approaches are limited. Devices should be capable of using execution traces and the outcomes of the assessment of policy quality (Task 1.iii) to automatically evolve existing policies in order to resolve detected divergence and conflicts between execution logs and policy specifications. We will leverage results in symbolic machine learning[40] to support policy evolution. Because of its general-purpose nature, symbolic machine learning will be used to support automated evolution of both generative and instantiated policies. Results from static analysis (e.g. modality conflict and lack of coverage) will be considered as negative examples to completeness and consistency of generative policies and used by the symbolic machine learning algorithm to automatically learn changes to existing structures of generative policies, needed to resolve detected incompleteness and inconsistencies of these policies. Run-time assessment of quality of instantiated policy (e.g. example logs of lack of compliance with instantiated policies) will also be seen as counter-examples of good quality execution behaviors, and will be used to automatically learn evolutions of instantiated policies, within the context of given generative policies. Evolved instantiated policies will enable devices to avoid future ill behaviors in similar contextual circumstances, so improving the quality of their instantiated policies over time. The evolution of generative and instantiated policies can happen in any order and be interdependent where necessary. The proposed automated learning of evolution of policies will build upon formal semantics foundations that will enable the technique to guarantee properties such as minimal changes, preservation of existing good behaviors, and satisfiability of domain specific constraints where needed.

Validation

We will validate our research from both a theoretical and experimental point of view. From a theoretical perspective, we will prove the correctness of our algorithms for inferring instantiated policies from given generative policies developed in Task 1(i), evaluate their complexity depending on the level of expressiveness of the generative policies, and measure their efficiency in terms of computational time. Similar evaluations will also be applied to the techniques for assessing the quality of policies (Task 1 (iii)) with respect to the metrics developed in Task 1(ii). For the policy evolutions (Task 1(iv)), a synthetic evaluation mechanism will be developed to assess the convergence of the learning-based revision and evolution algorithms depending on the size and diversity of synthetically generated execution traces. This will allow us to measure the performance of our techniques in an unbiased way and under stress conditions.

Using a scenario-based approach, we will analyze the requirements for specific use cases including firewall security and moving target defense. . Through linkage activities we will also analyze requirements concerning policy scenarios in SDC (Project P1) and in agile composition of code and data (Project P3). For each of the use cases, we will develop and end-to-end flow and provide proof points on how our proposed approach meets the coalition requirements for secured access control and protection against enemy attacks and for effective deployments of SDC and compositions of code and data. All use cases will include an element of variability introduced via dynamic behavior of the protected assets (for the security policies) and of the involved resources (for the SDC and the agile composition of code and data).. For each of the use cases, we will use a model simulator to a) demonstrate how our proposed model can be used to instantiate well-formed policies from high level constructs defined by the coalition; b) exercise the instantiated policies in our simulator to demonstrate how they meet the needs of different coalition missions with different security constraints or performance constraints; c) for each scenario, use the policy quality metrics we define to analyze and explain the trade-off between enforceability and risk at the device level as well as at and coalition/mission level. Using simulation, we will further demonstrate that, under specific test conditions, the instantiated policies derived using our model are well formed and that the formal properties of the high level generative policies hold such that a security policy on a specific asset can be relaxed without compromising the established coalition practices for security and access control. A similar analysis will be carried out for policies

[39] Leonidas Lymberopoulos, Emil Lupu, Morris Sloman. An Adaptive Policy-Based Framework for Network Services Management, Journal of Network and Systems Management, September 2003, Vol.11(3), pp 277–303.

[40] Mark Law, Alessandra Russo, Krysia Broda. Iterative Learning of Answer Set Programs from Context Dependent Examples. TPLP 16(5-6): 834-848, 2016.

related to SDC and to composition of code and data. By using model simulation we can further assess the overall performance of our proposed model for generative policies from a functional as well as non-functional requirements.

From an experimental point of view, we will develop a simulation testbed consisting of different devices with their own generative policies. This testbed will allow us to experimentally assess the generation of instantiated policies, collection of data for evaluation, on a large-scale, of our algorithms, and the "adequacy" of our set of metrics. In the latter case we will create different example scenarios and assess specifically, whether the proposed metrics are sufficient for most applications or whether additional metrics are required. Results of the simulations will be discussed with experts from both governments and industry.

In this context, experimentation will focus on demonstrating how our proposed model, metrics and tools are used by the coalition to generate specific policies for a particular mission and provide a qualitative measurement of the generated policy. Each experiment will be modeled based on real-life situations commonly encountered by coalition members, it involves multiple assets from different coalition members and also includes an element of uncertainty where mission requirements, and therefore the instantiated policies, may change during the course of the mission.

Military and DAIS ITA Relevance

Our approach addresses key requirements of future coalitions including: a verifiable model for independent policy generation by different assets; quality metrics for enforceability, risk assessment and conformance with the mission goals and the coalition members own rules of engagement; new algorithms for analyzing the run-time behavior of the system in coalition environments; new methods for contextual policy evolution such that policies can be localized and adapted to changing needs.

During coalition missions, we consider those scenarios where policies are used to coordinate the activities of different coalition members' assets in an effort to protect those assets and secure the flow of information between them. During the IPP, we have demonstrated that Generative policies are key to streamline mission operation by providing the appropriate degree of autonomy for coalition assets, so that they can derive the specific rules governing their field operations from high-level constructs defined by headquarters. Given the dynamic field of operations of coalition missions, our proposed formal model and advanced analytical capabilities will provide the mission commander and coalition partners with the metrics for assessing the quality of generated policies w.r.t the mission objectives and conformance with the constraints imposed by the coalition members. Given the complexity of the environment under which such missions are conducted and the diversity of assets they use, our model will accelerate the pace at which coalition missions are formed. It will significantly reduce the burden on the soldier and the time that humans traditionally spend on defining, reviewing and enforcing the policies.

To ensure relevance to military applications, the implementation and demonstration of our techniques will be based on a simulated environment representing two use cases: one from a military coalition scenario and another one from a civil services/NGO scenario. The emphasis will be on self-organizing autonomous systems and decision making that reflects the level of autonomy of the assets.

We see a growing interest for civilian and military applications for cognitive autonomous systems that can collaboratively work towards specific goals. Such systems must exhibit an adaptive behavior and a high-degree of autonomy for decision-making based on the specific operation context. We believe this market to be also a prime target for transition opportunity that we will pursue with IBM and other industrial partners in the DAIS ITA.

Task 2: Dynamic Policy-Based Autonomous Management of Security in Coalition Environments using Generative Security Policies

Primary Research Staff	Collaborators
Anand Mudgerikar (PGR), Purdue	Brian Rivera, ARL

Dinesh Verma, IBM US	
Elisa Bertino, Purdue	John Ingham, Dstl
Emil Lupu, Imperial	Seraphin Calo, IBM US
Nigel Wheadon, BAE Systems	Supriyo Chakraborty, IBM US
Alan Pilgrim, BAE Systems	
Saritha Arunkumar, IBM UK	
Greg Cirincione, ARL	
Unnamed PDR, Imperial	

Generative policies enable devices to generate their own policies that are validated, consistent and conflict free. The autonomy provided by generative policies can be applied in many domains of systems management, but a domain like security has several considerations that cannot be addressed in a generic way. In this proposed research work, we will investigate how devices involved in security enforcement can automatically generate their security policies -- enabling policy-based autonomous security management.

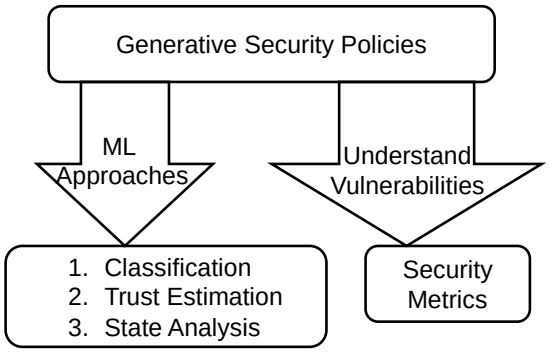

Figure P2-1. Research Trusts in Security Policies

The proposed research will increase autonomy of security devices, which is critical for effective security management in contexts that are highly dynamic and where subsystems can become disconnected from human administrators. While our work would be synergistic and consistent with the general architecture and analysis algorithms explored in the generative policy area, our primary focus will be on addressing the unique challenges that arise in the security domain[41]. These challenges include both exploring approaches to generate security policies automatically as well as estimating the security characteristics of this approach in different coalition contexts, and to understand the fundamental bounds on the performance of different algorithms for security policy generation. The work substantially extends the preliminary work on generating security policies done in the IPP around security appliances[42], security in virtualized environments[43], and has two broad thrusts as shown in Figure P2-1.

[41] It may be possible for some of our approaches to be used in other domains beyond security.

[42] S. Arunkumar et. al, Next Generation Firewalls for Dynamic Coalitions, IEEE SmartWorld Congress -- International Workshop on Distributed Analytics Infrastructure and Algorithms for Multi-Organization Federations, August 2017.

The key scientific question that this project aims to address is whether a generative-policy approach based on machine learning for policy refinement is a suitable approach to enhance flexibility without undermining security. The main reason for the use of machine learning techniques is that these techniques are today mature and already widely used in security for anomaly detection. However they have not yet been widely applied to other security tasks, such as access control, and trust management. We believe that the combination of generative policies and machine learning techniques will result in approaches suitable for distributed rapidly changing environments. A second reason for the use of machine learning is specific to the context of the DAIS-ITA initiative in which approaches and infrastructures are designed to support distributed analytics. We believe that we can leverage these techniques to further enhance the efficiency of security tasks.

To explore *security-specific approaches for policy generation*, we will study three different approaches to apply machine learning to generate security policies. Applying machine learning to security for policy generation requires dealing with issues such as availability of limited amount of data for training, and the existence of adversaries who can drive such systems astray by data poisoning measures.

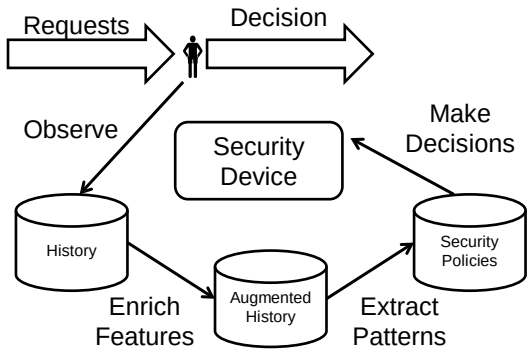

Figure P2-2. Learning from human decision

Each of the suggested approaches provides three different ways to address these limitations, and is applicable to a different class of security devices that are likely to be present in future coalition systems.

(i) Classification based Security Policy Generation: Future coalition environments will consist of ubiquitous devices that incorporate significant computational capabilities, and these devices will run sophisticated machine learning algorithms. Devices tasked with security related functions in a coalition environment can use clustering and classification approaches to automatically infer the policies that ought to be used. This approach is most suitable for security environments which are partly automated and partly managed by humans. In these, a device can observe the actions of a human administrator, understand the intent of the human, and then generalize that to create equivalent policies in similar future contexts. Human input is taken as input to classify security related activities into two groups - allowed and disallowed, and techniques for classification (including case-based reasoning, kNN clustering, decision trees and neural networks) can be used to learn and automate such policies driving these operations. We will evaluate such techniques in order to assess their strengths and weaknesses for security policy generation.

The main challenge to applying machine learning in this environment is that sufficient richness to extract patterns may not be present if human actions are just studied in isolation. To extract true patterns, the context of operations and richer attributes of actors involved in any request need to be determined (see Figure P2-2). If we consider requests for access to information and services being made by coalition partners, each device sees only limited aspect of each request -- such as the network addresses of requesters, and knows the decision made by the human administrator. However, to extract patterns, the device can learn much more if it also has more semantic context, such as the mission objectives, assignment of personnel to missions, current mapping of personnel to network addresses, and a way to assess the relevance of a document being requested to the mission objective. By

[43] D. Verma et. al, Dynamic and adaptive policy models for coalition operations, Proc. SPIE Defense & Security Symposium, April 2017.

providing this semantic context, each security device would have a history of requests that were made by coalition partners for previous missions. It can extract patterns from the accesses that were granted in the past by manual reconfiguration, and learn the features that determine whether or not access ought to be granted. This knowledge can then be converted into a set of access control rules that are based on the characteristics of the new incoming requests. This approach would work even when the mission objectives, personnel assignments, and relevance of documents are only partially known, since such a mapping is being built using the pattern mining/machine learning approach.

The approach works well for those security domains where some information about human behavior can be learned and enriched. An example use-case will be enabling databases that allow access to coalition partners automatically by learning the right operational security policies to support dynamically formed ad-hoc communities of interest. This approach will build on the initial thoughts introduced in the IPP on behavioral policies[44]. A preliminary approach for generating access permissions to data has been proposed[45] and has shown that machine learning techniques can be effective in automatically administering permissions. However this previous approach has many limitations, including the fact that it does not consider contexts and situations when generating permissions nor the contents of protected data. The ability of cognitive devices to collect context and situation information would allow one to provide the generation of fine-grained access permissions tailored to specific context, situation and data content.

(ii) *Trust Estimation Approach for Security Policy Generation:* This approach is applicable for class of security applications where a history of human operation may not be available, but an assessment of the impact of adversarial actions can be done, and damages done by an adversary can be contained. The approach consists of devices dynamically learning how much trust can be put into an external or internal entity -- by observing their behaviors and putting them into different categories of trust and risk.

When human participants in a mission need to make a security decision regarding access or admission to a resource, they take into account the characteristics of the person requesting access, the context, and the estimation of risk that is incurred by allowing access to that person. As an example, the doorman at a gated New York building may allow a polite and sober business-man access to a bathroom behind a locked door under some situations, but refuse the same request if it is made by an inebriated person.

Security devices can implement an analogous trust and risk estimation process to decide when to grant access. This is most suited for environments where one can define several security zones, each associated with a level of trust to access resources in the zone, risk if compromised, and a monitoring system which allows one to monitor the behavior of anyone allowed access into the system.

The trust estimation process will automatically determine, on a per request basis, whether the requester merits sufficient trust to be allowed access to a specific zone. The estimation of the trust depends on the past behavior of the requester in the current zone it has been provided access to, the closeness in properties of the requester to the new zone it wants access to, and an estimation of the risks and utility inherent in allowing the new access request. The trust estimation model would explore techniques to estimate these attributes (trust of requester, pattern based closeness to existing people with access, utility of access, and risks due to access) and study the increases in utility/vulnerability due to allowing such access.

As part of this task, we will investigate two types of trust policies: (a) trust estimation policies providing guidelines on how to estimate trust – for example which factors to take into account for estimating trust; (b) trust-based authentication and access control policies, and firewall rules by which one can specify attribute-based policies in which some of the conditions are predicates on trust and risk. An example would be a policy by which access to a zone is allowed only if trust is greater than 0.9 (in a [0,1] range). In particular policies of type (a) would allow us to use different trust models (such as measurement theory-based trust models[46] and subjective logic[47]). As part of this

[44] M. Touma, E. Bertino, B. Rivera, S. Calo and D. Verma, *Framework for behavioral analytics in anomaly identification*, Proceedings of SPIE Defense + Commercial Sensing Symposium, Anaheim, CA, April 2017.

[45] Q. Ni, J. Lobom S. Calo, P. Rohatgi, E. Bertino. Automating role-based provisioning by learning from examples. SACMAT 2009: 75-84.

[46] Y. Ruan et al., Measurement Theory-Based Trust Management Framework for Online Social Communities. ACM Trans. Internet Techn. 17(2): 16:1-16:24 (2017).

[47] Audun Jøsang, A logic for uncertain probabilities, Int. J. Uncertain. Fuzziness Knowl.-Based Syst. 9, 3 (June 2001), 279–311.

task and in collaboration with Task 1 we will investigate specific policy constructs required for expressing different trust models.

As our trust approach is in part based on data (such as history of past behavior and properties of relevant parties), the scope of trust can be either local or global depending on the data used for trust estimation. Therefore, we will also design policies by which one can indicate whether the trust evaluation can just take into account data local to a specific context for the purpose of trust estimation, or whether also non-local data must be considered and possibly from which sources such data must be acquired and provided. Additional policies will also be devised allowing one to indicate how recent such data must be and other data quality requirements.

Security domains where this approach can be applied include future firewall systems, SDN controllers of coalition partners (in a possible collaboration with proposals related to IPP Project 1), and to help attain the vision of SDN based security situational awareness in coalition contexts that was developed during the IPP phase[48].

(iii) *Security State Analysis*: While the previous two approaches looked at machine learning models that learnt from past behavior, security state analysis is a machine learning approach that tries to forecast future behavior. It uses semantic models built for system behavior along with the behavior observed in the past to create a forecast for system behavior as a result on an incoming operation. The goal is to understand the impact on the state of a system being protected when an operation is requested on the system. In order to analyze the security state, the system continuously monitors the operations that are being invoked on it, examines how its state changes in response to those commands, and thereby learns (using machine learning techniques) what the anticipated response of the system to an operation are. This state learning approach can be used to reduce the manual effort involved in defining the information model or state description of a system.

Once the state transitions that happen due to the impact of the system are learnt to an acceptable degree of fidelity, the system can determine which of the operations are likely to put the system into a risky situation. The system can use the risk profile for an operation to determine whether the operation ought to be permitted on the system. State estimation based approaches are suitable for use in coalition cyber-physical systems.

A new challenge that arises in generative security policy architectures using approaches described above is that new *vulnerabilities are introduced when devices generate their own policies*. As an example, consider a security appliance which is designed so that it can generate its own access control policies. Such an appliance allows more flexibility and requires less human touch, but also introduces new vulnerabilities. If the appliance was given a static set of access control policies, it would never violate them. However, when the appliance generates its own access control policies, there is a risk that it may provide access to an unwarranted party. An assessment of the security risk that the automatic generation of access control policies creates is important to determining whether or not the generative architecture provides a better system.

In order to address this question, we need to *define the right security metrics* to assess the effectiveness of different approaches. This will allow us to compare the generative security approach (or approaches) with the non-generative human defined approach. However, such security metrics need to consider not just the pure security aspect, but also the reduction in human effort for security policy definition that the generative aspect enables. Traditional security metrics need to be combined with metrics for usability, and metrics for reduction in system management effort. *Such security metrics, which combine potential increases in security vulnerabilities with usability, reduction in human effort, and overall improvement in system utility, have not been explored in depth before*.

We propose to define and investigate the nature of security risks that are inherent in the generative architectures. We would evaluate the security risk introduced in a solution by considering *different aspects*, including *the reduction in human effort, the increase in system usability, the new security vulnerabilities, and the speed with which security mechanisms and tools can be reconfigured to deal with situation and context changes*. We will build quantitative models that evaluate the risk in specific contexts. As an example, we will consider the probability of an attacker being present in making access requests to a virtualized environment[2] and consider the probability of such an intruder getting access with generative policy controls compared to a non-generative approach

[48] V. Mishra, D. Verma, and C. Williams, Leveraging SDN for Cyber Situational Awareness in Coalition Tactical Networks, NATO Symposium on Cyber Defence Situation Awareness, NATO-STO-IST-148, Sofia, Bulgaria, October 2016.

for manually defining policies. Security vulnerabilities introduced due to manual errors will be modeled, and we will assess the impact of net utility and intrusion probability developed due to the new architectures. This will allow us to identify the conditions under which a generative approach would be better than a manual policy definition approach. For example, we expect that a generative approach supported by machine learning techniques can be quicker in reconfiguring the security mechanisms (for example by changing firewall rules and access control rules) than a human user. In addition to the quantitative models, we will also build qualitative models for security metrics that incorporate various aspects. These qualitative models will take the form of questionnaires which provide a rating for the solutions among the different aspects, and combine the ratings in a partial order to compare the security offered by two different approaches.

The applications of machine learning techniques to security can be done via heuristics and assessing the results against available data. However, we intend to pursue an additional path in which we would develop mathematical models to understand the fundamental limits of machine learning algorithms for security policy generation, and determine the limits of effectiveness of such algorithms. Finally in order to deal with the potential sparsity of data, we will investigate the use of approaches commonly used in machine learning to address such areas. Machine learning on small and sparse data is an active area of research, and we may need to develop special algorithms which address learning in specific security contexts properly. We anticipate that one of the first areas of exploration would be fundamental limits on the amount of learning and training data that will be required for good use of machine learning algorithms in the context of security. We would also explore other techniques for small data learning, such as transfer learning, boosting, and statistical learning techniques which require less training data than neural network based approaches.

Validation

We will validate our research from both a theoretical and experimental point of view. From a theoretical perspective, we will derive fundamental limits and bounds on the limits of machine learning algorithms when used in the context of security applications. We would also show that the proposed approaches work by means of qualitative and quantitative analysis of different security scenarios.

From an experimental point of view, we will develop a simulation testbed consisting of different devices with their own generative policies for security. This testbed will allow us to experimentally assess the effectiveness of security approaches, generate data for applying machine learning algorithms to our scenarios, and determining the effectiveness of different security metrics. We will use the cross-area task in data generation as the source of data to run experiments and to validate our results. Results of the simulations will be discussed with experts from both governments and industry. We plan to run these experimental evaluations collaboratively with different partners and using the DAIS experimentation platform.

As an initial step towards validation of machine learning approaches for security purposes, we will model coalition scenarios for security (as identified in the Q1 milestone of the task) and include them in the simulation model for the system. This will generate simulated security incidents that can be used for the machine learning algorithms analysis and validation of the theory developed in Q2 and Q3 milestones of the research.

Military and DAIS ITA Relevance

This white paper addresses the following topics in the call for BPP white papers:

- *Dynamic Policy-Based Autonomous Management*: The white paper explores technologies that will enable dynamic policy based autonomous security management in various coalition contexts. The focus is on security.
- *Security Metrics*: The white paper explores security metrics that are relevant to characterize security behavior of dynamic policy based autonomous management schemes.

Security is a key requirement of coalition operations, and effective coalition operations require creating the right security policies for maximum mission effectiveness. The development of methods that can generate security policies on their own, and ease the task of system management for coalition operations, is of very high relevance to coalition operations.

In coalition environments, trust between partners is not absolute, so approaches which dynamically build up trust are important challenge to address. Observing the human behavior, and learning from them is an important aspect of the way coalition members interact with each other. By addressing these challenges in the context of specific coalition scenarios, this task will address the needs of coalition security operations.

The definition of the appropriate security metrics for coalition devices, especially when the devices are generating their own policies, has not been studied in the literature to any depth. Defining those metrics are likely to be very useful for coalition operations in both countries.

Clustering techniques can be used for intelligent assets such as UAVs and mules for them to learn how to protect themselves. The trust estimation technique can be used to protect services in dynamic communities of interest formed across coalitions, with possible applications to the effort around software defined coalitions. State estimation approaches can be used for military cyber-physical systems. Additional synergy may be obtained by applying the techniques to other domains beyond security.

Collaborations, Staff Rotations, and Linkages

Task 1 will analyze scenarios from Task 2 in P2 and from other projects, namely P1 and P3, to identify relevant policy domains and requirements from these policies. Such requirements will be taken into account in order to design specialized policy generation approaches as different policy domains may be characterized by different constraints and/or goals. Task 2 will analyze security-critical scenarios from other projects o in order to define and validate security approaches in this task. The applications of security depends on the nature of the activity being done, and this task will collaborate with other project to see how generative security policy ideas apply in context of their tasks. This will be especially true of projects which are creating new architectures for distributed control (Project 1) and optimizing the distributed infrastructure (Project 3 and Project 5).

Since a significant aspect of Task 2 requires the use of machine learning algorithms, close collaboration with projects 4 and 5, which are building machine learning techniques for interpretability and self-organization, will be used to further strengthen the application of those techniques for security.

Research Milestones		
Due	**Task**	**Description**
Q1	**Task 1**	Analysis of all existing policy analysis techniques and policy metrics. Analysis of existing formal models with respect to the use for the generative policy framework. Output: Scientific PapersParticipating Institutions: Imperial, Purdue, IBM US, DSTL
Q1	**Task 2**	Definition of different coalition scenarios that can benefit from generative security policies and identification of security policy domains from these scenarios. Output: Technical ReportParticipating Institutions: BAE, IBM US, ARL
Q2	**Task 1**	Definition of formal models for generative policies including relevant properties of these models. Definition of quality metrics for assessing policies. Such analysis will also include various scenarios showing the use of the different metrics for different policy domains. Output: Scientific PapersParticipating Institutions: Imperial, Purdue, IBM US, DSTL
Q2	**Task 2**	Identification and analysis of fundamental limits and challenges for applying machine learning for security.

Research Milestones		
Due	**Task**	**Description**
		Output: Scientific Papers Participating Institutions: IBM US, IBM UK, ARL, Purdue
Q3	**Task 1**	Definition of static methods for policy analysis. This will include formal definitions and analysis of such methods and experimental evaluations. Output: Scientific Papers, Demo Participating Institutions: Imperial, Purdue, IBM US, DSTL
Q3	**Task 2**	Approaches for the application of security metrics to different coalition scenarios. Output: Scientific Papers Participating Institutions: IBM US, ARL, BAE, Imperial
Q4	**Task 1**	Design and implementation of monitoring and data tools, including provenance-based tools. Participating Institutions: Imperial, Purdue, IBM UK, ARL
Q4	**Task 2**	Design and implementation of machine learning approaches for access control policy generation. Output: Scientific Papers, Participating Institutions: IBM US, IBM UK, Purdue, ARL
Q5	**Task 1**	Definition of dynamic methods for policy analysis. The work will include formal definitions and analysis of such methods and experimental evaluations. The experimental evaluation will also use the monitoring and data collection tools developed by the previous milestone. Output: Scientific Papers, Participating Institutions: Imperial, Purdue, IBM UK, DSTL
Q5	**Task 2**	Analysis of the effectiveness of the machine learning approaches along with a quantitative estimation of the effectiveness measures. Output: Scientific Papers, Participating Institutions: IBM US, IBM UK, ARL, Purdue
Q6	**Task 1**	A detailed comparison of the policy analysis methods, from both qualitative and quantitative point of views. Output: Scientific Papers, Participating Institutions: Imperial, Purdue, IBM US, DSTL, ARL
Q6	**Task 2**	Architectures for automatic policy determination using trust estimation. Output: Scientific Papers, Participating Institutions: IBM US, Purdue, ARL
Q7	**Task 1**	Definition of approaches for automatic policy evolution. Output: Scientific Papers, Participating Institutions: Imperial, Purdue, IBM UK, DSTL, ARL

Research Milestones		
Due	**Task**	**Description**
Q7	**Task 2**	Architectures and approaches for self-generation of policies in Cyber-Physical Systems using state analysis. Output: Scientific Papers, Participating Institutions: Imperial, IBM UK, IBM US, BAE
Q8	**Task 1**	Experimental application of the techniques for policy evolution in volatile, uncertain, complex, and ambiguous environments. Output: Scientific Papers, Participating Institutions: Imperial, Purdue, IBM US, DSTL, ARL
Q8	**Task 2**	Analysis of trade-offs for different generation approaches discovered during BPP. Output: Scientific Papers, Participating Institutions: IBM US, IBM UK, BAE, Purdue, Imperial, ARL

As a fundamental research project, we expect the primary output of the program to be research publications in refereed conferences and journals. Software development is not usually a part of the basic research agenda, but some software may get created as a part of the research investigation to validate the new approaches that are proposed. Where appropriate, and subject to the approval of all involved partners, we intend to put this software as open source.

Project 3: Agile Composition for Coalition Environments

Project Champion: Mark Herbster, UCL ; Bongjun Ko, IBM US

Email: m.herbster@cs.ucl.ac.uk, bongjun_ko@us.ibm.com
Phone: +44 (0) 20 3108 7091, 914-945-1741

Primary Research Staff	Collaborators
Christopher Gibson, IBM UK	Ananthram Swami, ARL
Dave Conway-Jones, IBM UK	Bong Jun Ko, IBM US
Don Towsley, UMass	Chris Williams, Dstl
Kevin Chan, ARL	Liang Ma, IBM US
Kin Leung, Imperial	David Wood, IBM US
Mark Herbster, UCL	James Lambert, Dstl
Prithwish Basu, BBN	Theodoros Salonidis, IBM US
Paul Yu, ARL	Tom La Porta, PSU
Shiqiang Wang, IBM US	
Ting He, PSU	
Unnamed PGR, UMass	
Faheem Zafari (PGR), Imperial	
Unnamed PGR, PSU	
Stephen Pasteris PDR, UCL	
Tiffany Tuor (PGR), Imperial	

Project Summary/Research Issues Addressed

In tactical coalition environments, operators from different coalition members require analytics that compete for limited resources. The resources themselves may also belong to different coalition members. For example, an operator could ask whether any seismic sensor has detected vibration within a spatial/temporal window which could be related to an explosion, or subscribe to notifications on such events. To serve the request, the coalition network needs to run distributed analytics, which may involve multiple machine learning models and multiple datasets.

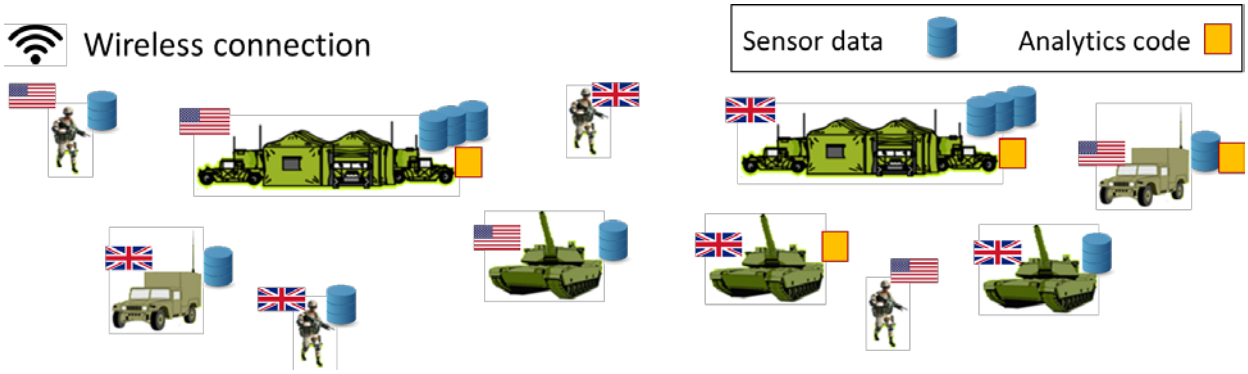

Figure P3-1. Exemplar scenario of distributed analytics in coalition environments

The dynamic coalition environments require the distributed analytics services be dynamically composed, deployed, and executed utilizing available (often limited) computation, storage, and communication resources, while satisfying the constraints imposed by coalition policies. In the exemplar scenario illustrated in Figure P3-1, data is collected from sensors located with soldiers, military vehicles, and command centers, from both the U.S. and the U.K. To provide analytics such as event detection, the collected data needs to be stored and processed in a distributed manner. Also, to achieve the desired level of performance and reliability of the distributed analytics services, the analytics tasks and data objects must be flexibly placed on top of the resources whose availability fluctuate over time. This requires sophisticated and adaptive resource management for distributed analytics that can operate effectively under coalition constraints, such as restrictions in the degree to which coalition partners can coordinate such control tasks, limitations in communication bandwidth, and access control policies for the data and analytics tasks across the coalition boundaries.

In Project 3 of BPP18, we tackle the problems of how to efficiently and flexibly control and manage distributed resources (computation, network, and storage) to support dynamic composition and execution of distributed analytics services in coalition environments. Specifically, we investigate the problem in the following two tasks:

- Task 1 explores how to represent, disseminate, and allocate the coalition resources for analytics services via distributed control mechanism, and investigates fundamental resource-performance tradeoffs for achieving the optimal distributed-analytics operations of coalition infrastructure within operational constraints and policy.
- Task 2 investigates where to place the analytics code and data in the distributed system via joint decision making of multiple elements in service placement/scheduling under dynamic and unpredictable changes of demands and resource availability, and further addresses the issue of validating the Quality of Analytics (QoA) of given service placement/scheduling across coalition boundaries.

Technical Approach

Task 1: Control of Software Defined Coalition for Distributed Analytics

Primary Research Staff	Collaborators
Dave Conway-Jones, IBM UK	Ananthram Swami, ARL
Don Towsley, UMass	Kevin Chan, ARL
Kin Leung, Imperial	Liang Ma, IBM US

Paul Yu, ARL	
Prithwish Basu, BBN	
Unnamed PGR, UMass	
Faheem Zafaru(PGR), Imperial	
Tiffany Tuor (PGR), Imperial	

A coalition partner may have multiple enclaves under its control (e.g., a battalion, squad). To form a software defined coalition (SDC) network to support distributed analytics, enclaves (domains) under different coalition partners need to peer with and expose resources to their partner enclaves. Each enclave appears in the SDC as an abstract aggregate of computation, communication, and storage capacities available to peering enclaves. The physical and logical views of the networked resources may differ under the aforesaid abstraction. Within this overall environment, enclave *controllers* coordinate with each other to create SDC *slices*. An SDC slice is a collection of resources provided by one or more enclaves to work together to provide virtual communications, computation and storage resources for coalition members under a *slice controller*.

The objective of the proposed task is to develop distributed resource control and resource representation/dissemination/allocation mechanisms and fundamental resource-performance tradeoffs for achieving the optimal distributed-analytics operations of coalition infrastructure within operational constraints and policy.

The key technical challenges we address are: (1) to determine resource-constrained distributed-analytics performance tradeoffs achieved with distributed control of a tactical coalition SDC composed of hybrid assets, (2) to understand distributed control mechanisms that assign communication, computation, and storage resources to different analytics tasks and determine how they are shared in the face of network dynamics, and (3) to compare the performance of our mechanisms against fundamental resource-vs.-performance tradeoffs.

By taking an infrastructure-centric view of the SDC, we will *develop fundamental performance limits and tradeoffs of distributed control of an SDC* and *design distributed control algorithms that achieve these limits*. We will use the following problems to illustrate our ideas and results:

(a) aggregation of sensor data from multiple locations under a time deadline constraint,

(b) spectral representation of correlated data streams, and

(c) summarization, aggregation and compression of distributed video streams.

More generally, we will consider distributed analytics services that consist of one or more *agile* code and data components related to each other by a graph representing the distributed task workflow, and SDC slices will be dynamically assigned to each such task while considering its requirements and the current resource availability.

Our technical approach will be split into the following two subtasks.

Subtask 1.1. Fundamental Performance Limits and Tradeoffs

Computation fidelity vs. latency with networked computation

Consider a set of compute resources in a multiple-enclave SDC— each with a certain amount of available CPU resources —connected via a wireless network of a given topology and available link bandwidths. The enclave controllers have full knowledge of the aggregate resource within the respective enclave as a function of time, and needs to advertise this networked computing resource to neighboring enclaves for new computation needs in the most efficient way. The overall networked computing resources for the SDC are characterized by a dynamic node and edge weighted graph $G(t)$, and each enclave controller has knowledge of a subgraph of $G(t)$. Node weights represent currently available CPU resources whereas edge weights represent available link bandwidths. Both are functions of time determined by network dynamics, such as node mobility and evolving computation needs.

First, we will evaluate the fundamental tradeoff between the performance of distributed computation achievable by this networked computing resource, and the latency of computation, especially when it is acceptable

to vary the *fidelity* of computation. Here fidelity refers to the quality of the output of the computation, which is a function of the amount of computational resources made available. Second, we will study the trade-space between communication and computation to attain a certain performance, under a global resource (e.g., energy) constraint.

We will consider an exemplar setup of a distributed analytics task where a set of marked nodes in the network produce sensor data, a function of which needs to be computed and made available at a given node within a given time deadline. What is the tradeoff between the fidelity of the final computed function (F), e.g., mean squared error from the true value, and the time deadline that can be met (T)? Given $G(t)$, what is the optimal (F, T) trade-space? Understanding this tradeoff will enable the enclave controller to make an informed decision on advertising the networked computation resource in a resource-efficient fashion. We will assume Poisson distributed nodes (controllers and switches) in a 2D area to develop the initial theory, and use a hidden Markov model for the evolving network topology from the enclave controller's perspective. Sweeping the (F, T) trade-space corresponds to turning a design knob of the distributed computing protocol, simple examples of which are: Sampling rate and choice of quantization levels of data at a sensor node, and the number of (multiple) paths used to transmit intermediate computation in a multi-hop communication protocol. Tuning these knobs (viz., reducing the quantization, choosing fewer multi-paths and lowering sampling rate) will change (viz., reduce) T but increase F.

Further, we will quantify – given a total consumed power – the tradeoff between amounts of computational resources (e.g., Giga Flops) vs. the amount of communication resources (e.g., bandwidth) that can be used to attain a given point in the (F,T) space.

Each enclave controller has a limited (enclave-level) view of the (F, T) tradeoff, a subgraph of $G(t)$. What is the minimum communication (amount, frequency) that the controllers must share among themselves to get a global picture of the (F, T) tradeoff? For this study, we will use the theory of partially observable Markov decision process (POMDP) to model the action of an enclave controller (communication to a neighboring enclave controller) and its effect on the local picture of the (F,T) trade-space.

Combining the above studies, we will address the problem of the creation of an SDC slice to execute the aforesaid task. We will address the question of how much information of the full (F, T) tradeoff is required by an SDC slice, and what is the minimum number of resources that should be dedicated to meet the SDC application need?

Connectivity vs. robust distributed computing performance

What level of network connectivity and density of availability of computation and storage resources is needed to ensure robust attainment of a distributed analytics objective under network dynamics? How do controller actions maintain the requisite level of connectivity via distributed control with good knowledge of SDC network resources in the home enclave but with limited global knowledge of the overall network?

We will leverage work in the Topic of "Computation Fidelity" above and our work on robust connectivity of networked resources using percolation theory from the IPP period, to investigate what networked computation resources, i.e., $G(t)$, is necessary to maintain a desired (F,T) tradeoff robustly, i.e., the performance is immune to a given amount of network dynamics.

Resource allocation by distributed control

In this topic, we will study how an enclave controller should distribute resources to multiple assets under its control to meet application needs. We will study the fundamental tradeoff of resources (e.g., communication, computation, storage) to meet the application need under the best possible controller action. We will also compare the performance of control protocols developed in Subtask 2, to these fundamental tradeoffs.

Consider two independent distributed computation tasks, viz., two separate sensor aggregations. Each task is characterized by the set of sensor locations, rate or amount of data at each sensor node, and the respective destinations of the results. The enclave controller's responsibilities are to assist the slice controllers to create SDC slices for the two tasks to meet the desired performance objectives. Forming an SDC slice is fundamentally a resource allocation problem. We will, based on results from the Topics of "Computation Fidelity" and "Connectivity" above, evaluate optimal resource allocation across multiple tasks, i.e., simultaneously achievable (F,T) regions for both tasks by allocating resources between the tasks optimally.

Characterization of scaling laws for analytics capacity

We will consider a simple distributed analytics scenario where the set of agile code and data items are given by $C = \{C_i\}$ and $D = \{D_i\}$ respectively, and the i-th analytics workflow is of the form $D_i \rightarrow C_i \rightarrow \{U_{i_1}, U_{i_2}, \dots, U_{i_k}\}$, where the U's denote users, D_i is composed with C_i, and the results are passed to the users. SDC slices need to be appropriately allocated to execute the code and store the data, both of which may be agile, i.e., either or both D_i and C_i may be transmitted from their respective production locations over the SDC network, get cached/replicated at available computational/storage resources located near the users, and then transmitted to suitable common processing resources for execution.

In this setting, *analytics capacity* is defined as the number of analytics workflows that can be scheduled and reliably completed within a deadline on a given SDC network. Instead of solving optimization problems for scheduling specific instances of analytics tasks on specific SDC networks $G(t)$, we will characterize the "scaling laws". This does not necessitate a precise solution to the optimal placement problem for the agile code and data. Instead, we will start exploring random load balanced placement schemes[49] and build on prior work on scaling laws for caching in wireless networks[50] to characterize the fundamental scaling laws of analytics capacity in the $O(.)$ sense.

We will also consider further generalizations that present us with tradeoffs: (1) D_i, C_i may be simultaneously shared across two or more analytics tasks. This may result in potentially *super-additive* gains for analytics capacity but at the same time may result in resource contention in SDC slices. (2) The analytics workflows may be represented by more complex graphs, e.g., computation workflow DAGs (directed acyclic graphs) that may involve edges like (C_i, D_j) and (C_i, C_j).

Finally, we will quantify the gap between the performance attained by distributed control schemes to be developed in the following Subtask 2 of this work, to the fundamental limits derived above.

Subtask 1.2. Control of Software Defined Coalitions (SDCs) in Support of Data Analytics

This subtask focuses on distributed control mechanisms and how their performance compares to the above performance limits. An important component of SDC control for data analytics is allocation of resources and services to coalition partners according to their availability and coalition requirements. Resource and service allocation should be carried out systematically and adaptively as discussed below.

[49] M. D. Mitzenmacher, "The Power of Two Choices in Randomized Load Balancing", Ph.D. Dissertation, Harvard University, 1996. S. Gitzenis, G. Paschos, and L. Tassiulas, "Asymptotic laws for joint replication and delivery in wireless networks," IEEE Transactions on Information Theory, vol. 59, no. 5, pp. 2760–2776, 2013.

[50] S. Gitzenis, G. Paschos, and L. Tassiulas, "Asymptotic laws for joint replication and delivery in wireless networks," IEEE Transactions on Information Theory, vol. 59, no. 5, pp. 2760–2776, 2013.

SDCs poses challenges to the problem of resource and service allocation. As a common design candidate and for ease of implementation of the SDC architecture based on existing enclave controllers, we consider a two-level hierarchical distributed control structure with slice controllers at the top level and enclave controllers at the bottom level. Suppose the goal is to create a slice to support distributed sensor analytics requiring resources in multiple enclaves. A slice controller is established, which obtains resource availability from the enclaves based on their dynamic operational conditions at the time, and determines if sufficient resources exist for the analytic application. If so, the slice controller, cooperating with other slice controllers and enclave controllers, determines resource amounts needed and the optimal configuration. It then requests resources and service from enclave controllers, where the latter allocate resources/services as described below. This raises several research questions:

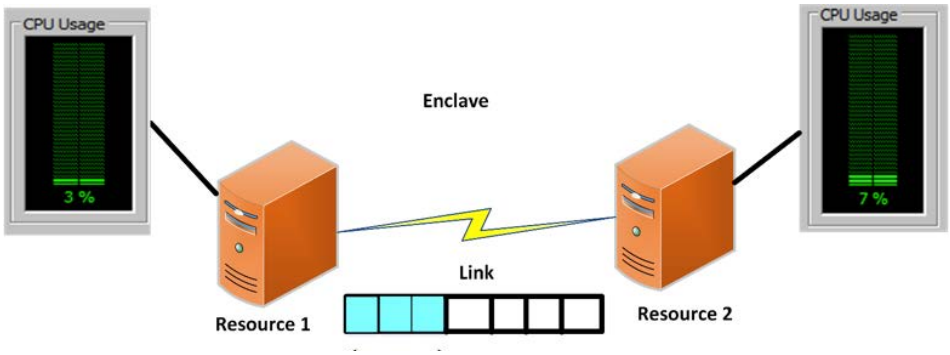

Figure P3-2. An SDC enclave with resources and limited link.

(1) How should resource availability within an enclave be represented and presented to slice controllers? (2) How should slice controllers determine what resources and services to ask for and from what enclaves? (3) If a request cannot be satisfied by the available resources and services, how should slice controllers negotiate with the analytics to lower their demands to a level that can be supported. (4) Given the decisions from the slice controller, how should individual enclaves allocate their resources and services? These questions are treated below.

Resource and service availability.

Representation of available resources: Monitoring and determining available computation, communication, and storage resources in *enclaves* and *slices* are fundamental to performance since it assists in the analysis, management, scheduling, load balancing, fault detection, and recovery of the enclave[51]. Distribution of control and the level of dynamism in an SDC imply that simple monitoring tools and techniques will be unsuitable in tactical environments. Based on network constraints, there is a need for new metrics such as *effective resources* to quantify actual resources available to analytics. For example, computation (CPU) resources 1 and 2 (Figure P3-2) are utilized at X% and Y% of maximum capacities, respectively. (Alternatively, we can express CPU capacity in unit of MIPS, million instructions per second.) The communication link between the two is a bottleneck and poses a significant constraint on logically considering both resources as one. Rather than advertise this enclave as having *(100-X) % of resource 1 + (100-Y)% of resource 2*, we propose to make the enclave appear logically as an abstraction of computation, connectivity and storage by using stochastic models to consider the link constraint for expected analytics, and represent the combined capacity of both resources as equivalent to *Z*% of a computational resource at a single node. To address the issue, we will propose novel lightweight but effective techniques to efficiently represent the resources that are still available. Moreover, this can be applied to *services* to suggest the need for effective services metrics.

Similarly, to handle multiple types of resources and services, there is a need to estimate performance metrics associated with resources and services in terms of latency, quality, energy and/or robustness so that the SDC controller can determine the optimal use of resources and services to satisfy analytics requirements. Our approach to addressing these issues here is to exploit two complementary notions of multi-resource models[52,53] and effective

[51] Huang, He, and Liqiang Wang, "P&P: A combined push-pull model for resource monitoring in cloud computing environment," IEEE 3rd International Conference on Cloud Computing (CLOUD), 2010.

[52] G.L. Choudhury, K.K. Leung and W. Whitt, "An Algorithm to Compute Blocking Probabilities in Multi-Rate Multi-Class Multi-Resource Loss Models," Advances in Applied Probability, Vol. 27, pp. 1104-1143, Dec. 1995.

bandwidth (EB)[54]. Multi-resource models are particularly useful to represent multiple types of resources such as computation, communication and storage, which are needed for a given analytics task. Using the example of Figure P3-2, a distributed task may request A% of resource (CPU) 1, B% of CPU 2 and a bandwidth of C bits per second on the link connecting CPU 1 and 2. If not all of the requested resources are available, the slice controller or enclave controllers "block" the task, as represented by loss in the models. The block task can negotiate with the SDC controller to lower its resource requests for lower performance. The idea of EB is an effective mathematical representation of bandwidth requirement of a data flow that captures its stochastic characteristics. Using a common cost (currency), we aim to extend the notion of EB to multiple resources in order to consider contention delays incurred by the task in using the resources.

Resource/Service Information Dissemination: As a first step, utilization of various resources and services throughout the enclave will be monitored and measured. Given the distributed nature of the SDC, we plan to develop distributed machine-learning techniques for the purposes of monitoring and collection of utilization measurements. Once collected, resource and service information will be made available to other controllers. The dynamic nature of the SDC means traditional pull and push methods[55] will not by themselves satisfy SDC requirements. To address this, we aim to derive hybrid schemes for distributing resource related information that will provide up to date status information without significantly straining the performance of the network.

Distributed resource allocation

SDC slice level multi-objective optimization: Since slices will run analytics applications, resource allocation must account for their requirements and provide appropriate resources. As applications with differing (QoS or coalition) needs will execute on different slices, we will explore and extend existing multi-objective optimization (MOO) frameworks[56, ,57,] to consider these different requirements and provide resources efficiently. Each slice may have different, conflicting objectives/goals (e.g., low latency versus strong encryption) requiring different resource requirements. To handle conflicting objectives among slices, we will explore and extend Cooperative Game Theory MOO[57,**Error! Bookmark not defined.**], including cooperative and competitive games. We will also explore other heuristic a pproaches such as Trust-based MOO frameworks[58] as they are potentially efficient in dynamic environments and provide close to optimal solutions. We will develop distributed algorithms for performing MOO-based resource allocation within the above frameworks. Tradeoffs between messaging overhead and the performance of the MOO techniques are expected in the distributed setting. We plan to include messaging overhead as part of the MOO framework. Hence the Pareto-frontier or the optimal solution will also include the messaging overhead, which allows us to investigate and achieve the desirable tradeoffs.

The outcome of MOO is that each participating slice identifies resource requests to be made to individual enclaves. Enclave controllers then determine whether they can be satisfied. Inability of an enclave controller to satisfy a request will necessitate negotiation with the requesting slice controller, which may trigger additional execution of MOO. This is a topic of our research.

Other issues include: (i) Handling resource and service availability dynamics; we will explore reactive and proactive MOO strategies. (ii) Multiple slice controllers may reside in the same location allowing the possibility of a centralized MOO resource allocation. (iii) We have assumed slice controllers do not reside with enclave controllers and consequently have unclear views of enclave resources. We will consider the case where slice and enclave controllers are collocated.

---

[53] G.L. Choudhury, K.K. Leung and W. Whitt, "An Inversion Algorithm to Compute Blocking Probabilities in Loss Networks with State-Dependent Rates," *IEEE/ACM Trans. on Networking*, Vol. 3, pp. 585-601, October 1995.

[54] C. Li, A. Burchard, J. Liebeherr, "A network calculus with effective bandwidth," *IEEE/ACM Transactions on Networking*, 2007.

[55] Zanikolas Serafeim, and Rizos Sakellariou, "A taxonomy of grid monitoring systems," *Future Generation Computer Systems* 21.1 (2005): 163-188.

[56] Luo, Zhi-Quan, and Shuzhong Zhang, "Dynamic spectrum management: Complexity and duality," *IEEE Journal of Selected Topics in Signal Processing* 2.1 (2008): 57-73.

[57] J. H. Cho, Y. Wang, I.R. Chen, K.S. Chan and A. Swami, "A Survey on Modeling and Optimizing Multi-Objective Systems," IEEE Communications Surveys & Tutorials, vol.PP, no.99, pp.1-1 doi: 10.1109/COMST.2017.2698366

[58] Deval Bhamare, et. al. "Multi-Objective Scheduling of Micro-Services for Optimal Service Function Chains," IEEE ICC 2017.

Optimization approach to enclave resource allocation: Using detailed resource and service information, enclave controllers can apply and extend existing optimization approaches[59,60] to optimally allocate resources within the enclave. However, to consider conflicting needs for multiple slice/tasks, our focus here is to exploit the MOO frameworks as discussed above at the enclave level. We plan to investigate MOO formulations with appropriate definitions of utilities and constraints, which differ at enclave and slice levels. As a result, a research topic is to develop corresponding solution techniques for the MOO problems.

Task 2: Distributed Analytics in Dynamic Coalition Environment: Placement, Scheduling, and Validation

Primary Research Staff	Collaborators
Christopher Gibson, IBM UK	Ananthram Swami, ARL
Mark Herbster, UCL	Bong Jun Ko, IBM US
Shiqiang Wang, IBM US	Chris Williams, Dstl
Ting He, PSU	David Wood, IBM US
Unnamed PGR, PSU	James Lambert, Dstl
Stephen Pasteris PDR, UCL	Theodoros Salonidis, IBM US
Kevin Chan, ARL	Tom La Porta, PSU

In Task 3.1 in the IPP, we studied static analytics code/data placement in an analytical framework[61,62]. We showed that the problem is generally NP-hard and developed max-flow-based algorithms that solved certain subproblems (e.g., scheduling under given code/data placement) optimally in polynomial time while achieving a guaranteed approximation for the overall problem. While the above framework addresses a static environment where the user demands and the available resources are fixed and known, tactical network environment imposes a number of unique challenges:

(1) Coalition policies impose restrictions on where to place the code/data, how to share resources, and accessibility of control plane information across domains, which complicates the management of analytics services.

[59] B. Spang, A. Sabnis, R. Sitaraman, D. Towsley, and B. DeCleene, "MON: Mission-optimized Overlay Networks," IEEE INFOCOM 2017, May 2017.

[60] G. Tychogiorgos and K.K. Leung, "Optimization-based Resource Allocation in Communication networks," *Computer Networks*, Vol. 66, pp. 32-45, June 2014.

[61] T. He, H. Khamfroush, S. Wang, T. La Porta, S. Stein, "It's Hard to be Social: Joint Service Placement and Request Scheduling for Social Edge Applications," submitted to *IEEE INFOCOM 2018*.

[62] S. Pasteris, S. Wang, M. Herbster, K. Chan and C. Makaya, "Data Distribution and Scheduling for Distributed Analytics Tasks," in *DAIS Workshop*, 2017.

(2) Both user demands and available resources will experience dynamic and unpredictable changes as the missions and network conditions evolve, which raises a challenge of adapting service placement and scheduling with incomplete knowledge of the environment.
(3) The physical resources are owned and managed by different coalition members (and possibly third parties), which raises a challenge of ensuring that each resource provider treats all coalition members appropriately according to the policy agreed in the coalition.

In this task, we propose to address the above challenges under a mathematical framework with realistic assumptions. As illustrated in figure P3-3, Subtask 1 addresses the joint decision making of multiple elements in service placement/scheduling with focus on addressing challenge (2), and Subtask 2 addresses the Quality of Analytics (QoA) validation under given service placement/scheduling with focus on addressing challenge (3). The outcome of Subtask 2 is fed back to Subtask 1 to inform future placement/scheduling. Both subtasks will respect restrictions in challenge (1).

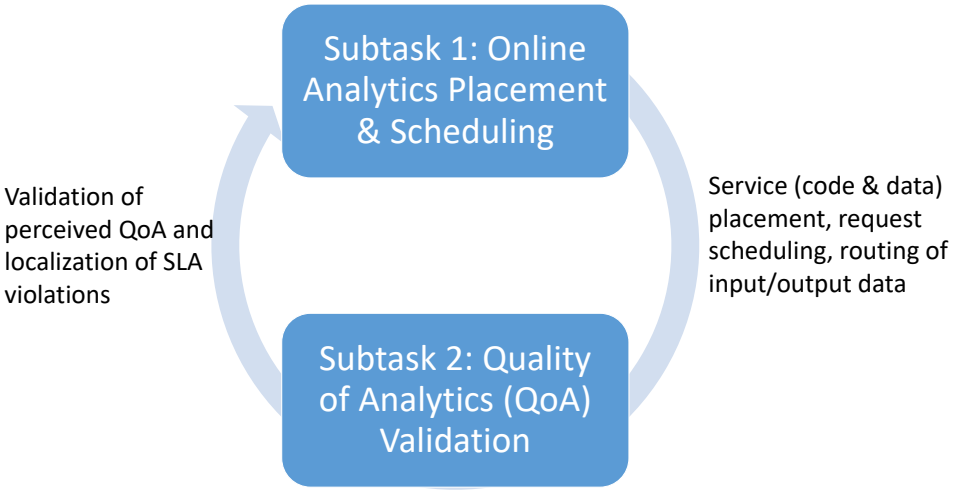

Figure P3-3. Task overview

Subtask 2.1. Online Code/Data Placement and Scheduling for Tactical Analytics Applications

In this subtask, we will study the problem of code/data placement (where "code/data" includes machine learning models), analytics workload scheduling, and routing of input/output data, jointly referred to as *service configuration*. As illustrated in figure P3-4, our objective is to promptly serve user demands in an online setting, where we consider both long-lasting services and on-demand services. Based on the predictability of user demands and resource availability, we will find the optimal service configuration at different time scales as detailed below.

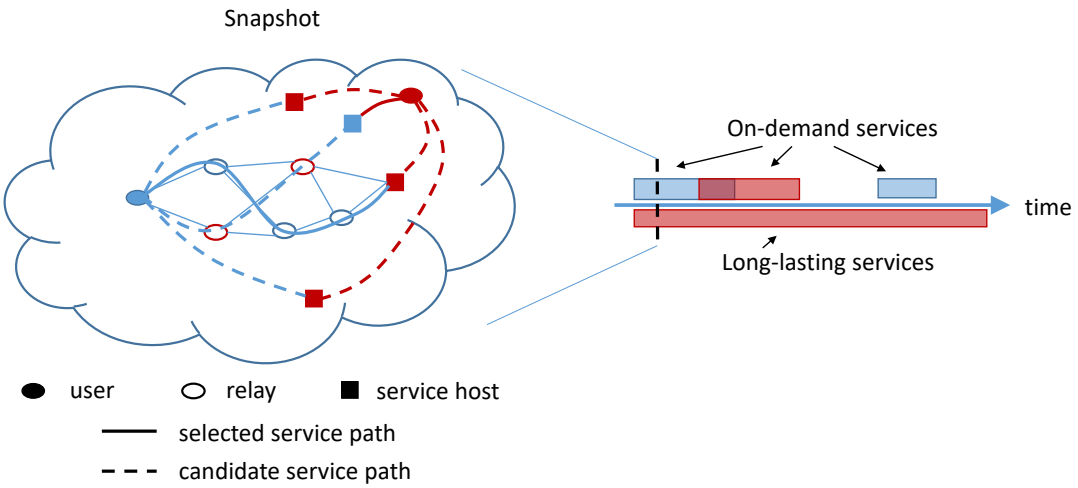

Figure P3-4. Online code/data placement and scheduling for analytics applications (different colors represent nodes/service demands of different coalition members)

Frame-based service configuration (FBSC): In this approach, we will divide the entire mission duration into smaller time windows called *frames* such that the demands and resources within a frame can be predicted (up to certain accuracy) at the beginning of each frame[63]. This framework suits long-lasting services and predictable services (e.g., for surveillance and patrolling), and allows us to apply solutions designed for static scenarios such as[61,62]. However, applying these solutions in an online coalition setting imposes new challenges:

Agile data/analytics under coalition constraints: In existing literature, the code and data are usually considered as atomic entities[64], which ignores possibility of partitioning code and data for distributed execution. We considered distributed analytics in the IPP, but assumed either fixed locations of code[62] or bundled code/data[61]. While our initial results are promising, they can be suboptimal due to the simplifying models. Moreover, the previous works do not explicitly address coalition constraints. We will address these issues in the BPP by employing a generalized mathematical framework that allows:

1. composable analytics data and execution across multiple coalition members (such as in the example shown in figure P3-1), where not only data can be distributed as in[62], but execution can also be distributed subject to dependency, synchronization, and policy constraints imposed by the analytics (e.g., barrier synchronization for MapReduce workloads),
2. joint code/data placement and execution scheduling, where fragments of code/data for an analytics application can be routed towards each other or an intermediate node for execution, and
3. heterogeneous resource capacities based on coalition memberships of nodes and workloads.

The above generalization substantially expands the solution space for possible service configurations. Moreover, there are usually limitations on how an analytics application can be fragmented, which create integral constraints. We will collaborate with Project 4 to define application fragmentation patterns that will be used as an input to our problem. Different analytics applications may also share data, which create non-additive resource consumptions. We will consider the abovementioned constraints in the problem formulation. The solution of the problem will include decisions on where to place the code/data and how to fragment the code/data. Each decision will be associated with a cost and the objective of decision making is to minimize the cost. The cost can be related to various aspects, including whether or not an application has been fragmented. Some of the cost parameters can be specific to the precision of analytics, which may be non-additive but are instead in the form of maximum or

[63] S. Wang, R. Urgaonkar, T. He, K. Chan, M. Zafer, and K. K. Leung, "Dynamic service placement for mobile micro-clouds with predicted future costs," *IEEE Transactions on Parallel and Distributed Systems*, vol. 28, no. 4, pp. 1002 – 1016, Apr. 2017.

[64] A. Fischer, J. F. Botero, M. T. Beck, H. De Meer, and X. Hesselbach, "Virtual network embedding: A survey." IEEE Communications Surveys & Tutorials 15.4 (2013): 1888-1906.

minimum. These lead to a problem that generalizes the NP-hard problem in[61] and is hence NP-hard. The NP-hardness is intuitive because a very specific instance of this problem is the knapsack problem (known to be NP-hard) where the goal is to maximize the value subject to limited resource capacity. We will identify solvable special cases, study the approximability of general cases, and develop solutions with guaranteed approximation bound.

Stable service configuration under runtime dynamics: Invoking the above placement/scheduling algorithms on a per-frame basis imposes new challenges, including when to start a new frame, and how to ensure system stability across frames. We will address these challenges by extending the above mathematical framework to incorporate the cost of adapting service configuration, and analyzing the impact of frame length on reconfiguration cost and optimality gap (due to dynamics within a frame). Inspired by our previous work [65],[63], we will use competitive analysis to find asymptotically optimal algorithms for determining the frame length, where the frame length can be adaptive based on the dynamics of the environment and task.

Adaptive service configuration via online learning: To complement the above prediction-based approach, we will explore an online learning approach[66] that adapts to the *unknown* user/resource dynamics. The idea is that as we start to serve users under a baseline configuration (e.g., random code/data placement, greedy scheduling, shortest path routing), we can observe the resulting performance and adapt the service configuration. Online learning (a.k.a. online optimization) provides a framework and a set of algorithms to systematically explore the solution space to minimize the overall regret. While online learning has been applied to routing[67,68,69], we face a much harder problem of simultaneously addressing placement, scheduling, and routing for multiple users and services. As different services may share resources, their performances will be correlated and their configurations need to be optimized jointly. A straightforward application of existing online learning algorithms is likely to converge slowly as the number of possible configurations is exponential in the number of user-service pairs.

We will address this challenge by decomposing the problem into smaller subproblems for which polynomial-time approximation algorithms exist. Noting that node resources (CPU, memory, etc.) remain largely unchanged, whereas the wireless link capacities vary rapidly, we decouple the problem into two subproblems: (1) *online placement and fragmentation of code/data under multiple types of resources and coalition constraints*, which is an extension of the online multiple knapsack problem[70], (2) *online transfer of code/data under coalition constraints*, which is an extension of the online shortest path routing problem[67]. We will develop algorithms for each subproblem and establish their performance bounds through competitive analysis or regret analysis. We will then combine the algorithms to optimize the overall service configuration, and analyze the convergence rate and the asymptotic optimality gap.

Subtask 2.2. Quality of Analytics (QoA) Validation in a Coalition Environment

Analytics services offered by coalition networks are inherently federated in that the physical assets supporting end-to-end analytics workflows are owned and managed by disjoint administrative domains (see figure P3-1). To ensure that the coalition effort is successful, an agreement between different coalition members needs to be made beforehand. A possible example of such an agreement can be that the U.K. sensors in one area will report to the U.S. if any suspicious event is detected. Each coalition member may have corroborating evidence about whether the sensors/nodes are cooperating according to the agreement.

---

[65] I.-H. Hou, T. Zhao, S. Wang, and K. Chan, "Asymptotically optimal algorithm for online reconfiguration of edge-clouds," in Proc. of ACM MobiHoc 2016.

[66] E. Hazan, Introduction to Online Convex Optimization. *Foundations and Trends in Optimization*, vol. 2, no. 3-4, pp. 157–325, 2015.

[67] T. He, D. Goeckel, R. Raghavendra and D. Towsley, "Endhost-based Shortest Path Routing in Dynamic Networks: An Online Learning Approach," in *INFOCOM*, 2013.

[68] V. Dani, T. P. Hayes and S. M. Kakade, "Stochastic Linear Optimization under Bandit Feedback," in *Annual Conference on Learning Theory*, 2008.

[69] K. Liu and Q. Zhao, "Online Learning for Stochastic Linear Optimization Problems," in *Information Theory and Applications Workshop*, 2012.

[70] Deeparnab Chakrabarty, Yunhong Zhou, and Rajan Lukose. "Online knapsack problems." Workshop on internet and network economics (WINE). 2008.

To ensure that each coalition member is properly rewarded for contributing resources to the coalition, it is crucial that the Quality of Analytics (QoA) delivered to each member adheres to the sharing policies between coalition members. Here, QoA refers to the quality of information provided by the analytics, measured by response time, availability, accuracy, etc. In this subtask, we aim at validating the QoA received by coalition users and detecting/localizing violations of QoA agreement from end-to-end performance measurements.

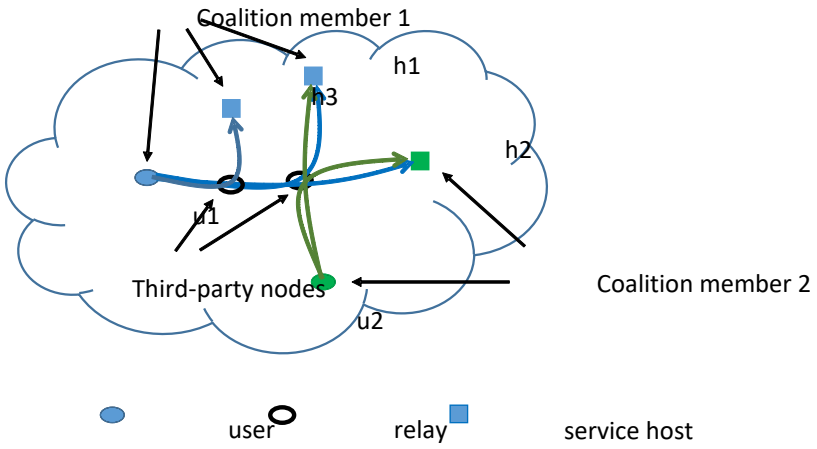

Figure P3-5. Flow-based service model: service 1 consists of flows between u1 and h1, h2, h3, and service 2 consists of flows between u2 and h1, h2.

Specifically, as illustrated in figure P3-5, we model the coalition network as a graph $\Gamma = (N, L)$, where N is the set of nodes representing end users, communication nodes, and processing/storage nodes, and L is the set of communication links. Nodes in Γ are owned and operated by different coalition members, and each node hosts part of data/code required by various analytics services. We model each analytics service as a set of flows in Γ, and the QoA is an aggregate of the performance metrics at nodes/links traversed by the flows. For example, the response time is the maximum sum of computation/communication latencies along the paths traversed by the flows. Similar aggregation functions exist for other QoA measures.

Given the agreement between a particular coalition member and its partners in terms of the performance received at individual nodes, the problem is to validate whether the received QoA conforms to the agreement, and if not, to localize the node(s) violating the agreement. We consider two types of QoA agreements: (1) *absolute QoA agreement*, which specifies the absolute performance (e.g., bound on the mean computation latency), and (2) *relative QoA agreement*, which specifies the relative performance (e.g., bound on the variation of mean computation latency for different users). Accordingly, we will investigate the following problems:

- The problem of **absolute QoA validation** can be formulated as a *network anomaly detection* problem, where a node/link is abnormal if its performance metric violates a predetermined bound. Our problem differs from the generic anomaly detection problem [71] in that each coalition member only observes aggregate measurements (e.g., response times/availability) at its own nodes. Since anomaly on an invidual node/link may not cause anomaly of an analytics service, the straightforward approach of applying anomaly detection on raw measurements will be ineffective in many cases. We will address this problem by inferring the performance of individual nodes/links from end-to-end QoA. However, different from exsiting works that aim at inferring the performance of all the nodes/links [72, 73], we are only interested in

[71] V. Chandola, A. Banerjee and V. Kumar, "Anomaly detection: A survey," ACM Computing Surveys (CSUR), vol. 41, no. 3, 2009.

[72] L. Ma, T. He, K. K. Leung, A. Swami and D. Towsley, "Inferring Link Metrics from End-to-end Path Measurements: Identifiability and Monitor Placement," *IEEE/ACM Transactions on Networking*, vol. 22, no. 4, pp. 1351-1368, 2014.

detecting/localizing nodes/links with abnormal performance. We will establish conditions for detectable anomalies and develop detection algorithms to optimally trade off detection accuracy, delay, and measurement cost by performing detection at multiple levels (e.g., paths, subpaths, links) and exploiting sparsity of abnormal nodes/links.

- The problem of **relative QoA validation** can be formulated as a *network discrimination inference* problem, where a node discriminates if it treats service requests from different coalition members differently. If multiple performance classes are allowed at a node, we can represent this node by multiple logical nodes, each corresponding to a performance class, and a node discriminates if it treats different requests within the same class differently. Network discrimination inference aims at detecting and localizing discriminating nodes from end-to-end measurements. The basic idea is that instead of finding a solution to the per-node/link performance that is consistent with the measurements, we are interested in detecting cases where no feasible solution exists, which signals the existence of discriminating nodes. Existing solutions based on this idea[74] use a specific performance metric, log of congestion-free probability, that is measured over many time intervals. To detect discriminations in the highly dynamic tactical environment, we will use performance measures (e.g., response times) capable of capturing transient behaviors. Using such measures faces several challenges, e.g., no unique mapping from the measurements to the performance of individual nodes/links, and normal performance fluctuations due to variations of the wireless channels. To address these challenges, we will develop algorithms to compute the minimal identifiable node/link sequences and the proper detection threshold to differentiate discrimination from normal fluctuations. We will also develop algorithms to localize the discriminating nodes by computing the most likely set of nodes/links such that allowing inconsistent performances at these nodes/links leads to a feasible solution.

For each sub-problem described above, we will first propose a centralized solution, then extend to a distributed mechanism using consensus and related techniques.

Validation and Experimentation

A key aim of the validation and experimentation is to measure the gap between best practical implementation of the proposed algorithms and the theoretical results, and to investigate the size and predictability of these variances. The effectiveness and correctness of the proposed approaches will be confirmed by showing that the simulation and experimentation results conform to the performance bounds obtained from theoretical analysis. The effectiveness will be further confirmed by comparing to other solution approaches and showing the benefit of our proposed approach. Such understanding will provide new insights for further improvements of the proposed algorithms for practical tactical environments. The process and results of the experimental validation will be documented in various technical reports and afford important insights into the future transition potential of the research.

To this end, the team will conduct experimentation on simulation, emulation platform, and prototype implementation of the algorithms. We will leverage on our past experience of developing distributed machine learning models on those edge devices as part of an IPP Project 3 task[75], as well as the implementation and CORE/EMANE emulation of distributed network measurement and distributed code/data migration in container-based environments[76,77]. The team will will also leverage on previous Dstl experimentation projects at IBM UK, which include:

---

[73] L. Ma, T. He, A. Swami, D. Towsley, and K. K. Leung, “Network Capability in Localizing Node Failures via End-to-end Path Measurements,” *IEEE/ACM Transactions on Networking*, vo. 25, no. 1, pp. 434-450, 2016.

[74] Z. Zhang, O. Mara and K. Argyraki, "Network Neutrality Inference," in *SIGCOMM*, 2014.

[75] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya, T. He, K. Chan, “When Edge Meets Learning: Adaptive Control of Distributed Learning Operations at the Edge,” submitted to *INFOCOM 2018*.

[76] A, Machen, S. Wang, K. K. Leung, B. J. Ko, and T. Salonidis, “Live service migration in mobile edge clouds,” *IEEE Wireless Communications*, accepted for publication, May 2017.

[77] S. Wang, K. Chan, R. Urgaonkar, T. He, and K. K. Leung, "Emulation-based study of dynamic service placement in mobile micro-clouds," in *Proc. of IEEE MILCOM 2015*, Oct. 2015.

- TIN05 - Requirements for an Experimentation and Analysis Framework,
- TIN06 - Experimentation and Analysis Framework for Network Technology Research
- TIN08 - Future C4ISR Architectures Network Management and Technologies Assessment D1.2 Final multi-bearer routing analysis and experimentation definition report,
- TIN43 - Dynamic Black WAN - Design and Exploitation of SDN in an emulated deployed network,
- TIN44 -Resilient Information Services for Dispersed C2 in Denied and Degraded Environments: Initial simulation of the ability to deliver basic information services in the deployed tactical domain which respond dynamically to variation in spectrum availability and command (user) demand.

More specifically, the plan and benefits of experimental validation in each task are as follows:

In Task 1, some part of the new distributed control mechanisms out of sub-task 1.2 will first be implemented and tested in a simulation environment, such as EMANE/CORE, with a plan of building a demonstration deployed on "real" devices such as within the ARL DAVC environment or the Dstl emulation framework. The measured performance of the implementation will help us calibrate the special network settings and confirm the performance limits to be devised in subtask 1.1.

As for Task 2, we will first evaluate each individual research outcome separately via extensive simulations, using data traces of user mobility (such as location traces of vehicles and humans) and analytics services (such as resource consumption measurements of analytics applications), which are either from public dataset repositories such as www.crawdad.org, collected by ourselves, or obtained from ARL and Dstl collaborators. Then, we will conduct further experiments by aggregating and implementing our research results in an emulation environment such as CORE/EMANE, and on a hardware prototype using the combination of edge devices (e.g., Raspberry-Pi devices), where we plan to use the same data trace as in the simulation to emulate network dynamics and general analytics requests workloads from real analytics services such as the distributed detection of events in a tactical scenario. Through these experiments, we aim to validate that our proposed algorithms improve the performance of distributed analytics in networked coalition systems.

Military and DAIS ITA Relevance

The work proposed in Project 3 is designed to enable coalition forces to access analytic services in the tactical theatre, for which the application of edge computation and distributed SDC resource control mechanism will enable better situational understanding empowering decision making. As future coalition operations are expected to be dynamic with the ever-increasing complexity of the tactical network, automated, dynamic resource management and allocation for distributed analytics services will be critical, and research in this project directly addresses key aspects of such capabilities.

More specifically, Task 1 addresses two key challenges to providing coalition partners the capability of flexible infrastructure configuration to meet mission demands and distributed analytics despite network dynamics: (1) to understand the fundamental performance limits for distributed SDC control and (2) develop distributed control mechanisms to achieve such performance limits through online resource allocation. Without the new distributed control mechanisms for SDC, coalition partners will not be allocated their required resources efficiently according to the current infrastructure conditions for carrying out their missions and services. Theoretical limits will be essential to allow network planning to occur prior to operational deployment, as will tools that can advise as to whether changes to networks would provide worthwhile improvements. If these “rules” can be implemented as automatically running (sub)systems, it would relieve the in-field operators of the currently manual task of network traffic prioritization and routing.

Task 2 will focus on the design of a methodology for the placement as well as scheduling of compute and data resources across the SDC, to enable the important capability of superior situational understanding and enhanced decision making through carefully determined service provisioning in tactical situation[78]. The algorithms for agile code and agile data deployment support different levels of dynamics that can occur in different stages of a tactical

[78] The U.S. Army Operating Concept: Win in a Complex World, http://usacac.army.mil/sites/default/files/documents/cact/ArmyOperatingConceptSummary.pdf

mission, and the proposed technique is suitable to different scenarios. The mathematical framework will provide rigorous guarantees on optimality, robustness, and complexity in adversarial (worst-case) settings in tactical environments. Also, the Quality of Analytics (QoA) validation mechanism will provide an important basis of a trust metric among different coalition members, which can guide the positioning of analytics services especially in critical scenarios. It will also provide the foundation for an adaptive data/service negotiation framework among coalition members.

Collaborations, Staff Rotations, and Linkages

Project 1 is investigating inter-domain SDC control mechanisms, such as optimal controller placement and East-West control protocol, which will provide infrastructure-level support for executing and controlling distributed analytics services in Project 3. Conversely, work in Project 3 will help the control-plane mechanisms in Project 1 make more informed decision with respect to the resource availability and analytics service placement. P1-P3 linkage will be provided by Kin Leung (Imperial), who is working on both of the projects.

Work on generative policies in Project 2 will provide the insights on dynamic security management that needs to be taken into account when controlling and executing distributed analytics services in coalition settings. Conversely, the performance objectives and QoA agreement requirements in running distributed analytics will provide an important workload for dynamic policy management.

Project 3 has a direct linkage with Project 4, which is exploring issues in self-awareness and self-composability of the analytics services. Project 3 team will work with Project 4, providing the perspectivies and mechanisms for positioning and scheduling distributed analytics services. This linkage will be facilitated by Tom La Porta (PSU).

Project 5 is looking at approaches for anticipatory situational understanding, which will provide models of distributed analytics to be subjected to the resource alloction and scheduling work in Project 3. Mark Herbster (UCL) will collaborate with Simon Julier (UCL) of Project 5 to ensure that both teams are appraised of progress in the respective projects.

Finally, group-behavior models to be explored in Project 6 can be leveraged to describe the composition and to inform the resource allocation decision for matching user demands on analytics services. This linkage will be explored by Don Towsley (UMass), who is working on both projects.

Investigators and students of P3 will participate in periodical conference calls and have mutual visits to ensure steady progress of our research. In particular, members from the Imperial team plan to visit colleagues at IBM US, UMass, BBN and ARL during the summers of 2018 and 2019 for technical exchanges and collaborations.

Research Milestones		
Due	**Task**	**Description**
Q1	**Task 1**	Slides or report: Initial mathematical models and results on quantifying computation fidelity vs. time deadline (BBN, UMass, and ARL); Initial definition of analytics capacity (BBN, UMass, Imperial, ARL).
Q1	**Task 2**	Find special cases of the frame-based service configuration (FBSC) problem which have polynomial-time algorithms for data placement. Write-up on polynomial-time algorithms for special cases of the FBSC problem. (UCL, PSU, IBM US) Identify and formulate the requirements and constraints of tactical analytics applications in wireless coalition systems. Provide results on the problem formulation. Slides on the formulation of the generic code/data placement and scheduling problem. (UCL, IBM US, IBM UK) Identify QoA measures, the corresponding per-node/link performance

Research Milestones		
Due	**Task**	**Description**
		metrics, and their relationship. Provide results on the metrics. Slides on the classification of QoA measures and associated observation models relating these measures to internal network states. (PSU, IBM US, IBM UK) Develop an efficient algorithm for computing the most efficient scheduling of a set of data between two nodes in a network when we have both bandwidth and latency restrictions. Write-up on the algorithm for optimal unicast routing when we have both bandwidth and latency restrictions. (UCL, IBM US)
Q2	**Task 1**	Slides or report: Initial mathematical models to represent availability of resources (Imperial, UMass, ARL)
Q2	**Task 2**	Develop a polynomial-time algorithm for giving a data placement for the FBSC problem that approximately obtains the constraints. Short paper on approximate algorithm for the FBSC problem. (UCL, IBM US) Formulate the adaptive service configuration problem (without prediction) using online learning framework, identify its hardness and approximability. Provide results on the problem formulation. Slides on the problem formulation and hardness/approximability results of adaptive service configuration. (IBM US, PSU, IBM UK) Formulate the absolute QoA validation problem for representative QoA measures capturing transient behaviours and establish the necessary/sufficient conditions for detectable violations. Provide results on the problem formulation. Slides on the problem formulation and detectability conditions for absolute QoA validation. (PSU, IBM US, IBM UK)
Q3	**Task 1**	Reports: Initial mathematical models for communication vs. computation tradeoff within one SDC slice (BBN, UMass, ARL); Comparison between resource allocation performance using the effective-bandwidth representation model for distributed control, and fundamental communication vs. computation tradeoff under optimal control (BBN, Imperial)
Q3	**Task 2**	Propose algorithm for online placement of code/data under multiple types of resources and coalition constraints, which does not consider the communication overhead. Paper on the algorithm for online code/data placement with multiple resource types and coalition constraints. (IBM US, PSU) Develop algorithms to detect/localize violations of absolute QoA agreement. Slides on algorithms for detecting/localizing violations of absolute QoA agreement. (PSU, IBM US, IBM UK) Develop an experimentation scenario based upon real-world networking and analytics traces to support research evaluation and validation. A trace-driven experimentation capability with flexibility to support research validation across Subtasks 1 and 2 in simulation and emulation. (IBM UK, IBM US, PSU, UCL) Combine results in Q1 and Q3 to develop algorithms for the FBSC problem when, in addition to the original bandwidth limitations, we now have non-negligible latencies. Paper on the algorithm for FBSC with non-negligible

Research Milestones		
Due	**Task**	**Description**
		latencies. (UCL, IBM US) Develop algorithms to find an optimal scheduling of data flow to go from one data distribution to a new (approximate) solution to the FBSC problem when the network changes, to address the problem of stable service configuration under runtime dynamics. Write-up on the algorithm for redistributing data for the FBSC problem in optimal time. (UCL, IBM US)
Q4	**Task 1**	Reports/papers: Quantify effectiveness of the proposed representation models for resource allocation (Imperial, UMass) Characterization of analytics capacity of simple analytics workflows (BBN, UMass, Imperial, ARL); Implementable and executable algorithms for resource allocation (IBM UK, Imperial, and UMass)
Q4	**Task 2**	Propose algorithm for online transfer of code/data under coalition constraints and given code/data locations. Technical report on online code/data transfer with coalition constraints. (IBM US, PSU) Propose algorithms to generate coresets based on distributed data for general machine learning problems. Paper documenting the coreset formulation, underlying assumptions, algorithms, and performance evaluation. The performance evaluation will be based on experiments with various distributed datasets and machine learning problems. (PSU, IBM US, IBM UK) Incorporate non-negligible latencies in the work on the FBSC problem done in Q3. Write-up on the algorithm for redistributing data for the FBSC problem when we have non-negligible latencies. (UCL, IBM US) Develop an extended algorithm for the FBSC problem when applications can be run on any machine and are not pre-assigned. Write-up on the algorithm for the FBSC problem when applications can be run on any machine. (UCL, IBM US) Paper on the algorithm for the FBSC problem when applications can be run on any machine and which computes optimal redistribution scheduling when we have non-negligible latencies. (UCL, IBM US)
Q5	**Task 1**	Report/paper: Performance comparison of executable resource allocation algorithm and fundamental tradeoff limits for resource allocation between two SDC slices (BBN, Imperial and ARL)
Q5	**Task 2**	Combine results in Q3 and Q4 and propose algorithm for online joint placement and transfer of code and data, study the convergence rate and optimality gap of this algorithm. Write-up on the algorithm and optimality results for online code/data placement and transfer in coalition environments. (IBM US, PSU) Formulate the problem of joint coreset construction and data quantization to support machine learning problems in resource-limited networks. Slides on problem formulation. (PSU, IBM US, IBM UK)
Q6	**Task 1**	Reports/papers and software: Multi-objective optimization (MOO) formulation for resource allocation (Imperial, UMass, ARL);

Research Milestones		
Due	**Task**	**Description**
		Characterization of analytics capacity of complex analytics workflows (BBN, UMass, Imperial, ARL); Testing of resource management algorithms through emulation (IBM UK, Imperial)
Q6	**Task 2**	Validate the performance of the online code/data placement and transfer algorithm proposed in Q5 via trace-driven simulations. Paper documenting the formulation, conditions, algorithms, and performance evaluation of adaptive service configuration without predictions. (IBM US, PSU, IBM UK) Develop algorithms to jointly quantize data and construct coresets to approximate machine learning cost functions subject to various resource constraints (e.g., battery, bandwidth, latency). Slides on the proposed algorithms. (PSU, IBM US, IBM UK)
Q7	**Task 1**	Report/paper: Performance evaluation of resource provisioning, allocation and control for multiple simultaneous SDC slices for robust control under network dynamics (BBN, UMass, Imperial, IBM UK)
Q7	**Task 2**	Validate performance of the proposed quantization and coreset construction algorithms analytically and empirically. Technical report documenting the problem formulation, algorithms, and performance evaluation. (PSU, IBM US, IBM UK) Develop emulation platform based on CORE/EMANE to validate the core set of algorithms proposed in this task. Demonstration showing benefits of the proposed algorithms in emulated wireless coalition systems. (IBM UK, IBM US)
Q8	**Task 1**	Report/paper and software: Assessment of MOO approaches for resource allocation (Imperial, UMass, ARL); Demonstrable algorithms for resource management running on practical devices (laptops/raspberry pies) coupled with emulation (IBM UK, Imperial)
Q8	**Task 2**	Compare the results with only performing quantization or only performing coreset construction under the same resource constraints. Paper on these results. (PSU, IBM US) Develop prototype to validate the core set of algorithms proposed in this task. Demonstration showing benefits of the proposed algorithms in prototyped wireless coalition systems. (IBM UK, IBM US)

Project 4: Instinctive Analytics in a Coalition Environment

Project Champion: Raghu Ganti, IBM US

Email: rganti@us.ibm.com **Phone: 1-914-945-2164**

Primary Research Staff	Collaborators
Graham Bent, IBM UK	Brian Henz, ARL
Hamish Hunt, IBM UK	Kevin Chan, ARL
Ian Taylor, Cardiff	Olwen Worthington, Dstl
Kaushik Roy, Purdue	Padraig Corcoran, Cardiff
Raghu Ganti, IBM US	Alun Preece, Cardiff
Thomas La Porta, PSU	Murat Sensoy, Cardiff and Ozyegin
Geeth de Mel, IBM UK	Peter Waggett, IBM UK
Sebastian Stein, Southampton	Swati Rallapalli, IBM US
Leandros Tassiulas, Yale	Elisa Bertino, Purdue
Heesung Kwon, ARL	Enrico Gerding, Southampton
Chris Simpkin (PGR), Cardiff	Richard Tomsett, IBM UK
Unnamed PGR, Cardiff	Gavin Pearson, Dstl
Unnamed PGR, Purdue	Marcus Brede, Southampton
Unnamed PGR, PSU	Tim Norman, Southampton
Valerio Restocchi (PDR), Southampton	Victor Valls Delgado (PDR), Yale
Sukankana Chakraborty (PGR), Southampton	
Edward Cater (PGR), Southampton	
Fan Bi (PGR), Southampton	
Bhargavi Parthasarathy (PGR), Southampton	

John V (Vinnie) Monaco, ARL	
Nick Nordlund (PGR), Yale	

Project Summary/Research Issues Addressed

One of the key challenges with performing distributed analytics in a coalition environment is to automatically compose complex services to dynamically match operational tasks to information resources, *accounting for impact*, in a many-to-many temporally and spatially complicated and complex situation. In a dynamic and agile environment, such as coalition environments, the state of the network and resources cannot be completely known or controlled due to the evolving nature of the network and constraints that may preclude partners from accessing complete state information about different parts of the system. In addition, there may be requests made to the system that have not been made before, requiring services to be created on the fly. Thus, the ultimate goal of the project is to formalize and theorize the fundamentals for a system such that it enables service elements to automatically configure themselves to perform analysis tasks based on user specified goals taking account of (system and user) context [79,80].

This project helps attain these goals by matching requests to services that may best fill the information need, and allocating resources in a constrained, coalition environment to maximize the utility of the system. The utility may be measured in several ways, all of which capture a notion on the urgency and importance of information to the overall user community.

Our goal for this project is to determine the best analytics services to meet requests, and then to allocate these resources to the outstanding requests; for resources, we consider both data and logic to perform analytics functions associated with distributed coalition settings. We consider that requests may be satisfied by more than one resource in some cases, and that in other cases there may be no perfect match between possible services and requests, thus yielding to the need for *best partial matches* w.r.t. mission context, especially in mission-critical situations. We also consider that resources are constrained physically (e.g., energy, bandwidth) and logically (e.g., user intentions, policy prohibition, and so forth) having varying utility in dynamic coalition context, thus making it impractical—if not impossible—to satisfy every request. We will explicitly consider a coalition environment in which some resources may be shared, and partners may not fully or honestly disclose the utility of their missions.

During the IPP phase of the DAIS ITA, we proposed novel approaches to represent service semantics by combing vector representations with graph semantics to brain inspired models; in terms of resource allocation in such semantically rich environments, we investigated dynamic and complex scheduling mechanisms so that analytics could be matched with highly variable requirements in the coalition operating environments[81]. In this BPP, through the task 1, will substantially expand that research by developing formal foundations for semantically aware service matchmaking by considering instinctive semantics for services as well as researching on mechanisms for resource selection—and allocation—when resource agents are not the typical benevolent agents that have been considered in the state-of-the-art distributed resource allocation research. Specially, we will look at reinforcement learning techniques to evolve the models for resource and request matching and adaptive learning mechanisms over online resource allocation techniques to respect the changes in the operating environment. Furthermore, in support of matchmaking, we will investigate techniques to model in-context utility of resources so that varying coalition conditions are considered when selecting resources for requests. Additionally, we will employ proper utility

[79] Verma, D., Bent, G.A., Taylor, I., Towards a distributed Federated Brain Using IoT Devices, COGWEB, COGNITVE '17, Athens, Greece, Feb 2017.

[80] Bent, G.A., De Mel, G., Rallapalli, S., Simpkin, C., Taylor, I., Decentralized Microservice Workflows for Coalition Environments. In conjunction with IEEE smart world conference (IEEE SWC 2017), August 4-8, 2017.

[81] Simpkin, S., de Mel, G., Bent, G., Khamfroush, H., Taylor, I., Ortiz, J., Stein, J., Rallapalli, S., He, T., La Porta, T., 2017, June. Instinctive analytics for coalition operations (Conference Presentation). In SPIE Defense+ Security (pp. 1019008-1019008). International Society for Optics and Photonics.

functions to quantify the semantics of specific analytic tasks and project them to be used in objective functions of the optimization problems, thus providing desirable assignment strategies.

To efficiently provide instinctive analytics services, we will perform high risk research that might lead to a future architecture that we describe as a distributed federated brain. The concept is based on the development of services that ultimately exhibited true cognitive capabilities and which might be implemented in completely different technologies to those used today. We suggest that Non Von Neumann architectures, such as those employed in neuromorphic processing and quantum computers, might be potential candidates. We recognise that the future computing environment will include both Von Neumann and Non Von Neumann machines and the coalition needs to be able to compose and orchestrate complex services utilising these different compute resources.

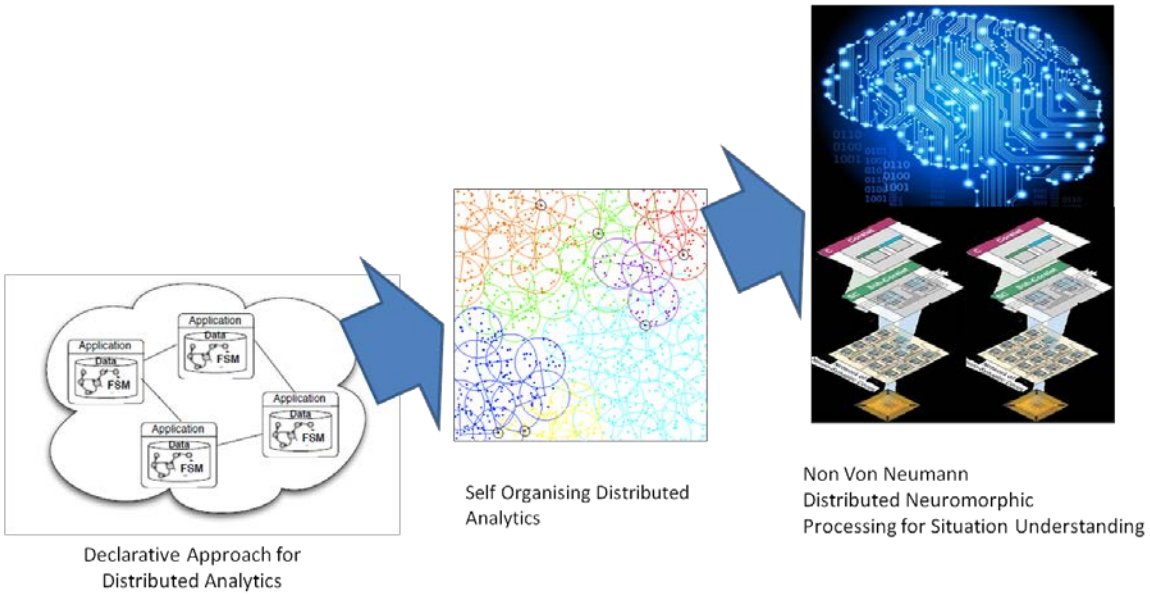

Figure P4-1. Evolution of a distributed federated brain

In the IPP, we investigated a simple model of a distributed brain by envisaging microservices that are distributed across a heterogeneous network with microservices being owned by different organizations. Rather than searching for microservices and then centrally compiling a workflow, as in the standard service oriented architecture model, in our model each microservice learns its role and binds this into its own symbolic vector representation (this is an online learning task). A user can request a high level task to be performed by declaratively specifying the precise service composition they require using a symbolic vector representation of the workflow. These vector representations need to capture not just the semantic meaning of the service composition of which the microservice is a part but also the order in which the microservices are called.

Whilst the use of symbolic vector representations offers an exciting new method for self-describing services and controlling distributed workflow it only represents the first two stages in the evolution of the distributed brain shown in figure P4-1. In this project, we seek to lay the foundations for achieving the final step of self-aware cognitive services that perform analytics in more brain like ways.

Technical Approach

This project comprises two related tasks. In the first task, we determine the best analytics services (henceforth referred to as *resources*) to meet requests, and then how to allocate these resources to the outstanding requests (including cases where requests may well exceed resource capacity); for resources, we consider both data and logic to perform analytics functions associated with distributed coalition settings. In the second task we explore ways to efficiently provide cognitive analytics services. This includes using neuromorphic computing architectures and using compact representations of services.

Task 1 will be conducted in three inter-related subtasks. The first subtask will focus on algorithms to process analytics service requests and determine the closest match to analytics processing and data available in the system. The second subtask will explore mechanism design for resource allocation. We will consider settings where service requesters may report their utility strategically, and we will design resource allocation mechanisms that are robust to such strategies. In the third subtask, we will use complex scenarios for analytics processing flow that involve multiple data streams including video, speech, audio as well as situational awareness data streams; we will explore resource allocation for different analytics tasks—especially w.r.t. the multimodality of coalition's information sources.

Task 2 also comprises three subtasks. The first subtask seeks to develop a mathematical framework for cognitive processing that can be applied to the challenge of distributed analytics. The second subtask investigates the types of distributed analytic processing that can be performed using cognitive processing. Subtask 3 investigates how future self-aware cognitive services might be realized in non Von Neumann architectures such as neuromorphic processors and quantum computers.

Task 1: Resource Allocation for Dynamically Formed Distributed Analytics Services

Primary Research Staff	Collaborators
Thomas La Porta, PSU	Kevin Chan, ARL
Geeth de Mel, IBM UK	Gavin Pearson, Dstl
Sebastian Stein, Southampton	Peter Waggett, IBM UK
Valerio Restocchi (PDR), Southampton	Graham Bent, IBM UK
Heesung Kwon, ARL	Swati Rallapalli, IBM US
Sukankana Chakraborty (PGR), Southampton	Murat Sensoy, Cardiff and Ozyegin
Edward Cater (PGR), Southampton	Elisa Bertino, Purdue
Fan Bi (PGR), Southampton	Enrico Gerding, Southampton
Bhargavi Parthasarathy (PGR), Southampton	Markus Brede, Southampton
Unnamed PGR, PSU	Timothy Norman, Southampton
Nick Nordlund (PGR), Yale	Richard Tomsett, IBM UK
Leandros Tassiluas, Yale	Victor Valls Delgado, Yale

The aim of this task is to (1) determine the best analytics services for existing and emerging requests in dynamic coalition environments; and (2) instantiate the identified analytic pipelines to meet the requirements of outstanding requests (inc. optimal response when demand exceeds supply). We will specifically focus on *best partial matches* w.r.t. mission context, especially in mission-critical situations as there may be no perfect match between possible services and requests. We propose to develop general matchmaking and resource allocation algorithms w.r.t. the perceived utility of resources, and to perform a detailed evaluation by applying the research to a complex video analytics scenario. In order to support this vision, the research in the task will be conducted in three inter-related subtasks: **(1) Analytics Matchmaking**: we will process analytics service requests and determine the

closest match to analytics processing and data available in the system; the result will be a set of possible solutions, and an achieved utility based on the request and the closeness of match with the solutions; **(2) Mechanism Design for Resource Allocation:** we will consider settings where service requesters may report their utility strategically, and we will design resource allocation mechanisms that are robust to such strategies; and **(3) Resource Allocation for Real-Time Analytics:** we will use a detailed video analytics processing flow developed in the IPP (along with the NS-CTA program), and explore different analytics tasks—especially w.r.t. the multimodality of coalition's information sources—to which we will apply and refine algorithms from subtasks 1 and 2.

Additionally, proper utility functions will be employed to quantify the semantics of specific analytics tasks and being used in objective functions of the optimization problems, the solution of which will provide desirable assignment strategies. Task level utility functions will express the priorities of individual tasks competing for resources in the distributed computational infrastructure. Proper synthesis of objective functions from individual utility functions may reflect global coalition objectives when central coordination is possible. When individual tasks compete autonomously for resources, proper mechanisms design frameworks will ensure effective allocation among the competing agents and in accordance to their global value.

Subtask 1.1: Analytics Matchmaking in Distributed Coalition Environments

In prior work, we have done extensive work on matching sensors of various types to competing missions with different requirements[82,83]. Specifically, we used semantic reasoning to match assets to requests[84], developed utility functions to capture the fit of sensor assignments to missions[85], and dealt with budgets[86,87]. There are three main differences with the work of this task when compared to the previously mentioned work:

1. The requests in the aforementioned work were formed w.r.t. domain ontologies or by interpreting domain specific tasks[88] with well-defined semantics so that the user intent could be inferred in a straightforward manner. However, through this proposal, we will investigate means to infer user intent from requests, especially when urgency and importance w.r.t. context needs to be captured to determine the requests that need to be satisfied right away and those requests that could be satisfied incrementally. Additionally, we will utilize and expand on the state-of-the-art on pragmatically aware query reformulation research to infer user intent, especially in situations where there is only a partial match to requests or potentially alternative means to achieve outstanding requests[89,90]. We envision such will enable systems to infer which resources to share, reassign, or to instantiate by create more complex contextual ranking function w.r.t. properties such as urgency, timeliness, required quality and importance.

---

[82] De Mel, G.R., Vasconcelos, W. and Norman, T., 2014. Intelligent Resource Selection for Sensor-task Assignment: A Knowledge-based Approach (Doctoral dissertation, Aberdeen University).

[83] Rowaihy, H., Johnson, M.P., Liu, O., Bar-Noy, A., Brown, T. and Porta, T.L., 2010. Sensor-mission assignment in wireless sensor networks. ACM Transactions on Sensor Networks (TOSN), 6(4), p.36.

[84] Gomez, M., Preece, A., Johnson, M., De Mel, G., Vasconcelos, W., Gibson, C., Bar-Noy, A., Borowiecki, K., La Porta, T., Pizzocaro, D. and Rowaihy, H., 2008. An ontology-centric approach to sensor-mission assignment. Knowledge Engineering: Practice and Patterns, pp.347-363.

[85] Rowaihy, H., Johnson, M.P., Pizzocaro, D., Bar-Noy, A., Kaplan, L., La Porta, T. and Preece, A., 2009, June. Detection and localization sensor assignment with exact and fuzzy locations. In International Conference on Distributed Computing in Sensor Systems (pp. 28-43). Springer, Berlin, Heidelberg.

[86] Johnson, M., Rowaihy, H., Pizzocaro, D., Bar-Noy, A., Chalmers, S., La Porta, T. and Preece, A., 2008. Frugal sensor assignment. Distributed Computing in Sensor Systems, pp.219-236.

[87] Johnson, M.P., Rowaihy, H., Pizzocaro, D., Bar-Noy, A., Chalmers, S., La Porta, T. and Preece, A., 2010. Sensor-mission assignment in constrained environments. IEEE Transactions on Parallel and Distributed Systems, 21(11), pp.1692-1705.

[88] Irvine, J.M., 1997, July. National imagery interpretability rating scales (NIIRS): overview and methodology. In Proceedings of the International Society for Optical Engineering (SPIE) (Vol. 3128, pp. 93-103).

[89] Viswanathan, A., de Mel, G. and Hendler, J.A., 2015. Pragmatics and Discourse in Knowledge Graphs.

[90] Viswanathan, A., Michaelis, J.R., Cassidy, T., de Mel, G. and Hendler, J., 2017, May. In-context query reformulation for failing SPARQL queries. In Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR VIII (Vol. 10190, p. 101900M). International Society for Optics and Photonics.

2. The sensor matching for mission work focused on sensor networks, thus relied on physical devices and locations, whereas in this work we are looking at a high level of abstraction that deals with information distilled from information resources operating in a network. Thus, we are not assigning a single, or multiple, distinct physical devices to detect known phenomena based on their location, but are instead (1) determining if processing services and data exist that can be used together to answer a query, and (2) determining the closeness of the information that we distil to the original request. There are two entities that need to be matched (processing services and data), and the compatibility of the data and processing service must also be matched.
3. The semantic matchmaking work in previous research only considered complete matches—though partial matches were considered w.r.t. individual resources, they were bundled together as resource packages to fully cater for the needs of requests—for resource requests w.r.t. to a predefined ontology. However, in coalition's analytics domain, we envision that partial matches will have to be considered, especially w.r.t. the utility provided by them, even when composite services are put together to satisfy requests. This is because parties involved in a coalition may compute the completeness—or value of the information—provided by analytics very differently; also, the parties involved in the coalition will naturally temper the analytics and the information coming from them w.r.t. the perceived provenance and trust matrices. Therefore, in this proposal, we aim to use such properties to develop contextual ranking mechanisms for analytics, especially when there are multiple matches—full or partial—to a request; this we envision is possible due to the inferred contextual properties such as task urgency and importance, user preferences, and, resource constrains and status w.r.t. existing and incoming requests.

Throughout the subtask, we perceive an ontology—or the domain model—associated with the matchmaking work to be an agile representation—i.e., we will consider means in which the ontology is expanded based on the selections made by the analytic users through techniques such as reinforcement learning and active learning mechanisms. Such approaches have already been applied in centralized service repository research but we aim to investigate techniques on doing so when the analytics are deployed in distributed coalition environments where systems do not possess a bird's-eye-view of the analytic space. Active learning techniques will enable our mechanisms to cope with unknown situation (e.g., by having a conversation with human experts), thus enhancing the future experiences of the matchmaking algorithms. However, the actual means of learning is opaque and non-intuitive for the end-user; this is especially true for coalition environments where the edge user is a generalist who has to interact with such learning systems to define and execute tasks. Motivated by this observation, in this task we will develop techniques to explain the learning (aka *Explainable AI*[91]) so that users can critique, understand and hence trust the systems they are using. Thus, these techniques will enable us to introduce the *instincts* human experts bring into the resource and request matching to algorithmic space too.

Subtask 1.2: Game Theory and Mechanism Design for Resource Allocation with Strategic Agents

Current resource allocation algorithms assume that service requesters truthfully report their requirements and mission utilities, even if this means their analytics tasks are delayed or rejected. This is unrealistic in a coalition environment, where requesters are drawn from across many different coalition partners; although they share the same broad objectives, requesters also pursue the interests of their own internal group. Thus, they should be treated as self-interested agents that may behave strategically (e.g., by misreporting analytics priorities or constraints); additionally, different coalition partners may view requests as having different utility and costs, thus adjusting their responses.

To address this key shortcoming, we will turn to the related fields of game theory and mechanism design[92], which provide tools for modelling self-interested behaviour and for incentivising agents to truthfully report their utilities. While there is existing work that has applied these approaches to resource scheduling[93,94], it does not deal

[91] https://www.darpa.mil/program/explainable-artificial-intelligence

[92] Nisan, N., Roughgarden, T., Tardos, E. and Vazirani, V.V. eds., 2007. Algorithmic game theory (Vol. 1). Cambridge: Cambridge University Press.

[93] Stein, S., Gerding, E.H., Rogers, A.C., Larson, K. and Jennings, N.R., 2011. Algorithms and mechanisms for procuring services with uncertain durations using redundancy. Artificial Intelligence, 175(14), pp.2021-2060.

[94] Conitzer, V. and Vidali, A., 2014, July. Mechanism Design for Scheduling with Uncertain Execution Time. In AAAI (pp. 623-629).

with the challenges inherent in coalition environments, including the high dynamism of analytics tasks, rapidly changing network compositions and demand, and balancing coalition objectives with the limited view of self-interested task requesters. Specifically, we will develop a new science of mechanism design in coalition settings by investigating the following:

- We will develop *online mechanisms for resource allocation in coalitions*—i.e., we will develop new mechanisms that do not know in advance what tasks will be submitted and need to make scheduling decisions immediately as new tasks arrive. We will build on prior work on online mechanism design[95], but will extend it to coalition environments; the key challenge in doing this is to consider highly heterogeneous resources and task requirements, and we will build on the matchmaking techniques developed in subtask 1 to achieve this;
- We will investigate *adaptive learning mechanisms for resource allocation in coalitions*—i.e., we will consider realistic coalition operations where accurate statistical knowledge of demands (as assumed by existing work[95,96]) is not known in advance and where conditions change rapidly over time. Thus, there is a need for allocation mechanisms to learn from and adapt to the prevailing situation, and which do not inhibit tactical operational success due to slow response to rapid change in user-context. On one hand, this requires the integration of machine learning techniques into mechanism design approaches (including those considered in subtask 1); on the other hand, this needs to be done in a way such that desirable properties of the mechanism design are preserved.
- We will also *balance global mission objectives with local interests*—i.e., mechanisms typically aim to maximise the social welfare within a system (i.e., the total sum of all agents' utilities). However, this may not always be appropriate. On a global level, the coalition may sometimes wish to prioritise the tasks of particular agents (e.g., if those are involved in the main effort or a very time-sensitive mission). Similarly, expectations and rational behaviour between suborganisations may also vary. Some may have a poorly calibrated view of their own requirements, which could lead to their tasks being allocated incorrectly. This also raises the question of how local and global objectives of different agents can be directly compared to each other. To address these issues, we will look at global control mechanisms that can calibrate and adjust task priorities between competing agents. Part of the utility functions could be extracted directly from task descriptions and augmented by global decision-makers who can prioritise certain task types or the higher-level missions they are part of. This could also explore synergies between different but related tasks (e.g., if the results of one service are likely to be useful to future service requests).
- Finally, we will *develop new decentralized resource allocation mechanisms*—i.e., we will move beyond the framework of mechanism design, which typically assumes a centralized allocation and the possibility of utility transfers, to investigate more general mechanisms that relax these assumptions. These will employ techniques from game theory to model how heterogeneous, self-interested agents will behave in complex resource allocation settings that are relevant to coalition operations. Specifically, we will look at how services should be distributed in these settings and how agents can learn to cooperate and coordinate despite their self-interested nature, for example through the introduction of appropriate policies, learning mechanisms or communication and negotiation protocols.

Subtask 1.3: Resource Allocation for Real-Time Analytics

One of the challenges in resource allocation problems is that they cannot be solved in an offline manner since the demand for resources is not known a priori. As a result, most resource allocation algorithms are heuristics that cannot maximize the use of resources in the system. A notable exception, however, is the case of the max-weight scheduling algorithm[97] (with variants for data analytics[98,99]), which can maximize the use of resources in a system

[95] Stein, S., Gerding, E., Robu, V. and Jennings, N.R., 2012, June. A model-based online mechanism with pre-commitment and its application to electric vehicle charging. In Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems-Volume 2 (pp. 669-676). International Foundation for Autonomous Agents and Multiagent Systems.

[96] Myerson, R.B., 1981. Optimal auction design. Mathematics of operations research, 6(1), pp.58-73.

[97] Tassiulas, L. and Ephremides, A., 1992. Stability properties of constrained queueing systems and scheduling policies for maximum throughput in multihop radio networks. IEEE transactions on automatic control, 37(12), pp.1936-1948.

[98] Destounis, A., Paschos, G.S. and Koutsopoulos, I., 2016, April. Streaming big data meets backpressure in distributed network computation. In Computer Communications, IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on (pp. 1-9). IEEE.

without statistical knowledge of the analytics arrival processes. However, optimality comes at the price of an exponential increase of the delay. This issue is critical in many systems, but in particular when delay sensitive applications compete for resources with throughput-intensive applications that are also delay tolerant. As a result, system utilization is usually sacrificed (overprovisioning) in order to obtain a good delay performance. The importance of providing services with low delay is widely acknowledged by both industry and academy, and has received a lot of attention in recent years[100,101,102,103,104]. For instance, in[100], authors show that low delay variability is crucial for providing many of their analytics—including web search and augmented reality—and identifies causes of the delay in their systems. These include multiple flows competing for computation and communication resources[105], and the use of multiple queueing layers interconnecting resources. The approaches in[101,102] take the delay issue to the extreme, and propose heuristic algorithms that work without[106] queues, thus enhancing the performance in terms of delay; however, in such work, the system utilization attributes are not clear w.r.t. resources.

In view of all this, we believe it is essential to establish the mathematical foundations that allow us to maximize the use of resource while providing low delay to real-time analytics. The technical approach we will follow consists of combining stochastic optimization techniques from control theory (max-weight[97]) with deterministic interior-point[107] algorithms in convex optimization. These two approaches are in marked contrast to each other: while max-weight algorithms make decisions in an online manner and create congestion, interior-point methods produce no congestion[108] but they can only be implemented in an offline manner. Hence, they cannot be used in real system. Our goal is to bring the knowledge of max-weight algorithms to interior-point methods, and design a new class of algorithms—which we call *approximate interior-point methods*—that can handle stochasticity, are resilient to system perturbations, and are able to provide low-delay.

---

[99] Huang, L. and Neely, M.J., 2011. Utility optimal scheduling in processing networks. Performance Evaluation, 68(11), pp.1002-1021.

[100] Chen, G.J., Wiener, J.L., Iyer, S., Jaiswal, A., Lei, R., Simha, N., Wang, W., Wilfong, K., Williamson, T. and Yilmaz, S., 2016, June. Realtime data processing at facebook. In Proceedings of the 2016 International Conference on Management of Data (pp. 1087-1098). ACM.

[101] Dean, J. and Barroso, L.A., 2013. The tail at scale. Communications of the ACM, 56(2), pp.74-80.

[102] Grosvenor, M.P., Schwarzkopf, M., Gog, I., Watson, R.N., Moore, A.W., Hand, S. and Crowcroft, J., 2015, May. Queues don't matter when you can jump them! In NSDI (pp. 1-14).

[103] Perry, J., Ousterhout, A., Balakrishnan, H., Shah, D. and Fugal, H., 2015. Fastpass: A centralized zero-queue datacenter network. ACM SIGCOMM Computer Communication Review, 44(4), pp.307-318.

[104] Kulkarni, S., Bhagat, N., Fu, M., Kedigehalli, V., Kellogg, C., Mittal, S., Patel, J.M., Ramasamy, K. and Taneja, S., 2015, May. Twitter heron: Stream processing at scale. In Proceedings of the 2015 ACM SIGMOD International Conference on Management of Data (pp. 239-250). ACM.

[105] Computation and communication resources correspond, respectively, to shared resources and global shared resources.

[106] Queues with packets that are on-the-fly

[107] Y. Nesterov and A. Nemirovskii, “Interior-point polynomial algorithms in convex programming,” SIAM Journal on Applied Mathematics, vol. 55, no. 4, 1994

[108] constraints are never violated, so no queues

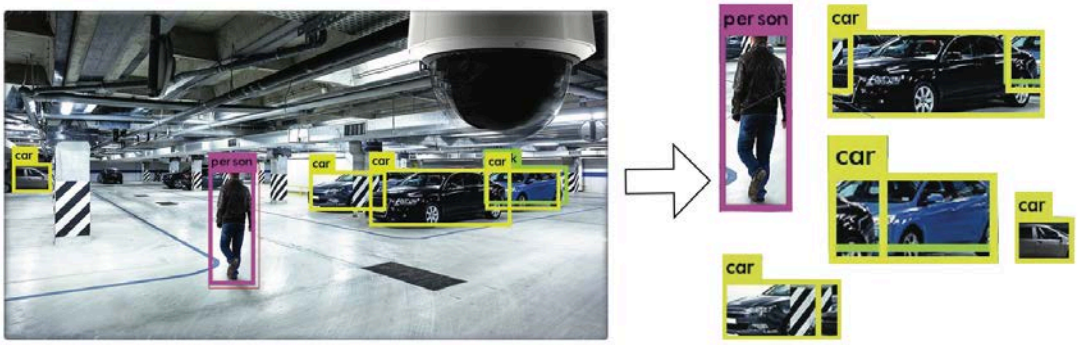

Figure P4-2. Object Detection with Specialized Image Classification Models.

As paradigm application, as shown by figure P4-2, we consider real-time surveillance analytics that combines object detection with specialized image/audio classification models[109]. The reasons for choosing this application are threefold: (1) the analytics has to be performed in real-time; (2) it involves the intensive use of computation and communication resources; and (3) it is highly suitable for the research proposed here as it requires the use of multimodality of data (videos, audio, location report, text) and trained models such as situational awareness, and processing services (detection, localization, tracking). We will explore resource allocation for different analytics tasks—especially w.r.t. the multimodality of coalition's information sources—e.g., in the case of tracking a person, this could be done with a wide range of sensors and processes (e.g. voice recognition is used to identify a person at a location using the mobile phone location and we then get a picture—or video—of the person at that location and then track them from a number of cameras. We can then instantiate a set of alternative workflows that change dynamically to maintain the track. We envision that the matching part of the proposal (subtask 1) will solve the problem of which models and processing services can best extract information requested. The resource allocation subtasks will determine where to perform the object detection and classification tasks, and which paths the data should be routed so that data transmission experiences no or very low congestion.

Task 2: Self-aware Cognitive Services for Distributed Coalition Environments

Primary Research Staff	Collaborators
Graham Bent, IBM UK	Brian J Henz, ARL
Hamish Hunt, IBM UK	Olwen Worthington, Dstl
Ian Taylor, Cardiff	Padraig Corcoran, Cardiff
Chris Simpkin, Cardiff	Alun Preece, Cardiff
Unnamed PGR, Cardiff	Peter Waggett, IBM UK
Kaushik Roy, Purdue	Swati Rallapalli, IBM US
Unnamed PGR, Purdue	

[109] Object detection algorithms can only detect broad classes of objects, whereas image/audio classification can provide more detailed information about the object itself.

Ragu Ganti, IBM US	
John V (Vinnie) Monaco, ARL	

The ultimate goal of DAIS ITA is to investigate the basic science that will enable the creation of a distributed cognitive computer system (or distributed brain) that can perform analytics on demand across heterogeneous networks of interconnected devices in a military coalition setting operating in synergy with human users providing understanding of dynamic and complex situations involving multiple actors. Some of the capabilities of such a system will be to (i) understand user requests for analysis, (ii) seamlessly compose the desired analytics functions from other functions and services available in the network, (iii) identify the right data set needed for the analytics, and (iv) bring together the data and analytics required to perform the function. Recent developments in the fields of neurosynaptic processing and quantum computing will clearly play a role in meeting these objectives and it is inevitable that future systems will make use of these technologies. The questions that we seek to address in this task will provide a mathematical basis for developing next generation cognitive services that can make use of both existing and these future technologies to perform distributed analytics. These next generation services will provide the possibility to perform new types of analytics and potentially solve problems that have been considered impossible using current technologies. The impact on future military coalition operations is therefore somewhat speculative but we maintain that performing distributed analytics using these technologies requires a new approach based on a sound mathematical framework that we propose to lay the foundations for in this task.

We consider the challenge from the perspective of an interacting network of cognitive services that are self-describing, can self-discover other services with which they need to interact (including data services, network services, policy and security services) and can self-organize into appropriate service workflows to achieve the user requirements. The task builds on work done in the IPP, where we developed an approach based on the Vector Symbolic Architecture (VSA) [110, 111, 112, 113] in which services composition and the associated workflow are represented as semantic vectors. VSAs use a hyper-dimensional vector space to combine data and object features, all represented as symbolic vectors, into new symbolic vector representations that semantically represent the component vectors and their relationships. VSA vectors are therefore said to be semantically self-describing. The vectors can be compared to measure the semantic similarities between them and the component vectors can be unbound from the compound vectors up to some limited capacity[114]. VSA encoding schemes enable compound vectors to store ordered sequences of symbols and we have demonstrated that these can be used to orchestrate complex distributed workflows in a decentralized communications network.

These types of representation have been demonstrated to be capable of supporting a wide range of cognitive tasks including reasoning[115], semantic composition[116], analogical mapping[117] and representing word meaning and

[110] Plate,T.A., Holographic reduced representations. IEEE Transactions on Neural Networks, 6 , 623– 641.(1995).

[111] Plate, T., Holographic Reduced Representation: Distributed Representation for Cognitive Structures (CSLI Publications, Stanford, 2003).

[112] Kanerva,P., Hyperdimensional Computing: An Introduction to Computing in Distributed Representation with High-Dimensional Random Vectors, Cogn Comput (2009) 1:139–159 DOI 10.1007/s12559-009-9009-8, January 2009.

[113] Eliasith, C., How to build a brain, Oxford University Press 2013.

[114] Kleyko, D Pattern Recognition with Vector Symbolic Architectures. Ph.D. Dissertation. Luleåtekniska universitet, 2016.

[115] D. Widdows and T. Cohen, Reasoning with Vectors: A Continuous Model for Fast Robust Inference, Log J IGPL; 23(2):141–173 October 2015.

[116] A. Neelakantan, B. Roth, A. McCallum, Compositional Vector Space Models for Knowledge Base Inference, Knowledge Representation and Reasoning: Integrating Symbolic and Neural Approaches: Papers from the 2015 AAAI Spring Symposium.

[117] R.W. Gayler and S.D. Levey, A distributed basis for analogical mapping.

order[118]. There is however no existing mathematical framework for specifying the required cognitive services. Task 2 is also comprised three subtasks. The first subtask seeks to develop a mathematical framework for cognitive processing that can be applied to the challenge of distributed analytics. The second subtask investigates the types of distributed analytic processing that can be performed using cognitive processing. Subtask 3 investigates how future self-aware cognitive services might be realized in non Von Neumann architectures such as neuromorphic processors and quantum computers.

Subtask 2.1: Mathematical Representations for Distributed Cognitive Processing

Distributed representations of cognitive structures are based essentially on two operations (binding and superposing/chunking). Cognitive structures use binding to associate roles to fillers (e.g. Role:Agent; Filler:John) and creates relationships by superposing role-filler bindings (e.g. John-Loves-Mary). These can then be further bound into more complex knowledge graph representations. Initial representations of cognitive structures used matrices to represent roles which act on vectors representing fillers where the binding operation corresponds to matrix multiplication and superposition to vector addition.

VSA representations allow for higher level abstractions to be formulated in the same format as their lower level components. Plate's Holographic Reduced Representation (HRR)[110] describes how to use such operations on vector symbols, via role-filler, pairs in order to maintain positional or temporal relationships between objects as well as to learn deep and shallow semantic relationships between objects. In[119] Kanerva describes the use of Binary Spatter Codes (BSC) in combination with Random Permutations (RPM) to achieve a computationally more efficient version of the same[112].

In this subtask, we will develop a rigorous mathematical framework for Self-aware Cognitive Services. The objective is to develop a framework in which each microservice is described by a symbolic vector and service composition is performed through defined algebraic operations that go beyond the simple binding and superposition operations currently used. To achieve this objective, we will exploit a very natural representation of HRR, BSC and RP at the level of Geometric Clifford Algebra (GA). As described in[120], GAs provide a geometric interpretation of the cognitive structures represented by HHRs, BSC and RP, that is philosophically consistent with many other approaches where cognition is interpreted in geometric terms. Binding of vectors in the GA representation is performed by means of the Geometric Product and chunking is just ordinary addition. GA also supports additional operations which we will investigate and exploit. Of particular relevance to subtask 4.3 are the links from GA representations to neural and quantum computation.

Subtask 2.2: Distributed Analytics Using Cognitive Computing Models

In this subtask, we will investigate an alternative approach to distributed analytics that uses cognitive computing models based on the Geometric Clifford Algebra to perform the tasks. The challenge is to identify how an interacting network of cognitive microservices might be capable of performing analytics in more efficient ways than traditional microservices, specifically in relation to the reduction of the network traffic burden by providing the services with cognitive capabilities which monitor their environment to determine the most appropriate actions to perform. This immediately raises the question of what is a cognitive service and how do we represent cognitive capabilities in our models. To achieve this objective, the microservices will be cognitive in the sense that they comply with established principles of cognition such as those defined by the Core Cognitive Criteria (CCC)[113] which to a large extent incorporates the four key attributes of the DAIS research program, namely composability, interactivity, optimality and autonomy[79]. In this approach microservices are considered as semantic concepts and can be processed as such. It is in this sense our distributed CCS can truly be described as a 'distributed federated brain'.

We believe that the use of GA is a promising candidate to provide the mathematical representation of such

---

[118] M.N. Jones and D.J.K. Mewhort, Representing word meaning and order information in a composite holographic lexicon, Psychological Review 2007, Vol. 114, No. 1, 1–37.

[119] Kanerva,P., Binary spatter codes of ordered k-tuples, Artificial Neural Networks–ICANN Proceedings, Lecture Notes in Computer Science vol. 1112, pp. 869-873, C. von der Malsburg et al. (Eds.) (Springer, Berlin, 1996).

[120] Aerts, D et al. On Geometric Algebra representation of Binary Spatter Codes, CoRR, eprint arXiv:cs/0610075, October 2006.

services since the algebra itself offers great conceptual (i.e. cognitive) gains obtained by using these intuitive algorithmic methods. A recent review of the applications of Clifford's Geometric Algebras[121] for performing analytic processing concludes that applications of these algebras are becoming increasingly important for a wide range of applications. In many cases the applications built using these representations offer better accuracy, higher speed, and a wider exception free and singularity free scope.

In this subtask, we will demonstrate the benefit of developing cognitive computing to address distributed analytical problems solutions using the unified mathematical framework. Initially, we will start by expanding on the research we have been working on in IPP P5, where we began exploring the use of symbolic vector architectures to represent and orchestrating complex decentralized workflows. This approach: (1) provided an extremely compact workflow representation; (2) enabled the encoding of workflows containing multiple coordinated sub-workflows in a way that allows the workflow logic to be unbound on-the-fly and executed in a completely decentralized way; (3) enabled the workflow and associated complex metadata to be embedded into a single vector; (4) exposed a completely self-contained workflow that can be passed around using standard group transport protocols to support mobile ad hoc networks. We plan to interface such a methodology with real-world scenarios to empirically evaluate the approach when applied to existing complex distributed workflows, and new scenarios specific to DAIS; and (5) show how the same workflow and services can be expressed as cognitive services. This will provide practical experience, identify research issues in applying such a methodology and provide a proof of concept application, along with results in order feed lessons learned into the design of our generalised mathematical framework.

The task will also inform subtasks 1 and 3 about the types of distributed analytical problems that can be addressed using cognitive computing approaches. We will show, by way of example, how applications that are being proposed for validation of other research activities in the DAIS ITA can be represented in the geometric algebra and how cognitive services can be specified using the algebraic description. This subtask will specifically undertake to investigate how different types of distributed analytics tasks can be performed using cognitive computing models by demonstrating how they can be decomposed into cognitive micro services using the mathematical framework being developed in subtask 1.

Subtask 2.3: Cognitive Services using Non Von Neumann Computing

The demands of future tactical environments will require new types of technologies to overcome the requirements imposed by limited communication bandwidth and power. The trend in traditional Von Neumann computing is towards computing devices that scale at best linearly with computational complexity whereas non Von Neumann computing models scale logarithmically with computational complexity and use significantly less power than current devices. A number of current research programs, such as DARPA's Systems of Neuromorphic Adaptive Plastic Scalable Electronics (SyNAPSE) program and the European Commission Human Brain Project, have begun the development of a new generation of brain-inspired neurosynaptic computational architectures that are compact and consume little power. To support these developments, a new generation of neuromorphic computing models is being developed[122, 123, 124, 125], in which both data and associated processing are distributed naturally within the network of processing elements. Such models have been shown to be applicable to a range of signal processing and analytics task[113,126].

These developments naturally lead to the question of whether these brain-inspired computing models can be extended to the service composition problem in which both data and associated processing are distributed naturally

---

[121] Hitzer,E., Nitta,T., and Kuroe,Y., Applications of Clifford Geometric Algebras, Advances in Applied Clifford Algebras: Volume 23, Issue 2 (2013), Page 377-404.

[122] Merolla, P.A., et al., A million spiking-neuron integrated circuit with a scalable communication network and interface. Science. 345 (6197): 668. doi:10.1126/science.1254642. PMID 25104385.

[123] Tait, A. N., Nahmias, M. A., Tian, Y., Shastri, B. J., & Prucnal, P. R. (2014). Photonic neuromorphic signal processing and computing. In Nanophotonic Information Physics (pp. 183-222). Springer Berlin Heidelberg.

[124] Sengupta, A., & Roy, K. (2015, July). Spin-transfer torque magnetic neuron for low power neuromorphic computing. In Neural Networks (IJCNN), 2015 International Joint Conference on (pp. 1-7). IEEE.

[125] http://www.nengo.ca

[126] Bucholtz, S., A theory of neural computing with Clifford algebras, PhD Dissertation, der Technischen Fakult¨at der Christian-Albrechts-Universit¨at zu Kiel, 2005.

within a network based on a non Von Neumann processing paradigm. Such an approach will potentially suggest a radically new approach to network processing in which the data and analytics are represented in fundamentally different ways to today's processing architectures and one in which the realization of the distributed brain may become significantly more like a real brain. Geometric algebras have been shown to be applicable to the analysis and design of feed- forward neural networks[127] and that the use of an adequate Clifford geometric algebra can alleviate the training of neural networks.

Similarly, Clifford Algebra underpins many of the quantum computer codes that are currently being developed[128]. By thinking beyond ones and zeroes and using the Geometric Clifford Algebra to represent the computation, the quantum computing platform can already solve problems that were considered too complex for classical computer systems to handle. A stretch goal of this subtask will be to investigate how the symbolic vector representation lends itself to the quantum computing paradigm and how this can be mapped onto the new generation of quantum computers. Interestingly, since quantum Clifford algebras have been demonstrated to solve pattern recognition in multispectral environment in a natural and effective manner, this has led to the speculation that the brain itself may function in a similar way to a Clifford Quantum Computer[129].

This subtask will therefore seek to demonstrate how cognitive services being developed in subtask 2 by using the geometric algebra representations developed in subtask 1, can be mapped to operate as a highly parallel non Von Neumann machines such as the next generation neuromorphic and quantum computers. This task will be composed of three steps:

1) Taking specific systems or simulations of specific systems and implementing a symbolic vector representation (SVR) on them.
2) Evaluating performance metrics, such as information loss and quality of service, on the system. The second step is import since it will enable us to determine how current neuromorphic architecture constraints affect SVR performance; and based on that, identify architectures that are optimized for SVR operations.
3) Evaluate how such new computing models can be applied across a coalition network and the types of inter-process communication that are required to support such a model.

Validation and Experimentation

Our ultimate goal is to determine the best resources to meet requests and to allocate the identified resources to outstanding requests in varying coalition contexts subject to the utility provided by the resources. To achieve the goal, in this BPP we aim to theoretically and empirically verify that: (1) the needed resources are identified for requests by semantic interpretation; (2) optimal performance bounds w.r.t. utility can be given for each of our problem; (3) sufficient simulations are performed for necessary heuristics; and (4) designed algorithms are thoroughly evaluated w.r.t. the multi-modal analytics exemplar and studies are conducted to determine their accuracy and operational characteristics. To validate the service allocation and re-provisioning, we plan to perform theoretical analysis, and simulation of non-Von Neumann cognitive services using a variety of simulation tools and available hardware platforms. These include Nengo[125], Compass[130] and Brian[131] simulators for neuromorphic computing and IBM Q[132] for quantum computing representations. We will also seek to demonstrate mapping to state

[127] Bayro-Corrochano, E,J. Geometric Neural Computing IEEE TRANSACTIONS ON NEURAL NETWORKS, VOL. 12, NO. 5, SEPTEMBER 2001.

[128] Matzke, D,J. Quantum Computation Using Geometric Algebra, Phd Dissertation, The University of Texas Dallas, May 2002.

[129] Valeri G. Labunets, Ekaterina V. Labunets-Rundblad, Jaakko T. Astola, "Is the brain a Clifford algebra quantum computer?", Proc. SPIE 4453, Materials and Devices for Photonic Circuits II, (6 November 2001); doi: 10.1117/12.447643.

[130] Preissl, R., et al Compass: A scalable simulator for an architecture for Cognitive Computing, SC '12: Proceedings of the International Conference on High Performance Computing, Networking, Storage and Analysis, Nov 2012.

[131] http://briansimulator.org

[132] https://www.research.ibm.com/ibm-q/

of the art architectures such as TrueNorth[133], SPIN[124] the Princeton Photonic Architecture[123].

Additionally, we will work with subject matter experts (SMEs) from both government and industry to carry out experimental studies so as to evaluate the efficacy of the research proposed here throughout the BPP; we will publish on algorithmic aspects of the discoveries as well as on the results obtained by applying those to the coalition domain in reputed conferences. Furthermore, we will work with SMEs, especially with military domain experts, to enhance and extend the real-time video analytics exemplar we have developed within the IPP and with the NS-CTA program to capture mission-critical scenarios for multi-modal real-time analytics service.

We propose to link Project 4 Tasks 1 & 2 by using the multi-modal analytics processing flow developed in the IPP to demonstrate how a distributed analytics tasks can be implemented using combinations of microservice as a baseline and then show how the same service composition can be implemented using a cognitive computing principles that use reasoning[115], semantic composition[116], analogical mapping[117] and the representation meaning and order[118] to perform the analytics. We will leverage and extend the work done as part of the NS-CTA which has trained deep learning models and assembled data set for object and action detection. Much of the software for the NS-CTA program on video analytics has been ported into the Network Science Research Laboratory (NSRL) at ARL; we will leverage these capabilities and the DAIS experimentation facility to evaluate our algorithms in larger scale on realistic systems and scenarios.

We will extend the video-analytics work into multi-mode information by considering text and audio along with video. The text may be in the form of annotations or independent text descriptions. We expect our models to be general and adaptable to multi-modal information, allowing for us, as a stretch goal, to determine how much information of different modes help respond to queries.

We propose to use CORE/EMANE to develop a representative future coalition network to demonstrate how such new computing models might be applied across a coalition network and the types of inter-process communication that would be required to support such a model.

Military and DAIS ITA Relevance

This project addresses the specific topics Optimizing the Matching of Coalition Resources to Tasks and Contextualization of Disparate Coalition Data Sources and Services in the call for BPP white papers to help reach the overall DAIS goal. The project specifically looks at data and processing resources and how best to match those resources to outstanding requests in distributed coalition environments.

In support of achieving this goal, in Project 4 Task 1, we consider situations in which resource matching is tempered with the utility of resources in-context; this will help us to systematically critique resource matches, especially when more than one resource can satisfy a request, insufficient resource is available or only partial matches are available for requests in mission-critical situations.

Once identified, these resource plans need to be executed efficiently on distributed coalition networks. In data-intensive domains—such as coalition networks—a key requirement is to trade-off between fresh data and model learning in support of efficient and effective decision making. The insights gleaned from approximate interior-point methods may provide clues to solve this problem by applying the efficiencies of online mechanisms to off-line congestion free optimizations, thus resulting in low-delays for service instantiation in coalition context.

Last but not least, in coalition setting, intentional or unintentional misreporting could occur; developing strategies to handle such situations will be critical for the success of future coalition operations. Here, we will explicitly consider situations in which some resources may be shared, and partners may not fully or honestly disclose the utility of their missions or resources. We will investigate the applicability of new learning paradigms by which we can enable the matchmaking algorithms to be more instinctive as humans do typically in day-to-day endeavours. This will further enable algorithmic discrimination is critical situations—e.g., our algorithms may

[133] Akopyan, F., Sawada, J., Cassidy, A., Alvarez-Icaza, R., Arthur, J., Merolla, P., Imam, N., Nakamura, Y., Datta, P., Nam, G.J. and Taba, B., 2015. Truenorth: Design and tool flow of a 65 mw 1 million neuron programmable neurosynaptic chip. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 34(10), pp.1537-1557.

prioritise one partner's request over another partner's request based the context (i.e., geolocation, mission importance, past performance, and so forth).

Project 4 Task 2 seeks to investigate the basic science that will be required to develop the next generation of cognitive services that are 'self-aware' in the sense that they: understand user requests for analysis; seamlessly compose the desired analytics functions from other functions and services available in the network; identify the right data set needed for the analytics; and bring together as a workflow the data and analytics required to perform the function. Future military networks will always seek to achieve maximum benefit from new and potentially disruptive technologies. The emergence of non-Von Neumann processing capabilities such as neuromorphic processors and quantum computers are likely to transform the future of the type of distributed analytics that the DAIS project seeks to address. In a coalition context the issues surrounding how these technologies might be shared and the impact on communications, policy and security all need to be addressed. Task 4.2 seeks to lay a foundation from which such important questions can be addressed.

Collaborations, Staff Rotations, and Linkages

Project 4 has a total of 7 students allocated across the two tasks. We will seek to ensure that our students work closely together across the two tasks and with students on other BPP projects as part of the student cohort. Students will be encouraged to spend time at the different partner institutions during project and we will investigate opportunities for students to spend time at the ARL Open Campus facility in Adelphi and IBM Research facilities in both UK and USA.

The team will work together to define and expand on the task once the research is started. While the teams will always work together, and leverage each other's work.

- La Porta and de Mel to co-lead subtask 1.1 on in-context utility functions for request/resource matching and algorithms for matchmaking in varying contexts; Sensoy will collaborate with de Mel and La Porta on this subtask. Parthasarathy will contribute to the learning aspect of the subtask. Stein will lead the subtask 1.2 on game-theoretic techniques for resource allocation, especially when non-benevolent agents are involved. Within subtask 1.2, Bi will focus on mechanism design, Cater on policy design and Chakraborty on decentralised mechanisms. Restocchi will contribute expertise on game theory to the subtask. La Porta, Tassiulas and Chan will collaborate with Stein on subtask 1.2 w.r.t. resource allocation, and de Mel and Sensoy will collaborate with Stein w.r.t. learning mechanisms. University of Southampton and IBM UK will have reciprocal research visits once per month and IBM UK will co-advise one of Stein's students as makes sense from the technical work. Tassiulas will lead the subtask 1.3 on mathematical foundations for delay tolerance real-time analytics. He will collaborate with La Porta and Kwon on the evaluation using video analytics. La Porta will link the video analytics work to the NS-CTA video analytics task and de Mel will work with graduate students to apply the research into military and industry problems. Gerding will co-supervise Bi, Brede will co-supervise Chakraborty and Norman will co-supervise Parthasarathy and Cater.

- Task 4.2 will be led by Bent. Hunt will lead subtask 2.1 on the development of the mathematical framework based on the Geometric Clifford Algebras. Hunt will collaborate with Ganti, Bent on this task. Subtask 2.2 will be led by Ganti on an alternative approach to distributed analytics that uses cognitive computing models. Ganti will collaborate with Taylor, Bent. Subtask 2.3 on cognitive services using non Von Neumann computing will be led by Taylor and Roy who will collaborate with Bent. Graduate students supervised by Corcoran, Taylor and Roy will work across the subtasks.

Additionally, our collaborators further augment the work across all tasks by adding valuable skills:

- ARL (Kwon, Chan, Monaco & Henz) and Dstl (Pearson, Worthington) have expertise on deep learning, computer vision, resource allocation in scarce environments, contextual modelling of utility, and neuromporphic computing and will thus having a crosscutting impact on all subtasks. IBM US (Rallapalli) and IBM UK (Tomsett, Waggett) offer expertise in service semantics, machine learning, distributed

computing, and Neuromorphic Computing which are complementary to the analytic matchmaking and mechanism design in this proposal.

- Cardiff (Sensoy, Corchoran & Preece) and Southampton (Gerding, Brede, Norman) offer expertise on semantic technologies, geometric algebra, multi-agent systems and game theory, which are important in modelling the dynamic environments in which this research occur.
- Purdue (Bertino) offers expertise on policy modelling in dynamic distributed environments which is important for service composition in this research.

Task P4.1 has tight linkages with (1) P2.2, "Generative Policies Analytics – Theory, Methods, and Tools" on the use of generative policies as means to govern service compositions in coalition environments; P2.2 will utilize the semantic inferences done about services to generate in-context policies; (2) P3.2, "Distributed Analytics in Dynamic Coalition Environment: Placement, Scheduling, and Validation." We already have one joint paper submitted and are working on an extension. There will be collaboration on the learning aspects in both projects, and shared knowledge on optimization frameworks and utility definitions; and (3) P6.1, "Fracture and Formation: Evolutionary and Psychological Modeling of Inter-Group Behavior", where Stein will collaborate with de Mel and Whitaker on game theoretic approaches for autonomous policy negotiations when faced with adversarial behaviors in group situations.

Task P4.2 has linkages with other BPP projects: (1) the semantic vector representation we are developing is relevant to P3.2 "Distributed Analytics in Dynamic Coalition Environment: Placement, Scheduling, and Validation" leveraged to describe the composability of analytics and to match user needs with analytics code/data; (2) the use of GA for the analysis and design of neural networks and the requirement for our cognitive agents to learn their representations has strong resonance with P5.1 "Learning and Reasoning in Complex Coalition Information Environments" and P5.2 "Interpretable Deep Neural Networks for Coalition Situational Understanding" and we propose to work closely with both projects on the potential use of SVA to provide a means for self-describing data; and (3) The need for the cognitive services to comply with policy and how that might be achieved will require co-operation with P3.2 "Generative Policies Analytics – Theory, Methods, and Tools" where we will consider how generative policies might be represented in cognitive services.

Research Milestones		
Due	**Task**	**Description**
Q1	**Task 1**	Comprehensive literature review on mechanism design for resource allocation with strategic agents → Technical report on existing techniques for dealing with strategic agents, focusing in particular on the limitations of that work in coalition settings (Southampton, Yale) Critical analysis of matching of data and processing for requests. Technical review on the state-of-the-art (IBM UK, PSU)
Q1	**Task 2**	Requirements for distributed analytics using a cognitive computing paradigm; Define success criteria. Technical review on the state-of-the-art (Purdue, IBM UK, IBM US)
Q2	**Task 1**	A review of optimization algorithms for data analytics in processing networks, with a particular focus on real-time video analytics → Technical report on existing techniques, challenges, and open problems (Yale, PSU) Define criteria for matching services and processing, and queries to service/processing pairs → Technical report on initial criteria for matching services and requests and a set of slides highlighting the findings (IBM UK, PSU)
Q2	**Task 2**	Review of geometric algebraic structures that can be used to perform

Research Milestones		
Due	**Task**	**Description**
		distributed cognitive computation; Review of cognitive computing solutions using neuromorphic computing architectures; Review of cognitive computing solutions using other non Von Neumann architectures. Technical report on existing techniques, challenges, and open problems. A paper on SVA representation of complex workflows. (IBM US,Purdue, IBM UK, Cardiff)
Q3	**Task 1**	Strategyproof mechanism for resource allocation with strategic agents in a dynamic coalition setting → Software implementation of resource allocation mechanism and paper describing the mechanism (Southampton, PSU) Algorithms for matching services and processing and queries to service/processing pairs → A paper on matching services to requests based on the identified criteria (PSU, IBM UK)
Q3	**Task 2**	Results of initial investigations into how symbolic vector representation (SVR) might be mapped onto different non Von Neumann architectures. A paper on mapping of SVR representations to non Von Neumann architectures (Cardiff, IBM UK, Purdue)
Q4	**Task 1**	Sophisticated utility functions dependent on processing and data pairs, and queries. A technical report on in-context utility function modelling and a set of slides (Yale, PSU)
Q4	**Task 2**	Initial Mathematical Framework; Initial results from distributed analytics using cognitive services; (Cardiff, IBM UK) Results from initial experimental validation using neuromorphic processing. A technical report on the Mathematical Framework and initial results (Purdue, IBM UK)
Q5	**Task 1**	Initial resource allocation algorithm assuming perfect statistical knowledge of the analytics requirements → A paper describing the resource allocation algorithm and the challenges to relax the perfect knowledge of the applications requirements (Yale, PSU)
Q5	**Task 2**	Mathematical formulation of cognitive services for distributed analytics; Initial results of mapping cognitive services to other non Von Neumann architectures. Define evaluation scenario and evaluation metrics for experimental validation. A paper describing cognitive service formulation and a technical report on the evaluation scenario (IBM US, Purdue, Cardiff, IBM UK)
Q6	**Task 1**	Extension of strategyproof mechanism to deal adaptively with changing system parameters using machine learning techniques → Software implementation and paper on adaptive mechanism (Southampton, PSU, Yale) Matching algorithms with utility functions from Q4 → A paper on matchmaking w.r.t. in-context utility of resources (PSU, IBM UK)
Q6	**Task 2**	Evaluation of the cognitive service computing paradigm in coalition networks; Comparison with alternative microservice composition approaches. A paper on decentralized cognitive service computing (IBM UK, IBM US, Cardiff)
Q7	**Task 1**	Extension of the algorithm to relax the perfect knowledge of the statistics of

Research Milestones		
Due	**Task**	**Description**
		the real-time analytics → A paper with the mathematical description of the extended algorithm, and validation using simulation (Yale, PSU)
Q7	**Task 2**	Final Mathematical Framework; Evaluation of the performance of cognitive processing for distributed analytics using metrics, such as information loss and quality of service. A paper on the mathematical framework and its application. (Cardiff, Purdue, IBM UK,IBM US)
Q8	**Task 1**	Extension of mechanism to allow balancing of various stakeholders' interests according to global mission priorities. Software implementation of extended mechanism and demonstrator of interface (Southampton, IBM UK) Algorithms for matching that incorporate utility function from Q4 and video analytics. A paper on dynamic formation of analytic services (Yale, PSU) A demo of the integrated research (ALL) Release of research-grade open-source software and tools (ALL)
Q8	**Task 2**	Final results from experimental validation using neuromorphic and quantum processing. A paper on experimental validation (Purdue, IBM UK,Cardiff) Release of research-grade open-source software and tools (ALL)

Project 5: Anticipatory Situational Understanding for Coalitions

Project Champion: Alun Preece, Cardiff

Email: PreeceAD@cardiff.ac.uk **Phone: +44 29 2087 4653**

Primary Research Staff	Collaborators
Chris Willis, BAE Systems	Pablo Bermell-Garcia, Airbus
Alun Preece, Cardiff	Vedran Galetic, Airbus
Federico Cerutti, Cardiff	Mark Hall, Airbus
Unnamed PGR, Cardiff	Alistair Nottle, Airbus
Unnamed PGR, Cardiff	Santiago Quintana-Amate, Airbus
Unnamed PGR, Cardiff	Jonathan Bakdash, ARL
Dave Braines, IBM UK	Raghuveer Rao, ARL
Ramya Raghavendra, IBM US	Erin Zaroukian (PDR), ARL
Supriyo Chakraborty, IBM US	Daniel Harborne (PGR), Cardiff
Simon Julier, UCL	Yulia Hicks, Cardiff
Amy Widdicombe (PGR), UCL	David Marshall, Cardiff
Moustafa Alzantot (PGR), UCLA	Ross Lund, Dstl
Mani Srivastava, UCLA	Gavin Pearson, Dstl
Tianwei Xing (PGR), UCLA	Richard Tomsett, IBM UK
Lance Kaplan, ARL	Rachel Bellamy, IBM US
Prudhvi Gurram (PDR), ARL	Murat Sensoy, Cardiff and Ozyegin

Project Summary/Research Issues Addressed

Anticipatory situational understanding (ASU) is fundamental to support decision-making and autonomy by all agents within the coalition. Situational understanding is the "unit's situation awareness to determine the relationships of the factors present and form logical conclusions concerning threats to the force or mission

accomplishment, opportunities for mission accomplishment, and gaps in information"[134]. This is asserted as corresponding to Level 2 situational awareness (SA) in Endsley's widely-used model, as shown in figure P5.1. Endsley's SA model provides us with an operational definition of understanding as: the spatio-temporal perception of environmental events (level 1), followed by their comprehension within a specific context (level 2), and finally, the ability to project or predict potential future events (level 3) due to change in variables such as time, or other events.[135]

Each agent in the coalition must be able to form an awareness of its environment, perform inferences on that awareness to identify concepts and relationships, predict how the environment will evolve, and assess how its actions can shape this future evolution. Project 5 will explore the algorithms and techniques that will be used to develop ASU. It will investigate how this can be carried out in a distributed coalition with heterogeneous agents, each of which has its own role, has access to its own sources of information (which can be hard or soft), has its own computational resources, needs to make its own decisions and can undertake different actions. The key scientific challenges lie in how the different levels of representation and reasoning interact with one another to allow the flow of information, uncertainty and reasoning between the different levels. To meet these challenges, Project 5 will develop new representations of the environment, integrating knowledge-based reasoning with machine learning, investigate new methods for human-machine collaboration, and identify new inference algorithms for multi-level distributed fusion and estimation.

Our key innovations are centered around new approaches to support transfer of information between different levels of abstraction in a fluid manner. Traditional approaches to ASU have adopted a model that representations live in a strict hierarchy in which low-level inference must be completed before high-level inference can be carried out. We believe that information processing agents should be able to translate, support, and move between different levels of abstraction from the state of individual targets to entire high-level summaries of an operation. Key to achieving this goal are dynamic models for individual agents and the coalition as a whole that will learn and encode (1) hierarchical information representations spanning the different levels of abstraction, including knowledge of past and current states in the world together with probabilistic dependencies among variables that capture the likelihood of future states, and (2) sharing mechanisms which make it possible for agents to share both their memories and the meta- information which describes the representation used to encode those entities. We will use these models to develop algorithms and procedures that can (a) estimate the current state of the world by fusing uncertain structured and unstructured data from sources ranging from machine sensors of varying modalities (e.g., acoustic, camera, pressure, location) to human agents and other social sensors (e.g., Twitter, Facebook, Instagram); (b) predict future states of the world by projecting sequences of actions and their consequences in time; and (c) reason about the feasibility and implications of the chosen actions in terms of driving the world to the desired state, maximizing the operational efficiency of coalition decision-making.

[134] http://www.globalsecurity.org/military/library/report/call/call_01-18_ch6.htm

[135] See also: *Understanding: Joint Doctrine Publication 04 (JDP 04)*, Ministry of Defence, 2010.

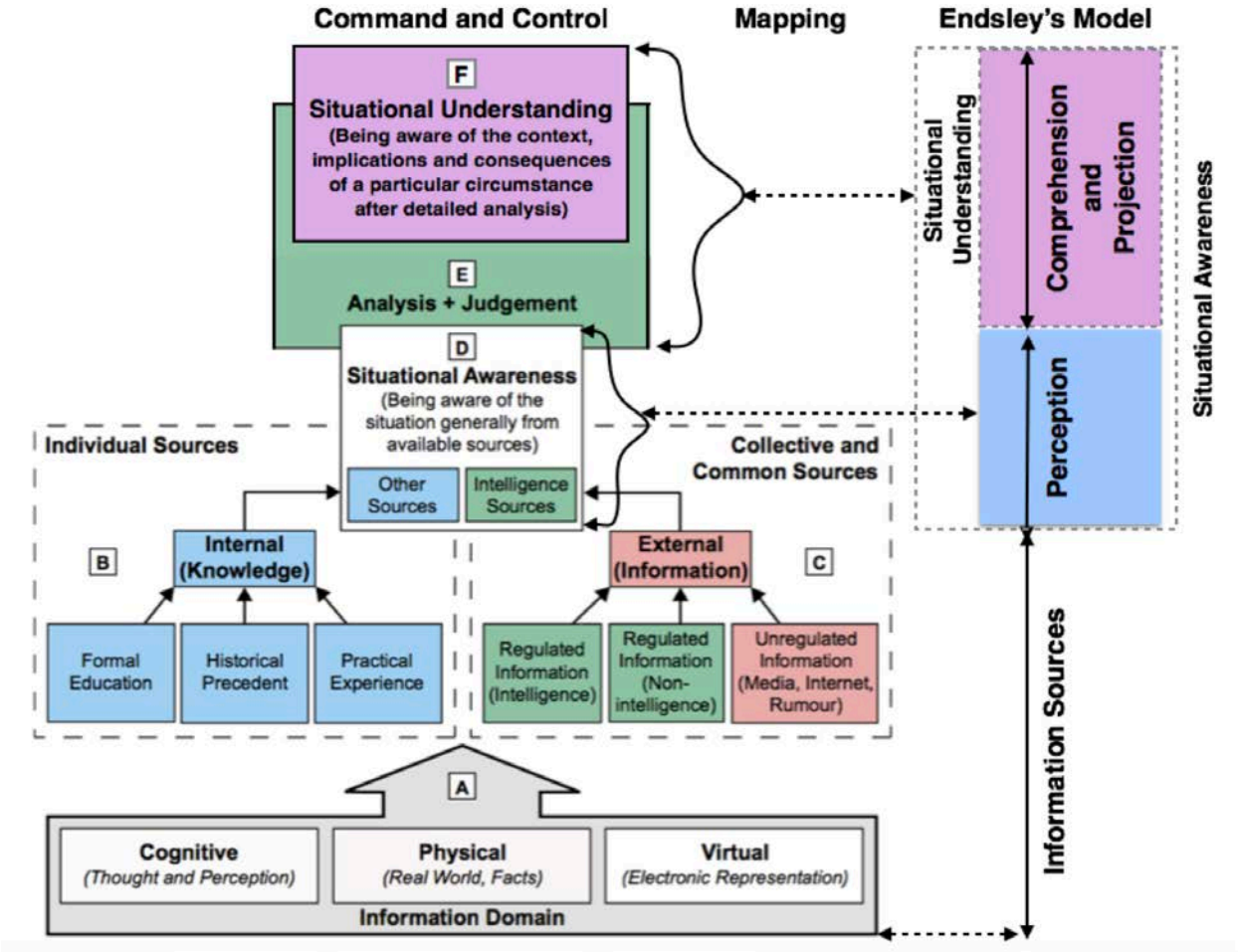

Figure P5.1. Mapping between different notions of situational understanding.

Technical Approach

Project 5 will develop the scientific underpinnings of an end-to-end robust and adaptive information fusion pipeline for the processing of collected hard and soft data including traditional signal processing as well as analysis of soft sources such as text and open source intelligence through to ASU. Our work will focus on the creation of theory-based dynamic models and mechanisms to integrate multiple fusion capabilities in a distributed decision-support context, spanning multiple levels of abstraction from the state of individual entities to high-level situation overviews. The research aims to produce approaches that can operate in heterogeneous environments typical in coalition operations, comprising both machine and human agents with different responsibilities and capabilities.

For operational efficiency within the dynamic coalition environment, a key focus of our approach is the ability for the pipeline to rapidly reconfigure itself to support situational understanding. This requires an awareness of the current situation together with the ability to predict what it could become, and it is closely linked to work in Project 4 in which prediction capabilities are required to inform proactive configuration of network services and other resources. We seek to attain this goal while maintaining transparency to human users by incorporating knowledge of the state of information components within the system, including key metadata that enables the system to respond and predict how the operational context will evolve.

We propose a layered conceptual architecture for ASU in the coalition context, illustrated in figure P5.2. The figure depicts a virtual view of the coalition: all four layers are distributed across the coalition. The lowest layer consists of a collection of data sources (physical sensors and human-generated content), accessible across the coalition, providing hard and soft data. The three upper layers roughly correspond to Levels~0--3 of the JDL Model.

For each layer, the figure shows the primary technical techniques employed, though others may be exploited also. The information representation layer uses incoming data streams to learn concepts and model entities together with their relationships at multiple levels of semantic granularity. The history of past observations is encoded in these representations, explicitly or implicitly. Technical techniques used in this layer are drawn predominantly from machine learning (ML), natural language processing (NLP), and vision/speech/signal processing (VSSP). Multi-agent systems (MAS) techniques will also play a role in communication of sensor-produced data and coordination among distributed processing services.

The information fusion layer employs algorithms and techniques developed to perform fusion over concepts and entities derived from the information representation layer. This layer estimates the current state of the world, providing the *perception* (situational awareness) as depicted in figure P5.1. While ML, NLP, and VSSP approaches play a role at this level also, knowledge representation and reasoning (KRR) and MAS have a significant role here.

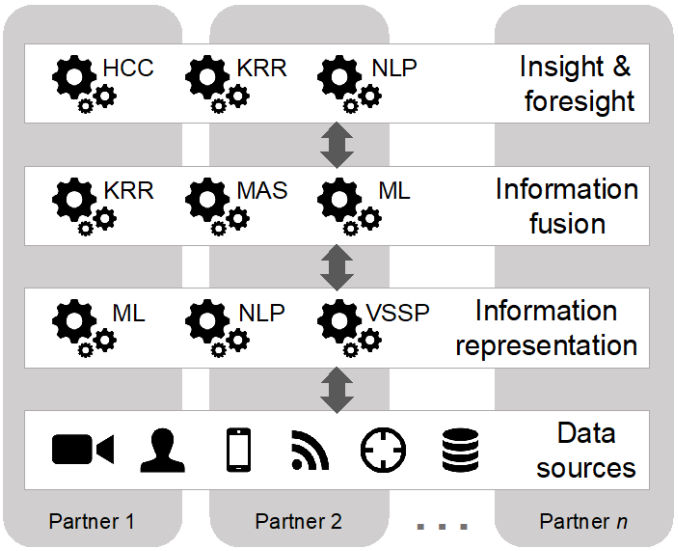

Figure P5-2. Situational Understanding layered model, distributed virtually across a coalition

The prediction and reasoning layer then uses the estimated current state, together with the state space of the models to predict the future state. KRR plays a key role in reasoning about the future state (providing the *foresight* necessary for situational understanding) while human-computer collaboration (HCC), NLP, and interpretable ML approaches address the interaction between this layer and human users.

The upper layers in figure P5.2 need to be open to humans to provide expert knowledge for reasoning; these layers also need to be open to the human user in terms of being able to generate explanations of the insight and foresight generated by the system. There is a bi-directional exchange of information occurring between the different layers: in the upward (feedforward) direction, the inferences at the lower layer act as input for the next higher layer; in the downward (feedback) direction, information is used to adjust the model and algorithm parameters and possibly task the sensors differently. Creating better systems to support ASU necessitates the development of mature models and algorithms that can over a period of time reduce the human intervention and attain greater autonomy, but without entirely replacing human involvement and oversight.

The proposed work in BPP18 focuses on a number of key challenges in the area of reasoning and machine learning illustration of a multi-layer view of a coalition network is shown in figure P5.3. Layer 1 depicts the different coalition agents (blue, green and yellow regions). Each agent collects multi-modal data locally, and cooperates with other agents, within constraints of their own organizational data-sharing policies. Layer 2 shows information pooling from human and machine agents required to achieve situational understanding. Based on the above description, coalition situational understanding can be broken down into the following reasoning and machine learning challenges.

Distributed learning and reasoning: The very existence of a coalition is contingent on the premise that the whole is greater than the sum of the parts, i.e., the shared model of the environment, learned using the information

combined and inferred from all the agents is greater than just the individual pieces of information. However, to train a shared model and realize the above goal, the learning algorithm used should, (1) be able to adjust to the variability in network topology connecting the various agents; (2) be sensitive to the reliability of the training data available from the agents; (3) account for the different granularities at which information is made available (e.g., raw data or model parameters) by the agents; and finally, (4) meet the privacy requirements of the agents.

Multiple time-scale learning and reasoning: Coalitions are often formed to monitor a particular geographic region for event(s) of interest. However, the periodicity of the monitored events could be different. The shared model should have the power to use the collective information from the agents to learn events that manifest themselves at different time scales. For example, on a particular road segment, the volume of traffic (or the congestion level) on a weekday, may be solely dependent on the time-of-day. However, the congestion level over a weekend, might depend on the schedule of a nearby sporting event. Thus, congestion is predicted as a result of two different events occurring at different time scales.

Model interpretability and tellability: These attributes refer to the bi-directional flow of information between models and humans. While deep learning based models are motivated by neuro-scientific advancements in the understanding of the working of the human brain, a critical distinction, that has often been made between the two, is attributed to the human ability to “think”. Informally, it is this ability to think, that allows humans to not only make a prediction, but also justify or rationalize it through a series of logically consistent and understandable choices leading up to the prediction. This justification, in turn, enables the decision maker to implicitly or explicitly associate a measure of confidence to the prediction and use that to determine the next steps of necessary actions. The counterpart to human thought process in deep learning models is often referred to as interpretability. The ability to interpret a prediction enables semantically meaningful information to flow from the models to humans. We refer to the information flow from humans to models as *tellability*. The notion of tellability is different from enriching the training data set with samples corresponding to the new hypothesis classes that we want the model to learn. Instead, it implies adding prior information to the model that is not part of the training data. Tellable information is typically based on human experience and not limited to the training data alone.

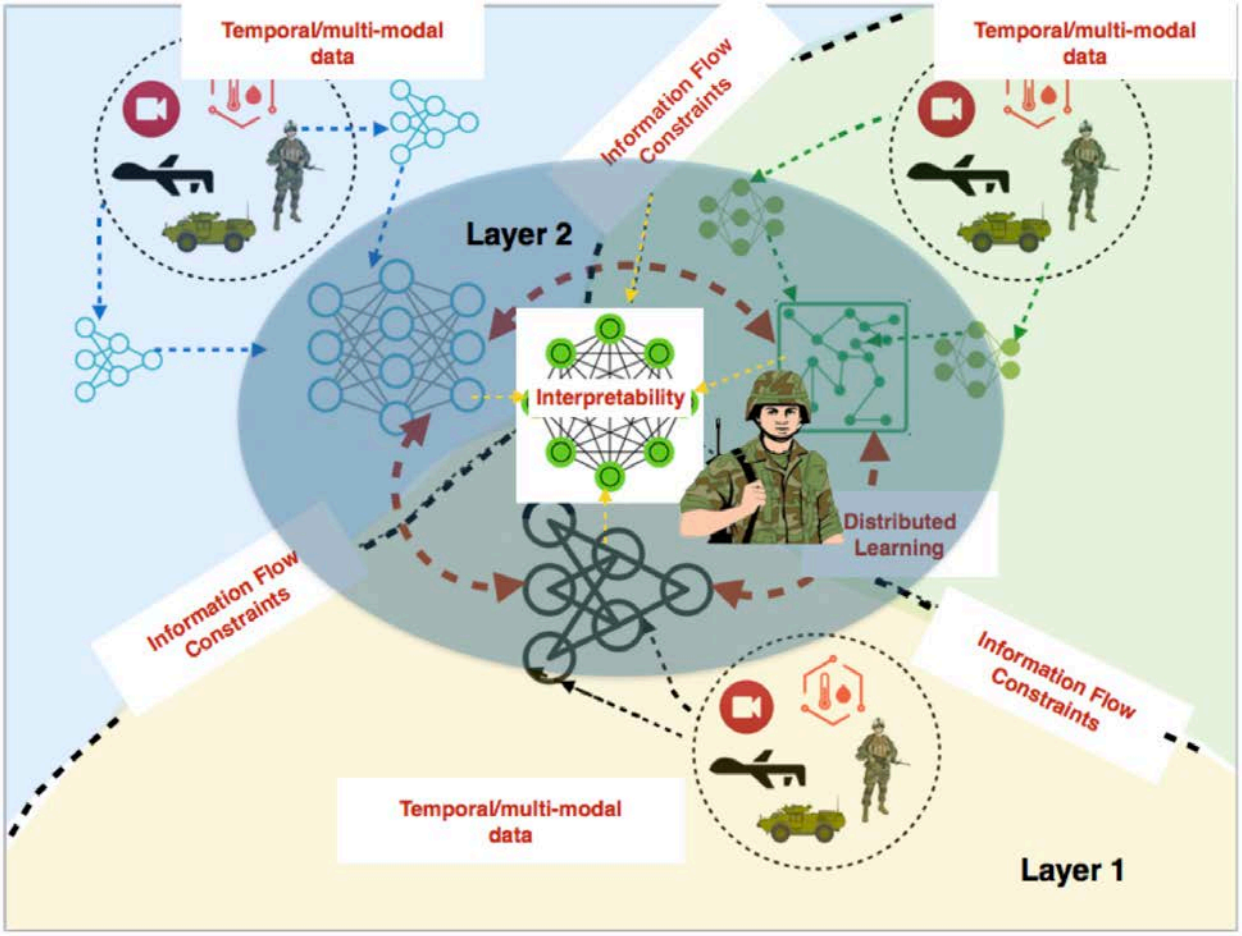

Figure P5-3. A multi-layer view of an ad-hoc military coalition. Information exchange occurs between the different agents under various domain-specific constraints to achieve distributed learning of an interpretable model.

In order to advance the current state of the art, in BPP18 we propose to undertake two research tasks:

- **Learning and Reasoning in Complex Coalition Information Environments**: Task 5.1 will focus on integrating learning and reasoning techniques for coalition situational understanding, focusing on dealing with uncertainly in the presence of sparse data.
- **Interpretable Deep Neural Networks for Coalition Situational Understanding**: Task 5.2 will focus on interpretability and tellability with a particular emphasis on temporal prediction and learning in the presence of coalition information flow constraints.

Task 1: Learning and Reasoning in Complex Coalition Information Environments

Primary Research Staff	Collaborators
Dave Braines, IBM UK	Jonathan Bakdash, ARL
Federico Cerutti, Cardiff	Rachel Bellamy, IBM US

Alun Preece, Cardiff	Daniel Harborne, Cardiff
Ramya Raghavendra, IBM US	Ross Lund, Dstl
Mani Srivastava, UCLA	Alistair Nottle, Airbus
Tianwei Xing (PGR), UCLA	Gavin Pearson, Dstl
Unnamed PGR, Cardiff	Santiago Quintana-Amate, Airbus
Unnamed PGR, Cardiff	Murat Sensoy, Cardiff and Ozyegin
Lance Kaplan, ARL	Chris Willis, BAE Systems
	Erin Zaroukian (PDR), ARL

This task is a continuation of TA2 Coalition Distributed Analytics & Situational Understanding, IPP Project 6, Task 1, aimed primarily at the topics *Distributed and Integrated Fusion for Situation Understanding* and *Enabling Analytics of Distributed Coalition Data*.

Research Issue/Technical Approach

We will integrate learning and reasoning for coalition situational understanding (CSU) in complex, contested environments to inform decision makers at the edge of the network. CSU requires[136] both *collective insight*—i.e., accurate and deep understanding of a situation derived from uncertain and often sparse data—and *collective foresight*—i.e. the ability to predict what will happen in the future.

CSU depends on human/machine collaboration: machine agents offer powerful affordances in terms of data analytics, but they need to provide levels of assurance (explanation, accountability, transparency) for their outputs, particularly where those outputs are consumed by decision makers without technical training in information science. Current machine learning (ML) approaches are limited in their ability to generate interpretable models (i.e., representations) of the world necessary for situational understanding[137]. Moreover, these approaches require large volumes of training data and lack the ability to learn from small numbers of examples as people and knowledge representation-based systems do[138]. An ability for domain experts to *tell* a machine relevant information increases the tempo and granularity of human-machine interactions and the overall responsiveness of the system in meeting mission requirements. We seek to *equip coalition machine agents with integrated learning and knowledge representation mechanisms that support CSU while affording assurance (explainability) and an ability to be told key information to mitigate issues with sparse data (tellability).*

[136] Preece, A., Cerutti, F., Braines, D., Chakraborty, S., & Srivastava, M. (2017). Cognitive Computing for Coalition Situational Understanding. DAIS 2017 — *Workshop on Distributed Analytics InfraStructure and Algorithms for Multi-Organization Federations at IEEE SmartWorldCongress* 2017.

[137] Lake, B., Ullman, T., Tenenbaum, J., & Gershman, S. (2016). Building Machines That Learn and Think Like People. *Behavioral and Brain Sciences*, 1-101.

[138] Guha, R. (2015). Towards a model theory for distributed representations. *2015 AAAI Spring Symposium Series*.

Background

During the IPP in Project 6, Task 1 we defined key attributes for CSU[136] and observed that an integration of computational techniques is necessary: no single technique will suffice. Table P5.1 summarises the CSU attributes and identifies the primary computational approaches to addressing each one.

CSU attribute		Primary approaches
Level of understanding	High	**KRR**
	Low	**ML, NLP, VSSP**
	High-to-Low	**KRR, ML, NLP, VSSP**
Temporal	Long	**KRR, ML, VSSP**
	Short	**KRR, ML, VSSP**
	Long-to-Short	**KRR, ML, VSSP**
Multimodal Data	Hard	**ML, VSSP**
	Soft	**ML, NLP**
	Hard & Soft	**ML, NLP, VSSP**
Distributed	Coalition	**MAS, ML**
	Heterogeneous	**KRR, MAS**
	Coalition & Heterogeneous	**KRR, MAS, ML**
Human-in-the-Loop	Interpretable	**HCC, KRR, ML**
	Tellable	**HCC, KRR, NLP**
	Interpretable & Tellable	**HCC, KRR, ML, NLP**

Table P5.1 - Summary of CSU problem attributes. HCC: Human-Computer Collaboration; KRR: Knowledge Representation and Reasoning; MAS: Multi-Agent Systems; ML: Machine Learning; NLP: Natural Language Processing; VSSP: Visual, Speech, and Signal Processing.

Figure P5.2 illustrates the distributed system architecture we envisaged in[136] for a heterogeneous coalition environment with a mixture of hard and soft data sources, providing a basis for the case study discussed in[139]. Data are collected by individual partners and transformed into information before being shared and fused to support collective insight and foresight[136]. However, there are specifically two questions that are left unanswered by previous research. First, how recent advancements in ML and VSSP for collective insight and foresight can be exploited while providing assured outputs for decision makers who are not information scientists? Second, which integrated reasoning and learning techniques can provide greatest benefits for collective situational understanding, especially in the presence of sparse data?

Assuring the outputs from ML and VSSP algorithms to generalist users is an active area of research (e.g. [140, 141]) and has clear implications for the perceived importance of information—i.e., a measure of its usefulness—being created at each layer in figure P5.2. A decision maker needs to be informed of possible risks involved in each layer, including the presence of inaccurate and biased information, to evaluate the overall result coming from support systems for CSU. A possible way to address this is to relate to the notion of fairness[142]. Consider the problem of ranking a set of individuals based on demographic, behavioural or other characteristics wherein rankers can, and often do, discriminate against individuals and disadvantaged members of protected groups despite seemingly automatic and objective metrics[143]. In[144] the authors formulate a fairness measure by taking

[139] Nottle, A., Harborne, D., Braines, D., Alzantot, M., Quintana-Amate, S., Tomsett, R., . . . Preece, A. (2017). Distributed opportunistic sensing and fusion for traffic congestion detection. *DAIS 2017 — Workshop on Distributed Analytics InfraStructure and Algorithms for Multi-Organization Federations at IEEE SmartWorldCongress* 2017.

[140] Diakopoulos, N. (2016). Accountability in algorithmic decision making. *Communications of the ACM*, 56-62.

[141] Pedreschi, D., Ruggieri, S., & Turini, F. (2008). Discrimination-Aware Data Mining. *4th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*.

[142] Yang, K., & Stoyanovich, J. (2017). Measuring fairness in ranked outputs. *International Conference on Scientific and Statistical Database Management* (pp. 22:1—22:6). Chicago: ACM.

[143] Zliobaite, I. (2015). A survey on measuring indirect discrimination in machine learning. CoRR, abs/1511.00148.

[144] Kekäläinen, K., & J., J. (2002, October). Cumulated Gain-based Evaluation of IR Techniques. *ACM Trans. Inf. Syst.*, 20(4), 422—446.

several well-known statistical parity measures proposed in literature and making them rank-aware by placing them within well-known IR evaluation techniques. However, existing research did not address the issue of fairness and biases in a coalition context. Moreover, the military operates in safety critical environments: decisions may have life and death consequences. Thus, human understanding of fairness, or lack thereof, and bias in algorithms is imperative. *One scientific focus in this BPP will thus be to aim to ensure that integrated CSU learning and reasoning techniques are bias-aware when fusing information from different sources*.

Coming to the second question, CSU requires a hybrid of computational techniques, as shown in table P5-1 and figure P5.2. The key issue in achieving top-to-bottom explainability and tellability in such a hybrid system is: while HCC, KRR, and MAS approaches are already interpretable and tellable (as all feature communicable models and inferences), approaches based on machine learning (ML, NLP, VSSP) are currently not. This issue is reflected by the large efforts in the ML community, including a recently-launched DARPA project.[145] State-of-the-art approaches in interpretable ML often focus on simple algorithmic models. For instance, in[146] the inferencing step is based on a decision list (Bayesian Rule Lists) that is mined from data. This aims at hitting "the *sweet spot* between predictive accuracy, interpretability, and tractability" by providing (1) more accurate results than SVM and other systems, on the task of predicting stroke risk on real data; and (2) an interpretable model in the form of a chain of if-then statements. In[147] the authors discuss an approach to derive explanatory arguments from a Bayesian network using a *support graph* constructed for a variable of interest that captures the support that variable of interest receives from the other variables. Once evidence is provided, the support graph is used to derive arguments that describe the *logical steps* needed to interpret the Bayesian judgement of the variable of interest.

In[148] we showed how Subjective Bayesian Networks (SBNs), first proposed in[149], can be useful as an interpretable model for supporting decision makers in situational understanding tasks and how they can excel in sparse data conditions. A SBN is an uncertain Bayesian network where the conditionals are subjective opinions instead of dogmatic probabilities, i.e., with an error bar around the inferred probability value. Those error bars become important in cases of sparse training data and give us a level of confidence in the quality of data collected and used in learning the model: they indicate when the probability of the value of a given variable is certain or not, considering evidence (i.e., the values of other visible variables). Specifically, the probability of a queried variable could be highly uncertain because this probability is highly tied to the values of some observed variables (which could represent a rare event). Perhaps one could determine what other evidence to seek (variable values to observe) to arrive at a more certain result by reversing the probabilistic reasoning. However, SBNs can currently represent only propositional knowledge (i.e., binary variables) and dependencies among those propositions. More expressive systems allow for tellability in a learning algorithm. For instance, in[150] the authors show how a very simple probabilistic system coupled with a language able to express subclass relations allows domain experts to express constraints that can be exploited by a classifier for better accuracy, thus mitigating issues related to sparse data. Unfortunately, such alternative approaches have a less robust probabilistic engine (i.e., they can handle only simple probabilities or simple distributions) than SBNs. *Another scientific focus in this BPP will therefore be to seek more expressive knowledge representations to support CSU while affording explainability and tellability to decision makers and domain experts who are not information scientists*. This will be validated following methodology proposed for instance in[151].

---

[145] https://www.darpa.mil/program/explainable-artificial-intelligence

[146] Letham, B., Rudin, C., McCormick, T. H., & Madigan, D. (2015). Interpretable classifiers using rules and Bayesian analysis: Building a better stroke prediction model. *The Annals of Applied Statistics*, 1350-1371.

[147] Timmer, S. T., Meyer, J.-J. C., Prakken, H., Renooij, S., & Verheij, B. (2017). A two-phase method for extracting explanatory arguments from Bayesian networks. *International Journal of Approximate Reasoning*, 475-494.

[148] Braines, D., Thomas, A., Kaplan, L., Sensoy, M., Ivanosvka, M., Preece, A., & Cerutti, F. (2017). Human-in-the-Loop Situational Understanding via Subjective Bayesian Networks. *The IJCAI-17 Workshop On Graph Structures For Knowledge Representation And Reasoning*.

[149] Ivanovska, M., Jøsang, A., Kaplan, L., & Sambo, F. (2015). Subjective networks: Perspectives and challenges. In *Proc. Of the 4th International Workshop on Graph Structures for Knowledge Representation and Reasoning* (pp. 107-124).

[150] Pujara, J., Miao, H., Getoor, L., & Cohen, W. W. (2015). Using Semantics and Statistics to Turn Data into Knowledge. *AI Magazine*, 65-74.

[151] Datta, A., Tschantz, M. C., & Datta, A. (2015). Automated experiments on ad privacy settings. *Proceedings on Privacy Enhancing Technologies* 2015.

Technical Approach

To make progress in this BPP, we propose to separate the research agenda into two sub-tasks:

- Learning and reasoning for collective insight
- Learning and reasoning for collective foresight

We view the state-of-the-art in the former as being closer to a point where we can run experimental validations involving humans performing CSU tasks: see the Validation section for further details.

Sub-task 1: Learning and reasoning for collective insight

As indicated above, our focus here is to advance the scientific understanding of learning and reasoning with probabilistic models. We will leverage state-of-the-art techniques in probabilistic reasoning such as SBNs[148] and more expressive systems: both non-monotonic deterministic approaches, e.g., Answer Set Programming[152], and probabilistic approaches, e.g., probabilistic logic programming[153]. We will critically assess advantages and disadvantages of each approach, and work towards a synthesis to ensure a balance between expressivity and robust probabilistic reasoning. We will evaluate the effectiveness of supporting decision makers in CSU by providing explainable approaches to reduce their cognitive burden and assess value of information. Drawing on prior work on fairness in ML (e.g.,[142]), we aim at providing metrics for biases in CSU and computational methods for dealing with biases in training data sets. In addition to probabilistic graph and logic based models we would also, for comparison purposes, consider deep learning approaches that were explored during IPP[154] and which are the focus of WP0008. For example, different tasks might require different levels of explanations for the decision makers: in some case no explanation at all is needed and perhaps deep learning approaches will be more accurate and thus preferred; in other cases, we might want to create post-hoc explanations out of black-box results; and the other end of the spectrum is where the decision maker needs full explanation of the process—see the Validation section for more details.

In view of the coalition context, our work will also focus on the challenges that arise when data sources, model storage, and computation involved are distributed among multiple organizations in a coalition. Traditionally, distributed inferencing over classical Bayesian Networks is done via message-passing based belief propagation over factor graph representations[155,156], but this does not account for the challenges faced in a coalition setting. We will model the ways in which communication among these entities may be constrained in terms of resources, policy, and availability, and the ways entities themselves exhibit behaviors (bias, incompetence, contested, adversarial, malicious…) that corrupt the learnt model and the inferred query response. Our research will also study the impact of information propagation latencies and uncertain computation and communication speeds which nudge learning and reasoning towards asynchronous approaches[157]. We will investigate the inefficiencies in maintaining synchrony that can in turn affect the learning rate, model quality, and accuracy of reasoning. We will build upon research done in IPP on exploring a subset of such issues in the context of distributed learning over deep networks[154].

By the end of the current BPP in this sub-task we aim to have contributed one or more novel methods for integrating learning and reasoning in a distributed coalition context that afford explainability (for assurance) and tellability (to mitigate against sparse data).

Sub-task 2: Learning and Reasoning for Collective Foresight

---

[152] Eiter, T., Ianni, G., & Krennwallner, T. (2009). Answer Set Programming: A Primer. In Reasoning Web. *Semantic Technologies for Information Systems* (pp. 40-110).

[153] De Raedt, L., & Kimmig, A. (2015). Probabilistic (logic) programming concepts. *Machine Learning*, 5-47.

[154] Chakraborty, S., Preece, A., Alzantot, M., Xing, T., Braines, D., & Srivastava, M. (2017). Deep Learning for Situational Understanding. *20th International Conference on Information Fusion (FUSION).*

[155] Kschischang, F. R., Frey, B. J., & Loeliger, H.-A. (2001). Factor graphs and the sum-product algorithm. *IEEE Transactions on information theory*, 498-519.

[156] Zarrin, S., Lim, & J., T. (2008). Belief propagation on factor graphs for cooperative spectrum sensing in cognitive radio. *New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on*, (pp. 1-9).

[157] Recht, B., Re, C., Wright, S., & Niu, F. (2011). Hogwild: A lock-free approach to parallelizing stochastic gradient descent. *Advances in neural information processing systems*, 693-701.

In this sub-task we will focus on the temporal dimension in learning and reasoning, since projection of future states and events is a key part of situational awareness[158]. Typically, the time dimension is incorporated into probabilistic graphical models such as Bayesian Networks by creating nodes that represent versions of a variable at different time steps[159] (which could be generalized to SBNs in a straightforward manner) and then capturing correlations across time via the edges, and in probabilistic logic-based approaches via temporal logic. We propose to explore a different face of time: dealing with patterns or sequences of primitive instantaneous events that carry special meaning. Inspired by the concept of complex event processing[160] that is used in streaming information systems, we propose to explore "complex events" as the organizing principle for time dimensions for the purposes of tellability and reasoning. We will treat complex events as probabilistic sequences of primitive instantaneous sensor events stitched according to a suitable sensory grammar[161], and map them naturally in both probabilistic graph and probabilistic logic based learning and reasoning which will take into consideration the overall target system. We will validate the performance of our techniques on metrics such as complex event prediction accuracy and false positives/negatives on suitable datasets exhibiting time dependencies—see the Validation section for more details.

By the end of the BPP in this sub-task we aim to have contributed to the literature a novel method for integrating temporal reasoning and learning approaches for CSU, and using complex events to reduce the semantic gap between the system's reasoning and prediction about temporal patterns and events and the human understanding of them.

Validation and Experimentation

Following the framework recently proposed in[162] we intend to validate our "collective insight" research via *human-grounded evaluation* (real humans performing simple CSU tasks) and the "collective foresight" approaches via *functionally-grounded evaluation* (no real humans; proxy CSU tasks), both with open source datasets.

In IPP we are conducting human-grounded evaluation envisaged in[148] — for which we recently completed the ARL HRPO review process and which was assessed not to require for MODREC approval —and, going forward into BPP, we plan to extend this approach using decision games as suggested by[163]. We will adapt/design a repeated decision-making game[164] using multimodal data with features of military relevance that can be run using open source data with generalist participants (e.g., undergraduate students). We will study the effect of aids and guidance offered to decision makers by collective insight provided by automated agents, thus exploiting results known in economic studies relating payoff structures and the amount of information[165].

Via functionally-grounded evaluation, we will validate computational properties and accuracy of fairness/bias metrics. Building on[151], we will test our theoretical advancement to data collected from a pool of service providers competing in the same market as a proxy for coalition operations.

---

[158] Endsley, M. R. (1995). Measurement of situation awareness in dynamic systems. *Human factors*, 65-84.

[159] Parate, A., Chiu, M.-C., Ganesan, D., & Marlin, B. M. (2013). Leveraging graphical models to improve accuracy and reduce privacy risks of mobile sensing. In *Proceeding of the 11th annual international conference on Mobile systems, applications, and services* (pp. 83-96).

[160] Wu, E., Diao, Y., & Rizvi, S. (2006). High-performance complex event processing over streams. In *Proceedings of the 2006 ACM SIGMOD international conference on Management of data* (pp. 407-418).

[161] Lymberopoulos, D., Ogale, A. S., Savvides, A., & Aloimonos, Y. (2006). A sensory grammar for inferring behaviors in sensor networks. In *Proceedings of the 5th international conference on Information processing in sensor networks* (pp. 251-259).

[162] Finale, D.-V., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning.

[163] Moffat, J., & Medhurst, J. (2009). Modelling of human decision-making in simulation models of conflict using experimental gaming. *European Journal of Operational Research*, 1147-1157.

[164] For an example, https://volunteerscience.com/experiments/shadow_force/ .

[165] e.g. Irwin, J. R., McClelland, G., McKee, M., & Schulze, W. D. (1998). *Payoff Dominance vs. Cognitive Transparency in Decision Making. Economic Inquiry*, 272-285.

Regarding our work on collective foresight, we intend to use temporal datasets of simple scalar sensor modalities and, once we have refined our methods, then also consider time series data of complex modalities. Candidate data sets include (i) the crowd-funded dataset http://crowdsignals.io (large set of rich longitudinal mobile and sensor data recorded from a demographically diverse cohort), (ii) the CASAS dataset http://ailab.wsu.edu/casas/datasets/ (a multimodal longitudinal sensor dataset capturing complex events corresponding to activities of daily living), and (iii) our own multimodal UK traffic dataset[166] (including video imagery and natural language). For these experiments, we will devise military-relevant proxy CSU tasks such as location or activity prediction.

Task 2: Interpretable Deep Neural Networks for Coalition Situational Understanding

Primary Research Staff	Collaborators
Alun Preece, Cardiff	Raghuveer Rao, ARL
Unnamed PGR, Cardiff	Ross Lund, DSTL
Simon Julier, UCL	Daniel Harborne (PGR), Cardiff
Amy Widdicombe (PGR), UCL	Yulia Hicks, Cardiff
Chris Willis, BAE Systems	David Marshall, Cardiff
Mani Srivastava, UCLA	Ramya Raghavendra, IBM US
Moustafa Alzantot (PGR), UCLA	Richard Tomsett, IBM UK
Supriyo Chakraborty, IBM US	Vedran Galetic, Airbus
Prudhvi Gurram (PDR), ARL	Alistair Nottle, Airbus
	Pablo Bermell-Garcia, Airbus
	Mark Hall, Airbus
	Santiago Quintana-Amate, Airbus

This task is a continuation of TA2 Coalition Distributed Analytics & Situational Understanding, IPP Project 6, Task 2, aimed primarily at the topics *Distributed and Integrated Fusion for Situation Understanding and Distributed Data Analytics in Coalition Environment.*

[166] A. Nottle, D. Harborne, D. Braines, M. Alzantot, S. Quintana-Amate, R. Tomsett, L. Kaplan, M. Srivastava, S. Chakraborty and A. Preece, "Distributed opportunistic sensing and fusion for traffic congestion detection," in *Workshop on Distributed Analytics InfraStructure and Algorithms for Multi-Organization Federations at IEEE SmartWorldCongress* 2017.

Research Issue

Situational Understanding (SU) is an essential element of military mission planning and execution at both the strategic and tactical levels. There is increasing emphasis on technology-driven autonomy and agility within the command hierarchy for quicker identification and exploitation of opportunities. Machine Learning (ML), based on sophisticated data-driven models and algorithms, is emerging as the linchpin of realizing *perception, comprehension,* and *projection*, the three key elements of SU[167]. However, successful decision making based on SU produced by machines depends not only on the quality of inferences that form the basis of SU but also providing, as warranted, the human or machine decision-maker, with adequate explanation to establish context, trust and collaboration[168]. The explanation is referred to as post-hoc interpretability aimed at providing a functional understanding of the model output in terms of its parameter space[169].

Deep Neural Networks (DNNs) have yielded inferences whose quality far exceeds those of traditional algorithms in multiple domains (NLP, vision, speech, games....). DNNs are multi-layer networks that are used to approximate a function mapping inputs to output classes. Each layer of the network performs a nonlinear projection of its inputs, in the process extracting a new set of abstract features, that are used as input for the next layer. Over multiple training epochs the network automatically chooses the near-optimal set of features that can approximate the function. However, these progressively abstract features learnt by the layers are not readily explainable; hence the opacity of DNNs.

While the underlying problem of interpretability of ML models is hard even in conventional settings, it is even harder in the setting, this white paper considers, which is a nexus of SU based on DNN models and distributed coalition operations in contested spaces.

Coalitions introduce factors such as *source bias, heterogeneous data, policy,* and *variable mutual trust* that constrain information flows and affect quality of data on which models and SU are based[170].

To build interpretable machine learning algorithms within a coalition setting, we identify three key challenges (i) White-box interpretability in the presence of data sparsity; (ii) Interpretability using heterogeneous spatio-temporal data; and (iii) Interpretability under adversarial settings. Our research proposal is divided into three inter-linked sub-tasks corresponding to these challenges.

Technical Approach

A cross-cutting problem across all the different sub-task areas is the need for a well-defined quantitative metric for model interpretability. Prior work has used heat maps over the input space of image pixels for expressing the interpretability of a model. An extensive summary of various state-of-the-art techniques is available in[170]. While these mechanisms are visually appealing and provide meaningful information to a human agent about the functioning of the model, they are qualitative in nature, primarily restricted to image data, designed solely for human agents, and cannot be used to quantitatively compare two models in terms of their interpretability.

---

[167] Mica R. Endsley, "Towards a Theory of Situation Awareness in Dynamic Systems", in Human Factors: *The Journal of the Human Factors and Ergonomics Society*, pp 32-64 (37), 1995.

[168] Marco Tulio Ribeiro, Sameer Singh, and Carlos Guestrin. 2016. "Why Should I Trust You?": Explaining the Predictions of Any Classifier. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '16).*

[169] Zachary C Lipton. "The mythos of model interpretability." arXiv preprint arXiv:1606.03490 (2016).

[170] Supriyo Chakraborty, Richard Tomsett, Ramya Raghavendra, Daniel Harborne, Moustafa Alzantot, Federico Cerutti, Mani Srivastava, Alun Preece, Simon Julier, Raghuveer M. Rao, Troy D. Kelley, Dave Braines, Murat Sensoy, Christopher J. Willis, Prudhvi Gurram," Interpretability of Deep Learning Models: A Survey of Results", in *workshop on Distributed Analytics Infrastructure and Algorithms for Multi-Organization Federations*, 2017.

Recently, an information-theoretic definition for quantifying the interpretability of a complex model was provided in[171]. The authors defined interpretability as the information shared with another target machine to improve its accuracy and robustness. This definition of interpretability, relative to a target model, is an attempt at generalization of the notion for both human agents and other machines. It also allows for comparison of different models based on the improvement they cause in the target model.

While an interesting first step, the definition does not take into account the computational effort required to generate the information, nor does it specify any constraint on the quantity of the information shared and its nature—extremely important factors to consider, especially within a coalition where information generation and sharing are often subjected to constraints. *One of our scientific goals in this BPP is to derive a computationally efficient interpretability metric for the coalition setting.*

Sub-task 1: White-Box Interpretability and Data Sparsity

The interpretability problem for DNNs was formulated with human agents as targets of model-generated explanations. Naturally, "black box" solution approaches were proposed that focused on generating explanations with respect to the input layer alone bypassing all the hidden layers. This was because the input layer contained human-understandable representation of the data. State-of-the-art techniques today use deep Taylor decomposition[172] to generate heat maps that identify the most relevant portions of the input layer that have contributed towards a particular output decision. These heat maps aim to serve as (limited) explanations for the model output.

However, this view is extremely restrictive, especially within a coalition, where machines are also required to interact with other machines. In addition, human agents might also require fine-grained explanations, in a feature space different from the input layer, depending on the task they need to perform. For example, if a model incorrectly detects a wooden pole as a human being, the agent needs to diagnose the reason and correct the model. It is not sufficient to simply generate a heat map on the input image, but also identify the feature space where humans and wooden poles are indistinguishable and is causing the model to make incorrect decisions.

A main focus of this sub-task will be to open up the deep model and identify the properties of suitable feature spaces for interpretability depending on the task of the target model (as in[171]). This will enable what we call as "white-box" interpretability. In the above example, we can consider human agents as the target model, and troubleshooting as the task in hand. We will explore the use of transfer learning to represent the features of the deep model in terms of the features of the target model and explore the possibility of a "challenge-response" form of interaction. The improvement in accuracy of the task can be used as a metric to determine the suitability of a particular layer for interpretability. As is evident, for interaction with machines, any feature layer can be used for interpretability as there is no need to generate an explanation for the feature space. To validate that the shared information is indeed helping the target machine to improve its accuracy, we can build on recent Satisfiability Modulo Theory (SMT) based formulations that have shown to scale for validating DNNs[173].

---

[171] Amit Dhurandhar, Vijay Iyengar, Ronny Luss, Karthikeyan, Shanmugam, "TIP: Typifying the Interpretability of Procedures", arXiv preprint arXiv:1706.02952 (2017).

[172] Grégoire Montavon, Sebastian Lapuschkin, Alexander Binder, Wojciech Samek, and Klaus-Robert Müller, "Explaining nonlinear classification decisions with deep Taylor decomposition". In *Pattern Recogn*. 65, C (May 2017), 211-222.

[173] Guy Katz, Barrett Clark, Dill David, Julian Kyle, and Kochenderfer Mykel. "Reluplex: An efficient SMT solver for verifying deep neural networks." arXiv preprint arXiv:1702.01135 (2017).

The above approach can also help in transfer learning with limited data (which we also refer to as sparse data)[174]. A trained interpretable model can be used to identify portions of the input data (or features) that are relevant to the output classes. The target model, can train using only these relevant features from the limited input data. Intuitively, this will reduce the impact of noise due to sparsity of training data (at the risk of overfitting without adequate regularization).

In summary, the goal of this sub-task in this BPP will be to (i) determine the feature representation for interpretability w.r.t a target model and (ii) quantify the effect of interpretability in transfer learning especially with sparse (or limited) data.

Sub-task 2: Interpretability Using Heterogeneous Spatio-Temporal Data

Coalition missions involve time-series data collated from a number of heterogeneous sources including structured sensory measurements (e.g., location traces, video feeds, radar measurements, surveillance imagery) and unstructured textual data (e.g., Twitter feeds, messaging channels and so on). Therefore, a key operational requirement of a model for situational understanding is to compactly represent time series data over long durations, learn event patterns that occur at different time scales and perform accurate prediction of future states. Finally, explainability of the predictions in situational understanding is particularly important in a multi-agent coalition context for trust-building and collaboration.

Despite the inherent challenges of modelling and classifying time-series data, machine learning models such as deep recurrent neural networks (RNNs) have exhibited very high performance in classification tasks. For example[175] trained a model using LSTM (long-short-term-memory) recurrent neural network cells that achieved better accuracy than humans on speech recognition. Similarly[176], developed an algorithm that exceeded the performance of board certified cardiologists in diagnosing heart arrhythmia from a sequence of ECG signals. RNNs have also been used as generative models to synthesize time series data—a potential information-flow control mechanism, using which fake but plausible data streams are shared in-lieu of actual, but, sensitive data. For example[177], demonstrated the feasibility of synthesizing ECG signals using a modified version of the hierarchical RNN model (see figure P5.4 above), and[178] used RNNs to generate textual descriptions for images.

The aforementioned temporal models are unfortunately not interpretable. Recent research has made some progress in this direction by creating interpretable models for image recognition (ConvNets), that generate heat maps to explain their output decision.

---

[174] Sinno Jialin Pan and Qiang Yan, "A Survey on Transfer Learning", in *IEEE Transactions on Knowledge and Data Engineering*, pp 1345-1359, 22 (10), 2010.

[175] Xiong, Wayne, et al. "Achieving human parity in conversational speech recognition." arXiv preprint arXiv:1610.05256 (2016).

[176] Rajpurkar, Pranav, et al. "Cardiologist-Level Arrhythmia Detection with Convolutional Neural Networks." arXiv preprint arXiv:1707.01836 (2017).

[177] Alzantot, Moustafa, Supriyo Chakraborty, and Mani Srivastava. "SenseGen: A deep learning architecture for synthetic sensor data generation." In *Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017 IEEE International Conference on. IEEE, 2017.

[178] Karpathy, Andrej, and Li Fei-Fei. "Deep visual-semantic alignments for generating image descriptions." In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 2015.

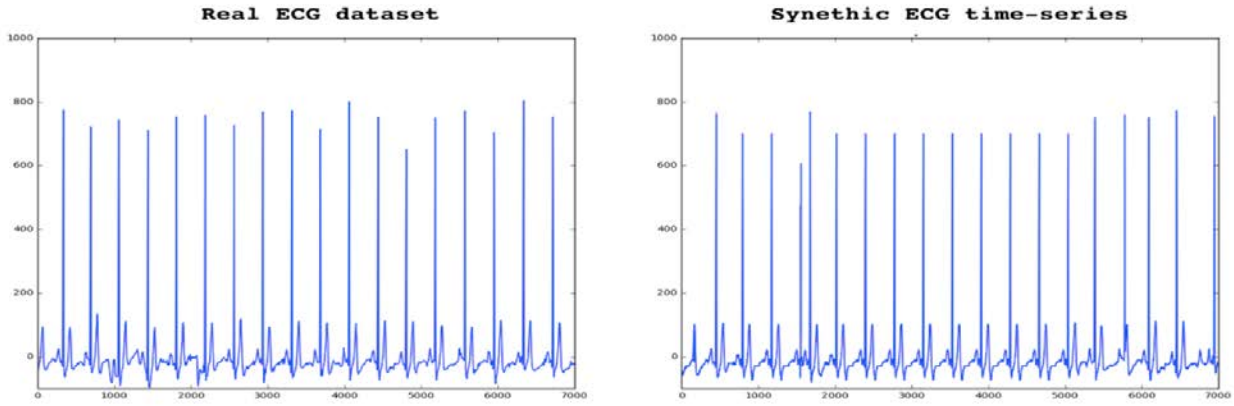

Figure P5-4. Synthetic ECG data generated using a modified Hierarchical RNN (from (Alzantot 2017))

Figure P5-5. Captioning a sequence of video frames (from (Ramanishka 2017))

[179]proposed an approach for building an interpretable model that generates a text description of the input video. The model generates spatiotemporal heat maps that relate output words in the predicted caption to regions in the input image/ video frames (see figure P5.5 above). However, in addition to being focused on images and videos, none of the above techniques address the interpretability problem in the presence of correlated and heterogeneous data sources—a setting unique to coalitions.

In this sub-task, our research agenda is to develop scalable interpretable models for temporal data and generalize these for both structured and unstructured data. Specifically, we will explore the use of graph embedding to capture the dependencies between heterogeneous time series data and use the embedding to effectively train LSTM models. We will also identify network architectures (possibly modified LSTMs) that can learn patterns over multiple time scales. Interpretability can be achieved in the form of uncovering small and large time dependencies that may be used by a human agent to perform root cause analysis, or to reason about other performance issues.

In summary, the goal of this sub-task in this BPP will be to build new interpretable machine learning models that can learn from heterogeneous datasets with spatio-temporal correlations.

[179] Ramanishka, Vasili, et al. "Top-down Visual Saliency Guided by Captions." In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 2017.

Sub-task 3: Interpretability Under Distributed Adversarial Attacks

The model training and scoring processes can be subjected to threats from adversaries that are external or internal to the coalition. The external threats arise in the form of (a) poisoning attacks on data sources compromising the training data thereby corrupting the model itself; or (b) in the form of adversarial examples[180], specifically crafted with knowledge of the model, to exploit its (complementary) feature space and elicit a (mis)classification. The internal threats arise primarily due to the variability in mutual trust between coalition members. An immediate consequence of this skepticism is the imposition of information-flow controls at each member. These policies typically aimed at protecting sensitive information, proprietary to a member, govern the granularity and also the level of uncertainty at which data are shared (very similar to the setting for which Generative Adversarial Networks (GANs)[181] were proposed). Recently, InfoGAN[182] demonstrated how GANs can be applied to learn interpretable latent representation of the data.

In this sub-task, we will adopt a two-pronged strategy for operating in these adversarial settings. First, for attacks that aim to compromise the integrity of the model or elicit a misclassification, we will explore interpretability to determine if the model is operating as designed. Specifically, we will use the interpretability property of the model, as a validation mechanism to ensure that the "correct" set of features are being used for a given input. This may not directly lead to isolation of the compromised sources but can inform that the model has been compromised. However, for adversarial examples, interpretability can not only provide insights into the misclassification but also help identify such malicious examples. Second, for data sharing under information-flow constraints, we will augment GAN-type distributed learning models to accommodate interpretability. Specifically, this will mean fusion of input data (from modalities different from images) with different levels of interpretability into a single model while still ensuring transparency of the model.

In summary, the goal of this sub-task in this BPP will be to (i) explore model interpretability to detect adversarial attacks (data poisoning and adversarial examples); and (ii) propose machine learning models that are interpretable under information-flow constraints.

In terms of linkages between the two tasks in this project, interpretable ML systems can be integrated into the T5.1 architecture for collaborative insight and foresight (cf. figure P5.2).

Validation and Experimentation

We will perform experimentation to validate the fundamental properties of interpretable machines, and improve the techniques developed under the research sub-tasks. Representative use cases we are already working on in the IPP are listed below with their expanded BPP scope.

Interpretable CNN for Congestion Detection: We will address congestion detection using open source traffic camera imagery[139]. We will build interpretable CNNs for vehicle activity detection within military settings, and identify features that lead to better interpretation. We will compare our model with other car

[180] Goodfellow, Ian J., Jonathon Shlens, and Christian Szegedy. "Explaining and harnessing adversarial examples." arXiv preprint arXiv:1412.6572 (2014).

[181] Goodfellow, Ian, et al. "Generative adversarial nets." In *Advances in neural information processing systems*. 2014.

[182] Chen, Xi, et al. "Infogan: Interpretable representation learning by information maximizing generative adversarial nets." *Advances in Neural Information Processing Systems*. 2016.

detectors using hand-crafted features (UCDD) and determine the effectiveness of interpretability. We will also inject artificial noise in the data samples and use interpretability to identify such samples.

***Interpretable Crowd Detector Using Heterogeneous Data*:** We will use heterogeneous open source data consisting of a time series of images and related text to detect crowds and provide their locations. The imagery will provide the initial detection, the text (or their vectorised representation generated using word2vec models[183]) will provide a location and fusion of the two will give a complete geo-located detection. We will develop novel techniques, that can exploit the correlation between heterogeneous datasets used for training the model to also increase it interpretability. Finally, for evaluating temporal interpretability, we will track the size and location of crowds over time and also use the open source dataset (CCV) for captioning activity sequences.

Experimentation with Human Participants: The effectiveness of an interpretability metric, and the generated explanation, are often determined by the utility received by a human agent in performing her respective tasks. In order to explore this and to produce a baseline for developing reliant interpretability metrics (for Sub-tasks 1 and 2), we propose conducting trials using human subjects (while adhering to MODREC and HRPO procedures and approvals for human-derived data use).

Military and DAIS ITA Relevance

The planned research aligns with ARL's Artificial Intelligence & Machine Learning and Human-Agent Teaming Essential Research Areas, targeted at addressing gaps in the coalition context related to **Generalizable and Predictable AI** (specifically the challenge of handling *Explainability and Programmability for AI and ML*) and **Learning in Complex Data Environment** (specifically the areas of *AI and ML with Highly Heterogeneous Data* and *Adversarial AI and ML in Contested Deceptive Environment*).

A key focus of this work is to enable non-technical members of the team to rapidly configure the system—through insertion of local knowledge, addition of emerging relevant information, and the tuning of system parameters—enabling the human/machine coalition to more rapidly react to the situation as it unfolds on the ground. We acknowledge and enforce heterogeneity in system components, models, and interfaces to reflect the reality of a coalition. Finally, data sparsity is a key challenge in these environments and will be a driver for our research. We will consider different bootstrapping techniques, injection of relevant human knowledge through our "tellability" concept, and further investigation and evaluation of Subjective Bayesian Network capabilities. We will reflect the reality of working with heterogeneous data in contested deceptive environments in our large experimentation endeavour and we will exploit SME expertise to this end.

The planned validation of the research should inform potential future systems operating in such environments: whilst the military environment is an obvious example we feel that the research is much more broadly applicable. Any situation involving rapidly formed teams from diverse organisational backgrounds will benefit from this work, for example: Law enforcement, anti-terrorism, community safeguarding, fire-fighting…

Our research will develop methods for interpretability of DNNs, and the resulting explainability of inferences, will lead to better decision making, better trust and accountability between humans and machines at the tactical edge, and let coalition partners reconcile individual SUs for consistencies and conflicts. It will enable military coalition operations to benefit from the tremendous performance advantages offered by DNNs in enabling models for SU that are both highly performant and interpretable. ARL and DSTL collaborators on

[183] Thomas Mikolov, Kai Chen, Greg Corrado, and Jeffrey Dean. "Efficient Estimation of Word Representations in Vector Spaces." arXiv preprint arXiv:1301.3781 (2013).

the team will contribute significantly to designing military-relevant scenarios for experimentation-driven validation of methods and solutions developed.

The experimental basis for the research should also provide the potential for a "fast track to impact", specifically in the case of potential DAIS transition projects or through adoption of results, software artefacts, or architectures in the wider research and development community. We intend to make all results and software available as Open Source to maximise the potential for impact within and beyond the DAIS community.

Both academia and industry partners will actively seek transition opportunities. We expect the research in this task to be fast-tracked to transition via Cardiff's Open Source Communications Analytics Research (OSCAR) Centre http://upsi.org.uk/oscar/ and its strategic relationships with several UK police forces. Fusion of open source intelligence from textual and visual social media has considerable potential in modern policing and counter-terrorism functions. Being a relatively new area with an active research community we will seek engagement and collaboration with this community through open-source release of prototype software. Finally, commercial transition opportunities will be explored by the industry partners through possible product offerings (Watson cloud services, services and processes at Airbus).

Collaborations, Staff Rotations, and Linkages

"DARPA Explainable AI Program (XAI)": Distinct from this program, our focus is on model interpretability in a distributed coalition setting under information-flow constraints. In addition, coalition operations rely on the evolution of foresight/predictions over time leading to the unique challenge of temporal interpretability.

We will seek opportunities for potential collaborations and mutual exchanges.

Project 3, Task 2 has elements of distributed learning for placement, scheduling and validation of tasks and resources in a coalition. We will explore potential linkages and seek opportunities for collaboration.

Project 4, Task 2 considers sub-symbolic approaches for robust service chains in a distributed analytics environment; we will collaborate with the team via T5.1 (where we will be generating service chain instances for integrated reasoning and learning) and T5.2 (for potential interpretability of T4.2 processes).

Project 6, Task 1 aims to generate models of group behavior so it will be interesting to explore how such models may inform SU, and how the reasoning and learning processes here may feed into such models.

Staff Rotations:

i. Invite PhD students for industry summer internships at IBM US, IBM UK, and BAE Systems.
ii. Short duration academic visits between team members.
iii. Visit to ARL facilities

Research Milestones		
Due	**Task**	**Description**
Q1	**Task 1**	Critical analysis of approaches to collective insight **Deliverable:** Paper analyzing critical analysis of different approaches including SBNs, deep learning, and (probabilistic) logic programming systems (Cardiff, IBM-UK, IBM-US, UCLA, ARL, Dstl)
Q1	**Task 2**	**Sub-task 1**: Interpretability metric and initial investigation into automatic identification of suitable feature space depending on the requirement of the target model ("challenge-response" interaction). **Deliverable:** Conference/Workshop paper that will build on the existing approaches and also quantify the computational effort in estimating the

Research Milestones		
Due	**Task**	**Description**
		suitable feature space. IBM-US; Cardiff, UCL, UCLA; ARL, DSTL
Q2	**Task 1**	Critical analysis of approaches to collective foresight **Deliverable:** Paper analyzing different approaches for collective foresights (distributed and temporal) (UCLA, Cardiff, IBM-UK, IBM-US, ARL, Dstl)
Q2	**Task 2**	**Sub-task 2:** Designing new temporal models for interpretability with heterogeneous time series data; Experimentation platform for crowd detector using (images and text data). **Deliverable**: Conference paper (on the interpretable crowd detector work) and software prototype. Cardiff; BAE, IBM-US, UCL, UCLA; ARL, DSTL
Q3	**Task 1**	Initial evaluation of systems for collective insight, including handling of bias **Deliverable:** Research grade software implementing initial approaches for comparison, leading to conference/workshop paper with preliminary evaluation of bias metrics (IBM-US, Cardiff, IBM-UK, UCLA, ARL, Dstl)
Q3	**Task 2**	**Sub-task 3**: Leveraging results from Sub-task 1, use interpretability to detect adversarial examples; conversely use interpretability to generate adversarial examples. **Deliverable:** Conference paper detailing the role of interpretability in generating and detecting adversarial examples. UCLA; Cardiff, IBM-US, IBM-UK, UCL.
Q4	**Task 1**	Preliminary proposal for collective foresight (distributed and temporal) **Deliverable:** Research grade software and conference paper on collective foresight (UCLA, Cardiff, IBM-UK, IBM-US)
Q4	**Task 2**	**Sub-task 1**: Analysis and prototype implementation of mechanisms for computing the suitable features for interpretability; Analyze the accuracy of interpretable features in transfer learning under data sparsity. **Deliverable**: Journal paper submission with detailed findings. UCL; Cardiff, IBM-US, UCLA; ARL
Q5	**Task 1**	Prototype for evaluating approaches for collective insight with humans in the loop **Deliverable:** Research grade software for experimentation, including accountability evaluation (IBM-UK, Cardiff, IBM-US, UCLA, ARL, Dstl)
Q5	**Task 2**	**Sub-task 2**: Analysis and prototype implementation of new temporal models for interpretability; Experimentation platform for Congestion detector (using interpretable CNNs). **Deliverable**: Conference paper (on novel temporal interpretable model) and software prototype. UCLA; Airbus, BAE, Cardiff, IBM-US; ARL, DSTL.

Research Milestones		
Due	**Task**	**Description**
Q6	**Task 1**	Human-grounded experimental evaluation of approaches for collective insight **Deliverable:** Journal paper submission on different approaches to learning and reasoning for situational understanding (Cardiff, IBM-UK, IBM-US, UCLA, ARL, Dstl) Conference/journal paper on algorithm accountability (IBM-US, Cardiff, IBM-UK, UCLA, ARL, Dstl)
Q6	**Task 2**	**Sub-task 3**: Augment GAN-based learning mechanisms for interpretability in a distributed setting; Analysis and prototype implementation. **Deliverable**: Conference paper on findings and software prototype. IBM-US; Cardiff, IBM-UK, UCL, UCLA.
Q7	**Task 1**	Functionally-grounded evaluation of collective foresight for distributed and temporal learning and reasoning **Deliverable:** Journal paper on collective foresight (UCLA, Cardiff, IBM-UK, IBM-US, ARL, Dstl)
Q7	**Task 2**	**Sub-tasks 1-3**: Human-subject study of interpretable temporal models under information-flow constraints. Feedback from the study will inform the suitability of the interpretability metric for human decision-makers. **Deliverable**: Journal Paper detailing the findings of • Human study • Suitability of the interpretability metric for temporal models • Evaluation on multiple use-cases using open-source data Cardiff; Airbus, BAE, IBM-US, IBM-UK, UCL, UCLA; ARL, DSTL
Q8	**Task 1**	Consolidation and release of open source materials **Deliverable:** Open source public release of research-grade of software, models, tools and algorithms, with documentation and tutorial (IBM-UK, ARL, Cardiff, Dstl, IBM-US, UCLA)
Q8	**Task 2**	**Sub-tasks 1-3**: Consolidation of scientific outputs. **Deliverable**: • Release of open-source software, models, tools and algorithms • Documentation in the form of technical reports/presentations/code repositories UCL; Airbus, BAE, Cardiff, IBM-US, IBM-UK, UCLA; ARL, DSTL,

In the milestones table above, the lead institution is first and underlined; other funded contributors are listed alphabetically; and the government collaborators are listed at end.

Project 6: Evolution of Complex Adaptive Human Systems

Project Champion: Roger Whitaker, Cardiff University

Email: WhitakerRM@cardiff.ac.uk **Phone: +44 (0)29 2087 6999**

Primary Research Staff	Collaborators
Diane Felmlee, PSU	Gavin Pearson, Dstl
Don Towsley, UMass	Grace-Rose Williams, Dstl
David Rand, Yale	Alun Preece, Cardiff
Liam Turner, Cardiff	Gualtiero Colombo (PGR), Cardiff
Roger Whitaker, Cardiff	Stuart Allen, Cardiff
Rachel Bellamy, IBM US	Sue Toth, ARL
Geeth de Mel, IBM UK	Chris Dearlove, BAE Systems
Dave Braines, IBM UK	Richard Tomsett, IBM UK
Unnamed PDR, Yale	Sebastian Stein, Southampton
Unnamed PDR, Yale	Edward Cater (PGR), Southampton
Rhodri Morris (PGR), Cardiff	Peter Johnson, Dstl (Bath)
Lauren Hudson (PGR), Cardiff	
Unnamed PGR, Cardiff	
Jian Li (PGR), UMass	
Cassie McMillan (PGR), PSU	
Cheryl Giammanco, ARL	
Malgorzata Turalska (PDR), ARL	

Project Summary/Research Issues Addressed

The purpose of Project 6 is to undertake basic research in understanding how complex adaptive human systems evolve in conditions relevant to coalition operations and how they can be proactively influenced. Groups are a fundamental element of human behavior, yet being able to interpret, understand and forecast group dynamics remains formative. This requires exploring the properties of groups, and the processes that lead to collective behavior. It also involves exploring the principles determining how such groups would react to external stimuli and interactions with other collectives.

There is substantial interdisciplinary literature concerning complex human systems spanning subjects such as sociology, anthropology, psychology, biology and economics. However the associated theory is generally "static", developed through wide-ranging methodologies that typically draw findings from different forms of human participation and observation. Based on such theory in isolation, it can be challenging to determine the strength of effect and interaction with other factors. However project 6 seeks to take forward the state-of-the-art by considering the dynamics that fuel group-level behavior in new ways. Specifically two issues are considered:

- Task T6.1 addresses the fracture and formation of groups, based on psychological modeling of inter-group behavior.

- Task T6.2 addresses understanding of group behavior through network motifs.

The tasks are complementary – while the first (T6.1) looks at understanding the human emergence of group level phenomenon that are caused by individual-level social psychology, the second (T6.2) focuses on sophisticated approaches to analyzing group behavior based on patterns of interactions between members.

These tasks address significant research issues. For the first task, these are summarized in Figure P6-1, which shows the technical advancement over the state-of-the-art, by developing computational models of group behavior that are grounded in relevant theory. This task seeks to research and validate causal computational models to understand the far-reaching implications of prejudice, bias and inter-group conflict. These have been considered a "problem of the century[184]", underlying phenomena such as hate, ethnocentrism, xenophobia and warfare. Modeling gives analysts and coalition decision makers an ability to gain knowledge of group behavior in these scenarios for planning and forecasting. Maintaining post-conflict security, peace-keeping and involvement in asymmetric warfare are common problems facing coalition operations. Developing a common understanding of group behavior and dynamics provides important tactical advantages, and we explore how computational models can be formulated to provide analyst insight. We also note that interactions between groups, and the resulting inter-group relations, can be viewed as a human negotiation process over cooperative or other resources. This introduces a new form of policy generation that extends game-theoretic negotiation to incorporate psychological influences: we explore how more accurate modeling of human behavior can be used in automated policy generation for conflicted situations.

[184] Fiske, S. T. (2002). What we know now about bias and intergroup conflict, the problem of the century. *Current Directions in Psychological Science, 11*(4), 123-128.

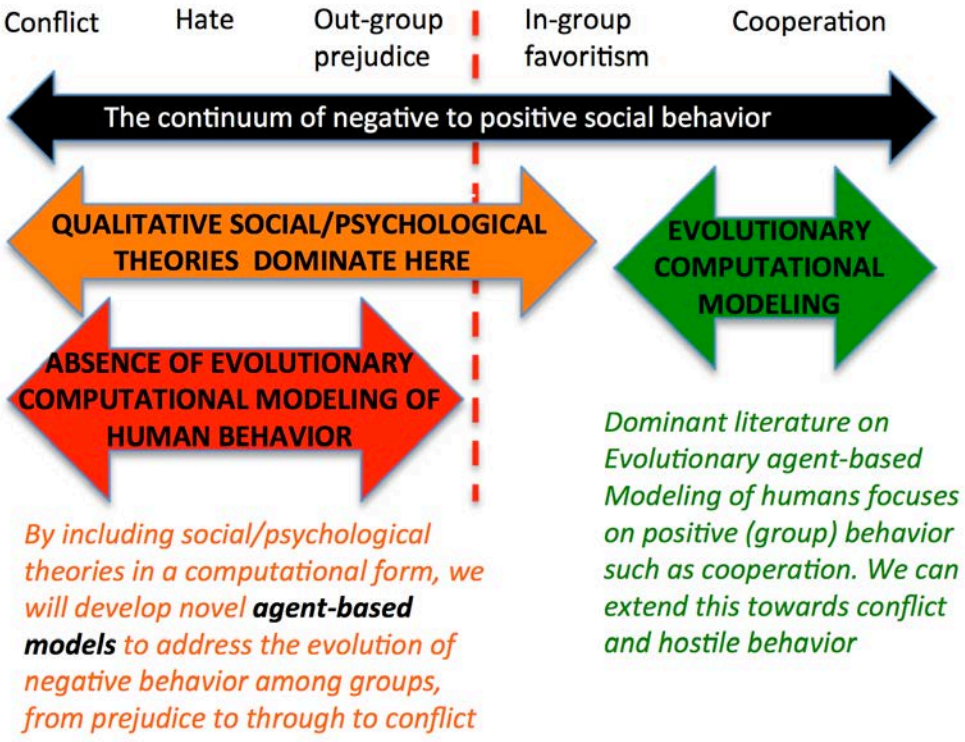

Figure P6-1. Negative to cooperative behaviorial spectrum

The second task focuses on characterizing traceable interactions that allow group behavior to be understood and harnessed to interpret the nature of group interactions through motifs. Network motifs are recurring, significant patterns of interaction between sets of nodes, representing the basic building blocks through which interactions can be considered. These interactions are governed by an internal network structure, of which fleeting glimpses may be externally observed through motifs. Consequently the research challenge is to build theory and techniques that allow inferences to be made on the nature of a group and its interactions. Specifically this will be achieved by extending the state-of-the-art concerning static networks, dynamic networks and the role of networks on inter-group behavior. This will allow "reverse engineering" of intelligence from partial information in potentially noisy and obfuscated environments. In particular, the confidence in which decisions and inferences can be made will be highlighted.

Understanding the interaction dynamics of external groups in conflict, insurgency and peace-keeping situations is of value to coalition forces. The closed and subversive nature of such networks means that being able to build knowledge on a wider network from observation of sub-structures and interactions is highly valuable. Achieving this in a coalition setting will help to build a shared understanding of a common threat, which enhances military intelligence. Particularly important scenarios where this is useful include: adversarial networks such as terrorist cells, sources of positive and negative online communication, determining good structures for tactical military networks, examining differences in coalition networks and in knowing how networks of networks can be organized. The current state-of-the-art in motifs does not allow this to be achieved to full effect, presenting a significant knowledge gap.

Technical Approach

The technical approach for the project involves concurrent tasks that are designed to make structured progress. This is assured through achievements in the IPP that have affirmed the viability and significance of the planned research.

In both Tasks, the organization is delivered by key questions that motivate the activity. In the first task (T6.1) we ask:

- How can computational models be extended to include social and psychological theory?
- How can real world scenarios be included in simulations?
- How can analyst understanding be enhanced to aid objective observation?
- How can understanding of automated policy negotiation in conflicted situations between groups be enhanced?

In the second task (T6.2) we ask:

- How do motifs characterize different groups of interest to DAIS-ITA?
- How do motifs change over time in dynamic, mutable networks and can we capture this by new concepts (*T-motif*)?
- Can motifs be used to gain insight into inter-group behavior, such as cooperative alliances or escalating conflict between external groups?
- What motif-structures occur in coalition networks, and are they similar to other subgraph structures?
- How do we account for missing data or erroneous data (presence of a link when one does not exist)?

These questions motivate the technical approaches to both tasks, characterized by explicit goals. In the first task the explicit goals are to:

1. Ground evolutionary agent based simulation in social and psychological theory.
2. Determine how real-world scenarios can be modeled and explained in terms of social and psychological theory.
3. Optimize how coalition stakeholders, such as analysts, engage with evolutionary modeling to support decision-making.
4. Determine the effects of including human influence in game theoretic negotiation for policy.

In the second task the explicit goals are to:

1. Determine presence and role of motifs in coalition-relevant human social networks from analysis of data.
2. Develop tools to analyze motifs in a temporal setting and to develop new insights into the latent behaviors of dynamic networks.
3. Determine the extent to which motifs predict behavioral and structural features within and between groups.

The different goals warrant different methodological approaches. These include data analysis (T6.1 Goal 2, T6.2 Goal 1, 3), theoretical and methodological developments (T6.1 Goals, 1, 4, T6.2 Goals 2, 3), simulation (T6.1 Goals 1, 4, T6.2 Goals 2, 3) and user interaction (T6.1 Goal 3).

These goals offer the opportunity for good interrelation between tasks. Specifically actions that individuals take, both internally towards their in-group, and the response to an out-group, are influential to growth, cohesion and behavioral characteristics of the group. Agent-based modeling in the first task will seek to elaborate on this issue, while Motifs in task 2 can be used to capture interaction behavior within and between groups as a temporal sequence of events between actors. This provides opportunities for new insights: a link between actions of individuals and the collective mission of a group that fuels conflict. The project champion (Cardiff) provides this bridge between tasks, bringing additional partners from both tasks where opportunities arise.

In terms of verifying the output, this will be accomplished in accordance with the research methodologies commensurate with exploration of each Goal. These will include:

- Triangulation across different sources of data and multiple data sets (both tasks)
- Benchmarking techniques and sensitivity analysis from simulation (both tasks)
- User observation, participation and feedback for human-computer interaction (first task)
- Analysis and proof for new techniques and theory (second task)

Supercomputing resources will be used to examine large parameter spaces, and undertake distributed simulation. In particular Supercomputing Wales resources will be accessed, which is part-funded by the European Regional Development Fund (ERDF) via Welsh Government.

Task 1: Fracture and Formation: Evolutionary and Psychological Modeling of Inter-Group Behavior

Primary Research Staff	Collaborators
Roger Whitaker, Cardiff	Alun Preece, Cardiff
Liam Turner, Cardiff	Gualtiero Colombo (PGR), Cardiff
Rhodri Morris (PGR), Cardiff	Stuart Allen, Cardiff
Unnamed PGR, Cardiff	Grace-Rose Williams, Dstl
Rachel Bellamy, IBM US	Richard Tomsett, IBM UK
Geeth de Mel, IBM UK	Sebastian Stein, Southampton
David Rand, Yale	Edward Cater (PGR), Southampton
Unnamed PDR Yale	
Unnamed PDR , Yale	
Cheryl Giammanco, ARL	

We are seeking to research and validate causal computational models to understand the far-reaching implications of prejudice, bias and inter-group conflict. These fuel phenomena such as hate, ethnocentrism, xenophobia and warfare. Modeling gives analysts and coalition decision makers an ability to gain knowledge of group behavior in particular scenarios for planning and forecasting. Maintaining post-conflict security, peacekeeping and involvement in asymmetric warfare are common problems facing coalition operations. Developing a common understanding of group behavior and dynamics provides important tactical advantage.

To date, computational modeling of human behavior predominantly addresses “positive concepts”. Evolutionary biology, psychology and economics have made progress in understanding how and why cooperation emerges, complemented in sociology by social exchange theory. However, moving towards conflict in Figure P6-1, computational insights on negative human behaviors rapidly diminish. Beyond in-group favoritism[185], [186], few additional computational contributions exist concerning negative behavior. This presents a major knowledge-gap concerning the evolution of inter-group conflict.

Our IPP research[187] has identified a limited number of computational models for inter-group conflict. Observations of this literature include i) layering of theories and variables in a model, impeding the engagement of

[185] Hammond, R. A., & Axelrod, R. (2006). The evolution of ethnocentrism. *Journal of Conflict Resolution*, *50*(6), 926-936.

[186] Fu, F., Tarnita, C. E., Christakis, N. A., Wang, L., Rand, D. G., & Nowak, M. A. (2012). Evolution of in-group favoritism. *Scientific reports*, *2*, 460.

[187] Whitaker, R. M., & Preece, A. D. (2017). From evolution to revolution: understanding mutability in large and disruptive human groups.

non-expert users[188]; ii) lack of a principled approach in grounding computational models based on validated theory[189]; and iii) high-level abstractions that obfuscate interactions between individual actors and groups[190,191].

Furthermore, we note that *qualitative* sociological and psychological theories dominate our current understanding of negative inter-group behavior, concerning group motivation, identity and social influence. These are isolated from computational modeling. During the IPP, we identified[192] major theories that have potential quantitative representations, including *Social Impact Theory*[193], *Social Identity Theory*[194] and *Identity Fusion Theory*[195].

We also observe[196] the limited use of external data to parameterize simulations for complex and contested environments. Considering the correlation between such data and simulation results builds confidence for model applicability. This relates to capability concerning situational awareness (P4). Finally we note that interactions between groups, and the resulting inter-group relations, can be viewed as a human negotiation process over cooperative resources. This introduces a new form of policy generation extending game-theoretic negotiation to incorporate psychological influences, consistent with P2.

Technical approach

We address evolutionary modeling of inter-group behavior to understand the conditions under which groups may form and fracture. Our hypothesis is that *social and psychological theory can be incorporated into evolutionary agent-based models, to understand the motivations and dynamics that lead to inter-group conflict.*

We focus on the following research questions.

1. *Model extension to include social and psychological theory:* How can different theories be embedded through agents, their cognition and evolution? What effects do alternative theories produce and what are the differences? Do compound effects occur from including multiple theories and what are most dominant? How can models be consistently compared?
2. *Real world scenario inclusion:* What cues and characteristics can be derived from real world data for situational awareness? Agents can include what features? How can real-world data be used to inform the analyst's selection of appropriate theories for a scenario? To what extent can input parameter selections be informed by real-world data?
3. *Analyst understanding:* How can we ensure that different coalition analysts make consistent interpretations of complex social models in different cultural contexts? Can traceability be embedded in models as a

---

[188] Bernard, M. L., Backus, G. A., Bier, A. B., & Branch, S. F. (2014). Behavioral Influence Assessment (BIA): A multi-scale system to assess dynamic behaviors within groups and societies across time. *Advances in Cross-Cultural Decision Making*, *5*, 161.

[189] Bier, A. B., & Bernard, M. L. (2014). Validating a hybrid cognitive-system dynamics model of team interaction. *Advances in Cross-Cultural Decision Making*, *5*, 209.

[190] McPherson, M. (1983). An ecology of affiliation. *American Sociological Review*, 519-532.

[191] Choucri, N., Goldsmith, D., Madnick, S., Mistree, D., Morrison, J. B., & Siegel, M. (2007). Using system dynamics to model and better understand state stability.

[192] Whitaker, R. M., et al (2017). From evolution to revolution: understanding mutability in large and disruptive human groups. SPIE.

[193] Nowak, A., Szamrej, J., & Latané, B. (1990). From private attitude to public opinion: A dynamic theory of social impact. *Psychological Review*, *97*(3), 362.

[194] Hogg, M. A. (2016). Social identity theory. *Understanding Peace and Conflict Through Social Identity Theory*, 3-17.

[195] Swann Jr, W. B., Gómez, Á., Seyle, D. C., Morales, J., & Huici, C. (2009). Identity fusion: the interplay of personal and social identities in extreme group behavior. *Journal of personality and social psychology*, *96*(5), 995.

[196] Turner, L.D., Colombo, G., Whitaker, R.M., Felmlee, D. (2017). Parameterising the Dynamics of Inter-Group Conflict from Real World Data. First International Workshop on Distributed Analytics InfraStructure and Algorithms for Multi-Organization Federations, IEEE SMARTWORLD.

means to aid objective observation? Can the system understand the analyst's particular situation so as to help manage their attention and support appropriate and rapid decision-making? What HCI requirements are influential and optimal?

4. *Group effects on policy decision-making:* Can understanding of automated policy negotiation in conflicted situations between groups be enhanced? How does the incorporation of social and psychological influence affect game theoretic negotiation? What are the implications for the extension to reasoning based on human psychological influence?

We address these questions through four subtasks.

Subtask 1: Model extension

Goal: Ground evolutionary agent based simulation in social and psychological theory.

Our approach to incorporating social and psychological theory in evolutionary computational models builds on the IPP stage, based on: the proof of concept generative models[197]; a comprehensive understanding of the related literature[198]; and ongoing collaboration between Cardiff and Yale[199] addressing the origins of inter-group conflict[200]. This draws on previous fundamental evolutionary modeling from both Cardiff and Yale, independently published in *Nature Scientific Reports*, concerning in-group evolution[201] and the importance of social comparison behavior[202].

We will use agent-based modeling to incorporate social[203] and psychological theories such as *Social Impact Theory*[204], *Social Identity Theory*[205] and *Identity Fusion Theory*[206] within individual decision-making processes, to understand the emergence of negative and conflicting behavior. We will develop new ways to encode these theories within agents, using techniques including reinforcement of actions and distortion of views. We will then observe the decision-making of individuals and groups in the presence of a social dilemma (events giving options for helping, shirking or impeding another individual or group). This will expose forces within and between groups that fuel the escalation and de-escalation of conflict.

We will investigate the conditions under which divergence within groups emerges (i.e., group fracture) and conditions where groups grow in membership and mission (i.e., formation). Our modeling and validation approach will cross check the extent that social and psychological theories of decision-making and influence for the individual are consistent with seminal theories concerning *intergroup contact*[207], *the nature of prejudice*[208] and *intergroup conflict*[209].

Subtask 2: Real world scenario inclusion

---

[197] Turner, L.D., Colombo, G., Whitaker, R.M., Felmlee, D. (2017). Parameterising the Dynamics of Inter-Group Conflict from Real World Data. First International Workshop on Distributed Analytics Infrastructure and Algorithms for Multi-Organization Federations, IEEE SMARTWORLD.

[198] Whitaker, R. M., et al (2017). From evolution to revolution: understanding mutability in large and disruptive human groups. SPIE.

[199] Eshghi, S., Williams, G-R., Colombo, G., Turner, L.D., Rand, D, Whitaker, R, Tassiulas., L. (2017). Mathematical models for social group behavior. IEEE SMARTWORLD.

[200] Whitaker, R. M., Colombo, G. B., Rand., D. The Evolution of Prejudice, *in preparation.*

[201] Whitaker, R. M., Colombo, G. B., Allen, S. M., & Dunbar, R. I. (2016). A dominant social comparison heuristic unites alternative mechanisms for the evolution of indirect reciprocity. *Scientific reports*, *6*, 31459.

[202] Fu, F., Tarnita, C. E., Christakis, N. A., Wang, L., Rand, D. G., & Nowak, M. A. (2012). Evolution of in-group favoritism. *Scientific reports*, *2*, 460.

[203] Bharathy, G. K., & Silverman, B. (2013). Holistically evaluating agent-based social systems models: a case study. *Simulation*, *89*(1), 102-135.

[204] Nowak, A., Szamrej, J., & Latané, B. (1990). From private attitude to public opinion: A dynamic theory of social impact. *Psychological Review*, *97*(3), 362.

[205] Hogg, M. A. (2016). Social identity theory. *Understanding Peace and Conflict Through Social Identity Theory*, 3-17.

[206] Swann Jr, W. B., Gómez, Á., Seyle, D. C., Morales, J., & Huici, C. (2009). Identity fusion: the interplay of personal and social identities in extreme group behavior. *Journal of personality and social psychology*, *96*(5), 995.

[207] Pettigrew, T. F. (1998). Intergroup contact theory. *Ann. review of psychology*, *49*(1), 65-85.

[208] Allport, G. W. (1979). *The nature of prejudice*. Basic books.

[209] Tajfel, H., & Turner, J. C. (1979). An integrative theory of intergroup conflict. *The social psychology of intergroup relations*, *33*(47), 74.

Goal: Determine how real-world scenarios can be modeled and explained in terms of social and psychological theory.

Subtask 1 facilitates modeling in support of generalizable results for conflict modeling. An immediate question concerns the extent to which parameterization can be used to interpret and explore real world scenarios. From the IPP, we have investigated[210] the extent to which data sets capturing real-world conflicts can be used for agent-based modeling. The answer to this is affirmative: using real world data sources (e.g., Social Conflict Analysis Database, SCAD) we can extract the frequency and impact of events, and establish inter-group relationships. These data make it possible to represent realistic scenarios and potential input parameters for agent based models, emulating the interaction between conflicting groups. Although correlation does not infer causation, and external data can be noisy, we can gain preliminary confidence concerning the alignment of models with real world events.

This provides a new basis for "tellability": being able to explore a possible narrative based on its relation to fundamental theory in sociology and psychology. This task is also closely links to P6 with regard to fusing disparate and distributed data sources and extracting understanding. We will also explore the inclusion of heterogeneity in an agent's capability. For example, situational factors (e.g., location or proximity to conflict or the network "edge") may be influential in distorting an agent's external vision or decision-making. These issues are currently unexplored[211].

Subtask 3: Analyst understanding

Goal: Optimize how coalition stakeholders, such as analysts, engage with evolutionary modeling to support decision-making.

Agent-based models that are grounded in social and psychological theory offer powerful utility to inform analysts and stakeholders. Currently there is no "industry standard" software package or convention for social and inter-group modeling, leaving a significant weakness for coalition defense capabilities. This is due to the complexity in modeling human groups.

The approach in subtask 1 allows alternative possible theories to be selected for inclusion in simulation. However, two immediate challenges emerge. Firstly we need to ensure that a non-academic expert (i.e., who hasn't developed the model), such as the analyst, can readily engage with the underlying models to probe their effect in particular scenarios. Secondly, we need to promote consistency of interpretation, for example ensuring that different coalition analysts, from different countries and different military experiences, are able to extract the same observations and value from the information provided, often in the presence of a non-western cultural lens.

This results in an interaction design issue: to understand human construction and interpretation of the conceptual models we adopt, including associated data. We will use a multi-method approach involving ergonomics and human factors, to critically assess how analysts construct their understanding as to how evolutionary agent based models based on social/psychological theory may function and provide insights. Studying the approach taken by analysts with different backgrounds and knowledge as they do a wide range of structured tasks will develop this insight. Such tasks will explore and reflect the complexity of constructing a human understanding of a model that has collective effects or feedback.

We will use this to articulate the human-computer interaction requirements needed to provide an intuitive rather than deliberative approach to using software for agent-based simulations, and develop design principles to guide the design of human interfaces. We will explore the use of traceability of processes to support user objectivity, which is a fundamental contribution. As a final validation of the design methodology, we will deploy the software to assess how analysts from different coalition countries (US and UK) engage with the design, and to what extent similar value of information is deduced.

Subtask 4: Group effects on policy decision-making

Goal: Determine the effects of including human influence in game theoretic negotiation for policy.

---

[210] Turner, L.D., Colombo, G., Whitaker, R.M., Felmlee, D. (2017). Parameterising the Dynamics of Inter-Group Conflict from Real World Data. First International Workshop on Distributed Analytics Infrastructure and Algorithms for Multi-Organization Federations, IEEE SMARTWORLD.

[211] Whitaker, R. M., et al (2017). From evolution to revolution: understanding mutability in large and disruptive human groups. SPIE

We will extend game theoretic negotiation to include social and psychological effects on decision-making. Specifically, we will investigate game theoretic approaches, tempered with evolutionary computational models, for autonomous policy negotiations when conflicts occur within or between groups. This will investigate combining normative reasoning with game theory, and optimisation of policies (e.g., how could we generate a particular set of policies that encourage self-interested group-based agents to behave in a particular way). Additionally, we will research models for incentives and self-interest to understand agents who frequently deviate from set policies.

Moreover, we note that the previous work in this space has mainly assumed rational interaction theory[212], and closed world logical models were proposed[213]. Such crisp knowledge representations are not suited for fuzzy concepts such as social and psychological effects present in human-machine teams. We will thus explore how social and psychological effects may be manifested in a range of human policy scenarios—e.g., policy making between coalition members where group norms have variance or strong internal networks; interest-based negotiations could be useful in such situations as previously considered for coalition agents to achieve collective goals[214]. For external groups, we will consider conflict escalation. We will include mixed human-autonomous system collectives, where social influence is felt by the human but not by the machine.

To enable agents to interpret social and psychological effects, agents require pragmatic models of discourse. Past work for web agents concerning large knowledge graphs[215] will be generalised to interpret social and psychological constructs. Through collaboration with P2, we seek to benefit from generative policy models. These address complexity and uncertainty, especially when resources need to generate policies for themselves; for example an agent may instantiate a policy for itself due to changes in mission goals influenced by human team members though a series of iterative refinements. Regarding policy refinement we will determine if mission policy can be formulated to optimise the functioning of a complex social group: beginning with an abstract mission statement, through refinement techniques used to generate group-specific concrete forms that consist of social primitives. Recognition (from observing social signatures) and response to (through social influence) changes in social context will be evaluated.

Validation and Experimentation

Subtask 1 will involve assessing the extent to which including social and psychological theories pertaining to individual agent decision-making result in the group effects as predicted by seminal qualitative theories concerning conflict (intergroup conflict theory, intergroup contact theory and the nature of prejudice). This will involve extensive simulation, staging the inclusion of complexity, implemented using supercomputing facilities[216]. Cross-checking with sociologists (Dstl) and psychologists (Yale, ARL) will support incremental model development.

Subtask 2 will extend validation of the modeling from Subtask 1 to real-world scenarios. Through real-world conflict data sets (e.g., SCAD), we will validate the extent to which agent based models based on social theory can be parameterized to align with the characteristics of real-world conflict escalation. This will allow us to determine the "tellability" of potential scenarios in terms of social and psychological theory.

Subtask 3 involves examining how coalition stakeholders, such as analysts, engage with modeling developed in Subtask 1, to support their decision-making. Through participant observation, user behavior in undertaking structured tasks and deriving knowledge will be studied. This will involve online and physical activities that are examined to determine design principles for user interaction with concepts, input and output. We will deploy the

---

[212] Galliers, J.R., 1988. A theoretical framework for computer models of cooperative dialogue, acknowledging multi-agent conflict (Doctoral dissertation, Open University).

[213] Vasconcelos, W.W., Kollingbaum, M.J. and Norman, T.J., 2009. Normative conflict resolution in multi-agent systems. Autonomous agents and multi-agent systems, 19(2), pp.124-152.

[214] Parizas, C., De Mel, G., Preece, A.D., Sensoy, M., Calo, S.B. and Pham, T., 2015, July. Interest-based negotiation for policy-regulated asset sharing. In International Workshop on Coordination, Organizations, Institutions, and Norms in Agent Systems (pp. 300-319). Springer International Publishing.

[215] Viswanathan, A., de Mel, G. and Hendler, J.A., 2015. Pragmatics and Discourse in Knowledge Graphs.

[216] Whitaker is Director of Supercomputing Wales, a £15M investment in research supercomputing facilities for Wales, UK.

software encapsulating the modeling from Task 1 to assess how analysts from different coalition countries (US and UK) engage with the final design, and to what extent value of information are similarly deduced.

Subtask 4 will validate the modeling from Subtask 1 to determine the effects of including human influence in game theoretic negotiation for policy. This will be predominantly simulation based, and benchmarked against alternative methodologies that exclude social and psychological influences on human decision-making. We will adopt scenarios that include mixed human-autonomous system collectives, and deduce the impact of including human influences in policy negotiation for groups.

Task 2: Understanding Group Behavior through Motifs

Primary Research Staff	Collaborators
Dave Braines, IBM UK	Gualtiero Colombo (PGR), Cardiff
Diane Felmlee, PSU	Stuart Allen, Cardiff
Don Towsley, UMass	Alun Preece, Cardiff
Liam Turner, Cardiff	Sue Toth, ARL
Roger Whitaker, Cardiff	Chris Dearlove, BAE Systems
Lauren Hudson (PGR), Cardiff	Gavin Pearson, Dstl
Jian Li (PGR), UMass	
Cassie McMillan (PGR), PSU	
Malgorzata Turalska (PDR), ARL	

In the coalition environment, problems related to hostile and extreme external group-behavior may frequently emerge, such as in asymmetric warfare, insurgency and post conflict peace-keeping. A common understanding of how and why groups behave in particular ways is fundamental for military intelligence, informing policy, resource deployment, and wider scenario modeling. However a persistent challenge concerns detecting and understanding the dynamics of partially visible groups. Group dynamics are governed by a group's internal network structure, concerning the connections (i.e., relationships) that allow a group to coordinate itself. Behavior, interactions and communication may only be visible between particular nodes in the network and at particular points in time, presenting a major obstacle for coherent modeling.

We plan to advance the state-of-the-art by exploring the use of motifs to understand the external networks facing coalition operations, where noise and obfuscation is present. Network motifs refer to recurring, significant patterns of interaction between sets of nodes[217],[218]. They represent the basic, building blocks of graphs. While an external network of interest may not be fully visible to the coalition, motifs represent important atomic sub-structures more likely to be visible, from which inferences can be made.

[217] Alon, Uri. 2007. Network Motifs: Theory and Experimental Approaches. *Nature* 3: 450-461.

[218] Shenn-Orr, S. S., Milo, R., Mangan, S. and Alon, U. 2002. Network Motifs in the transcriptional regulation network of *Escherichia coli*. *Nature Genetics* 31: 64-68.

In recent years, research on social networks (i.e., connecting people) has expanded dramatically[219]. Studies repeatedly establish the importance of social network characteristics for a wide range of interaction processes, such as those in close relationships (e.g., [220,221]), social organizations, science[222], communication, crime and deviance, social media, as well as in war and terrorist activity (e.g., [223,224]).

However, research seldom investigates network motifs within graphs that capture important human ties and interactions among these social networks. Additionally, most studies of motifs have focused on their presence in *static* graphs and little is known about how they change over time. Changes are potentially useful in coalition environments, as they imply changes within the overall (hidden) network.

This whitepaper focuses on the following questions:

1. Do motifs characterize different groups of interest to DAIS-ITA such as terrorist networks, different social networks, and communication ties? Do various coalition networks exhibit discrete patterns of motifs, or are they universal? What are good models for studying these networks?
2. How do motifs change over time in dynamic, mutable networks? Do different dynamic networks exhibit different temporal behavior? How should such behavior be modeled? One research goal is to introduce the concept of *temporal motif (T-motif)* and investigate its utility in addressing dynamic change in networks.
3. Can motifs be used to gain insight into inter-group behavior, such as cooperative alliances or escalating conflict between external groups? Does the presence of motifs within a group give insight into hidden structures and the mechanisms, such as the detection of hierarchies or informal coalescence, that drive in-group tension or cooperation?
4. Motifs appear in communication networks: do coalition networks exhibit similar subgraph structures? Are some subgraph structures better than others? Are motifs within constituent networks similar to those associated with the high-level network?
5. Last, answers to the above questions rely on the availability of high-quality network datasets thus raising the question, how do we account for missing or erroneous data (presence of a link when one does not exist)?

Technical approach

We outline three main research threads. The first focuses on *motifs in static networks*, the second on *motifs in dynamic networks*, the third on the role of motifs on *inter-group behavior*.

Motifs in networks consist of basic representations of small sets of vertices and edges in a graph. They identify local patterns of structural regularity that occur more often than would be expected in random graphs with the same number of edges.

---

[219] e.g. Felmlee, Diane and Colleen H. Sinclair. Forthcoming. Social Networks and Personal Relationships. In the *Cambridge Handbook of Personal Relationships*, 2nd Ed. edited by Anita Vangelisti and Daniel Perlman.

[220] Faris, Robert and Diane Felmlee. 2014. "Casualties of Social Combat: School Networks of Peer Victimization and Their Consequences. *American Sociological Review* 79: 228-57.

[221] Felmlee, Diane and Robert Faris. 2016. Toxic Ties: Networks of Friendship, Dating, and Cyber Victimization. *Social Psychology Quarterly* 79.

[222] Lungeanu, A. & Contractor, N. S. 2015. The effects of diversity and network ties on innovations: The emergence of a new scientific field. American Behavioral Scientist, 59(5), 548-564.

[223] Everton, Sean. 2012. *Disrupting Dark Networks. Cambridge University Press.*

[224] Krebs, Valdis E. 2002. "Mapping Networks of Terrorist Cells." *Connections* 24(3): 43-52.

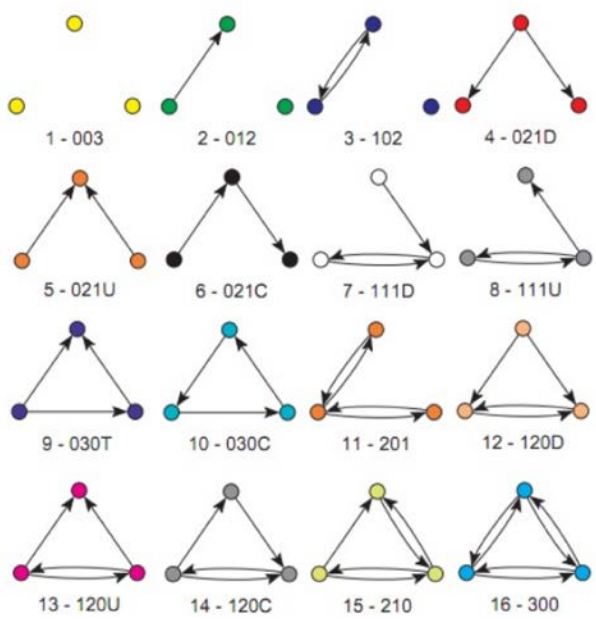

Figure P6-2. Examples of triadic motifs

Triads, or the (potential) ties connecting subsets of three actors, are considered to be the structural foundation of social networks[225,226]. Study of triads allows us to better understand a variety of network phenomena, including transitivity, the tendency for actor *i* to be tied to actor *k* if a tie exists between actor *i* and actor *j* and between actor *j* and actor *k*. Other motifs include in-/out-stars.

We address the research questions with the following subtasks:

Subtask 1: Comparisons of Metrics and Models of Multiple Social Networks. *Goal: to determine presence and role of motifs in coalition-relevant human social networks from analysis of data.*

Little research on network motifs considers in any depth human networks, focusing instead on biological or physical networks. The study of human networks represents a major, and crucial, gap in the literature that we intend to address.

The approach considered here will be useful in identifying key network fragments that we expect to find in specific types of external groups. Another strength of our approach to network research is that the identification of network motifs can be used to predict change over time in external groups. If we know that terrorist networks exhibit a tendency to be composed largely of triads that exhibit balance, or closure, for example, then we can expect the presence of imbalanced triads to be unstable, and to change over time.

We plan to examine network motifs/subgraphs, in social networks, and to undertake a comparison of differing genres of social interconnections. This includes the development of algorithms for computing prevalence of different motifs in random networks. We will identify the important motifs associated with different genres of social networks by comparing their prevalence to that of random networks with the same degree sequence[227]. In preliminary IPP work, we have begun to examine network motifs in several types of social networks, including those of multiple terrorist groups, email communication, friendship ties, twitter online messaging, travel routes, and advice ties. Initial results show that certain motifs appear to be universal in social networks. On the other hand, certain types of networks exhibit unique types of triadic motifs. In particular, aggressive, twitter communication

[225] Holland, P. and Leinhardt, S. 1975. Pp. 1-45 in *Sociological Methodology* (Ed). Heise, D.; Jossey-Bass: San Francisco.

[226] Wasserman, S. and Faust, K. 1994. *Social Network Analysis*. Cambridge University Press: New York.

[227] Milo, R., et al. 2002. Network Motifs: Simple Building Blocks of Complex Networks. Science 298: 824-827.

networks are composed of a higher proportion of imbalanced, stressful triads than predicted, unlike most other types of social networks.

The motif compositions of terrorist groups are more similar to those of friendship and positive alliance networks than to those of online communication or advice networks. These results suggest that interconnections among insurgents are similar to those of friendship. These initial findings provide support for the argument that the terrorist groups studied here developed out of deep ties, as compared to the argument that such groups represented connections among relatively isolated cells. However, it is possible that new, online recruitment methods used to develop certain insurgencies may produce network ties that are more disparately connected than those we observed. A task for future work would be to use simulations to compare the likely motifs arising under the conditions of online recruitment.

In future work we also intend to examine network data with the use of an exponential random graph model (ERGM)[228,229,230]. The ERGM enables testing of nodal, dyadic, and structural tendencies (e.g., [221]). Our goal is to examine the effects of key motifs, while controlling for other network properties in a multivariate framework.

So far we have only focused on social networks; we will also study motifs in communication networks, focusing on two aspects: 1) whether motifs are invariant across different coalition networks, and 2) how they compare with those in social networks.

Subtask 2: Dynamic Motifs in Dynamic Networks. *Goal: to develop tools to analyze motifs in a temporal setting and to develop new insights into the latent behaviors of dynamic networks.*

There has been little work on how motifs behave and change over time, with a few exceptions regarding the growth of subgraphs[231]. Nevertheless, an examination of motifs over time has the potential to substantially further our understanding regarding the dynamic mutability of human groups.

We will develop new robust algorithms to study how subgraphs change over time in a dynamic network. We will use these algorithms to characterize the temporal behavior of motifs and whether this behavior can be used to classify networks as well as to identify anomalous behavior. We will also attempt to extend the definition of motif to account for temporal changes with the goal of developing a definition for a "T-motifs". Another goal is to develop a notation and/or language to define the motifs and capture their structure, dynamicity and tempo, and subsequently use this to predict wider network structures based on limited local observations. Our ability to pursue these research directions require new representations of temporal motifs and new algorithms for studying their behavior. This is the focus of the research thread described here.

A dynamic network dataset consists of records that identify a contact between two individuals, either uni- or bi-directional, and a time stamp. This allows one to construct a sequence of directed (undirected) graphs summarizing the dataset. We will explore two different approaches for studying the temporal behavior of subgraphs/motifs in this setting. The first consists of performing a static motif analysis of each timestamp (as described previously) to create a motif summary of each snapshot. This could be the empirical subgraph distribution for each snapshot or its entropy as examples. This produces a new time series that can be analyzed using classical techniques.

The above approach does not account for changes in subgraphs associated with specific sets of nodes. The second approach will focus on summarizing changes in subgraphs associated with the same nodes. This poses several challenges, the foremost being how to summarize these changes. We will explore the use of edit distance, i.e., the number of (directed) edge deletions and additions needed to transform a subgraph in one snapshot to that in the next subgraph. This can be used to produce different time series related to different edit distance statistics.

---

[228] Hunter, David R., Mark S. Handcock, Carter T. Butts, Steven M. Goodreau, and Marina Morris. 2008. "Ergm: A Package to Fit, Stimulate, and Diagnose Exponential-Family Models for Networks." *Journal of Statistical Software* 24:1-29.

[229] Morris, Martina, Mark S. Hancock, and David R. Hunter. 2008. Specification of Exponential –Family Random Graph Models: Terms and Computational Aspects. Journal of Statistical Software 24: 1548-7660.

[230] Wasserman, Stanley and Philippa Pattison. 1996. "Logit Models and Logistic Regressions for Social Networks: An Introduction to Markov Graphs and p*." *Psychometrika* 61: 401-25.

[231] Paranjape, A. Benson, A.R. Leskovec, J. 2017. Motifs in Temporal Networks. WSDM'17.

Another way of capturing changes is by calculating a transition probability matrix describing how subgraphs change over time. Comparison of the stationary distribution of this Markov chain to the empirical subgraph distribution will shed light on the role of randomness over time.

The problem has several dimensions. For example, the time granularity of individual snapshots can affect results. Moreover, behavioral differences as a function of snapshot granularity can provide useful information. There is the challenge of large datasets involving thousands to tens of thousands of nodes. We will adapt our recent results[232,233] on sampling to analyze static graphs to the case of dynamic graphs. Last, we intend to explore different definitions of the novel concept of a temporal motif (T-motif) as part of this task. Last, datasets may be incomplete and/or replete with errors. We will model missing data as a consequence of a sampling process and extend our earlier work on sampling to handle it.

Subtask 3: Motifs and Emergence of Inter-group Behavior. *Goal: to determine the extent to which motifs predict behavioral and structural features within and between groups.*

During the IPP period we explored event driven models for the evolution of group behavior[234]. This modeling approach involves actions taken in response to a social dilemma, based on individual and group-derived strategies. The social dilemma tests the extent of positivity or negativity towards a third party in the presence of interaction opportunities with others.

Actions that individuals take, both internally towards their in-group, and the response to an out-group, are influential to growth, cohesion and behavioral characteristics of the group. Motifs can capture interaction behavior within and between groups as a temporal sequence of events between actors. This provides opportunities for new insights: a bridge between individual actions and collective mission of a group that fuels conflict.

From a biological perspective, recent work[235] highlights the importance of motifs in the evolution of cooperation. In the DAIS-ITA context of modeling group behavior, this can be significantly extended. Motifs can be tracked within the simulation of inter-group behavior to assess how a more diverse range of group behaviors, from cooperation and alliance, to hostility and warfare, emerges. Specifically we can use motifs to identify features that correlate with escalation and de-escalation of tension between groups in dynamic scenarios. Within groups, motifs are a basis for detecting potential mutation, such as breakaway sub-groups or opinion divergence. No framework exists for characterizing conditions that lead to internal division; motifs are ideal for supporting new insights into the substructures that lead to the escalation of divergence and tensions within groups. We will adopt an agent-based simulation, which provides a dynamic context to observe the emergence of motifs. We will compare findings from simulations with real-world social media data that has been a-priori collected from collaboration with P6 and the wider Cardiff Crime and Security Institute to identify whether the simulation findings relate to real online conflict situations. Additionally, we will explore offline conflict scenarios through open data provided by established ongoing projects (e.g. Social Conflict Analysis Database and Armed Conflict Location and Event Data Project). This analysis aims to increase the value of information at coalition disposal.

Application of motifs within groups offers an important new mechanism to discover in-group hierarchy and structure in the presence of noise and obfuscation. These characteristics are typical in social networks belonging to subversive external groups that operate with restricted visibility. Motifs represent events between individuals, and snapshots of information flow. The importance of individual actors is reflected through their roles in multiple motifs, from which prediction of overall network structure and hierarchy is possible. *Motif degree* will be defined and examined in this context. This supports the identification of agents of influence: critical nodes in the network with enhanced roles in dissemination and connectivity of the group. Motifs are potentially well suited to this because

---

[232] Wang, P. Lui, J.C.S. Towsley, D. Zhou, J. "Minfer: A Method of Inferring Motif Statistics From Sampled Edges," Proc. ICDE, May 2016.

[233] Wang, P. Qi, Y. Lui, J.C.S. Towsley, D. Zhao, J. Tao. J. "Inferring Higher-Order Structure Statistics of Large Networks from Sampled Edges," to appear in *IEEE Transactions on Knowledge and Data Engineering*.

[234] Whitaker, R.M, Turner, L.D., Colombo, G.B., Verma, D., Felmlee, D., & Pearson, G. (2017, August). Intra-group Tension Under Inter-group Conflict: A Generative Model Using Group Social Norms and Identity. In *Advances in Cross-Cultural Decision Making: Proceedings of the AHFE 2017 International Conference on Cross-Cultural Decision Making, July 17-21, 2017, The Westin Bonaventure Hotel, Los Angeles, California, USA* (Vol. 610, p. 167). Springer.

[235] Gianetto, D. A., & Heydari, B. (2016). Sparse cliques trump scale-free networks in coordination and competition. *Scientific reports*, 6.

they are not eliminated by partial network obfuscation. We will determine through simulation the extent to which detection of points of influence and structure is possible using motifs, in the presence of such obfuscation. Furthermore, another novel avenue for our research would be to examine directly the influence of motifs on motifs over time. In other words: Do motifs of type A give rise to motifs of type B some time later?

Validation and Experimentation

We will validate our work using several approaches, as described below.

1. **Analyses of data sets:** We will test our algorithms on a variety of datasets and use these datasets as a source of validation. We are gathering data from the following sources for our analyses, and obtaining longitudinal data whenever possible. Data sets include:
   - Terrorist network data sets [John Jay & ARTIS Transnational Terrorism Database (JJATT), 2009]. (http://doitapps.jjay.cuny.edu/jjatt/data.php]
   - Twitter Aggressive/Bullying data [Felmlee Twitter Cyber Aggression Data[236]]
   - Friendship network data sets [National Longitudinal Study of Adolescent Health[237]]
   - Networks of military intervention in disputes between nations (yearly) [Correlates of War Data sets (http://www.correlatesofwar.org/data-sets)]
   - Networks of alliances between nation states (yearly) [Correlates of War Data sets (http://www.correlatesofwar.org/data-sets)]
   - Networks of groups and actors involved in social or armed conflict [Social Conflict Analysis Database (SCAD) (https://www.strausscenter.org/scad.htmlhttps://www.strausscenter.org/o.html) and Armed Conflict Location and Event Data Project (ACLED) (https://www.acleddata.com/data/)]
   - Cosponsorship Network Data [US Legislature[238]]
   - Advice Networks [Law Firm Network[239]]
   - Travel networks [US Airport networks (https://openflights.org/data.html)]
   - DAIS-ITA networks[240]

2. **Simulations of Scenarios:** We will use simulations to emulate scenarios concerning the escalation of intergroup behavior, such as when cooperation is impeded by prejudice and hostility. We will also use simulation to develop test cases concerning the obfuscation of network structure. The python framework developed in the IPP is readily extensible and will support the detection of motifs using supercomputing facilities (Supercomputing Wales).
3. **Experimental Data**: We will test further our hypotheses using an experimental approach with the use of data from DAIS-ITA.

In addition, we will consult regularly with government colleagues regarding additional possible data sets of relevance to our research agenda.

Military and DAIS ITA Relevance

[236] Sterner, Glenn and Diane Felmlee. 2017. The Social Networks of Cyberbullying on Twitter. *International Journal of Technoethics* 8(2):1-15.

[237] Bearman, Peter, Jones, Jo, and J. Richard Urdy. 1997. The National Longitudinal Study of Adolescent Health: Research Design.

[238] Fowler, James H. 2006. "Connecting the Congress: A Study of Cosponsorship Networks" Political Analysis 14 (4): 456-487.

[239] Lazega, Emmanuel. 2001. *The Collegial Phenomenon: The Social Mechanisms of Cooperation among Peers in a Corporate Law Partnership*. Oxford University Press.

[240] e.g. as recorded in the CENSE environment and evident in the Science Library at http://sl.dais-ita.org/science-library - this will include the ability to have multiple time-series snapshots to show the evolution of key networks over time and it may be possible to include additional relevant data from NIS ITA and NS-CTA (with appropriate permissions) in order to increase the available volume and time period.

This project has fundamental military relevance. Understanding the dynamics of external groups in conflict, insurgency and peacekeeping situations is of value to coalition forces. In regards to the first task, there are numerous applications of this modeling in a military and DAIS-ITA context. For example, interventions for coalition peacekeeping operations in unstable regions and responses to asymmetric warfare can be informed by knowledge of inter-group dynamics. For the second task, the closed and subversive nature of such networks means that being able to build knowledge on a wider network from observation of sub-structures and interactions is highly valuable. Together this supports decision-making, for example allowing policies and interventions to be grounded by social and psychological theory. Achieving this in a coalition setting will help to build a shared understanding of a common threat, which enhances military intelligence.

Finally, we will consult regularly with our colleagues from the government to better situate our research so that it will address military needs more successfully. We will elicit specific coalition scenarios to which we can apply our work, for example.

Each task in the project also has specific points of relevance:

Task T6.1

The modeling approach and careful development of software design, supports an analyst in extracting maximum value of information, placing the human at the front and center in a rationale process for decision making. The HCI elements of the research (subtask 3) explore the model as a way for the analyst to organize their own thoughts and perceptions. In particular the modeling does not pre-suppose a “western lens” - groups of interest may not be of western origin and therefore can have a different drivers and responses. Modeling with different input parameters will help the analyst to maintain an objective view that can otherwise be potentially challenging to form.

Modeling will also provide deeper insights into alternative interventions, for example allowing analysts to observe second and third order effects, that are otherwise potentially obfuscated. Observing the social, cultural and behavioral elements of a group in this way will enable the provision of more efficient and effective operations. There are no “industry standard” models or software packages that support academically rigorous modeling of group behavior. Therefore the research has the potential to fulfill an important capability for coalitions, and has been specifically targeted to support the analyst. As the research progresses we will assess the opportunity to transition the research to a commercial or open source package.

We expect to undertake regular demonstration of the modeling capabilities, using boot camps, and Autumn Fall Meetings alongside conference and web dissemination, in which the investigators (Yale) are well experienced.

Task T6.2

A potential application of subgraph analysis is to understand the dynamics of tactical coalition networks. Certain subgraph structures are indicative of robust communications. The same work can also be used in a more defensive context: there may be differences between coalition partner networks, and such differences are important to understand in order to better coordinate coalition partner interaction. Last, various subgraph structures may be indicative of robust and healthy interconnections between disparate coalition subnetworks (enclaves). Alternatively, certain subgraph structures (e.g., imbalanced triads and/or 4-node ties) could point to the presence of inefficient, and potentially stressful and deleterious interconnections.

Particularly important scenarios where this is useful include:

- adversarial networks such as terrorist cells
- determining good structures for tactical military networks
- examining differences in coalition networks
- knowing how networks of networks can be organized.

The techniques and methods that emerge will support new capabilities that can be shared through open-source means. Milestones and deliverables reflect this.

Collaborations, Staff Rotations, and Linkages

Collaborations within and outside of the DAIS-ITA programme will be at the forefront of all project activities.

Task T6.1

Linkage and collaborations will be in three directions. Concerning P2, IBM-UK will form linkages (via de Mel), building on previous experiences and interactions concerning policy, discourse and agent-based modeling.

Real world scenario inclusion (T6.1, subtask 2) will explore real world data sets (open source) to better understand how the military influences and exploits their relationships with the local population. This will involve interaction with P4 to determine situational awareness, exploring how to best extract knowledge for noisy, partial and distributed data sources.

Linkage to T6.2 will be maintained through Whitaker and Turner (Cardiff). This will involve linking agent-based modeling of groups, and the role of reciprocation and interaction, with motif structures that represent such interactions.

Task T6.2

There are linkages to P1, P2 and T6.1 as follows. P1 is concerned with developing paradigms for interconnecting SDC enclaves and for controlling and managing these enclaves. This includes developing appropriate inter- and intra-enclave topologies. We will work with P1 personnel to apply our motif/subgraph analysis tools to the problem of designing good inter- and intra-enclave topologies.

Policies are inherently graphical in nature reflecting relationships among different entities, both organizations and individuals. We will work with P2 personnel to understand these structures and how our motif/subgraph analysis tools can be used to help in designing good and consistent policies, especially in joint coalition-driven decision situations.

As described above, there are links to T6.1 through the representation of the fraction and formation of groups being expressed as motifs. The agent-based methodology in T6.1 conveniently allows for interactions and reciprocation to be expressed through motifs.

There is also a linkage to the EDIN C2 task under NS-CTA, which is concerned with the analysis of time varying graphs. With Towsley being a participant in that NS-CTA task, we will take advantage of theories, algorithms, and tools that come out of that task to apply to motifs. Similarly, we expect that motif problems to be of interest to some of the participants in that NS-CTA task and to stimulate joint activities.

Staff Rotations

Each year there will be two rotations of graduate students or postdocs across the Atlantic, one from the UK to the US and the second from the US to the UK. In addition:

- In T6.1 meeting/visits or workshops will be convened to understand scope of sociological and psychological modeling for: group dynamics, analyst understanding and policy generation. Where appropriate these will be aligned with conferences or other events.
- In T6.2 Dave Braines will visit US partners once each year. The ARL collaborator will visit either UMass or Penn State once a year for a week.

This is in addition to task meetings that will take place during the AFMs and the bootcamps.

Research Milestones		
Due	**Task**	**Description**
Q1	**Task 1**	Mechanisms to model group motivations from individual behaviour (Yale (lead), Cardiff, ARL, Dstl); output: a conference submission
Q1	**Task 2**	Common principles and metrics for motif-based analysis of networks and groups (PSU (lead), Cardiff, UMass, IBM-UK, Dstl); output: a conference submission
Q2	**Task 1**	Definition of techniques and prototyping to enhance the value of information from conflict and related data sets (Cardiff (lead), ARL, Dstl, IBM-US); output: a conference submission
Q2	**Task 2**	Principles and metrics for dynamic groups; output – conference submission (PSU, UMass (joint lead), Cardiff, IBM UK, Dstl); output: a conference submission.
Q3	**Task 1**	Scope of policy decision-making in the context of groups, and preliminary comparisons of policy negotiation approaches IBM-UK (lead), Yale, Cardiff); output: a conference submission.
Q3	**Task 2**	Efficient algorithms for studying motifs in large dynamic networks (UMass (lead), all institutions); output: conference submission.
Q4	**Task 1**	Design principles for enhanced and objective analyst engagement with simulation software (IBM-US, Cardiff UK, Dstl, ARL); output: a conference submission.
Q4	**Task 2**	Approaches to detecting inter-group tension through motifs (Cardiff (lead), all institutions); output: conference submission
Q5	**Task 1**	In-depth assessment of "tellability" of real-world scenarios from social and psychological theory as a result of evolutionary agent-based modelling (Cardiff (lead), all institutions). Output: conference submission.
Q5	**Task 2**	Detecting points of group influence and network structure under obfuscation (Cardiff (lead), all institutions); conference/journal submission Extensions to dynamic network algorithms to handle missing data and errors (UMass lead), all institutions); output: conference or journal submission.
Q6	**Task 1**	Benchmarking the implications on policy making from inclusion of social and psychological theory in agent-based models to support negotiation (IBM-UK (lead)), Yale, Cardiff). Output: conference submission.
Q6	**Task 2**	Comparison of different classes of dynamic networks (PSU (lead), all institutions); output: conference submission
Q7	**Task 1**	Evaluation of design strategies to support analyst engagement and use of agent-based models to inform objective understanding and decision making for group scenarios in a coalition setting (IBM-US (lead), Cardiff, Yale, Dstl, ARL). Output: conference submission.
Q7	**Task 2**	Validation of motifs and *T*-motifs in assessing the escalation of conflict and mutation of groups (UMass (lead), all institutions)

Q8	**Task 1**	Analysis of agent based models to understand i) group motivations; ii) dynamics from social and psychological influences on human behaviour (Yale (lead), all institutions); output: conference or journal submissions. Deliverable: Research-grade software, models, tools and algorithms developed in Task 1
Q8	**Task 2**	Establishing overall value of information provided by motifs for coalition operations Deliverable: Research-grade software, models, tools and algorithms developed in Task 2