DAIS ITA

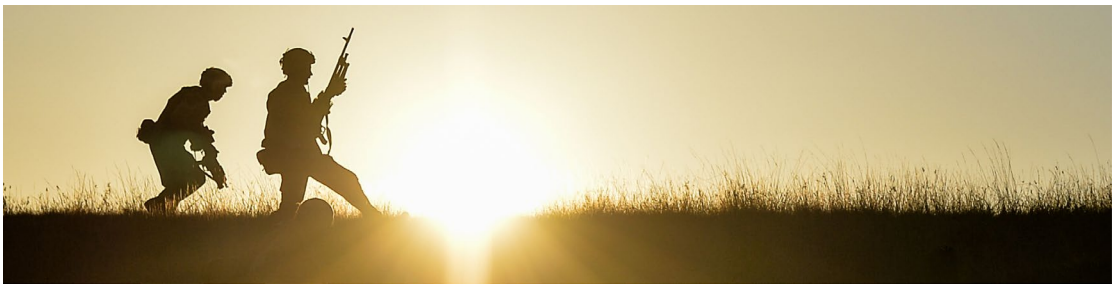
Distributed Analytics and Information Sciences International Technology Alliance

Final Report

September 2021

Written September 2021, updated April 2022

Agreement W911NF-16-3-0001



[dstl] The Science Inside

DEVCOM ARMY RESEARCH LABORATORY

Overview

This is the final report for the Distributed Analytics & Information Sciences (DAIS) International Technology Alliance (ITA) research program. DAIS ITA was an inter-disciplinary US/UK collaboration across government, academia and industry from 2016 to 2021.

The DAIS ITA has delivered world leading inter disciplinary scientific outputs, enabling generation after next information integration and exploitation, for distributed coalition multi-domain operations in dynamic and contested environments. It has developed the science underpinning the following future military capabilities:

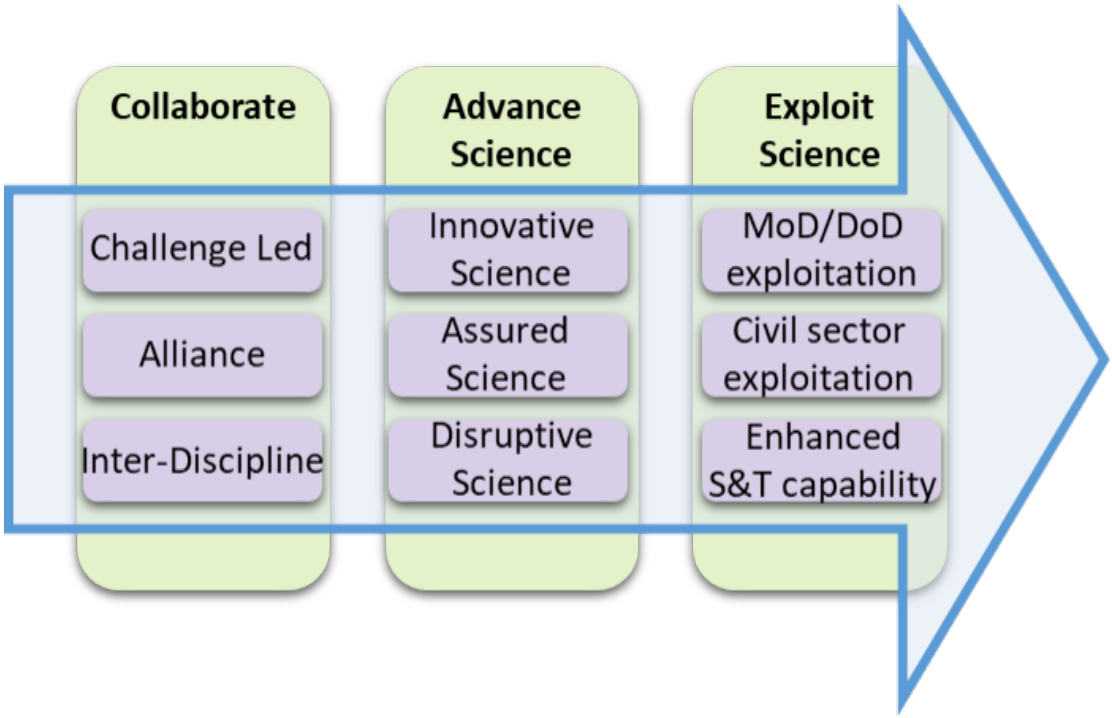
- Resilient Coalition Networks for Degraded, Intermittent and Latent (DIL) tactical networks including developing a new architecture called Software Defined Coalitions (SDC) for dynamic, agile and robust configuration, provisioning and sharing of information infrastructure assets among coalitions, and techniques for dynamic context-aware management of coalition networks.

- Artificial Intelligence (AI) in Contested Multi-Doman Coalition Operations including:

    - Adaptable AI able to rapidly adapt in dynamic situations and learn as the operation proceeds exploiting synergies between humans and machine intelligence;
    - Uncertainty-aware AI enabling human users to rapidly achieve an appropriate degree of trust in AI systems when making high-stakes decisions;
    - Distributed Coalition AI able to share data and models with partners whilst operating under a range of privacy constraints and in DIL communications environments;
    - Distributed Analytics enabling dynamic integration of coalition analytic and information services in (near) real-time in DIL communication environments.

- Integrating ad hoc Coalition Teams and Understanding Dynamic Audiences including (1) techniques to enable assessment of a dynamic information environment, and (2) computational social science for coalition cognitive co-ordination and the evolutionary basis of inter-group conflict.

DAIS ITA was a 5 year (2016-2021) collaborative partnership between the US and UK bringing together researchers from U.S. Army DEVCOM Army Research Laboratory (ARL) and UK Defence Science and Technology Laboratory (Dstl) to work alongside a consortium (led by IBM) of universities and industrial research laboratories in both the US and UK: involving ~70 faculty/research staff and funding a cohort of ~36 PhD students



It conducted basic research: its outputs include world-leading scientific publications (461 external publications since Sept 2016), open source code, low technology readiness level (TRL) demonstrators and trained researchers (PhDs). It has achieved significant gearing by publishing with 142 researchers from 86 non-DAIS organisations.

Several of these scientific outputs are already transitioning into higher Technology Readiness Level (TRL) civil and military funded development programmes and many more have the potential for transition.

DAIS ITA assured excellence by publishing results at highly selective international conferences (such as the Association for the Advancement of AI (AAAI) Conference on AI) and journals (such as Nature), as well as through an annual independent peer review by a joint US/UK panel of experts. The panel said:

“Overall, the DAIS-ITA is a challenging, well integrated, and well-managed program. The program addresses a wide range of coalition-relevant problems. The Peer Reviewers are mindful that this is not simple: The Program’s leadership has managed to keep the participants largely focused on militarily – and especially coalition – issues and problems, while keeping the technical level at basic research. This is a rare achievement: to pose (militarily) relevant issues, and thence to encourage the participants – academics, students and industry and laboratory scientists – to abstract these issues to basic research problems with high-value output that is welcomed at selective conferences and in prestigious journals. The Peer Reviewers stress that this, while not quite unique, is extremely rare amongst funded programs.”

In June 2021, the DAIS ITA was the recipient of a team award from the U.S. – UK Science and Technology Stocktake: a testament to the excellence of the scientific collaboration.

The DAIS ITA Legacy Site (https://dais-legacy.org/) contains a selection of key technical achievements as well as historical program documents including the Biennial Program Plan (BPP) documents, and annual reports. The legacy of the DAIS ITA comes in three main forms:

These showcase demonstrations and presentations of key DAIS ITA achievements

a) A list of publications that have arisen from the program (see our Science Library https://dais-legacy.org/science-library/)
b) Open source software available on github at https://github.com/dais-ita/
c) A set of final showcase demonstrations and presentations (available at https://dais-legacy.org/clusters/)

These showcase demonstrations and presentations of key DAIS ITA achievements have been designed around a closely linked set of three clusters:

- AI in Contested Multi-Doman Coalition Operations
- Resilient Coalition Networks
- Integrating Ad hoc Coalition Teams and Understanding Dynamic Audiences

The majority of report that follows will list and link to the showcase materials prepared to summarize key DAIS ITA achievements—presentations of research outputs and technology demonstrations. Before we proceed with such materials, we first offer a summary the DAIS ITA program's diverse and prolific publication record.

Summary of Publications

The data and statistics in this document cover the duration of the program and have been summarised from the publicly available DAIS ITA Science Library where a full list of DAIS ITA publications and most up to date statistics are available.

External Publications

Paper Type	2016	2017	2018	2019	2020	2021	2022	Total
Journal	0	7	18	31	20	15	**3**	**98**
Patent	0	0	0	1	5	0	**0**	**6**
External Conference	4	88	97	104	48	46	**3**	**236**
Total External	**4**	**95**	**115**	**136**	**73**	**65**	**6**	**494**

Other Publications

Paper Type	2016	2017	2018	2019	2020	2021	2022	Total
Internal Conference	0	50	44	62	77	0	0	**233**
Invited Talk	1	5	1	5	0	2	0	**14**
Book Chapter	0	2	1	2	0	1	0	**6**
Book	0	0	0	2	0	5	0	**7**
Demo	0	7	12	13	3	0	0	**35**
Technical Report	0	1	7	4	16	11	2	**41**
Poster	0	1	2	5	0	0	0	**8**
Total Internal	**1**	**66**	**67**	**93**	**96**	**19**	**2**	**344**

Total Publications

Paper Type	2016	2017	2018	2019	2020	2021	2022	Total
Total External	4	95	115	136	73	65	6	**494**
Total Internal	1	66	67	93	96	19	2	**344**
Total Program	**5**	**161**	**182**	**229**	**169**	**84**	**8**	**838**

Collaborative Behavior

Collaboration Type	Publication Count	Percentage
Single Institute	138	16%
Collaborative	681	81%
International	505	60%
Government	311	36%
Active DAIS Authors	**298**	

Clusters

AI in Contested Multi-Doman Coalition Operations

Military operations typically involve working with partners to resolve rapidly evolving situations where adversaries are adapting their tactics, techniques and procedures, and the behaviour of the civilian population is changing. Thus, there is a need for:

Adaptable AI

AI which can rapidly adapt in dynamic situations and learn as the operation proceeds exploiting synergies between humans and machine intelligence (inc. novel Neuro-Symbolic Learning (NSL) AI systems which combine reasoning and deep learning);

- Adversarial Domain Adaptation Learning for Accelerating Artificial Intelligence Based Military Solutions. Adjusting machine learning classifiers for new environments using limited training samples through generative adversarial networks (GANs)
- The FastLAS System for Interpretable Machine Learning. Logic-based AI that learns rules from examples.
- Adaptive Artificial Intelligence Systems for Human-Machine Federated Decision Making. Adapting neural layers using human provided or learned hard logic at the symbolic layer.
- Cogni-Sketch: Enabling Rapidly Formed Human-Agent Coalition Teams through Extensible Information Exchange. Software platform enabling human-agent interaction.
- Adapting Artificial Intelligence Systems to Recognise New Patterns of Distributed Activity. Improved human-AI teaming, AI learning (inc. NSL) and DAIS technology integration: running in real-time at edge.
- Advancing Artificial Intelligence with Neural-Symbolic Learning and its Application to Generative Policies in Distributed Coalition Operations. Adapting to changes between data used for training an AI and reality.
- Reinforcement Learning for Military Network Control. Efficient learning of complex decision spaces for real-time control of the network.
- State-Action Separable and Embedding for Reinforcement Learning. Taming complexity to enable learning of optimal network control policies.

- Characterizing New Devices on a Network with Zero-Shot Learning. Characterising previously unseen devices by inspection of their traffic.
- Online Multi-Task Learning with Long-Term Memory. Learning to recognize and adjust network analytics for different operating environments.
- Enhancing Situation Understanding through Negative-Ties Enhanced Pipelines. Improving AI analysis with user knowledge.

Trusted AI

Enable human users to rapidly achieve an appropriate degree of trust in AI systems when making high-stakes decisions;

- Achieving Rapid Trust of Adaptable Artificial Intelligence Systems. High level design and matching to user roles.
- Uncertainty-Aware Artificial Intelligence and Machine Learning. Revealing when the AI does not know in real-time at the edge.
- Real-Time Explainable Artificial Intelligence: Time-Series and Multi-Modal Data. Revealing what the AI is paying attention to in real-time at the edge.
- Testing the Reliability and Consistency of Explanation Metrics. New tests expose problems with saliency metrics.

Resilient AI

AI which is resilient to adversary attacks which seek to deceive the AI systems;

- Model Poisoning Attacks and Defences in Federated Learning. (aka Distributed Coalition AI). Defending against partner attacks.
- Efficient Attacks Using Side-channels. Defending against adversary use of AI explanations to develop attacks.
- Gradient Free Attacks on Multiple Modalities. Reducing the amount of data required, about a model, to launch a successful deception attack.

Distributed Coalition AI

AI systems able to share data and models with partners whilst operating under a range of privacy constraints and in degraded communications environments;

- Adaptive Federated Learning in Resource Constrained Edge Computing Systems. Sharing parameters, not data, and synchronising models with a minimal number of messages.
- Compressed Model Updates for Efficient Federated Learning. Minimising size of messages for shared learning and model synchronisation.
- One Shot Federation for Coalition Model Sharing. Incremental and intermittent shared learning using a representation of the data distribution (not the data itself).
- Coresets via Multipronged Data Reduction. Significantly reducing comms usage by summarisation of training data.
- Coresets Learning via Distributed Clustering and Local Gradients. Multi-dimension data summarisation (reducing comms usage) which also enables machine learning.

Integrated Distributed Analytics

Able to integrate analytic services in (near) real-time with partners in degraded communication environments;

- Vector Symbolic Architectures and Hyperdimensional Computing for Coalition Operations - An Overview. Dynamic decentralised discovery of assets (e.g. information services & data) and chaining them together (i.e. workflow construction and orchestration) to perform a task.
- Dynamic Communications Replanning using a Vector Symbolic Architecture. Demonstration of maintaining network connectivity via the vector symbolic architecture technology.
- Combining Vector Symbolic Architecture Aspects and Artificial Intelligence Services Using Edge Deployment. Feasibly integrating centralised control and distributed adaptability of coalition services in tactical environments.
- Semantic Vector Mapping for Coalition Operations. Achieving service interoperability without having to use an agreed set of terms to define the service.
- A Compositional Reinforcement Learning Framework for Workflow Generation. Learning how to construct coalition workflows with sparse rewards by leveraging the inherent hierarchical structure present in the application domain.

Edge AI

AI able to operate on the constrained computing environment at the edge of tactical networks;

- Edge AI Software Development Kit for Coalition Analytics. Enabling algorithm development, test and management.
- Model Pruning for Efficient Federated Learning in Coalitions. Modifying AI models so they can run on edge devices with minimal loss in performance.
- Energy Efficient Vector Symbolic Architectures (VSA) using 'In Memory' Hyperdimensonal Computing. Significant energy saving using novel 'in memory' computing hardware.
- Energy Efficient Vector Symbolic Architecture Using Spiking Neural Networks. Potential of sparse VSA to enable significant energy saving using novel SNN computing hardware.
- Leveraging Binarised Neural Networks for SDC Control. Using binary representations of model weights to allow Machine Learning models on mobile hand-held devices.

Resilient Coalition Networks

To support distributed analytics tasks, coalitions require a robust tactical network infrastructure. With connectivity likely to be Degraded, Intermittent and Latent (DIL), networks need to be agile to changing coalition situations, easy and rapid to configure and resilient to failures. The network also needs to enable effective and flexible sharing of partners' information and resources such as local services and data-stores, edge devices such as hand-held radios and sensors. Policies defining the behaviour of the network need to be able to adapt autonomously as the tactical situation unfolds (partners, missions and adversary action). Finally, the placement of data and services across the network needs to be optimised both for efficiency and contingency in case of network failure or fragmentation.

This cluster of Key Outcomes has therefore been subdivided as follows:

Control and Architecture of Software Defined Coalitions

A novel network control architecture which enables management of multiple coalition enclaves, flexible resource sharing and rapid adaptation in the case of fragmentation:

- Enhancing Coalition Networking using Software Defined Coalitions – An Overview. Extending Software Defined Networking to create a new concept achieving robustness and agility in multi-domain coalition networks.
- Control Plane Architecture of Software Defined Coalitions. To facilitate controller discovery, network reconfiguration and recovery from fragmentation.
- Software Defined Coalitions Controller Synchronization. Development of mechanisms and policies to optimise the rapid creation of slices of shared resource for specific coalition tasks.
- Robust Network and Learning Architectures for Software Defined Coalitions. Network robustness through a hybrid SDC/MANET architecture which uses ML to predict fragmentations.
- Reinforcement Learning for Military Network Control. Efficient learning of complex decision spaces for real-time control of the network.
- State-Action Separable and Embedding for Reinforcement Learning. Taming complexity to enable learning of optimal network control policies.

- Joint Reinforcement and Transfer Learning for Distributed Service Configuration in Fragmented Software Defined Coalitions. Enhancing SDC robustness by using ML techniques to speed up the network's recovery following reconnection of fragmented domains.

- Graph Attention Networks for Congestion and Mobility Prediction. Techniques to avoid retraining Machine Learning models when network topologies change.

- Leveraging Binarised Neural Networks for SDC Control. Using binary representations of model weights to allow ML models on mobile hand-held devices to make lightweight inferences even when disconnected from the domain controller. The concept is extended for the training of the models using federated learning.

- Resource Sharing in Software Defined Coalitions to Support Coalition Missions. A comparison of game-theoretic approaches for optimising resource sharing between coalition partners having different objectives.

- Game Theoretic Resource Allocation in a Coalition. A short demonstration of the resource allocation technique developed to realize SDC resource sharing.

- Online Resource Allocation Using Distributed Bidding Approaches. A comparison of a variety of auction-style approaches for allocating edge tasks to a central server.

Policy based adaptive network management

A policy based management system which can learn partner policies and adapt the behaviour of the infrastructure accordingly.

- Policy Generation for Edge Devices in Coalitions. Allowing autonomous edge devices to learn how to operate in new and uncertain environmental contexts. The edge devices learn from other devices using local observations.

- Advancing Artificial Intelligence with Neural-Symbolic Learning and its Application to Generative Policies in Distributed Coalition Operations. Allowing systems to perform edge of network policy learning for a range of tactical applications such as the management of networks, logistics and sensors.

- Answer Set Grammar for Efficient Generation of Policies in Coalition Environments. Allowing systems to autonomously adapt their operating policies to maximise their effectiveness and minimise risk.

Rapid characterization of coalition network infrastructure

Adaptive placement of services and data so that they are available at the right place and time;

- Data Plane-based Technique for Network Topology Inference. Supporting service placement through inference of the state of a target network across coalition boundaries without requiring direct control plane access.
- Dynamic Placement of Distributed Analytics Services. Techniques to support agile placement of analytics services to edge devices as opposed to being hosted centrally.
- A Security-Constrained Reinforcement Learning Framework for Software Defined Networks. Development of a RL framework which uses IDS data to optimise network metrics of interest such as throughput while at the same time developing policies to prevent malicious data propagating into the network.

Integrating Ad hoc Coalition Teams and Understanding Dynamic Audiences

Coalition operations occur in a complex and highly dynamic socio-technical information environment. Thus, there is a need to:

Achieve rapid cognitive co-ordination amongst ad hoc Combined, Joint, Interagency, Intergovernmental and Multinational (CJIIM) Coalitions and CJIIM teams

- Efficient Collective Problem Solving: Designing effective problem solving teams using agent-based modelling.

Understand the interplay between groups and individuals and thus the potential of interventions to influence behaviour

- Modelling the Emergent Behaviour of Human Social Groups. Agent-based modelling of way in which group and individual psychological behaviours interact, give rise to effects such as prejudice and devotion to a cause, and the emergence of opposed groups.
- Effect of Organizational Structure on Cultural Influence. Modelling spread of cultural features within an organisation.
- Winning hearts and minds: Maximizing influence in social networks. Mathematics of optimal solutions under different conditions.
- Dynamic Patterns of Terrorist Networks. Changes in network behaviour in build-up to an attack.

Rapidly assess dynamically evolving behaviour of audiences in response to unfolding events, competing narratives and disinformation

- Understanding Social Networks from the Local Behaviours within the Network. Enabling analysis when only have visibility of part of network and without processing language.
- Identifying Patterns and Signatures of Negative Behaviours in Networks. Detecting the inception of negative behaviours and their network effects.
- Predicting Spread of Negative Attitudes and Behaviors in Social Networks. Graph-based methods offer improved prediction over traditional statistical approaches.
- Enhancing Situation Understanding through Negative-Ties Enhanced Pipelines. Improving AI analysis with user-knowledge.

Key Achievements

A Compositional Reinforcement Learning Framework for Workflow Generation

Military / Coalition Issue

Dynamic management of large, distributed coalition systems for tactical use is critically important to mission success. The internal structure and topology of these systems—and the performance and resource availability of individual microservices—can change frequently, so workflows designed to achieve specific tasks need to adjust accordingly. Reinforcement Learning (RL) can be used to plan workflows in highly dynamic systems with a minimal amount of labelled data. However, these microservice systems are often highly sparse in terms of useful actions, and the workflows that require discovery can be highly complex, causing standard RL algorithms to struggle.

Core idea and key achievements

Standard machine learning (ML) techniques can be used to model complex systems and structures given a sufficiently large dataset for training. However, collecting labelled data at a sufficient scale is highly time and resource consuming, and in dynamic systems, where the underlying structure of the data can change over time, classical ML can struggle to adapt. Reinforcement Learning (RL) techniques do not require labelled data and are designed to interact directly with environments, so can adapt over time. However, standard RL can struggle significantly with multi-task scenarios, where multiple goals need to be learned by the same agent. Multi-task RL (MTRL) is a new sub-field that seeks to address this, by producing algorithms that aim to learn multiple skills more efficiently than learning each skill using a separate agent. Most MTRL algorithms fail to harness the inherent hierarchical structure present in many domains, where some goals can be broken down into smaller sets of skills. Our MTRL algorithm takes advantage of this underlying structure to increase the efficiency of learning and produce vector representations of possible workflows in parallel with learning. Our MTRL algorithm has the following characteristics:

Learns in sparse reward environments (only a small set of possible workflows are useful).

Learns a compositional structure of workflows within an environment, allowing for planning and execution of extended workflows.

Produces vector representations of workflows, which can be used for analysis and interpretability down-the-line.

Implications for Defence

The direct military relevance of this demo is to learn goal-oriented workflows of distributed coalition microservices to facilitate self-organization and coordination for service discovery, selection, planning, and execution. Wider applications of the underlying multi-task reinforcement learning algorithms could include robotics and AI-driven military simulations for modelling tactics and strategy.

Readiness & alternative Defence uses

Technological readiness level: 2-3. Pseudocode for the algorithm is described in a paper currently under review and is available as source code.

Resources and references

D'Arcy, Millar, et al. "Reinforcement Learning using Compositional Plan Vectors and Trajectory Experience Replay"

https://pypi.org/project/gym-craftingworld/

https://gym-craftingworld.readthedocs.io/en/latest/

Organisations

Cardiff University, IBM UK

A Security-Constrained Reinforcement Learning Framework for Software Defined Networks

Military / Coalition Issue

For military coalitions It is critical that coalition partners ensure that networking is managed in a security-aware manner to prevent attacks from undermining resilience, while at the same time ensuring that communication flows are timely delivered.

Core idea and key achievements

The use of machine learning (ML) techniques in the control plane of software defined networks (SDNs) provides enhanced approaches to traffic engineering, such as maximizing quality of service (QoS). Generally, QoS is determined by the interplay within various network functionalities such as rate control, routing, load balancing, and resource management. This interplay can become very complex. The benefit of ML techniques is that they can model complexity given sufficient representative data to train upon. However, the diversity and scale of current networks together with the diversity of traffic behavior hinder the task of gathering data that captures enough sets of behaviors for training. This poses a challenge to classical ML. Reinforcement Learning (RL), on the other hand, relies on learning optimal policies online based on system state using a model-free approach. These policies are more likely to transfer over to a new environment, and these characteristics make them more suitable for network control. RL based frameworks have thus already been proposed for specific functions within networks, such as for controlling routing, traffic rate control and load balancing. Current uses of RL for network control focus on optimizing a single functionality, which makes these existing solutions difficult to deploy in real networks. This is particularly problematic for security. For example, learning a policy which maximizes the throughput of the network (functionality 1: optimal rate control for QoS) can unknowingly facilitate the propagation of a high throughput Denial of Service (DoS) attack. To address such shortcomings, we have developed a framework, Jarvis-SDN, to extends current reinforcement learning (RL) techniques with security-constraints.

In Jarvis-SDN, the RL agent learns ‘intelligent policies’ which maximize functionality but not at the cost of security. The goal is making sure that RL-agent does not allow malicious-looking or suspicious flows to propagate into the network at the same rate as benign flows.

The security policies for constraining explorations in are learnt in a semi-supervised manner in the form of ‘partial attack signatures’ from packet captures of IDS datasets that are then encoded in the objective function of the RL based optimization framework. These signatures are learnt using a Deep Q-Network (DQN).

Our analysis shows that DQN based attack signatures perform better than classical machine learning techniques, like decision trees, random forests and deep neural networks (DNN), for common attacks.

Implications for Defence

Our approach will allow to optimize network metrics of interest while at the same time ensuring security.

Readiness & alternative Defence uses

Provides a conceptual framework for the use of RL techniques for security of SDN. One instantiation has been implemented for an SDN controller with the goal of intelligent rate control with protection from DoS attacks.

Resources and references

Key papers: Mudgerikar, Anand, Elisa Bertino, Jorge Lobo, and Dinesh Verma. "A Security-Constrained Reinforcement Learning Framework for Software Defined Networks."

Organisations

Purdue, IBM US, Imperial

Achieving Rapid Trust of Adaptable Artificial Intelligence Systems

Military / Coalition Issue

Military operations typically involve working with partners to resolve rapidly evolving situations where adversaries are adapting their tactics, techniques and procedures, and the behaviour of the civilian population is changing. Thus, military AI systems will need to learn as operations proceed and users will be exposed to partners AI systems. Thus users must be able to rapidly understand the capabilities and limitations of such AI system when making high-stakes decisions.

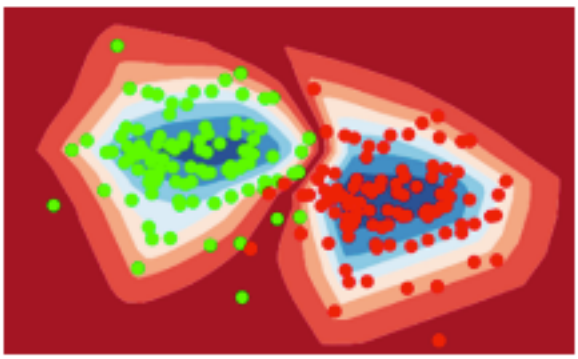
Core idea and key achievements

Rapidly achieving appropriate trust can be achieved by designing AI systems to be:

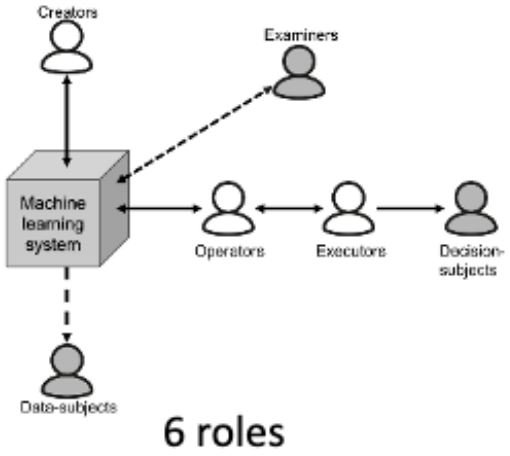
• interpretable, revealing to the user what they know;

• uncertainty-aware, revealing to the user what they do not know.

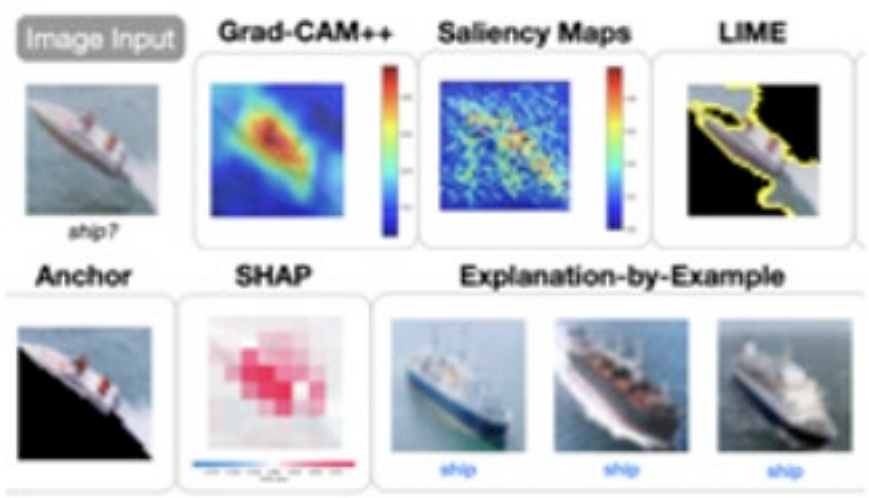
The interpretability of AI systems is a well-recognised problem; this research has highlighted the importance of uncertainty-aware AI systems (particularly for military operations), and how these two interact. Further, such trust calibration must be appropriate to the role of the user. The research has enumerated 6 roles covering the spectrum of use cases (within literature on interpretable AI) and provided 6 scenarios which demonstrate how these roles interact with an AI system (including how the role influences the interpretability required).



Uncertainty-aware AI



The research also examined end-user explanation preferences and found that explanation-by-example was preferred in image, audio and sensory modalities, whereas LIME was preferred for text classification.



Implications for Defence

These techniques will allow users to quickly obtain a sufficiently accurate mental model of the AI system, allowing them to understand when and when not to trust its outputs. Supports the safe use of AI systems by formalising the design, implementation and testing of trust in AI. Enables Defence to adopt AI systems which learn and adapt at the 'pace of the fight' – necessary to ensure the users' tempo of understanding and action is not overmatched by their adversaries.

Readiness & alternative Defence uses

Provides the high level design requirements and a framework for the design, implementation and testing of military AI systems. Presented at UK Defence's AI Fest 3 and concepts embraced by AI

research & development community. The entries on ‘Uncertainty-aware AI’ and ‘Adapting AI systems to recognise new patterns of distributed activity’ provide further details.

Resources and references

Key papers:

Rapid Trust Calibration through Interpretable and Uncertainty-Aware AI

Interpretable to whom? A Role-based Model for Analyzing Interpretable Machine Learning Systems

NeurIPS, 2020: How Can I Explain This To You? An Empirical Study of Deep Neural Network Explanation Methods

Organisations

IBM UK, IBM US, Cardiff University, UCLA, Dstl, ARL

Adapting Artificial Intelligence Systems To Recognise New Patterns Of Distributed Activity

Military / Coalition Issue

Military operations typically involve working with partners to resolve rapidly evolving situations where adversaries are adapting their tactics, techniques and procedures, and the behaviour of the civilian population is changing. Thus, military information processing systems need to be able to recognise significant patterns of activity which are distributed in time and space in near real-time, without generating too many false alarms.

Core Idea and Key Achievements

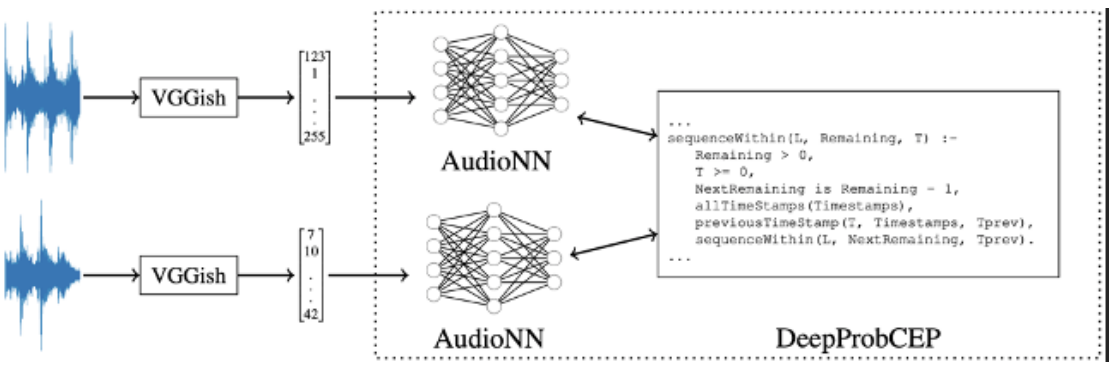
In the language of information processing, this requires the ability to recognise the relationship between a set of individual events. Deep learning Artificial Intelligence (AI) systems are constantly improving their ability to recognise such individual events. We have developed techniques which enable:

• Humans to inject new knowledge, or hypotheses, about patterns of activity through addition of new rules (which means patterns can be recognised in situations where there is insufficient time or data to train a deep learning model);

• Significantly-reduced need for training data (especially important when examples of the patterns-of-interest are relatively rare), faster AI model training, and improved detection accuracy over 'pure' deep learning approaches.(1)

Further we have demonstrated that such architectures are loosely coupled (so suitable for open architectures) and the resulting applications can run on edge of network devices (so are suitable for tactical sensor systems).

(1) In trials our techniques trained the best-performing model 3-4 times faster and with up to 100 times reduction in annotated training data required.



An example AI system configuration with deep learning-based services (VGGish & AudioNN) and then by a probabilistic logic program (DeepProbCEP) with learned probabilities.

Implications for Defence

Enables Defence to process in near-real time streaming data from a future Internet of Battlefield Things (including network, CEMA (cyber electromagnetic activities), ISTAR (intelligence, surveillance, target acquisition, and reconnaissance) and HUMS (health and usage monitoring systems) data). Enables Defence to adopt AI systems which learn and adapt at the 'pace of the fight' – necessary to ensure our tempo of understanding and action is not overmatched by our adversaries.

Readiness and Alternative Defence Uses

This work is technology readiness level (TRL) 3/4. The individual components are available as open source software – DeepCEP and LiveEvents. While the approach has been demonstrated on video and audio data, it is applicable in general to other time-series data (e.g. electro-magnetic spectra and cyber traffic).

Resources and References

- Vilamala, M. R., et al. "A hybrid neuro-symbolic approach for complex event processing in noisy and adversarial settings." Proc 36th International Conference on Logic Programming. 2020.
- Xing, Tianwei, et al. "Neuroplex: learning to detect complex events in sensor networks through knowledge injection." Proceedings of the 18th Conference on Embedded Networked Sensor Systems. 2020.

Organisations

Cardiff University, UCLA, ARL

Adaptive Artificial Intelligence Systems for Human-Machine Federated Decision Making

Military / Coalition Issue

Military operations typically involve multiple parties and a variety of devices that collaboratively adapt and respond to rapidly evolving situations. To achieve operational goals faster and with better outcomes military information processing systems must be able to support human-machine federated decision making, that use and share insights learned from (local) data by partners, adapt them to contextual changes, and integrate prior human knowledge.

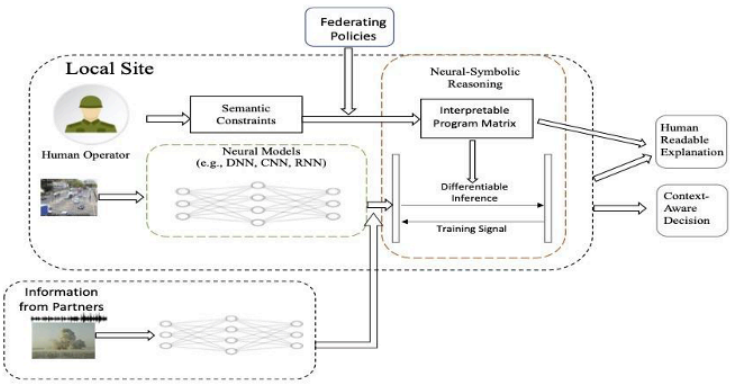
Core idea and key achievements

Limited availability of data (due to changing contexts) can be compensated by domain-specific semantics and constraints. Pure Deep Learning (DL) methods are effective in extracting insights from raw data (e.g. sensors) but require large quantities of data with distributions similar to that used during training. We have developed techniques for injecting semantics and constraints into Deep Learning AI systems to allow data-efficient domain adaptation of predictive models and coherent federated inference for decision making. Specifically, our techniques enable:

● representation of semantic constraints and human knowledge in an interpretable program matrix form, and exact symbolic inference to be performed in a pure differentiable way.

● end-to-end integration of differentiable inference with DL-based systems to control and guide their adaptation, during the learning process, to new shared data, boost their predicted accuracy in the presence of limited data, and provide explanations to predicted inference from data.

Our techniques are able to learn predictive models from heterogeneous data in a more accurate and data efficient manner than pure DL methods taking into account partial information, and spatial and temporal constraints.



Implications for Defence

Military operators will be able to enhance DL-based systems using expert domain knowledge and inject constraints for federating models from different parties. Existing DL models can be adapted quickly to changing conditions (e.g. different environments, changes in weather, lighting condition), than a pure DL method. Our system can generate explanations to help decision makers understand its output and increase trust in AI models.

Readiness & alternative Defence uses

TRL 3/4. The system will be made available as open source software. While the approach has been tested on images and structured data, it is applicable in general to other time-series data (e.g. video, network traffic data).

Resources and references

Aspis, Yaniv, et al. "Stable and supported semantics in continuous vector spaces." Proceedings of the International Conference on Principles of Knowledge Representation and Reasoning. Vol. 17. No. 1. 2020.

Organisations

Imperial College London, IBM UK.

Adaptive Federated Learning in Resource Constrained Edge Computing Systems

Military / Coalition Issue

Military data available at dispersed locations is confidential and even coalition partners are reluctant to share. Tactical networks that support analytics services for military operations have limited resources and can change dynamically over time. A key challenge is how to train analytics models using all distributed data at the network edge subject to the bandwidth limitation and data-privacy constraints for coalition partners.

Core idea and key achievements

We have enhanced federated learning (FL) to train analytic models where the private data remains local on the network-edge nodes and only model parameters are shared between different nodes. The new method includes local model updates at the edge nodes and global parameter aggregations by a central server. The technique aims to coordinate these different FL operations to achieve the most efficient model training subject to the limited availability of resources.

To devise the new method, we first derived a fundamental performance bound of FL, which captures the FL performance expressed as a function of different system parameters and settings (such as communication and computation resource availabilities and network topologies). Using the theoretical bound, we developed a control algorithm that adapts the internal steps of FL to best utilize the available resources.

The control algorithm derived from our theoretical analysis determines the best trade-off between local update and global aggregation operations for FL under a given resource budget. Through extensive evaluation by experiments and use of practical datasets, both on a networked prototype system and in a larger-scale simulated environment, we have shown that the proposed approach performs very close to the optimum for various machine-learning models and different data distributions.

Implications for Defence

This technology enables distributed training or adaptation of analytics models in resource-constrained environments, to allow coalition partners to help each other learn similar tasks without a need of sharing their sensitive data for privacy or lack of communication resources. The new approach provides the cutting-edge capability over our adversaries.

Readiness & alternative Defence uses

A set of algorithms are described in published papers and many of them are also available as open source code.

Resources and references

Key papers/patents include:

Wang, Shiqiang, et al. "When edge meets learning: Adaptive control for resource-constrained distributed machine learning." IEEE INFOCOM 2018-IEEE Conference on Computer Communications. IEEE, 2018.

Wang, Shiqiang, et al. "Adaptive federated learning in resource constrained edge computing systems." IEEE Journal on Selected Areas in Communications 37.6 (2019): 1205-1221 which won the IEEE ComSoc Leonard G. Abraham Prize (2021)

Patent US20190318268A1: Distributed machine learning at edge nodes

Open source code: https://github.com/IBM/adaptive-federated-learning

Organisations

IBM US, Imperial, PSU, ARL

Addressing for Intelligent Routing in Mobile Military Networks

Military / Coalition Issue

In military networks, which are operating in increasingly congested and contested settings, it is vital to prioritise and control traffic both at the network and application layers. Further, the current use of IP addresses ties the source and destination of a packet to locations within the network, and thus highly mobile military networks suffer from needing to re-route and re-address network elements.

Core idea and key achievements

DAIS ITA research has shown how vector based approaches can be used to reconfigure battlespace communication plans, and to enable service discovery and orchestration in tactical coalitions information systems.

The core idea is that a vector-based approach can also be used to represent both source and target identities (replacing IP addresses). This allows us to specify the source and target of a packet to include attributes such as Role, Type, Status (by no means an exhaustive list):

Thus, a battlefield order could be tagged with source “Mission Commander | Orders | Manual | One-off” and target “Soldier | Platoon 1 | Chat” to be issued to all of the soldiers in platoon 1 in their chat application. The message would then be routed using intelligent routers with knowledge of the state of the network. It would replace both unicast and multicast traffic. To improve the performance on the wire, hardware architectures, such as phase-change-memory, in the router could be employed to act on the packets at “wire-speed”.

Implications for Defence

Applying these techniques would create a new level of resilience and flexibility in tactical networks to allow them to adapt to battlefield conditions, including electronic attacks. It would allow the battlespace network to prioritise traffic such as individual messages and order, and if the network is too congested to adopt delay-tolerant approaches for lower priority traffic (e.g. use store-and-forward messaging).

Readiness & alternative Defence uses

The core idea is currently technology readyiness level (TRL) 1, but most of the related technology is at TRL2+, so enabling rapid development and demonstration of the concept.
An issue that would need to be addressed is the confidentiality of addresses. They could be represented using random binary vectors, but these could conceivably be learned over time. One option is to investigate the impact of use either encryption or dynamic vector space mapping to thwart such an attack and to determine the performance implications of these approaches

Resources and references

Simpkin, Christopher, et al. "A scalable vector symbolic architecture approach for decentralized workflows." COLLA (2018).

Simpkin, Chris, et al. "Constructing distributed time-critical applications using cognitive enabled services." Future Generation Computer Systems 100 (2019): 70-85.

Simpkin, Chris, et al. "Efficient orchestration of node-red iot workflows using a vector symbolic architecture." Future Generation Computer Systems 111 (2020): 117-131.

The underlying vector symbolic architecture code has been published as Open Source.

Organisations

IBM UK, Cardiff University

Advancing Artificial Intelligence with Neural-Symbolic Learning and its Application to Generative Policies in Distributed Coalition Operations

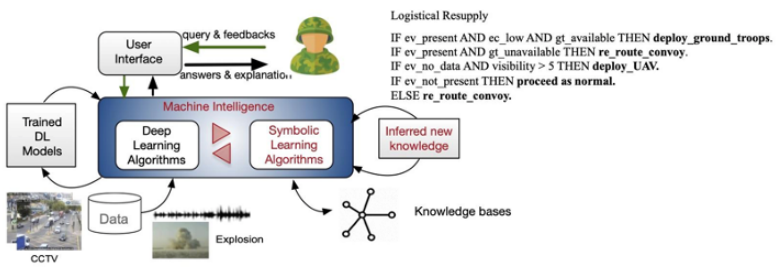
Military / Coalition Issue

Coalition operations may require rapid reconfiguration for a given task. Devices, systems and services (hardware and software) owned by different coalition partners will be required to integrate and operate seamlessly as a unified system. Furthermore, there is a lack of communication to back-end compute infrastructure, malicious adversaries present, and there is a requirement for human-machine interaction to support troops and deployed personnel. The coalition environment adds an additional challenge of trust, where parties within the coalition may not fully trust one another.

Core Idea and Key Achievements

This demonstration presents a policy learning framework which enables devices to be rapidly brought online into a mission environment. Devices can autonomously learn their behaviour, called policies, through local communication to nearby devices. Policies can be learned from a small number of examples and are explainable to humans. The demonstration includes the Answer Set Grammar Generative Policy Model which enables autonomous behaviour through the generation of policies in varying operational contexts, where the generative model is learned from policy examples. The demonstration also includes the Neural-Symbolic Generative Policy Model, which extends the framework to learn from unstructured data present in a military environment (e.g. imagery, video, audio, sensor data). The Neural-Symbolic extension is robust to distributional shift in input data during learning, reducing the likelihood of an adversarial attack.

Specifically, we have integrated FastLAS into a neural-symbolic architecture, called NSL, that extracts symbolic features from heterogeneous contextual data, by means of pre-trained Deep Learning (DL) systems, and uses these features to learn context-aware optimal patterns of behaviour. We have demonstrated that the learned models are highly accurate, even when the DL predictions are highly uncertain, are interpretable, require 3-4 orders of magnitude less training data, and are 3-4 times faster than pure DL approaches.



Implications for Defence

Both FastLAS and NSL systems are loosely coupled (they can integrate multiple Artifical Intellegence (AI) systems for feature extraction from unstructured data, and different symbolic learning solvers), and require limited computational power. As a result, these systems can perform 'edge of network' learning for a range of tactical applications (e.g. network management, logistics, sensing).

Enables Defence to learn and adapt, in near-real time, patterns of behaviour from streaming data (including network, ISTAR (intelligence, surveillance, target acquisition, and reconnaissance) and HUMS (health and usage monitoring systems) data). Enables Defence to outperform enemy forces by adopting AI systems capable of autonomously learning new AI services that efficiently process information quicker and more intelligently at the 'pace of the fight'.

Readiness and Alternative Defence Uses **links need updating**

This work is a technology readiness level (TRL) 4. FastLAS and NSL are available as open source software. While the approach has been demonstrated on images and structured data, it is applicable in general to other time-series data (e.g. network traffic, access control policies, decision-making strategic policies).

Resources and References

Law, Mark, et al. "Representing and learning grammars in answer set programming." Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 33. No. 01. 2019.

Law, Mark, et al. "Fastlas: scalable inductive logic programming incorporating domain-specific optimisation criteria." Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 34. No. 03. 2020.

Cunnington, Daniel, Alessandra Russo, Mark Law, Jorge Lobo, and Lance Kaplan. "NSL: Hybrid Interpretable Learning From Noisy Raw Data." arXiv preprint arXiv:2012.05023 (2020).

Organisations

Imperial College London, IBM UK, Purdue University, ARL.

Adversarial Domain Adaptation Learning for Accelerating Artificial Intelligence Based Military Solutions

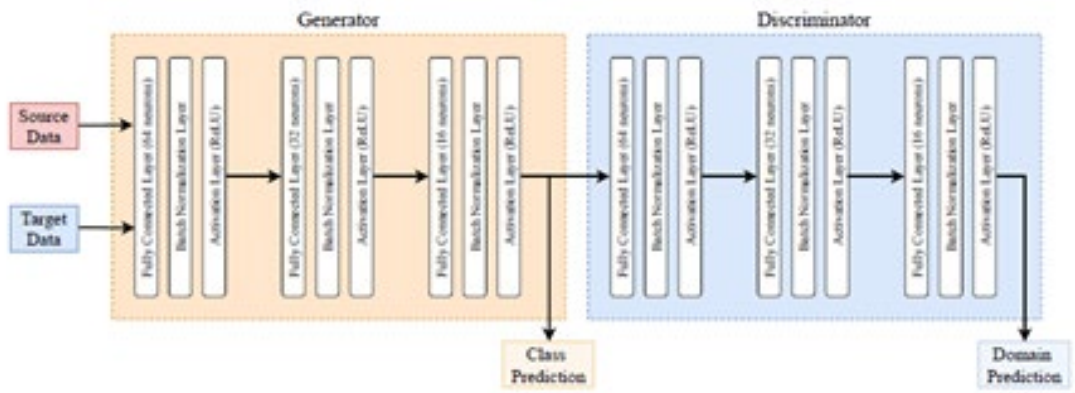
Military / Coalition Issue

Training deep learning (DL) models requires large amounts of labeled data. Collecting and labeling data is often time consuming, and thus unfeasible in applications with time constraints.

Core idea and Key Achievements

Our approach takes advantage of knowledge sharing in coalitions. We propose the use of Domain Adaptation (DA) to reduce the amount of labeled data required for training a DL models. DA is a transfer learning technique that allows one to transfer knowledge from a source domain with adequate training data, to a different but similar target domain with minimal or no new training data. We use a specific form of DA, referred to as adversarial DA, that GANs for creating a domain-invariant mapping of the source and target datasets. Our DA generative adversarial network (GAN) architecture consists of a generator and discriminator that are deep neural networks (DNNs) with the same layer configuration (see figure).

They both consist of 9 layers with 3 sets of fully connected layers,



a batch normalization layer, and a reLU activation layer stacked on top of each other. The fully connected layers have 64, 32, 16 neurons in that order. The last layer of the generator serves as input to the discriminator as well as feeds into a soft-max layer to predict the class of the data sample. Similarly, the final layer of the discriminator feeds into a soft-max layer to predict the domain the sample belongs to. The algorithm is below.

Algorithm 1: Algorithm for adversarial domain adaptation using our GAN architecture.

input : Adam optimizer has learning rate l and decay rates β_1 and β_2
output: The generator G as a classifier
for *n training iterations* **do**
  Select d samples from the source dataset;
  Select d samples from the target dataset;
  Decrease the discriminator gradient using Adam optimiser using loss:
    $-\frac{1}{d}\sum_{i=1}^{d}[\log D(G(x_s^{(i)}))] + [\log(1 - D(G(x_t^{(i)}))]$
  Decrease the generator gradient using Adam optimiser using loss:
    $\frac{1}{2}[L_{class} + L_{domain}]$
    where, $L_{class} = -\frac{1}{2d}\sum_{i=1}^{2d} y^{(i)}[\log(G(x^{(i)})] + (1 - y^{(i)})[\log(1 - G(x^{(i)})]$
    and, $L_{domain} = -\frac{1}{d}\sum_{i=1}^{d}[\log(D(G(x_t^{(i)}))]$
end

We have tested our DA GAN approach for training DL models for intrusion detection for two different cases. The experiments show that our approach achieves higher accuracy than the base case (e.g., no TL is used) and a fine-tuning approach.

Implications for Defence

Our approach supports an approach to address the scarcity of training datasets.

Readiness and Alternative Defence Uses

Provides a technique that can be immediately engineered and applied. However more experiments may be required for assess the suitability of the technique for a large variety of application domains and data.

Resources and References

Singla, Ankush, Elisa Bertino, and Dinesh Verma. "Preparing network intrusion detection deep learning models with minimal data using adversarial domain adaptation." In Proceedings of the 15th ACM Asia Conference on Computer and Communications Security, pp. 127-140. 2020.

Organisations

Purdue, IBM US

Anomaly Detection With A Robotic Edge Device

Military / Coalition Issue

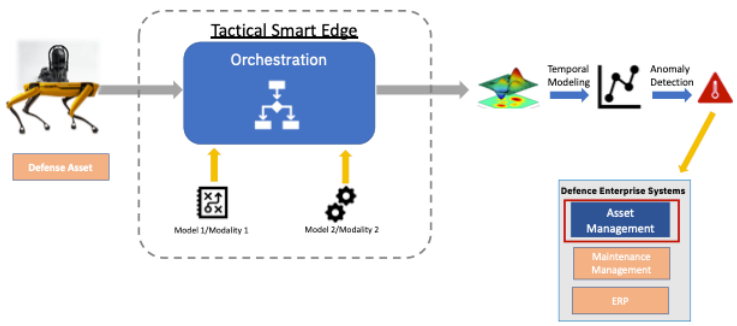
A tactical edge is a dynamically changing environment. Any anomalous event can potentially have massive financial and operational repercussions for military. In addition, human life can be at risk. This work focuses on anomaly detection using a robotic edge device which senses multimodal information from the environment over time to detect changes in environment and flag anomalies.

Core idea and key achievements

Developed an initial multi-modal anomaly detection methodology which aligns information from multiple modalities (e.g. visual, thermal, audio etc.) and uses a temporal modeling methodology to detect anomalous events. The methodology is unsupervised and uses changes in patterns over time for anomaly detection.

Implications for Defence

Anomaly detection at the tactical edge is a particularly important problem for defence purposes. A roaming edge-device such as a robot can be immensely useful for such an application as it can detect anomalies in places where it's risky to send people and can spot things obscured from aerial view (e.g. under shrubbery, exploded buildings etc.). Subtle anomalies which would otherwise elude the human eye can also be detected using advanced sensing (e.g. IR imaging). Anomalies can appear in many forms such as (1) presence of suspicious devices, (2) soldiers who need assistance (during a conflict), or (3) overheating military equipment. Hence analysis of multimodal data is essential. An example pattern for the military would be: during normal period, a robotic edge-device roams around a tactical edge facility and captures multimodal information (visual, audio, thermal etc.) at specific places. This is sent to an edge node which incrementally updates an AI model of what is "normal" at these locations. If at a future time point, some anomalous event occurs, the multimodal anomaly detection module flags it and raises an exception in the defence enterprise asset management system so that next steps are taken.



Readiness & alternative Defence uses

The capability for version 1 of an edge anomaly detection system that incorporates the described functionality is currently in progress within IBM Research. It incorporates and extends DAIS research in model selection, model management, and model fingerprinting. It also incorporates some non-DAIS IBM research and integrates with existing edge deployment and management software. Further progress has been set out to provide a vision for the next stage of anomaly detection system in the near future and a road map towards version 2. Various parts of the capabilities of the described system are at different maturity levels that approximate to TRL levels 3, 4 and 5. Thus, ready to prototype a military Edge AI production facility, and experiment with a range of potential usage patterns.

Resources and references

tbc

Organisations

IBM US

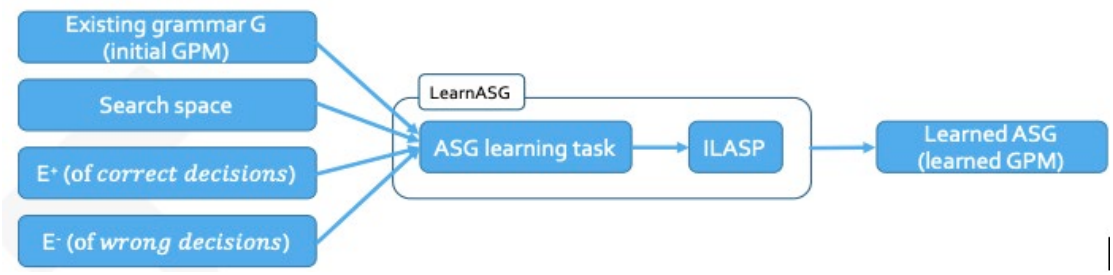
Answer Set Grammar For Efficient Generation Of Policies In Coalition Environments

Military / Coalition Issue

Coalition parties are governed by their own sets of policies for guiding their operations. Policy technologies can be used to manage IT systems and networks, but they rely on centralized services. Coalition environments are highly dynamic and with no access to centralized infrastructures. Systems have to autonomously adapt their policies to maximize their effectiveness while minimizing risk. Self-generative policies can provide a key solution to self-autonomous management of devices in coalition setting. But they have to be learned in a context-dependent manner to accommodate changes and resolve conflicts with policies from other parties' devices.

Core idea and key achievements

Grammars characterise a language and provide mechanisms for automatically generating acceptable sentences. Policies can be seen as sentences of a given language, and the self-generative policy model, from which they are derived, as the grammar that defines "acceptable" policies. In coalition settings, acceptable policies need to not only conform to a syntactic form but also satisfy context-specific semantic properties to guarantee their enforceability. Grammars of self-generative policies need to be context-sensitive. We have proposed a new class of context-sensitive grammars, called Answer Set Grammars (ASG), as a self-generative policy model. We have defined a formal language to specify these models as production rules annotated with semantic constraints expressed in Answer Set Programming. These annotations capture context-specific semantic properties that need to take into account during the policy instantiation process. Policies derived by the ASG's production rules and satisfying the context-dependent semantic constraints are acceptable policies. We have developed two algorithms for (i) learning ASG from examples of context-dependent decisions, and (ii) instantiating policies from a learnt ASG, respective.



We have applied the framework to autonomous vehicles and logistic resupply of coalition forces and shown how intelligent devices can learn generative policies from few examples of past decisions, achieving higher accuracy than existing machine learning systems for classification. These two applications demonstrate our generative policy model to be flexible, able to learn from few examples, to explain learned outcomes and to capture human-driven policy rules.

Implications for Defence

Military operators will be able to use our ASG algorithms on autonomous devices to enable them to learn and instantiate context-dependent optimal policies in response to changes in the environment in, and in the coalition partners within which they operate.

Readiness & alternative Defence uses

Our system is at TRL 4 level. It has been validated in the lab and is ready to be tested in a real environment. It has also been used in other DAIS achievements (e.g., [1c.02], [1c.07], [1c.16]).

Resources and references

Law, Mark, et al. "Representing and learning grammars in answer set programming." Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 33. No. 01. 2019.

Bertino, Elisa, et al. "Generative Policies for Coalition Systems-A Symbolic Learning Framework." 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2019.

Organisations

Imperial College London, Purdue University and Universitat Pompeu Fabra.

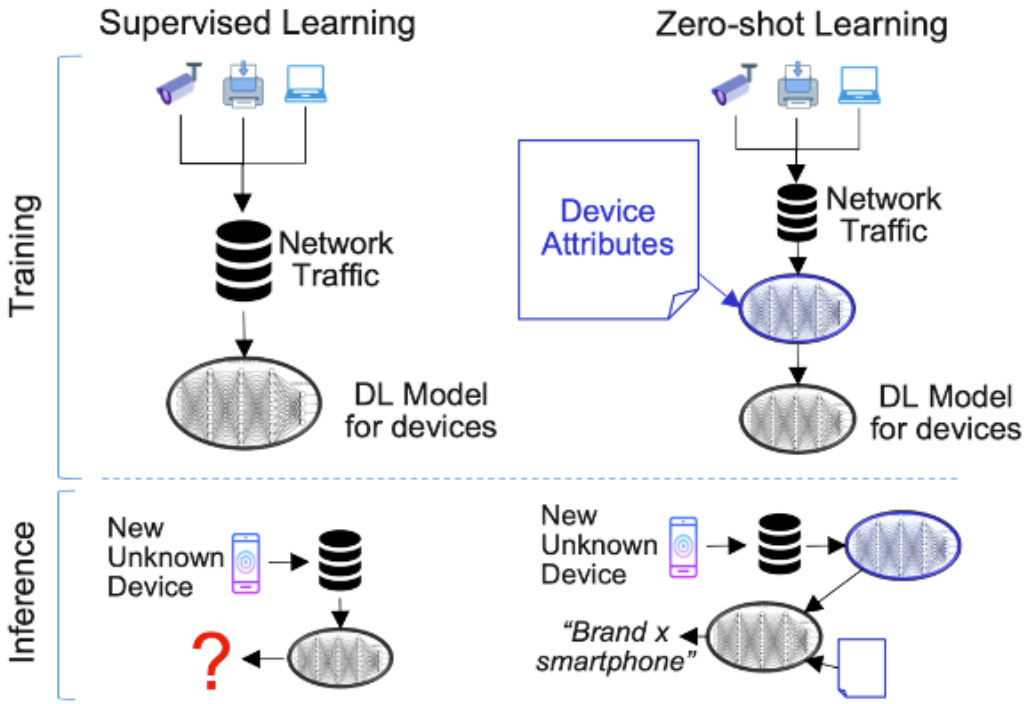
Characterizing New Devices On A Network With Zero-Shot Learning

Military / Coalition Issue

Operating a Coalition network effectively and securely requires the ability to detect and characterize previously unseen devices on the network by analysing network traffic data. A traditional Deep Learning (DL) model which is trained to recognize a set of known devices cannot recognize nor characterize a new device connecting to the network as traffic data associate with such device cannot have been included in the data used to train the DL model.

Core idea and key achievements

Our approach trains a DL model to recognize a set of key device traffic attributes which are shared across multiple devices, thus it can recognize a new device and characterise it.



Initial experiments on two datasets comprising of 21 known and 27 unknown devices, respectively, show the capability of our approach to recognize unknown devices (f1 score 0.58, as opposed to 0 for traditional fully supervised DL models) at the cost of a moderate decrease in performance for known devices recognition (f1 score from 0.77 to 0.65

Implications for Defence

This approach allows an agent to identify or characterise a new device on a monitored network, even though it has never been seen before. This has obvious applications to network management and security.

Readiness & alternative Defence uses

The technology has been tested with promising results as a demo on two datasets of network traffic data from IoT devices [3]. More experiments are underway involving multiple datasets. The component needs a network traffic data sniffer and feature extractor to provide network traffic data in proper input format. It relies on modern opensource deep learning libraries [4] for the DL model definition and training. This work is also connected to Project 10 (for example 10.2 neuro-symbolic), since the attribute information can be seen as additional input to a neural network.

Resources and references

C. H. Lampert, H. Nickisch, S. Harmeling. "Attribute-Based Classification for Zero-Shot Visual Object Categorization." IEEE TPAMI, 2014.

S. Liu, M. Long, J. Wang, M. I. Jordan. "Generalized zero-shot learning with deep calibration network." NeurIPS, 2019.

UNSW IoT Devices Traffic Dataset: https://iotanalytics.unsw.edu.au/iottraces.html

Pytorch: https://pytorch.org/

Tensorflow: https://www.tensorflow.org/

Organisations

IBM Research

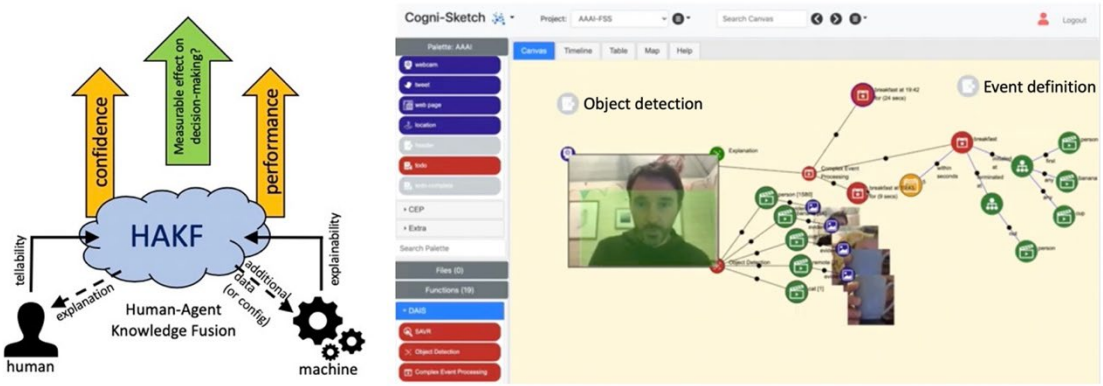
Cogni-Sketch: Enabling Rapidly Formed Human-Agent Coalition Teams Through Extensible Information Exchange

Military / Coalition Issue

There is much potential power to be gained from human-machine teams working together on a variety of situation awareness or problem-solving/understanding tasks. The ability to rapidly introduce, understand, interact with, and configure machine agents is critical, especially in a coalition setting where the machine agents may be unfamiliar. Can we create an approach that enables an efficient and productive human-agent collaborative environment? Can we do so in a way that does not require expensive and time-consuming support from technical specialists and integrators?

Core idea and key achievements

Human-Agent Knowledge Fusion (HAKF) has been defined as an underpinning principle for building such systems, defining the tellability and explainability flows that can enable inter-agent communication and support performance improvement and improved trust.



Creation experimental embodiments of the HAKF principles as an extensible platform named Cogni-sketch to allow information and knowledge sharing between human and machine agents, with each being able to read and write their knowledge to the environment, extend the schema and provide explanations or new local knowledge.

Implications for Defence

An experimental platform to explore options for human-agent teaming and different techniques for interactions. Plug-in architecture supports many forms of extensions, with new machine agents, visualisation types, reasoning systems, import/export and pluggable processes to support or observe team behaviour such as problem solving.

Next step is to test value to different human-agent teams supporting different business functions. Through hardening and exposure to broader examples, this could become a more permanent

capability for specific tasks such as intelligence analysis or situation awareness, and the creation of institutional repositories of task-relevant information.

Readiness & alternative Defence uses

TRL 3/4. The Cogni-sketch code is under active development by IBM UK and has been used in several experiments and use-cases ranging from open-source intelligence analysis to information fusion and agent integration. A secure cloud-based version is available for use on request by DAIS collaborators. Will be released as open-source on github before the end of DAIS in Sep-2021 and support multiple showcase demos.

Resources and references

Braines, D., Cerutti, F., Vilamala, M. R., Srivastava, M., Preece, L. K. A., & Pearson, G. (2020). "Towards human-agent knowledge fusion (HAKF) in support of distributed coalition teams". AAAI FSS 2020.

Braines, D., Preece, A. Roberts, C., & Blasch, E. (2021). "Supporting Agile User Fusion Analytics through Human-Agent Knowledge Fusion" in press

Numerous "videos/demos" available

Organisations

IBM UK, Cardiff University

Combining Vector Symbolic Architecture Aspects and Artificial Intelligence services Using Edge Deployment

Military / Coalition Issue

Extant battle management systems are inflexible; set up at the start of the mission and unchangeable. Using a dynamic routing environment for the allocations tend to overload the network with overhead. Using machine learning systems on partitioned networks causes them to learn in isolation, when the partition ends, the system will need to discard some of the data, and only use data from one of the partitions (or from the system in the pre-partitioned state)

Core idea and key achievements

We show two methods to make allocations dynamic: centralised software defined coalitions (SDC) control and decentralised vector symbolic architecture (VSA). The centralised SDC uses a top-down approach where users are directed to use a service at a particular location, it uses Machine Learning approaches to ensure that users get the best response times as possible, including using coalition resources when available. If the network is partitioned, the fragments of the network will operate independently, and when the partition ends the system uses a combination of Reinforcement and Transfer Learning to boost recovery times by two orders of magnitude.

Implications for Defence

Using these technologies the coalition can achieve the best of both worlds; centralised control and distributed adaptability.

Readiness & alternative Defence uses

The VSA code is at technology readiness level (TRL)2+ and SDC is at TRL1, we hope during the development of the demo that we can make it more ready.

Resources and references

Simpkin, Christopher, et al. "A scalable vector symbolic architecture approach for decentralized workflows." COLLA (2018).

Simpkin, Chris, et al. "Constructing distributed time-critical applications using cognitive enabled services." Future Generation Computer Systems 100 (2019): 70-85.

Simpkin, Christopher, et al. "Dynamic distributed orchestration of Node-Red IoT workflows using a vector symbolic architecture." 2018 IEEE/ACM Workflows in Support of Large-Scale Science (WORKS). IEEE, 2018.

Singla, Ankush, Elisa Bertino, and Dinesh Verma. "Preparing network intrusion detection deep learning models with minimal data using adversarial domain adaptation." Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. 2020.

Leung, Kin K., et al. "Reinforcement and transfer learning for distributed analytics in fragmented software defined coalitions." Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications III. Vol. 11746. International Society for Optics and Photonics, 2021.

Zhang, Ziyao, et al. "Efficient Reinforcement Learning with Implicit Action Space" 4th Annual Fall Meeting of the DAIS ITA, 2020

The underlying vector symbolic architecture code has been published as Open Source.

Organisations

Imperial College, Purdue University, Cardiff, IBM UK, IBM US, ARL and Dstl

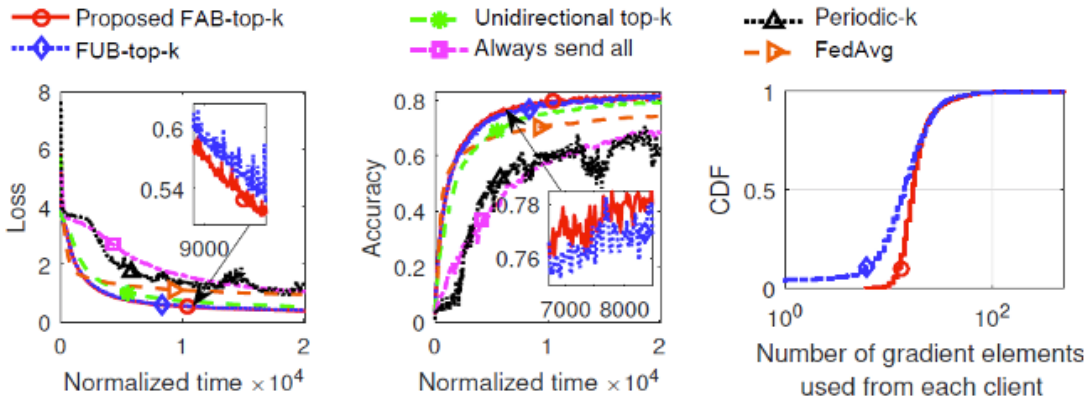
Compressed Model Updates for Efficient Federated Learning

Military / Coalition Issue

Modern military scenarios largely benefit from agile analytics available in the battlefield. Most of such analytics applications are driven by machine learning models for purposes such as image recognition, anomaly detection, etc. A key challenge in the coalition environment is that data to train these models may not be shareable across coalition boundaries. In addition, new data may be collected during the military operation that can be used to adapt existing models to the current environment. To facilitate model training or adaptation in such challenging situations, federated learning can be applied, which includes multiple rounds of parameter updates between clients and the server. However, since the size of modern deep learning models can be very large, transmitting them across the coalition network with limited bandwidth can be very difficult.

Core idea and key achievements

In this work, we propose a method for compressing the exchanged information between federated learning participants (clients) and the server.



The key idea is a top-k sparsification method that is applied to the communication both from clients to the server (uplink) and from the server to clients (downlink). The algorithm is designed to guarantee a minimum amount of information to be included in each round's update. In addition, an online learning subroutine finds the near-optimal sparsity (i.e., value of k) over time. Our experiments show that transmitting 1% of model parameters can be sufficient for achieving training convergence in the smallest amount of time.

Implications for Defence

This work is one of the several core technologies for federated learning developed within the DAIS ITA. It allows future military applications to adapt to rapidly changing environments by training/adapting their underlying models to the most up-to-date observations (data), while preserving the privacy and other regulatory constraints in the coalition.

Readiness & alternative Defence uses

A simulation code and a demo illustrating the effectiveness of compressed model updates is available.

Resources and references

Han, Pengchao, Shiqiang Wang, and Kin K. Leung. "Adaptive gradient sparsification for efficient federated learning: An online learning approach." 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2020.

Open source code: Adaptive_Gradient_Sparsification_FL

Organisations

IBM US, Imperial

Control And Architecture of Software Defined Coalitions
Enhancing Coalition Networking Using Software Defined Coalitions – An Overview

Military / Coalition Issue

Military missions require use of various infrastructure assets including communication links, computational servers, data storage, databases, sensors and other resources. Dynamicity and agility of military operations demand near real-time configuration, re-configuration and provisioning of these resources, while supporting efficient and robust sharing of assets among coalition partners or armed forces. State-of-the-art techniques currently cannot achieve this.

Core Idea and Key Achievements

To address the above issue, the DAIS ITA team has proposed a new architecture called Software Defined Coalitions (SDC), which significantly extends capabilities offered by the existing Software Defined Network (SDN). The key idea of SDN is to separate control functions from the communication switches and links, and implement the control functions by software on a centralized controller for each administrative domain of the network. Due to the software implementation of control functions, SDN is easy to change, flexible, reconfigurable, agile and efficient.

Besides communication resources, coalition operations also make use of other infrastructure resources such as data servers, storage, databases, sensors, etc. The proposed SDC architecture is composed of multiple domains of such resources, where various domains possibly owned by different coalition partners are dynamically joined together to form the SDC infrastructure. The main objective of the proposed SDC is to enable efficient, reconfigurable, agile and robust control and sharing of a variety of resources across domains and among coalition partners for supporting different military operations.

Communication switches and links form the Data Plane for transferring user data, while domain controllers are connected to form the Control Plane for exchanging control information. In addition to managing resources within each domain, the new technical challenges of SDC lie on the management and control of different types of resources across domains. Our design challenges include: (a) how, when and what information domain controllers synchronize with each other, (b) how the control plane can be made robust, (c) what architectural or programming abstractions should be used for exchange of resource status information among controllers, (d) how resources can be shared across domains, and (e) how SDC can quickly respond to infrastructure fragmentation and reconnection.

Key achievements on SDC include the development of designs and techniques for:
-SDC Controller Synchronization
-Resource Sharing in SDC to Support Coalition Missions
-Control Plane Architecture of SDC
-Robust Network and Learning Architectures for SDC
-Joint Reinforcement and Transfer Learning for Distributed Service Configuration in Fragmented SDC

In the process, the team has also developed novel techniques to overcome various machine-learning issues such as model complexity and excessive learning time, which are applicable beyond the control and management of SDC. The techniques include:
-Reinforcement Learning for Military Network Control
-Graph Attention Networks for Congestion and Mobility Prediction
-Binarized Neural Network
-State-Action Separable and Embedding for Reinforcement Learning

Implications for Defence

The collection of new techniques will enable defence to realise the concept of SDC for dynamic, agile and robust configuration, provisioning and sharing of infrastructure assets among coalition partners or armed forces, which are unmatched by our adversaries.

Readiness and Alternative Defence Uses

This work is technology readiness level (TRL) 2/3. Many of the SDC techniques have been prototyped in practical systems or environments, including the demos of controller placement and synchronization, resource sharing, robust network architecture, and learning in fragmented SDC. These techniques are ready for adoption, modification and enhancement for implementation on practical defence systems.

Resources and References

Please refer to the SDC Achievements and Demos as highlighted in this presentation for related publications and resources.

Organisations

Imperial College, Yale University, IBM US, Purdue University, ARL, Dstl

Control Plane Architecture of Software Defined Coalitions

Military / Coalition Issue

Military missions require the use of infrastructure assets including communication links, computational servers, data storage, databases, sensors and other resources. Dynamicity and agility of military operations demand near real-time configuration, re-configuration and provisioning of these resources, while supporting efficient and robust sharing of assets across armed forces or coalition partners. State-of-the-art techniques cannot currently achieve this.

Core idea and Key Achievements

A new architecture called Software Defined Coalitions (SDC) has been developed, which extends the existing Software Defined Networking (SDN), to address the above issue. With SDC, the network control logic is implemented as software at the SDC controller which is programmable to enable rapid configuration for mission objectives. The controller maintains also a conceptually centralized view of the network status that can be valuable for many networking applications. However, due to high network dynamics the controller may be fragmented from the nodes it manages rendering impossible their reconfiguration. An approach that improves the robustness of SDC is therefore needed.

Key achievements include the development of:

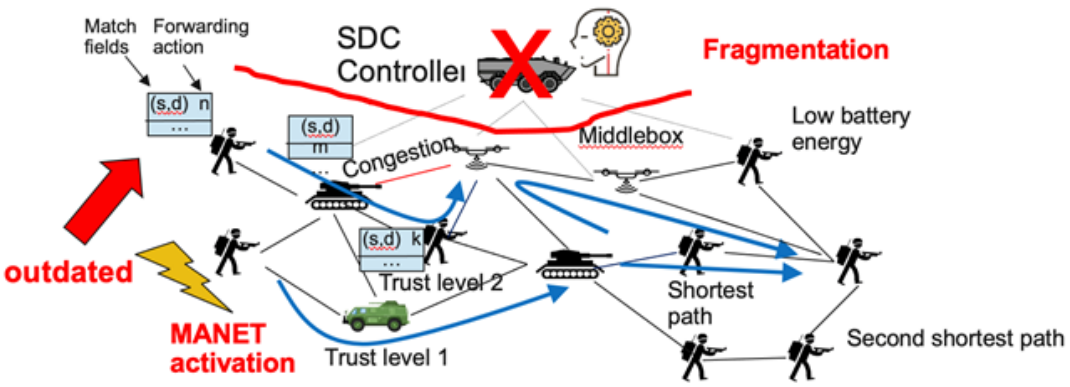
Hybrid SDC/MANET (mobile ad-hoc network) architectures where the SDC controller can interface and dynamically switch the control mode to a distributed MANET protocol (e.g., OLSR) to handle network fragmentation events.

Distributed verification mechanisms for discovery of the controller by the mobile nodes and switching the control mode accordingly.

Algebra to support continuous and frequent network configuration updates by the SDC controller

Novel paradigm to enable inter coalition coordination through the SDC controllers

Testbed experiments with real mobile devices showing the benefits of hybrid SDC/MANET for dynamic routing and failover



Implications for Defence

The hybrid SDC/MANET architecture and accompanying mechanisms will enable defence to realise the concept of SDC even in the most challenging ad hoc network environments, reap the benefits of centralized and programmable network control and deliver intelligent cloud-like services involving multiple coalition enclaves that were impossible to realize by relying only to traditional MANET protocols.

Readiness and Alternative Defence Uses

This work is technology readiness level (TRL) 2/3. Many of the SDC techniques have been prototyped in practical systems or environments, including the demo Hybrid SDN/MANET. Further work will enhance the readiness of the new techniques for practical defence systems.

Resources and References

Samples of related publications include:

Poularakis, Konstantinos, et al. "Bringing SDN to the mobile edge." 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). IEEE, 2017.

Poularakis, Konstantinos, Qiaofeng Qin, Erich M. Nahum, Miguel Rio, and Leandros Tassiulas. "Flexible SDN control in tactical ad hoc networks." Ad Hoc Networks 85 (2019): 71-80.

Poularakis, Konstantinos, Qiaofeng Qin, Kelvin M. Marcus, Kevin S. Chan, Kin K. Leung, and Leandros Tassiulas. "Hybrid SDN control in mobile ad hoc networks." In 2019 IEEE International Conference on Smart Computing (SMARTCOMP), pp. 110-114. IEEE, 2019.

Gokarslan, Kerim, Geng Li, Patrick Baker, Franck Le, Sastry Kompella, Kelvin M. Marcus, Vinod K. Mishra, Jeremy Tucker, Y. Richard Yang, and Paul Yu. "A Highly Reliable and Programmable

Software Defined Coalition (SDC) Architecture using Multiple Control Plane Composition with Distributed Verification."

Xiang, Qiao, Jingxuan Zhang, Kai Gao, Yeon-sup Lim, Franck Le, Geng Li, and Y. Richard Yang. "Toward optimal software-defined interdomain routing." In IEEE INFOCOM 2020-IEEE Conference on Computer Communications, pp. 1529-1538. IEEE, 2020.

Li, Geng, Y. Richard Yang, Franck Le, Yeon-sup Lim, and Junqi Wang. "Update algebra: Toward continuous, non-blocking composition of network updates in sdn." In IEEE INFOCOM 2019-IEEE Conference on Computer Communications, pp. 1081-1089. IEEE, 2019.

Organisations

Yale University, IBM US, UCL, Imperial College, ARL, Dstl

Coresets Learning via Distributed Clustering and Local Gradients

Military / Coalition Issue

In military operations it will often be the case that each mobile device in the coalition network has collected its own set of data from its surroundings, whilst bandwidth limitations prohibit the direct aggregation of the datasets onto a central server. Often, some machine learning task will have to be performed using the distributed dataset as a whole. This project considers how to do such tasks while broadcasting (between the mobile devices) only a small amount of information.

Core idea and key achievements

This project consists of 3 papers about performing machine learning on a distributed dataset without broadcasting much information between devices. The first paper in on the compression (i.e. summarisation) of a local dataset (the compressed datasets can then be easily transmitted to a central server and aggregated). It is assumed that the datasets are in the form of a set of vectors. The compression is comprised of the set of centres of the regions of a Voronoi diagram along with the number of points in the corresponding regions and, for each corresponding region, a vector representing the gradient of a linear approximation of the "probability" density of the points in the region. After transmission, the dataset can then be recovered approximately by sampling from the linear distributions. The second paper builds an approximation of the aggregated dataset where the approximation is a Voronoi diagram along with the number of points in each region. Our distributed algorithm is an approximation (to any degree of accuracy – higher accuracies requiring more information broadcasted) of K-means++ whilst requiring only a very small amount of data to be broadcast. The third paper considers building a classifier via online-to-batch conversion of an online learning algorithm. Our distributed algorithm exactly implements the classic online-to-batch conversion meta-algorithm but only needs to broadcast the mistakes made by the online learning algorithm – a quantity that scales linearly with the bound on the performance of the resulting classifier.

Implications for Defence

These techniques will allow machine learning tasks over distributed datasets to be performed when we have bandwidth constraints in a wireless network of devices.

Readiness & alternative Defence uses

All 3 algorithms were coded up in Python as part of the project.

Organisations

UCL, IBM (US and UK), PSU

Coresets via Multipronged Data Reduction

Military / Coalition Issue

Tactical military operations often occur in poorly-connected or even adversarial networking environments where it is difficult to apply advanced ML (e.g., deep learning) to real-time data as (i) bringing data to the infrastructure is too time and bandwidth consuming, while (ii) running ML at the edge devices (e.g., mobile devices, IoT devices) collecting data is too slow and memory/power-intensive. It is thus highly desirable to have intelligent yet light-weighted ways to collect small data summaries informative enough for training ML models that approximate the models trained on the full dataset.

Core idea and key achievements

Developing efficient and effective data summarization algorithms that:

• significantly reduce the data size and thus the communication cost in data collection

• provably approximate the full dataset in terms of quality of models trained on the reduced data

Our approach is to use coreset, which is a small weighted dataset in the same feature space as the full dataset such that a model trained on the coreset approximates a model trained on the full dataset, with a controllable approximation error.

We investigate coreset-based ML in three aspects:

(1) robust coreset supporting multiple ML tasks,

(2) joint coreset + quantization + dimensionality reduction for better communication efficiency,

(3) efficacy in preserving privacy in comparison to federated learning,

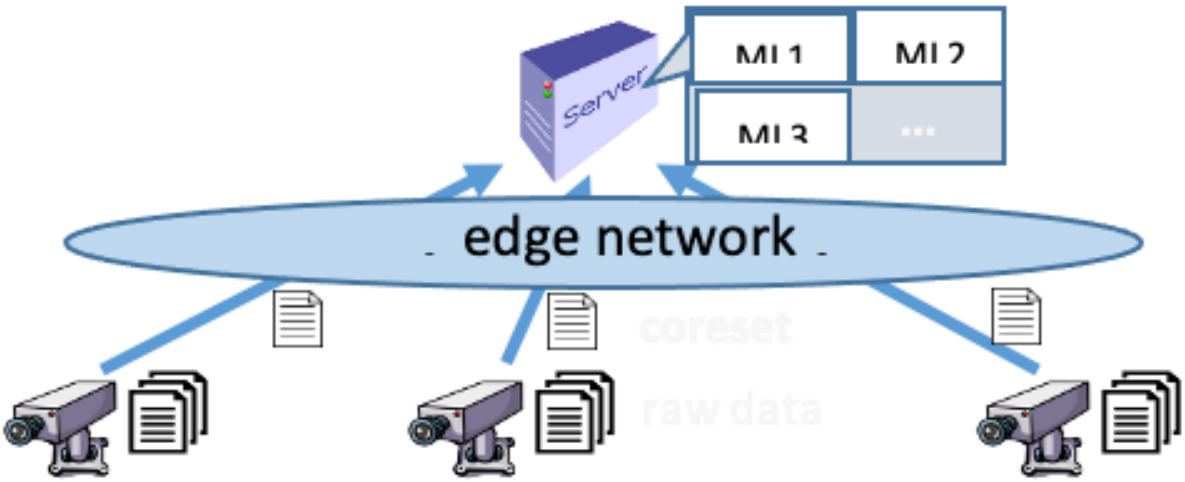
which progressively advance the state of the art.

Implications for Defence

In contrast to heuristic data reduction techniques such as random sampling, our coreset-based data summarization techniques extract the most informative data points and thus significantly reduce the communication cost while guaranteeing the quality of the trained models. While coreset has been used to speed up ML in centralized setting, its use for communication reduction in the training of multiple models of interest is our novel contribution. Our robust coreset can greatly benefit the real-time information extraction in the field with limited bandwidth. We are also the first to combine coreset with quantization and dimensionality reduction, which has demonstrated great promise in further reducing communication cost without compromising model quality, that is highly desirable in tactical environments. Furthermore, our recent results on privacy-quality tradeoff can be utilized in exchanging information across coalition boundaries.

Readiness & alternative Defence uses

Besides algorithms, we developed experimental implementations (code), case studies on real datasets, and a demo based on the virtual world scenario developed by IBM UK.



Resources and references

Lu, Hanlin, et al. "Robust coreset construction for distributed machine learning." IEEE Journal on Selected Areas in Communications 38.10 (2020): 2400-2417.

Lu, Hanlin, et al. "Sharing Models or Coresets: A Study based on Membership Inference Attack." arXiv preprint arXiv:2007.02977 (2020).

Lu, Hanlin, et al. "Communication-efficient k-means for edge-based machine learning." 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2020.

Lu, Hanlin, et al. "Joint coreset construction and quantization for distributed machine learning." 2020 IFIP Networking Conference (Networking). IEEE, 2020.

Lu, Hanlin, et al. "Robust Coreset Construction for Distributed Machine Learning." 2019 IEEE Global Communications Conference (GLOBECOM). IEEE, 2019.

Organisations

PSU, IBM US, UCL, ARL

Data reduction for distributed machine learning using coreset

Military /Coalition Issue

Tactical military operations often occur in poorly-connected or even adversarial networking environments where it is difficult to apply advanced ML (e.g., deep learning) to real-time data as (i) bringing data to the infrastructure is too time and bandwidth consuming, while (ii) running ML at the edge devices (e.g., mobile devices, IoT devices) collecting data is too slow and memory/power-intensive. It is thus highly desirable to have intelligent yet light-weighted ways to collect small data summaries informative enough for training ML models that approximate the models trained on the full dataset.

Core idea and key achievements

Developing efficient and effective data summarization algorithms that:

• significantly reduce the data size and thus the communication cost in data collection

• provably approximate the full dataset in terms of quality of models trained on the reduced data

Our approach is to use coreset, which is a small weighted dataset in the same feature space as the full dataset such that a model trained on the coreset approximates a model trained on the full dataset, with a controllable approximation error.

We investigate coreset-based ML in three aspects:

(1) robust coreset supporting multiple ML tasks,

(2) joint coreset + quantization + dimensionality reduction for better communication efficiency,

(3) efficacy in preserving privacy in comparison to federated learning,

which progressively advance the state of the art.

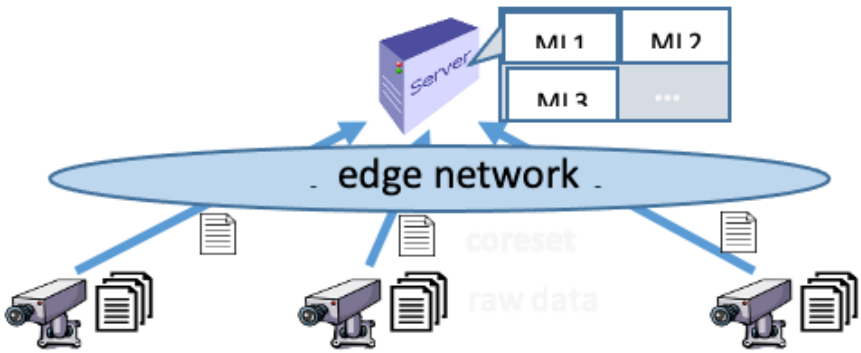
Implications for Defence

In contrast to heuristic data reduction techniques such as random sampling, our coreset-based data summarization techniques extract the most informative data points and thus significantly reduce the communication cost while guaranteeing the quality of the trained models. While coreset has been used to speed up ML in centralized setting, its use for communication reduction in the training of multiple models of interest is our novel contribution. Our robust coreset can greatly benefit the real-time information extraction in the field with limited bandwidth. We are also the first to combine coreset with quantization and dimensionality reduction, which has demonstrated great promise in further reducing communication cost without compromising

model quality, that is highly desirable in tactical environments. Furthermore, our recent results on privacy-quality tradeoff can be utilized in exchanging information across coalition boundaries.

Readiness & alternative Defence uses

Besides algorithms, we developed experimental implementations (code), case studies on real datasets, and a demo based on the virtual world scenario developed by IBM UK.



Resources and references

Lu, Hanlin, et al. "Robust coreset construction for distributed machine learning." IEEE Journal on Selected Areas in Communications 38.10 (2020): 2400-2417.

Lu, Hanlin, et al. "Sharing Models or Coresets: A Study based on Membership Inference Attack." arXiv preprint arXiv:2007.02977 (2020).

Lu, Hanlin, et al. "Communication-efficient k-means for edge-based machine learning." 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2020.

Lu, Hanlin, et al. "Joint coreset construction and quantization for distributed machine learning." 2020 IFIP Networking Conference (Networking). IEEE, 2020.

Lu, Hanlin, et al. "Robust Coreset Construction for Distributed Machine Learning." 2019 IEEE Global Communications Conference (GLOBECOM). IEEE, 2019.

Organisations

PSU, IBM US, UCL, ARL

Data Plane-Based Technique for Network Topology Inference

Military / Coalition Issue

Military coalition networks often suffer from suboptimality caused by lack of a global view of the network state. Knowledge of the global network state (including topology and performance metrics) is the key to many network operations such as service placement and traffic engineering. Directly acquiring the network state of coalition partners in the control plane is subject to constraints by policies. A question of interest is: Can we develop a data plane-based technique to learn the state of coalition networks from measurements readily available at our own nodes?

Core idea and key achievements

We address the above challenge by developing topology inference algorithms that infer the structure and state of a target network from end-to-end measurements at a subset of nodes, using techniques from network topology tomography. While existing algorithms are limited to trees or union of trees denoting routing topologies, our algorithms can

infer not only the routing topology but also the placement of in-network processing units (e.g., virtualized network functions),

infer how each measurement path traverses the internal nodes/links and the network functions,

guarantee consistent reconstruction of all the measurements while existing algorithms may fail under non-tree-based routing.

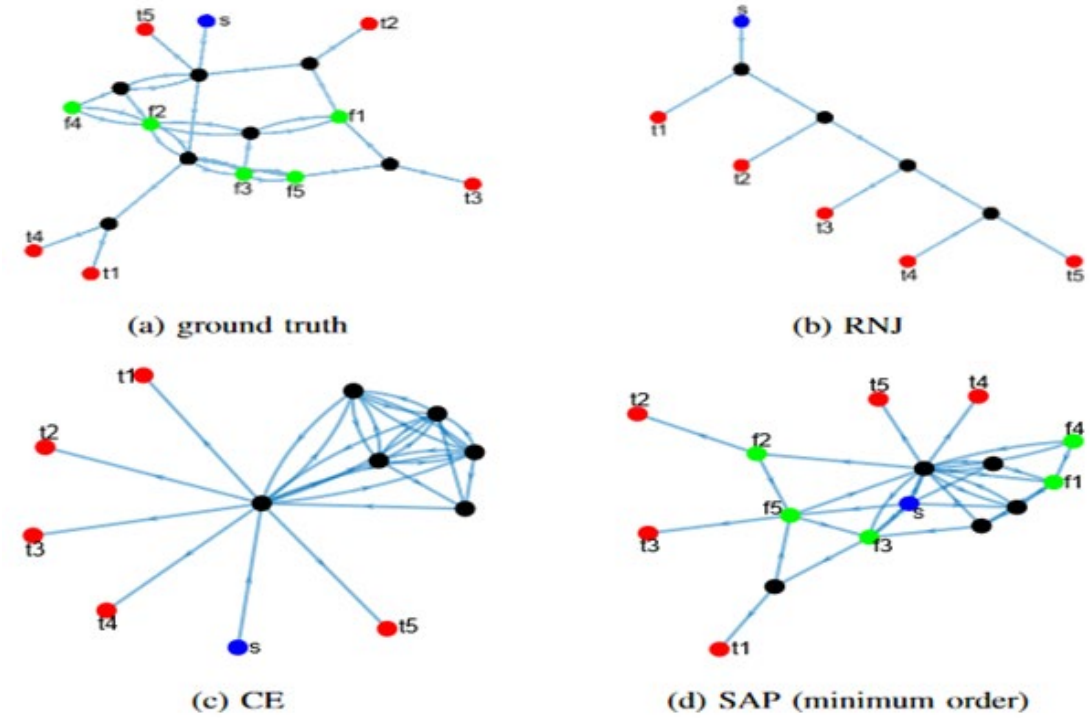
We use a novel two-step approach by first solving a possibly under-constrained linear system to infer the sum weight of links traversed by the same set of paths (called category weight), and then inferring a logical topology based on the category weights and the service chains. Our solution has guaranteed accuracy in several special cases and improved accuracy in the general case compared to state-of-the-art algorithms.

Implications for Defence

From the perspective of network management (e.g., network slice allocation), the proposed algorithms can provide a logical view of the coalition network state across coalition boundaries without requiring direct control plane access, thus facilitating easy deployment of services and migration of algorithms designed for single-domain networks. From the perspective of security and privacy, the proposed algorithms provide a view of what an adversary can infer from end-to-end measurements at a subset of compromised nodes, thus facilitating vulnerability analysis and design of defences (e.g., periodic updates of slice allocation as a moving target defence).

Readiness & alternative Defence uses

Besides algorithms, we developed experimental implementations code and case studies on real network topologies.



Resources and references

Lin, Yilei, et al. "Looking glass of NFV: Inferring the structure and state of NFV network from external observations." IEEE/ACM Transactions on Networking 28.4 (2020): 1477-1490.

Y. Lin, T. He, S. Wang, K. Chan and S. Pasteris, "Looking Glass of NFV: Inferring the Structure and State of NFV Network from External Observations," IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, 2019, pp. 1774-1782, doi: 10.1109/INFOCOM.2019.8737393.

Lin, Yilei, et al. "Waypoint-based topology inference." ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020.

Lin, Yilei, et al. "Multicast-based weight inference in general network topologies." ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE, 2019.

Organisations

PSU, IBM US, ARL, UCL

Distributed Coreset Construction for Efficient Machine learning in Coalitions

Military / Coalition Issue

As the use of machine learning models rapid grows, there is a growing issue of how to update and replace those models as improvements are made over time, whether due to increased training, better algorithms, or adding new categories of "targets" to identify. Existing models tend to be fairly large in size creating yet more contention for the limited bandwidth at the edge of networks where the sensors that require the models are generally located.

Core idea and key achievements

This demonstration shows how that by parameter clustering and optimisation a core-set of parameters can be automatically selected to represent the whole model that uses only a fraction of the data size, yet retains high accuracy, and that this can be achieved across a distributed set of sensors.

Implications for Defence

This solution potentially allows machine learning model retraining on devices while in the field, for example to achieve better accuracy in local conditions. By using this technology model sizes, and thus bandwidth required for distribution, can be reduced by 90% and still achieve accuracy within 6% of optimal, or a reduction of 70% and be within 1% of optimal. This could potentially allow over the air updates, or more regular updates, to occur to ensure best fit to the operational conditions.

Readiness & alternative Defence uses

This technology has been show to work with existing image recognition machine learning model algorithms and while most applicable to defence, can also be used in any situation where you may have a locally distributed compute capability across a network of smaller devices, but that the communications links back to a base may be insufficient to allow reasonable data transfer of ML models.

This work has been continued by IBM Research US, and may be incorporated into a future product offering.

Resources and references

Lu, Hanlin, et al. "Robust coreset construction for distributed machine learning." IEEE Journal on Selected Areas in Communications 38.10 (2020): 2400-2417.

Lu, Hanlin, et al. "Joint coreset construction and quantization for distributed machine learning." 2020 IFIP Networking Conference (Networking). IEEE, 2020.

Organisations

Penn State , UCL, ARL, IBM US, IBM UK

Dynamic Communications Replanning Using a Vector Symbolic Architecture

Military / Coalition Issue

The Military relevance of this task is in a future coalition context where analytics applications can be automatically composed from sensors and services that may be distributed across the coalition network and owned by different coalition partners. This is sometimes referred to as the Internet of Battlefield Things (IoBT). How is it possible to discover the required component services and compose the necessary workflows to perform distributed analytics tasks? Is it possible in contested environments to be resilient against network fragmentation and loss of computational assets?

Core idea and key achievements

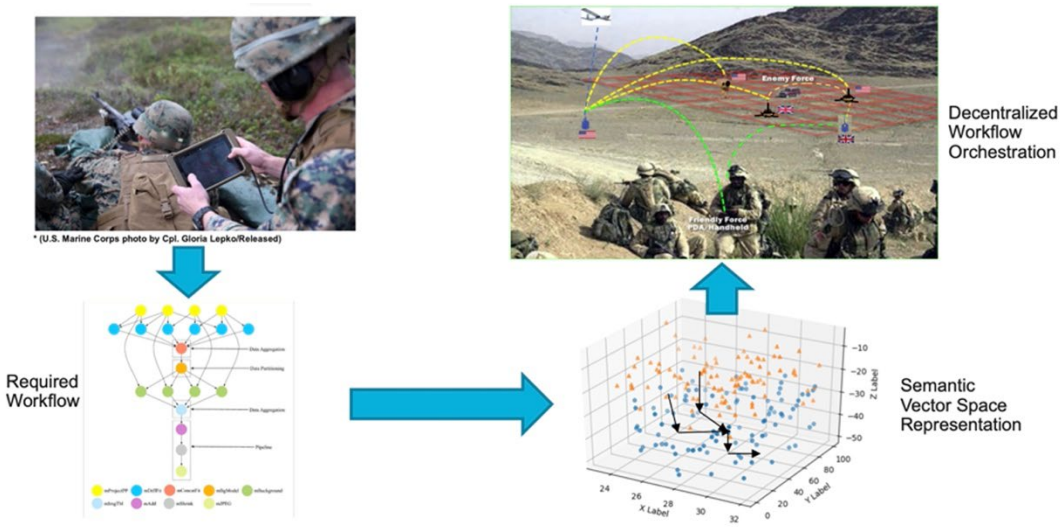
The core idea is that sensors, data and services (essentially anything) can be described as symbolic semantic binary vectors. Essentially everything is described as a vector of vectors. These vectors have mathematical properties that can be exploited to provide a new way of performing service decentralized peer-to-peer service discovery with no requirement for centralized control. Our key achievement has been to show how to create these vectors from service and sensor descriptions and how these vectors can be bundled together to create new vectors that describe the service workflows that describe the required analytics applications.

Implications for Defence

Using vector representations of sensors, data and services provides an important new way to rapidly configure available assets to perform new tasks in highly dynamic military operations. In a coalition setting the use of semantic vector representations offers the potential to discover and make use of assets owned by other coalition partners to perform required tasks.

Readiness & alternative Defence uses

We have already demonstrated that how the vector representation can be used to perform tasks such as dynamic communications re-planning and to discover and orchestrate NATO Future Mission Network (FMN) services. These demonstrations have used representative simulations of mobile ad-hoc networks (MANET) environments. Higher technology readiness levels (TRLs) could be archived by demonstrating the technology operating in actual wireless networks.



Resources and references

Simpkin, Christopher, et al. "A scalable vector symbolic architecture approach for decentralized workflows." COLLA (2018).

Simpkin, Chris, et al. "Constructing distributed time-critical applications using cognitive enabled services." Future Generation Computer Systems 100 (2019): 70-85.

Simpkin, Chris, et al. "Efficient orchestration of node-red iot workflows using a vector symbolic architecture." Future Generation Computer Systems 111 (2020): 117-131.

Organisations

IBM UK, Cardiff University, IBM US

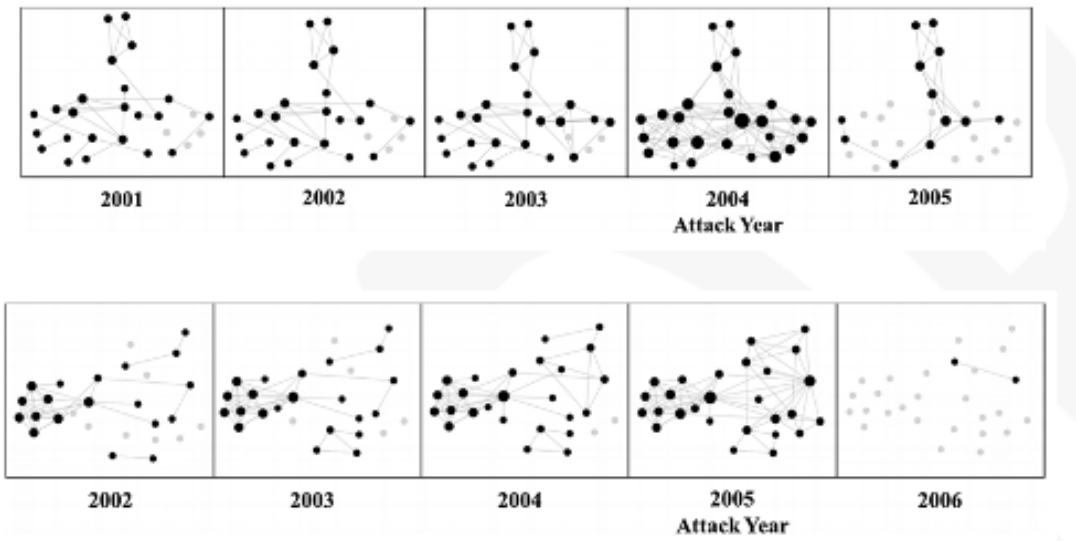
Dynamic Patterns of Terrorist Networks

Military / Coalition Issue

Terrorist networks have a trade-off to consider between efficiency (of communication) vs security (to disruption) and need to "manage" this balance. This can be detected by network analysis if data is available. By sharing known data about terrorist organisations and operatives, can awareness be achieved, and insight into potential impending attacks?

Core idea and key achievements

By applying analytics to available terrorist network data for 11 attack events, we identified that these networks showed increased connectivity as the attack year approached, and substantial decreased connectivity after the attack (due to network disruption by law enforcement).



We used various descriptive network measures including Separable Temporal Exponential Random Graph Models (STERGMs) to measure network density as the basis for this analytics.

Implications for Defence

Our findings have the potential to inform counterterrorism efforts by suggesting which actors make the most influential targets for law enforcement. We discuss how these strategies should vary as extremist networks evolve over time. This could be used in a number of settings: e.g., to help predict group activities and attacks, to determine where costly resources such as detailed monitoring should be applied. Other behaviours may be observed for long-running terrorist groups rather than attack-focused networks that seek to perpetrate a single event.

Readiness & alternative Defence uses

This work is technology readiness level (TRL) 1/2. For the available data this technique has shown strong predictive potential for attack events, based on increased connectivity as the event nears. However, the data was limited and may have been subject to biases (e.g., collection bias). To take the work forward it would be valuable to apply this to broader terrorist network data, which is not publically available. The same tension between security and efficiency may apply in other non-terrorism settings and the STERGM method may be useful in calibrating the performance over time of other networks.

Resources and references

McMillan, Cassie, Diane Felmlee, and Dave Braines. "Dynamic patterns of terrorist networks: Efficiency and security in the evolution of eleven islamic extremist attack networks." Journal of quantitative criminology 36, no. 3 (2020): 559-581.

Organisations

Penn State, IBM UK

Dynamic Placement of Distributed Analytics Services

Military / Coalition Issue

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. 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.

Core idea and key achievements

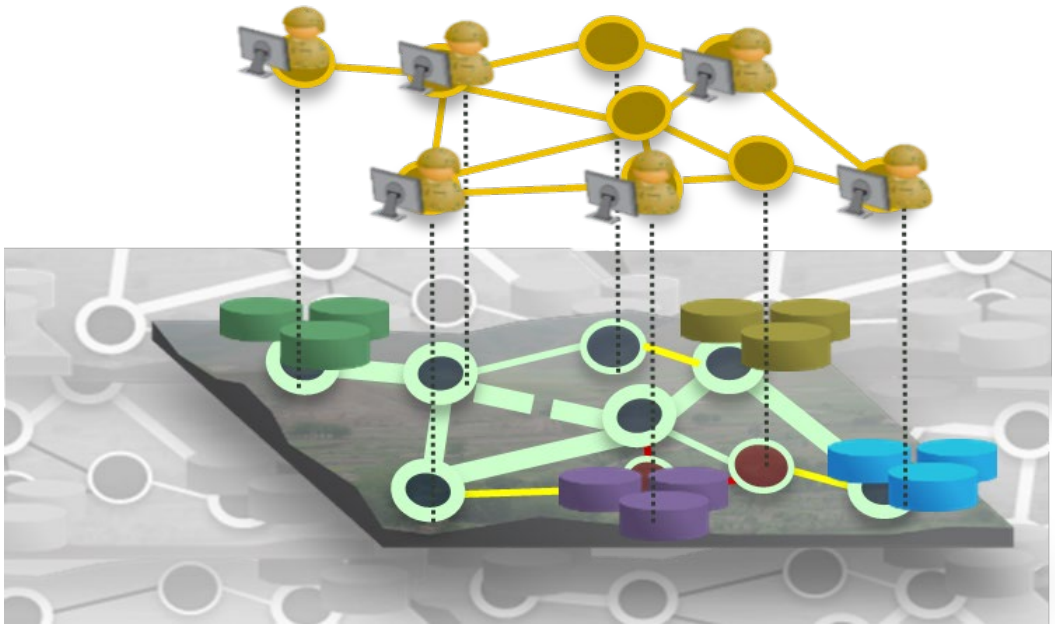
We have developed a set of algorithms to determine where to place analytics services and what services should be placed, in dynamically changing environments. Our algorithms have the following key characteristics:

efficient execution with bounded time and space complexity;

provable optimality guarantee in worst case scenarios;

adaptable to system and user dynamics.

These results were obtained using analytical techniques from the fields of online learning, approximation algorithms, and optimization. Such guaranteed worst-case performance is very useful for ensuring expected system behaviour even in highly dynamic settings.



Implications for Defence

Current tactical analytics approaches use centrally located services requiring significant amounts of computing and networking resources. In the future, distributed analytics can significantly enhance coalition operations at the tactical edge, providing situation awareness for a variety of applications (e.g., ISR, C2). The techniques that we have developed will support agile analytics to soldiers in the field by dynamically placing services at suitable locations. Our algorithms have theoretical worst-case guarantees which ensure robustness in challenging environments.

Readiness & alternative Defence uses

A set of algorithms are described in published papers and many of them are also available as source code.

Resources and references

Key papers:

He, Ting, et al. "It's hard to share: Joint service placement and request scheduling in edge clouds with sharable and non-sharable resources." 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2018.

Pasteris, Stephen, et al. "Maxhedge: Maximizing a maximum online." The 22nd International Conference on Artificial Intelligence and Statistics. PMLR, 2019.

Pasteris, Stephen, et al. "Service placement with provable guarantees in heterogeneous edge computing systems." IEEE INFOCOM 2019-IEEE Conference on Computer Communications. IEEE, 2019.

Farhadi, Vajiheh, et al. "Service placement and request scheduling for data-intensive applications in edge clouds." IEEE/ACM Transactions on Networking 29.2 (2021): 779-792.

Basu, Prithwish, et al. "Decentralized placement of data and analytics in wireless networks for energy-efficient execution." IEEE INFOCOM 2020-IEEE Conference on Computer Communications. IEEE, 2020.

Pasteris, Stephen, et al. "Online Learning of Facility Locations." Algorithmic Learning Theory. PMLR, 2021.

Organisations

UCL, PSU, IBM US, BBN, Southampton, Yale, ARL

Edge Ai Software Development Kit For Coalition Analytics

Military / Coalition Issue

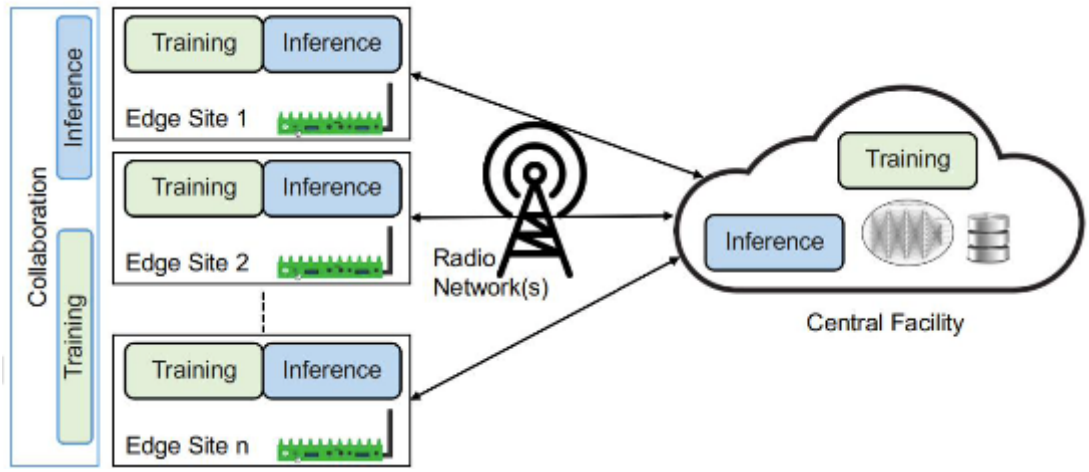
Typically AI involves large amounts of data being collected, transferred and processed in data centres. This presents severe challenges to the use of AI at the edge of the network due to the limited connectivity and compute capability available; to which there are added challenges associated with trust, confidentiality and integrity in coalition operations.

Core idea and key achievements

Developed an initial Edge AI software development kit (SDK) to enable production and test of tailored solutions for AI in these situations. The SDK offers flexibility to cover different usage patterns, such as one or a combination of: efficient data collection; data anonymisation; edge training; edge inferencing; edge model adaptation; collaborative training and collaborative inference.

Implications for Defence

Edge AI allows the military to deploy, train and run more effective AI systems at the edge. This brings a clear advance in capability with two major advantages being: lower bandwidth requirements; and better AI capability at the edge of the network. An example pattern for the military would be: from a catalogue of pre- trained AI models held in central storage, the best model for the task (e.g. vehicle identification) is selected through a ranking process; this model is pruned to compress it where it can then be efficiently transferred to edge devices (because it is smaller); the pruned model is executed on the edge devices and due to pruning, more effective models can be run on an equivalent device (makes better use of bandwidth and CPU/memory); as the situation progresses the edge devices co-operate to tweak the model using transfer learning (one device can help another) and federated



learning (devices work collaboratively for mutual benefit) at the edge; federated inference (devices jointly make predictions) may also take place; finally the model can optionally be

transferred efficiently (because it is compressed) back to the central catalogue if desired such that it can be selected and re-used in future operations.

Readiness & alternative Defence uses

The capability for version 1 of an Edge AI SDK that incorporates all of the described functionality is currently in progress within IBM Research. It incorporates and extends DAIS research such as coresets, federated learning and model selection. It also incorporates some non-DAIS IBM research and integrates with existing edge deployment and management software. Further progress has been set out to provide a vision for the Edge AI SDK in the near future and a road map towards version 2. Various parts of the capabilities of the SDK are at different maturity levels that approximate to TRL levels 3, 4 and 5. Thus, ready to prototype a military Edge AI production facility, and experiment with a range of potential usage patterns.

Resources and references

Keith Grueneberg, Xiping Wang, and Seraphin Calo. "DAIS Edge Transition" Technical Report and Demonstration April 2022

Organisations

IBM UK, IBM US

Effect of Organizational Structure on Cultural Influence

Military / Coalition Issue

Cultural influence represents how ideas, concepts, beliefs and ways of working embed themselves and transfer across a population. Such culture is rarely uniform even in “strict” organisations, and it is interesting to understand the extent that there are effects such as polarisation or diversity. This can help to support organisational design for complex operations or it can be used to evaluate existing operational structures in new ways.

Core idea and key achievements

A model has been developed that extends the literature by including the concept of “cumulative culture”. This is a hallmark of humans and represents the ability to ratchet cultural innovations (i.e., new ideas) on top of each other, such that they can carry forward from one generation to the next. The approach can be applied over any network structure, and combined with the level of bidirectional influence that is present in any relationship.

Implications for Defence

The techniques are useful internally, e.g., assessing or evaluating organisational structures to assess their cohesiveness. They are also useful externally, for example to assess external actors, regimes or groups with respect to their cultural characteristics. This may for example, be useful in assessing points of weakness or division given an organisational or social network structure. It can also be used to support the design implications of social structures (e.g., cultural implications of adding additional links, or enforcing greater downward control).

Readiness & alternative Defence uses

The research has been carried out at low technology readiness level (TRL) to establish the concepts and compare them with baselines from the literature. These techniques can now be taken and translated to practical scenarios for operational analysis. This could for example be useful in evaluating alterative structures for particular operations, or to support training concerning awareness on group dynamics.

Resources and references

Morris, Rhodri L., Liam D. Turner, Roger M. Whitaker, and Cheryl Giammanco. "Breadth verses depth: the impact of tree structure on cultural influence." In International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation, pp. 86-95. Springer, Cham, 2020.

Morris, Rhodri, Liam Turner, Roger Whitaker, and Cheryl Giammanco. "The Impact of Peer Pressure: Extending Axelrod's Model on Cultural Polarisation." In 2019 IEEE International Conference on Cognitive Computing (ICCC), pp. 114-121. IEEE, 2019.

Further work (Journal publication) is in preparation.

Organisations

Cardiff, ARL

Efficient Attacks Using Side-Channels

Military / Coalition Issue

Explanations are increasingly required by the coalitions to build transparent and trustworthy AIs. Especially in safety-critical settings, coalition members may not rely on the AI systems if their predictions are not understandable. However, the explanations give rise a potential side channel which an adversarial user can leverage for attacking the models. In this work, we investigate in depth how one can leverage explanation information to attack neural networks. We also propose a differential privacy-based strategy to defend against these attacks.

Core idea and key achievements

Nowadays, attacking a black-box AI system usually requires many queries of the system which render the attack algorithm impractical. The core idea is to design attack algorithms to subvert systems by reducing the number of queries. Explanations happened to leak information such that the attacker can fool the system strategically.

The key achievements are as follows:

• First, we exploit explanations as a side-channel that is available to an attacker, in addition to the model decision, and develop query-efficient black box attacks.

• Second, we propose a differential privacy (DP) based provable defence to minimize the advantage that an adversary, with access to explanation, enjoys in gradient estimation.

Implications for Defence

Explanations are proposed to produce more transparent AI to increase human's trust and reliance. However, the work exposes the potential risk of such explanations – they can be leveraged for more efficient attack. The proposed defence mechanism demonstrates that the system can reduces the adversarial advantage while maintaining the fidelity of explanations.

Readiness & alternative Defence uses

Attack feasibility and demonstration of defence efficiency, level 3

Resources and references

Abadi, M., Chu, A., Goodfellow, I., McMahan, H.B., Mironov, I., Talwar, K. and Zhang, L., 2016, October. Deep learning with differential privacy. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 308-318).

Patel, Neel, Reza Shokri, and Yair Zick. "Model explanations with differential privacy." arXiv preprint arXiv:2006.09129 (2020).

Organisations

IBM US, UCLA

Efficient Collective Problem Solving

Military / Coalition Issue

Teamwork lies at the cornerstone of the modern workplace, allowing organizations to tackle problems whose complexity reaches beyond the abilities of individuals. Similarly, the complexity of modern military operations creates a demand for efficient collaborative decision making and problem solving. Since an effective operability in dynamic environments requires precise dissemination and transfer of information across the command-and-control structure, the key question remains what types of social interactions are most suitable for achieving necessary Command and Control (C2) capabilities.

Core idea and Key Achievements

Our approach is to model collaborative problem solving and study how well groups of agents address tasks of increasing complexity. The developed simulation environment enables us to test how the structure of the social network used to share information and modes of information accumulation affect the accuracy and speed of collective work.

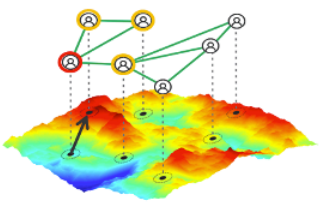
Key achievements include:

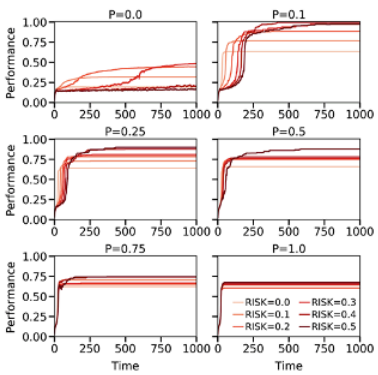
Determining that the detailed structure of the social network used to share information has limited impact on the group performance and that sparsely connected teams perform equally well or better than densely connected ones.

Showing that collective decisions are reached faster in densely connected teams, however at a cost of lower accuracy.

Observing that intermittent switching between group work and individual work results in a significant increase in overall team performance, when compared to constant group work.

Demonstrating that in order to solve highly complex tasks, collective problem solving needs to incorporate a certain level of risk, which can be optimized to improve group performance.





Implications for Defence

Future C2 structures need to match the variability and dynamism of modern military operations. Our agent-based simulation techniques provide an environment for testing various C2 configurations and assessing their viability. We can also use our modelling approach to guide design of war games, which in turn can be utilized to validate and further improve the simulation.

Readiness and Alternative Defence Uses

This project is simulation driven and as such, our observations are limited by the constraints of this environment. Further progress would require human testing, in order to test overlap of theory and practice, as well as to extend simulations into more specific military scenarios.

Resources and References

Turalska, Malgorzata, Geeth R. De Mel, Rosie Lickorish, Liam Turner, Roger Whitaker, and Dave Braines. "Optimizing the efficiency of collective decision making in groups." In Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications III, vol. 11746, p. 117460L. International Society for Optics and Photonics, 2021.

github repository

Organisations

ARL, IBM UK, Cardiff, Southampton

Energy Efficient Vector Symbolic Architecture Using 'In Memory' Hyperdimensonal Computing

Military / Coalition Issue

The benefits of using symbolic semantic vectors to perform unambiguous communication and decentralized service workflow construction has been described in other key achievements. Edge of network coalition operations, particularly in the context of IoBT operations, are often performed in energy constrained environments where savings in computation energy efficiency can become the limiting factor in determining where to deploy the sensors and services. Is it possible to use new technologies based on 'In Memory' processing to achieve significant energy savings?

Core idea and key achievements

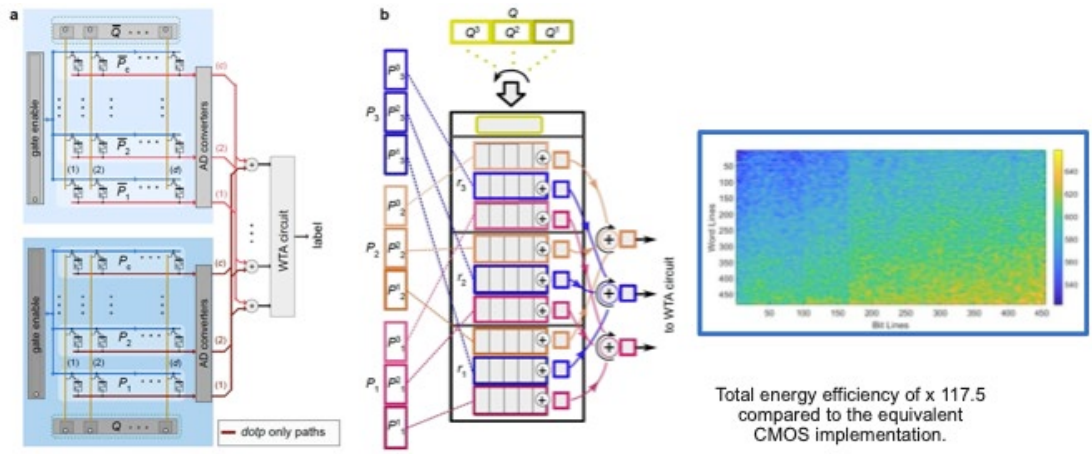
Many of the symbolic semantic vector operations that are required can be performed in a highly parallel fashion using a new generation of 'In-Memory' and 'Near-Memory' processing devices. We have demonstrated, using an experimental phase change memory device (PCM), that many of the computationally expensive operations that required to perform workflow composition using symbolic semantic vectors can be performed on such devices. Energy savings of greater than 100x what can be achieved when using dedicated CMOS devices have been measured. Ongoing work is focused on re-implementing the logic of our vector mapping and the binding and bundling operations to make greater use of this technology with the aim of implementing all the required operations on a single highly compact and energy efficient device.

Implications for Defence

In memory processing using these new generation of devices to perform vector operations is called hyperdimensional computing. This new generation 'In Memory' processing avoids what is termed the Von Neumann bottleneck and offers the potential for extremely low power processing particularly for vector intensive operations which are becoming increasingly important in Artificial Intelligence and image processing applications.

Readiness & alternative Defence uses

The PCM device used in our evaluation is an experimental device developed by IBM Research who are currently developing devices with more memory capacity which we also plan to evaluate. Whilst we have demonstrated their efficacy for energy efficient workflow composition, they are also showing promise in other areas of Artificial Intelligence processing in areas such as image and document classification. Utilising these devices could have a significant impact on future edge of network IoBT/IoT type operations.



Total energy efficiency of x 117.5 compared to the equivalent CMOS implementation.

Resources and references

Graham Bent, Christopher Simpkin, Ian Taylor, Abbas Rahimi, Geethan Karunaratne, Abu Sebastian, Declan Millar, Andreas Martens, Kaushik Roy, "Energy efficient 'in memory' computing to enable decentralised service workflow composition in support of multi-domain operations," Proc. SPIE 11746, Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications III, 117461Q (12 April 2021); https://doi.org/10.1117/12.2586988

Organisations

IBM Europe, Cardiff University

Energy Efficient Vector Symbolic Architecture Using Spiking Neural Networks

Military / Coalition Issue

Edge of network coalition operations, particularly in the context of IoBT operations, are often performed in energy constrained environments where savings in computation energy efficiency can become the limiting factor in determining where to deploy the sensors and services. Emerging Spiking Neural Network devices are extremely energy efficient but require a new programming paradigm. Is it possible to use SNN technologies to perform vector process operations and therefore to achieve the desired energy savings?

Core idea and key achievements

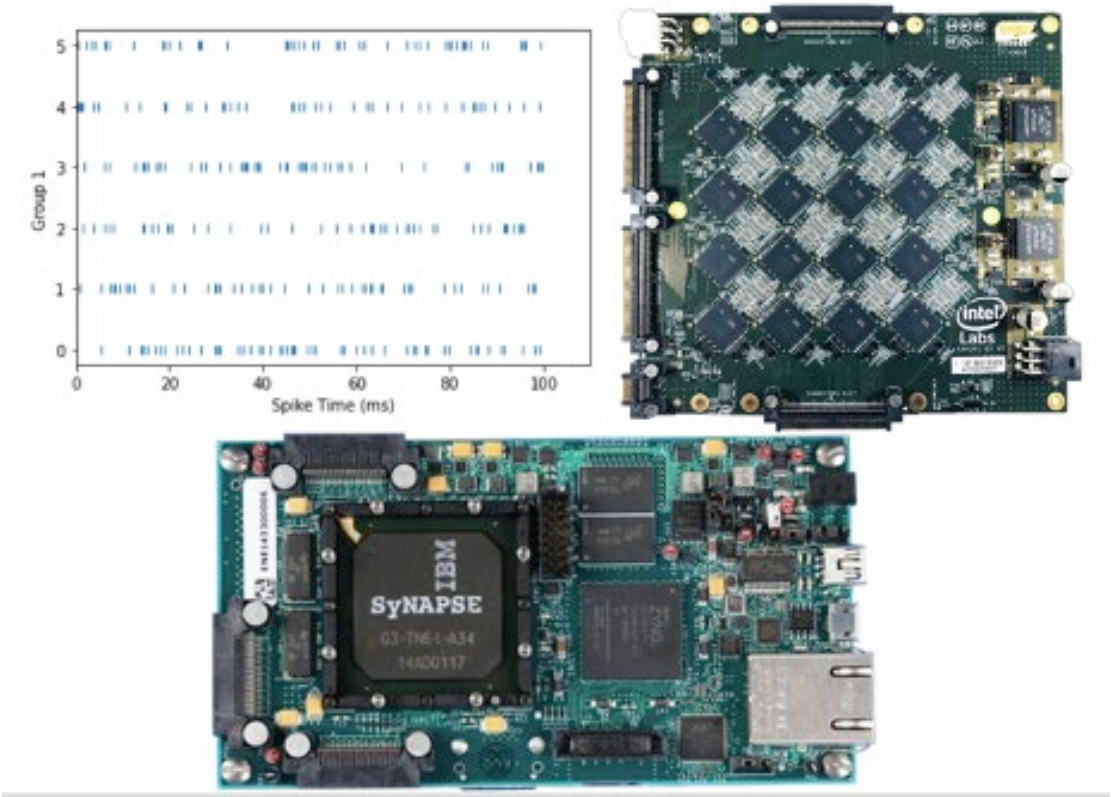
Our work using symbolic semantic vectors has been focussed on the use of high dimensional binary vectors to perform the required vector binding and bundling operations. We have shown that it is possible to use SNN devices to perform the required vector processing operations on these vectors but because of the spike density there is little energy saving to be gained. A key achievement is to show that it is possible to perform equivalent operations using sparse vector representations which are more amenable since the equivalent spike density is reduces by a factor of at least x10 on what are already energy efficient devices.

Implications for Defence

The development of SNN devices and their use in energy constrained environments (e.g., drones, edge devices) is a potential disruptive technology that needs to be exploited for defence applications. Our use case for these types of devices was to perform efficient vector processing and our work has illustrated that there are many more potential applications where they can be exploited. Particularly in the areas of AI and machine learning.

Readiness & alternative Defence uses

A number of experimental SNN devices have been developed by organisations such as IBM and Intel and these devices have been shown to operate at significantly lower power than traditional microprocessor architectures (typically x100-x1000 more energy efficiency). The challenge is how to process the devices to perform the required operations. These devices have been successfully demonstrated to be capable of performing energy efficient image processing and we have shown in our work, they can be used for symbolic vector processing. These types of devices will start to become commercially available in the near term and are ideally suited to the low energy requirements for future IoBT/Iot operations.



Resources and references

Roy, Deboleena, Priyadarshini Panda, and Kaushik Roy. "Synthesizing images from spatio-temporal representations using spike-based backpropagation." Frontiers in neuroscience 13 (2019): 621.

Srinivasan, Gopalakrishnan, and Kaushik Roy. "Restocnet: Residual stochastic binary convolutional spiking neural network for memory-efficient neuromorphic computing." Frontiers in neuroscience 13 (2019): 189.

Frontiers in Neuroscience 2020: "Event-driven Backpropagation for Spiking Neural Networks: Enabling Spike-based Learning in State-of-the-art Deep Architectures."

Organisations

IBM Europe, Cardiff University, Purdue University

Enhancing Coalition Networking using Software Defined Coalitions – An Overview

Military / Coalition Issue

Military missions require use of various infrastructure assets including communication links, computational servers, data storage, databases, sensors and other resources. Dynamicity and agility of military operations demand near real-time configuration, re-configuration and provisioning of these resources, while supporting efficient and robust sharing of assets among coalition partners or armed forces. State-of-the-art techniques currently cannot achieve this.

Core Idea and Key Achievements

To address the above issue, the DAIS ITA team has proposed a new architecture called Software Defined Coalitions (SDC), which significantly extends capabilities offered by the existing Software Defined Network (SDN). The key idea of SDN is to separate control functions from the communication switches and links, and implement the control functions by software on a centralized controller for each administrative domain of the network. Due to the software implementation of control functions, SDN is easy to change, flexible, reconfigurable, agile and efficient.

Besides communication resources, coalition operations also make use of other infrastructure resources such as data servers, storage, databases, sensors, etc. The proposed SDC architecture is composed of multiple domains of such resources, where various domains possibly owned by different coalition partners are dynamically joined together to form the SDC infrastructure. The main objective of the proposed SDC is to enable efficient, reconfigurable, agile and robust control and sharing of a variety of resources across domains and among coalition partners for supporting different military operations.

Communication switches and links form the Data Plane for transferring user data, while domain controllers are connected to form the Control Plane for exchanging control information. In addition to managing resources within each domain, the new technical challenges of SDC lie on the management and control of different types of resources across domains. Our design challenges include: (a) how, when and what information domain controllers synchronize with each other, (b) how the control plane can be made robust, (c) what architectural or programming abstractions should be used for exchange of resource status information among controllers, (d) how resources can be shared across domains, and (e) how SDC can quickly respond to infrastructure fragmentation and reconnection.

Key achievements on SDC include the development of designs and techniques for:

-SDC Controller Synchronization

-Resource Sharing in SDC to Support Coalition Missions

-Control Plane Architecture of SDC

-Robust Network and Learning Architectures for SDC

-Joint Reinforcement and Transfer Learning for Distributed Service Configuration in Fragmented SDC

In the process, the team has also developed novel techniques to overcome various machine-learning issues such as model complexity and excessive learning time, which are applicable beyond the control and management of SDC. The techniques include:

-Reinforcement Learning for Military Network Control

-Graph Attention Networks for Congestion and Mobility Prediction

-Binarized Neural Network

-State-Action Separable and Embedding for Reinforcement Learning

Implications for Defence

The collection of new techniques will enable defence to realise the concept of SDC for dynamic, agile and robust configuration, provisioning and sharing of infrastructure assets among coalition partners or armed forces, which are unmatched by our adversaries.

Readiness and Alternative Defence Uses

This work is technology readiness level (TRL) 2/3. Many of the SDC techniques have been prototyped in practical systems or environments, including the demos of controller placement and synchronization, resource sharing, robust network architecture, and learning in fragmented SDC. These techniques are ready for adoption, modification and enhancement for implementation on practical defence systems.

Organisations

Imperial College, Yale University, IBM US, Purdue University, ARL, Dstl

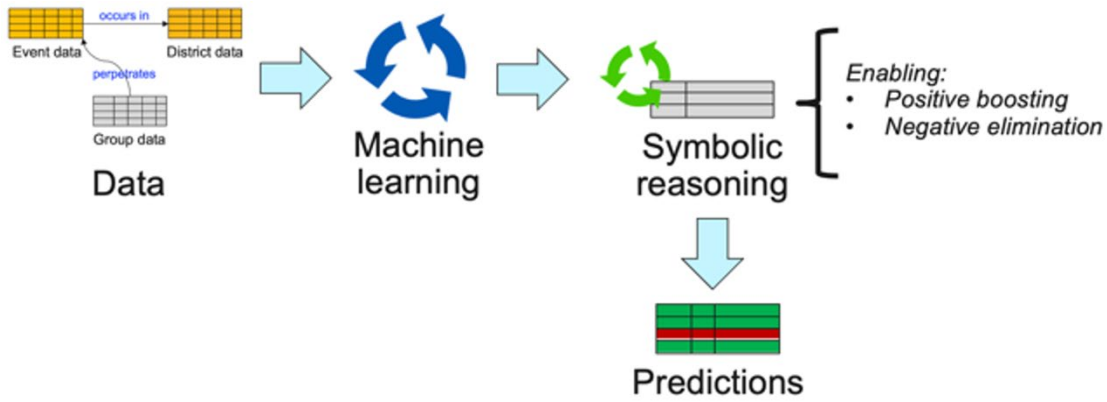
Enhancing Situation Understanding Through Negative-Ties Enhanced Pipelines

Military / Coalition Issue

Datasets are often focused on positive data, with any negative relationships or knowledge omitted. By explicitly capturing or inferring negative tie information, can we improve artificial intelligence (AI) or machine learning (ML) pipelines by taking into account this additional negative information?

Core idea and key achievements

We investigated terrorism data from the Indian sub-continent that was used in previous research, and identified a number of potential negative ties within that dataset. We defined a processing pipeline to add a symbolic post-processing step to a traditional AI/ML process, enabling the negative ties information to be used to boost or eliminate results proposed by the core process. We used a combination of data augmentation, by fusing the terrorist event data with related demographic census data, and inference to predict missing values, and to determine the features that most strongly predict the perpetrator of each incident.



We explore the potential for capturing such information from human users in a form that enables integration with the proposed pipeline, using techniques that are possible for less technical users, as well as supporting more technical data analysts through traditional methods such as Jupyter notebooks and Python code.

Implications for Defence

By placing such analytic methods into the hands of intelligence analysts it is possible for them to augment available data sources, both through definition of negative ties, and through inference of missing values. By using explainable methods, we were able to provide insight into the features that most affect the predictions, and highlight those cases that caused most confusion to the system.

Readiness & alternative Defence uses

This work is technology readiness level (TRL) 1/2. The research so far has defined the architecture for the post-processing pipeline in conjunction with any AI/ML model, and explored the potential techniques for the definition of negative tie information. Further research to measure the results both in terms of suability and performance improvements would be useful.

Resources and references

Verma, D., Yarlagadda, R., Gartner, S., and Felmlee, D. 2019. Location, location, location: Understanding patterns of terrorism in India (2007-2017), Using Artificial Intelligence Machine Learning. The International Journal of Technology, Knowledge, and Society 15, no. 4 (2019): 23-39.

Verma, D. C., Gartner, S. S., Felmlee, D. H., Braines, D., & Yarlagadda, R. (2020, April). Using AI/ML to predict perpetrators for terrorist incidents. In AI & ML for MDO Applications II (Vol. 11413, p. 114130G). International Society for Optics & Photonics.

Enabling rapidly formed human-agent coalition teams through extensible information exchange

Organisations

IBM US, Penn State, IBM UK

Federated Inference Using Self-Generated Policy

Military / Coalition Issue

When operation at the tactical edge or in any distributed environment, it may not always be possible to share data across sites or edge nodes. One approach to address this limitation is to federate the results of the model inference across site. In this demo, we will show a rule-based approach of federated inferencing, where the rules are self-generated based on contextual conditions.

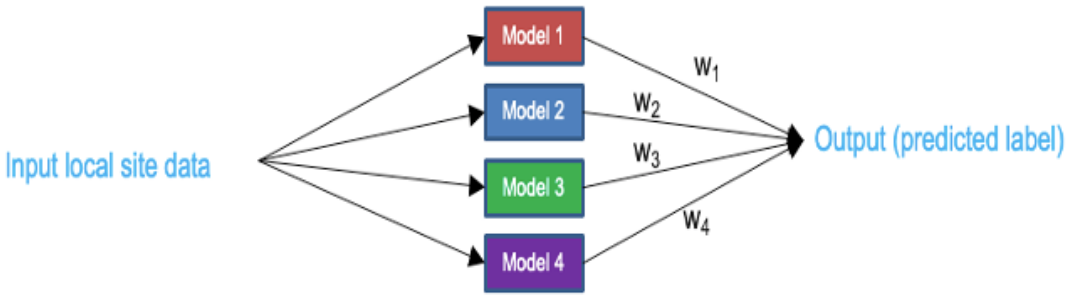
Core idea and key achievements

• Inferencing across the tactical edge when data cannot be shared for variety of reasons, e.g Security/Reliability and Network Bandwidth.

• Peer to peer connectivity to edge nodes when connectivity to central site of cloud is limited.

• Dynamic policy generation of classification ensemble weights to alleviate the need for end user to manually author and edit policies.

• Classification of events or data using ensemble approach across distributed edge nodes.



Implications for Defence

The key achievements in the previous section have implications in military defense settings as well as civilian. Classification of data, without connectivity to a shared or cloud server, may be challenging in an edge setting such as a military base. In some cases, trained models may not be mature enough to accurately classify certain data. Federated Inferencing can help in some cases by reaching out to nearby coalition bases to find more mature models to improve the accuracy of machine based classification.

Readiness & alternative Defence uses

Version 1 of the Edge AI SDK that incorporates all of the described functionality is currently available within IBM Research. Ready to prototype a military Edge AI production facility, and

experiment with a range of potential usage. Deployed in an experimental 5G Edge testbed at IBM Research.

Resources and references

Verma, Dinesh, Seraphin Calo, and Greg Cirincione. "Distributed AI and security issues in federated environments." Proceedings of the workshop program of the 19th International conference on distributed computing and networking. 2018.

Organisations

IBM US

Federated Learning in a Resource Constrained Networked Environment

Military / Coalition Issue

The ability to re-train or enhance the training of machine learning models while already deployed in order to adapt to local situations will be a key requirement. Being able to do so across a distributed set of compute capability would enhance robustness and potentially speed up learning convergence.

Core Idea and Key Achievements

This demonstration shows how the training of machine learning models can be allocated and distributed across an array of loosely networked nodes, and then recombined into a working model. In a highly distributed, low power environment, there may never be a single device with either enough processing power, or network connected for sufficient time, or with sufficient bandwidth in order to process the training set to completion in a single period of time or connectivity. This initial demonstration was based on work completed for the DAIS AFM 2019, and the underlying science has been continued and extended as part of recent work Adaptive Federated Learning in Resource Constrained Edge Computing Systems

Implications for Defence

This solution potentially allows machine learning model retraining on devices while in the field, in order to achieve better accuracy in local conditions. By being distributed this solution reduces training time by sharing the computational burden with other local devices, while increasing resilience by not having to rely on them.

Readiness and Alternative Defence Uses

This technology while most applicable to defence, can also be used in any situation where you may have a locally distributed compute capability across a network of smaller devices, but that the communications links back to a base may be insufficient to allow reasonable data transfer of ML models.

This work has been continued by combining it with some of the coreset modelling work and model pruning. Both of these help reduce the networking requirements between devices and so increase the utility of this solution at the edge of networks.

Resources and References

Conway-Jones, Dave, et al. "Demonstration of federated learning in a resource-constrained networked environment." 2019 IEEE International Conference on Smart Computing (SMARTCOMP). IEEE, 2019.

Organisations

IBM US, Imperial, PSU, IBM UK

Game Theoretic Resource Allocation in a Coaliltion

Military / Coalition Issue

In a coalition environment it makes sense to be able to share any available computing resources between the coalition members in order to help achieve the best overall outcome.

Core idea and key achievements

By using a game theoretic approach to resource demands and allocation we can show that we can achieve an allocation of resources among the partners, that is both Pareto optimal, and stable.

Implications for Defence

This solution potentially allows partners with varying computing resource capabilities and differing task objectives to rapidly form coalitions and a shared capabilities, by offering up any spare resource capacities that they have to the wider group, such that they can be made use of by those in need. The information shared to do this can be in an abstracted form so as not to compromise full details of national capability.

Readiness & alternative Defence uses

While the theoretical research is low TRL, this has been modelled in software and demonstrated at DAIS AFM 2019.

This concept aligns well with programs such as the NATO Protected Core Network (PCN) and Future Mission Network (FMN) where coalitions can potentially utilise shared networks.

Resources and references

Zafari, F., Leung, K., Towsley,D., Basu, P., Swami, A., Li, J., & Conway-Jones, D. (2019). "Demonstration of Game Theoretic Resource Allocation in a Coalition". AFM 2019.

Organisations

Imperial, UMass, Raytheon BBN, ARL, IBM UK

Gradient Free Attacks on Multiple Modalities

Military / Coalition Issue

Coalitions are often characterized by ad-hoc teams with distributed learning requirements. In such a setting, distributed learning is needed for collaborative situational understanding. However, since the learning is performed in an ad-hoc way, the coalition's decision may be compromised in multi-modalities by inference-time adversaries. This work will show the feasibility and the efficiency of inference time attacks, including images, text, and audio.

Core idea and key achievements

Nowadays, attacking a black-box AI system usually requires many queries of the system, which renders the attack algorithm impractical. Existing black-box approaches to generating adversarial examples typically require a significant number of queries, either for training a substitute network or performing gradient estimation. We introduce GenAttack, a gradient-free optimization technique that uses genetic algorithms for synthesizing adversarial examples in the black-box setting.

The key achievements are as follows:

• First, we show that the query efficiency of GenAttack leads to 237 times fewer queries than ZOO, one of the first black-box attack algorithms.

• Second, we demonstrate that efficient attack can be mounted on black-box models, indicating that further robustness of models needs to be attained in multiple domains, including images, text, and audio.

Implications for Defence

When coalitions perform learning in a distributed manner, it is possible that some parties may be compromised, and the machine learning model may be subverted during inference time. We show that black-box attacks can be mounted efficiently, and study these vulnerabilities can help us build more robust machine learning models.

Readiness & alternative Defence uses

GenAttack: Practical Black-box Attacks with Gradient-Free Optimization", in ACM GECCO, 2019. "Did you hear that? adversarial examples against automatic speech recognition", in NIPS 2017 Machine Deception workshop "Generating natural language adversarial examples", EMNLP 2018

Resources and references

Attack feasibility and demonstration of defence efficiency, level 3

Organisations

IBM US, UCLA,

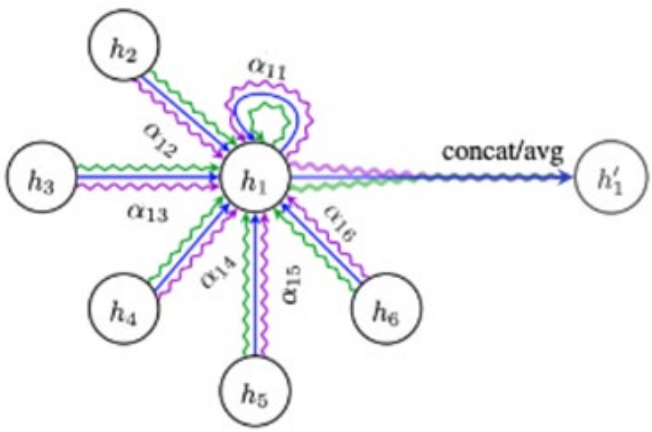
Graph Attention Networks for Congestion and Mobility Prediction

Military / Coalition Issue

Network topology in military networks, especially in mobile battlefield environments, constantly changes requiring to dynamically adapt network control decisions, resource allocations and other policies. Such policies are often realized with the help of Machine Learning (ML) which is a promising approach that can perform better than the traditional model+optimize methods. Yet, the aforementioned network dynamics bring significant challenges to the application of ML in these networks. Most of the ML models would require to be re-trained from scratch every time the topology of the network changes, e.g., when a group of mobile nodes fragment from the rest of the network thereby changing the network topology. Such re-training is not only time-consuming and computation-costly but in many cases impossible as training data may not be available/easy to access. Ideally, we would like the ML model to be robust to network topology changes and fragmentation events.

Core idea and key achievements

With the Software Defined Coalition (SDC) architecture proposed in the DAIS program, information about the status of the network (e.g., traffic loads, resource availability) and the mission (e.g., accomplishment of goals) are aggregated at a logically-centralized network entity, the SDC controller. Such information constitutes valuable data that typically ML methods applied in this context use to train their models. The SDC controllers have powerful computation resources and can leverage advanced ML methods such as Graph Attention (GAT) neural networks for model training. The unique benefit of GAT is that, once trained, a set of attention coefficient values (αij in the figure) are defined which are useful to make predictions even if the network topology changes. This generalizability property of GATs provides the desirable level of robustness to the ML model.



Key achievements include:

Robust machine learning models based on the Graph Attention (GAT) neural network architecture that are applicable even when network topology changes – no retraining of new models required.

Application of GAT method for two different use-cases; prediction of network traffic dynamics and mobility of nodes/fragmentation events.

Interpretability of decisions made by the neural network by explaining the attention coefficient values.

Implications for Defence

The GAT method will allow the development of robust ML models that are not affected by network topology changes and fragmentation events. This way, network operations can continue, and smart predictions and decisions can be still made without interruptions for model re-training.

Readiness & alternative Defence uses

TRL 2/3. Software prototype under preparation for the final DAIS meeting.

Resources and references

Related publications include: *Traffic prediction

Qin, Qiaofeng, et al. "Learning-aided SDC control in mobile ad hoc networks." Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications III. Vol. 11746. International Society for Optics and Photonics, 2021.

Organisations

Yale University, IBM US, IBM UK, ARL

Human Agent Reasoning Using Controlled Natural Language

Military / Coalition Issue

Data captured by humans is often expressed in semi-structured or unstructured text making it difficult to extract knowledge for integration within a common operational picture.

Core idea and key achievements

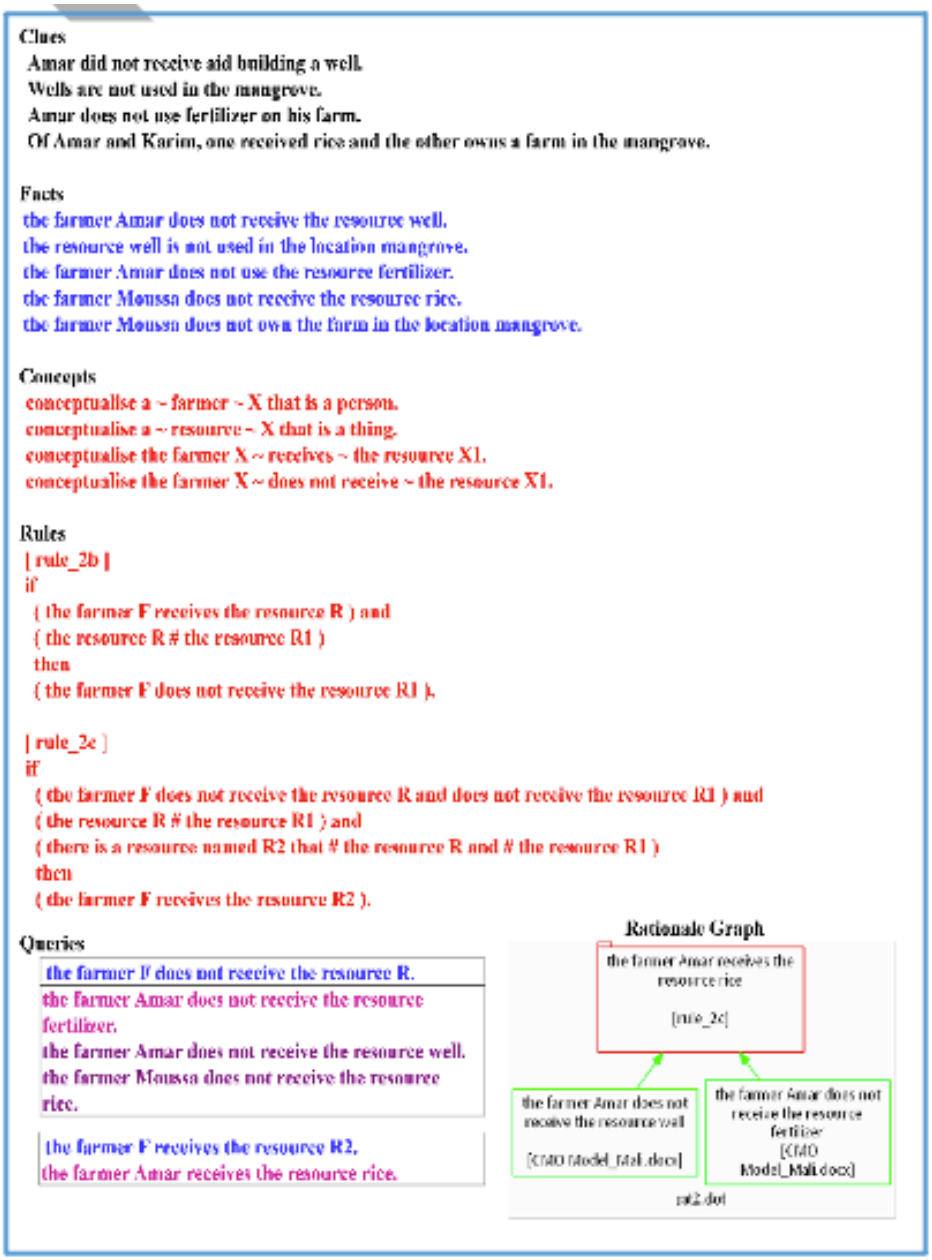
Conceptual model and initial natural language processing capability for use in fact extraction and human-AI agent problem solving. This system uses Controlled English (CE), a machine readable and human understandable language for fact extraction, and syntactic and semantic analysis, and may be used to represent concepts, facts, assumptions, and logical inference rules indicating relationship constraints. The CE system enables user to represent and evaluate the reasoning steps and rationale leading to conclusions, with the aim of identifying inconsistent hypotheses and cognitive biases. The CE system generates “rationale graphs” using natural language to illustrate the reasoning steps, the facts and premises leading to an inference. The CE system has been applied to numerous logic problems, most recently a food security problem for coalition partners to resolve.

Implications for Defence

In addition to natural language processing for fact extraction from semi-structured or unstructured data, multiple hypotheses can be tested iteratively using the CE system to generate rationale graphs. Unlike machine learning algorithms that may be challenging for humans to understand, the CE system’s formal representation of information in context and use of rationale graphs provide a level of transparency within human-AI agent reasoning to facilitate detection of inconsistent hypotheses and cognitive biases, such as the confirmation bias.

Readiness & alternative Defence uses

TRL 3. Conceptual model and CE system with base functionality. Collaborative Planning Model (CPM) was developed using a prior iteration of the CE system to represent and exchange the rationale for sub-plans between coalition planners. In a dynamic coalition planning experiment with Soldiers representing elements of a US and UK distributed Brigade, anecdotal evidence suggested that CPM facilitated the identification of inconsistent hypotheses within sub-plans.



Resources and references

Cheryl Giammanco and David Mott. Human-Agent Reasoning about Civil-Military Consideration Using Controlled Natural Language

Patel, Jitu, Michael C. Dorneich, David Mott, Ali Bahrami, and Cheryl Giammanco. "Making Plans Alive." Proc. 6th Knowledge Systems for Coalition Operations (2010).

Organisations

IBM UK, ARL DEVCOM

Identifying Patterns and Signatures of Negative Behaviours in Networks.

Military / Coalition Issue

Adversarial groups seek to disrupt otherwise stable coalitions through negative social network ties, which work to fracture alliances. Through our work here, we now understand the local structures that are foundational and operative within such networks. This better enables us to anticipate and identify future disruptive ties. This work informs the cognitive dimension within information environment operations, which can be used to protect decision-making of coalition forces and disrupt decisions of adversaries.

Core idea and key achievements

Much research has been conducted on social networks comprised of positive ties, while relatively little research has been conducted on their corollary, negative-tie social networks. Therefore, this work contributes to our understanding of how, at a foundational and structural level, negative-tie social networks differ from positive-tie social networks.

We use Exponential Random Graph Models (ERGMs) to statistically model these negative-tie and positive-tie social networks, enabling us to discover and specify the precise mechanisms that contribute to the development of such negative-tie social networks. Specifically, we find that both positive-tie and negative-tie social networks contain more reciprocated dyads than expected by random chance. In contrast, we find that positive and negative networks differ in two key ways: triadic closure defines positive-tie networks only, while degree distributions are heavily skewed within negative-tie networks only. These constitute unique structural patterns that can be identified in new networks, enabling us to detect the inception of negative ties and their effects within otherwise stable coalitions and alliances.

Implications for Defence

Now that these underlying, structural signatures have been identified within positive and negative networks, novel networks can be analysed with these precise signatures in mind. They will indicate the presence of benevolent and malevolent actors and ties within networks, contributing to the stability of coalitions as action can be taken against any negative, hostile actors and ties.

Readiness & alternative Defence uses

Social Network Analysis is needed to investigate these structural signatures in novel networks, while our work here serves as the standard against which new analyses can be compared. As we have identified, triadic closure and degree distribution can now be utilized to investigate to what extent actors and ties comprise negative ties within that network.

Resources and references

Key related work:

Cassie McMillan, Diane Felmlee and James Ashford "Reciprocity, transitivity, and skew: Comparing local structure in 40 positive and negative social networks." American Soc Assoc. 2021

Diane Felmlee, Cassie McMillan and Roger Whitaker "Dyads, Triads, and Tetrads: A Multivariate Simulation Approach to Uncovering Network Motifs in Social Graphs." Applied Network Science.

McMillan, Cassie, and Diane Felmlee. "Beyond dyads and triads: a comparison of tetrads in twenty social networks." Social Psychology Quarterly 83, no. 4 (2020): 383-404.

Cassie McMillan, Diane Felmlee, James Ashford and Emma Jayes "A Comparison of Local Structure in Positive and Negative Networks"

Felmlee, Diane, Cassie McMillan, Don Towsley, Kun Tu, Roger Whitaker, and Gavin Pearson. "Social Network Motifs: A Comparison of Social Groups."

Felmlee, Diane Felmlee, Cassie McMillan, Roger Whitaker, Mudhakar Srivasta, Cheryl Giammanco and Emma Jayes "Identifying Social Network Patterns with Exponential Random Graph Models"

Organisations

IBM UK, IBM US, Cardiff University, ARL, PSU

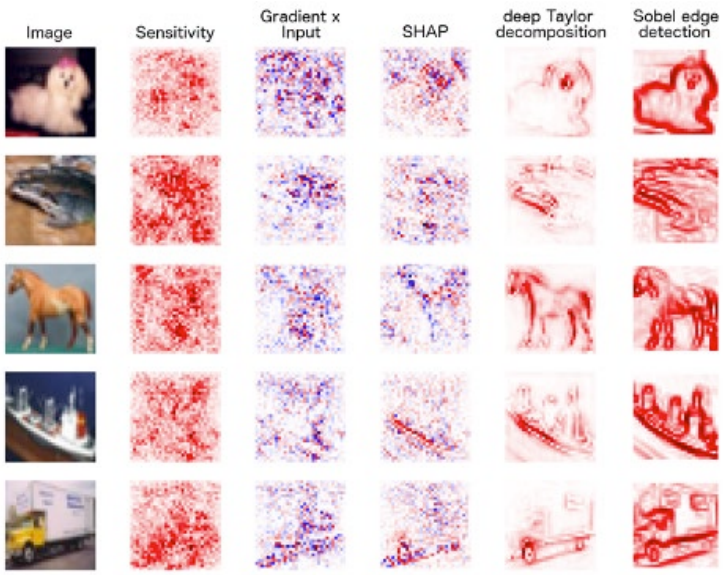
Inconsistency In Explanation Metrics

Military / Coalition Issue

Deep learning models have been shown to perform extremely well in a variety of domains and are being increasingly used for critical decision making. These models operate as black-boxes and rely on multiplicity of layers to extract abstract (often un-interpretable) features that are specifically tailored towards improving performance on the task. For efficient human-machine hybrid coalition networks, where the human decision maker can trust the model output, it is therefore imperative to augment model output with ``explanations'' that introduce transparency to the model decision making. Given this important role of explanations in establishing trust, several metrics have been proposed to assess their fidelity and faithfulness to the model decision. These metrics are important to determine the suitability of an explanation mechanism based on end-user requirement.

Core idea and key achievements

Saliency maps are used for providing post-hoc explanations. These maps are typically projections on the input domain quantifying the relevance of the input features towards the model decision. For example, in the context of images and videos, saliency maps indicate the relevance of each pixel towards the model output. Metrics have been proposed to assess the quality of saliency maps. We proposed a set of reliability measures, adopted from psychometric testing, to quantify the consistency of these saliency metrics. Using several tests, we demonstrated that (i) different metrics did not produce consistent ranking on the same sample and model, (ii) global saliency metrics, computed over all test samples also had high variance. Our results highlight that current metrics are highly unreliable and call on the community to develop better saliency metrics.



Implications for Defence

While explanations are being mandated as part of several regulatory policies (e.g., GDPR), their reliability and consistency also plays a key role in bootstrapping trust between human and machines.

Readiness & alternative Defence uses

Conceptual understanding demonstrated via initial experiments, level 1.

Resources and references

Tomsett, Richard, et al. "Sanity checks for saliency metrics." Proceedings of the AAAI conference on artificial intelligence. Vol. 34. No. 04. 2020.

Organisations

IBM UK, IBM US, Cardiff, ARL

Joint Reinforcement and Transfer Learning for Distributed Service Configuration in Fragmented Software Defined Coalitions

Military / Coalition Issue

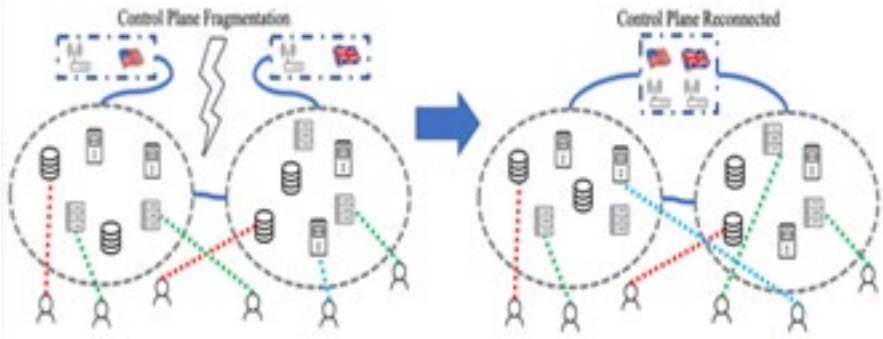
Military missions use infrastructure assets such as communication links, computational servers, data storage, databases, sensors and other resources. Dynamicity and agility of tactical operations demand near real-time configuration and provisioning of these resources. New capability requirements also include efficient re-configuration and and sharing of resources among coalition partners, despite infrastructure failures and fragmentations due to attacks or natural system evolutions.

Core idea and key achievements

A new architecture called Software Defined Coalitions (SDC) has been developed, which extends the existing Software Defined Networking (SDN), to support military missions. An SDC is composed of multiple domains, each of which has a set of available resources for sharing among coalition partners. Reinforcement learning (RL) has been proposed to control SDC under given operating conditions. To cope with sudden changes such as SDC fragmentation due to attacks by adversaries or natural system evolutions, a new technique has been developed to join RL with transfer learning (TL) in order to speed up the learning process for the RL for achieving close the optimal performance after SDC domains are reconnected following fragmentation. Thus, the joint RL and TL technique enhances the robustness of the SDC architecture in light of possible fragmentation. The DAIS team has also devised various techniques to realize the SDC capabilities; see related DAIS Outcomes on “Controller Synchronization and Placement,” “Resource Sharing in the SDC,” and “RL for Network Control,” respectively.

Key achievements include the development of:

- Joint RL and TL technique based on generative adversary network (GAN) to produce augmented training data for RL following SDC fragmentation
- Prototype of the proposed RL and TL technique to quantity the speed up of RL following SDC fragmentation



Implications for Defence

The new technique will enable defence to apply RL for control and sharing of infrastructure assets among armed forces despite possible infrastructure fragmentation. It supports efficient, agile and robust configuration and use of resources, which are unmatched by our adversaries. The joint RL-TL technique is also applicable to other defence systems where the operating environments suddenly change.

Readiness & alternative Defence uses

TRL 2/3. Many of the new techniques have been implemented or applied to practical systems, including the joint RL-TL for SDC fragmentation. Further work will help adapting the techniques to defence environments.

Resources and references

Zhang, Ziyao, et al. "Efficient Reinforcement Learning with Implicit Action Space." 4th Annual Fall Meeting of the DAIS ITA, 2020

Singla, Ankush, Elisa Bertino, and Dinesh Verma. "Preparing network intrusion detection deep learning models with minimal data using adversarial domain adaptation." In Proceedings of the 15th ACM Asia Conference on Computer and Communications Security, pp. 127-140. 2020.

Leung, Kin K., Anand Mudgerikar, Ankush Singla, Elisa Bertino, Dinesh Verma, Kevin Chan, John Melrose, and Jeremy Tucker. "Reinforcement and transfer learning for distributed analytics in fragmented software defined coalitions." In Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications III, vol. 11746, p. 117461W. International Society for Optics and Photonics, 2021.

Organisations

Imperial College, Purdue University, IBM US, ARL and Dstl

Leveraging Binarised Neural Networks for SDC Control

Military / Coalition Issue

The success of many military missions heavily relies on the timely access and analysis of data that often come from different sources that can be widely distributed across the military network. On the one hand, the distributed nature of the data complicates their analysis which often forces network operators to adopt simple distributed mechanisms for network control that run based on local data. On the other hand, the analysis of the data is difficult by itself and when not possible or too time-consuming the network operators have nothing but to rely on simple heuristic policies or empirical rules to manage their networks and support their missions.

Core idea and key achievements

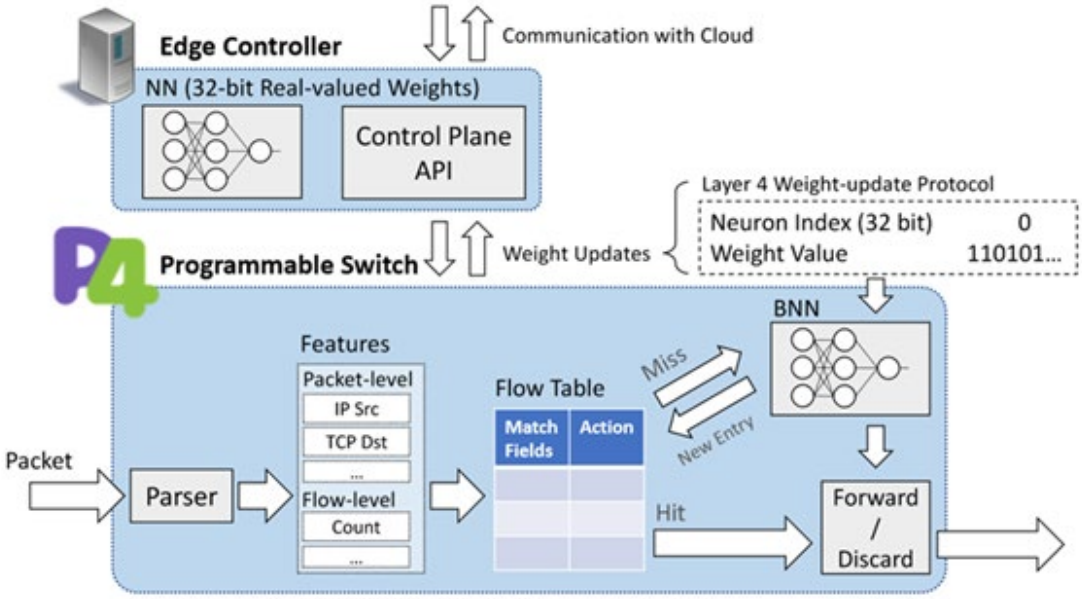
With the Software Defined Coalition (SDC) architecture proposed in the DAIS program, data like network traffic measurements, resource availability and mission states are gathered at one or multiple logically-centralized network entities, the SDC controllers. This centralization facilitates the analysis of data and the derivation of corresponding optimal network policies. In addition, the SDC controllers can use their available data and computation resources to train Machine Learning (ML) models to uncover hidden information in the data, predict otherwise unexpected events and improve their overall network operations. However, due to high network dynamics the controllers may be fragmented from the nodes they manage rendering impossible the access to the trained ML models to infer the network policies. An approach that is robust to network fragmentation events is therefore needed.

Key achievements include the development of:

The adoption of Binarized Neural Networks (BNN) to perform the inference of the ML model in a lightweight manner such that even resource-constrained mobile handheld devices can afford to run. Therefore, model inference is possible even when the controllers are fragmented from the rest of the network.

An extension of this ML architecture for collaborative training among multiple BNN models distributed in a network using the Federated Learning (FL) paradigm.

A proof-of-concept prototype implementation using the P4 Software Defined Network (SDN) programming language.



Implications for Defence

The BNN and P4 SDN language together will allow to run ML models everywhere in the military network even at lightweight handheld devices and this way make intelligent decisions for network control, resource allocation and dissemination of information according to the mission needs in a distributed, robust and flexible manner.

Readiness & alternative Defence uses

TRL 2/3. Software prototype based on the P4 language available.

Resources and references

Samples of related publications include:

Qin, Qiaofeng, et al. "Line-speed and scalable intrusion detection at the network edge via federated learning." 2020 IFIP Networking Conference (Networking). IEEE, 2020.

Qin, Qiaofeng, et al. "Learning-aided SDC Control with Programmable Switches." DAIS AFM 2020

Organisations

Yale University, Imperial College, IBM US, ARL

Minimising Coalition Information Exchange

Military / Coalition Issue

Communicating information between coalition entities requires there to be a common understanding of the language and the concepts being exchanged. Where information has to be rapidly conveyed, or where the communications are limited, the use of specialized symbols is often used but this requires the various parties to know the precise meaning of the symbols and in coalitions the same symbol may have different meaning. Is it possible to communicate information in an unambiguous way? Can communication bandwidth be minimised by conveying information symbolically at different levels of abstraction so that meaning is preserved?

Core idea and key achievements

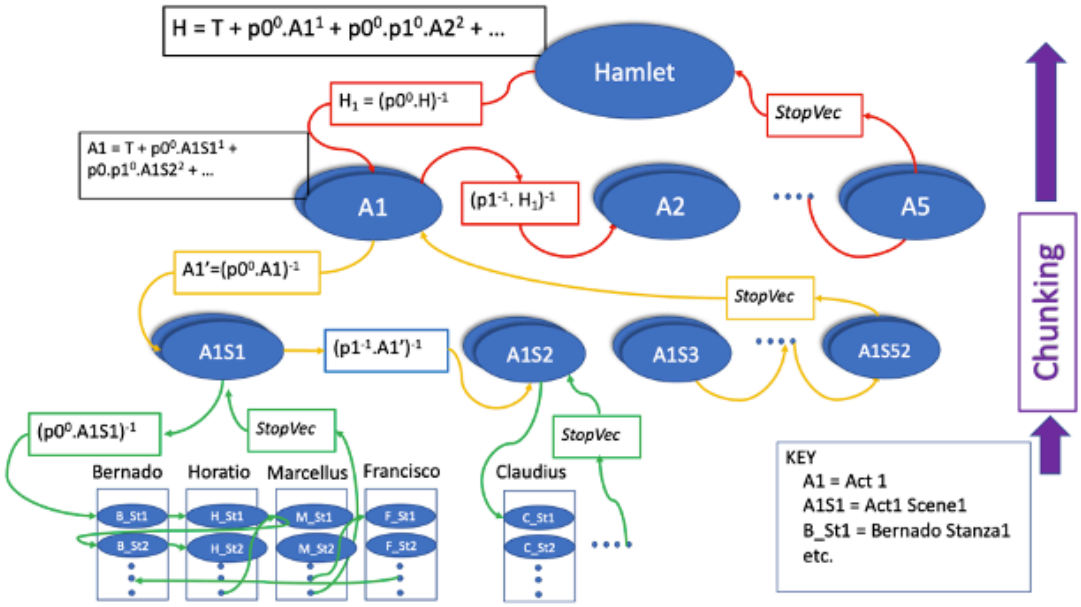
The core idea is to use semantic symbolic vectors as a unified way of exchanging information. We have developed a method of hierarchical vector binding where vectors at all levels of the hierarchy have the same structure but where vectors at higher levels in the hierarchy represent higher semantic abstractions of the underlying content of which they are composed. Information exchange is achieved by first transmitting a vector at the highest level of semantic representation. If the receiving party can interpret the vector, then no further exchange is required. If more information is required, then a request can be made for the vectors at lower semantic levels until a sufficient unambiguous understanding of the message has been achieved.

Implications for Defence

Using vector representations of information provides an important new way to rapidly convey information unambiguously in bandwidth constrained environments.

Readiness & alternative Defence uses

We have already demonstrated how information can be represented at different levels of semantic abstraction by encoding large documents (e.g. Shakespeare plays) where vectors at the highest level semantically represent the entire play whilst at the lower levels in the hierarchy the vectors can represent Acts or scenes down to the words spoken by individual actors). The same approach could be applied to a range of military requirements including intelligence reporting and command and control.



Resources and references

Simpkin, Chris, et al. "Coalition C3 Information Exchange Using Binary Symbolic Vectors." MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM). IEEE, 2019.

Organisations

IBM UK, Cardiff University, Dstl, IBM US

Model Poisoning Attacks And Defences In Federated Learning

Military / Coalition Issue

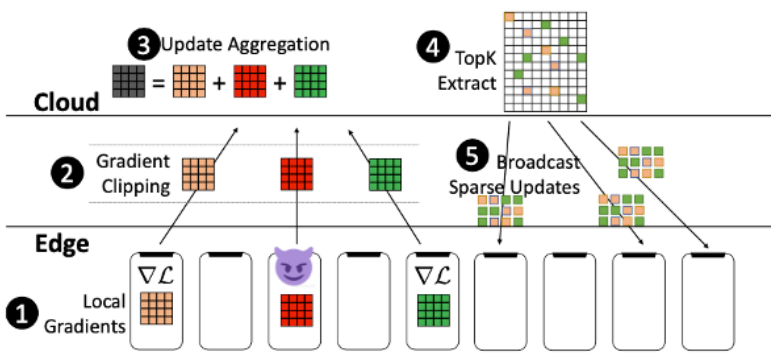
Federated learning is being increasingly adopted for information sharing and distributed model training between coalition members while simultaneously addressing their data sensitivity concerns. It allows the coalition members to perform local model training at the edge and only share insights in the form of model parameters with a central server. The server mediates a multi-round model training protocol, between the members, to assimilate all the local information into one global model. This global model, shared between the agents, is then used for critical decision making. It is thus imperative to analyse and assess adversarial mechanisms that can be used to introduce vulnerabilities into the global model, and ways to mitigate them.

Core idea and key achievements

There are two key achievements. First, we proposed model-poisoning attack to introduce targeted backdoor into the global model trained using federated learning. We demonstrated that it is possible for an adversary to manipulate the model weights and introduce targeted misclassification by the global model while maintaining attack stealth. This is a class of attacks different from the more traditional Byzantine attacks considered in prior works. We then evaluated the efficacy of the attack in a p2p setting. Second, we proposed a provable defence that combines ideas of top-k sparsification together with gradient clipping to bound the adversarial impact on the global model. We performed a large-scale evaluation of both the attack (under colluding attackers) and defence effectiveness.

Implications for Defence

Understanding the risks of deploying federated learning will allow the decision maker to remain vigilant of possible attacks. Proposed defence mechanism together with secure aggregation techniques could introduce resilience and reduce the risk of deployment.



Readiness & alternative Defence uses

Attack feasibility and demonstration of defence efficiency, level 3.

Resources and references

Bhagoji, Arjun Nitin, et al. "Analyzing federated learning through an adversarial lens." International Conference on Machine Learning. PMLR, 2019.

Tomsett, Richard, Kevin Chan, and Supriyo Chakraborty. "Model poisoning attacks against distributed machine learning systems." Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications. Vol. 11006. International Society for Optics and Photonics, 2019.

"Provably Defending Against Backdoor Attacks in Federated Learning with Sparsification" (under submission)

https://github.com/inspire-group/ModelPoisoning

Organisations

IBM US, IBM UK, ARL, Princeton

Model Pruning For Efficient Federated Learning In Coalitions

Military / Coalition Issue

In a military coalition, partners wish to train a global machine learning model utilizing data from all participating members. However, since the collected data can be sensitive, they have to be kept private to each member. Thus, we use a paradigm called federated learning, where only the model parameters, not the raw data, are shared among participants. To address the problem of limited communication and computation resources on military edge devices, we propose an adaptive pruning method that selects a proper subset of model parameters adaptively over time to accelerate training.

Core idea and key achievements

A machine learning model containing the full parameter set may be too large so that it either exceeds edge devices' capacities or slows down the training. On the other hand, using too few parameters may cause convergence to a suboptimal final accuracy. We balance the trade-off by constantly estimating the importance of each parameter and finding the subset of parameters that not only preserve the model accuracy but also accelerate the training process. We have achieved:

• Automatic acceleration on model training and inference and an implementation of a prototype (see figure below).

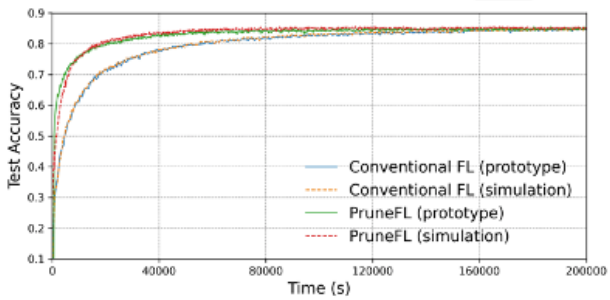


Figure: comparing training speed of conventional federated learning with our approach (both simulation and prototype).

• A mathematical proof of the convergence of our algorithm.

Implications for Defence

Our approach accelerates training or adaptation of a machine learning model in a dynamic environment where the edge devices have limited resources. It significantly reduces the time required to reach a target model accuracy, particularly benefiting time-sensitive military tasks.

Moreover, the final model is smaller than the original model, and therefore, it reduces inference time. This is an enabler for real-time processing in some tasks, for example, an object recognition task of a high frame rate video on a surveillance camera.

Readiness & alternative Defence uses

Our algorithm is easy to implement – we have developed a prototype and the code is open source.

Resources and references

- Paper: Y. Jiang, S. Wang, V. Valls, B. J. Ko, W.-H. Lee, K. K. Leung, L. Tassiulas, "Model pruning enables efficient federated learning on edge devices", in Workshop on Scalability, Privacy, and Security in Federated Learning (SpicyFL) in Conjunction with NeurIPS 2020, long talk, Dec. 2020.
- Code: https://github.com/jiangyuang/PruneFL

Organisations

Yale University, IBM US, Imperial.

Modelling the Emergent Behaviour of Human Social Groups

Military / Coalition Issue

Coalition operations require the ability to understand, predict and adapt to the behaviours of complex social situations involving sets of interacting actors and individuals; in which the behaviour of groups emerges from the psychological behaviours of individuals. This is wide ranging, from disaster relief, to extremists, to conflict and to adversarial online activities as seen through dis-information campaigns.

Core idea and Key Achievements

The research has established ways in which agents in computerised “agent-based models” can be embedded with individual psychological behaviours. Then “multi-agent models” are used to extend the psychological behaviours to groups, resulting in the evolution of collective effects that define how group behaviours emerge. This provides insight into the factors which impact the cultural spread of particular behaviours, including negative social behaviours such as hate, and the way in which human groups form, sustain and evolve. The research has focused on i) prejudice, ii) identity, and iii) cognitive dissonance.

Implications for Defence

The “multi-agent models” make it possible to explore particular scenarios of how groups may evolve. This can aide training, planning, and wider understanding of how human psychology, at the individual level, can influence the collective behaviour and evolution of groups, such as under stress or cultural distrust. Further, it provides insight into the interactions motivating behavioural responses in individuals such as devotion to a cause.

Readiness and Alternative Defence Uses

The research has established the concepts and capabilities at a fundamental level, resulting in two Nature publications (Scientific Reports) and a further pending IEEE transactions publication. This represents low technology readiness level (TRL) research. However, there is substantial potential to translate this into online social networks (e.g., the detection of strength of identity fusion for online analysis of social media interactions) to address, for example, scenarios concerned with identity fusion and devotion to a cause.

Resources and References

Whitaker, Roger M., Gualtiero B. Colombo, and David G. Rand. "Indirect reciprocity and the evolution of prejudicial groups." Scientific reports 8, no. 1 (2018): 1-14.

Whitaker, R. M., Colombo, G. B., & Dunham, Y (2021). The evolution of strongly-held group identities, through agent-based cooperation Scientific reports, 11(1), 1-16.

Whitaker, R. M., Colombo, G. B., Turner, L., Dunham, Y., Doyle, D., Roy, E.M., Giammanco, C.A., (2021), The Coevolution of Social Networks and Cognitive Dissonance. IEEE Transactions on Computational Social Systems, Accepted for publication.

Whitaker, Roger M., Diane Felmlee, Dinesh C. Verma, Alun Preece, and Grace-Rose Williams. "From evolution to revolution: understanding mutability in large and disruptive human groups." In Next-Generation Analyst V, vol. 10207, p. 1020703. International Society for Optics and Photonics, 2017.

Whitaker, Roger M., Liam Turner, Gualtiero Colombo, Dinesh Verma, Diane Felmlee, and Gavin Pearson. "Intra-group tension under inter-group conflict: a generative model using group social norms and identity." In International Conference on Applied Human Factors and Ergonomics, pp. 167-179. Springer, Cham, 2017.

Organisations

Cardiff, Penn State, Yale, ARL, Dstl, IBM

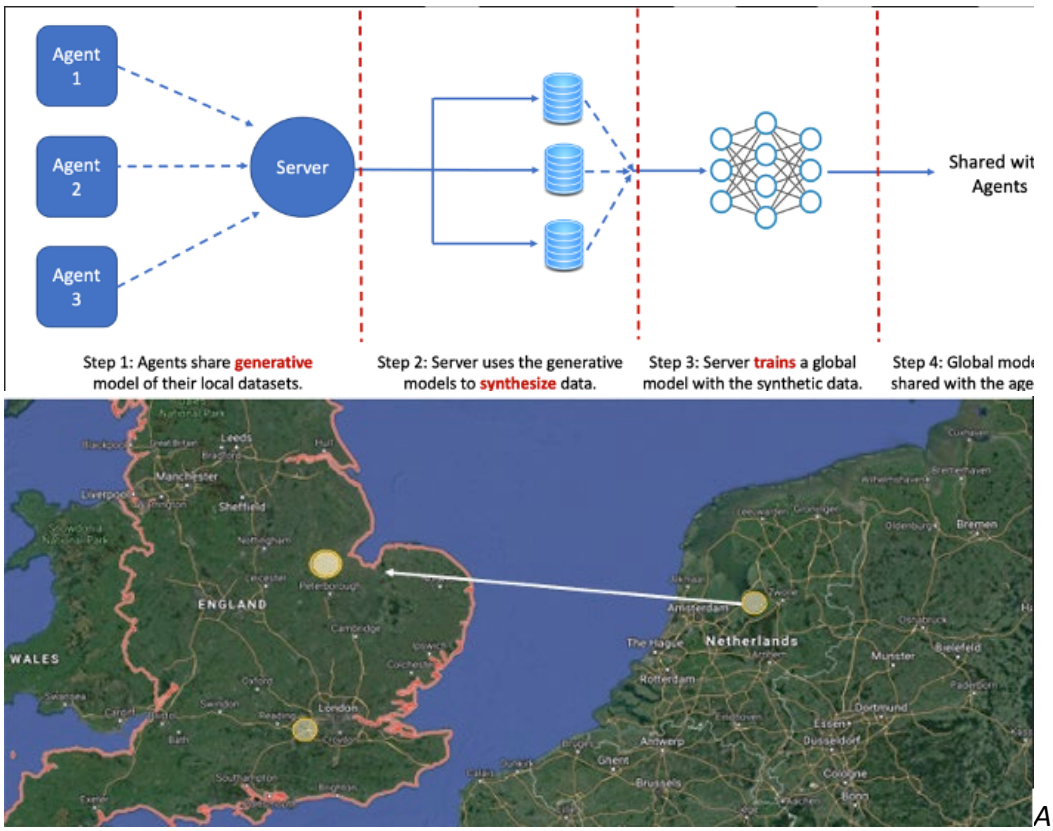
One Shot Federation for Coalition Model Sharing

Military / Coalition Issue

One Shot Federation is a collaborative machine learning method that addressed agent bandwidth and synchronization concerns. This is particularly relevant when operating in environments with disrupted and intermittent networks, and when there is a need to share knowledge with other partners in bandwidth-constrained environments. Bandwidth is a constraint for edge devices, and sharing large volumes of traffic is often prohibitive. Additionally, synchronization of model updates between different agents is often restrictive in real deployments.

Core idea and key achievements

One Shot Federation allows each agent to share information about their local data distribution, instead of the raw data, that a server synthesizes samples from. Each agent's samples are utilized to collaboratively train a machine learning model with, that is equivalent in performance to a model produced by centralized training. This method circumvents the bandwidth issue that would be created via centralized training, as agents do not have to send their data to each other, and the server use does not require synchronization of model updates.



Agent 2, located in the Netherlands, is sending their model to Agent 1, where a server will combine the models through One Shot Federation

Implications for Defence

Our technical innovation allows incremental sharing and consolidation of strategic information from members of a coalition. Members can train local models and only share their model parameters, and maintain the privacy of the collected data while simultaneously contributing to the coalition objective through information sharing. A significant benefit of our approach is that the model aggregation (fusion) can be performed asynchronously and does not require the coalition members to be actively sharing their model updates at the same time.

Readiness & alternative Defence uses

Readiness level is laboratory demonstration, level 3.

Organisations

IBM US, Imperial College, Pennsylvania State University, Purdue University, University College London

Online Multi-Task Learning With Long-Term Memory

Military / Coalition Issue

In military operations we may have a collection of mobile devices that are receiving data from their surroundings, and we may wish to perform some online machine learning task with their collected data. We assume that the machine learning task would be aided by the knowledge of the "environment" that a particular mobile device is currently in. Due to the mobile devices being "mobile" the devices themselves will move between different environments over time. The devices do not necessarily have to move together and hence different devices will be in different environments at different times. We assume we have no a-priori knowledge of the different environments themselves, or when a particular device changes environment, and hence this work is about how to learn these things online.

Core idea and key achievements

We consider two types of online machine learning task which are fundamental in the literature:

• Prediction with expert advice. We assume we have a finite set of algorithms ("experts"). At any point in time these algorithms observe some data (e.g. the current instance of the device's video feed) and issue a prediction (e.g. whether a threat is detected). The algorithms themselves have different performances in different environments.

• Linear interpolation with a Reproducing Kernel Hilbert Space (RKHS). We have a (potentially infinite) set of functions that map possible data observations to real numbers. A function is consistent with the observed data if it maps each piece of observed data to 0 or 1 (its prediction about that datum). The functions form an RKHS which applies a "complexity" to each function. Functions that are less complex and more natural are easier to learn. The functions vary in predictive performance over the different environments.

In both tasks we learn if the prediction is correct immediately after it is made. We adapt both these learning tasks to our model and for them develop two very different algorithms. This work was done over two papers, both published at NeurIPS 2020: the paper entitled "online matrix completion with side information" developed the mathematical tools needed for the RKHS algorithm, whilst the paper entitled "online multitask learning with long-term memory" introduced both the algorithms themselves.

Implications for Defence

This project develops techniques for performing machine learning on mobile devices which move between different environments.

Readiness & alternative Defence uses

The paper entitled “online multitask learning with long-term memory” contains the pseudo-code for both algorithms

Resources and references

Herbster, Mark, Stephen Pasteris, and Lisa Tse. “Online Multitask Learning with Long-Term Memory.” arXiv preprint arXiv:2008.07055 (2020).NeurIPS 2020

Herbster, Mark, Stephen Pasteris, and Lisa Tse. “Online Matrix Completion with Side Information.” Advances in Neural Information Processing Systems 33 (2020).

Organisations

UCL

Online Resource Allocation Using Distributed Bidding Approaches

Military / Coalition Issue

It is important that coalition partners are able to share edge computing resources while disclosing only the information they desire. The set of algorithms we developed allow clients to disclose the utility (importance) of their jobs to server, or not, thus allowing coalition partners to keep some aspects of their jobs private. Likewise, coalition partners do not have to share information about their servers with their partners.

Core idea and key achievements

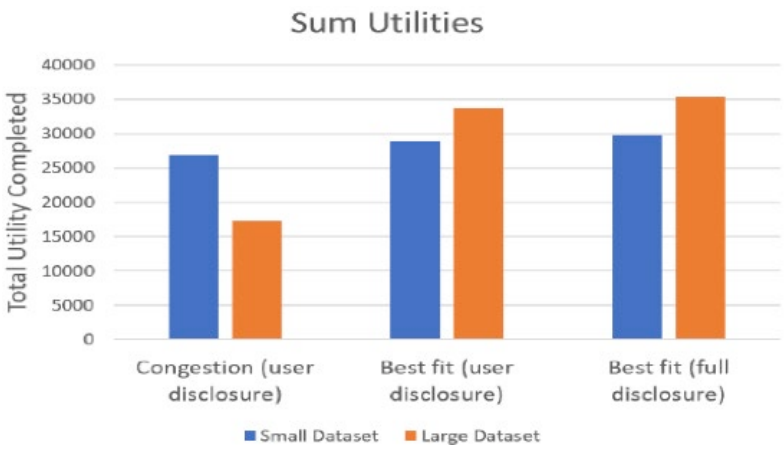
We devised and evaluated algorithms that allocate resources to users for submitted jobs. We examined various auction mechanisms that arrive at very close to optimal solutions and use centralized knowledge. We also devised simple distributed bidding algorithms which can quickly allocate resources to jobs in which the servers do not coordinate. The algorithms consider requirements for memory, bandwidth, processing, and deadlines. Our results show our algorithms are close to optimal.

Implications for Defence

Coalition partners may share edge-based computing resources without having to disclose key attributes of their jobs. This will provide a much more scalable infrastructure for performing real-time distributed analytics tasks which require high computational power. This will increase the pace at which information is available to the field.

Readiness & alternative Defence uses

The algorithms have been developed and tested in a simulation environment. More testing is required on real systems.



Resources and references

Stein, Sebastian, Mateusz Ochal, Ioana-Adriana Moisoiu, Enrico Gerding, Raghu Ganti, Ting He, and Tom La Porta. "Strategyproof reinforcement learning for online resource allocation." (2020): 1296-1304.

C. Rublein, F. Mehmeti, S. Stein, T.F. La Porta, "Online Resource Allocation in Edge Computing Using Distributed Bidding Approaches", accepted at IEEE MASS 2021.

Bi, Fan, Sebastian Stein, Enrico Gerding, Nick Jennings, and Tom La Porta. "A truthful online mechanism for allocating fog computing resources." (2019): 1829-1831.

M. Towers, F. Mehmeti, S. Stein, T.F. La Porta, C. Rublein, G. De Mel, Auction-based Mechanisms for Resource-elastic Tasks in Edge Cloud Computing, submitted.

Organisations

Penn State University, University of Southampton, IBM, IBM-UK

Policy Generation for Edge Devices in Coalitions

Military / Coalition Issue

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.

Core idea and key achievements

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. The key achievements addressed these gaps to provide a machine learning based policy learning system demonstrated by edge devices learning how to behave when presented with a new context, situation or environment. The system developed utilises a grammar and as such does not suffer with the explainability problems of many black box machine learning systems. This is because the grammar can be inspected and understood by human users in order to fully articulate the generative policy model under which the device is currently operating.

Implications for Defence

The demonstration shows autonomous edge devices being introduced to a context with which they are not familiar. The edge devices must learn how to behave and they can do this based on the behaviour of other devices in their local area. They are able to do this in isolation on the edge device, without connection to back end infrastructure and thus being compatible with slow and unreliable communication links. Whilst the demonstration is shown for edge devices, the technology can easily be applied to any policy learning scenario either at the edge or within the back office coalition military systems.

Readiness & alternative Defence uses - Check URL

The main technology utilised is an inductive machine learning technique developed during the DAIS programme, known as FastLAS. This has been released as open source software on GitHub at https://github.com/spike-imperial/FastLAS. It has been used throughout the DAIS demonstrations and experiments in this field and is still under active development. The key functionality is in place and would require hardening for operational military usage alongside development of new code into a wider policy learning system.

Resources and references -

White, Graham, Daniel Cunnington, Mark Law, Elisa Bertino, Geeth De Mel, and Alessandra Russo. "A Comparison Between Statistical and Symbolic Learning Approaches for Generative Policy Models." In 2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA), pp. 1314-1321. IEEE, 2019.

Cunnington, Daniel, Graham White, Mark Law, and Geeth de Mel. "A demonstration of generative policy models in coalition environments." In International Conference on Practical Applications of Agents and Multi-Agent Systems, pp. 242-245. Springer, Cham, 2019.

Aspis, Yaniv, Daniel Cunnington, Mark Law, Alessandra Russo, Krysia Broda, Jorge Lobo, Ankush Singla, Elisa Bertino, and Dinesh Verma. "Continuous Federated Learning of Global Policies in Coalition Environments."

White, Graham, John Ingham, Mark Law, and Alessandra Russo. "Using an asg based generative policy to model human rules." In 2019 IEEE International Conference on Smart Computing (SMARTCOMP), pp. 99-103. IEEE, 2019.

Law, Mark, Alessandra Russo, Elisa Bertino, Krysia Broda, and Jorge Lobo. "Fastlas: scalable inductive logic programming incorporating domain-specific optimisation criteria." In Proceedings of the AAAI Conference on Artificial Intelligence, vol. 34, no. 03, pp. 2877-2885. 2020.

Vilamala, Marc Roig, Mark Law, Harrison Taylor, Tianwei Xing, Luis Garcia, Dave Braines, Dan Cunnington et al. "Towards Maintaining and Reusing Complex Event Processing Systems."

Cunnington, Daniel, Irene Manotas, Mark Law, Geeth de Mel, Seraphin Calo, Elisa Bertino, and Alessandra Russo. "A generative policy model for connected and autonomous vehicles." In 2019 IEEE Intelligent Transportation Systems Conference (ITSC), pp. 1558-1565. IEEE, 2019.

Organisations

IBM UK, Imperial, Purdue

Predicting Spread of Negative Attitudes and Behaviors in Social Networks

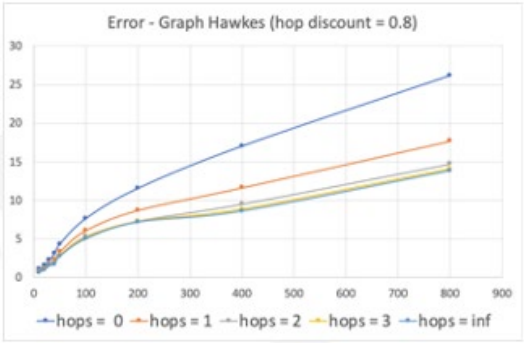
Military / Coalition Issue

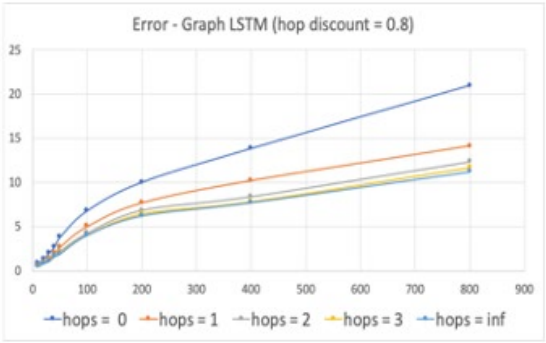
Understanding user behavior on a social network is a challenging problem. It is important to understand how this behavior changes in terms of the influencer, the influenced, and the temporal dimension.

Core idea and key achievements

This work uses utterance of curse words as a proxy for user behaviour. Utterance of curse words typically exhibit both temporal and spatial clusters, i.e., the propensity of a node in a social network uttering a curse work is highly dependent on the node's neighbour uttering curse words in the recent past. This work introduces a new modelling technique, based on Graph LSTMs (Long Short-term Memory), that improves predictability of who and when will utter curse words next. Evaluations on the Twitter dataset show that considering network effects improves prediction performance by over 30%, in comparison with traditional statistical models such as the Hawkes Point Process.

Unlike prior efforts, this new model fundamentally captures the behavior both along the graph and the time dimension. Core to the construct is the graph convolution operator that convolves a signal (number of curse word utterances per unit time) over a neighborhood in a graph. Combined with a LSTM layer the model captures how the signal spreads over time on the graph structure. In addition, the new model supports what-if analysis in the form of predicting how changes to the graph structure or how initial point of infusion (who uttered the curse word first) can influence its overall spread on the social network.





We have tested our approach for modeling the spread of curse words on Twitter. This new approach is compared with an adaptation of Hawkes Point Process to graphs, wherein an entity in a social network may be excited (to utter a curse word) based on the total excitation potential of all the nodes in a k-hop radius around the said node. The proposed approach shows over 30% improvement over the baseline for capturing the positional (who) and temporal (when) dynamics of curse word spread on a social network.

Implications for Defence

This new method offers a method of studying the spread of opinions on a social network. It can be used for what-if analysis when polarizing opinions are injected into a social network through select entities.

Readiness & alternative Defence uses

This work is technology readiness level (TRL) 3-4. It provides a technique that can be immediately engineered and applied. However more experiments may be required for assess the suitability of the technique for a target social network.

Resources and references

NASN 2021: M. Srivatsa, Diane Felmlee, Roger Whitaker, Supriyo Chakraborthy, Cheryl Giammanco. Modeling Spread of Curse Words on a Social Network

Organisations

IBM US, PSU, Cardiff, ARL

Privacy-Preserving Learning Techniques Based on Generative Adversarial Networks

No video

Military / Coalition Issue

In many situations, coalition partners are available to transfer knowledge among each other in order to reduce the need for training datasets, provided that the privacy of their own datasets is protected.

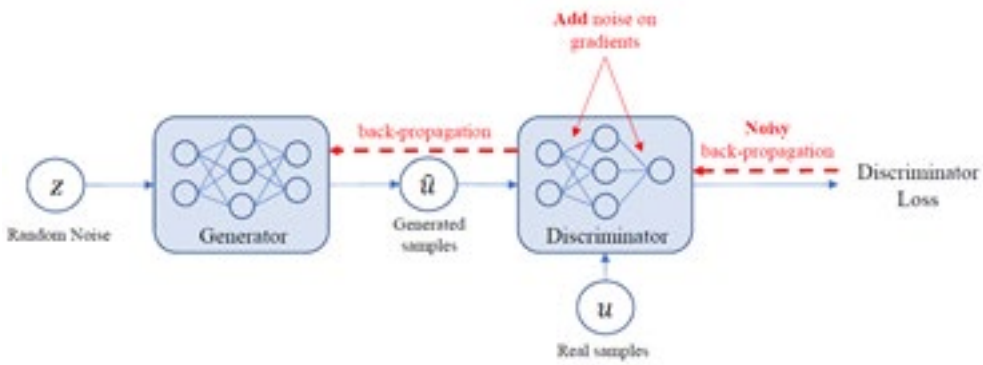
Core idea and key achievements

Our approach builds on our previous work [1] that uses generative adversarial networks (GANs) to adapt a model learning at a source party for use in a target party that has limited training dataset. Our approach thus allows a source domain to perform transfer learning by domain adaptation based on GANs and at the same time keep private its training dataset. The approach is based on the well-known differential privacy (DP) model; an important parameter in this model is the budget parameter epsilon; recommended values for epsilon are values not higher than 1.

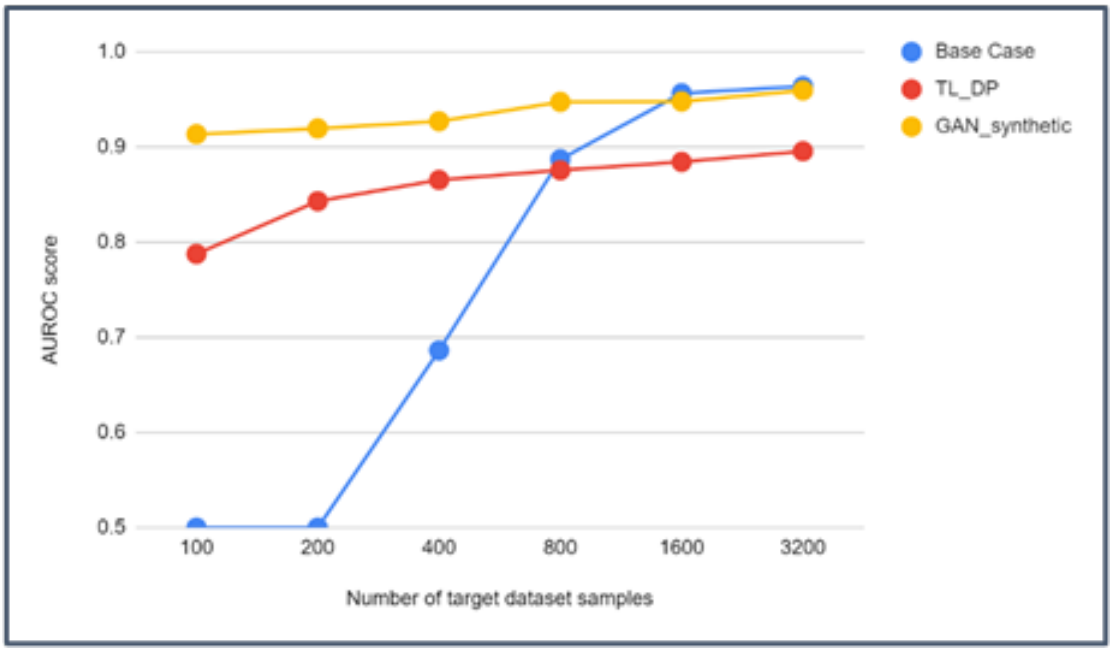
The approach consists of two steps:

The first step uses a differentially-private GAN (DP-GAN) to generate a privacy-preserving dataset from the source dataset; the DP-GAN adds noise to the gradient of the discriminator during training.

The second step uses another GAN to generate the target domain classifier using as input the synthetic dataset and the small target domain dataset.



Results show that our approach achieves good accuracy; see the results below for experiments with value of epsilon equal to 0.9833558483.



Implications for Defence

Our approach will support transfer learning, thus providing an approach to address the scarcity of training datasets, while at the same time ensuring data privacy.

Readiness & alternative Defence uses

Provides a technique that can be immediately engineered and applied. However more experiments may be required for assess the suitability of the technique for different application domains and data.

Resources and references

A paper is under preparation.

Organisations

Purdue, IBM US

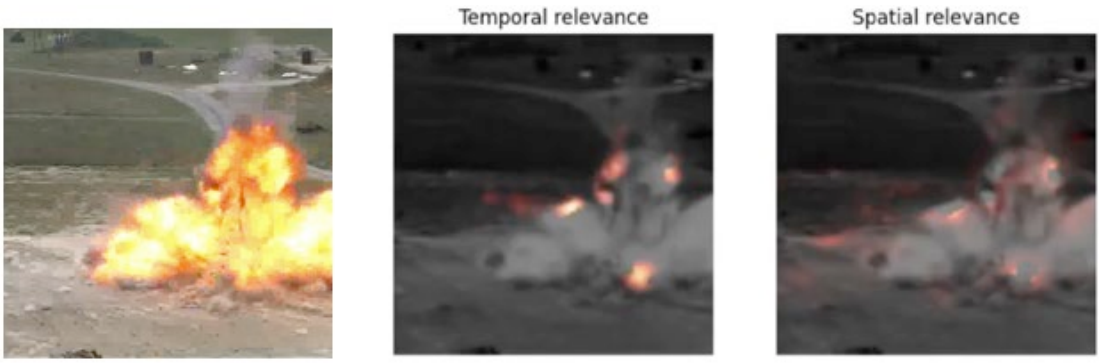
Real-Time Explainable Artificial Intelligence: Time-Series and Multi-Modal Data

Military / Coalition Issue

As artificial intelligence (AI) based assets are increasingly employed in operating environments, and operators need to make decisions based on the output of such assets, they need to be able to "calibrate their trust" in the asset see also Achieving Rapid Trust of Adaptable Artificial Intelligence Systems; explainable AI (XAI) is a key part of trust calibration. Commonly, XAI is seen as a matter of being able to ask an AI system, "Why?" in response to an output. In real-time settings such as monitoring live sensor feeds it can be more convenient to see live explanations at least while an operator is becoming familiar with a new asset.

Core Idea and Key Achievements

The Selective Relevance XAI technique operates in real-time on an edge processor and highlights changes in continuous time-series data, for example, between frames of a video or in an audio stream. Moreover, it can operate on multiple modalities simultaneously, filtering the most relevant and fast-changing features in a set of multimodal sensor feeds. In the images below of an explosion detected by a 3D Convolutional Neural Network, Selective Relevance highlights the origin of the blast (centre, bottom) and parts of the leading edge of the debris cloud as being the most relevant temporal (motion) features of the detected event; other elements of the debris are highlighted as being of spatial relevance (right).



Implications for Defence

By highlighting temporal and multimodal features, Selective Relevance allows an operator to receive explanations that focus on the most relevant features and modalities, i.e., highly tailored and compact explanations. These reveal what the AI is (and is not) paying attention to in a scene, across multiple senses (vision, audio, and others). The end-goal is improved trust and hence robustness of the human-machine system. Paying attention to the most relevant temporal features in multiple modalities also guards against adversarial attacks via spoof input – an attacker

would need to spoof the input in multiple modalities in a way that generated false conclusions and plausible explanations for those false conclusions.

Readiness and Alternative Defence Uses

This work is technology readiness level (TRL) 3/4. Selective Relevance is available as open source software integrated into the PyTorch framework via our torchexplain package. The approach has been tested with multiple deep neural network video processing architectures including C3D, MARS, MERS and SlowFast.
In addition to the default audio-video deployment (SAVR: Selective Audio Visual Relevance) Selective Relevance is applicable to other time-series data (e.g. electro-magnetic spectra and cyber traffic).

Resources and References

Hiley, Liam, et al. "Discriminating spatial and temporal relevance in deep Taylor decompositions for explainable activity recognition." arXiv preprint arXiv:1908.01536 (2019).

Taylor, Harrison, et al. "VADR: Discriminative multimodal explanations for situational understanding." 2020 IEEE 23rd International Conference on Information Fusion (FUSION). IEEE, 2020.

Hiley, Liam, et al. "SAVR: Selective Audio Visual Relevance for Explainable Coalition Situational Understanding (demo)" DAIS Annual Fall Meeting 2020

Organisations

Cardiff University, IBM US, IBM UK, ARL

Reinforcement Learning For Military Network Control

Military / Coalition Issue

Efficient and robust control and management of large communication and computation infrastructures for tactical use are critically important to mission success. Traditional optimisation-based control techniques usually over-simplify the original problems and ignore the availability of network operation data. To address these shortcomings, reinforcement learning (RL) has been widely applied for system control. However, state-of-the-art RL often encounters issues such as huge state-action spaces, inefficient knowledge representation, dynamic changes of environments, and violation of underlying mathematical assumptions. These factors greatly increase computational complexity and hinder learning, thus significantly limiting the applicability of RL for national defence.

Core idea and key achievements

To overcome the inadequacies of optimisation-based control paradigms, RL has been applied to design and control the novel architecture named Software Defined Coalitions (SDC) for sharing infrastructure assets. Specifically, the DAIS team has developed new techniques to address various RL issues for large-scale infrastructures, including state-action space explosion, inefficient knowledge representation of states and actions, learning of sudden changes in operating environments (e.g., SDC fragmentation), and violation of underlying mathematical assumptions. The new techniques not only offer advantages over the optimisation-based methods, but also greatly reduce the computation and learning time, thus extending the applicability of RL to management of very large systems such as SDC. Please also see the related DAIS Outcomes on “Controller Synchronization and Placement,” “Resource Sharing in SDC,” and “Joint Reinforcement and Transfer Learning for Fragmented SDC.”

Key achievements include the development of:

Efficient deep RL techniques to overcome huge state-action spaces

Techniques for state-space decomposition and hierarchical RL

Jointly trained state-action embeddings to speed up learning for RL

Joint RL and transfer learning (TL) techniques for dynamic changes in operating environments such as SDC fragmentation

Techniques to solve non-Markov process and extend RL applicability

Implications for Defence

The new techniques will enable defence to apply RL for real-time control and sharing of infrastructure assets among armed forces. They support efficient, agile and robust configuration and use of resources, which are unmatched by our adversaries. The techniques are also applicable to other systems such as radio spectrum sharing in electromagnetic warfare.

Readiness & alternative Defence uses

TRL 2/3. Many of the new techniques have been implemented or applied to practical systems, including the joint RL-TL for SDC fragmentation. Further work will help adapting the techniques to defence environments.

Resources and references

Zhang, Ziyao, et al. "Macs: Deep reinforcement learning based sdn controller synchronization policy design." 2019 IEEE 27th International Conference on Network Protocols (ICNP). IEEE, 2019.

Pritz, Paul J., Liang Ma, and Kin K. Leung. "Joint State-Action Embedding for Efficient Reinforcement Learning." arXiv e-prints (2020): arXiv-2010.

Leung, Kin K., et al. "Reinforcement and transfer learning for distributed analytics in fragmented software defined coalitions." Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications III. Vol. 11746. International Society for Optics and Photonics, 2021.

Zhang, Ziyao, et al. "Efficient Reinforcement Learning with Implicit Action Space." 4th Annual Fall Meeting of the DAIS ITA, 2020

Zhang, Ziyao, et al. "State Decomposition, Distributed and Hierarchical Reinforcement Learning for SDC." 4th Annual Fall Meeting of the DAIS ITA, 2020

Chen, Zheyu, et al. "Learning Technique to Solve Non-Markovian Decision Process for Networked Resource Allocation ."

Organisations

Imperial College, IBM US, Purdue University, Yale University, Dstl, ARL

Resource Sharing In Software Defined Coalitions To Support Coalition Missions

Military / Coalition Issue

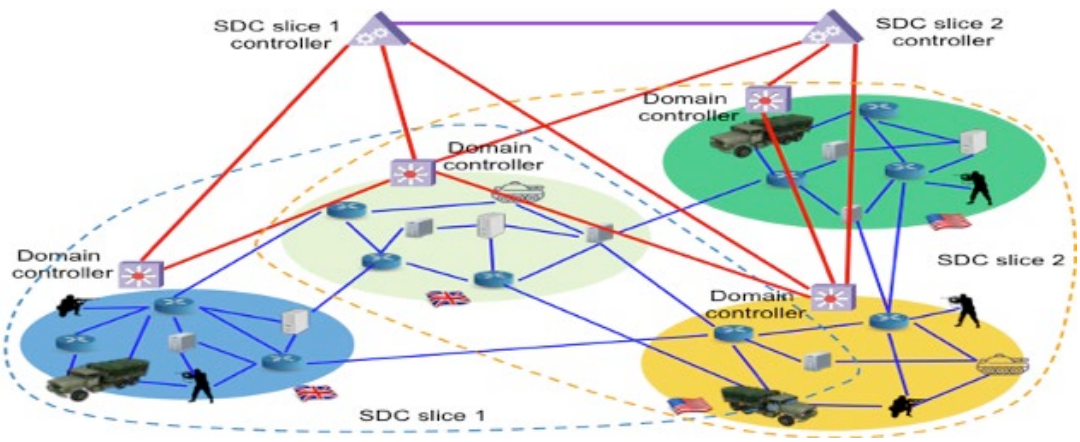
Military missions require the use of infrastructure assets including communication links, computational servers, data storage, databases, sensors, and other resources. Dynamicity and agility of military operations demand near real-time configuration, re-configuration and provisioning of these resources, while supporting efficient and robust sharing of assets across armed forces or coalition partners. State-of-the-art techniques cannot currently achieve this.

Core idea and key achievements

A new architecture called Software Defined Coalitions (SDC) has been developed, which extends the existing Software Defined Networking (SDN) paradigm, to resolve the aforementioned issue. A typical SDC is composed of multiple domains, each of which has a set of available resources. Each domain contains one domain controller and the controllers are connected through the control plane to exchange control information. The software control logic implemented in controllers can be programmed to enable rapid configuration and control of resources. We focus here on resource allocation and sharing in SDC, which includes both centralized and distributed solution techniques for single and multiple objective functions. Other SDC achievements are described in related DAIS Outcomes on “Controller Synchronization and Placement” and “RL for Network Control” and “Joint Reinforcement and Transfer Learning for Fragmented SDC.” Key achievements on SDC resource sharing include the development of:

Distributed technique to optimize trade-offs between communications and computation in sensor networks

Optimization-based techniques (with single objective function) for allocation and sharing of SDC resources



Game-theoretical frameworks (with multiple objective functions) for resource sharing in SDC

Implications for Defence

The collection of new techniques will enable defence to realize the concept of SDC for dynamic, agile and robust configuration, provisioning and sharing of infrastructure assets among armed forces or coalition partners, which are unmatched by our adversaries.

Readiness & alternative Defence uses

TRL 2/3. Many of the SDC techniques have been prototyped in practical environments, including the demo of SDC resource allocation. Further work will enhance readiness of the new techniques for practical use.

Resources and references

Samples of SDC related publications include:

Zafari, Faheem, Jian Li, Kin K. Leung, Don Towsley, and Ananthram Swami. "Optimal energy consumption for communication, computation, caching, and quality guarantee." IEEE Transactions on Control of Network Systems 7, no. 1 (2019): 151-162.

Zafari, Faheem, Kin K. Leung, Don Towsley, Prithwish Basu, Ananthram Swami, and Jian Li. "Let's share: A game-theoretic framework for resource sharing in mobile edge clouds." IEEE Transactions on Network and Service Management 18, no. 2 (2020): 2107-2122.

Organisations

Imperial College, University of Massachusetts, BBN, and ARL

Robust Network And Learning Architectures For Software Defined Coalitions

Military / Coalition Issue

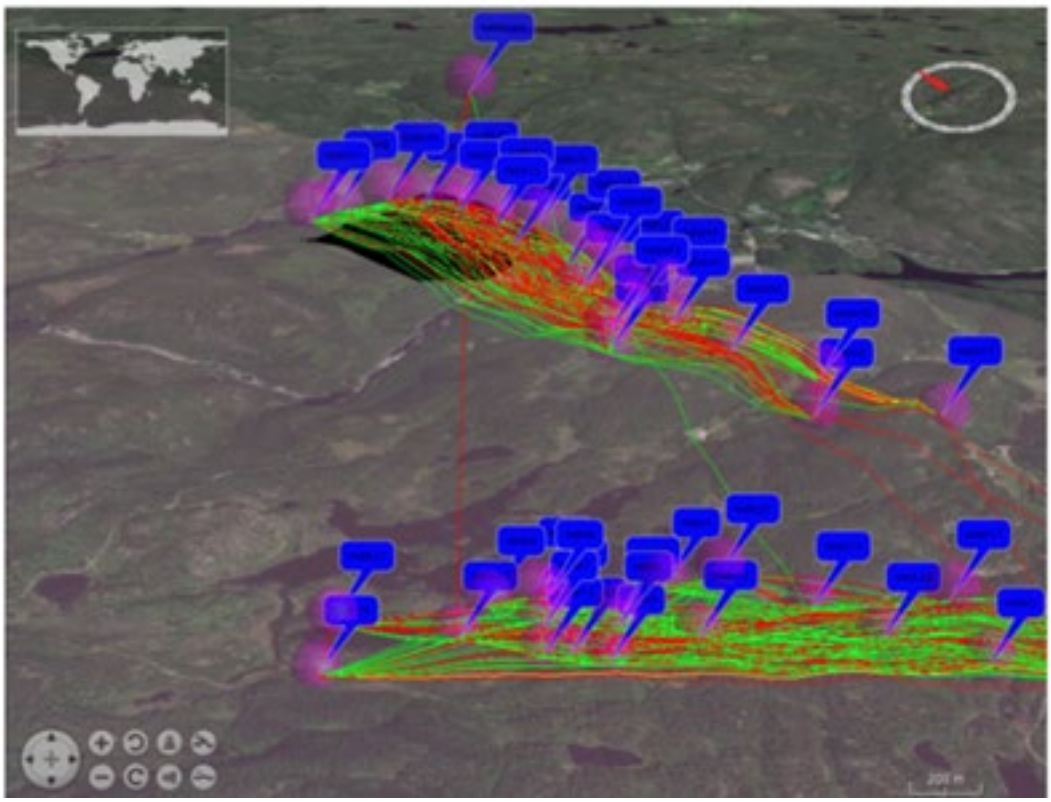
Military missions increasingly rely on communication and data analytic capabilities to efficiently conduct operations. Such capabilities should be available within the tactical unit formations even when the latter have little or no connectivity to the network infrastructure and the back-end cloud facilities of the Army. Therefore, the network and data analytic solutions must be robust to network failures and fragmentation events as well as easy to deploy and re-deploy every time the connectivity in the tactical network changes.

Core idea and key achievements

A new architecture called Software Defined Coalitions (SDC) has been developed, which extends the existing Software Defined Networking (SDN), to support military missions. With SDC, the network is managed by a designated network entity, the controller, which is programmable and thus automates many network operations. If combined with Machine Learning (ML) methods, the controller can reach an even higher level of network automation and realize with relative ease sophisticated data analytic services such as prediction of enemy's presence in a region through processing camera video feeds and other similar situation awareness services. Yet, the robustness of this solution can still be a problem since mobility and failures in the network may fragment the nodes from the controller rendering impossible their access to the ML model and the delivery of the required service. To address this challenge, we argue that both the network architecture of SDC and the ML architecture used in this context need to be carefully designed to be robust to network failures and fragmentation events.

Key achievements include:

Robust network architecture for SDC based on the idea of hybrid operation that combines the benefits of two paradigms: (i) logically-centralized and programmable network control of SDC and (ii) adaptivity and responsiveness to failures of traditional distributed mobile ad hoc network (MANET) protocols (e.g., OLSR).



Robust learning architecture for SDC that adopts a recently proposed family of Graph Attention (GAT) neural networks which are able to make predictions without model re-training even when network fragmentation events happen.

Prototype of the proposed robust network and learning architecture to quantify the benefits for a situation awareness service using a real dataset (Anglova in the figure) of a tactical ad hoc network.

Implications for Defence

Bringing the concepts of SDC and ML from the strategic and network infrastructure levels all the way down to the tactical level, within the tactical unit formations, where network automation and intelligent data-driven decisions are needed the most.

Readiness & alternative Defence uses

No content provided.

Resources and references

Related publications include:

Poularakis, Konstantinos, et al. "Hybrid SDN control in mobile ad hoc networks." 2019 IEEE International Conference on Smart Computing (SMARTCOMP). IEEE, 2019.

Poularakis, Konstantinos, et al. “Flexible SDN control in tactical ad hoc networks.” Ad Hoc Networks 85 (2019): 71-80.

Qin, Qiaofeng, et al. “Learning-aided SDC control in mobile ad hoc networks.” Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications III. Vol. 11746. International Society for Optics and Photonics, 2021.

Organisations

Yale University, Imperial College, IBM US, IBM UK, ARL

Semantic Vector Mapping for Coalition Operations

Military / Coalition Issue

We have shown that in order to unambiguous communicate information or to describe sensors and services different coalition partners can use symbolic semantic vector representations. In coalitions different partners may use completely different language (including foreign language) to describe the same semantic concepts. Whilst this could be addressed by agreeing a coalition sematic vector space, different coalition partners may not be willing to share all the details of their semantic vector space or the training data necessary to construct a common coalition semantic vector space.

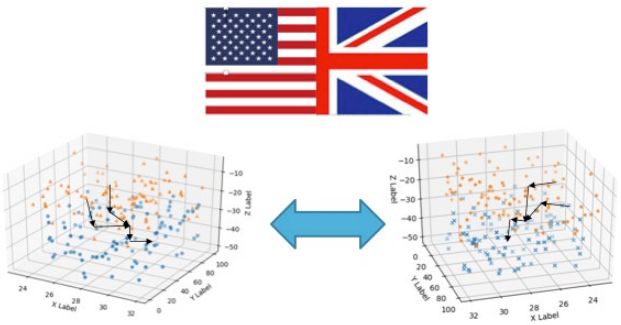
Is it possible to map semantic vectors between different vector spaces so that unambiguous communication or sensor and service descriptions can be exchanged and between coalition partners required to achieve specific mission goals?

Core idea and key achievements

The core idea is that semantic vector spaces generated independently using vector space embedding techniques (e.g., Word2Vec) from either different knowledge bases or document corpora will produce different semantic vectors but that the relationship between the vectors (e.g., cosine distance) will be maintained. Using completely different document corpora we have shown that this is indeed the case and that it is possible to use algebraic techniques and neural network techniques to learn the necessary mapping where the coalition partners only need to exchange a relatively small number of vectors that represent the same concepts.

Implications for Defence

This capability address key issues for interoperability in coalition operations where information needs to be exchanged or sensors and services need to be shared. This is specifically applicable in situations where the same capabilities exist in other parts of the coalition but have not been explicitly described because of sensitivity.



Mapping between coalition vector spaces

Readiness & alternative Defence uses

The approach has been demonstrated using different libraries of open-source data for word vector embeddings, but this could be extended to other types of military data including knowledge bases. Techniques for generating the vector space embeddings are described in another of our key outcomes.

Resources and references

Graham Bent, Declan Millar, Douglas Summers-Stay, Shalisa Witherspoon and Jae-Wook Ahn. "Semantic Vector Space Mapping for Edge of Network Coalition Operation" DAIS AFM 2020

Organisations

IBM UK, Cardiff University, ARL, IBM US

Software Defined Coalitions Controller Synchronization

Military / Coalition Issue

Military missions require the use of infrastructure assets including communication links, computational servers, data storage, databases, sensors and other resources. Dynamicity and agility of military operations demand near real-time configuration, re-configuration and provisioning of these resources, while supporting efficient and robust sharing of assets across armed forces or coalition partners. State-of-the-art techniques cannot currently achieve this.

Core idea and key achievements

A new architecture called Software Defined Coalitions (SDC) has been developed, which extends the existing Software Defined Networking (SDN), to address the above issue. An SDC is composed of multiple domains, each of which contains a set of infrastructure resources. Each domain has one domain controller and the controllers are connected through the control plane to exchange control information. As SDC is a logical (virtual) architecture, multiple SDCs can run simultaneously on the same set of physical resources. The software control logic implemented in controllers is programmable to enable rapid configuration for mission objectives, although controllers must synchronize status information of resources in their own domains with each other at times for proper operations and efficiency. Resources can be shared across domains among coalition partners and system control can be enhanced by reinforcement learning (RL); see the related DAIS Key Outcomes on “Resource Sharing in SDC” and “RL for Network Control,” respectively.

Key achievements include the development of:

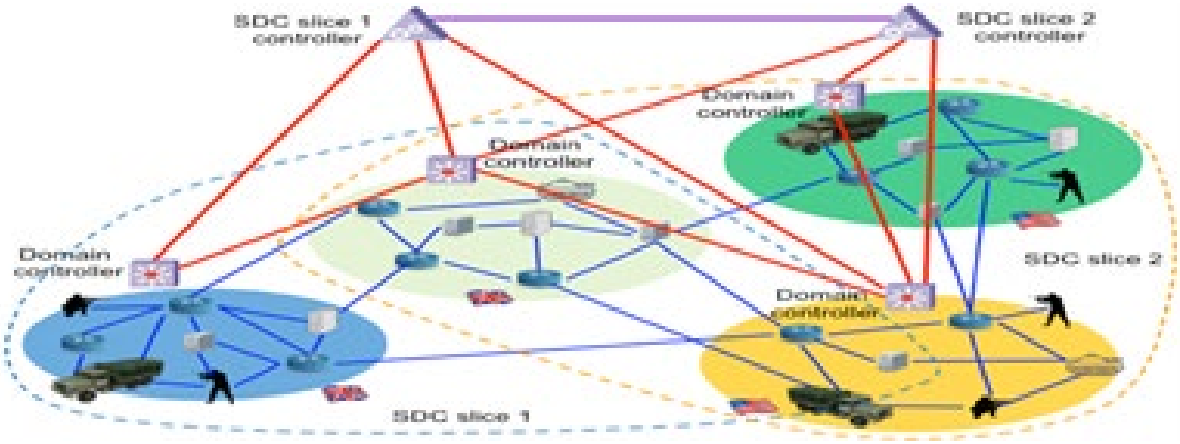
Fundamental understanding of benefits of controller synchronisation for various network structures and synchronisation levels

Development of mechanisms/policies for controller synchronisation

Algorithm for placing controllers to balance control delay & overheads

Emulations on practical controller platforms showing the impact of adaptive synchronization for routing and load balancing applications

Testbed experiments with real SDN-enabled mobile devices showing the traffic overheads of controller operation and dynamic placement.



Implications for Defence

The collection of new techniques will enable defence to realise the concept of SDC for dynamic, agile and robust configuration, provisioning and sharing of infrastructure assets among armed forces or coalition partners, which are unmatched by our adversaries.

Readiness & alternative Defence uses

TRL 2/3. Many of the SDC techniques have been prototyped in practical systems or environments, including the demos of controller placement and controller synchronization. Further work will enhance the readiness of the new techniques for practical defence systems.

Resources and references

Samples of SDC related publications include:

Controller synchronisation - Zhang, Ziyao, et al. "How advantageous is it? An analytical study of controller-assisted path construction in distributed SDN." IEEE/ACM Transactions on Networking 27.4 (2019): 1643-1656.

Synchronization policy - Poularakis, Konstantinos, et al. "Learning the optimal synchronization rates in distributed SDN control architectures." IEEE INFOCOM 2019-IEEE Conference on Computer Communications. IEEE, 2019.

Synchronization policy based on deep RL - Zhang, Ziyao, et al. "DQ scheduler: Deep reinforcement learning based controller synchronization in distributed SDN." ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE, 2019.

Efficient deep RL architecture - Zhang, Ziyao, et al. "Macs: Deep reinforcement learning based sdn controller synchronization policy design." 2019 IEEE 27th International Conference on Network Protocols (ICNP). IEEE, 2019.

Controller placement - Qin, Qiaofeng, et al. "SDN controller placement at the edge: Optimizing delay and overheads." IEEE INFOCOM 2018-IEEE Conference on Computer Communications. IEEE, 2018.

Organisations

Yale University, Imperial College, IBM US, ARL, Dstl

State-Action Separable and Embedding for Reinforcement Learning

Military / Coalition Issue

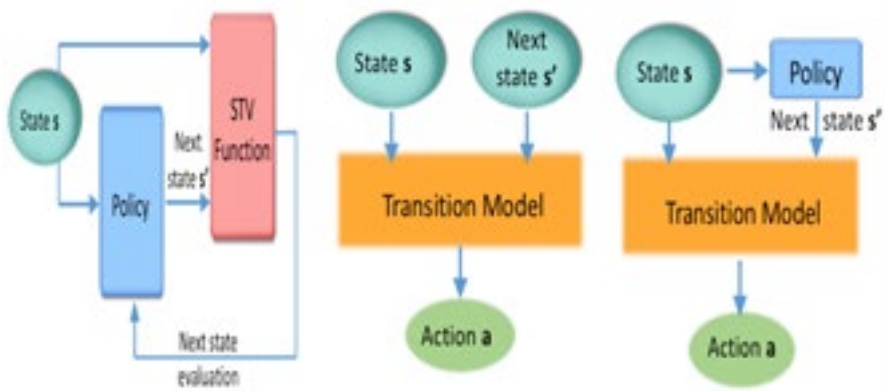
Reinforcement learning (RL) has been widely applied for system control in many domains. However, state-of-the-art RL often encounters issues such as huge state-action spaces, inefficient knowledge representation of states and actions, and violation of underlying model assumptions. As a result, RL techniques are often computationally complex and require long learning time, thus limiting their applicability to national defence.

Core idea and key achievements

The DAIS team has developed new techniques to address these RL issues, including state-action space explosion, inefficient knowledge representation of states and actions, learning with sudden changes in operating environments, and violation of underlying model assumptions. We focus here on two new techniques. First, a new technique called state-action separable RL (sasRL) has been proposed to separate state transitions from actions taken, while considering impact of actions through simple supervised learning, thus alleviating the issue of large state-action spaces. Second, a new embedding approach has been developed that uses a model of the environment to obtain joint embeddings for states and actions, from which the optimal policy can be learned. In this way, the embedded representations obtained enable better generalization over both states and actions by capturing similarities in the embedding spaces. Both new techniques greatly reduce the computation and learning time, thus extending the applicability of RL. Please also see the related DAIS Outcomes on “RL for Network Control” and “Joint Reinforcement and Transfer Learning for Fragmented SDC.”

Key achievements include the development of:

- sasRL technique to overcome huge state-action spaces
- Jointly trained state-action embedding to speed up learning for RL



Implications for Defence

The new techniques will enable defence to apply RL for real-time control and sharing of infrastructure assets among armed forces. They support efficient, agile and robust configuration and use of resources, which are unmatched by our adversaries. The techniques are also applicable to other systems such as radio spectrum sharing in electromagnetic warfare.

Readiness & alternative Defence uses

TRL 2/3. Both new techniques have been applied to practical problems studied in the literature and the sasRL has been prototyped in Leung, Kin K., et al. "Reinforcement and transfer learning for distributed analytics in fragmented software defined coalitions." Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications III. Vol. 11746. International Society for Optics and Photonics, 2021. They can be readily applied to defence systems.

Resources and references

Zhang, Ziyao, et al. "Efficient Reinforcement Learning with Implicit Action Space." 4th Annual Fall Meeting of the DAIS ITA, 2020

Pritz, Paul J., Liang Ma, and Kin K. Leung. "Joint State-Action Embedding for Efficient Reinforcement Learning." arXiv e-prints (2020): arXiv-2010.

Leung, Kin K., Anand Mudgerikar, Ankush Singla, Elisa Bertino, Dinesh Verma, Kevin Chan, John Melrose, and Jeremy Tucker. "Reinforcement and transfer learning for distributed analytics in fragmented software defined coalitions." In Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications III, vol. 11746, p. 117461W. International Society for Optics and Photonics, 2021.

Organisations

Imperial College, IBM US, Yale University, Purdue University, Dstl and ARL

The Fastlas System For Interpretable Machine Learning

Military / Coalition Issue

When deploying artificial intelligence systems in military settings, it is often important that the behaviour of such systems can be verified, audited and explained. It is difficult to extract meaningful explanations from a black-box machine learning system, presenting a potential barrier to the adoption of machine learning in military settings. FastLAS is a new logic-based machine learning system that learns interpretable rules, making it possible to generate explanations for each decision.

Core idea and key achievements

Previous state-of-the-art logic-based machine learning algorithms could be grouped into two categories: approximate and exact systems. The former do not guarantee finding the best set of rules and tend to perform poorer when evaluated on test data; the latter are systems that guarantee finding the best set of rules, but limited in their scalability over large search spaces. FastLAS is a new exact system that does scale to large search spaces.

Rather than optimising over the full search space straight away, FastLAS takes a novel approach of using the labelled data to carefully construct a small subset of the search space that is guaranteed to contain at least one optimal solution. It has been shown to be much more scalable, and 2-3 order of magnitude faster, than other current state-of-the-art exact systems, and able to learn rules that have a higher predictive accuracy than those found by state-of-the-art approximate systems. The first version of FastLAS has strong restrictions on the rules that can learn, limiting its applicability. The recently developed second version, called FastNonOPL overcomes many of these restrictions, widening the applicability of the approach; for example, FastNonOPL is capable of learning knowledge that is only indirectly observable, and can handle non-deterministic knowledge and data which are only partially defined.

Implications for Defence

Military operators will be able to deploy this system to tabular data to learn set of rules for prediction and decision making, which can be expressed to humans in natural language. Existing Deep Learning models can be integrated with our logic-based Machine Learning systems to support learning of interpretable complex rules from unstructured data in the presence of limited data . The systems can also take into account expert domain knowledge from different parties when learning in federating setting. Our system can generate explanations to help decision makers understand its output and increase trust in their outputs.

Readiness & alternative Defence uses

Our systems are at TRL 4 level. They have been validated in the lab and are ready to be deployed in a real environment. FastLAS has also been used in several other DAIS achievements (e.g., [1c.02], [1c.07], [1c.16]). Although it has mainly been used to learn policies within DAIS, FastLAS is a general-purpose rule-learner that can be used in a wide variety of applications.

Resources and references

- Law, Mark, et al. "Fastlas: scalable inductive logic programming incorporating domain-specific optimisation criteria." Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 34. No. 03. 2020.
- IJCAI 2021 (To appear): Scalable Non-observational Predicate Learning in ASP. Law, M., Russo, A., Bertino, E., & Broda, K.
- GitHub repository: https://github.com/spike-imperial/FastLAS

Organisations

Imperial College London, Purdue University, Universitat Pompeu Fabra.

Uncertainty-Aware Artifical Intelligence And Machine Learning

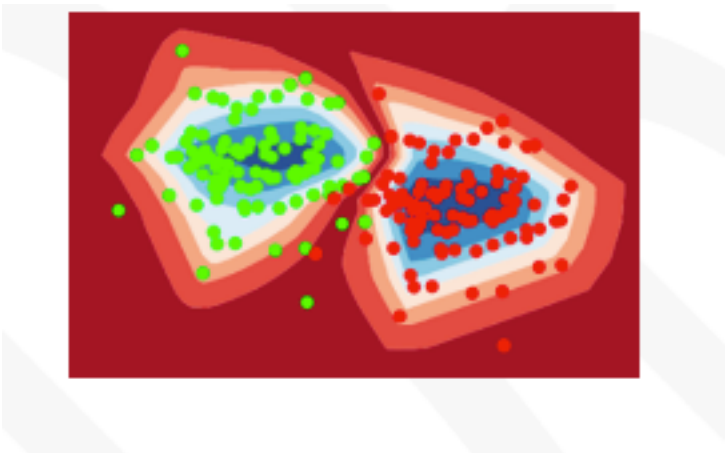
Military / Coalition Issue

Military coalitions must operate in dynamic and contested environments with constrained sharing policies leading to limited data to adapt AI systems. This leads to the possibility of high epistemic uncertainty that causes AI to makes poor recommendation potentially leading to disastrous decision making.

Core idea and key achievements

Developed methods to extract the epistemic uncertainty inherent in neuro-symbolic AI&ML systems trained with limited data. At the symbolic layer exact inference algorithms have been modified to percolate second-order probabilities to enable the answering of queries with confidence bounds.

At the neural layer, evidential deep learning (EDL) is specially trained to characterize the amount of relevant evidence for the various alternatives in light of the input (sensor) data and the data to train the AI network. In many different applications, it is demonstrated that EDL can detect out-of-distribution test samples. Furthermore, accuracy increases when deferring decision-making on highly uncertain test data.

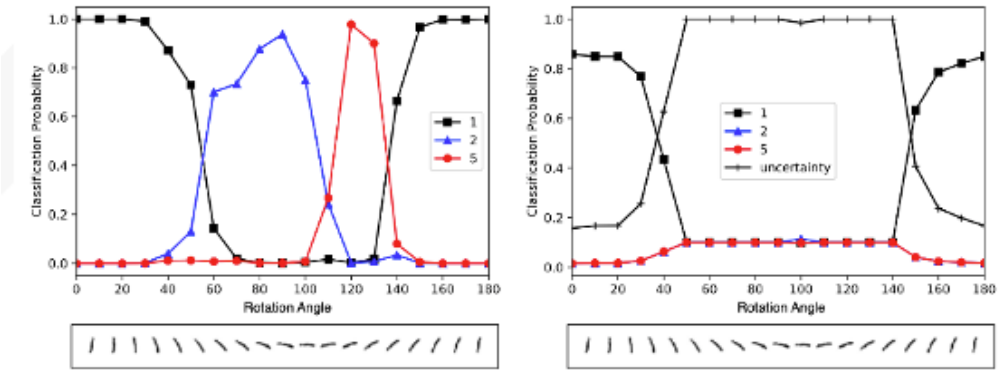


Uncertainty response in EDL relative to the training data

Implications for Defence

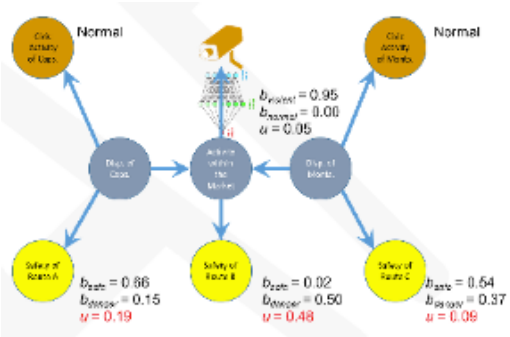
The EDL framework can be applied to numerous target classification systems. It allows such a systems to alert decision makers when it no longer is able to provide reliable recommendations,

which is possibly due to changes in the operational environment relative to how the system was trained.



Confidence of standard DL (left) and EDL (right) due to distribution shifts by rotating digits in MNIST data.

This enables decision makers to rely on the system only when it is reliable.



Second-order Bayesian network integrated with EDL operating on a surveillance camera

Readiness & alternative Defence uses

Provides a framework for training deep learning systems to be uncertainty-aware. Presented at UK Defence's AI Fest 3 and concepts embraced by AI research & development community. Initial methods have been tested on simulated and academic data sets. Work is needed to develop relevant military data sets for evaluation and advancement of the training framework and inference methods that enable uncertainty-aware AI&ML.

Resources and references

More details can be found on the Evidential Learning and Reasoning (ELR) asset page

Cerutti, Federico, et al. "Probabilistic logic programming with beta-distributed random variables." Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 33. No. 01. 2019.

Sensoy, Murat, Lance Kaplan, and Melih Kandemir. "Evidential deep learning to quantify classification uncertainty." arXiv preprint arXiv:1806.01768 (2018).

Sensoy, Murat, et al. "Uncertainty-aware deep classifiers using generative models." Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 34. No. 04. 2020.

EDL github

SLProbLog github

Organisations

Cardiff University, ARL

Understanding Social Networks from the Local Behaviours Within the Network

Military / Coalition Issue

Understanding networks is critical to multi-domain operations. Network structures in dynamic contexts are rarely static, and often function with considerable complexity. These networks could represent diverse concepts such as communication, social network activity, online media or many other issues. To understand such networks, traditional graph theory has limitations because we can often only observe part of the network. Therefore being able to make assessments through the presence of substructures is important.

Core idea and Key Achievements

This achievement summarises the progress made in using graphlets (small induced substructures) to analyse potentially complex network structures without recourse to global network characteristics. This includes:

• Applications to social media for the detection and assessment of disinformation, disruption and controversy;

• Alternative ways to understand paths through the network by the way that they "cut through" graphlets, thus enabling prediction as to how information and influence is liable to spread;

• Ways to use graphlets (through network embedding) to provide an alternative network representation, which enables machine learning of patterns and behaviours.

Implications for Defence

The military can use these techniques in settings where only partial network information is available – the presence of graphlets can be collected from dynamic, disconnected and temporal snapshots of networks and used for analysis through these techniques. Further, they avoid the need for processing the language content of social media.

Readiness and Alternative Defence Uses

The research has been carried out at a fundamental level but has been applied in interesting real-world network scenarios, including those relating to disinformation, and COVID19. This means that the work can be readily applied to other data sets of operational relevance.

Resources and References

Davies, C., Ashford, J., Espinosa-Anke, L., Felmlee., D, Preece, A., Srivatsa, M., Turner, L., and Whitaker, R.M., (2021), Multi-Scale User Migration on Reddit, Workshop on Cyber Social Threats, International Conference on Web and Social Media (ICWSM), accepted for publication.

Hudson, L, Whitaker, R.M., Allen, S.M., Turner, L., Felmlee, D., The Centrality of Edges based on their role in Induced Triads, (2021), IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), in submission.

Tu, Kun, Jian Li, Don Towsley, Dave Braines, and Liam D. Turner. "gl2vec: Learning feature representation using graphlets for directed networks." In Proceedings of the 2019 IEEE/ACM international conference on advances in social networks analysis and mining, pp. 216-221. 2019.

Ashford, James, Liam Turner, Roger Whitaker, Alun Preece, Diane Felmlee, and Don Towsley. "Understanding the signature of controversial Wikipedia articles through motifs in editor revision networks." In Companion Proceedings of The 2019 World Wide Web Conference, pp. 1180-1187. 2019.

Organisations

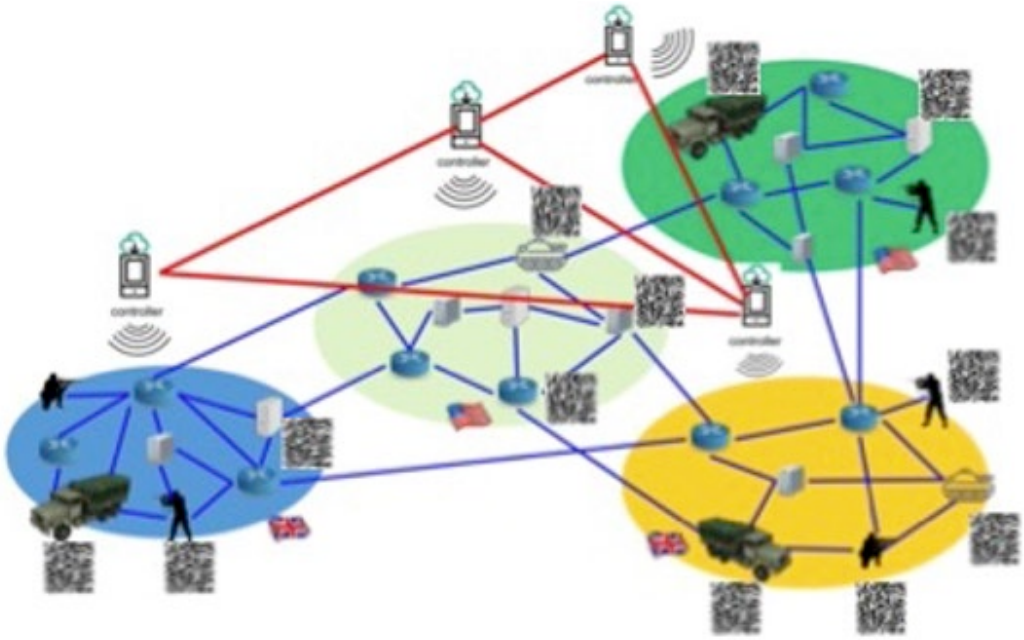
Cardiff, IBM UK, IBM US, UMass, Penn State

Vector Symbolic Architectures and Hyperdimensional Computing for Coalition Operations - An Overview

Military / Coalition Issue

Future military coalition operations at the network edge will require multiple sensors, devices and services owned by different coalition partners to be dynamically combined into workflows that can perform new complex tasks on demand. The coalition challenge is one of interoperability. How do we describe sensors, devices, and services so that they can be discovered and interconnected to achieve this mission goals? To address this challenge, we have been investigation the possibility of using a mathematically precise representation of information, where the information is encoded in the form of symbolic vectors.

A Vector Symbolic Architecture (or VSA for short) is a biologically-inspired method for representing and manipulating concepts and their meanings. Symbolic vectors simultaneously represent a semantic description of a concept and because they are vectors, they also are a pointer to the concepts. Chris Eliasmith, in his book 'How to Build a Brain' shows how these vector representations can be used to perform `brain like' neuromorphic cognitive processing. In our work we make use of large binary vectors with dimension typically in the range 1000 to 10,000 bits. We call such vectors 'hypervectors'. The fundamental idea behind this work is that any type of information, including complex service descriptions and service workflow, can be constructed from component vectors using a process of hierarchical vector binding and bundling such that the resulting vector is the same size as the component vectors. We can think of these vectors as mathematical symbols of symbols (hence Vector Symbolic). These vectors/symbols can be exchanged to unambiguously convey information across coalitions but more importantly they can be used to perform decentralized command and control of distributed coalition assets.



The idea is illustrated here where the square symbols illustrate the symbolic hypervectors. Descriptions of sensors, services are converted into this symbolic representation and stored locally. The required configuration of these assets is constructed as a symbolic vector of vectors and injected into the communications network. Through a process of peer-to-peer vector exchange the required assets are discovered and linked together to perform the required task.

We have prepared a video presentation that explain VSA in more detail - (https://ibm.ent.box.com/v/Showcase-1a11-video) and a video presentation that shows how decentralized workflow construction is executed in a representative TacCIS environment - (https://ibm.ent.box.com/v/Showcase-1a02-video). We also have a video presentation which explains how VSA can be used for unambiguous communication exchange in coalition operations, by using semantic symbolic vectors where coalition partners may use different terminology/language to describe the same assets (https://ibm.ent.box.com/v/Showcase-1a04-video).

Finally, we have been investigating how VSA operations can be performed in energy constrained environments using new emerging devices that can perform 'In Memory' and/or neuromorphic (i.e. spiking neural network) processing. Energy savings of the order of x100 are achievable in comparison to equivalent standard hardware implementations. Two video presentations giving further detail are available (https://ibm.ent.box.com/v/Showcase-1f01-video) and (https://ibm.ent.box.com/v/Showcase-1f02-video).

Organisations

Cardiff, IBM Research US, IBM Research Europe, Purdue, ARL and Dstl

Winning Hearts and Minds: Maximizing Influence in Social Networks

Military / Coalition Issue

When military efforts include civilian engagement (e.g. crowdsourcing activities), maximum participation, especially in the presence of an adversary relies on tactical interaction with the public. Here the main challenge is the identification and effective incentivisation of key individuals in a social network who can then spread influence in the rest of the population. The issue is particularly relevant in coalition settings, where competition may arise between allies as they compete to recruit human agents (or soft sensors) in a network to accomplish self-agendas or to have greater control over a joint operation.

Core idea and key achievements

The problem is widely explored in several real-world scenarios where in each case we present theoretical solutions that exploit network topology to determine optimal allocation of limited resources to counter adversarial influence in social networks. More specifically, we characterise optimal strategies under various constraints, such as network uncertainty and presence of negative (or antagonistic) ties. We also examine the impact of propagation errors and the effect of constrained access to nodes in a network. In every case, we derive optimal solutions both under complete knowledge of the adversary's strategy and under game-theoretic settings without any information about the adversary. Lastly, we design a human-subject experiment to establish if people employ rational or inherently biased strategies when maximising opinion spread in the real-world context.

Implications for Defence

The proposed algorithms can be readily used to offer real-time solutions to the competitive influence maximisation problem in several defence scenarios (for example, penetration of local networks for knowledge and support in combat zones). The work can also help identify vulnerabilities in any given network that can further aid the mitigation of misinformation spread. Finally, it can serve as a foundation for empirical analysis of online and offline behaviour within several defence (and security) operations.

Readiness & alternative Defence uses

The work is currently at technology readiness level (TRL) 3. An alternative use of the game in the human-subject experiment could be to exploit it as a training tool for military personnel.

Resources and references

Chakraborty, Sukankana, Sebastian Stein, Markus Brede, Ananthram Swami, Geeth de Mel, and Valerio Restocchi. "Competitive influence maximisation using voting dynamics." In Proceedings of the 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, pp. 978-985. 2019.

Brede, Markus, Valerio Restocchi, and Sebastian Stein. "Effects of time horizons on influence maximization in the voter dynamics." Journal of Complex Networks 7, no. 3 (2019): 445-468.

Eshghi, Soheil, Setareh Maghsudi, Valerio Restocchi, Sebastian Stein, and Leandros Tassiulas. "Efficient influence maximization under network uncertainty." In IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 365-371. IEEE, 2019.

Brede, Markus, Valerio Restocchi, and Sebastian Stein. "Transmission errors and influence maximization in the voter model." Journal of Statistical Mechanics: Theory and Experiment 2019, no. 3 (2019): 033401.

Brede, Markus, Valerio Restocchi, and Sebastian Stein. "Resisting influence: how the strength of predispositions to resist control can change strategies for optimal opinion control in the voter model." Frontiers in Robotics and AI 5 (2018): 34.

Stein, Sebastian, Soheil Eshghi, Setareh Maghsudi, Leandros Tassiulas, Rachel KE Bellamy, and Nicholas R. Jennings. "Heuristic algorithms for influence maximization in partially observable social networks." In SocInf@ IJCAI. 2017.

Organisations

University of Southampton (UK), IBM (UK and US), ARL (US).