Abstract—In this position paper, we discuss the critical need for integrating zero trust (ZT) principles into next-generation communication networks (5G/6G) for both tactical and commercial applications. We highlight the challenges and introduce the concept of an intelligent zero trust architecture (i-ZTA) as a security framework in 5G/6G networks with untrusted components. While network virtualization, software-defined networking (SDN), and service-based architectures (SBA) are key enablers of 5G networks, operating in an untrusted environment has also become a key feature of the networks. Further, seamless connectivity to a high volume of devices in multi-radio access technology (RAT) has broadened the attack surface on information infrastructure. Network assurance in a dynamic untrusted environment calls for revolutionary architectures beyond existing static security frameworks. This paper presents the architectural design of an i-ZTA upon which modern artificial intelligence (AI) algorithms can be developed to provide information security in untrusted networks. We introduce key ZT principles as real-time Monitoring of the security state of network assets, Evaluating the risk of individual access requests, and Deciding on access authorization using a dynamic trust algorithm, called MED components. The envisioned architecture adopts an SBA-based design, similar to the 3GPP specification of 5G networks, by leveraging the open radio access network (O-RAN) architecture with appropriate real-time engines and network interfaces for collecting necessary machine learning data. The i-ZTA is also expected to exploit the multi-access edge computing (MEC) technology of 5G as a key enabler of intelligent MED components for resource-constraint devices.

I. INTRODUCTION

Wireless communication has become the key enabler of emerging technologies such as autonomous vehicles, vehicle to everything (V2X) networks, smart cities, and internet-of-things (IoT) [1]. The fifth-generation (5G) networks provide a massive volume of heterogeneous devices with seamless connectivity and computational resources for autonomous and intelligent operation [2], [3]. Further, sixth-generation (6G) – and beyond – networks incorporate more agile radio environments, including satellite and unmanned aerial vehicle (UAV) communications, to provide a three-dimensional (3D) radio [4], [5]. However, traditional network security frameworks have obvious weaknesses in providing security assurance in such a complex and dynamic network environment.

Traditional network security models assume a network perimeter, as the trust zone, which is protected against unauthorized access. Any subject operating in the trust zone, after appropriate authentication and authorization, is deemed trusted. However, due to the agile radio environment, mobility, and heterogeneity of next-generation tactical networks, identification of the network perimeter is challenging if not impossible. More importantly, such models allow lateral movement of subjects in the trust zone after authentication.

The third generation partnership project (3GPP) has developed enhanced security frameworks specifically designed for 5G network architecture [6]. They introduce several security levels for various network functions including network access, user/application domains, and service-based architecture (SBA) security. The frameworks incorporate appropriate authentication, authorization and, key agreement protocols for the security of various technologies, such as device-to-device (D2D) and V2X communications, software-defined networking (SDN), and network function virtualization (NFV).

Most existing security protocols assume a strong trust relationship among network entities and services providing authentication and authorization. Such assumptions can lead to serious security vulnerabilities. A few scenarios where these vulnerabilities are exploited to deploy privacy attacks, denial-of-service (DoS), man-in-the-middle, and impersonation attacks, are discussed in [7].

Zero trust architecture (ZTA) is a solution to address security requirements in a network with untrusted infrastructure. A ZTA provides network assurance under the assumption that no subject, requesting access to the network resources, can be trusted even after initial authentication and authorization. Every access request is individually authorized and monitored during the access period for compliance with security policy rules. A dynamic trust evaluation for every access request is the key tent of zero trust (ZT). Authorizing the individual access requests by a subject rather than authorizing the subject requesting access is a key tenet of ZTA.

Dynamic risk assessment and trust evaluation are key elements of a ZTA. We introduce the architecture of an intelligent ZTA (i-ZTA) which provides a framework to employ artificial intelligence (AI) engines for information security in untrusted networks. We discuss the adoptability of open radio access network (O-RAN) for the integration of such i-ZTA. Further, we argue how the multi-access edge computing (MEC) technology of 5G networks can be exploited to provide resource-constraint devices with the necessary computational resources for realizing the envisioned i-ZTA.

The rest of the paper is organized as follows. Section II

Intelligent Zero Trust Architecture for 5G/6G Tactical Networks: Principles, Challenges, and the Role of Machine Learning

Keyvan Ramezanpour, Member, IEEE, Jithin Jagannath, Senior Member, IEEE
Marconi-Rosenblatt AI/ML Innovation Laboratory,
ANDRO Computational Solutions, LLC, USA
introduces ZT principles and the necessity for the i-ZTA. Challenges of integrating i-ZTA into existing networks and the distinct features of next-generation networks enabling i-ZTA are discussed in Section III. The envisioned architecture for the i-ZTA is explained in Section IV, and the paper concludes in Section V.

II. Why Intelligent Zero Trust Architecture

Ubiquitous connectivity through 5G networks is perceived by the U.S. Department of Defense (DoD) as a critical strategic technology that provides nations with long-term economic and military advantage [8]. Next-generation networks are especially important for mission-critical communications and tactical edge networks (TEN), involving a large volume of heterogeneous and resource-constraint devices. They provide necessary computational resources (through cloud computing) and seamless, reliable, and robust connectivity through a wide range of new radio access technologies (RAT), including satellite, UAV, D2D, and massive beamforming communications.

The deployment of a TEN, based on next-generation networks (5G/6G), is cost-effective (both in terms of CAPEX and OPEX) while programmable based on the needs of the particular environment. Hence, the deployment time of TEN with varying environmental needs reduces significantly. However, perimeter-based security models exhibit weaknesses in providing network assurance in a heterogeneous and dynamic network environment.

Even if perimeter security frameworks provide carefully-tailored protocols for various functions of 5G networks, the static nature of them still allows lateral movements in the network perimeter. Either due to internal human errors, social engineering attacks, or dynamics of 5G networks, an authenticated subject (which is trusted) can acquire unauthorized access to sensitive resources. Hence, i-ZTA will be the key technology for secure communication and data sharing from core 5G to tactical edge networks.

A. Zero Trust Principles

The main tenets of zero trust (ZT) are outlined in the special publication 800-27 of the U.S. National Institute of Standards and Technology (NIST) [9]. The key ZT principles are summarized in Fig. 1 and explained below.

- **Zero Trust**: All network assets and functions, including devices, computing resources, and services, are considered untrusted irrespective of the location in the network. Hence, all communications must meet the same security requirements as third parties.
- **Trust/Risk Evaluation**: Trust evaluation and risk assessment is conducted for every access request. The assessment is carried out continuously (during the period of the access) and dynamically (based on situational conditions).
- **Least Privilege**: Any access, if granted, should be authorized with the least privileges. The access is only granted for a specific resource (depending on the sensitivity of the resource) and is not valid for a different resource.
- **Dynamic Policy**: A dynamic policy is necessary for making decision on granting access. The key decision factors include security state (credentials, software version/patches, location, etc.) and behavioral attributes of the subject and network assets.
- **Integrity Check**: The security state of all network assets and requesting subjects are monitored continuously, preferably in real-time. The security posture of devices, and behavioral patterns of users/network assets, are evaluated with an automated system in terms of compliance with security policy rules.

B. Intelligent MED

The realization of ZT principles with static policies is overwhelming and challenging. Automated real-time monitoring and dynamic security evaluation are the key features of a ZTA. Further, with the growing volume of users, the ZTA components are dealing with big data. Hence, intelligent monitoring, evaluation, decision-making (MED), using artificial intelligence (AI), are the critical enablers of ZTA in the next-generation networks.

The MED components of an i-ZTA are shown in Fig. 2. The location of different blocks in this diagram reflects the logical interaction of the components and does not necessarily show their physical locations in the network. In this paper, we use the following terminology when referring to the i-ZTA. A **subject** is any user, application, or service requesting access to a network resource. The network **assets** refer to all devices, network infrastructure, and functions (including cloud services) involved in the communication. The network **resource** contains sensitive information that must be protected against unauthorized access.

The core of an i-ZTA comprises of a policy enforcement point (PEP) and a policy decision point (PDP). The PEP is the first point of contact for access request. It also establishes the connection between the subject and the requested resource if an access is granted. The decision on granting access is made by the PDP. It uses all available internal and external information about the security state of the subject and network assets for deciding.

The information used by the i-ZTA core to grant and monitor a connection is provided by several peripheral modules as
shown in Fig. 2. We divide these modules into two categories of static (right side of the figure) and dynamic (left side). The static modules (not specific to i-ZTA) include data access policy, public key infrastructure (PKI), identity (ID) management, and industry compliance. These modules, collectively, define the security policy rules for secure communication and integrity check rules. The policy rules can be dynamically adjusted by the i-ZTA core.

The dynamic modules in the diagram of Fig. 2, are the distinct features of an i-ZTA. These include continuous diagnostics and mitigation (CDM), threat intelligence (for identifying new security vulnerabilities), activity logs (behavioral information on user/assets and network traffic), and security information and event management (SIEM) for collecting information on long-term security state and potential attacks.

In addition to the peripherals, the core PEP and PDP functions incorporate appropriate AI engines for realizing the entire MED chain. Intelligent agent and portal (IGP) is the AI engine of the PEP which provides devices with situational awareness. The processing engine of PDP is intelligent policy engine (IPE) that makes decisions on granting access based on all information provided by INSSA, IGP, and policy rules. The details of the corresponding learning algorithms will be explained later in Section IV.

The i-ZTA of Fig. 2 divides the network into three logical, and possibly physical, planes. Data communication between the subject and network resources is carried out in data plane, which also includes the initial access request by the subject. The i-ZTA components (PEP and PDP) communicate in the control plane for making decisions and configuring connections. These two planes also exist in the current 5G network architectures. The third plane of the i-ZTA is metadata plane used for communicating all data required by the AI engines.

III. CHALLENGES AND OPPORTUNITIES

The realization of an i-ZTA, with real-time processing of big data might appear challenging. However, next-generation network architectures provide appropriate computational resources and interfaces for data collection needed by AI applications. In this section, we address part of the challenges and solutions for realizing the envisioned i-ZTA.

A. Real-time Processing

Seamless connectivity in beyond 5G networks implies that multiple RAT technologies are used dynamically in a single session of data communication. Furthermore, heterogeneous devices, with different security specifications, credentials, privileges, and computing resources participate in the communication. Hence, real-time monitoring and security evaluation of all involving devices is the necessity of an i-ZTA.

Next-generation network architectures integrate NVF cloud computing for the realization of real-time functions for intelligent processing engines, with commercial off-the-shelf hardware. A promising example is the O-RAN architecture that provides (near-)real-time (10ms to 1s) RAN intelligent controller (RIC), central (CU), distributed (DU), and radio units (RU). While initial use cases of real-time engines in O-RAN focus on connectivity management in multi-RAT and quality of experience (QoE) optimization [10], integration of i-ZTA functions is an emerging critical application.

B. Communication Overhead

Dynamic access in multi-RAT also implies a broadened attack surface. Third-party devices have now a wider range of access points to the network. They can manipulate an authorized user equipment (UE) to access network resources, or simply promote a hostile network environment to increase the perceived risk of access, hence, forcing the i-ZTA to decline access. Distributed location of network assets and massive volume of UEs has also facilitated the class of unintrusive precision cyber attacks which do not require privileged access to deploy the attack [11].

Detection and mitigation of such a broad attack surface require an analysis of network traffic by the i-ZTA, from
Fig. 3: Architecture of multi-access edge computing (MEC) integrated at the edge of 5G network with i-ZTA core, IGP and federated learning (FL) components.

C. Computational Requirements

The multi-RAT network and D2D communications allow attackers to exploit UEs without intrusion into the network. Hence, the envisioned i-ZTA requires all authorized devices to dynamically monitor their network environment for potential risks, as part of the intelligent MED. The major concern, however, is the limited computational resources of UEs, especially IoT node and sensor devices. We argue that multi-access edge computing (MEC) [12] in 5G networks can be leveraged to address this issue.

The MEC is a prominent example demonstrating the unique capabilities of 5G networks, which brings the computing resources as close as possible to the network edge. Hence, a high volume of devices, possibly with high mobility, may have access to high performance computing resources with low-latency connectivity. The MEC adapts a similar service-based architecture (SBA) of 5G networks according to 3GPP specifications. The deployment of MEC can be considered as a mapping onto a network application function (AF) interacting with other network core functions.

An example of MEC architecture deployed in a local area data network (LADN) is shown in Fig. 3. The MEC orchestrator is a 5G AF with centralized functions for managing the operation of MEC hosts. It also interfaces with the network exposure function (NEF) in the 5G core for overall management. A unique feature of 5G networks enabling the integration of this MEC architecture is the exposure of the network core to the LADN. The 5G core network is able to steer traffic to the applications in the LADN, where the MEC host operates.

The MEC hosts are deployed at the edge of 5G RAN to minimize latency and improve user QoE. An interesting feature of this architecture is the exposure of MEC hosts to radio information provided by the CUs and DUs of the RAN. The MEC platform may use radio information, e.g., signal power and quality, to further reduce latency by avoiding unnecessary routing traffic via the core network.

While MEC enables the deployment of some intelligent MED components, it is also protected by the i-ZTA. The 5G core incorporate appropriate functions such as NEF and policy control (for traffic steering) and unified data management (for user authentication, authorization, and service continuity) to provide untrusted AFs with requested services. While these functions provide static security measures, the i-ZTA core (Fig. 2) provides the dynamic security measures to authorize accesses to the MEC and monitor the sessions.

IV. ENVISIONED INTELLIGENT ZERO TRUST ARCHITECTURE

In this section, we introduce a novel unified framework (i-ZTA) with AI engines for information security in untrusted networks. The envisioned i-ZTA opens new research areas in the application domain of AI for information security. The key elements of the i-ZTA include:

- **IPE:** It employs an AI trust algorithm to authorize access requests based on subject privileges and security state, security policy rules, the network state, and a score that reflects the confidence level of the access. Specifically, the IPE is envisioned to employ reinforcement learning (RL) to maximize usability with the least privileges.
- **INSSA:** This engine can employ such models as a graph neural network (GNN) for the security state of the network. It carries out the risk assessment in accessing a given resource in the network. The INSSA also implements an anomaly detection to identify potential attacks.
- **IGP:** It is the user AI engine to model the security state of a subject. The IGP analyzes the security posture of the network traffic to the subject and provides it with environmental awareness. The learning objective of IGP is to keep a high confidence level of the subject in accessing the network resources.

A. Overall Architecture

The architecture of the i-ZTA integrated in the O-RAN architecture is shown in Fig. 4. It exploits the O-RAN real-time processing and data collection for realizing the intelligent policy engine and AI network state analysis, and the MEC for intelligent agent and portal components of MED. The O-RAN further provides appropriate interfaces for near-real time monitoring of remote devices and services.

In our envisioned i-ZTA, the PEP is divided into three components: agent, portal, and gateway. The agent is a lightweight...
software module on every network asset requiring access to the resources. The portal, residing on the PEP, performs a similar task but is intended for resource-constraint devices, such as IoT and sensor devices. The gateway is an agent residing in front of the network resource and is directly configured by the policy administrator (PA).

The agent and the portal incorporate AI algorithms, that work together in a federated learning approach, as described below. We refer to the learning components of the agent and the portal as IGP, collectively.

B. Intelligent agent/portal (IGP)

We define the environmental awareness (ENA) of a subject as the first tenet of trust evaluation. The role of IGP is to provide the network assets, that require access to the resources, with an ENA score, and a model for their security posture. The subjects with higher ENA value might obtain higher confidence score in risk assessment by the IPE.

We envisage the agent to employ a reinforcement learning (RL) engine that conducts three main tasks: 1) It analyzes the traffic of the device in the network which provides an initial risk assessment on the network environment; 2) It learns the flow of unnecessary communication in the device that may reduce its confidence level in accessing certain resources; 3) It provides a model for the communication pattern of the device which is passed along with an access request to the PEP for overall risk assessment.

The portal is divided into two major components: 1) access request management from resource-constraint devices without computational capability to host the intelligent agent, and 2) a learning component that supports federated learning of the agents. We envision the importance of federated learning for collaborative and distributed learning of a comprehensive model for the network environment.

As discussed above, every agent employs RL to learn its network environment and best practices in communicating with network entities. The RL model used by multiple agents can be a common model, trained in the federated learning approach with the following clear advantages.

- By aggregating the experience of multiple agents, a more comprehensive model of the local network environment is trained by distributed subjects.
- The visibility of individual agents on the network environment is increased.
- It provides subjects with a model for a network environment that is able to detect distributed attackers exploiting multiple subjects.

C. Intelligent network security state analysis (INSSA)

The second tenet of trust evaluation is the dynamic risk assessment for every access request. In a 5G network, the mobility of heterogeneous devices in a varying environment calls for a dynamic model of the network state that provides information about the risks of accessing a particular resource by a given subject. We propose using a graph neural network (GNN) to model the state of the 5G network which is of particular interest in risk assessment by the IPE.

Graph neural networks have been shown to be successful as a scalable approach for resource allocation in large area wireless networks [13]. In these applications, the GNN models the channel state between pairs of communicating nodes and the goal is an optimal allocation of spectrum resources to the nodes. The INSSA employs a GNN to model the communication patterns of a 5G network and the goal is to assign risk
The envisaged INSSA employs reinforcement learning to meet the following objectives: 1) compliance with a set of security policy rules, 2) authorizing accesses with the least privileges, and 3) maximizing network usability. The RL algorithm dynamically assigns appropriate scores to all nodes in the network so as an assurance score (as the reward) is maximized, by inspecting how strictly the policy rules are met by the nodes while the network is available to all users.

A second critical task of the INSSA is anomaly detection. The goal of this task is to detect and prevent potential attacks, such as DoS and distributed DoS (DDoS), that target the PEP. Additionally, INSSA protects the network against a more subtle DoS attack which we call intelligent DoS (iDoS) in this paper. As discussed above, the i-ZTA incorporates environmental information of the network to evaluate the access request. A potential attacker can indirectly make the PE deny access by promoting a hostile network environment, hence increasing the risk of granting the access. The INSSA uses the GNN model of the network to detect such activities and potential attacks.

The INSSA follows an adversarial learning approach [14] for risk assessment and anomaly detection. In addition to the node risk scores, the risk of operating in a network environment contributes to the overall network assurance score. The block diagram of Fig. 5 illustrates the flow of the proposed adversarial learning. While the GNN (as the RL agent) attempts in maximizing network usability with least privileges, an adversarial network is trained with the objective of maximizing privileges compliant with the security policy rules. The result is a GNN model of the network trained to assess the risk of access in the presence of intelligent distributed attackers exploiting network assets.

**D. Intelligent policy engine (IPE)**

The endpoint of trust evaluation is the IPE. Like the agent/portal and INSSA, the IPE incorporates an AI engine to make the final decision on granting a requested access based on the agent and network state. The IPE employs a neural network with long- and short-term memories to evaluate the risk of granting access to an agent based on all previous activities of the agent and the network. The IPE provides a C-score as the confidence-level of the access.

The IPE policy is optimized through an RL algorithm to minimize the probabilities of false positives and false negatives. After making a decision (access grant or denial), the IPE monitors the security state of the session (how strictly the agent conforms to the security policy rules). The IPE also receives the future state of the agent from the INSSA to evaluate the reward return corresponding to the decision. The IPE uses the collected information to evaluate the risk of the agent for its future transactions.

The memory of IPE policy is an important feature for risk assessment. A potential intelligent attacker does not deviate from the security policy rules with observable traces. Rather, it attempts in exploiting multiple network assets by taking incremental steps toward malicious activities or unauthorized access to sensitive information, distributed over space and time. While the spatial security state is modeled by the INSSA, the IPE provides the temporal model.

It is important for the IPE to incorporate all previous and future states of the subject and the network for risk assessment. We divide the learning policy of the IPE into two sub-components with long- and short-term memories. The short-term memory allows granting access to agents which corrected their security state over time. The long-term memory enables IPE to detect adversaries exploiting vulnerabilities with incremental steps over time.

An example concept-level architecture of the IPE neural network (NN) with long- and short-term information is shown in Fig. 6. The NN consists of a few recurrent layers followed by convolutional layers. It has been demonstrated that recurrent NN, such as long short-term memory, is powerful in temporal modeling of a time-series signal and convolutional layers are capable of filtering noisy spectral components and extracting local features of the signal [15]. Hence, the IPE NN extracts temporal information on the security behavior of the subject, over medium to long time periods, while the convolutional layers extract local (shorter time periods) security features of the subject.

It is envisaged that all components and AI engines, introduced in this section, work together in a cohesive framework to meet the enhanced security needs of military as well as commercial 5G/6G networks in the future. Using this framework, sensitive applications may benefit from widespread adoptibility and low-cost deployment of these networks without compromising information security.

**V. CONCLUSION AND FUTURE WORK**

Network assurance in the untrusted environment of 5G/6G networks demands for dynamic authorization, risk assessment

![Fig. 5: Adversarial learning methodology to maximize network assurance with objectives of minimum privileges, maximum usability and strict compliance with security policy.](image-url)
untrusted networks. The application of AI for providing information security in the context of zero trust (ZT) principles is discussed in this paper motivates new research directions in risk assessment. It is our sincere hope that the i-ZTA vision (GNN) for network modeling and adversarial learning for state analysis (INSSA) which employs graph neural networks for realizing ZT principles in untrusted networks. The i-ZTA adopts an SBA-based design with AI engines for realizing ZT principles in untrusted networks. The i-ZTA core includes the intelligent policy engine (IPE) and the intelligent agent portal (IGP) for dynamic authorization of network assets and monitoring of network assets. Realization of zero trust (ZT) principles, necessary for providing information security in such environments, require real-time processing of big data. In our opinion, the envisioned intelligent architecture (i-ZTA) in this paper can help guarantee ZT principles for tactical application by leveraging distinct technologies of 5G networks as the key enablers of the i-ZTA.

The i-ZTA adopts an SBA-based design with AI engines for realizing ZT principles in untrusted networks. The i-ZTA core includes the intelligent policy engine (IPE) and the intelligent agent portal (IGP) for dynamic authorization of access requests. The former uses reinforcement learning, with the objective of maximizing an assurance score, and the latter uses federated learning to provide users with environmental awareness score (EVA). Dynamic monitoring of the network assets is also realized with the intelligent network security awareness score (EVA). Dynamic monitoring and local security features (Conv. layers) of network activities.

and monitoring of network assets. Realization of zero trust (ZT) principles, necessary for providing information security in such environments, require real-time processing of big data. In our opinion, the envisioned intelligent architecture (i-ZTA) in this paper can help guarantee ZT principles for tactical application by leveraging distinct technologies of 5G networks as the key enablers of the i-ZTA.

The i-ZTA adopts an SBA-based design with AI engines for realizing ZT principles in untrusted networks. The i-ZTA core includes the intelligent policy engine (IPE) and the intelligent agent portal (IGP) for dynamic authorization of access requests. The former uses reinforcement learning, with the objective of maximizing an assurance score, and the latter uses federated learning to provide users with environmental awareness score (EVA). Dynamic monitoring of the network assets is also realized with the intelligent network security awareness score (INSSA) which employs graph neural networks (GNN) for network modeling and adversarial learning for risk assessment. It is our sincere hope that the i-ZTA vision discussed in this paper motivates new research directions in the application of AI for providing information security in untrusted networks.

REFERENCES

[1] X. Shen, R. Fantacci, and S. Chen, “Internet of vehicles,” Proceedings of the IEEE, vol. 108, no. 2, pp. 242–245, 2020.

[2] J. Jagannath, N. Polosky, A. Jagannath, F. Restuccia, and T. Melodia, “Machine learning for wireless communications in the Internet of Things: A comprehensive survey,” Ad Hoc Networks, vol. 93, p. 101913, 2019.

[3] M. Yao, M. Sohul, V. Marojevic, and J. H. Reed, “Artificial intelligence defined 5G radio access networks,” IEEE Communications Magazine, vol. 57, no. 3, pp. 14–20, 2019.

Keyvan Ramezanpour completed a PhD in Electrical Engineering in the Bradley Department of Electrical and Computer Engineering at Virginia Tech. Dr. Ramezanpour currently is a senior researcher at the Marconi-Rosenblatt AI/ML Innovation Lab at ANDRO Computational Solutions. His research expertise include secure implementation of cryptographic algorithms on field programmable gate arrays (FPGA), Systems-on-Chip (SoC) and application-specific integrated circuits (ASIC), and unsupervised deep learning techniques for security assessment of hardware implementations. His research interests include security architecture of next-generation networks and security assessment and analysis of networks, devices and circuits using deep learning.

Jithin Jagannath [SM’19] is the Director of the Marconi-Rosenblatt AI/ML Innovation Lab at ANDRO Computational Solutions. He is also the Adjunct Assistant Professor at the University at Buffalo, State University of New York. He received his Ph.D. degree from the Northeastern University. Dr. Jagannath heads several of the ANDRO’s research and development projects in the field of 5G and beyond, signal processing, SIGINT, machine learning, MIMO, cognitive radio, and cross-layer optimization. He is the Principal Investigator of several research projects including RIFs and SBIRs funded by the U.S. Army, Navy, SOCOM, and DHS. He is an IEEE Senior member and serves as an IEEE SPS Applied Signal Processing Systems Technical Committee member. Dr. Jagannath’s recent research has led to several peer-reviewed publications and nine U.S. Patents (granted, pending). He also renders his service as Editor, TPC Member, and Reviewer to several leading journals and conferences.