Techniques for Realizing Secure, Resilient and Differentiated 5G Operations

Akram Hakiri*, Aniruddha S. Gokhale†, Yogesh Barve†, Valerio Formicola†† §, Shashank Shekhar‡, Charif Mahmoudi‡, Mohammad Ashiqur Rahman**, Uttam Ghosh¶, Syed Rafay Hasan‖ and Terry Guo‖
*University of Carthage, ISSAT, Tunis, Tunisia.
†Vanderbilt University, Nashville, TN, USA
‡Siemens Technology, Princeton, NJ, USA.
**Florida International University, Miami, FL, USA
¶Meharry Medical College, School of Applied Computational Sciences, Nashville, TN, USA.
‖Tennessee Tech University, Nashville, TN, USA.
†† California Polytechnic State University Pomona, CA, USA.
Corresponding Authors: akram.hakiri@issatm.rnu.tn and a.gokhale@vanderbilt.edu

***Abstract*—The 5G ecosystem is designed as a highly sophisticated and modularized architecture that decouples the radio access network (RAN), the multi-access edge computing (MEC) and the mobile core to enable different and scalable deployments. It leverages modern principles of virtualized network functions, microservices-based service chaining, and cloud-native software stacks. Moreover, it provides built-in security and mechanisms for slicing. Despite all these capabilities, there remain many gaps and opportunities for additional capabilities to support end-to-end secure operations for applications across many domains. Although 5G supports mechanisms for network slicing and tunneling, new algorithms and mechanisms that can adapt network slice configurations dynamically to accommodate urgent and mission-critical traffic are needed. Such slices must be secure, interference-aware, and free of side channel attacks. Resilience of the 5G ecosystem itself requires an effective means for observability and (semi-)autonomous self-healing capabilities.**

To address this plethora of challenges, this paper presents the SECurity and REsiliency TEchniques for Differentiated 5G OPerationS (SECRETED 5G OPS) project, which is investigating fundamental new solutions that center on the zero trust, network slicing, and network augmentation dimensions, which together will achieve secure and differentiated operations in 5G networks. SECRETED 5G OPS solutions are designed to be easily deployable, minimally invasive to the existing infrastructure, not require modifications to user equipment other than possibly firmware upgrades, economically viable, standards compliant, and compliant to regulations.

***Index Terms*—Zero-Trust, Side Channel Attack, Adaptive Slicing, Hardware-level Security, Network Augmentation.**

I. Introduction

The fifth generation (5G) networking is expected to support new services ranging from small group of users, such as self-assembling robots, to mass market services, such as holographic mixed reality, cellular-connected drones, autonomous supply chain, and massive twinning. These services have a variety of performance requirements, e.g., a reliable, low latency communication channel, secure and resilient operations. For example, Urban Air Mobility (UAM) [1] is an upcoming new transportation modality comprising *air taxis* flying at lower altitudes and ferrying passengers within a suburban area [2] [3]. UAMs will be relying on 5G for all their safety-critical and operational needs due to their low latency, reliable, secure and scalable communication needs, and high mobility [4].

5G also offers a clean separation between the radio access network (RAN), the multi-access edge computing (MEC) and the mobile core that enables different and scalable deployments [5]. Specifically, it leverages modern principles of virtualized network functions, microservices-based service chaining, and cloud-native software stacks. Moreover, it provides different classes of services for a range of application needs, provides a built-in security mechanism that uses secure tunnels and effective authentication/authorization mechanisms, and supports effective means for network slicing [6].

Despite these capabilities, many challenges remain unresolved and opportunities manifest for additional capabilities to be introduced into the 5G ecosystem. For instance, although 5G provides basic authentication mechanisms based on SIM cards, when resources must be shared during natural disasters, zero trust solutions are required in the operator's network. Moreover, user equipment (i.e., end devices) may require modifications to support zero trust solutions.

One research challenge involves assuring security, e.g., as indicated in the Zero Trust model referred to in the NIST 800-207 [7] and the CISA Zero Trust model [8], where applications are operating atop a shared 5G network infrastructure. Likewise, although mechanisms for network slicing and tunneling exist, new algorithms and mechanisms are needed to dynamically adapt network slice configurations to accommodate urgent and mission-critical traffic. These slices must be secure, interference-aware, and free of side-channel attacks. Finally, resilience of the 5G ecosystem itself requires effective resource monitoring and nearly autonomous self-healing capabilities. Any new solution must be easily deployable, minimally inva-

§This work has been performed while at Siemens Technology US

ISBN 978-3-903176-52-2

sive to the existing infrastructure, require no modifications to user equipment (other than possibly firmware upgrades), be economically viable, standards compliant, and compliant to regulations.

In summary, although many prior efforts at handling various challenges in 5G exist [9] [10], little research has focused on end-to-end secure operations and resilience in 5G that provides differentiated services. To address this plethora of challenges, we present the *SECurity and REsiliency TEchniques for Differentiated 5G OPerationS (SECRETED 5G OPS)* project, which is making the following contributions:

- **Zero trust solutions across the 5G ecosystem:** we aim at solving cybersecurity issues to protect network resources by implementing implicit trust and continuously validating an efficient Zero Trust security verification process in 5G networks.
- **Attack Resistant Slice Selection:** we propose a Dynamic Slice Selection Algorithm (DSSA) to enable secure, authenticated, attack-resistant, interference-aware, adaptive, and dynamic service function chaining and network slice assignment and isolation within 5G Networks.
- **Hardware-level Cyber Threats Security:** we propose multi-target Hardware-level solutions to secure 5G network infrastructure, including user equipment, access networks, mobile core and external IP networks.
- **Intelligent scattering to identify spoofing:** we introduce the concept of intelligent scattering environment (ISE), which provides a reconfigurable intelligent surface mechanism for controlling the propagation of electromagnetic waves in smart rich scattering wireless environments to improve the security and the performance of 5G system and beyond.

The remainder of this paper is organized as follows: Section II delves into our solution approach to support high-performance, secure and holistic management of 5G and beyond. Section III provides concluding remarks describing potential future directions and open research problems in this realm.

II. Proposed SECRETED 5G OPS Solution

This section delves into the proposed SECRETED 5G OPS solution to enhance 5G security and resilience at different levels.

A. Thrust Area 1: Zero Trust Solutions

In many operational contexts, critical data must be communicated securely, while simultaneously assuring the real-time QoS properties of the system. A common example of application with these requirements is manufacturing operation and industrial operations. The SECRETED 5G OPS project addresses the problem of assuring increased cyber-security of critical applications hosted on 5G networks by tackling security risks at multiple layers of the 5G infrastructure, as well as considering the attack surface in the user equipment, the edge computing applications, and up to the cloud trusting levels. We tackle these cyber-security threats by focusing on approaches indicated by Zero Trust architectures and related security pillars. We consider the execution of applications with real-time constraints operating in 5G networks.

SECRETED 5G OPS aims to solve this problem by defining and executing fine-grained cyber-security verification tasks for real-time industrial systems that implement an efficient and continuous Zero Trust security verification process in 5G networks. For example, we consider the design of micro-segmentation in client-server communications and machine-to-machine communications. Micro-segmentation involves managing and supervising resource allocation and security tasks for individual communication flows between (communication) endpoints running applications in a user equipment and in virtualized environments, e.g., software applications hosted in virtual machines and micro-services running in software containers.

These applications will be accessed from a 5G user device (e.g., smartphone, tablet, and/or laptop) or from a non-5G user device connected to the 5G network through a 5G-enabled router (e.g., Scalance 5G), and the servers will be hosted in the 5G nodes called Multi-Access Edge Computing (MEC) and in the Edge Cloud. More precisely, this project addresses the need to define network micro-segmentation that enables the real-time monitoring capability required by a Zero-Trust implementation. Our solution is leveraging the 3GPP specifications on network slicing to define and implement a QoS service that addresses current challenges in ensuring the viability of communications over a 5G network to include security QoS assurance.

B. Thrust Area 2: Interference-aware, Software-defined Adaptive Network Slicing and Dynamic Resource Management

SECRETED 5G OPS provides the Dynamic Slice Selection Algorithm (DSSA) that allows or restricts the Network Function Chains (NFCs) to associate with only the authenticated slice using an encrypted hash function technique. The DSSA solution approach enables high accuracy rates in selecting the most trustable slice for installed network chaining services. Selecting a secure slice instance is critical before using it for service provisioning. To that end, we provide a reliable platform to the Telecommunication Service Providers (TSPs) and MNOs (Mobile Network Operators) to select the best available network instances to construct their required network slices. Moreover, we also propose a selective filtering mechanism that can filter out malicious slices.

All these capabilities yield the following benefits: (1) service and resource availability, (2) low data loss, (3) optimized utilization of network resources, (4) maintaining data integrity, and (5) developing a flexible and trusted shared environment. Our ideas can apply to a multi-tenant environment, where the lower cost of new infrastructure deployment, low energy module installation, and long life cycles of implemented network slices will help TSPs and MNOs to improve the quality-of-experience/service (QoE/QoS). Service providers will also be able to cover the maximum region within a resource-restricted

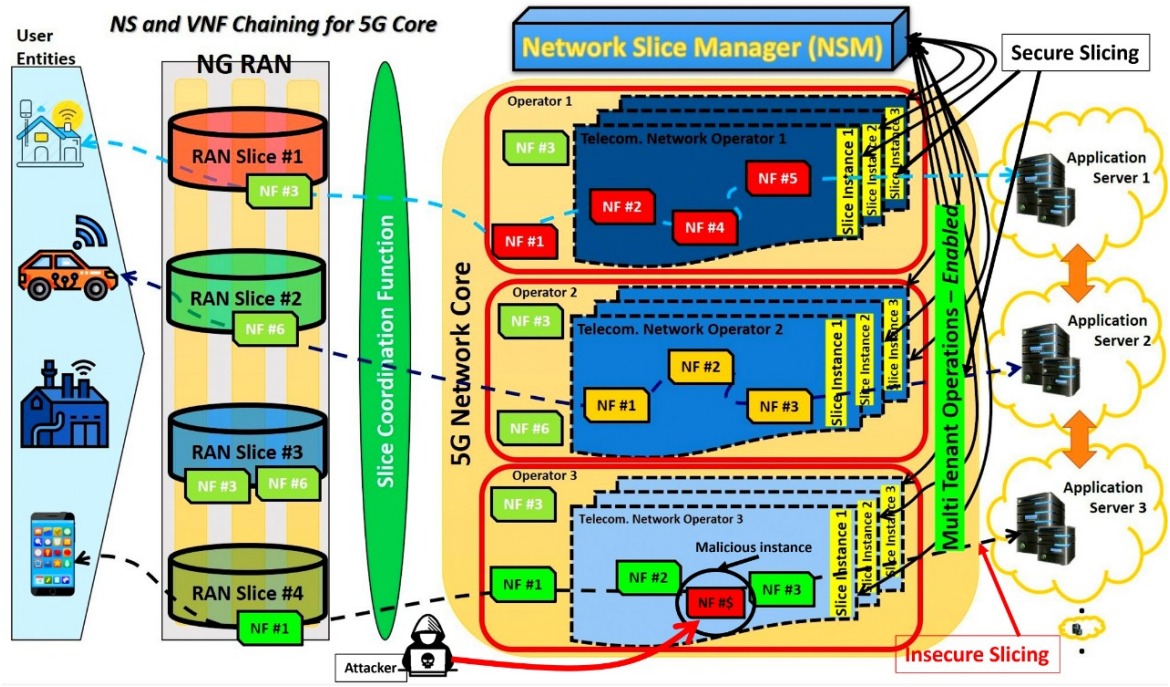

Fig. 1. Virtual Network Function (VNF) Embedding and Service Function Chaining (SFC) Over Shared Slices for 5G Applications

environment. Most importantly, developing a trustworthy networking environment is our primary target through this project.

Our system model runs on a generalized 5G RAN architecture (as shown in Figure 1), where the selective secure service layering is performed. This architecture can be deployed over any real network topology. A virtualization layer has been realized via multiple shared hypervisor units over the hypervisor plane (H-plane). The control plane (C-plane) holds the SDN controllers. SDN-enabled switches are at the Data Plane (D-plane) controlling the flow of services from the physical units to the control plane via the H-plane.

Function chaining is done over the topology. In particular, a single network service can be a collection of multiple network functions, which are embedded over SDN nodes. The set of network services in turn creates a network slice. Individual slices are built using the virtual instances of the underlying physical nodes.

Our approach carefully selects virtual instances so that no vulnerable or affected instance is selected. DSSA uses a unique end-to-end hashing technique to select the most trusted instances over the existing topology. If any instance over the slice is identified as being affected, the entire slice will be newly created using the secure sources.

We generalize the case of dynamic slice creation as follows: at the start, each network resource is allocated a secure ID and is then assigned to every SDN instance over the H-plane. Whenever a service path is created, a secure hash algorithm is deployed to judge the authenticity of the service path using a flag function. Our approach minimizes false selection of instances and improves the currently selected instances over a slice. This flow can be repeated to obtain the average count of the flag, which makes the algorithm more secure and safer to implement.

After the trusted slice is formed, robust virtual network function (VNF) chaining will be performed to balance end-to-end slicing. For dynamic slicing, resources like VNF instances can be created or removed by the respective TNOs. Due to the multi-tenant operation, slice agreement policies must be maintained to avoid any malicious trespassers inside any slice. Our approach helps to minimize the faulty selection of dynamically generated network slices, and restricting the flow over an insecure network slice. Additionally, our proposed approach helps in maximizing the secure service availability and provide the TSPs and MNOs a safe platform to select a better slice. The overall QoE and QoS of the network will be improved significantly.

C. Thrust Area 3: Handling Hardware Security Threats from Untrusted 5G Network

SECRETED 5G OPS project focuses on the following solutions to handle hardware security threats:

- An intrusion detection system that is updated to assess all the memory locations that are been accessed and keep track of the memory location targeted by each data request. An optimization of hardware resources is needed to ensure that memory location is stored for only certain period of clock cycles. In principle, the solution is simple, but at each design abstraction level, calculating the memory location and keeping track of it requires additional processing infrastructure.
- Battery management or power management systems of the UE are monitored for anomalous activities.

- A quarantining strategy for suspected base stations is devised in a cooperative network environment. Once the Attack Detection Unit (ADU) in the UE detects malicious activities, it informs the 5G operator via an end-to-end encrypted logical channel. This quarantining strategy then finds an alternative route or provides an extra layer of filtering on the suspected stations' network traffic.

The SECRETED 5G OPS project offers the following approaches in support of our proposed solutions.

1) Select the earliest possible reliable assessment of 5G data packets within a budgeted hardware cost to realize a memory or power system attack. Since false positives and negatives can mar the quality of such systems, this task will explore the overall design space to bring these rates (false positives and negatives) down to a minimum.
2) Provide deeper insights into the challenges that 5G operators will face to achieve safe (and transparent to the users) operation in the presence of a compromised 5G base station.

We have achieved some preliminary success towards understanding the effects of attack on power management systems. We have explored the idea of monitoring the power rail of wired connected UE. A trusted ecosystem is proposed with trusted device loads, different benchmarks applications and the power rail data is gathered while these trusted devices are connected to all the UEs. Multi-level perceptron-based machine learning algorithm is used to detect a zero-day attack. It is observed that when the attack is idle, machine learning model (as illustrated in Figure 2) is able to detect different types of application running in the trusted device with 99% accuracy, but as soon as in an idle untrusted IoT device is subjected to attack the accuracy dropped significantly - up to 29 %, which is indicative of an anomaly in the power system.

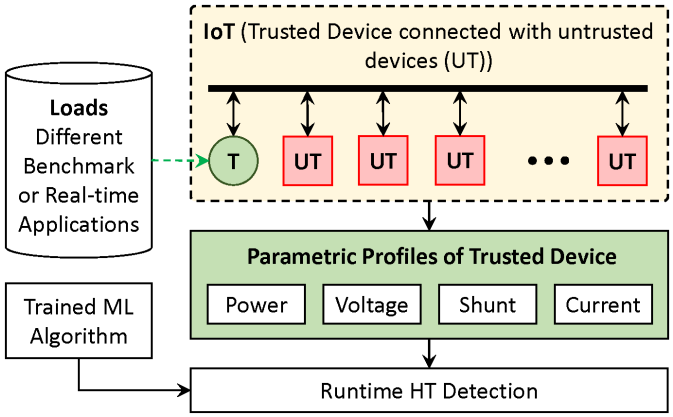

Fig. 2. Trusted Ecosystem for HT Detection during Runtime: Steps involved for HT detection using the proposed ML-based ecosystem

D. Thrust Area 4: Network Augmentation via Intelligent Scattering Environment (ISE) for Identity Spoofing Detection (ISD) at Physical Layer

One means to detect an identity spoofing attack is to monitor a UE's physical location and detect location discrepancy based on some wireless channel state information (CSI) at the communication physical layer. For instance, both Received Signal Strength (RSS) and Wireless Channel Impulse Response (CIR) are related to the UE's physical location, but the latter is more promising for Identity Spoofing Detection (ISD). In particular, a CIR contains more information of the propagation environment than a RSS. Thus, a CIR-based ISD is more promising. CIR-based ISD monitors the received CIR, where estimating CIR is a routine function in a cellular communication system. In a 5G system setup, an ISD unit can naturally be placed at the Base Band Unit (BBU) at a base station. CIR, known as a type of Radio Frequency (RF) fingerprinting or Physical Unclonable Function (PUF), is expressed in the time domain as shown in Equation 1.

$$h(t) = \sum_{l=1}^{L} \alpha_l (t - \tau_l) e^{j\theta_l} \tag{1}$$

where L is the total number of propagation multipath components corresponding to the l-th component, α_l, τ_l and θ_l are overall effective path gain (inverse of path loss), propagation delay, and inserted phase rotation, respectively.

In the SECRETED 5G OPS project, we argue that a CIR is hard to imitate and is determined by the radio propagation scattering environment between the transmitter and the receiver. In particular, a CIR-based ISD is more robust than a RSS-based ISD, since the CIR usually contains more information about the radio propagation environment. Indeed, rich multipath favors ISD, though in some line-of-sight propagation (NLOS) dominated scenarios, CIR-based ISD is difficult and inaccurate.

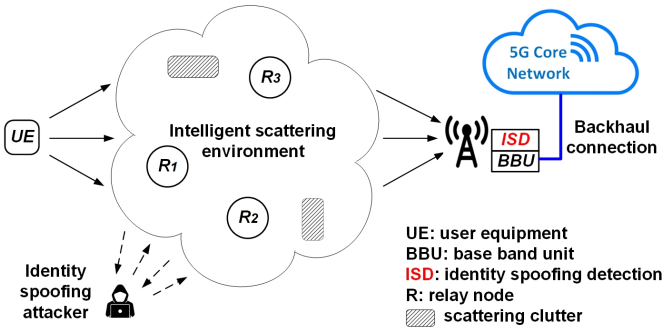

Fig. 3. Conceptual system setting with intelligent scatting environment (ISE)

In the SECRETED 5G OPS project, we introduce the concept of Intelligent Scattering Environment (ISE), which is reconfigurable, similar to changing a password. Figure 3 depicts such an idea, where the relay nodes are miniature full-duplex amplify-and-forward radio relays deployed in the field by the authorized parties (e.g., the military end users and 5G network operator), and all of them are connected with the authority. These relays introduce additional multipath components and alter the natural CIR. Assuming that M relays are deployed in the field, the effective CIR in the time domain is given by Equation 2.

$$\tilde{h}(t) = \sum_{l=61}^{L} \alpha_l(t-\tau_l)e^{j\theta_l} + \sum_{m=1}^{M} \rho_m(t-\nu_m)e^{j\phi_m} \quad (2)$$

where the first summation is the natural CIR $h(t)$, the second summation corresponds to artificial multipath components, and the amplitude ρ_m is dependent on the m-th relay's amplification.

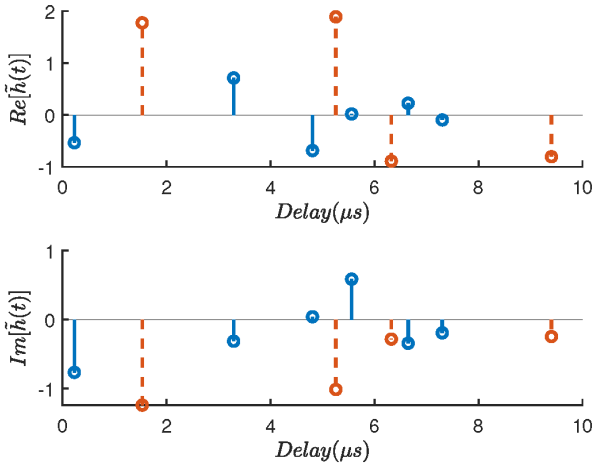

Fig. 4. CIR profile with 6 natural path components (solid lines) and 4 added path components (dash lines)

We have achieved some preliminary results using CIR profile with 6 natural path components. Figure 4 shows the real and imaginary parts of $\tilde{h}(t)$. When a relay is not powered on or is sleeping, its corresponding amplitude is equal to zero. The M relays can be formed into multiple subsets and selected by the authority via encrypted communication links, where each subset of relays generates a unique effective CIR. ISE can lead to the following two benefits at a minimum: (1) a natural CIR is unique and typically unmanageable (similar to human biometric data)—and the loss of such information can lead to catastrophic outcomes—so ISE with reconfigurable CIR makes it hard for an attacker to detect and infer the CIR and (2) as the carrier frequency moves towards millimeter wave (mmWave) bands, the CIR becomes sparse, so applying ISE helps ISD through increasing the multipath components.

III. Conclusion

This paper presents the SECRETED 5G OPS project, which is use-inspired research that addresses fundamental challenges stemming from the need to operate securely and resiliently in 5G networks. First, it motivates our research thrusts using a diverse set of use cases drawn from both defense and civilian domain and discussed challenging issues Then, it describes ongoing progress on SECRETED 5G OPS project including a proof-of-concept that integrates i) Zero Trust architecture with critical applications, ii) adaptive network slicing and dynamic slice creation, filtering of malicious slices, maximizing reward, QoE and QoS, iii) a methodology for detecting and mitigating hardware attacks from untrusted 5G users on UE's power and memory systems, and iv) network augmentation for identity spoofing detection by leveraging artificially enriched channel impulse response.

The aim of this paper was to highlight the fundamental challenges in realizing end-to-end security and resilience in 5G networks, and to illustrate the possible directions including the ones taken by the SECRETED 5G OPS project. As this is work-in-progress, many directions for future work are possible. One such direction involves the deployment of large-scale experiments to maximize the protection and device-level enhancements using the relay-aided Intelligent Reflecting Surface (IRS) [11] to enable devices as relays to extend the wireless coverage and enhance the system performance when the transmitter and receiver are relatively close to each other. Fully developing, deploying and evaluating the ideas is ongoing work.

Acknowledgments

This work was partially funded by the Tunisian Ministry of Higher Education (MES) under the Young Researchers Incentive Program (19PEJC09-04). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of MES.

References

[1] D. P. Thipphavong, R. Apaza, B. Barmore, V. Battiste, B. Burian, Q. Dao, M. Feary, S. Go, K. H. Goodrich, J. Homola *et al.*, "Urban Air Mobility Airspace Integration Concepts and Considerations," in *2018 Aviation Technology, Integration, and Operations Conference*. Reston, USA: American Institute of Aeronautics and Astronautics, 2018, p. 3676.

[2] C. Silva, W. R. Johnson, E. Solis, M. D. Patterson, and K. R. Antcliff, "Vtol urban air mobility concept vehicles for technology development," in *2018 Aviation Technology, Integration, and Operations Conference*. Reston, USA: American Institute of Aeronautics and Astronautics, 2018, pp. 1–16.

[3] K. R. Antcliff, K. Goodrich, and M. Moore, "NASA Silicon Valley Urban VTOL Air-Taxi Study," in *On-demand mobility/emerging tech workshop, Arlington*, vol. 7, 2016.

[4] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, and L. Xiong, "A survey on security aspects for 3gpp 5g networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 170–195, 2020.

[5] J. Nakazato, M. Nakamura, T. Yu, Z. Li, K. Maruta, G. K. Tran, and K. Sakaguchi, "Market analysis of mec-assisted beyond 5g ecosystem," *IEEE Access*, vol. 9, pp. 53 996–54 008, 2021.

[6] T. W. Nowak, M. Sepczuk, Z. Kotulski, W. Niewolski, R. Artych, K. Bocianiak, T. Osko, and J.-P. Wary, "Verticals in 5g mec-use cases and security challenges," *IEEE Access*, vol. 9, pp. 87 251–87 298, 2021.

[7] V. Stafford, "Zero Trust Architecture," *NIST Special Publication*, vol. 800, p. 207, 2020.

[8] CISA, "Zero Trust Maturity Model," Cybersecurity & Infrastructure Security Agency (CISA), Tech. Rep., Jun. 2021.

[9] S. Guo, Y. Qi, Y. Jin, W. Li, X. Qiu, and L. Meng, "Endogenous Trusted DRL-based Service Function Chain Orchestration for IoT," *IEEE Transactions on Computers*, vol. 71, no. 2, pp. 397–406, 2021.

[10] F. Girke, F. Kurtz, N. Dorsch, and C. Wietfeld, "Towards Resilient 5G: Lessons Learned from Experimental Evaluations of LTE Uplink Jamming," in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, IEEE. USA: IEEE, 2019, pp. 1–6.

[11] Q. Wu, S. Zhang, B. Zheng, C. You, and R. Zhang, "Intelligent reflecting surface-aided wireless communications: A tutorial," *IEEE Transactions on Communications*, vol. 69, no. 5, pp. 3313–3351, 2021.