ARL-TR-9571 • Sep 2022

DEVCOM
ARMY RESEARCH
LABORATORY

Context-Aware Networking and Cybersecurity for Resilient Networking (Summary Technical Report, Oct 2017–Sep 2020)

by Kevin Chan, Eric Graves, Kelvin Marcus, Terrence Moore, Jake Perazzone, Lisa Scott, Ananthram Swami, Andrew Toth, Gunjan Verma, and Paul Yu

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

ARL-TR-9571 ● SEP 2022

Context-Aware Networking and Cybersecurity for Resilient Networking (Summary Technical Report, Oct 2017–Sep 2020)

Kevin Chan, Eric Graves, Kelvin Marcus, Terrence Moore, Jake Perazzone, Lisa Scott, Ananthram Swami, Andrew Toth, Gunjan Verma, and Paul Yu
DEVCOM Army Research Laboratory

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* September 2022	**2. REPORT TYPE** Summary Technical Report	**3. DATES COVERED (From - To)** 1 October 2017–30 September 2020

4. TITLE AND SUBTITLE Context-Aware Networking and Cybersecurity for Resilient Networking (Summary Technical Report, Oct 2017–Sep 2020)	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Kevin Chan, Eric Graves, Kelvin Marcus, Terrence Moore, Jake Perazzone, Lisa Scott, Ananthram Swami, Andrew Toth, Gunjan Verma, and Paul Yu	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) DEVCOM Army Research Laboratory ATTN: FCDD-RLC-NT Adelphi, MD 20783-1138	**8. PERFORMING ORGANIZATION REPORT NUMBER** ARL-TR-9571
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

ORCID IDs: Kevin Chan, 0000-0002-6425-5403; Eric Graves, 0000-0002-4453-9134; Terrence Moore, 0000-0003-3279-2965; Paul Yu, 0000-0003-1577-3914

14. ABSTRACT

This report summarizes research results over the life of the Experimental Methods in Network Science project covering approximately 2017–2020. The project focused on two main topics: context-aware networking and cybersecurity for resilient networking. Context-aware networking aims to improve the performance of tactical networks and services they support using context awareness to enhance current state-of-practice methods that do not necessarily account for dynamics of the environment and limitations of resource-constrained edge devices and networks. Cybersecurity for resilient networking aims to enhance the security of tactical networks in the presence of dynamic and sophisticated adversaries.

15. SUBJECT TERMS

Network and Computational Sciences, tactical networking, cyber resilience, context-aware networking, Summary Technical Report, STR

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Kevin Chan
a. REPORT Unclassified	**b. ABSTRACT** Unclassified	**c. THIS PAGE** Unclassified	UU	37	**19b. TELEPHONE NUMBER (Include area code)** (301) 394-5640

Contents

List of Figures

1. Introduction

This report summarizes research results over the life of the Experimental Methods in Network Science project covering approximately 2017–2020. The project focused on two main topics: context-aware networking and cybersecurity for resilient networking. Context-aware networking aims to improve the performance of tactical networks and services they support using context awareness to enhance current state-of-practice methods that do not necessarily account for dynamics of the environment and limitations of resource-constrained edge devices and networks. Cybersecurity for resilient networking aims to enhance the security of tactical networks in the presence of dynamic and sophisticated adversaries.

The US Army Combat Capabilities Development Command Army Research Laboratory research staff involved in this project had significant influence in shaping and collaborating in multiple external partner programs in related topics. Outcomes of these programs were fed into the mission-funded projects. The partner programs include United States–United Kingdom Distributed Analytics and Information Sciences International Technology Alliance (DAIS ITA), Internet of Battlefield Things Collaborative Research Alliance (IoBT CRA), The Technical Cooperation Program (TTCP), and NATO Science and Technology Organization Information Systems Technology (NATO STO IST) Panel.

The impact of this research includes network-emulation experiments validating viability of algorithms and techniques to support theoretical outcomes, significant reporting of research results in the networks and communications research community, and contributions to Army Concept Science & Technology (S&T) documents. Highlights that are summarized in the following sections include development of optimal control in cascading failures for network control using sandpile modelling and determining conditions that can prevent cascading failures; physical layer security authentication protocols that increase lifetimes of secret keys by an order of magnitude; and contributions to the Command and Control (C2), Fires and Cyber S&T concept documents.

2. Technical Summary

2.1 Context-Aware Networking

With the growing scope of operations and dynamics required with moving toward realizing multidomain operations (MDO), it is necessary to exchange more information within and across operational domains. The increased information exchange and synchronization of multidimensional and multimodal information has the potential to enhance situational awareness and performance for joint operations. With expanded operations, this approach leverages multiple environmental contexts, gaining further understanding of dynamically evolving operational conditions and environments. However, in a congested and contested operational environment involving resource-constrained devices and networks, it is necessary to devise efficient means to configure and adapt networks. Tactical networked operations are assumed to operate in a denied, disconnected, intermittent-connectivity, limited-bandwidth (DDIL) environment with low size, weight, and power (SWAP) devices.

The research can be organized around the concept of the operations process cycle adapted to networked operations: learning and inferring network context, planning network control and analysis, and executing intelligent network adaptation through dynamic network reconfiguration. The research concepts of the cycle are thematically interrelated and holistically provide a more complete consideration of cross-layer resilience and robustness of a complex networked operational environment. These techniques are applicable to a broad range of challenges and Army functions as identified by project contributions to concept developer S&T documents.

To align with MDO, military commanders will have to learn the environmental context in which they operate, plan strategies to improve network performance, and execute adaptation of networked resources. The cycle of "assess, adapt, execute" is illustrated in Fig. 1. MDO assumes significant dynamics of the operational environment and resource-constrained platforms, so this research enhances understanding of efficient approaches to the provisioning and adaptation of these resources. We have made advancements in various topics such as dynamic resource allocation, distributed optimization, distributed machine learning (ML) and deep learning (DL) to best deal with the high complexity and scale of these systems. Through the development of novel techniques to account for the unique operating environmental challenges and constraints and applications, this research resulted in methods to understand network context, approaches to adapting networks to enhance performance, and techniques tested and validated on relevant tactical network environments.

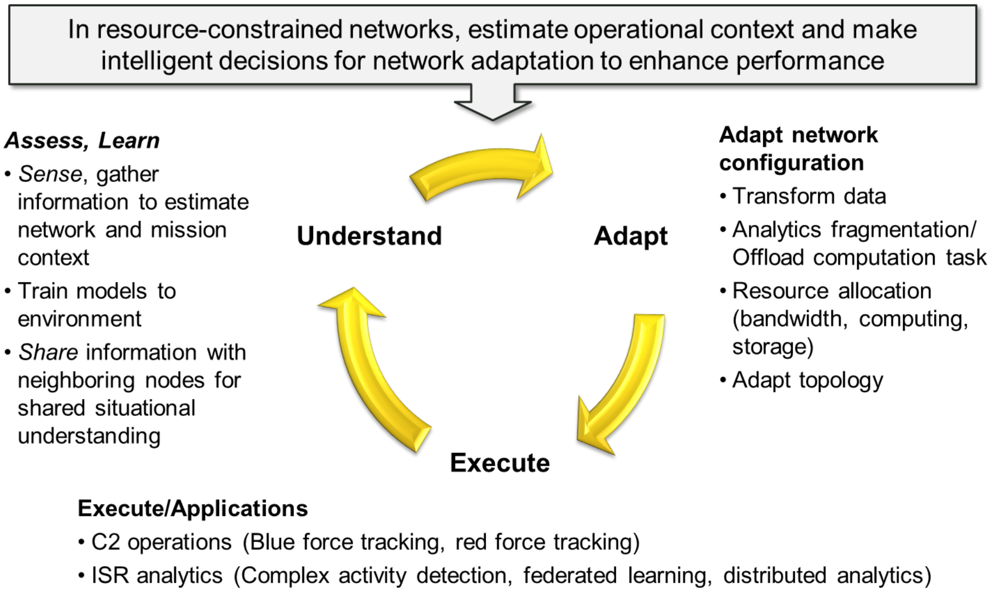
In resource-constrained networks, estimate operational context and make intelligent decisions for network adaptation to enhance performance
Assess, Learn
• *Sense*, gather information to estimate network and mission context
• Train models to environment
• *Share* information with neighboring nodes for shared situational understanding
Understand
Adapt
Execute
Adapt network configuration
• Transform data
• Analytics fragmentation/ Offload computation task
• Resource allocation (bandwidth, computing, storage)
• Adapt topology
Execute/Applications
• C2 operations (Blue force tracking, red force tracking)
• ISR analytics (Complex activity detection, federated learning, distributed analytics)

Fig. 1 Diagram of context-aware networking including the understand, adapt, and execute cycle

The research results summarized in this report seek to increase understanding of networked operations and improve how they perform under a variety of tactical network settings, such as coalition networks, IoBT, and MDO. With a growing volume of information available in tactical and strategic networks, network operators and commanders will require enhanced capabilities to analyze information. The approach of this project sought out network adaptation techniques that consider various network contexts for a tactical network setting and to understand generalized aspects of any of the findings.

There is great potential benefit of deploying advanced analytics, including artificial intelligence (AI) and ML in tactical environments; however, there is a lack of understanding of ML's potential impact in tactical networks for a variety of reasons. The limits to the extent that advanced analytics can be realized and provide benefit in the tactical networked environment is not known. Additionally, some ML techniques or approaches may provide performance enhancements that are worth the cost of extra computational demands in these environments. Some challenges include the resource-constrained nature of the devices and limited network resources coupled with the dynamic, hostile operational environment. We have analyzed and evaluated ML techniques and feasibility on tactical edge platforms, including Raspberry Pi and mobile GPU resources. Additionally, we explored distributed approaches to allow for placement of complex analytics over multiple nodes. Also, we considered other adaptations to ML, particularly model pruning and efficient data exchange methods for training and inference. We consider two ways to approach the interaction between ML and tactical networks: adapt ML applications to work on tactical networks despite challenges imposed by the operational environment and develop ML-based approaches to enhance the performance of tactical networks. The research in this report primarily deals with the latter.

2.1.1 Key Research Questions and Efforts

This research includes theoretical development, modeling, and experimental validation to enhance the performance and resilience of multilayer networks to provide situation understanding to analysts in contested, complex environments. These interrelated research efforts, when integrated, can enable cross-layer network optimization techniques. Here are three key research areas and research questions relevant to the context-aware networking focus area of the report:

Research Area 1: Learn: Context and Inference – Develop networked applications that consider the end user, mission requirements, and environmental context. We emphasize situations where the "user" is actually an inference engine, for example, an ML algorithm.

- Can we create a system that efficiently gathers relevant networked information and makes it available to processes within nodes and among local nodes?
- Can we identify meaningful subsets of features for sensing and inference of networked information?
- Can we devise analytics that can make cross-layer network reconfiguration recommendations to improve performance in evolving mission context?

Research Area 2: Plan: Control and Analysis – Based on awareness of network contexts, devise centralized and decentralized network control and reconfiguration approaches with the aim to improve network performance.

- Can we make meaningful inferences from available network statistics/information to adapt network resources efficiently?
- What ML or optimization strategies are useful to improve network performance while considering extra overhead or distributed approaches?

Research Area 3: Execute: Adaptation and Reconfiguration – Devise approaches and technology to realize network reconfiguration with the purpose of providing robustness and resilience of multiple network layers.

- Can we adaptively reconfigure networked resources to exploit dynamic operational environments and evolving mission requirements?

- What frameworks can be developed that enable testing of dynamically allocated analytics?
- What cross-layer reconfiguration strategies are tractable and effective?
- What are meaningful reward functions for effective networking behavior in representative scenarios?

These research areas are aligned with the aforementioned operations process cycle for networked operations. In the remainder of this section, we summarize outcomes of several research efforts. Each of these efforts pertain to one or more of the process cycles in Fig. 1 as well as the associated research questions.

2.1.2 Distributed Analytics

The distributed analytics research effort focused on the challenge of accelerating decision-making at the edge—enhancing system performance through intelligent adaptation of network resource allocation and exploitation of information at the edge. Recent developments propose a micro-edge cloud computing approach, in which computing resources are made available closer to severely resource-constrained devices. Given these resource-constrained devices operating over DDIL networks, limited capacity to host different services and applications, and a diversity of service and task requests, we have developed algorithms to address adaptation and reconfiguration challenges in this network paradigm.

Work in this area resulted in numerous results, furthering insights into a range of topics relevant to distributed analytics. In Panigrahy et al. (2020a, 2020b), we developed the power-of-two (POT) choice algorithms for resource allocation of tasks in distributed networks. With limited resources at the edge, optimal allocation of resources, considering latency and communication costs, is a critical issue. We proposed a novel algorithm that we showed was fairer than the state of the art, while retaining performance optimality. A key aspect of the research was to cast the problem in the framework of bulk service queueing systems. We generalized existing queueing results to cover the case in which servers are heterogeneous and resources may be shared across multiple users. The theoretical results and numerical evaluation yield design guidelines for resource placement (Panigrahy et al. 2020b). We extended these results to the 2-D case and studied the tradeoff between communication costs and load balancing. In a classical POT choice algorithm, a user is associated with the less loaded of the two closest servers (the closeness captures communication costs). Using a classical balls-and-bins approach, we established lower bounds on the asymptotic expected maximum load for a spatial POT policy. We proposed two nonuniform server sampling-based POT policies that achieve the best of both the performance metrics (Panigrahy et al.

2020a). We extended these results to graphs, which capture allowed communication links, and in which communication cost is in terms of number of hops rather than Euclidean distance. We performed extensive simulations over a wide range of network topologies. The proposed server sampling process leads to a drastic reduction in the overall systemwide implementation cost while obtaining a similar load distribution profile as that of POT policy (Panigrahy et al. 2022).

We also developed a series of methods that enables training of ML models in a distributed networked environment to account for limited bandwidth that inhibits exchange of training data to a central node; these novel methods use distributed coresets construction (Lu et al. 2020a, 2020b, and 2020c). To understand what resources are available in distributed environments, we also developed topology and Network Function Virtualization (NFV) inference techniques (Panigrahy et al. 2020a; Wheatman et al. 2020). We combined our approaches to network tomography, summarized in He et al. (2021), with ideas from higher-order statistics to infer the underlying routing topology of an arbitrary set of monitor paths using the joint distribution of end-to-end measurements, without making any assumptions on routing behavior. Our approach, called the Möbius Inference Algorithm, uses cumulants of this distribution to quantify high-order interactions among monitor paths, and it applies Möbius inversion to "disentangle" these interactions. We provide a more practical variant called Sparse Möbius Inference, which uses various sparsity heuristics to reduce the number and order of cumulants required to be estimated. We show the viability of our approach using synthetic case studies based on real-world internet service provider topologies (Smith et al. 2020).

Other work involved approaches toward optimal task resource allocation in a variety of distributed settings while also considering dynamics of environment and diversity of resource availability and resource requirements (Zhao et al. 2018; Pasteris et al. 2019; Tran et al. 2019; Wheatman et al. 2020). To ensure quality-of-information guarantees in analytics, communications, computation, and caching, costs must be jointly optimized to minimize energy consumption. We formulated the problem of identifying the optimal data compression rates and cache placement as a mixed-integer nonlinear programming problem with nonconvex functions, which is NP-hard in general. We proposed a variant of the spatial branch-and-bound algorithm that can provide an ϵ-global optimal solution to the problem. Our extensive numerical experiments show that our optimization framework improves energy efficiency by up to 88% compared to any optimization that only considers either communication and caching or communication and computation (Zafari et al. 2020). Computation of multiple edge analytics can be facilitated by resource sharing among different domains or coalition partners (or edge cloud servers), each of which may have different utilities. We model resource sharing as a multiobjective optimization problem and present a solution framework based on Cooperative Game Theory. We prove that for a monotonic, nondecreasing utility function, the game is canonical and convex. We propose a core algorithm and a variant that reduces resource fragmentation (Zafari et al. 2021). These results provide analysis and experimentally validated approaches toward the placement of analytics and execution of distributed analytics including ML training and network inference. These results enhanced the fundamental understanding of networks and analytics relevant to MDO and coalition networks.

2.1.3 Network Control

Control and analysis of networks enhances network resilience and robustness by understanding the current network and environment state as well as determining methods to move to a more desirable network configuration to enhance performance metrics.

We studied the concept of IoBT and the need for quick discovery and synthesis of Internet of Things (IoT) networks (Cisneros-Velarde et al. 2019; Pylorof et al. 2019; Ghosh et al. 2020). Our results include addressing the synthesis problem and developing techniques that scale to large regions and large networks while producing cost-effective solutions. Ghosh et al. (2020) and Cisneros-Velarde et al. (2019) explore two different representations of the synthesis problems using satisfiability modulo convex (SMC) optimization and mixed-integer linear programming (MILP). Our findings suggest that MILP outperforms SMC in some settings for smaller problem sizes. The fact that SMC's expressivity matches our problem ensures that it uniformly generates better-quality solutions at larger problem sizes. Additionally, we developed and analyzed robust network control algorithms using sum of squares programming to identify requirements for system stability (Cisneros-Velarde et al. 2021).

Complex systems are challenging to control because the system responds to the controller in a nonlinear fashion, often incorporating feedback mechanisms. Interdependence of systems (such as communications, information and social networks, or power, water, and phone networks) poses additional difficulties, as cross-system connections enable malicious activity to spread between layers, increasing systemic risk. We studied conditions for optimal control of cascading failures in a system of interdependent networks, using the sandpile model. We explored the propagation of cascades across networks using realistic network topologies, such as heterogeneous degree distributions, as well as intra- and interlayer degree correlations. We find that three properties—scale-free degree distribution, internal network assortativity, and cross-network hub-to-hub connections—are all necessary components to significantly reduce the size of large cascades in the sandpile model. We demonstrated that correlations present in the structure of the multilayer network influence the dynamical cascading process and can prevent failures from cascading. These findings highlight the importance of internal and cross-network topology in optimizing robustness of interconnected systems (Turalska et al. 2019, 2021).

Complex networks are heterogeneous in node and link attributes, and one aspect of this heterogeneity manifests itself in the so-called friendship paradox, that is, on average people have fewer friends than their friends do, or the average degree of a node is less than that of its one-hop neighbors. We proposed a local network metric, called the friendship index (FI), to quantify characteristics of this paradox. We used the FI metric to measure disparity within a network, and we examined the aggregated FI value both theoretically for a class of networks and experimentally across a suite of synthetic and real-world networks. By conducting a correlation study between the proposed metrics and degree assortativity, we experimentally demonstrated that the phenomenon of the friendship paradox is related to the well-known phenomenon of assortative mixing (Pal et al. 2019).

Recent social networks research focused on the modeling and analysis of how opinions evolve as a function of individual relationships—attempting to model the implications of both friendly and antagonistic relationships. In Bovet and Chan (2018), Cisneros-Velarde et al. (2019), and Turalska et al. (2019), we studied the boomerang effect in opinion dynamics and model and analyze the presence of opinion polarization using structural balance property. Our analysis shows that in signed networks, the opinions show persistent fluctuations. Additionally, opinions and influence in various networks are impacted by false and misleading information, thus leading toward networked information instability. Modeling and understanding of these phenomena enables control of dissemination of such harmful information in these networks, limiting potential harmful downstream impact to networked operations.

We also studied the influence maximization problem using a dynamic model under competitive settings in a signed network, where two adversaries compete to spread their influence in the network. Here, nodes are dynamic and are free to continually change their states and influence propagates under voting dynamics. Theoretical results and numerical evaluation provide insights on the optimal allocation of resources. We show that optimal strategy varies with the fraction of negative links in a network under adversarial settings (Chakraborty et al. 2019, 2020).

2.1.4 Tactical Networks

This effort focused on developing various services that are suitable for operation on tactical networks. Semantically Managed Autonomous Resilient Tactical Networks (SMARTNET) is an effort that developed semantically managed C2 across multigenre tactical networks. We collaborated with NATO and TTCP partners to assess numerous aspects of communication protocols in tactical/coalition settings. We also worked with DAIS ITA to develop approaches to improve resilience of software defined networking (SDN) for tactical networks.

2.1.4.1 SMARTNET

SMARTNET is a bilateral Project Arrangement between the United States and Australia's Defence Science and Technology Group. This program aims to develop semantically managed autonomous and resilient C2 applications across multigenre tactical networks to enhance robustness and resilience of networked applications; augment Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) applications deployed in disconnected, intermittent, and limited (DIL) networking environments through various information management techniques; and develop a prototype with relevant hardware/software (HW/SW) to demonstrate the concept in a tactical network environment. The concept involved the idea to prioritize, transform, and control information over the tactical network (Fig. 2) in accordance with changing Mission, Platform, Environmental and Network conditions/contexts.

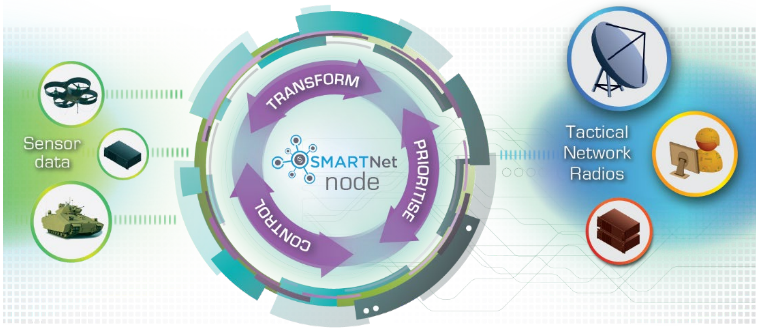

Fig. 2 SMARTNET concept including prioritization, transformation, and control of information in tactical networks

Key accomplishments included development of information dissemination techniques for C2 applications in DIL environments to enhance robustness and resilience (Judd and Chan 2017; Chan et al. 2018; Craggs et al. 2021); development of network simulation and emulation experiments and initial in-lab experimentation with integrated HW/SW (Chan et al. 2019b, Craggs et al. 2021; and enhancement of network experimentation capabilities (Judd et al. 2018; Chan et al. 2019a; Chan et al. 2019b; Judd et al. 2019). Specifically, work on optimizing the configuration of SMARTNET modeling and parameterization of assigning value to message types to determine relative performance yielded an improvement of nearly 50% over the baseline as validated through simulation (Craggs et al. 2021). These research results were validated in DEVCOM Army Research Laboratory's Network Science Research Laboratory with plans to execute a field trial in October 2020. The field trial was planned to demonstrate the SMARTNET concept and vision, involving middleware to enhance information delivery using cross-layer context awareness. The experiments were to include execution of SMARTNET software integrated with tactical radios in a tactically relevant scenario. The field trial was cancelled due to COVID-19.

2.1.4.2 Protocol Assessment

Research on improving tactical network performance included methods to enable understanding and adaptation, such as messaging middleware and other publish/subscribe standards. Other efforts studied the potential of agility provided by these methods. Portions of this research were executed in collaboration with our NATO allies, in the NATO IST panel groups IST-118 and IST-150 (Meiler et al. 2017; Manso et al. 2018a, 2018b, 2019; Johnsen et al. 2019; Jansen et al. 2021), where the group identified and experimentally tested and validated their performance in NATO-related field experiments.

Our team designed and conducted a video analytics experiment to assess the benefits of applying the SDN paradigm to tactical environments. This experiment was leveraged in various incarnations for collaborative work (Marcus et al. 2018). It was instrumental in the creation of a new international collaborative project within TTCP C4I TP43 (Communications), where the group identified important aspects of applying SDN for tactical networks. Specific aspects included requirements for coalition interoperability, security, quality of service management, and trust management. Other research outcomes included the development of an unmanned ground sensor scenario with a US Army military advisor for the collaborative project.

2.1.4.3 Software Defined Networking

In collaboration with DAIS ITA, we designed and analyzed two complementary approaches for robust control of highly dynamic mobile networks via SDN. In complex tactical networks that span regions of differing dynamics, hybrid architectures that combine the conceptually centralized control plane of Software Defined Coalitions (SDCs) with a distributed control plane have demonstrated promising tradeoffs between performance and robustness that inform the control of a robust network infrastructure for distributed analytics tasks.

First, we designed a novel system to perform distributed verification of interoperating control planes and demonstrated a significant reduction in downtime when evaluated in military settings (EMANE). In a related effort, we demonstrated a technique to significantly improve the routing success through coalition partners that advertise only a subset of their routes due to privacy concerns. Our technique for distributed verification of safety and security requirements reduced routing downtime by up to 75% (Gokarslan et al. 2019; Li et al. 2019; Xiang et al. 2019).

Second, we designed and analyzed an approach for autonomous operation of switches that become disconnected from the SDN control plane (i.e., fragmented). However, switches often do not have sufficient computational capability or information to perform the complex computation of the controllers. Therefore, we proposed the use of lightweight binarized neural networks to reduce computation and memory requirements by a factor of 32 and enable disconnected operation at line speed (Qin et al. 2020). A similar idea is applied to deciding when to switch between SDCs and mobile ad-hoc network protocols by running local models at switches to predict the fragmentation event with the use of graph attention networks that are robust to topology changes. We showed improved pathloss prediction while using only 9.5% of the input features on the Anglova scenario (Qin et al. 2021).

Synchronization of distributed controllers is critical to eliminating anomalies and network instability due to inconsistencies between the views of the different controllers. To address this challenge, we formulated the controller synchronization problem as a Markov decision process and applied reinforcement learning techniques combined with deep neural networks to train a smart, scalable, and fine-grained controller synchronization policy. This policy significantly outperforms the Open Network Operating System (ONOS) and greedy SDN heuristics by 56% and 30%, respectively (Zhang et al. 2019).

2.2 Cybersecurity for Resilient Networking

The presence of near-peer adversaries makes security of paramount importance in MDOs and autonomous maneuvers will be required to ensure the resilience of tactical cyber networks. Network resilience is the ability of network services to operate despite adversary duress and dynamics, maintaining measures of performance (e.g., uptime, link failure rate, and detection rate) across multiple layers (physical through application layers). We studied appropriate countermeasures and defenses against intelligent adversaries that surveil and learn. This section summarizes research in three related efforts: robust detection and authentication, deception strategies, and moving target defense (MTD). These research activities leverage research in the Cyber and IoBT CRAs and International Technology Center – Pacific (ITC-PAC) program. Selected research outcomes fed into Foundational Research for Electronic Warfare in Multi-Domain Operations (FREEDOM) Essential Research Program and have transitioned to Command, Control, Communication, Computers, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) Automated Cyber through Cyber CRA Applied Research and Engineering 6.2 Program.

The military tactical area of operations is a complex environment with both environmental and adversarial challenges. There is a constant need to protect the confidentiality and integrity of data communications in this tactical space. Resilience is the ability of the tactical network to operate under adversary duress and dynamics. Robustness is the ability of the network resources to withstand families of attacks. Our research furthers fundamental understanding on how it is possible to efficiently deploy detection techniques, effectively use deception to thwart potential adversarial attacks, and autonomously maneuver to ensure resilient tactical cyber networks. These research outcomes continue to influence efforts on improving robustness and resilience of Army tactical networks.

We focused on autonomous network maneuvers to ensure resilient tactical networks. Resilience is the ability of the tactical network to operate under adversary duress and dynamics. Because adversaries are present in or around our networks, the security of the operations is of paramount importance and must be jointly considered with other measures of resilience (e.g., uptime, link failure rate). We consider the passive adversary that eavesdrops as well as the active adversary that injects malicious activity.

Some broad concepts summarizing the goals to bolster the resilience of the network against sophisticated, dynamic adversaries include detection of adversaries through adversarial ML techniques for traffic obfuscation and cyber deception through dynamic honeynets; detection of the adversary using ML techniques for distributed and efficient intrusion detection and fundamental limits of intrusion detection in distributed ML protocols; and approaches for robustness using ML techniques that exhibit strong performance against a variety of noise, adversarial injection and mislabeling, and DL techniques to provide robustness against network attacks including rewiring and feature masking. Taken together, these approaches enhance the resilience of Army networks against the adversary and improve their robustness so the mission can be accomplished even under extreme dynamics and hostility.

2.2.1 Key Research Questions

Our approach aims to enhance the awareness and robustness of attacks and adversarial influence from multiple perspectives. We have organized this research into four related efforts: network traffic obfuscation, practical security, MTD, and network systems diversity for resilience. The following list of questions were addressed in the research efforts:

- Research Question 1: Can we devise distributed detection and authentication techniques to provide detection capabilities over multiple dimensions (across network layers, distributed across the network, and across time)?
- Research Question 2: Can we devise effective strategies for adaptation and monitor placement to enable honeypots, honeynets, and moving target defense?
- Research Question 3: Can we develop strategic deception to place deception and decoy capabilities that enable adversarial detection by deceiving the adversary?
- Research Question 4: Can we develop moving target defense to enhance strategies to adapt networks to provide robustness to adversarial attack?
- Research Question 5: Can we develop provable authentication secure protocols against attacks on physical layer communications?
- Research Question 6: Can we develop network traffic obfuscation techniques to fool an adversary to bypass network traffic detection or network flow dynamics?

2.2.2 Network Traffic Obfuscation

Securing network transmissions by not allowing adversaries to infer types of network transmission or to understand dynamics of information flows in network is a crucial step towards improving resilience in networked operations. One approach applied Adversarial Machine Learning (AML) techniques to perturb network traffic to prevent eavesdroppers from classifying network traffic type (Verma et al. 2018). One constraint beyond typical AML techniques is the requirement that the network traffic still contain useable payloads as well as adhere to the network protocol. Thus, it is necessary to find map back functions from features to packet and network flows that are meaningful and pass network checksums, for example. Another result involved adding network chaff to prevent eavesdropping attacks from determining the source of network transmissions over multiple hops of a wireless network (He et al. 2017; Ciftcioglu et al. 2018). This location privacy result is immediately applicable to providing resilience to the Mobile Edge Cloud network paradigm.

2.2.3 Practical Security

The project conducted research on provably secure and implementable protocols and made progress along two related directions. First, the project developed provably secure authentication protocols at the physical layer that leveraged the use of multiple antennas and artificial noise to improve performance. We showed how, in the 10-antenna case, the lifespan of a secret key can be increased from 3 uses to 89 uses by allocating 10% of its fingerprinting power to artificial noise (Perazzone et al. 2019a, 2021). A novel use of RF fingerprinting techniques to create a cryptographic side-channel was also proposed (Perazzone et al. 2018a). New results in characterizing the capacity regions for secret key-enabled authenticated communications were obtained as well as a coding scheme that outperforms previous schemes (Perazzone et al. 2018b).

Second, the project developed methods for authentication in the presence of adversaries of various capabilities and in different channel types. In this work, a myopic adversary has a noncausal noisy version of the transmitted sequence and can choose the channel state with the goal of having the receiver decode to an incorrect message. The myopic model bridges the gap between oblivious and omniscient adversaries. We showed channel conditions exist where authentication is impossible with a deterministic encoder (Beemer et al. 2019a), but possible with a stochastic encoder. With such an encoder, we then showed the capacity region can be as large as that of the nonadversarial channel (Beemer et al. 2020a). That is, the authentication capability can be obtained with very little overhead.

A keyless structured authentication coding scheme was developed for the binary adversarial channel that allows the receiver to decode the legitimate transmission or to detect adversarial interference (Beemer et al. 2019b). The practicality of the scheme stems from its bounded-complexity decoding and is the subject of a patent application (Beemer et al. 2020c). Further, we developed a coding scheme resilient to adversarial interference in multiple access channels, gave results on the error-correcting authentication capacity region, and presented a code construction for the real addition binary arbitrarily varying multiple access channel (Beemer et al. 2020b).

2.2.4 Moving Target Defense

MTD is a proactive approach to cybersecurity. As opposed to passive approaches for detection of threats and patching of known vulnerabilities, MTD seeks to increase the complexity and uncertainty for the attacker by dynamic changes to the attack surface (Cho et al. 2020). As part of a collaboration with an ITC-PAC group, ARL developed approaches using SDN to change the perceived attack surface of the IP/port address space using virtual addresses managed by the SDN controller. These approaches reduce the rate an attacker is successful in finding a host user (scanning attack) approaching 1/e for large address space (i.e., the chances the attacker will find a network host is reduced almost 37%) (Sharma et al. 2018, 2019). In addition to the security benefits of such an approach, the group also addressed issues of network scale by using multiple SDN controllers. This improves the reliability against a single point of failure with the security side benefit of enabling the reduction of the effective MTD interval thereby more frequently changing the attack surface (e.g., two controllers can reliably reduce the interval by 33%, three controllers by 50%, and, in general, N controllers by (N–1)/(N+1)×100% for a fixed number of host and address spaces) (Narantuya et al. 2019). Another critical issue addressed is the performance loss generated by MTD actions. This performance loss might result in an increase of file transfer duration by up to 19.73% (Dishington et al. 2019) and an increase of maintenance plus opportunity costs of 7% (Mendonca et al. 2020). Various strategies can be used to mitigate this, such as pausing the MTD action a specified time until remaining jobs complete can reduce the number of failed or dropped jobs in half while still nearly maintaining the security benefit (Kim et al. 2020). Adding a second server/controller that alternately completes jobs while the other initiates the MTD action can increase the server response time by 28.7%, hence increasing the probability that a job completes (does not fail) by 44.3% (Mendonca et al. 2021).

This research effort also considered approaches to help inform MTD actions. When assets in the network are ranked it is important to prioritize the actions. ARL developed an attack graph analysis to guide where to initiate MTD actions. For example, in one scenario with 600 hosts this approach has an attack path prediction accuracy of 86% (compared to an existing state-of-the-art approach that has an accuracy of 74%) with one-third the cost in terms of computation time (Yoon et al. 2020a). Dynamic metrics (Sharma et al. 2020; Mendonca et al. 2021) have also been developed to help a user determine when the risk of scan or exploitation or compromise exceeds a threshold for their requirements. Another approach to inform the MTD action is consideration of resources (Dishington et al. 2019; Yoon et al. 2021). Under this scenario, ARL has designed several ML approaches (Lee et al. 2021; Yoon et al. 2021; Kim et al. 2022) that determine where to allocate resources and when to initiate MTD actions to optimize the security performance with minimal effect on the network performance. Currently, ARL is interested in integrated intrusion detection to inform the proactive MTD mechanism (Kim et al. 2022).

A particular application space of concern for this research is in-vehicle network security (Yoon et al. 2020b; Lee et al. 2021), although the work has applicability in other domains, such as enterprise systems (Cho et al. 2020; Kim et al. 2020; Mendonca et al. 2020). The ITC-PAC is part of a collaboration between ARL and international (University of Queensland [Australia] and Gwangju Institute of Science and Technology [South Korea]) and domestic (Virginia Tech) partners.

2.2.5 Network Systems Diversity for Resilience

Diversity of network systems has proven to be an indicator of resilience of network systems by limiting the damage of any single vulnerability (Cho and Moore 2019; Zhang et al. 2022). Given a system with a particular set of vulnerabilities, we have investigated the benefits of adapting an existing network system (Cho and Moore 2018; Moore et al. 2019) with consideration of increasing diversity to maintain service after the network has been attacked (Zhang et al. 2021b). These results demonstrate that if network nodes are clustered into task groups, then the probability of maintaining the task can be increased by 5% (Cho and Moore 2018) to 9% (Moore et al. 2019). We have recently used ML techniques to determine which network adaptations to take (Zhang et al. 2021a, 2021c) and are currently considering the potential of adapting the approach as an MTD in collaboration with the ITC-PAC.

3. Army Impact

Through engagement with then Team Ignite and now Task Force Ignite, our research impacted several Army Futures Command (AFC) operational command documents contributing to several S&T appendices that outline future technology and research capabilities that will impact future Army operations. Through engagements with AFC, Task force Ignite, and other collaborators, research results from this project informed several conceptor documents' preparation, including C2, Cyber, and Fires (AFC 2021a, 2021b, 2021c).

Contributions to the semantically adaptive network control conceptor document (AFC 2021a) were based on research efforts found in Section 2.1.3, Network Control, particularly drawing from results in context-aware network adaptation and SDN control in Chan et al. (2019a), Poularkis et al. (2019), and Qin et al. (2021). Specifically, our research aimed at identifying semantics of the network context and operational environment to improve network adaptation and resilience decisions. Research conducted and findings obtained from Section 2.2, Cybersecurity for Resilient Networking, contributed to the conceptor document on Cyberspace and Electromagnetic Operations (AFC 2021b). Specifically, the contributions focused on context-aware networking to enhance network and cyber robustness through evaluation of tradeoffs between packet loss and packet delay (Judd et al. 2019), network agility via MTDs such as IP or software diversity (Cho and Moore 2018, 2019; Moore et al. 2019; Zhang et al. 2021a, 2021b, 2021c; Zhang et al. 2022), and network obfuscation employing adversarial ML techniques to successfully produce adversarial examples with a 90% success rate (Verma et al. 2018). The Fires conceptor document included research complex activity detection results that demonstrated the feasibility of multitarget, multiview detection of complex events at the tactical edge (Liu et al. 2019). This concept was suggested for potential application to the automatic target recognition requirement.

4. References

Distributed Analytics

He T, Ma L, Swami A, Towsley D. Network tomography: identifiability, measurement design, and network state inference. Cambridge University Press; 2021 May.

Lin Y, He T, Wang S, Chan K. Waypoint-based topology inference. IEEE ICC 2020 – 2020 IEEE International Conference on Communications (ICC); 2020 June 7–11; Dublin, Ireland. IEEE; 2020a. p. 1–6.

Lin Y, He T, Wang S, Chan K, Pasteris S. Looking glass of NFV: inferring the structure and state of NFV network from external observations. IEEE/ACM Transactions on Networking. 2020b;28(4):1477–1490.

Liu X, Ghosh P, Ulutan O, Manjunath B, Chan K, Govindan R. Caesar: cross-camera complex activity recognition. In: Proceedings of the 15th ACM Conference on Emerging Networking EXperiments and Technologies (CoNEXT); 2019 Dec 9–12; Orlando, FL.

Lu H, Liu C, He T, Wang S, Chan K. Sharing models or coresets: a study based on membership inference attack. International Workshop on Federated Learning for User Privacy and Data Confidentiality in Conjunction with ICML 2020 (FL-ICML 2020); 2020a July 17–18; Vienna, Austria.

Lu H, Liu C, Wang S, He T, Narayanan V, Chan K, Pasteris S. Joint coreset construction and quantization for distributed machine learning. 2020 IFIP Networking Conference; 2020 June 22–26; Paris, France. IEEE; 2020b. p. 172–180.

Lu H, He T, Wang S, Liu C, Mahdavi M, Narayanan V, Chan K, Pasteris S. Communication-efficient k-means for edge-based machine learning. 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS); 2020 Nov 29–Dec 1; Singapore. IEEE; 2020c. p. 595–605.

Panigrahy NK, Basu P, Towsley D, Swami A, Leung KK. On the analysis of spatially constrained power of two choice policies. ACM SIGMETRICS Performance Evaluation Review. 2020a;48(3):51–56.

Panigrahy NK, Vasantam T, Basu P, Towsley D, Swami A, Leung KK. On the analysis and evaluation of proximity-based load balancing policies. IEEE Transactions on Modeling and Performance Evaluation of Computing Systems (TOMPECS). Forthcoming 2022.

Panigrahy N, Basu P, Nain P, Towsley D, Swami A, Chan K, Leung K. Resource allocation in one-dimensional distributed service networks. Performance Evaluation (Elsevier). 2020b;142.

Pasteris S, Vitale F, Wang S, Chan K, Herbster M. MaxHedge – maximising a maximum online with theoretical performance guarantees. AISTATS 2019. 22nd International Conference on Artificial Intelligence and Statistics; 2019 Apr 16–18; Naha, Okinawa, Japan.

Smith KD, Jafarpour S, Swami A, Bullo F. Topology inference with multivariate cumulants: the Möbius inference algorithm. IEEE/ACM Transactions on Networking; 2020 May 16 [accessed 2022 Apr].

Tran T, Chan K, Pompili D. COSTA: cost-aware service caching and task offloading assignment in mobile-edge computing. 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON); 2019 June 10–13; Boston, MA. IEEE; c2019. p. 1–9.

Wheatman KS, Mehmeti F, Mahon M, Qiu H, Chan K, La Porta T. Optimal resource allocation for crowdsourced image processing. 2020 17th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON); 2020 June 22–25; Como, Italy. IEEE; c2020. p. 1–9.

Zafari F, Li J, Leung KK, Towsley D, Swami A. Optimal energy consumption for communication, computation, caching and quality guarantee. IEEE Transactions on Control of Network Systems. Mar 2020;7(1):151–162.

Zafari F, Leung KK, Towsley D, Basu P, Swami A, Li J. Let's share: a game-theoretic framework for resource sharing in mobile edge clouds. IEEE Transactions on Network and Service Management. June 2021;18(2):2107–2122.

Zhao T, Hou I, Wang S, Chan K. RED/LED: an asymptotically optimal and scalable online algorithm for edge-cloud reconfiguration. IEEE Journal on Selected Areas in Communications (JSAC) Special Issue on Caching. Aug 2018;38(6).

Network Control

Bovet G, Chan K. Reinforcement learning for quality of experience optimization in tactical networks. MILCOM 2018. 2018 IEEE Military Communications Conference; 2018 Oct 29–31; Los Angeles, CA.

Chakraborty S, Stein S, Brede M, Swami A, de Mel G, Restocchi V. Competitive influence maximization using voting dynamics. IEEE/ACM Int'l Conf on

Advances in Social Networks Analysis and Mining (ASONAM); 2019 Aug 27–30; Vancouver, British Columbia, Canada.

Chakraborty S, Stein S, Brede M, Swami A, de Mel G. Competitive influence maximization on signed networks. 4th Annual Fall Meeting of the DAIS ITA; 2020 Sep.

Cisneros-Velarde P, Oliveira DFM, Chan KS. Spread and control of misinformation with heterogeneous agents. In: Cornelius S, Granell Martorell C, Gómez-Gardeñes J, Gonçalves B, editors. Complex Networks X. CompleNet 2019. Springer Proceedings in Complexity. Springer, Cham; c2019.

Cisneros-Velarde P, Chan K, Bullo F. Polarization and fluctuations in signed social networks. IEEE Transactions on Automatic Control: Technical Notes and Correspondence. Aug 2021;66(8).

Ghosh P, Bunton J, Pylorof D, Vieira M, Chan K, Govindan R, Sukhatme G, Tabuada P, Verma G. Rapid top-down synthesis of large-scale IoT networks. IEEE ICCCN 2020. International Conference on Computer Communications and Networks; 2020 Aug 3–6; Honolulu, HI. p. 1–9.

Ghosh P, Bunton J, Pylorof D, Vieira M, Chan K, Govindan R, Sukhatme G, Tabuada P, Verma G. Synthesis of large-scale instant IoT networks. IEEE Transactions on Mobile Computing; 2021 July 26.

Pal S, Yu F, Novick Y, Swami A, Bar-Noy A. A study on the friendship paradox: quantitative analysis and relationship with homophily. Applied Network Science. Dec 2019;4(71).

Pylorof D, Bakolas E, Chan K. Design of robust Lyapunov-based observers for standalone and networked nonlinear systems with sum-of-squares programming. IEEE Control Systems Letters. Apr 2020;4(2):283–288.

Turalska M, Burghardt K, Rohden M, Swami A, D’Souza RM. Cascading failures in scale-free interdependent networks. Physical Review. Mar 2019;E99:032308.

Turalska M, Swami A. Greedy control of cascading failures in interdependent networks. Scientific Reports. 2021;11(1):3276.

Tactical Networks

Chan K, Marcus K, Judd G, Boyd P. Semantically managed autonomous and resilient tactical networking (SMARTNET) and hybrid C2 operations.

ICCRTS 2018. International Command and Control Research and Technology Symposium; 2018 Nov.

Chan K, Judd G, Szabo C, Radenovic V, Boyd P, Marcus K. Networked information transfer strategies for multidomain command and control. ICCRTS 2019. International Command and Control Research and Technology Symposium; 2019a Oct.

Chan K, Judd G, Johnson W, Boyd P, Szabo C, Marcus K. Representing and reasoning over military context information in complex multi domain battlespaces using artificial intelligence and machine learning. 2019 SPIE Defense & Commercial Sensing (DCS) Conference on Artificial Intelligence and Machine Learning for Multi Domain Battle Applications; 2019b Apr.

Craggs D, Chen X, Lee K, Szabo C, Radenovic V, Chan K. Optimizing communication strategies in contested and dynamic environments. ICECCS 2020. 2020 25th International Conference on Engineering of Complex Computer Systems (ICECCS); 2021 Mar 4–6; Singapore. p. 197–205.

Gokarslan K, Li G, Baker P, Le F, Kompella S, Marcus KM, Mishra VK, Tucker J, Yang YR, Yu P. Highly reliable and programmable software defined coalition (SDC) architecture using multiple control plane composition with distributed verification. DAIS ITA Annual Fall Meeting 2019.

Jansen N, Manso M, Toth A, Chan K, Bloebaum T, Johnsen F. NATO core services profiling for hybrid tactical networks – results and recommendations. ICMCIS 2021; 2021 May.

Johnsen F, Bloebaum T, Jansen N, Bovet G, Manso M, Toth A, Chan K. Evaluating publish/subscribe standards for situational awareness using realistic radio models and emulated testbed. ICCRTS 2019; 2019 Oct.

Judd G, Chan K. Enhancement of battlespace information management systems for coalition networks using C2 agility design concepts. ICCRTS 2017; 2017 Nov.

Judd G, Lorke R, Boyd P, Chan K. Upping the IQ of Army's digital communications. International Conference on Science and Innovation for Land Power; 2018 Sep.

Judd G, Radenovic V, Boyd P, Chan K, Marcus K, Szabo C, Coyle A. Achieving intelligent and resilient information exchange across complex and contested tactical edge networks. MILCIS; 2019 Nov.

Li G, Mudvari A, Gokarslan K, Baker P, Kompella S, Le F, Marcus KM, Tucker J, Yang YR, Yu P. Magnalium: highly reliable SDC networks with multiple control plane composition. 2019 IEEE International Conference on Smart Computing (SMARTCOMP); 2019 June 12–15; Washington DC. p. 93–98, doi:10.1109/SMARTCOMP.2019.00035.

Manso M, Johnsen F, Chan K, Jansen N. Mobile tactical force situational awareness: evaluation of message broker middleware for information exchange. ICCRTS 2018; 2018a Nov.

Manso M, Johnsen F, Lund K, Chan K. Using MQTT to support mobile tactical force situational awareness. 2018 International Conference on Military Communications and Information systems (ICMCIS); 2018b May 22–23; Warsaw, Poland.

Manso M, Guerra B, Freire F, Jansen N, Chan K, Toth A, Johnsen F, Bloebaum T. Mobile tactical forces: experiments on multi-broker messaging middleware in a coalition setting. ICCRTS 2019; 2019 Oct.

Marcus K, Chan K, Hardy R, Yu PL. An environment for tactical SDN experimentation. MILCOM 2018. 2018 IEEE Military Communications Conference (MILCOM); 2018 Oct 29–31.

Meiler P, Johnsen F, Bloebaum T, Manso M, Alcaraz Calero J, Wang Q, Owens I, Jansen N, Barz C, Sliwa J, Chan K. Improving integration between tactical and HQ levels by making SOA applicable on the battlefield. ICCRTS 2017; 2017 Nov.

Poularkis K, Qin Q, Marcus K, Chan K, Leung K, Tassiulas L. Hybrid SDN control in mobile ad hoc networks. SMARTCOMP 2019 Workshop on Distributed Analytics Infrastructure and Algorithms for Multi-Organization Federations (DAIS); 2019 Mar.

Qin Q, Poularakis K, Tassiulas L, Leung KK, Le F, Yu P. Learning-aided SDC control with programmable switches. DAIS ITA AFM 2020.

Qin Q, Poularakis K, Martens A, Chan KS, Tassiulas L. Learning-aided SDC control in mobile ad hoc networks. Proc. SPIE 11746, Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications; 2021.

Verma G, Marcus K, Chan K. Optimizing the quality of information of networked machine learning agents. Elsevier JNCA Journal of Network and Computer Applications. Jan 2022;197(103242).

Xiang Q, Le F, Lim Y-S, Mishra VK, Yu P, Tucker J, Yang YR. SFP: toward interdomain coalition programming. DAIS ITA Annual Fall Meeting 2019.

Zhang Z, Ma L, Poularakis K, Leung KK, Tucker J, Swami A. MACS: deep reinforcement learning based SDN controller synchronization policy design. IEEE Int'l Conf on Network Protocols (ICNP); 2019 Oct. p. 1–11.

Obfuscation

Ciftcioglu E, Hardy R, Chan K, Scott L, Oliveira D, Verma G. Chaff allocation and performance for network traffic obfuscation. IEEE The International Conference on Distributed Computing Systems (ICDCS) 2018; 2018 July.

He T, Ciftcioglu E, Wang S, Chan K. Location privacy in mobile edge clouds: a chaff-based approach. IEEE Journal on Selected Areas in Communications. Nov 2017;24(11).

Tomsett R, Chakraborty S, Chan K. Model poisoning attacks against distributed machine learning systems. 2019 SPIE Defense & Commercial Sensing (DCS) Conference on Artificial Intelligence and Machine Learning for Multi Domain Battle Applications; 2019 Apr.

Verma G, Ciftcioglu E, Sheatsley R, Chan K, Scott L. Network traffic obfuscation: an adversarial machine learning approach. MILCOM 2018; 2018 Oct.

Practical Security

Beemer O, Kosut J, Kliewer J, Graves E, Yu PL. Authentication against a myopic adversary. 2019 IEEE Conference on Communications and Network Security (CNS); 2019 June 10–12. IEEE; 2019a.

Beemer O, Kosut J, Kliewer J, Graves E, Yu PL. Structured coding for authentication in the presence of a malicious adversary. ISIT 2019. IEEE International Symposium on Information Theory; 2019 July 7–12. IEEE; 2019b.

Beemer O, Graves E, Kliewer J, Kosut O, Yu PL. Authentication with mildly myopic adversaries. 2020 IEEE International Symposium on Information Theory (ISIT); 2020 June 21–26. IEEE; 2020a. p. 984–989.

Beemer O, Graves E, Kliewer J, Kosut O, Yu PL. Authentication and partial message correction over adversarial multiple-access channels. IEEE International Workshop on Privacy and Security for Information Systems (WPS); 2020b.

Beemer O, Kosut O, Kliewer J, Graves E, Yu PL. Method for efficient authentication in unsecured environments. United States patent application 63/048,893. Filed 2020c July 7.

Perazzone JB, Graves E, Yu PL, Blum RS. Inner bound for the capacity region of noisy channels with an authentication requirement. ISIT 2018b.

Perazzone J, Yu PL, Sadler BM, Blum RS. Cryptographic side-channel signaling and authentication via fingerprint embedding. IEEE Transactions on Information Forensics and Security. Sep 2018a;13(9):2216–2225.

Perazzone JB, Yu PL, Sadler BM, Blum RS. Artificial noise and physical layer authentication: MISO regime. IEEE Conference on Communications and Network Security (CNS); 2019a.

Perazzone JB, Yu PL, Sadler BM, Blum RS. Physical layer authentication via fingerprint embedding: min-entropy analysis: invited presentation. 2019 53rd Annual Conference on Information Sciences and Systems (CISS); 2019b.

Perazzone JB, Yu PL, Sadler BM, Blum RS. Artificial noise-aided physical layer authentication with imperfect CSI. IEEE Transactions on Information Forensics and Security. 2021;16:2173-2185.

Moving Target Defense

Cho J-H, Sharma DP, Alavizadeh H, Ben-Asher N, Yoon S, Moore TJ, Kim DS, Lim H, Nelson FF. Toward proactive, adaptive defense: a survey on moving target defense. IEEE Communications Surveys and Tutorials. First quarter 2020;22(1):709–745. arxiv.org/abs/1909.08092 https://doi.org/10.1109/COMST.2019.2963791.

Dishington C, Sharma DP, Kim DS, Cho J-H, Moore TJ, Nelson FF. Security and performance assessment of IP multiplexing moving target defence in software defined networks. IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom); 2019 Aug 5–8. p. 288–295. doi.org/10.1109/TrustCom/BigDataSE.2019.00046.

Kim DS, Kim M, Cho J-H, Lim H, Moore TJ, Nelson FF. Design and performance analysis of software defined networking-based web services adopting moving target defense. In: 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks-Supplemental (DSN-S) Volume; 2020 June 29–July 2. p. 43–33. doi.org/10.1109/DSN-S50200.2020.00024.

Kim S, Yoon S, Cho J-H, Kim DS, Moore TJ, Free-Nelson F, Lim H. DIVERGENCE: deep reinforcement learning-based adaptive traffic inspection and moving target defense countermeasure framework. IEEE Transactions on Network and Service Management, early access; 2022 Jan. doi.org/10.1109/TNSM.2021.3139928.

Lee J, Kim W, Cho J-H, Kim DS, Moore TJ, Nelson FF, Lim H. Deep learning approach for attack detection in controller area networks. Proceedings of Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications III, vol. 11746, p. 117460W, SPIE Defense _ Commercial Sensing; 2021 Apr 12. doi.org/10.1117/12.2587015.

Mendonca J, Cho J-H, Moore TJ, Nelson FF, Lim H, Zimmermann A, Kim DS, Performability analysis of services in a software-defined networking adopting time-based moving target defense mechanisms. Proceedings of the 35th Annual ACM Symposium on Applied Computing (SAC'20); 2020 Mar 30–Apr 3. p. 1180–1189. doi.org/10.1145/3341105.3374016.

Mendonca J, Cho J-H, Moore TJ, Nelson FF, Lim H, Kim DD. Performance impact analysis of services under a time-based moving target defense mechanism. The Journal of Defense Modeling and Simulation. Aug 2021;15485129211036937. doi.org/10.1177/15485129211036937.

Narantuya J, Cho J-H, Kim DS, Moore TJ, Nelson FF. SDN-based IP shuffling moving target defense with multiple SDN controllers. IEEE/IFIP International Conference on Dependable Systems and Networks (DSN); 2019 Jun 24–27. p. 15–16. doi.org/10.1109/DSN-S.2019.00013.

Sharma DP, Cho J-H, Moore TJ, Nelson FF, Lim H, Kim DS. Random host and service multiplexing for moving target defense in software-defined networks. IEEE International Conference on Communications; 2019 May 20–24. p. 1–6. doi.org/10.1109/ICC.2019.8761496.

Sharma DP, Kim DS, Yoon S, Lim H, Cho J-H, Moore TJ. FRVM: flexible random virtual IP multiplexing in software-defined networks. 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE); 2018 Aug 1–3. doi.org/10.1109/TrustCom/BigDataSE.2018.00088.

Sharma DP, Enoch SY, Cho J-H, Moore TJ, Nelson FF, Lim H, Kim DS. Dynamic security metrics for software-defined network-based moving target defense. Journal of Network and Computer Applications. 15 Nov 2020;170:102805. doi.org/10.1016/j.jnca.2020.102805.

Yoon S, Cho J-H, Kim DS, Moore TJ, Nelson FF, Lim H. Attack graph-based moving target defense in software-defined networks. IEEE Transactions on Network and Service Management. Sep 2020a;17(3):16531668. doi.org/10.1109/TNSM.2020.2987085.

Yoon S, Cho J-H, Kim DS, Moore TJ, Nelson FF, Lim H, Leslie N, Kamhoua C. Moving target defense for in-vehicle software-defined networking: IP shuffling in network slicing with multiagent deep reinforcement learning. Proceedings of Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications II, vol. 11413, p. 11413U, SPIE Defense + Commercial Sensing; 2020b 27 April–1 May. doi.org/10.1117/12.2557850.

Yoon S, Cho J-H, Kim DS, Moore TJ, Free-Nelson F, Lim H. DESOLATOR: deep reinforcement learning-based resource allocation and moving target defense deployment framework. IEEE Access. Apr 2021;9:70700–70714. doi.org/10.1109/ACCESS.2021.3076599.

Network Systems Diversity for Resilience

Cho J-H, Moore TJ. Percolation-based network adaptability under correlated failures. IEEE International Conference on Computer Communications (INFOCOM 2018); 2018 Apr 15–19. p. 2186–2194. doi.org/10.1109/INFOCOM.2018.8486342.

Cho J-H, Moore TJ. Software diversity for cyber resilience: percolation theoretic approach. In: El-Alfy E-SM, Eltoweissy M, Fulp E, Mazurczyk W, editors. Nature-inspired Cyber Security and Resiliency: Fundamentals, Techniques, and Applications. Institution of Engineering and Technology; 2019. doi.org/10.1049/PBSE010E_ch12.

Moore TJ, Cho J-H, Chen I-R. Network adaptations under cascading failures for mission-oriented networks. IEEE Transactions on Network and Service Management. Sept 2019;16(3):1184–1198. doi.org/10.1109/TNSM.2019.2917934.

Zhang Q, Cho J-H, Moore TJ. Network resilience under epidemic attacks: deep reinforcement learning network topology adaptations. IEEE Global Communications Conference (GLOBECOM); 2021a 7–11 Dec. p. 1–7. doi.org/10.1109/GLOBECOM46510.2021.9686036.

Zhang Q, Cho J-H, Moore TJ, Chen I-R. Vulnerability-aware resilient networks: Software diversity-based network adaptation. IEEE Transactions on Network and Service Management. Sep 2021b;18(3):3154–3169. doi.org/10.1109/TNSM.2020.3047649. arxiv.org/abs/2007.08469.

Zhang Q, Cho J-H, Moore TJ, Nelson FF. DREVAN: Deep reinforcement learning-based vulnerability-aware network adaptations for resilient networks. IEEE Conference on Communications and Network Security; 2021c Oct 4–6. p. 137–145. doi.org/10.1109/CNS53000.2021.9705041.

Zhang Q, Mohammed AZ, Wan Z, Cho J-H, Moore TJ. Diversity-by-design for dependable and secure cyber-physical systems: a survey. IEEE Transactions on Network and Service Management. Mar 2022;19(1):706–728. doi.org/10.1109/TNSM.2021.3091391. arxiv.org/abs/2007.08688.

AFC Documents

[AFC] Army Futures Command concept for command and control 2028: pursuing decision dominance; 2021a July 14. AFC Pamphlet No. 71-20-9. https://api.army.mil/e2/c/downloads/2021/10/06/ffd892d0/afc-concept-for-command-and-control-2028-pursuing-decision-dominance-oct21.pdf

[AFC] Army Futures Command concept for cyberspace and electromagnetic operations 2028; 2021b June 29. AFC Pamphlet No. 71-20-8. https://api.army.mil/e2/c/downloads/2021/07/08/fbd7fb76/20210629-afc-pam-71-20-8-cyberspace-and-electromagnetic-warfare-operations-approved.pdf

[AFC] Army Futures Command concept for fires 2028; 2021c Sep 15. AFC Pamphlet No. 71-20-6. https://api.army.mil/e2/c/downloads/2021/10/06/869ca62b/afc-concept-for-fires-2028-oct21.pdf

List of Symbols, Abbreviations, and Acronyms

2-D	two-dimensional
AFC	Army Futures Command
AI	artificial intelligence
AML	Adversarial Machine Learning
ARL	Army Research Laboratory
C2	Command and Control
C4ISR	Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance
C5ISR	Command, Control, Communication, Computers, Cyber, Intelligence, Surveillance and Reconnaissance
COVID-19	coronavirus disease 2019
CRA	Collaborative Research Alliance
DAIS ITA	Distributed Analytics and Information Sciences International Technology Alliance
DDIL	denied, disconnected, intermittent-connectivity, limited bandwidth
DEVCOM	US Army Combat Capabilities Development Command
DIL	disconnected, intermittent, and limited
DL	deep learning
EMANE	Extendable Mobile Ad-hoc Network Emulator
FI	friendship index
FREEDOM	Foundational Research for Electronic Warfare in Multi-Domain Operations
GPU	graphics processing unit
HW/SW	hardware/software
IoBT	Internet of Battlefield Things
IoT	Internet of Things

IP	Internet Protocol
ISR	Intelligence Surveillance Reconnaissance
IST	Information Systems Technology
ITC-PAC	International Technology Center – Pacific
MDO	multidomain operations
MILP	mixed-integer linear programming
ML	machine learning
MTD	moving target defense
NATO	North Atlantic Treaty Organization
NATO STO IST	NATO Science and Technology Organization Information Systems Technology
NFV	Network Function Virtualization
NP	nondeterministic polynomial-time
ONOS	Open Network Operating System
POT	power-of-two
RF	radio frequency
S&T	Science and Technology
SDC	software defined coalition
SDN	software defined networking
SMARTNET	Semantically Managed Autonomous Resilient Tactical Networks
SMC	satisfiability modulo convex
SWAP	size, weight, and power
TTCP	The Technical Cooperation Program

1 DEFENSE TECHNICAL
(PDF) INFORMATION CTR
DTIC OCA

1 DEVCOM ARL
(PDF) FCDD RLD DCI
TECH LIB

1 DA HQ
(PDF) DASA(R&T)

9 USARMY AFC
(PDF) L BROUSSEAU
J REGO
A LINZ
K WADE
S BRADY
J REGO
T KELLY
E JOSEPH
B SESSLER

2 DEVCOM HQ
(PDF) FCDD ST
C SAMMS
M HUBBARD

83 DEVCOM ARL
(PDF) FCDD RLC
C BEDELL
B SADLER
B PIEKARSKI
H EVERITT
FCDD RLC CA
L KAPLAN
FCDD RLC ES
G VIDEEN
S HILL
Y PAN
FCDD RLC I
B MACCALL
FCDD RLC N
BM RIVERA
A SWAMI
FCDD RLC NT
K CHAN
E GRAVES
K MARCUS
T MOORE
J PERAZZONE
L SCOTT
A SWAMI
A TOTH
G VERMA
P YU
FCDD RLD
P BAKER
A KOTT
K JACOBS
FCDD RLD D
T ROSENBERGER
FCDD RLD E
KS FOSTER
FCDD RLD F
K KAPPRA
FCDD RLD FR
M TSCHOPP
FCDD RLD SM
L BLUM
FCDD RLH
J CHEN
PJ FRANASZCZUK
C LANE
K MCDOWELL
FCDD RLH B
JJ SUMNER
FCDD RLH F
JR GASTON
FCDD RLH T
D STRATIS-CULLUM
FCDD RLL
T KINES
FCDD RLL D
J S ADAMS
FCDD RLL DP
J MCCLURE
FCDD RLR
B HALPERN
S LEE
D STEPP
FCDD RLR E
RA MANTZ
C VARANASI
FCDD RLR EL
JX QIU
MD ULRICH
FCDD RLR EN
RA ANTHENIEN JR
FCDD RLR IC
MA FIELDS
SP IYER
FCDD RLR IM
JD MYERS
FCDD RLR IN
XN WANG
FCDD RLR
P REYNOLDS
FCDD RLR P
LL TROYER
FCDD RLR PC
D POREE

FCDD RLR PL
MK STRAND
FCDD RLS
J ALEXANDER
M GOVONI
M WRABACK
FCDD RLS C
M REED
FCDD RLS CC
S BEDAIR
FCDD RLS CE
TR JOW
K XU
FCDD RLS CL
M DUBINSKIY
FCDD RLS E
RD DELROSARIO
FCDD RLS ED
K JONES
FCDD RLS EA
A ZAGHLOUL
FCDD RLS S
WL BENARD
FCDD RLS SO
W ZHOU
FCDD RLW
S KARNA
JF NEWILL
AM RAWLETT
SE SCHOENFELD
J ZABINSKI
FCDD RLW B
R BECKER
FCDD RLW M
ES CHIN
FCDD RLW S
V CHAMPAGNE
AL WEST
FCDD RLW T
RZ FRANCART
FCDD RLW TC
JD CLAYTON
FCDD RLW W
TV SHEPPARD
FCDD RLW WA
B RICE
R PESCE-RODRIGUEZ
FCDD RLW M
A HALL