IEEE Open Journal of the Computer Society

Received XX Month, XXXX; revised XX Month, XXXX; accepted XX Month, XXXX; Date of publication XX Month, XXXX; date of current version XX Month, XXXX.

Digital Object Identifier 10.1109/XXXX.2022.1234567

Addressing Security Orchestration Challenges in Next-Generation Networks: A Comprehensive Overview

Sadeep Batewela, ***Student Member, IEEE,*** **Pasika Ranaweera,** ***Member, IEEE,*** **Madhusanka Liyanage,** ***Senior Member, IEEE,*** **Engin Zeydan,** ***Senior Member, IEEE,*** **and Mika Ylianttila,** ***Senior Member, IEEE***

[1]Center for Wireless Communications, University of Oulu, Finland. e-mail:sadeep.batewelavidanelage@student.oulu.fi
[2]School of Electrical and Electronic Engineering, University College Dublin (UCD), Ireland. e-mail:pasika.ranaweera@ucd.ie
[3]Network Softwarization and Security Labs (NetsLab), School of Computer Science, University College Dublin (UCD), Ireland. e-mail:madhusanka@ucd.ie
[4]Centre Tecnològic de Telecomunicacions de Catalunya, Castelldefels, Barcelona, Spain, 08860. Email: engin.zeydan@cttc.cat
[5]Center for Wireless Communications, University of Oulu, Finland. e-mail:mika.ylianttila@oulu.fi

Corresponding author: M. Liyanage (e-mail: madhusanka@ucd.ie).

This work is partly supported by the European Union under the ENSURE-6G project (Grant Agreement No. 101182933) and CONNECT phase 2 project by Research Ireland (Grant no. 13/RC/2077_P2), UNITY-6G project, funded from European Union's Horizon Europe Smart Networks and Services Joint Undertaking (SNS JU) research and innovation programme under the Grant Agreement No 101192650.

ABSTRACT

Security Orchestration (SO) plays a pivotal role in ensuring robust, scalable, and efficient management of security mechanisms in next-generation 5G and beyond 5G (B5G) networks. This paper presents a comprehensive analysis of the technical challenges related to SO in these advanced network technologies, focusing on key areas such as network security monitoring, interface standardization, privacy, scalability, multi-domain orchestration, and policy implementation. Additionally, we discuss lessons learned from existing works, identify remaining research gaps, and propose future directions for enhancing SO in 5G and B5G environments. Emerging technologies such as artificial intelligence (AI), blockchain, quantum computing and trusted execution environments (TEE) are also examined for their potential to address these challenges. The paper provides a taxonomy of SO-related issues and offers a roadmap for researchers and practitioners to navigate the evolving landscape of security in 5G and B5G networks.

INDEX TERMS Security Orchestration, 5G and Beyond, Zero-touch Networks, Security Automation

I. INTRODUCTION

Various security solutions have been developed and deployed by different organizations to prevent known and unknown attacks and their harmful effects [1], [2]. These security solutions include antivirus, firewalls, Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS), and Security Information and Events Management (SIEM) [1], [3]. Different security solution providers create, implement and manage security solutions with different technologies and concepts. These discrepancies prevent them from being easily integrated and working together to effectively and efficiently support the Security Operations Center (SOC) [4]. The SOC is a centralised function responsible for actively and passively responding to security attacks and ensuring service availability. SO is the ultimate solution or savior for integrating various security tools from different vendors into a unified system. It acts as a support system for the security experts in a SOC. The proactive, independent and collaborative support system enabled by SO allows security personnel to perform their tasks successfully and efficiently. At the same time, SO brings people, practices and technologies onto a common platform where collaborative actions and efforts improve security operations and management. SO empowers Security Automation (SA) that uses Information Technology (IT), automation algorithms and Artifical Intelligence (AI) to automatically respond to threats without human intervention.

Most cyber-security methods and procedures in use today are manual or semi-automated. They mainly monitor the

network infrastructure and activities of organizations in order to take the necessary measures when abnormal behaviors or activities are detected. These measures include the generation of security alerts and the activation of alarms that can be noticed by security personnel to take further action to prevent attacks. Even if security personnel take action within a short time interval, it takes a considerable amount of time for the occurrence of an incident to be detected, and then it takes even longer to take corrective action. It is necessary for security experts to be able to provide available security solutions as quickly as possible and facilitate choice. This leads to seamless security operations and availability of services to prevent potential threats from security breaches. This time-consuming and inefficient human response to security threats can be handed over to an SO platform. A comprehensive overview of the network helps to respond successfully to a threat or attack. These multi-vendor/multi-technology security solutions usually have their own way of working and how they respond to an attack. A SO framework provides a common platform for all security solutions from different providers and integrates them into a single unit. The SO framework monitors the security status of the underlying infrastructure, identifies suspicious activity and acts accordingly to prevent an attack without human intervention. Therefore, the SO framework acts as a user interface between the human and the network, whereby the human can be involved in security management if required.

A. Related Work

After an extensive search, we were able to categorize the existing related surveys into three main categories: (i) surveys on the automation of information security management systems [5]–[10], [10], [11], (ii) surveys on SO in organizations and enterprises [4], [12], (iii) surveys on SO in 5G and B5G technologies [13]. The first category deals with SA, i.e. the automated handling of cyber incidents and the management of security events that replace manual processes. Some works, such as [5]–[9], discuss the possibilities of SA in Information Technology (IT). Raydel et al. [5] discusses the possibilities of automating Information Security Management Systems (ISMS) using the security ontology in the context of ISO 27001. The main focus of this paper is on the process of information security management. Keith et al. [6] discuss inherent limitations of automation based on human and social factors. The authors also present design guidelines and future research directions for the automation of end-user security systems. Raydel et al. [7] analyze the possibility of automating security controls in ISMS in the context of ISO 27001. The authors claim that with a combination of security controls about 30% of the maximum level of automation could be achieved. Sikender et al. [8] give an overview of SA in IT and mainly discuss the elements of SA and how SA helps to secure technical systems. Sikender et al. [9] review the control recommendations provided by standards such as ISO/IEC 27001 and NIST SP 800-53. In addition, the authors discuss the limitations of SA and the importance of SA in any security control. Sravanthi et al. [11] discuss how automation technologies such as AI/Machine Learning (ML)/Deep Learning (DL) can be used to move from detection-focused security to prevention-focused security. The authors discuss how AI can be used to enhance the capabilities of prevention techniques, e.g. by analyzing sensor data and identifying patterns to support IPS and security event management. However, it does not cover SO in 5G and B5G and only focuses on the use of AI/ML and DL in automating the management of security events. Michael et al. [10] provides an overview of advanced anomaly detection, prevention and defence techniques supported by automation and ML. The authors discuss in detail the difficulty of mitigating zero-day attacks, the use of automation and the challenges. However, they do not discuss SO in 5G and B5G technologies or the use of these technologies to combat zero-day attacks.

The second category focuses on surveying SO solutions in IT infrastructures and organizations. Most of the existing surveys related to SO focus on the IT infrastructure of organizations [13]. Both [4], [12] talk about SO in general, and the focus was placed on SO in organizations and enterprises. Islam et al. [4] gives an overview of SO in organizations and enterprises, focusing on the main functions, core components, main drivers, and an SO taxonomy based on resource type, execution environment, deployment type, automation strategy, and task mode. Kinyua et al. [12] investigates the use of AI/ML in Security Orchestration, Automation, and Response (SOAR) solutions. SOAR solutions are designed to integrate and automate various security tasks and countermeasures in accordance with the security administrator in enterprises and organizations. Nguyen et al. [14] review SOAR approaches in Internet of Things (IoT)/Cyber Physical-based Systems (CPS). The authors identify gaps and propose research directions for advanced SOAR with holistic operation and increased automation. Fernando et al. [15] discuss automation of security requirements in service-based business processes. The authors mainly focus on the security requirement modeling, translation and enforcement mechanisms.

The third category, where there is not much work, is about SO in 5G and B5G technologies. SO in 5G and B5G technologies is much more complicated than SO in traditional IT infrastructures due to softwarization, heterogeneity, strict use case requirements, number of connected devices and huge traffic volume. Zheng et al. [13] authors focus on SA and SO in IoT environments. Nerijus et al. [16] review security challenges in fog computing as well as the security challenges in orchestration. The authors find that security and privacy are critical in fog computing orchestration. However, this paper does not specifically address SO or SO challenges in fog computing. Daniele et al. [17] survey about network security configuration automation in vitalized and cloud-based networks. The authors discuss the utilization of SDN,

NFV and policy-based management in security automation. However, it does not directly cover the full scope of 5G/B5G. Yang et al. [18] survey about automation and orchestration challenges and solutions for Zero Trust Architecture (ZTA). The authors analyze the possibilities of utilizing state-of-the-art AI techniques to automate and orchestrate ZTA. However, this survey does not cover 5G/B5G.

B. Paper Motivation

This survey provides a comprehensive overview of SO and its challenges in 5G and B5G networks, focusing on security monitoring, interface definitions and standardization, SO policies, scalability, multi-domain SO, Security Service Level Agreement (SSLA) monitoring and management, End to End (E2E) security and integration of Intent-Based Networking (IBN). In pursuit of this goal, we review the contributions from academia and industry, focusing on the implementations of SO, specifically in 5G and B5G technologies and use cases. In addition, we will talk about enabling technologies that can be used to address identified challenges while identifying the lessons learned and future research directions. Even though security in 5G and B5G caught the researcher's eye [19], [20], neither SO in 5G and B5G nor challenges have been researched extensively. We thoroughly discussed existing related surveys in Section A and summarized in Table 1. However, none covers the holistic picture of SO in 5G and B5G technologies by looking at the background, evolution, taxonomy, functionalities, and components. Moreover, No such work covers the technical challenges and related research direction in the context of 5G and B5G network technologies. Our primary motivation is to explore how SO can enhance security management in 5G and B5G technologies by leveraging enabling technologies, addressing potential challenges, proposing solutions, and identifying key areas for future research.

C. Paper Contribution

To our current knowledge, there is no comprehensive study that addresses the integration of Security Orchestration (SO) in the context of 5G and Beyond 5G (B5G) technologies, taking into account aspects such as 5G architecture, requirements, use cases and security considerations in a unified way. This study highlights the need to develop an SO framework equipped with universal knowledge and a holistic network perspective, and aims to pave the way for the realization of future zero-touch networks. The following is a summary of the main contributions of this paper: At the same time, it is essential to create an SO framework that has universal knowledge and a holistic view of the network to successfully enable SO, leading to future zero-touch networks. The main objective of this work is to extend the SO landscape in 5G and B5G networks and enable the interplay of novel technologies for better security management, while identifying a potential SO framework for 5G and B5G networks. The following is a summary of the main contributions of this work:

- Perform a comprehensive analysis of SO, including its evolution, key functions, main components and associated risks in the context of 5G and B5G networks.
- Examine the technical challenges in SO for 5G/B5G technologies, such as scalability, privacy, multi-domain integration and standardization, while proposing possible solutions and research directions.
- Highlight lessons learned from existing work and identify remaining research gaps to provide a roadmap for future progress in SO.
- Explore the potential of emerging technologies such as AI, blockchain, quantum computing and Trusted Execution Environments (TEE) in addressing SO challenges in next-generation networks.
- Demonstrate the critical role in developing secure, scalable and adaptable solutions for evolving 5G/B5G applications and use cases.

This study not only expands the understanding of SO in 5G/B5G technologies, but also serves as a compass for future research efforts towards robust frameworks for SO.

II. Security Orchestration

A. Evolution of Security Orchestration

Like the network service orchestration, the SO is also a new technological trend. The academic community and research industry are still in the process of defining the true meaning, scope and context of SO-related concepts. It is a long way to the current progress and will continue to evolve. The evolution of SO is summarized in Figure 1.

SO in physical networks: Dealing with the security aspects of physical networks was mainly done manually. The human network administrator played an important role. Security tools and supporting systems enabled the early detection of abnormal network activity. However, under extreme circumstances, system administrators had to process millions of these daily alerts. To combat cyberattacks, situation awareness and threat assessment systems have therefore been developed that utilise information fusion techniques [21], which is the first step towards SO.

SO in web services: Many early works of SO focused on orchestrating the security services of web-based services. In the early days of the Internet, securing web services was a challenging and complex task that attracted the attention of the research community. For this purpose, it was necessary to identify the functions required for the integration of services in SO [22]. Identity management and threat analysis are two main areas where SO is used for secure web services [23]–[25]. Service-Oriented Architecture (SOA) aims to create a more flexible system landscape that facilitates the integration of new components. However, managing security in these architectures has been very difficult. To address this problem, the authors of [26] define an appropriate archi-

TABLE 1: An overview of significant surveys on SO/SA

Ref.	Organizational SO/SA	Applications/Use Cases	Technical Challenges	Enabling Technologies	Remarks
[4]	H	H	H	L	Surveys SO in organizations and enterprises, focusing on main functionalities, core components, key drivers, and SO taxonomy based on the resource type, execution environment, deployment type, automation strategy, and task mode. It does not cover 5G technologies or how to enable SO in 5G and B5G.
[12]	H	M	L	H	A survey on SOAR solutions from an AI/ML perspective in organizations and enterprises (multi-vocal review). It does not cover how to leverage AI/ML for SO in 5G and B5G.
[13]	M	M	H	L	Discusses the challenges and advancements in SA and SO for IoT systems, as well as future directions. It does not cover how to leverage 5G and B5G technologies to enable SO in IoT.
[10]	M	M	H	H	Examines the literature and outlines the research undertaken in the autonomous management of anomalies with the use of ML. It does not cover how to leverage 5G and B5G technologies to manage anomalies.
[5]	M	M	L	L	Provides an analysis of the automation possibilities in information security management. The only focus is the information security management process. It does not cover SO in 5G and B5G technologies.
[6]	M	L	M	L	Discusses the inherent limitations, design guidelines, and research directions for automating end-user security. Does not cover SO in 5G and B5G technologies.
[7]	L	L	L	L	Outlines the security applications that enable automation of information security control operations to improve the effectiveness of information security management. It does not cover SO in 5G and B5G technologies.
[8]	M	M	L	L	Discusses the importance, role, and elements of SA in IT while listing available automation tools and platforms. It does not cover SO in 5G and B5G technologies.
[9]	M	M	L	M	Demonstrates the gaps and issues currently in the SA field and suggests future research directions. It does not talk about gaps and issues of SO in 5G and B5G technologies.
[11]	M	L	L	H	A survey of automation technologies based on AI/ML/DL implemented to advance prevention-centric security. The only focus is on AI/ML/DL and does not cover SO in 5G and B5G technologies.
[15]	M	H	M	L	This survey examines initiatives to automate service-based business processes and address security requirements, focusing on web-based use cases.
[14]	H	M	L	M	A survey on current SOAR approaches and research directions towards advanced automation. Main focus is on CPS and IoT.
[17]	M	M	H	H	A broad survey on network security configuration automation, covering methodologies and research trends but does not directly address the full scope of SO in 5G/B5G networks, such as multi-domain orchestration and scalability challenges. However, its discussion on security automation complements SO-related research.
[18]	L	M	H	H	A survey on utilizing AI to address gaps in ZTA automation and orchestration, mainly covers trust evaluation, authentication, attack detection, and monitoring and related AI based solutions.
Ours	**L**	**H**	**H**	**H**	**A comprehensive survey of SO in 5G and B5G technologies, background, motivation, role, enabling technologies, applications and use cases, technical challenges, learned lessons and possible research directions.**

tectural framework called Security Meta-Services Orchestration Architecture (SMSOA). Chahal et al. [27] propose an open-source continuous vulnerability assessment tool called Orchestrated Continuous Vulnerability Assessment (OCVA). This scanning tool aims to orchestrate continuous vulnerability assessments of all automated cybersecurity detection processes of web applications.

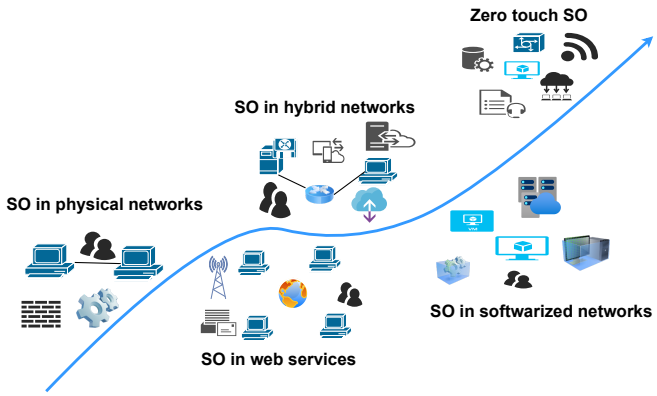

FIGURE 1: Evolution of Security Orchestration.

SO in hybrid (physical and virtualized) networks: According to ESTI NFV [28], hybrid networks consist of traditional physical network appliances and virtual network appliances. If part of the network has Physical Network Functions (PNFs), handling security in hybrid networks is quite a challenge, as both Physical Security Functions (Physical Security Function (PSF)s) and Virtual Security Function (VSF)s are present. SO could be used here in a hybrid way, as PSFs can be handled manually according to standardization specifications or the operator's security requirements. VSFs can be orchestrated in the same way as security functions in web services. Jaeger et al., [29] suggests orchestrating both PSFs and VNFs using a security orchestrator where the security orchestrator or a Security Element Manager (SIM) manages the PSFs directly. The security orchestrator can also use the VIM to activate and configure the VSFs offered by the NFV infrastructure.

SO in softwarized networks: The softwareization of networks has had a major impact on the telecommunications industry. SDN and NFV play an important role in 5G and B5G networks and can enable value- added services. With the new features introduced into the network paradigm by SDN and NFV, such as softwarization and virtualization, SO can be deployed with minor changes. Most of the security

features that exist as VSFs and Security as a Service come into play here. Without SO, it will be quite difficult to manage security in softwareized networks. A lot of work is focused on finding a better SO architecture and a compatible security orchestrator in softwareized networks [30], [31].

Zero touch SO: The next goal of SO is to fully automate security-related tasks. It also eliminates the dependence on human expertise and the human factor. With the use of VSFs enabled by SDN and NFV,E2E security will be strengthened, while security management in future networks will be optimized and automated. To reduce both CAPEX and OPEX, NFV uses virtualization to decouple hardware from network and security operations. On the other hand, SDN enables the softwareization of network control and management by splitting the data and control plane, increasing flexibility in network management and control. Software Defined Networking (SDN) and Network Function Virtualization (NFV) are the basis for a true zero-touch SO. In this regard, NFV/SDN security frameworks that are adaptive and policy-based can make a significant contribution to self-protection and self-healing [32], [33]. At the same time, concepts such as Zero Touch Network and Service Management (ZSM) and Intent-Based Networking (IBN) with the help of AI/ML and Distributed Ledger Technologies (DLT) could play a key role in the realization of zero-touch SO. ZSM proposes to integrate automation into the management of network services and enable self-configuration, self-optimization, self-healing and self-monitoring according to policies [34]. The purpose of IBN is to develop network management solutions that are controlled by intents [35]. These concepts heavily utilize AI/ML, Explainable Artificial Intelligence (XAI), DLT technologies and closed-loop automation to achieve their goals. SO can adapt relevant functions, architectural models and use cases from the aforementioned concepts, making the realization of zero-touch SO easier and more meaningful. Apart from that, AI/ML algorithms can detect security risks, categorize different attacks and take measures to ensure trust and security through self-configuration. With benefits such as increased accuracy and diversity, distributed AI/ML solutions help accelerate security control and analytics [36].

B. Functionalities of Security Orchestration:

The functionalities of SO can be divided into four main components, as shown in Figure 2. They are detection, response, mitigation and prevention. At the same time, SO acts as middleware for connecting all these different functions and components.

Detection: Detection is the first step in establishing network security. Detection means detecting unauthorized access and anomalies in the data flow and identifying potential threats. Detection ranges from detecting a simple error flow to sharing the complete analysis of the network to the response unit (decision agent) and the network administrator. SO should be able to fully monitor the network and it is imperative to detect known and unknown threats in real time.

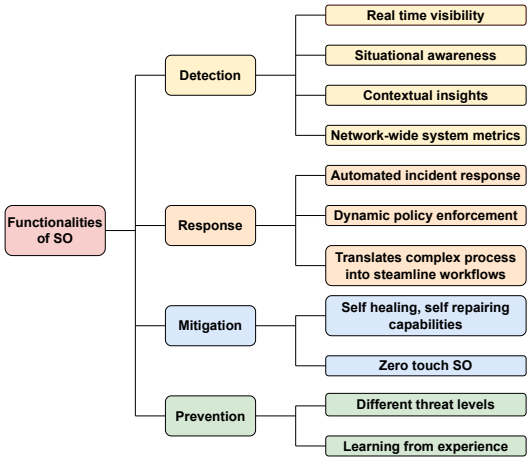

FIGURE 2: Functionalities of Security Orchestration.

The framework should be adaptive and intelligent to detect unexpected threats by utilising metrics from the network system as well as processes and actions from the physical environment [37]. SO is expected to create situational awareness. SO is expected to collect threat data and extract critical characteristics from a large amount of threat data to provide contextual insight to the network administrator or response unit to take appropriate action. An adaptive architecture can respond to unforeseen types of attacks by using different monitoring inputs. The new services and functions of the IoT system introduce previously unknown types of vulnerabilities. Modern AI algorithms use ML to classify attacks according to their threat level to detect, adapt and respond to potential cybersecurity issues. In contrast to conventional infrastructures, detection uses measures from the physical environment as well as metrics and processes of the network system [37].

Response: Response means taking the appropriate action according to the data and the primary analysis of the detection unit. This complex process involves several steps, such as further data analysis, investigation, evaluation of the action and deciding on the appropriate course of action. SO transforms this complex workflow into a series of simple actions through automation and orchestration by dynamically creating, modifying, managing and removing security servicess [4]. High-level security policies defined by a network operator govern the desired system behaviour that is achieved with virtual SFCs [38]. Executable SO actions were created from these security policies. This is necessary to enable an automated response to incidents and to automate the deployment and configuration of security services and repetitive tasks [4]. The enforcement of user-defined policies enables automatic configuration of security features in advance. SO should also be able to determine the endpoint of human interaction until zero-touch SO is achieved. SO is responsible for maintaining the minimum security of the individual services/slice in accordance with the Service Level Agreement (SLA)s.

Mitigation: SO must find the vulnerabilities and affected endpoints to decide on mitigation solutions. SO maintains a database of threats. Once the response unit detects an attack, the mitigation unit searches for possible mitigation solutions based on the database. The mitigation unit then initiates relevant mitigation services and removes them as soon as the threat has been eliminated. The mitigation process is fully automated, intelligent and learns from previous experience. To minimize the impact of complex and novel attacks, security services should evolve with new detection and mitigation mechanisms [38]. With self-repair and self-healing capabilities, SO should be able to defend itself against cyberattacks and mitigate the damage caused without human intervention [39].

Prevention: Prevention means that SO is intelligent enough to prevent security attacks before they occur. SO can use ML, DL and strategic learning methods to detect and prevent attacks. The database mentioned in Mitigation above consists of potential cybersecurity risks, could be classified according to threat level. Using the available database, SOs can take reactive countermeasures to stop cyberattacks and dynamically adapt to the situation after the information collected and assessed by the monitoring probes is available [40]. Once the threat has been eliminated, the prevention mechanisms deployed should be automatically removed and the system should return to normal operating mode so that it can reach its maximum efficiency.

C. Key Components of Security Orchestration Systems

Most research does not define the security orchestrator as a single element, but rather as a plane, as shown in Figure 3. There, other supporting functions and architectural elements are defined as planes. The support of the other planes, such as the security enforcement plane and the user plane, is crucial for the functionality of the security orchestration plane.

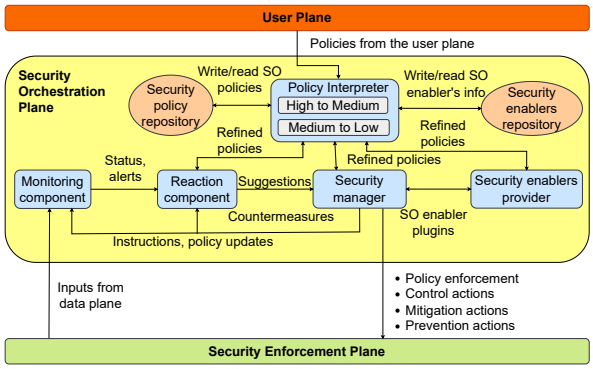

FIGURE 3: Key components of security orchestration

Policy Interpreter: The module is responsible for fine-tuning the security policies. First, the policy interpreter refines the high-level security policies into medium-level security policies that specify workflows and security procedures. It then refines the medium-level security policies into low-level configurations based on the selected enablers.

Security Enablers Provider: The module recognizes the available security plugins according to the required capabilities and the corresponding resource requirements. The enabler plugins are also managed by it.

Monitoring Component: The module is responsible for collecting critical security-related real-time data from physical or virtual appliances that is relevant to system behaviour. If it detects abnormal behaviour in the system, alerts are generated and sent to the reaction module. Several monitoring probes are installed in the infrastructure to monitor the behaviour of the data flow and resources.

Reaction Component: The module takes appropriate countermeasures according to the alerts it receives from the monitoring component. To respond to a detected threat, the reaction component selects policies from the appropriate repository and reconfigures the security enablers.

Security Manager: The module operates according to the security policies selected by the reaction component. It manages the orchestrated deployment of security enablers in the security enforcement plane according to the requirements of the security policy. The security manager enables the onboarding of different drives to achieve interoperability.

D. Security Orchestration vs Security Automation

In general, SO is confused with SA. According to Islam et al., [4], SO is a technique for integrating various security systems and connecting security tools that serve as a connected layer. SO streamlines security procedures and drives security automation. Integration, orchestration, and automation are the three pillars of enabling SO. It offers automated, coordinated, and policy-based security procedures in various technological areas. SO accelerates, reduces the probability of errors, and increases the efficiency of security operations. This is, in fact, an enabler for SA that can be observed as a cause-and-effect relationship between SO and SA. Due to the mechanisms and procedures launched by SO, outcomes expected from SA can be achieved, thus becoming an enabler [41]. Figure 4 shows the differences between SA and SO.

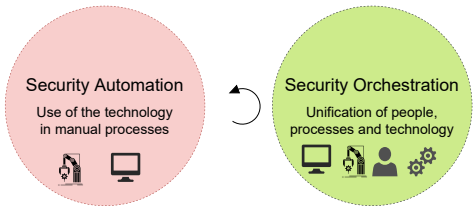

FIGURE 4: Comparison of SA and SO

E. Risk of Security Orchestration

While SO and SA enable more efficient and smarter security deployment through comprehensive network and service management, automation can be a challenge for security.

SO reveals a new set of threat surfaces and vulnerabilities by replicating minor security issues and amplifying their impact [42]. Most of these security issues are not yet visible because SO is not yet fully implemented and operational. SA could easily prevent threats. However, this could lead to botnet infections or DDoS attacks. Additionally, due to zero-touch security, attacks could propagate in closed loops, making detection of these attacks impossible [6]. At the same time, SO services can lead to QoS degradation in network services and use cases due to resource availability and SO processing overhead. SO has its limitations, and understanding these limitations contributes to better network operations. Predefining security policies or decisions can have significant drawbacks. Since many security decisions are context-dependent, a predefined security policy can become a "one-size-fits-all" approach to end-user security in some situations. Rigid, predefined security policies could lead to automation failures [43]. There is a trade-off between the risks and the benefits. When security is automated, the benefits are higher, as are the risks. As for the ratio of SO and risks versus benefits, not only are the risks high, but so are the benefits when security is fully orchestrated. As mentioned earlier, SO/SA risk pillars still exist today. As systems enable many automated or semi-automated operations, these vulnerabilities are likely to become even more pronounced [6].

III. TECHNICAL CHALLENGES RELATED TO SECURITY ORCHESTRATION IN 5G AND B5G NETWORK TECHNOLOGIES

This section addresses the current and anticipated technical hurdles in the implementation of SO in 5G and B5G technologies. These specific challenges were identified as the most critical in our analysis of SO implementation in these technologies. We have paid particular attention to the following areas:

- Network security monitoring for security orchestration in 5G and B5G technologies.
- Interface definition and standardization in relation to security orchestration in 5G and B5G technologies.
- Security and privacy challenges related to security orchestration in 5G and B5G technologies.
- Development and implementation of security orchestration policies in 5G and B5G technologies.
- Scalability considerations for security orchestration in 5G and B5G technologies.
- Multi-Domain Security Orchestration.
- Additional topics such as SSLA monitoring and management, end-to-end security management and the effective integration of IBN in SO.

In addition, this section briefly presents possible solutions to each technical challenge and highlights relevant previous research and work in these areas.

A. Network Security Monitoring for Security Orchestration in 5G and B5G Technologies

1) Introduction

Network security monitoring is a combination of network monitoring and security monitoring, as shown in Figure 5, and is critical to the overall SO chain of action in 5G and B5G technologies [44]. Proper network security monitoring ensures rapid detection of threats, attacks and unauthorized access. Traditional security monitoring, which depends mainly on hardware, could not cover all security requirements in 5G and beyond, where softwareization and virtualization of networks has taken place. Therefore, SO should be able to introduce new monitoring techniques that are compatible with 5G and B5G technologies such as NFV, SDN, edge computing and IoT. All network components should be monitored, including physical, hybrid and virtual networks. At the same time, SO must utilise the capabilities of NFV and SDN for better and more reliable network security monitoring and management. Every research paper in SO includes monitoring in the scope of work. However, many do not have a clear definition or way of working on how monitoring should be implemented. Therefore, monitoring remains one of the biggest technical challenges for SO in 5G and B5G technologies. Without a suitable solution and framework for monitoring network security, the realization of SO in 5G and beyond is impossible. When exploring the challenges, there are some grey areas that require careful attention. These include the placement of monitoring probes, the type of monitoring probes (physical, virtual or both), the processing of available information and the heterogeneity of monitoring interfaces. The monitoring component should be able to collect real-time information about the network related to the behaviour of the system. Once it has analysed and processed this information, the SO plane could get a holistic overview of the network status.

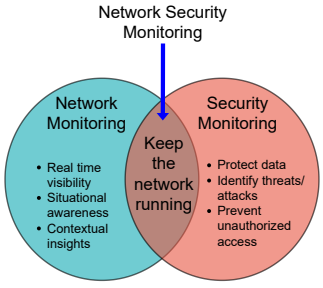

FIGURE 5: Comparison of network and security monitoring.

2) Possible solutions and existing works

To enable the monitoring services, the authors of [39], [45] propose to deploy a distributed set of security monitoring probes, such as traffic and resource monitoring probes and IDS, in the data plane, SDN, NFV and IoT infrastructure domains. These security probes can be physical or virtual

depending on the requirements. The use of virtual security probes has advantages over physical probes, such as scalability, easy deployment on demand and ease of configuration and manageability. They can be easily discarded when the need no longer exists. If the part of the network is physically realized and supports PSFs, there is still a need for physical monitoring probes. The OSS/BSS could control these probes and the monitoring component should be able to distinguish between virtual and physical probes [29].

Jabalpur et al [37], [46] proposes a Security Monitoring Analytic System (SMAS) that queries VIM about the deployed security services while monitoring the host's resources. It also retrieves the logs of the security functions. These works propose to use the existing infrastructure of the NFV architecture and the monitoring functions in SO by defining only the necessary interfaces and communication functions. Many research papers [30], [32], [39], [40], [47]–[50], which focus on researching IoT threats and vulnerabilities using the functionalities of SDN and NFV, propose the implementation of a VSF that can be used as monitoring points to detect different types of attacks. For example, these VSFs can detect active attacks deployed as vAAA, AI-based virtual anomaly detection systems, vIDS, vfirewalls and vIoTHoneyNets. Deep packet inspectors deployed as VSFs can detect passive attacks such as traffic analysis or sniffing/eavesdropping attacks on private IoT communications. There are two primary methods of anomaly detection: ML-based anomaly detection to identify unknown threats such as zero-day attacks, and signature-based intrusion detection, which uses a rule-based approach. Therefore, the monitoring component includes the detection filters, the list of signatures and the associated actions such as alerts, statistics and logs [39]. SDN offers features that can be used to improve the monitoring capabilities of SO. Since SDN separates the control and data plane and takes over the control and monitoring functionalities. The monitoring component can use OpenFlow to gain insights into the data traffic in the network if an API is available between OpenFlow and the monitoring component. Zaalouk et al. [51] presents an advanced SDN architecture that decouples the control and monitoring functionalities to offload the SDN controller and thus improve the performance of security services.

3) Summary

The security monitoring framework continuously monitors the fulfillment of SLAs across the network and ensures that all SLAs are met and the network is secure. The monitoring and response components include state-of-the-art algorithms and methods for analysing threats and correlating information from different sources. Proper monitoring improves security and trust, including self-healing, self-repair and self-protection capabilities, both at the core and at the edge. There are still some research problems that future researchers should explore in relation to monitoring. Many research papers mention the use of physical and virtual security probes. However, there is little explanation of how the monitoring end analyzes these different inputs. The question still remains whether these inputs should be differentiated and treated differently or whether there should be no difference.

B. Interface Definition and Standardization Related to Security Orchestration in 5G and B5G technologies

1) Introduction

The SO plane needs to communicate and interact with different planes with different functions, e.g. the user plane, the security enforcement plane, and the management plane, to ensure E2E security in 5G and B5G. The SO plane enforces most of the security functions in the network using NFV MANO, SDN controller or IoT controller. Various VNFs can be deployed through the NFV MANO, e.g. virtual IDS, virtual firewall, virtual switch/router, virtual IPS, virtual VPN, virtual honeypot/honeynet, virtual bandwidth control and virtual secure web proxy. The SDN controller handles basic security measures for SDN operations such as dropping, forwarding, mirroring and bandwidth reduction of traffic flow. IoT controllers offer various APIs for handling important IoT security mechanisms, e.g. for interface management, traffic protection management and power management. The user plane defines and handles the security policies that are enforced at the SO plane, while the management plane provides real-time network updates to the system administrator and communicates with monitoring and response modules.

Although interoperability and intercommunication are critical to the realization of SO in 5G and B5G technologies, there has not been enough focus on establishing/defining adequate standardization for protocols, message formats, and interfaces between the northern and southern boundaries of the SO plane and adjacent planes. Without a unified communication and interface definition, different research groups and organizations would continue to use their own definitions, which would slow down the realization and growth of SO in 5G and B5G technologies. At the same time, other independent developments and innovations will not be compatible with each other. Therefore, universal standardization to define the interfaces and intercommunication for SO in 5G and B5G technologies is essential.

2) Possible solutions and existing works

VSFs offered by the NFVI should be accessible from the outside as security functions so that the security orchestrator can activate and configure them with the help of the VIM [29]. The authors of [29] present a reference point for managing the ETSI NFV management and orchestration entities, such as the VNF Manager, NFV Orchestrator and the VIM, which would enable SO in a hybrid network. Here, the security orchestrator acts as a centralised trust manager to achieve NFV-wide trust management, which is

very important for interacting with VNF components. VIM provides an API that allows users to create and delete chains, add and remove functions to chains and retrieve details about already deployed chains. Jabalpur et al. [37], [46], suggest that the security orchestrator can use this API to configure and control security services and monitor the provided functions. The Policy Interpreter refines high-level policies into medium-level policies and then into low-level settings according to the selected enablers with the help of the security enablers provider. In this process, the security enabler provider provides plugins to the security orchestrator to access the required/selected enablers and manage them via the corresponding translator plugins. Zarca et al. [30], [32], [39], [40], [47], [48] proposes different plugins and protocols for different interfaces and use-cases. For example, to implement XACML-based vAAA, the security orchestrator selects an XACML plugin to translate the mid-level authorization security policy into an XACML sentence that can be used to configure the XACML-based vAAA. The security orchestrator selects a PANA plugin to translate the mid-level authentication security policy to a PANA configuration when PANA is used for network authentication [48]. The security orchestrator connects to IoT controllers via REST APIs and network protocols such as Constrained Application Protocol (CoAP) and Lightweight M2M (LWM2M). Through northbound APIs exposed by certain vendors (often REST interfaces), it handles MANO orchestrators (e.g. OpenMANO) and SDN controllers (e.g. ONOS) [39].

Hermosilla et al. [33] mention that the southbound orchestration interface includes a set of activities that the security orchestrator needs to control the SDN controller, the IoT controller and the NFV-MANO components. Most existing controllers, including ONOS and OpenDaylight, support a northbound API for managing SDN controllers. The Security Orchestrator manages the IoT controller via a custom interface and protocols such as CoAP, supporting operations such as rebooting, flashing and configuring the device. Last but not least, the orchestrator controls NFV-MANO via a specified northbound interface, which enables tenant and data centre management techniques and VNF life-cycle management, among other things. Salva et al. [45] proposes a model with a Service Infrastructure Manager (SIM) which has the same functionality as the VNF manager in the ETSI MANO architecture. The security orchestrator notifies SIM of a VSF development request, and SIM (Juju) communicates with VIM (OpenStack) to start the VSF installation processes. Zaalouk et al. [51] propose an orchestrator agent in their architecture. This is an application that is installed on each SDN controller and enables the controller to communicate with the orchestrator. Luo et al. [31], proposes Service-Oriented Software-Defined Security (SOSDSec) architecture in which the SOSDSec orchestrator consists of command connectors. These are a set of interfaces that send commands to various security controls via product-specific APIs.

3) Summary

The northbound interfaces of the SO plane handle all communication with the user/system administrator. In contrast, the southbound interfaces handle real-time monitoring and security enforcement activities at the security enforcement plane. The enforcement of security is mainly done by the SDN controller, NFV MANO and IoT controller. Although many research papers claim that this intercommunication and interoperability of the southbound interface can be realized by enabling relevant plugins during medium to low-level policy translation, there is still no standard method for addressing this issue. The use of protocols and message formats is still a question, as the underlying technologies such as SDN and NFV are still in the development phase. No attention has been paid to the northbound interface, and no research work looks in depth at the communication between the user plane and the policy interpreters. There is a lot of room for research and standardization bodies to define and standardize communication (protocols, message formats) and interfaces so that everyone can adhere to a universal platform that supports innovation and more security enablers and plugins. Standardization will lead to faster realization of SO while enabling constant growth.

C. Security and Privacy Challenges Related to Security Orchestration in 5G and B5G technologies

1) Introduction

SO in 5G and B5G technologies are in the development phase. Therefore, many security and privacy issues in SO are still unknown and there is still room for improvement. One of the biggest security challenges in SO are the attacks on the SO plane. This would shut down all security-related activities such as detection, response, mitigation and prevention, leaving the entire network vulnerable to any security attack. At the same time, attacks on the north and south bound interfaces of the SO layer could cause serious security problems. As a result, SO could not deploy the required security measures in the enforcement plane, and the system administrator would be blindsided by the monitoring component without updates. For this reason, dynamic policy adjustments from the user plane to the policy interpreter are not possible. SO inherits the vulnerabilities of the 5G and B5G technologies and platforms used to realize SO. For example, there are pre-existing vulnerabilities of ORAN, ZSM, SDN, NFV, IoT, MEC and network slicing as well as vulnerabilities introduced by the softwarization of the network. Security issues related to VMs, VNFs, hypervisors and containers are also a major concern with regard to the SO in 5G and B5G [19]. Because of zero-touch SO, attacks can propagate in closed loops, making it extremely difficult to detect and mitigate these attacks [52].

AI/ML can be integrated with SO to optimize workflows, monitoring or decision making in 5G and B5G technologies. However, security and privacy issues that arise with ML/AI will also affect SO. Potential security concerns against ML systems include poisoning attacks, data manipulation, data injection, logic corruption, model inversion, model evasion, membership inference, and model extraction attacks [53]. Furthermore, since data processing is invisible to users, attacks on the data that AI models collect for learning purposes could lead to privacy concerns [54]. SO should be able to handle the AI/ML based attacks. These AI/ML-based attacks evolve using AI approaches to learn security risks in a widely distributed network. As a result, rule-based detection techniques are useless.

2) Possible solutions and existing works

One of the critical problems with VMs are VM migration attacks. A MitM attacker can change any VM OS or application state during the VM transfer [55]. When moving to VMs, manipulating the VNF images is comparatively easy. VNF images can be cryptographically checked and signed during the launch to detect such activities. In addition, the trust status of an NFV platform can be verified remotely using remote attestation technology. Such remote attestation systems can be developed using blockchain as a technology [19]. Multiple SDN controllers can be deployed in the core to avoid a single SDN failure point. AI techniques can be used in the development of SO systems to improve overall security, especially in the execution of edge-based federated learning, to enable early detection of attacks and to ensure communication efficiency and data protection [56]. At the perimeter, ML-based algorithms can monitor the activities of other sub-nets and identify malicious traffic originating from other sub-nets. By improving the dynamic provisioning of VNFs on demand, ML-based adaptive security techniques are very effective against attacks on SDN/NFV. Network security with Quantum Machine Learning (QML) can potentially defend against quantum computing attacks [57]. Blockchain can address some security and privacy concerns in SO. Blockchain enables secure authentication, data-sharing, and high privacy [58]. Security-by-Design (SbD) is a strategy in which security requirements are taken into account at the very beginning of the design of a product, service or software [19]. Integration of SbD in SO in the design phase ensures better safety by minimizing the impact of expected safety risks.

3) Summary

Security and privacy issues remain one of the main concerns when implementing the SO in 5G and B5G. The SO plane can be a single point of failure of the network as it centrally manages all security and privacy in the network. There are many research papers dealing with SO, but none has paid enough attention to the security and privacy issues of SO. This may be due to the fact that SO is still in the development phase and has not yet been fully realized. However, considering these aspects in the development phase would lead to a better and more secure design. Functionalities of innovative technologies such as ML/AI and blockchain can be used to solve the security and privacy issues in SO. Furthermore, these security and privacy issues need to be resolved before SO becomes fully functional in B5G. In this case, more attention is needed from the research community.

D. Security Orchestration Policy Definition and Implementation in 5G and B5G technologies

1) introduction

The authors of [59] define a policy as "a definite goal, course or method of action to guide and determine present and future decisions". In general, a policy is a guideline for how to react in certain situations. Network policies reduce the complexity of network configurations, especially in 5G and B5G networks. Network administrators must be able to regulate system behavior at a high level of abstraction. This requires security policies to provide critical features such as interoperability and flexibility. Policy models should be independent of the underlying infrastructure and technology and address the challenges of 5G and B5G such as scalability, heterogeneity and vendor lock.

SO policies intend to include security policies and model other important aspects, such as dependencies and enforcement priority in 5G and B5G. Dependencies could mean that a certain security policy depends on the enforcement of another security policy or on the occurrence of a certain event. The security administrator must be able to model more complex behaviors, such as orchestrating the deployment of security policies by considering a combination of security policies. Prior to SO policy enforcement, the detection of conflicts, anomalies and dependencies between security policies is mandatory. These dependencies or conflicts can occur in two ways: within the same orchestration policy or between different orchestration policies. Different high-level terms need to be resolved as part of the policy refinement process using different contextual data. As a result, several additional criteria must be considered to close the information gap on human concepts defined in the High-level Security Policy Language (HSPL) to the Medium-level Security Policy Language (MPLS). Security policies must be automatically, intelligently and dynamically updated to achieve zero-touch SO with self-repair and self-healing capabilities in 5G and B5G. Policy models should be able to learn from experience and feedback from the enforcement plane and dynamically update their security policies.

2) Possible solutions and existing works

Zarca et al. [30], [32], [39], [40], [47], [48] proposes a novel security policy management framework to address

the heterogeneity of security enablers that span different levels of abstraction. A technology-independent refinement process is enabled by decoupling the desired goal (high-level configuration) from the low-level configurations and underlying components. The authors focus on the orchestration of elements that must interface with related control and management modules to enforce appropriate security policies across domains such as SDN, NFV and IoT. To refine the policy from HSPL to MSPL, Zarca et al. [30] propose using a common language like Common Information Model (CIM) from Distributed Management Task Force (DMTF) to retrieve details about the competencies offered by different components and specific network configurations. A semantically aware orchestration framework for autonomous and policy-driven security management and VSF SFC in softwarized IoT scenarios is presented by Zarca et al. [60]. Different approaches to detect conflicts in IoT system architecture and policies are enabled using rule reasoning and semantic technologies. AI can be used to improve the performance and capabilities of policy models. In this way, AI-based highly dynamic attacks can be easily prevented and mitigated. At the same time, AI and learning can be used in policy models to achieve zero-touch SO.

3) Summary

The SO framework provides AAA, network filtering and forwarding, and channel protection, while the SO policy models are constantly evolving to support more features. Nevertheless, there is a lack of research in the area of 5G and B5G SO policy modeling. The research community has paid virtually no attention to AI-based SO policy modeling, which has tremendous potential for providing zero-touch, self-repair and self-healing capabilities in 5G and B5G. The lack of adequate standardization is also a problem, as there should be a universal way to define policy models that promote innovation and novelty.

E. Scalability Aspects of Security Orchestration in 5G and B5G technologies

1) Introduction

Realization of IoT and Internet of Everything (IoE) in the 5G and B5G era would connect billions of heterogeneous devices to the network [54]. By enabling new, improved services for people and using their network capabilities to develop ubiquitous information systems, IoT and IoE would significantly transform the industrial and domestic environment [61]. Increasing connectivity will lead to a massive exchange of data, and malicious attackers will exploit the vulnerabilities of devices to the fullest [62]. The heterogeneity of IoT devices makes it necessary for SO to ensure the same desired protection in different programming environments. The management and authentication of different gateways and devices, the monitoring of massive data traffic, the convergence of security policies across different domains, the dynamics of IoT environments and mobility management are problems that SO must overcome in terms of scalability in 5G and B5G technologies.

2) Possible solutions and existing works

Network softwarization technologies in 5G, such as SDN, NFV and MEC, can be used to improve scalability and flexibility in SO. Many research papers have integrated SDN, NFV and MEC features into their SO frameworks. VSFs such as vIDS, vFirewalls, vHoneynets, vAAA and vChannel-Protection can be dynamically deployed and provisioned at the edge in a timely manner to improve scalability [45], [47], [48]. Moving to the edge would help handle the huge IoT traffic that will flood networks in the 5G and B5G era. SDN offers dynamic reconfiguration capabilities, new network rules on demand, providing softwareized services on top of the architecture and enforcing security measures such as firewall rules [47]. These virtual network probes, deployed at the edge as IDS, can monitor traffic from IoT devices with greater scalability and provide critical information to the monitoring module, which issues security alerts in the event of potential attacks [49]. Security policies enable a technology agnostic SO framework that allows system administrators to define high-level security requirements independent of the underlying technologies, providing an important tool for improved scalability [30], [32], [39], [40], [47], [48].

3) Summary

One of the key goals of SO in 5G and B5G is to realize a scalable and dynamic security framework that can cope with colossal IoT traffic, billions of heterogeneous devices and thousands of security vulnerabilities. Therefore, a new type of context-aware, holistic security framework is required. To provide security service function chaining, dynamic reconfiguration and customization of virtual security applications, the SO framework should be able to orchestrate SDN controllers, NFV managers and IoT controllers. Figure 6 shows different approaches for solving the scalability problems of SO in 5G and B5G. The research has particularly focused on SO in IoT environments using SDN, NFV and MEC/Fog. One focus of this work is to improve scalability and ensure sound SO. The use of AI/ML technologies to improve the scalability of SO in 5G and B5G technologies has not yet been explored in the literature. There could be huge potential to improve scalability at the edge through AI/ML and distributed learning algorithms.

F. Multi-Domain Security Orchestration

1) Introduction

To meet the requirements of demanding 5G and B5G use case scenarios and achieve sophisticated performance matrices, network management, automation and E2E services

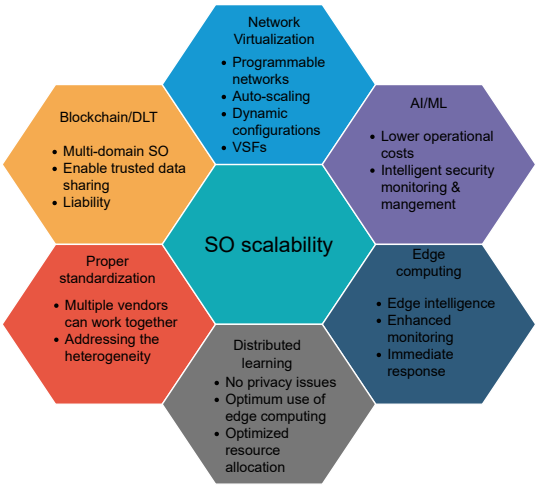

FIGURE 6: Approaches for addressing scalability challenges in security orchestration

across multiple domains are required [53]. Network slices allocated to different applications cannot be covered by a single Mobile Network Operator (MNO) and must be extensible across multiple administrative domains [63]. When it comes to the security of multiple domains, there are two main problems. (i) domains that enforce different security policies, and (ii) domains with different security authorities [64]. Because organizations operate in different environments, security policies may differ from area to area. Different policy interpretations use different security mechanisms to implement a single security policy. The security of multiple domains must be managed by a centralized security framework that comprehensively understands the network and is independent of the underlying virtualization and network infrastructure technologies. Although SO is very important for handling security and better service delivery in multi-domain environments, there are only a handful of papers that address multi-domain SO in 5G and B5G technologies, and almost all of them are related to network slicing.

2) Possible solutions and existing works

Shalitha et al. [65] propose a framework to simplify SO in a federated network slicing system to enable effective security management in 5G and B5G networks. As shown in Figure 7, the proposed framework introduces a Local Security Orchestrator (LSO) to manage security within a single domain and a Global Security Orchestrator (GSO) to manage security in a federated network slicing ecosystem. Khettab et al. [66] propose an architecture that provides SECaaS in an inter-domain platform using SDN and NFV. IDS/IPS, Deep Packet Inspection (DPI) and other various VSFs are deployed and managed with this architecture. A blockchain-based system called BSec-NFVO is presented by Rebello et al. [67], ensuring auditability,integrity and non-repudiation and securing orchestration processes in virtualized networks. The main contribution of this work is that it proposes blockchain technology and transaction models that provide traceability in the NFV context with multiple tenants and domains. Ortiz et al. [42] present an architecture that focuses on zero-touch security in 5G and utilizes state-of-the-art methods such as AI, TEE and DLT in multi-domain environments.

3) Summary

Due to the demanding nature of multi-domain SO, it will be challenging to achieve SO in a multi-domain environment. However, to realize zero-touch, self-repair, and self-healing networks, E2E security management is a must. The research community needs to pay more attention to multi-domain SO, because there is still a long way to go to achieve SO in a multi-domain. One of the key proposals to realize multi-domain SO in 5G and B5G is the establishment of two SO management entities at local and global levels. However, global security management can be a single point of failure, which means that an attack would jeopardize the security of the entire network.

G. Other Issues

1) SSLA monitoring and management in 5G and B5G technologies

With the goal of achieving the necessary QoS from a security perspective, SSLAs provide a clear framework for defining security requirements while analysing compliance [42]. SSLA is a representation of security policies in the form of obligations and specifications that represents an agreement between the service provider and the end user. SO must ensure compliance with the SSLAs so that each service/slice receives the agreed level of security. In addition, SO should be able to handle critical challenges such as monitoring the fulfillment of SSLAs in real time, taking the necessary actions in case of a breach and allocating the limited resources in a way that each service receives its minimum level of security.

2) End-to-End security management in 5G and B5G technologies

The relationship between a network service and a collection of dedicated physical resources is one-to-one in the traditional network infrastructure [68]. However, due to virtualization and softwareization, this formerly simple relationship will become significantly more complex in 5G and beyond. As a result, E2E security management must support network services, physical infrastructures and virtual infrastructures that span multiple domains. SO needs to figure out how to enforce strict and consistent security and management policies between these network services, physical and virtual infrastructure, taking into account their inter dependencies while also considering semantics.

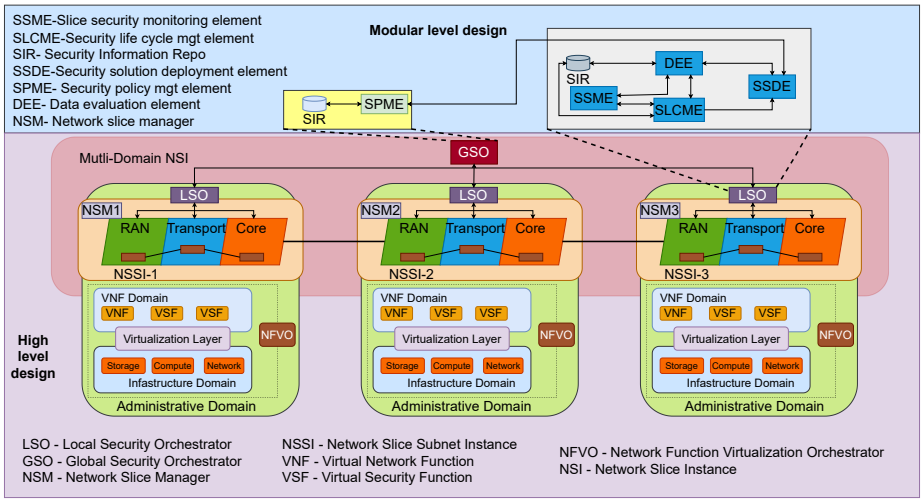

FIGURE 7: Multi-domain security orchestration framework [65]

3) Proper Intent-Based Networking (IBN) business conversion for security orchestration in 5G and B5G technologies

IBN enables simplified network management and automated orchestration, allowing users to determine what policies they want to enforce on their network, rather than how the underlying mechanisms of the network should enforce those policies. Although intents enable the simplification and abstraction of SO, reducing the complexity and proper business implementation of intents can be a challenge. First, there should be a way to monitor and validate the successful implementation of intents related to SO. If alternative intents were implemented, the administrator would want to know why this approach was implemented. Secondly, it may not be possible to implement SO intents immediately due to limited resources and capabilities. Also, SO intents may conflict with current SO policies and states. Explainable SO could be a solution that improves transparency.

To summarize all above technical challenges, Table 2 provides a comparative summary of related works.

IV. Lessons Learned and Future Research Directions in Security Orchestration in 5G and B5G Network Technologies

A. Security Orchestration Taxonomy

1) Lessons learned

SO is a policy-based, adaptive and intelligent security process/framework with dynamic security reaction, attack mitigation, and prevention capabilities relying on monitoring methodologies, cyber situational awareness tools, previous intelligence, and experience. Even though the ultimate goal of SO is to realize zero-touch SO to enable self-repair, self-protection and self-healing capabilities, current implementations still require the presence of humans in various tasks, such as defining policies and responding to unknown scenarios. When deploying SO in networks beyond 5G, this needs to change, which would support a fully autonomous networking paradigm. The SO plane is responsible for the management of SO in the underlying network and usually consists of a policy interpreter, a security enablers provider, a monitoring component, reaction component and a security manager. However, these components and functionalities may vary due to the different requirements and use cases in 5G and beyond networks. For example, Bagaa et al. [38] presents an AI-based reaction agent that incorporates AI and ML models to dictate the SO decisions while hosting a System Model Database (SMD) that stores the necessary information related to enablers and policies. Molina et al. [60] introduces a policy conflict detector and a security orchestrator optimizer to detect and avoid policy conflicts and optimize SO operations. SA is only one part of SO. SO encompasses the automation, coordination and integration of technologies and services to realize a fully secured network while providing E2E security. The integration of AI will further improve the SO in 5G and other technologies. However, there is a trade-off between the risks and benefits of SO. These risks, such as replication of minor security issues and enhancing their impact, propagation of closed-loop attacks, and degradation of quality of service (QoS) can be minimized by using novel technologies such as AI/ML, distributed learning, TEE, blockchain, and proper standardization.

2) Remaining research problems

- How to determine the boundary between human-touch and zero-touch security orchestration?
- How to replace human-touch security orchestration functions while preserving ethical, fair, and policy-complying manner?
- How to facilitate dynamic, autonomous, and intelligent decision-making based on prior knowledge by trusting the information providers?

TABLE 2: Comparative Summary of Related Works

Ref	Description	Monitoring	Interface Definition and Standardization	Security and Privacy Issues	Policy Definition and Implementation	Scalability	Multi-domain SO	Other Issues
[69]	Discussed AI-enabled ORAN research directions, opportunities, and challenges in 6G security.	✓						
[70]	Presented an XAI-based green security architecture for dynamic adjustment of security policies considering energy efficiency and desired security levels for ORAN.	✓	✓	✓		✓		
[71]	Presented the vision of the MARSAL project, which is managing and orchestrating network resources in an elastic and transparent manner to ensure E2E service delivery, including security in B5G.					✓	✓	
[31]	Presented a service-oriented approach to SO for software-defined infrastructure abstracting security controls as security services.		✓					
[51]	Proposed a security orchestrator framework for security that leverages SDN control and network monitoring features.	✓	✓					
[48]	Proposed an innovative policy-based architecture to handle AAA and channel protection.	✓	✓		✓	✓		
[47]	Presented and evaluated an innovative situational-aware and policy-based security architecture for dynamic channel protection and AAA management in IoT networks composed of SDN and NFV.	✓	✓		✓	✓		
[40]	Proposed a comprehensive architectural design for the extent of the ANASTACIA H2020 project.	✓	✓		✓	✓		
[30]	Introduced an innovative policy-based architecture utilizing available IoT security techniques and SDN/NFV-based security mechanisms.	✓	✓		✓	✓		
[49]	Developed a novel architecture for security protection techniques using the envisioned software-based network enablers.	✓	✓		✓	✓		
[39]	Presented a novel mechanism that enables enforcement, orchestration management, and orchestration of the honeynets.	✓	✓		✓	✓		
[45]	Proposed utilizing NFV-MANO to deploy virtual firewalls automatically to safeguard NB-IoT.	✓	✓			✓		
[29]	Presented a security orchestrator framework according to the ETSI NFV Reference Architecture.	✓	✓					
[33]	Proposed a security orchestration architecture to automate dynamically VSFs in MEC UAVs.	✓	✓					
[68]	Proposed a security-oriented MANO framework (SecMANO).							✓
[37]	Design of an automated, dynamic security orchestration solution to safeguard edge servers.		✓					
[46]	Presented a software-based security system that could be configured to react to threats automatically by establishing and managing security function chains.		✓					
[66]	Explored how both NFV and SDN can be utilized to secure network slices when required, ensuring optimal resource allocation.					✓		
[65]	Proposed a framework to facilitate effective security management by streamlining the SO in a federated network slicing system.						✓	
[42]	Presented an intelligent, reliable, and efficient 5G security framework utilizing AI, ML, DLT, and TEE features for closed-loop E2E security management.						✓	✓
[32]	Presented a zero-touch, policy-driven, and semantic-aware SO framework to provide autonomous, conflict-free SO in SDN/NFV-aware IoT situations while assuring optimal VSF allocation and SFC.		✓		✓	✓		
[31]	Presented a service-oriented approach to SO for software-defined infrastructure using abstract security services		✓					
[55]	The lifecycle of the VM, trusted proof of VM, and other notions are presented, solving the issue of migrating a VM from one host to another trustily			✓				
[19]	Discussed 5G security and privacy issues, potential solutions, recent developments, and research directions.			✓				
[56]	Focused on the problem of secure transmission in cooperative dual-hop networks with unreliable relays.			✓				
[57]	Discussed Quantum machine learning			✓				
[58]	Evaluated the use of cloud and fog as hosting platforms for blockchains.			✓				
[67]	Proposed a blockchain-based system that secures orchestration processes in virtualized networks while guaranteeing integrity, auditability, and non-repudiation.						✓	
[72]	Proposed a SO framework that leverages SFC while optimizing QoS (including end-to-end delay, bandwidth, jitters), available resources and capabilities of VNFs.						✓	

- Which methods/techniques enable self-repair, self-protection, and self-healing capabilities in zero-touch SO in 5G and B5G network technologies?
- What are the risks of SO/SA deployments in 5G and B5G network technologies, and how to overcome them?
- What communication protocols and standards can be leveraged to enable zero-touch SO within the novel 5G and B5G SO architectures, and how to coordinate among different SDOs?

3) Future directions

The security policy repository is the place where custom policies are stored [33]. This serves as a playbook for the entire SO process. However, there may also be situations in which the playbook is useless and the security manager does not know how to react. This is where human intervention is required. The use of AI/ML, game theory, distributed learning and concepts such as ZSM and ORAN could potentially reduce human interaction in SO. Developing a smart and intelligent decision module/algorithm that dynamically decides when to engage human presence could be a

potential research question. Novel AI/ML techniques can be used to support essential security functions such as efficient prediction of security anomalies and intelligent decision making [38], [42]. However, significant research is still needed to achieve dynamic and automatic reconfiguration of AI systems in case of unknown attacks and faster and more accurate decision making. The adaptation of SDN/NFV and policy models in SO, supported by ML and big data analytic techniques, improves self-repair, self-prediction and self-healing techniques. In addition, TEE, DLT and ZSM could be used to achieve zero-touch SO, which requires more attention from the research community [42].

There are also risks associated with network automation in SA/SO. Especially in zero-touch SO, where automation is enabled in a closed loop, attacks can spread faster and undetected, putting the entire network at risk. SO increases the threat landscape if it is not properly configured and maintained. SO operations could lead to resource exhaustion and severely impair the QoS of other network services. Game theory can be used to determine optimal strategies for resource allocation. To solve these problems, further research is needed to find new ways for keeping up-to-date policies, automation logics and monitoring techniques. To successfully realize zero-touch security, more research needs to be done in the area of communication between different technologies, frameworks and applications. Common standards must be defined, developed and adopted. The ANASTACIA project [73]has done important work and developed a comprehensive framework for SO that paves the way to zero-touch SO. The integration of enabling technologies such as SDN, NFV, network slicing, MEC, ZSM and ORAN to realize a unified SO framework needs to be further explored. The use of protocols such as TLS (Transport Layer Security), IPsec (Internet Protocol Security) and EAP (Extensible Authentication Protocol) to enable zero-touch security needs to be thoroughly researched.

B. Technical Challenges

1) Lessons learned

Achieving zero-touch, self-healing and self-repair networks through SO is still a long way off due to various challenges in the areas of architecture, application, technology, policy and standardization. 5G and B5G technologies are still at an early stage of deployment or limited to concepts and implementation in test environments. In addition, SO in 5G and B5G technologies is still in the initial research phase. Therefore, the technical challenges related to the implementation of SO have not yet been thoroughly investigated and most of these challenges are not yet known. Therefore, it is better to deal with the known challenges first. Adequate standardization of interaction, interfaces, policy models and communication between different technologies is one way to overcome the technical challenges of SO and improve collaboration and interoperability. SbD is another solution where the principles and concepts of SO are already taken into account in the development and design phase, leading to a smooth integration of SO. Furthermore, most of the security and privacy challenges of SO are related to the underlying technologies, e.g. security and privacy issues related to software protection, AI/ML, IoT, edge computing and network slicing. Therefore, the continuous improvement and further development of these technologies are also important for the successful implementation of SO. Well-defined SSLAs are beneficial for both the users and the network administrator, as satisfaction or breach can be easily measured.

2) Remaining research problems

- How can AI/ML, big data, and DLT be leveraged to address existing technical challenges?
- How to overcome security and privacy issues with edge intelligence, which is highly data-dependent?
- How to tackle the security and privacy issues due to SO and zero-touch security?
- How to achieve multi-domain SO while addressing scalability and secure cross-domain communication?
- How to monitor the satisfaction of SSLAs and ensure immediate actions in case of a violation?
- How to identify and resolve conflicts or dependencies between SO policies?

3) Future directions

AI/ML can be used to improve monitoring and decision making and develop new algorithms for SO policy. DLT/blockchain can be used to address privacy and trust issues and improve scalability [42]. These AI/ML models are being moved to the edge to improve privacy, security issues and response time. The use of AI/ML at the edge is referred to as Edge Intelligence (EI) [74]. The data used to train AI/ML models comes from various sources and is shared by edge servers. Since the outcome of these models is highly data-dependent, EI is very vulnerable to many security attacks [75]. Blockchain can secure distributed edge services and ensure that resource transactions are secure and not vulnerable to malicious nodes [76].

The data used in AI/ML models can lead to privacy issues as they contain privacy-sensitive data. Therefore, more research is needed on novel routing protocols and trusted network topologies to preserve privacy. Federated learning is a distributed data training method for edge AI models that protects user privacy and supports local ML models. In addition, homophobic encryption and secure multi-party computation are considered in the development of privacy-preserving AI model parameter sharing methods [75]. Enabling zero-touch security itself can lead to other security concerns if not handled carefully. One of the main benefits of establishing a communication feedback loop between performance monitoring, identification, adaptation and optimiza-

tion of the network is the possibility of self-optimization. This closed automation allows deception attacks, man-in-the-middle attacks and DoS attacks to take place [52]. The flexibility of software technologies can be used to improve the scalability of multi-domain networks. Separating security orchestration from other domains by defining an E2E security orchestration/management domain could be a way to reduce complexity and enable independent development of security orchestration at both domain and cross-domain levels [42]. In addition, secure cross-domain communication could be achieved by introducing a lightweight communication bus, the so-called inter/cross-domain integration fabric [42], [52], [53]. However, appropriate standardization is required when defining SO-related protocols, message formats and interfaces. Ensuring secure data transmission, dealing with privacy issues, effective monitoring and supporting slicing could be some of the open research questions related to the integration fabric.

Compliance with the SSLA can be monitored via the Network Slice Manager. However, possible interfaces must be researched and defined. There can be a separate module or component in the SO plane to check the compliance of SSLA and to act in case of violations (e.g.: Policy and SSLA Management Function [42]). Understanding resource availability and network security capabilities is needed to manage SSLAs properly. Moreover, optimal resource allocation, automation of the SSLA life cycle and the definition of Security Service Level Objectives (SLOs) are some of the future research directions. Semantic technologies and rule reasoning could identify the policy conflicts that may occur in the SO process [60]. As part of the SO level, a policy manager is introduced, which consists of a policy interpreter and a policy conflict detector. However, the resolution of these conflicts in terms of QoS, satisfaction of SSLAs, and resource availability has not yet been investigated in the research literature, nor are there any possible research directions.

V. Future/Related Technologies for Security Orchestration

A. Artificial Intelligence

AI, supported by ML and big data analysis techniques, are crucial prerequisites for fully autonomous networks [53]. AI can uncover hidden patterns from vast amounts of time-varying data while drawing faster and more accurate conclusions [42]. Novel AI/ML techniques enable SO capabilities, including accurate prediction of security anomalies, intelligent enforcement of security policies and precise deployment decisions for mitigation and preventive actions. Lower operating costs, faster time to value, reduced risk of human error and minimal human interaction are some of the key benefits of AI in SO. Various AI/ML techniques can enable intelligent functions for network monitoring, management and operation. For example, neural networks could be used to detect DoS attacks and network intrusions [77] and K-Nearest Neighbors (K-NN) supervised learning algorithms in malware defections [78]. Deep Learning (DL) enables resource allocation, network security, mobility prediction, traffic classification, and traffic forecasting [79].

Network security design has broadly embraced ML techniques, such as reinforcement learning, unsupervised learning, and supervised learning. These can precisely identify and specify the particular security policies to impose in the data plane [38]. Reinforcement learning (RL) models could be used for response and automation in SO. RL is highly adaptive and is used for real-time deployment in rapidly changing cyber security situations. It can represent autonomous software agents that perform inspections and execute sequential tasks as efficiently as possible without prior knowledge [80]. Artificial Neural Networks (ANN) could be trained to find invisible Cyber Threat Intelligence (CTI) patterns without the need for specialized human knowledge to make predictions in data [12]. The main focus of most research related to AI/ML is the use of AI/ML capabilities for intelligent security monitoring and response [81]. However, there is still much to be done in the area of SO, including detection, incident response, mitigation and prevention of attacks. Only a handful of studies address the use of workflow orchestration and automation with AI/ML to increase the effectiveness and efficiency of SO. Therefore, significant effort and research is required to implement E2E security orchestration using AI/ML techniques.

In many situations, AI can be a double-edged sword, as it has the potential to either protect or violate security and privacy [54]. The lack of transparency and interoperability could lead to problems with data protection, trust, legal compliance and accountability. For example, the General Data Protection Regulation (GDPR) gives people the right to receive an explanation of how an automated system arrived at a judgment [53]. A huge amount of data is required to create accurate and efficient learning models. At the same time, some of the required data is not available for privacy and commercial reasons. The quality of the available data, i.e. accurate, adequate, comprehensive and timely data, is also an issue. The quality of data is essential for providing relevant insights and decisions. In addition, data patterns can change over time, so the AI/ML models need to be retrained to account for the variations in the datasets and thereby improve predictive capabilities [82]. Many AI/ML models are black box models because their logic is difficult to explain. The interpretation of AI/ML models will provide accountability, reliability and transparency. To solve this problem, XAI enables to move to a more transparent AI. It tries to provide a set of methods that generate more comprehensible models while maintaining a high-performance [83]. If it is possible to integrate the full capabilities of AI/ML techniques into SO, AI/ML can be essential in improving advanced SO functions such as self-protection, self-planning, self-healing, and self-optimization. AI/ML can also accelerate the process of practical implementation of SO. The development of

AI/ML capabilities and SO processes and workflows is essential for the realization of zero-touch networks.

B. DLT/Blockchain

Like AI, DLT is also a promising technology that qualitatively and quantitatively expands the possibilities of SO. Among DLTs, blockchain is the most popular in the telecommunications industry due to its properties such as immutability, decentralization, anonymity, provenance, and security. In a Peer-to-Peer (P2P) network, a blockchain is an open database that manages an immutable distributed ledger [84]. Blockchain is therefore an indispensable technology that will reliably and securely enable various services in future networks [85]. DLT/blockchain can be used to solve some of the most important technical challenges in the SO, such as multi-domain SO, scalability and security, privacy and trust issues. INSPIRE-5Gplus defines a security-oriented architecture and contains a domain integration fabric that enables cross/inter-domain communication. Blockchains have been deployed to achieve trusted data sharing and as part of the data collection capabilities via the integration fabric [42]. Blockchain capabilities can be used in SO to enable features such as intelligent resource management, enhanced security features including privacy, authentication and access control, data integrity, availability and accountability, and scalability [85].

In addition, DLT/blockchain has the potential to act as an enabling technology to support SO-related service models in 5G and B5G technologies. Some of these services are secure slice brokering, automated SSLA management, secure VNF management and scalable IoT as well as user privacy protection. The vulnerabilities of AI/ML are mainly due to corrupted data in both the training and testing phase [86]. In a multi-tenant/multi-domain environment, DLT could be used to realize the trust aspects, such as protecting the integrity of AI data through immutable data sets and distributing trust among many stakeholders [75]. In addition, the blockchain can make the decision-making process of machine learning methods more comprehensible and solve many data protection, trust and security issues. SO and DLT/blockchain in network security are emerging research areas and have not yet reached their full potential. Therefore, the integration of blockchain into SO will accelerate the realization of SO. To achieve this, extensive research and focus is required.

C. Quantum Computing

Quantum Computing (QC) enables exponentially faster computing by using quantum superposition to realize the advantage of quantum parallelism [87]. Within the next few years, QC will be commercially available and will have a positive and negative impact on network security. QC could be used to enhance SO functions such as vulnerability detection, mitigation and prevention in 5G and B5G technologies [75]. Moreover, QC can solve computationally challenging SO optimization problems, including efficient resource allocation. Blind Quantum Computing (BQC), also known as secure quantum computing, could be used to improve data privacy in SO in 5G and B5G technologies. With quantum advances in supervised and unsupervised learning for classification and clustering applications, QML could improve security and privacy in SO. Figure 8 shows the use of BQC and QML to extend the capabilities of SO. On the other hand, QC represents a major challenge for existing cryptographic systems. Since QC is still in the development phase, it is not easy to predict all use cases of quantum computing in SO. However, aligning the research focus on QC-enabled SO will enable many potential use cases to realize zero-touch SO in 5G and B5G networks.

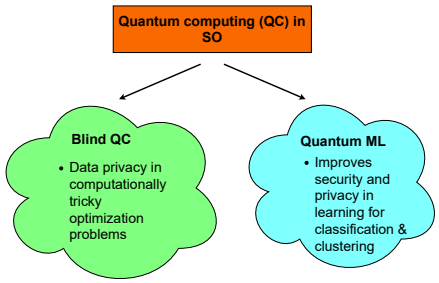

FIGURE 8: Important Quantum Computing Methods in Security Orchestration.

D. Trusted Execution Environment

TEE is an isolated, secure and integrity-protected computing environment with storage and memory capabilities that is independent of the rest of the system and in which applications can be executed securely [88]. Even in the presence of malicious operators or kernels, TEE is designed to provide integrity and secrecy in virtualized environments. As shown in the figure 9, the functionalities of TEE in SO can be used to address issues such as trust, security and privacy in multiple domains [42]. In addition, TEE is used in processing to ensure trustworthiness when passing important processing data to an external party and can also be a critical component of slice isolation. To identify the domain(s) or partners responsible for the errors and failures and hold these domains accountable for the damage caused to customers, INSPIRE-5Gplus uses TEE to establish Liability-Aware Security Management (LASM) [42], [89]. The performance overhead, the compilation requirements, the setup effort, the need for changes at source code level and the incompatibility are some of the problems of TEE. TEE is a matter of SbD. The security orchestrator/manager must decide where to deploy TEE depending on the SSLAs, taking into account security and performance metrics. Integrating TEE into the network development process would allow security processes to be managed and executed smoothly while ensuring privacy, trust and liability in SO. There are few research studies on TEE in SO. Therefore, the research community needs to pay attention to utilizing the capabilities of TEE to realize the full potential of SO.

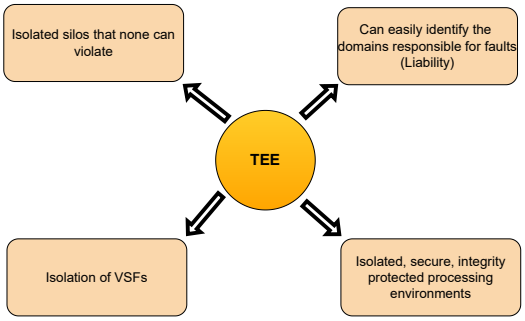

FIGURE 9: TEE functionalities that can be leveraged in security orchestration

VI. Conclusion

SO has emerged as a key technology for addressing the evolving security challenges in 5G and B5G network environments. This paper presents a comprehensive analysis of SO, covering its evolution, functionalities, key components and risks. The technical challenges specific to 5G and B5G such as network security monitoring, interface standardization, scalability and multi-domain orchestration have been explored in detail, as well as potential solutions and existing work. We have highlighted the critical need for robust SO systems that ensure security and privacy while providing scalability and interoperability in these advanced networks. Emerging technologies such as AI, DLT, Quantum Computing, and TEE hold great promise when it comes to overcoming the limitations of traditional approaches to SO. Despite significant progress, some challenges remain, including standardization gaps, the efficient implementation of policies and the integration of multiple domains. Future research must focus on developing intelligent, adaptive and automated SO solutions capable of handling the complexity and heterogeneity of 5G and B5G networks. By leveraging cutting-edge technologies, the research community can pave the way for secure, resilient and efficient next-generation networks.

REFERENCES

[1] A. Ahmed and E. Ahmed, "A Survey on Mobile Edge Computing," in *10th IEEE International Conference on Intelligent Systems and Control (ISCO)*, 2016, pp. 1–8.

[2] F. Ullah, M. Edwards, R. Ramdhany, R. Chitchyan, M. A. Babar, and A. Rashid, "Data exfiltration: A review of external attack vectors and countermeasures," *Journal of Network and Computer Applications*, vol. 101, pp. 18–54, 2018.

[3] E. Cole, *Network security bible*. John Wiley & Sons, 2011, vol. 768.

[4] C. Islam, M. A. Babar, and S. Nepal, "A multi-vocal review of security orchestration," *ACM Computing Surveys (CSUR)*, vol. 52, no. 2, pp. 1–45, 2019.

[5] R. Montesino and S. Fenz, "Automation possibilities in information security management," in *2011 European Intelligence and Security Informatics Conference*. IEEE, 2011, pp. 259–262.

[6] W. K. Edwards, E. S. Poole, and J. Stoll, "Security automation considered harmful?" in *Proceedings of the 2007 Workshop on New Security Paradigms*, 2008, pp. 33–42.

[7] R. Montesino and S. Fenz, "Information security automation: how far can we go?" in *2011 Sixth International Conference on Availability, Reliability and Security*. IEEE, 2011, pp. 280–285.

[8] S. M. Mohammad and S. Lakshmisri, "Security automation in information technology," *INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)–Volume*, vol. 6, 2018.

[9] R. Montesino, S. Fenz, and W. Baluja, "Siem-based framework for security controls automation," *Information Management & Computer Security*, 2012.

[10] M. Donevski and T. Zia, "A survey of anomaly and automation from a cybersecurity perspective," in *2018 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2018, pp. 1–6.

[11] R. Sravanthi and T. Nisha, "Moving from detection centric to prevention centric security using automation: A survey," in *Journal of Physics: Conference Series*, vol. 1964, no. 4. IOP Publishing, 2021, p. 042048.

[12] J. Kinyua and L. Awuah, "Ai/ml in security orchestration, automation and response: Future research directions," *Intell. Autom. Soft Comput*, 2020.

[13] Y. Zheng, A. Pal, S. Abuadbba, S. R. Pokhrel, S. Nepal, and H. Janicke, "Towards iot security automation and orchestration," in *2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. IEEE, 2020, pp. 55–63.

[14] Nguyen, Phu and Dautov, Rustem and Song, Hui and Rego, Angel and Iturbe, Eider and Rios, Erkuden and Sagasti, Diego and Nicolas, Gonzalo and Valdés, Valeria and Mallouli, Wissam and others, "Towards smarter security orchestration and automatic response for CPS and IoT," in *2023 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*. IEEE, 2023, pp. 298–302.

[15] j. Lins, Fernando AA and Sousa, Erica TG and Rosa, Nelson S, "A survey on automation of security requirements in service-based business processes," vol. 13, no. 1, pp. 3–29, 2018.

[16] N. Šatkauskas, A. Venčkauskas, N. Morkevičius, and A. Liutkevičius, "Orchestration security challenges in the fog computing," in *Information and Software Technologies: 26th International Conference, ICIST 2020, Kaunas, Lithuania, October 15–17, 2020, Proceedings 26*. Springer, 2020, pp. 196–207.

[17] Bringhenti, Daniele and Marchetto, Guido and Sisto, Riccardo and Valenza, Fulvio, "Automation for network security configuration: State of the art and research trends," *ACM Computing Surveys*, vol. 56, no. 3, pp. 1–37, 2023.

[18] Cao, Yang and Pokhrel, Shiva Raj and Zhu, Ye and Doss, Robin and Li, Gang, "Automation and orchestration of zero trust architecture: Potential solutions and challenges," *Machine Intelligence Research*, vol. 21, no. 2, pp. 294–317, 2024.

[19] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196–248, 2019.

[20] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5g and beyond," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3682–3722, 2019.

[21] M. E. Kuhl, M. Sudit, J. Kistner, and K. Costantini, "Cyber attack modeling and simulation for network security analysis," in *2007 Winter Simulation Conference*. IEEE, 2007, pp. 1180–1188.

[22] A. Goutam, R. Kamal, and M. Ingle, "Service integration towards security orchestration," *International Journal of Information and Education Technology*, vol. 2, no. 2, p. 179, 2012.

[23] R. Warschofsky, M. Menzel, and C. Meinel, "Automated security service orchestration for the identity management in web service based systems," in *2011 IEEE International Conference on Web Services*. IEEE, 2011, pp. 596–603.

[24] T. Koyama, B. Hu, Y. Nagafuchi, E. Shioji, and K. Takahashi, "Security orchestration with a global threat intelligence platform," *NTT Technical Review*, vol. 13, no. 12, 2015.

[25] S. Chollet and P. Lalanda, "An extensible abstract service orchestration framework," in *2009 IEEE International Conference on Web Services*. IEEE, 2009, pp. 831–838.

[26] A. Baouab, O. Perrin, N. Biri, and C. Godart, "Security meta-services orchestration architecture," in *2009 IEEE Asia-Pacific Services Computing Conference (APSCC)*. IEEE, 2009, pp. 28–33.

[27] N. S. Chahal, P. Bali, and P. K. Khosla, "A proactive approach to assess web application security through the integration of security tools in a security orchestration platform," *Computers & Security*, vol. 122, p. 102886, 2022.

[28] G. ETSI, "V1. 1.1:,"network functions virtualisation (nfv); management and orchestration," esti ind," *Spec. Group (ISG) Network Functions Virtualisation (NFV), Sophia-Atipolis Cedex, France [online]*, 2014.

[29] B. Jaeger, "Security orchestrator: Introducing a security orchestrator in the context of the etsi nfv reference architecture," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1. IEEE, 2015, pp. 1255–1260.

[30] A. Molina Zarca, J. Bernal Bernabe, I. Farris, Y. Khettab, T. Taleb, and A. Skarmeta, "Enhancing iot security through network softwarization and virtual security appliances," *International Journal of Network Management*, vol. 28, no. 5, p. e2038, 2018.

[31] S. Luo and M. B. Salem, "Orchestration of software-defined security services," in *2016 IEEE International Conference on Communications Workshops (ICC)*. IEEE, 2016, pp. 436–441.

[32] A. M. Zarca, M. Bagaa, J. B. Bernabe, T. Taleb, and A. F. Skarmeta, "Semantic-aware security orchestration in sdn/nfv-enabled iot systems," *Sensors*, vol. 20, no. 13, p. 3622, 2020.

[33] A. Hermosilla, A. M. Zarca, J. B. Bernabe, J. Ortiz, and A. Skarmeta, "Security orchestration and enforcement in nfv/sdn-aware uav deployments," *IEEE Access*, vol. 8, pp. 131 779–131 795, 2020.

[34] M. Liyanage, Q.-V. Pham, K. Dev, S. Bhattacharya, P. K. R. Maddikunta, T. R. Gadekallu, and G. Yenduri, "A survey on zero touch network and service (zsm) management for 5g and beyond networks," *Journal of Network and Computer Applications*, p. 103362, 2022.

[35] E. Zeydan and Y. Turk, "Recent advances in intent-based networking: A survey," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*. IEEE, 2020, pp. 1–5.

[36] S. Wang, M. A. Qureshi, L. Miralles-Pechuaán, T. Huynh-The, T. R. Gadekallu, and M. Liyanage, "Explainable ai for b5g/6g: Technical aspects, use cases, and research challenges," *arXiv preprint arXiv:2112.04698*, 2021.

[37] E. Jalalpour, M. Ghaznavi, D. Migault, S. Preda, M. Pourzandi, and R. Boutaba, "A security orchestration system for cdn edge servers," in *2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*. IEEE, 2018, pp. 46–54.

[38] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, "A machine learning security framework for iot systems," *IEEE Access*, 2020.

[39] A. M. Zarca, J. B. Bernabe, A. Skarmeta, and J. M. A. Calero, "Virtual iot honeynets to mitigate cyberattacks in sdn/nfv-enabled iot networks," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1262–1277, 2020.

[40] A. M. Zarca, J. B. Bernabe, R. Trapero, D. Rivera, J. Villalobos, A. Skarmeta, S. Bianchi, A. Zafeiropoulos, and P. Gouvas, "Security management architecture for nfv/sdn-aware iot systems," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8005–8020, 2019.

[41] "Top 5 best practices to automate security operations," May 2019. [Online]. Available: https://www.microsoft.com/security/blog/2017/08/03/top-5-best-practices-to-automate-security-operations/

[42] J. Ortiz, R. Sanchez-Iborra, J. B. Bernabe, A. Skarmeta, C. Benzaid, T. Taleb, P. Alemany, R. Muñoz, R. Vilalta, C. Gaber *et al.*, "Inspire-5gplus: Intelligent security and pervasive trust for 5g and beyond networks," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 2020, pp. 1–10.

[43] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security," *BT technology journal*, vol. 19, no. 3, pp. 122–131, 2001.

[44] C. authored by A&T and P. A. N. A. 9, "Network security monitoring: The nexus of network and security operations." [Online]. Available: https://cybersecurity.att.com/blogs/security-essentials/network-security-monitoring-the-nexus-of-network-and-security-operations

[45] P. Salva-Garcia, E. Chirevella-Perez, J. B. Bernabe, J. M. Alcaraz-Calero, and Q. Wang, "Towards automatic deployment of virtual firewalls to support secure mmtc in 5g networks," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2019, pp. 385–390.

[46] E. Jalalpour, M. Ghaznavi, D. Migault, S. Preda, M. Pourzandi, and R. Boutaba, "Dynamic security orchestration for cdn edge-servers," in *2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*. IEEE, 2018, pp. 329–331.

[47] A. Molina Zarca, D. Garcia-Carrillo, J. Bernal Bernabe, J. Ortiz, R. Marin-Perez, and A. Skarmeta, "Enabling virtual aaa management in sdn-based iot networks," *Sensors*, vol. 19, no. 2, p. 295, 2019.

[48] A. M. Zarca, D. Garcia-Carrillo, J. B. Bernabe, J. Ortiz, R. Marin-Perez, and A. Skarmeta, "Managing aaa in nfv/sdn-enabled iot scenarios," in *2018 Global Internet of Things Summit (GIoTS)*. IEEE, 2018, pp. 1–7.

[49] I. Farris, J. B. Bernabé, N. Toumi, D. Garcia-Carrillo, T. Taleb, A. Skarmeta, and B. Sahlin, "Towards provisioning of sdn/nfv-based security enablers for integrated protection of iot systems," in *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE, 2017, pp. 169–174.

[50] G. Bugár, M. Vološin, T. Maksymyuk, J. Zausinová, V. Gazda, D. Horváth, and J. Gazda, "Techno-economic framework for dynamic operator selection in a multi-tier heterogeneous network," *Ad Hoc Networks*, vol. 97, p. 102007, 2020.

[51] A. Zaalouk, R. Khondoker, R. Marx, and K. Bayarou, "Orchsec: An orchestrator-based architecture for enhancing network-security using network monitoring and sdn control functions," in *2014 IEEE Network Operations and Management Symposium (NOMS)*. IEEE, 2014, pp. 1–9.

[52] C. Benzaid and T. Taleb, "Zsm security: Threat surface and best practices," *IEEE Network*, vol. 34, no. 3, pp. 124–133, 2020.

[53] ——, "Ai-driven zero touch network and service management in 5g and beyond: Challenges and research directions," *IEEE Network*, vol. 34, no. 2, pp. 186–194, 2020.

[54] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "Ai and 6g security: Opportunities and challenges," in *Proc. IEEE Joint Eur. Conf. Netw. Commun.(EuCNC) 6G Summit*, 2021, pp. 1–6.

[55] X. He and J. Tian, "A trusted vm live migration protocol in iaas," in *Chinese Conference on Trusted Computing and Information Security*. Springer, 2017, pp. 41–52.

[56] C. Ma, J. Li, M. Ding, H. H. Yang, F. Shu, T. Q. Quek, and H. V. Poor, "On safeguarding privacy and security in the framework of federated learning," *IEEE network*, vol. 34, no. 4, pp. 242–248, 2020.

[57] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum machine learning," *Nature*, vol. 549, no. 7671, pp. 195–202, 2017.

[58] M. Samaniego, U. Jamsrandorj, and R. Deters, "Blockchain as a service for iot," in *2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*. IEEE, 2016, pp. 433–436.

[59] C. Basile, A. Cappadonia, and A. Lioy, "Network-level access control policy analysis and transformation," *IEEE/ACM Transactions On Networking*, vol. 20, no. 4, pp. 985–998, 2011.

[60] A. Molina Zarca, M. Bagaa, J. Bernal Bernabe, T. Taleb, and A. F. Skarmeta, "Semantic-aware security orchestration in sdn/nfv-enabled iot systems," *Sensors*, vol. 20, no. 13, p. 3622, 2020.

[61] L. Atzori, A. Iera, and G. Morabito, "Understanding the internet of things: definition, potentials, and societal role of a fast evolving paradigm," *Ad Hoc Networks*, vol. 56, pp. 122–140, 2017.

[62] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer networks*, vol. 76, pp. 146–164, 2015.

[63] T. Taleb, I. Afolabi, K. Samdanis, and F. Z. Yousaf, "On multi-domain network slicing orchestration architecture and federated resource control," *IEEE Network*, vol. 33, no. 5, pp. 242–252, 2019.

[64] J. Vazquez-Gomez, "Multidomain security," *Computers & Security*, vol. 13, no. 2, pp. 161–184, 1994.

[65] S. Wijethilaka and M. Liyanage, "Security orchestration framework for federated network slicing," *IEEE EUCNC*, 2021.

[66] Y. Khettab, M. Bagaa, D. L. C. Dutra, T. Taleb, and N. Toumi, "Virtual security as a service for 5g verticals," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2018, pp. 1–6.

[67] G. A. F. Rebello, I. D. Alvarenga, I. J. Sanz, and O. C. M. Duarte, "Bsec-nfvo: A blockchain-based security for network function virtualization orchestration," in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE, 2019, pp. 1–6.

[68] M. Pattaranantakul, R. He, A. Meddahi, and Z. Zhang, "Secmano: Towards network functions virtualization (nfv) based security management and orchestration," in *2016 IEEE Trustcom/BigDataSE/ISPA*. IEEE, 2016, pp. 598–605.

[69] S. Soltani, M. Shojafar, R. Taheri, and R. Tafazolli, "Can open and ai-enabled 6g ran be secured?" *IEEE Consumer Electronics Magazine*, vol. 11, no. 6, pp. 11–12, 2022.

[70] P. Porambage, J. Pinola, Y. Rumesh, C. Tao, and J. Huusko, "Xcaret: Xai based green security architecture for resilient open radio access

networks in 6g," in *2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. IEEE, 2023, pp. 699–704.
[71] J. S. Vardakas, K. Ramantas, E. Datsika, M. Payaró, S. Pollin, E. Vinogradov, M. Varvarigos, P. Kokkinos, R. González-Sánchez, J. J. V. Olmos *et al.*, "Towards machine-learning-based 5g and beyond intelligent networks: The marsal project vision," in *2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*. IEEE, 2021, pp. 488–493.
[72] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, "Qos and resource-aware security orchestration and life cycle management," *IEEE Transactions on Mobile Computing*, vol. 21, no. 8, pp. 2978–2993, 2020.
[73] A. P. Consortium, accessed on 27.07.2021. [Online]. Available: http://www.anastacia-h2020.eu/
[74] G. Plastiras, M. Terzi, C. Kyrkou, and T. Theocharidcs, "Edge intelligence: Challenges and opportunities of near-sensor machine learning applications," in *2018 ieee 29th international conference on application-specific systems, architectures and processors (asap)*. IEEE, 2018, pp. 1–7.
[75] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6g security and privacy," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1094–1122, 2021.
[76] S. Xu, Y. Qian, and R. Q. Hu, "Edge intelligence assisted gateway defense in cyber security," *IEEE Network*, vol. 34, no. 4, pp. 14–19, 2020.
[77] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications surveys & tutorials*, vol. 18, no. 2, pp. 1153–1176, 2015.
[78] J. W. Branch, C. Giannella, B. Szymanski, R. Wolff, and H. Kargupta, "In-network outlier detection in wireless sensor networks," *Knowledge and information systems*, vol. 34, no. 1, pp. 23–54, 2013.
[79] C. Zhang, P. Patras, and H. Haddadi, "Deep learning in mobile and wireless networking: A survey," *IEEE Communications surveys & tutorials*, vol. 21, no. 3, pp. 2224–2287, 2019.
[80] M. H. Ling, K.-L. A. Yau, J. Qadir, G. S. Poh, and Q. Ni, "Application of reinforcement learning for security enhancement in cognitive radio networks," *Applied Soft Computing*, vol. 37, pp. 809–829, 2015.
[81] L. H. A. Reis, A. Murillo Piedrahita, S. Rueda, N. C. Fernandes, D. S. Medeiros, M. D. de Amorim, and D. M. Mattos, "Unsupervised and incremental learning orchestration for cyber-physical security," *Transactions on emerging telecommunications technologies*, vol. 31, no. 7, p. e4011, 2020.
[82] J. Ali-Tolppa, S. Kocsis, B. Schultz, L. Bodrog, and M. Kajo, "Self-healing and resilience in future 5g cognitive autonomous networks," in *2018 ITU Kaleidoscope: Machine Learning for a 5G Future (ITU K)*. IEEE, 2018, pp. 1–8.
[83] A. Adadi and M. Berrada, "Peeking inside the black-box: a survey on explainable artificial intelligence (xai)," *IEEE access*, vol. 6, pp. 52 138–52 160, 2018.
[84] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5g beyond," *IEEE network*, vol. 33, no. 3, pp. 10–17, 2019.
[85] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6g: Challenges, opportunities and research directions," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*. IEEE, 2020, pp. 1–5.
[86] M. Barreno, B. Nelson, R. Sears, A. D. Joseph, and J. D. Tygar, "Can machine learning be secure?" in *Proceedings of the 2006 ACM Symposium on Information, computer and communications security*, 2006, pp. 16–25.
[87] C. Wang and A. Rahman, "Quantum-enabled 6g wireless networks: Opportunities and challenges," *IEEE*, 2021.
[88] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: what it is, and what it is not," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1. IEEE, 2015, pp. 57–64.
[89] C. Gaber, J. S. Vilchez, G. Gür, M. Chopin, N. Perrot, J.-L. Grimault, and J.-P. Wary, "Liability-aware security management for 5g," in *2020 IEEE 3rd 5G World Forum (5GWF)*. IEEE, 2020, pp. 133–138.

Sadeep Batewela earned a Bachelor's in Electrical and Electronic Engineering from the University of Peradeniya, Sri Lanka, in 2016, and a Master's in Wireless Communication Engineering from the University of Oulu in 2019. Currently pursuing a PhD at the Centre for Wireless Communications, he also works as a SoC Modelling Engineer at Nokia. His research covers security orchestration, ORAN security, and game theory for 5G/B5G networks.

Pasika Ranaweera is an Assistant Professor at the School of Electrical and Electronic Engineering, University College Dublin (UCD), Ireland. Previously, he was a Postdoctoral Researcher and project manager of the CONFIDENTIAL-6G project. He earned his Ph.D. from UCD in 2023. He is a member of NetSLab and PEL research groups at UCD. More info: https://people.ucd.ie/pasika.ranaweera

Madhusanka Liyanage(Senior Member, IEEE) is an Associate Professor/Ad Astra Fellow and Director at the Network Softwarization and Security Labs (NetsLab), School of Computer Science, University College Dublin, Ireland. Dr. Liyanage's research interests are 5G/6G, Blockchain, Network security, Artificial Intelligence (AI), Explainable AI, Federated Learning (FL), Network Slicing, Internet of Things (IoT), and Multi-access Edge Computing (MEC). More info: www.madhusanka.com

Engin Zeydan received his Ph.D. in Electrical Engineering from Stevens Institute of Technology, USA, in 2011. He is a Senior Researcher at CTTC and Project Coordinator of the UNITY-6G project. Previously, he coordinated the H2020 MonB5G project. His research interests include telecommunications, data engineering, and network security.

Mika Ylianttila is a Professor at the Centre for Wireless Communications, University of Oulu, Finland, leading the NetSEC research group. He has authored over 200 peer-reviewed articles and serves as an associate editor for IEEE Transactions on Information Forensics and Security. He is an IEEE Fellow.