


# Unleashing Security: Shaping the Resilient Future of 5G/B5G Network Orchestration

Aitor Landa Arrue , Aitor Urbieto   
Ikerlan Technology Research Centre  
Basque Research and Technology Alliance (BRTA)  
Arrasate-Mondragón, Spain  
{alanda,aurbieta}@ikerlan.es

Iñaki Garitano   
Department of Electronics and Computing  
Mondragon Unibertsitatea  
Arrasate-Mondragón, Spain  
igaritano@mondragon.edu

**Abstract**—In the era of Industry 4.0, expanding device connectivity via 5G and Beyond 5G (B5G) networks introduces significant security challenges, and advanced solutions for attack detection and mitigation are needed. This study focuses on the complexities of distributed architecture inherent to 5G/B5G networks, underscoring the crucial role of network service orchestration, Moving Target Defense strategies, and advanced attack detection mechanisms. This research identifies cutting-edge mechanisms for ensuring the security of service orchestration through an in-depth state-of-the-art analysis, focusing on artificial intelligence-driven solutions for zero-touch networks. By minimizing human intervention, these networks offer enhanced security and efficiency.

**Index Terms**—5G, B5G, Split Learning, MTD, Orchestration, Zero-touch, Cybersecurity

**Contribution type:** *Research in development.*

## I. INTRODUCTION

The Industrial Revolution 4.0 brings a massive escalation of connected devices, known as the Internet of Things (IoT). The need to provide these devices with reliable, secure, and high-speed communication solutions means that 5th Generation (5G) technology standard communications will play a crucial role in this scenario [1]. 5G communications are characterized by low latency and high bandwidth, which makes it possible to connect IoT devices massively, i.e., massive Machine-Type Communications (mMTC), at high speed [2].

In this scenario, orchestration tools enable scalable, fault-tolerant, and distributed solutions. However, they are not exempt from external threats. These threats can be caused by inherited vulnerabilities in the software used, improper use or misconfiguration of services and tools, or the absence of security mechanisms in the developed solution [3].

The security of 5G and Beyond-5G (B5G) networks has become a priority due to the growth of connected devices and the reliance on critical infrastructures, particularly in industrial IoT environments [2]. These environments are characterized by complex networks of interconnected devices that play a vital role in operational efficiency, real-time monitoring, and automated decision-making. Ensuring the integrity, confidentiality, and availability of services in industrial environments contributes to developing innovative strategies to strengthen the security and reliability of emerging networks [4].

In the context of 5G/B5G networks, their distributed nature leads to multi-domain architectures that require orchestration solutions due to their complexity. Networks orchestrated by Artificial Intelligence (AI) are proposed to manage multi-domain scenarios, minimizing human interaction [1], [5].

Standardization groups, such as ETSI ZSM ISG([6]), are already working on specifications for these networks.

As threats are also increasing with the rise of connected devices, an essential matter in communication networks is attack detection and mitigation to minimize their impact on network performance [7].

The document is structured in four sections: first, an overview of the context is provided in section I, and for a deeper insight section II explains the leading technologies. Then, the relevant state-of-the-art is provided during section III. After that, the main challenges of each technology are described in section IV. Finally, the section VI summarizes the conclusions of the conducted research.

## II. BACKGROUND

The following sections introduce the technologies analyzed during this paper to understand the following sections. Technologies such as 5G architecture, zero-touch networks, attack detection using machine learning, and attack mitigation using moving target defenses are explained.

### A. 5G architecture

The architecture of the 5G network is described by 3GPP TS 23.501 [6] and is distributed both geographically and logically. These standards support the use of cloud and edge computing to enhance network performance and resource utilization. Core network services are hosted in the cloud due to its superior computing and storage capacities, while applications needing lower latency or stricter performance metrics are placed at the edge, close to users. This setup follows the Service-based Architecture (SBA) outlined in 3GPP TS 23.502 [8] and is supported by network slicing from 3GPP TS 23.501 [6], which allows the network to process data efficiently and meet diverse service requirements. The logical distribution of network functions as microservices (see Fig. 1) within the SBA ensures the network is scalable and adaptable.

### B. Attack detection

Attack detection aims to analyze network traffic and identify patterns, distinguishing between regular networks and malicious behavior. Specifically, this analysis focuses on detecting Distributed Denial of Service (DDoS) attacks perpetrated by one or more network clients, compromising network availability. Shallow learning and deep learning algorithms are utilized as subcategories of statistical methods for attack detection. This is due to their widespread use and superior

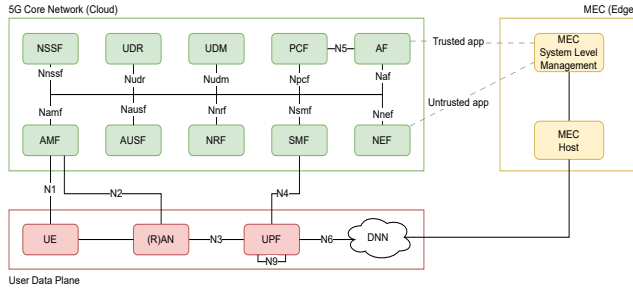


Figure 1: 5G Core Network and MEC integration architecture.

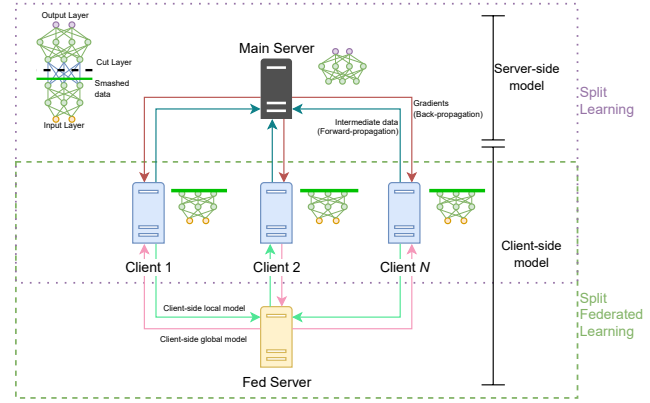


Figure 2: Split Learning architecture.

predictive performance. In this case, the detection problem is classified as a classification problem.

1) *Machine Learning for attack detection:* ML is a field of AI that focuses on developing systems and algorithms to learn from experience or data and improve their performance. The goal is for these models to generalize and apply their knowledge to new or unseen situations, improving their performance over time.

Furthermore, DL is preferred due to its ability to generalize and learn when handling complex problems. In attack detection, ML is commonly utilized for tasks such as pattern recognition, classification, clustering, dimensionality reduction, computer vision, and natural language processing [9].

Indeed, several neural networks stand out for their contributions. Autoencoders are useful for data classification and privacy protection by encoding raw data [10]. Convolutional Neural Networks (CNNs) excel in analyzing network traffic to detect attack patterns through feature extraction [11]. Recurrent Neural Networks, with their short-term memory capabilities, are optimal for sequential data analysis, impacting time-based detection [12]. Restricted Boltzmann Machines and Deep Belief Networks offer unique structures for probabilistic analysis and data distribution, significantly enhancing threat identification and classification in cybersecurity [13], [14].

2) *Distributed Learning in B5G networks:* As stated in [15], B5G networks are transitioning towards ubiquitous networking and computing. Federated Learning (FL) is an interesting option for decentralized training, where the models are trained in each domain, and their weights are shared with a coordinator. This coordinator aggregates the different local models and generates a global model that is then shared with the network domains [16]. Although the model weights are shared, training data is stored on local devices.

However, while FL distributes model training and enhances data privacy, it may not be the best approach for resource-constrained devices such as Industrial IoT (IIoT) devices. Therefore, a recent alternative to FL is Split Learning (SL) [17]. This approach involves splitting a model by its layers and distributing the training of those layers among devices rather than training a complete model on different devices and then sending their weights to an aggregator. The server or device with more computing resources trains the more complex or heavy layers. The layers' outputs are communicated to the central server for aggregation and creation of the final model. The layer responsible for cutting the model for distribution is known as the cut layer. The data sent from

the client to the server is called smashed data.

Split Federated Learning (SFL) pretends to join the best features of both distributed learning methods as a hybrid approach where FL and SL are combined. SFL trains the client-side model in parallel mode FL, and the model is split into different parts and sent to the clients, as in SL. In SFL, a *fed server* is introduced on the client side, i.e., a server dedicated to synchronizing the client-side model [18] by aggregating them. The network is divided into two main domains: client-side and server-side. As stated, the clients and the *fed server* are placed on the client side. In the case of server-side, the primary server is located in Figure 2.

### C. Attack Mitigation

Attack mitigation aims to minimize the impact of threats on the system [7]. Once detected, threats are contained through defined steps or processes. This paper analyzes the following two methods for mitigation: the use of Moving Target Defense (MTD) techniques and zero-touch architectures as the basis of a mitigation solution.

1) *Moving Target Defense:* Traditional defenses such as IDS and IPS take static actions in attack mitigation or incident response. Attackers can model these actions, allowing them to change their attack strategy and adapt to those actions to bypass the countermeasures [19]. The defender is at a disadvantage compared to the attacker because countermeasures are not readily adaptable, and changing them frequently to match the behavior of the attacker is costly. To address this issue and level the playing field, MTD was developed to introduce uncertainty for the attacker by periodically modifying the attack surface when an attack is detected [20], [21].

MTD is a deception technique. This means that the system will change in some way to make the attackers believe they are attacking a real target, even if that target may not exist. MTD is classified as Spatial MTD or Temporal MTD.

Spatial MTD, based on the type of the parameters that are modified, the spatial MTD is classified as follows (see Figure 3):

- **Shuffling MTD.** Dynamically configure network system information.
- **Diversity MTD.** Diversifies the configurations of network information systems.

- **Redundant MTD.** Increase the redundancy of servers, hardware, and OS configurations.

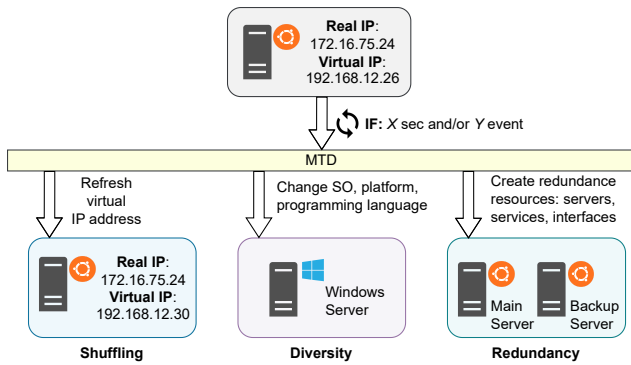


Figure 3: MTD techniques based on attributes.

Temporal MTD is focused on time triggering. The MTD actions can be time-, event- or hybrid-driven. Time-driven strategies ensure that any information obtained by the attacker will expire quickly. Event-driven MTD implies that the switching time is variable, and the attack surface changes based on the attack event. The strategy is triggered by information such as security alarms [22]. Hybrid MTD is triggered by both time and event. Indeed, the network parameters are randomized in a fixed period to trigger the transfer of the attack surface, and an analysis engine collects real-time security events and evaluates potential attacks by analyzing existing attacks [23].

2) *Zero-touch Networks:* Zero-touch networks focus on network automation and self-managing, using AI to enhance the functionalities offered by the networks [24]. To this end, several projects are underway to standardize this type of network, among which the following stand out, e.g., ETSI ZSM (see Figure 4), ETSI ENI ISG, 3GPP SA TSG. In the European Union, the group led by ETSI is one of the most important ones, which defines a framework characterized by its service-based, policy-driven, modular, extensible, scalable, and fault-resistant architecture [24]. The logic behind zero-touch networks is composed of closed-loop mechanisms. Closed loops are means to achieve automatized configurations without any external intervention. These loops are continuously repeated, allowing them to receive continuous feedback from the network. Because of that feedback, the network can improve its configurations and optimize itself.

### III. RELATED WORK

This section explains the current state of orchestration, attack detection, and attack mitigation in 5G/B5G networks; hence, the primary objective is to protect the networks from cyberattacks. To address these, attack management focuses on detection and mitigation mechanisms and orchestration mechanisms provided by the zero-touch network architecture. The zero-touch network architecture is also proposed as the base architecture for B5G networks. The section is divided into three main blocks, each addressing a specific topic.

#### A. Zero-touch architecture in B5G

Ortiz et al. [25], as part of INSPIRE-5G+ project, proposed a network architecture based on ETSI ZSM [26], which results

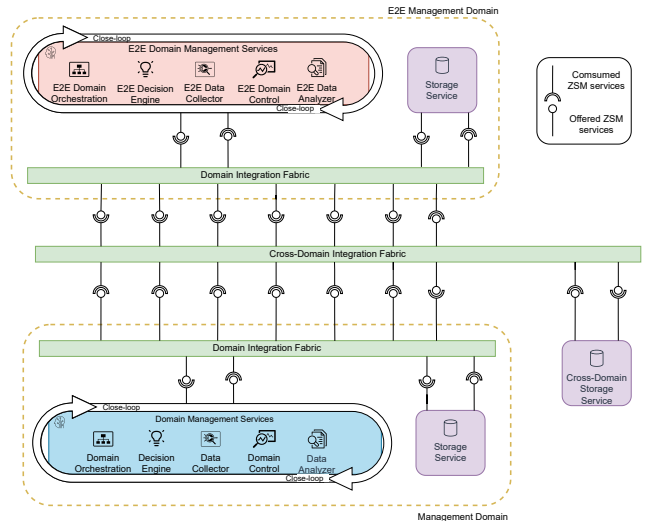


Figure 4: ETSI ZSM architecture

in a solution integrating zero-touch networks, MTD mitigation techniques, and FL-based attack detection [25]. In addition, it also has a trust and repudiation module for the solution trustability, which uses Distributed Ledger Technologies (DLTs). Mitigating the threats is done by fulfilling a Security Service Level Agreement (SSLA) and applying security policies through the relevant services to ensure compliance.

Several frameworks based on zero-touch architecture have recently been implemented. One framework proposed by [7] focuses on mMTC networks within 5G technology. The architecture suggests detecting anomalous traffic to avoid DDoS attacks. The system analyzes the Subscription Permanent Identifier (SUPI). If anomalous traffic is detected, the user identified with that SUPI is disconnected and added to a blacklist. Chergui et al. [27] proposes a new framework for managing massive and dynamic network segmentation in 5G/B5G networks. This framework complies with ETSI ZSM and ENI standards and manages the resources needed for network services during their life-cycle management through Service Level Agreements (SLAs). The text proposes using Federated Learning (FL) in a zero-touch architecture to predict SLA policy violations.

In the European Union, several other projects have been developed, including INSPIRE5G+ [25], 5GZORRO, and ACROSS, all of which focus on 5G/B5G technologies.

Carrozzo et al. [28], as part of the European 5GZORRO project, take zero-touch network architecture as a reference and describe the use of DLTs together with Smart Contracts as the technology to be used to ensure trustability.

Giannopoulos et al. [29] takes part in the ACROSS project, which focuses on developing a secure architecture based on zero-touch platforms aligned with the ETSI standard (ETSI ZSM [26]). The architecture is a highly scalable solution that manages distributed networks through instance orchestration within a domain and multi-domain orchestration. One of its features is traffic engineering, which predicts and reacts to different network events. In addition, the goal is to achieve a high degree of automation across different domains based

on the zero-touch architecture. The section on orchestration security proposes using three mechanisms: trusted execution environments, improved security of AI models through defenses against data and model manipulation, and software-defined security (SD-SEC).

While the proposed solutions achieve a high degree of automation by applying actions from previously declared policies in SSLAs, these may not be efficient when executing attack mitigation mechanisms. Since SSLAs are static agreements, they do not adapt when the state of the network changes, potentially rendering the initial policies obsolete over time. Moreover, if the network is overloaded or threatened, a policy specified in the SSLA could worsen the situation. To address these limitations, it is crucial to implement dynamic monitoring and automated responses that not only detect SSLA violations but also assess ongoing network status to ensure that mitigation actions remain effective.

Table I provides a comprehensive summary of the key topics and findings in the reviewed literature.

### B. Attack detection in B5G networks

Naeem et al. [30] proposed a semi-supervised active learning framework in ZSM, which is based on the assumption that the majority of data on the client side is not labeled. Only a small portion of labeled data is available. In this work, multiple-class attack classification is performed using the attacks identified by the CSE-CIC-IDS2018 dataset. The dataset includes network traffic where seven different attacks are performed: brute force, heartbleed, botnet, DoS, DDoS, web attacks, and network infiltration. Naeem et al. [30] underscore the architecture detailed in [31] where because of their perspective of security, the domain services are slightly changed, from ETSI defined architecture [26].

Jaysasinghe et al. [32] proposes a hierarchical FL model for ZSM networks. In this case, an anomaly detection process is divided into two stages in the security management domain. During the first stage, the anomalies from the users are detected using ML algorithms just for superficial traffic filtering, and the traffic is stored in a database to retrain the local model in the future. The packets classified as anomalies will be dropped from the network at stage 1, and then the second anomaly detector will analyze the rest again. That second detector has a more complex ML algorithm and database. For anomaly detection UNSW-NB 15 [33] dataset is used, which includes normal and malicious traffic. The malicious traffic is divided into nine attacks: fuzzers, analysis, backdoors, DoS, exploits, generic, reconnaissance, shellcode, and worms

Ben Saad et al. [34] also take zero-touch architecture as the scenario for deploying an FL algorithm. In this case, they develop a framework that protects the DL models from poisoning attacks by detecting and mitigating them. Poisoning attacks are critical for the ML/DL model due to their capacity to compromise the future decisions of the model. While this vulnerability affects all AI models generically, it should not be dismissed because it impacts 5G/B5G networks. Modifying the preconditions of the models could seriously compromise the network's security, leading to the misclassification of attacks or detecting normal traffic as anomalous, rendering the solution useless, or even gaining control over the network.

Despite SL is not currently used for attack detection, given the orientation of 5G towards massive communications, exploring Split Learning as a mechanism to train models may be of interest. Similar to previous work, [35] compares FL and SL through various experiments. The experiments show that when the data is Independent and Identically Distributed (IID) and balanced, models trained by SL converge faster than those trained by FL, whereas FL is a more efficient choice for non-IID data. Indeed, SL fails to learn in the latter case. Hafi et al. [36] discuss the challenges, requirements, and future directions of integrating split federated learning into B5G networks. The paper proposes using SFL as an IDS for threat detection, with the training phase split between different hosts. For instance, each host learn the characteristics by training an autoencoder, and then the model is trained on the central server.

Besides, Hafi et al. [36] discuss the benefits of using zero-touch networks in conjunction with SFL. This approach reduce training time while maintaining high accuracy values and data privacy in a multi-tenancy environment.

In Table II, the works on distributed learning and their respective topics are presented.

### C. Attack mitigation in B5G networks

After detecting attacks, it is necessary to mitigate the impact of the attack on the system so that the damage caused is the least possible and causes the least possible disruption to the services offered to the end user.

Using MTD techniques, a combination of diversity and shuffling techniques is proposed in [37]. Specifically, VM Live Migration shuffling is proposed to change the location of VMs and OS diversification. However, the paper mentions that combining both MTD techniques substantially increase the use of extra resources, so their applicability to an Industrial IoT environment must be evaluated [4].

In [38], a framework is developed to mitigate DDoS slow-rate attacks. The attacks are mitigated by Reinforcement Learning (RL), where the model acts as a controller that chooses what actions should be taken in the network. The framework consists of six modules: traffic monitoring modules, Intrusion Detection System (IDS), MTD module, statistics and rule manager, Intrusion Prevention System (IPS), and reactive forwarding rules module. Specifically, shuffling techniques are used in the step where MTD is used.

Javadpour et al. discussed the SCEMA framework [39], [40], which aims to reduce implementation costs while keeping the security level unchanged or even higher. As the previous work, Yunfaicela-Naula et al. [38], it uses Random Route Mutation (RRM), which is based on backward attack path to calculate the path cost and on a modification of Three-tier Attack Graph (TAG) to calculate compromise probability of a host. The critical paths more vulnerable than others are selected, and then all the hosts in these paths are shuffled. Some hosts are less critical than others and could be used as part of the army of the attackers. Therefore, the critical ones should be shuffled sooner than the host, whose impact could be lower. Hence, the goal for attack mitigation is to design a low-complexity MTD method that shuffles only the hosts with more connections to the critical server.



Table I: State-of-the-art of zero-touch networks.

●Addressed topic. ○Not addressed topic. ◐Partially addressed topic.

Ref.	Attack Detection	Attack Mitigation	Standard Compliance	Trustworthy Solution	Policy-based Mitigation	Remarks
[25]	●	MTD	●	●	●	They use zero-touch architecture as the base of the network using ETSI ZSM [26] defined architecture.
[7]	●	Blacklisting	◐	○	○	DDoS attack detection. SUPI blacklisting based on threshold
[28]	○	<i>Undefined</i>	○	●	○	The paper presents the conceptual architecture based on zero-touch networks improved by AI and DLT distributed security and trust.
[29]	●	AI/ML-based	●	●	○	They aim to achieve a highly scalable orchestration based on zero-touch network architecture.

Table II: State-of-the-art of distributed learning approaches for attack detection.

●Addressed topic. ○Not addressed topic. ◐Partially addressed topic.

Ref.	Federated Learning	Split Learning	Split Federated Learning	5G/B5G Application	Attack Detection	Remarks
[17]	●	●	●	●	○	They also provide information about other alternatives inside SL, such as Parallel Split Learning.
[25]	●	○	○	●	●	The paper contributes to INSPIRE5G+ project which proposes a solution considering attack detection by FL, mitigation by MTD and trustworthiness.
[30]	●	○	○	●	●	An integrated scenario with zero-touch networks is considered, where the data is mostly unlabeled. Federated semi-supervised learning is used to train the few labeled data available.
[32]	●	○	○	●	●	The detection process is divided into two stages, first a simpler one to detect anomalies faster and the second one to inspect thoroughly the remaining traffic.
[34]	●	○	○	●	◐	Poisoning attack detection is performed.
[36]	●	●	●	●	◐	The paper is a survey and a theoretical approach, attack detection is tackled just as a potential use case.

Similar to SCEMA [40], other works [41], [42], [43] that seek to optimize the use of MTD with cost-effective approaches use game theory, usually Markov Decision Process (MDP), which identifies two main costs, the costs of the attacker and the defender. The cost of the attacker refers to the resources required to compromise a host of the defenders. Likewise, defense cost refers to the effort or cost of the defense action to prevent or mitigate the attack. The goal of MTD techniques in game theory is to maximize the payoff of the defender while minimizing the payoff of the attacker.

There has been limited research on integrating MTD in 5G/B5G networks. Soussi et al. propose MERLINS [44], based on their previous work [45], an MTD framework that employs Deep Reinforcement Learning (DRL) algorithms to mitigate Advanced Persistent Threats (APT). Escaleira et al. [46] propose an MTD-as-a-Service (MTDaaS) solution using three MTD types: shuffling, diversity, and redundancy. The focus is on exchanging between different versions of an application, where more than one version can coexist simultaneously to deceive attackers. For the decision-making, DRL is used. However, despite using the three types simultaneously, the impact of the decision-making in the system is barely measured, which in large deployments or resource-consuming applications could result in network and host overhead problems. Abdelhay et al. [47] suggest a solution for privacy and security that uses MTD to shuffle IPs and mitigate DDoS attacks in the 5G core network.

As illustrated in Table III, the characteristics of each

mitigation mechanism are summarized.

#### IV. OPEN CHALLENGES

This section discusses the primary challenges of zero-touch networks, attack detection, and attack mitigation. For each subsection, the challenges from the research conducted in this paper are inferred, as well as future directions and next steps.

##### A. Zero-touch networks architecture

Concerning network orchestration, zero-touch networks seem to be a clear direction in which technology is evolving. These networks are intended to automate their management to the point of not needing human interaction. Ortiz et al. [25] propose a good starting point as it already suggests proof-of-concept architecture integrating other services. However, this solution uses predefined SSLAs and policies to decide what reaction to take upon detection of an attack. Although SSLAs define the minimum requirements that all mechanisms in the network should fulfill when defining reactive action in case any SLA is violated, it could deal with the automatization issue in case the policies get deprecated, or the network suffers an attack that was not previously considered. Therefore, other dynamic mechanisms that can decide the reactive actions over the network and service based on the SSLA requirements might be a suitable option.

Within zero-touch networks, trustworthiness is still a crucial issue. Generally, as Palma et al. [48] discuss in their paper, blockchain mechanisms often address this problem. In the case of [48], [28], DLTs are used to create Smart Contracts

Table III: MTD as attack mitigation state-of-the-art.

●Addressed topic. ○Not addressed topic. ◐Partially addressed topic. MDP: Markov Decision Process. RRT: Renewal Reward Theory. S: Shuffling. D: Diversity. R: Redundancy. APT: Advance Persistent Threats. HARM: Hierarchical Attack Representation Model. CES: Cost-Effective Shuffling.

Ref.	Decision process	Cost-effective	MTD technique	MTD trigger	Mitigated attack	5G/B5G application	Remarks
[37]	HARM	●	S, D	<i>Undefined</i>	<i>Undefined</i>	○	The authors propose different shuffling and diversity combination approaches and their impact on the performance.
[38]	DRL	●	S	Event	Slow-rate DDoS	○	The paper integrates DL-based attack detection with DRL attack mitigation using MTD against slow-rate DDoS attacks.
[39], [40]	SCEMA	●	S	Time	DDoS	○	Based on TAG model, the main difference is in the third tier, where in this work Petri networks are used.
[41], [43]	MDP & CES	●	S	Event & Payoff	DDoS	○	They propose the use of Trilateral Game, considering attacker, defender, and user.
[42]	RRT	●	S	Time	Covert Channel attacks	○	They use two cost measures: adaptation and attack cost. It uses an adaptation analysis engine to measure the adaptation cost and make shuffling decisions.
[44], [45]	DRL	●	S	Hybrid	APT	●	MERLINS mitigates APTs and can operate under SLAs.
[46]	DRL	○	S, D, R	Time	Zero-day attacks	●	They propose MTD-as-a-Service (MTDaaS) approach for Cloud Network Function (CNF) agnostic architecture.
[47]	<i>Undefined</i>	○	S	Time	DDoS	●	This approach also mentions the privacy topic, addressing it by SDP zero-trust technique.

between the services, guarantee trust between them, and trace the operations that are carried out.

Considering the zero-touch architecture and its potential as the basis for future communication networks, Alotaibi et al. [49] demonstrated that the proposed architecture for hierarchical federated learning could be adapted to the ZSM architecture [26]. However, looking forward to massive or ultra-massive communications, FL could be less efficient than other approaches, such as SL or SFL.

### B. AI-driven attack detection

As discussed in section II, the target attacks of this work are DDoS attacks perpetrated by one or more clients against network services and infrastructure. Regarding attack detection, two trends are straightforward: shallow and DL algorithms. However, there are not many works where these two streams are complementary. Combining both algorithms makes it possible to reduce traffic prediction delays by using a simpler and faster algorithm to split malicious and benign traffic. Moreover, considering the distributed nature of 5G networks, where services are in the cloud and at the edge, it is logical to think about integrating these two streams of attack detection with FL or SL, thus adapting to the reality of each environment and being able to adjust the model periodically.

Furthermore, SL or SFL are interesting alternatives that split the model between different devices. Considering the zero-touch architecture, integrating SFL into these networks could be beneficial. This involves training locally on the devices in each domain, utilizing their computational capacity for ubiquitous computing.

To the best of our knowledge, attack detection and network traffic analysis using SL is still unexplored. However, CNNs-based SL algorithms are widely used for image identification [18], [35], [50], [51]. Since CNNs are used for both imaging and attack detection [11], [12], the performance efficiency of SL/SFL versus FL could be extrapolated to attack detection. It should be noted that the training data in this case may differ, so further analysis is required.

Additionally, in SL/SFL and FL, data privacy is ensured using methods such as differential privacy [50]. Moreover, considering its ability to allow the workload distribution between devices when splitting the model (Figure 2), these methods are an interesting alternative to investigate in the 5G/B5G network security field. Constrained devices are found in this environment, and the reduced computational capacity is a limitation when training AI models, such as IIoT devices. Hafi et al. [36] also supports this possibility by establishing attack detection as a potential use case for SL.

### C. Mitigation techniques

In terms of mitigating attacks or threats, some studies propose the development of a reactive module in zero-touch networks as a way to respond to these attacks. Applying MTD techniques to mitigate network attacks and automating their execution using AI, such as RL, could be considered.

One effective method in implementing Moving Target Defense (MTD) strategies within 5G/B5G networks involves integrating shuffling techniques, such as RRM and Random Host Mutation (RHM), with diversity strategies. Evaluating the cost-efficiency of this combined approach is crucial to

ensure that the MTD mechanisms do not introduce excessive overhead to the network infrastructure. Furthermore, while some studies advocate for a trilateral game theory model for MTD decision-making, the analyzed research favoring 5G solutions recommends utilizing DRL algorithms. This preference underscores the importance of optimizing cost-effectiveness while minimizing the impact on network performance. Therefore, a thorough examination is necessary to determine the most appropriate MTD approach for 5G and B5G networks, focusing on balancing security enhancements against potential performance drawbacks.

Furthermore, utilizing MTD mechanisms with zero-touch networks are an interesting approach to assure a high degree of automatization in the reaction performed when an SSLA is violated or an attack is detected.

## V. FUTURE WORK

Regarding future work for the research on **zero-touch networks**, it involves testing the orchestration features of a deployed zero-touch network to test relevant services and its operation. Specifically, the role of RL in zero-touch networks is a field to investigate. Beyond resource allocation, a promising research direction is to use RL to perform the decision-making in the domain orchestration for attack mitigation together with the zero-touch networks. The research is focused on analyzing the role that SSLAs play in orchestrating zero-touch networks and whether RL algorithms is complementary to them. SSLAs play a crucial role in defining network requirements and policies. In this way, predefined network requirements are maintained, but policy reaction instructions are replaced. The reaction is based on an RL model that makes decisions depending on the violated policy and network state. This approach aims to enhance decision-making flexibility and enable dynamic updates in response to network incidents.

As future approaches for **attack detection**, SFL need to be studied for DDoS attack detection and model training using both SFL and FL to evaluate their effectiveness, advantages, and disadvantages. DDoS attacks compromise network availability, bringing down critical services and leaving end users without service. Due to the increase of connected devices and the enablement of massive communications, DDoS attacks play a significant role in 5G/B5G networks. Furthermore, the integration of SFL and zero-touch architecture for traffic analysis is a potential research line.

As stated in the previous section III, the integration of MTD mechanisms in 5G and 6G is scarcely addressed. Thus, this is a potential area for further research in **attack mitigation** beyond intrusion detection and prevention systems. Specifically, various methods for calculating the cost of MTD decision-making have been proposed in the area of MTD. However, these methods are not equally weighted in each job or considered. Therefore, the impact of this cost weighting on MTD mechanisms requires investigation.

## VI. CONCLUSIONS

Our comprehensive review highlights the necessity of orchestration in the security of 5G/B5G networks to address the rise in cyber threats due to the increment of connected devices. By integrating (1) zero-touch network principles and leveraging artificial intelligence for (2) proactive attack

detection and (3) dynamic mitigation, we propose a novel approach to network security. This approach adapts to the complexities of distributed network architectures and offers a base for future advancements in network management and security. The analysis of SL and FL presents a promising approach for enhancing attack detection capabilities without compromising data privacy or system performance. As the digital landscape evolves, adapting and integrating these mechanisms into the orchestration of 5G/B5G networks will ensure robust and resilient communication infrastructures. Future research aims to improve these strategies, emphasizing real-world applicability and scalability to protect against the next generation of cyber threats effectively.

## ACKNOWLEDGEMENTS

This work has been partially supported by CyberSEAS, European program H2020-SU-DS-2020, under grant agreement number 101020560. It was also partially supported by the Department of Economic Development, Sustainability, and Environment of the Basque Government under the ELKARTEK 2023 program, project BEACON (with registration number KK-202300085).

## REFERENCES

- [1] C. Benzaid and T. Taleb, "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, 3 2020.
- [2] P. Varga, J. Peto, A. Franko, D. Balla, D. Haja, F. Janky, G. Soos, D. Ficzer, M. Maliosz, and L. Toka, "5G support for Industrial IoT Applications— Challenges, Solutions, and Research gaps," *Sensors* 2020, Vol. 20, Page 828, vol. 20, no. 3, p. 828, 2 2020.
- [3] 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 Management (ZSM) for 5G and beyond networks," *Journal of Network and Computer Applications*, vol. 203, p. 103362, 7 2022.
- [4] C. C. Lin, C. T. Tsai, Y. L. Liu, T. T. Chang, and Y. S. Chang, "Security and Privacy in 5G-IIoT Smart Factories: Novel Approaches, Trends, and Challenges," *Mobile Networks and Applications*, vol. 1, pp. 1–16, 7 2023.
- [5] A. Martín, J. Egaña, J. Flórez, J. Montalbán, I. G. Olaizola, M. Quartulli, R. Viola, and M. Zorrilla, "Network resource allocation system for QoE-aware delivery of media services in 5G networks," *IEEE Transactions on Broadcasting*, vol. 64, no. 2, pp. 561–574, 6 2018.
- [6] TSGS, "TS 123 501 - V15.3.0 - 5G; System Architecture for the 5G System (3GPP TS 23.501 version 15.3.0 Release 15)," 2018.
- [7] R. Niboucha, S. B. Saad, A. Ksentini, and Y. Challal, "Zero-Touch Security Management for mMTC Network Slices: DDoS Attack Detection and Mitigation," *IEEE Internet of Things Journal*, vol. 10, no. 9, pp. 7800–7812, 5 2023.
- [8] TSGS, "TS 123 502 - V17.12.0 - 5G; Procedures for the 5G System (5GS) (3GPP TS 23.502 version 17.12.0 Release 17)," 2024.
- [9] A. Shrestha and A. Mahmood, "Review of deep learning algorithms and architectures," *IEEE Access*, vol. 7, pp. 53 040–53 065, 2019.
- [10] J. Zhang, L. Pan, Q. L. Han, C. Chen, S. Wen, and Y. Xiang, "Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 3, pp. 377–391, 3 2022.
- [11] H. Liu, B. Lang, M. Liu, and H. Yan, "CNN and RNN based payload classification methods for attack detection," *Knowledge-Based Systems*, vol. 163, pp. 332–341, 1 2019.
- [12] A. Chawla, B. Lee, S. Fallon, and P. Jacob, "Host Based Intrusion Detection System with Combined CNN/RNN Model," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11329 LNAI, pp. 149–158, 2019.
- [13] Y. Imamverdiyev and F. Abdullayeva, "Deep Learning Method for Denial of Service Attack Detection Based on Restricted Boltzmann Machine," *Big Data*, vol. 6, no. 2, pp. 159–169, 6 2018.
- [14] A. Voulodimos, N. Doulamis, A. Doulamis, and E. Protopapadakis, "Deep Learning for Computer Vision: A Brief Review," *Computational Intelligence and Neuroscience*, vol. 2018, 2018.

- [15] Q. Li, Z. Ding, X. Tong, G. Wu, S. Stojanovski, T. Luetzenkirchen, A. Kolekar, S. Bangolae, and S. Palat, "6G Cloud-Native System: Vision, Challenges, Architecture Framework and Enabling Technologies," *IEEE Access*, vol. 10, pp. 96602–96625, 2022.
- [16] T. E. T. Djaidja, B. Brik, A. Boulouache, S. M. Senouci, and Y. Ghamri-Doudane, "Federated learning for 5G and beyond, a blessing and a curse- an experimental study on intrusion detection systems," *Computers & Security*, vol. 139, p. 103707, 4 2024.
- [17] Z. Lin, G. Qu, X. Chen, and K. Huang, "Split Learning in 6G Edge Networks," 6 2023.
- [18] C. Thapa, M. A. Chamikara, and S. A. Camtepe, "Advancements of Federated Learning Towards Privacy Preservation: From Federated Learning to Split Learning," *Studies in Computational Intelligence*, vol. 965, pp. 79–109, 2021.
- [19] S. Sengupta, A. Chowdhary, A. Sabur, A. Alshamrani, D. Huang, and S. Kambhampati, "A Survey of Moving Target Defenses for Network Security," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 1909–1941, 7 2020.
- [20] Z. Zhou, C. Xu, X. Kuang, T. Zhang, and L. Sun, "An Efficient and Agile Spatio-Temporal Route Mutation Moving Target Defense Mechanism," *IEEE International Conference on Communications*, vol. 2019-May, 5 2019.
- [21] J. Gabirondo-Lopez, J. Egana, J. Miguel-Alonso, and R. Orduna Urrutia, "Towards Autonomous Defense of SDN Networks Using MuZero Based Intelligent Agents," *IEEE Access*, vol. 9, pp. 107184–107199, 2021.
- [22] T. A. Nguyen, M. Kim, J. Lee, D. Min, J. W. Lee, and D. Kim, "Performance evaluation of switch-over Moving Target Defence mechanisms in a Software Defined Networking using stochastic reward nets," *Journal of Network and Computer Applications*, vol. 199, p. 103267, 3 2022.
- [23] J. Tan, H. Jin, H. Zhang, Y. Zhang, D. Chang, X. Liu, and H. Zhang, "A survey: When moving target defense meets game theory," *Computer Science Review*, vol. 48, p. 100544, 2023.
- [24] C. Benzaid and T. Taleb, "ZSM Security: Threat Surface and Best Practices," *IEEE Network*, vol. 34, no. 3, pp. 124–133, 5 2020.
- [25] J. Ortiz, R. Sanchez-Iborra, J. B. Bernabe, A. Skarmeta, C. Benzaid, T. Taleb, P. Alemany, R. Muñoz, R. Vilalta, C. Gaber, J. P. Wary, D. Ayed, P. Bisson, M. Christopoulou, G. Xilouris, E. M. De Oca, G. Gür, G. Santinelli, V. Lefebvre, A. Pastor, and D. Lopez, "INSPIRE-5Gplus: Intelligent security and pervasive trust for 5G and beyond networks," *ACM International Conference Proceeding Series*, 8 2020.
- [26] ZSM, "GS ZSM 002 - V1.1.1 - Zero-touch network and Service Management (ZSM); Reference Architecture," 2019.
- [27] H. Chergui, A. Ksentini, L. Blanco, and C. Verikoukis, "Toward Zero-Touch Management and Orchestration of Massive Deployment of Network Slices in 6G," *IEEE Wireless Communications*, vol. 29, no. 1, pp. 86–93, 2 2022.
- [28] G. Carrozzo, M. S. Siddiqui, A. Betzler, J. Bonnet, G. M. Perez, A. Ramos, and T. Subramanya, "AI-driven zero-touch operations, security and trust in multi-operator 5G Networks: A conceptual architecture," *2020 European Conference on Networks and Communications, EuCNC 2020*, pp. 254–258, 6 2020.
- [29] D. Giannopoulos, G. Katsikas, K. Trantzas, D. Klonidis, C. Tranoris, S. Denazis, L. Gifre, P. Vilalta, P. Alemany, R. Muñoz, A. M. Bosneag, A. Mozo, A. Karamchandani, L. De La Cal, D. R. López, A. Pastor, and A. Burgaleta, "ACROSS: Automated zero-touch cross-layer provisioning framework for 5G and beyond vertical services," *2023 Joint European Conference on Networks and Communications and 6G Summit, EuCNC/6G Summit 2023*, pp. 735–740, 2023.
- [30] F. Naeem, M. Ali, and G. Kaddoum, "Federated-Learning-Empowered Semi-Supervised Active Learning Framework for Intrusion Detection in ZSM," *IEEE Communications Magazine*, vol. 61, no. 2, pp. 88–94, 2 2023.
- [31] G. Chollon, D. Ayed, R. A. Garriga, A. M. Zarca, A. Skarmeta, M. Christopoulou, W. Soussi, G. Gur, and U. Herzog, "ETSI ZSM Driven Security Management in Future Networks," *Proceedings - 2022 IEEE Future Networks World Forum, FNWF 2022*, pp. 334–339, 2022.
- [32] S. Jayasinghe, Y. Siriwardhana, P. Porabage, M. Liyanage, and M. Ylianttila, "Federated Learning based Anomaly Detection as an Enabler for Securing Network and Service Management Automation in Beyond 5G Networks," *2022 Joint European Conference on Networks and Communications and 6G Summit, EuCNC/6G Summit 2022*, pp. 345–350, 2022.
- [33] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," *2015 Military Communications and Information Systems Conference, MilCIS 2015 - Proceedings*, 12 2015.
- [34] S. Ben Saad, B. Brik, and A. Ksentini, "Toward Securing Federated Learning Against Poisoning Attacks in Zero Touch B5G Networks," *IEEE Transactions on Network and Service Management*, vol. 20, no. 2, pp. 1612–1624, 6 2023.
- [35] Y. Gao, M. Kim, S. Abuadba, Y. Kim, C. Thapa, K. Kim, S. A. Camtepe, H. Kim, and S. Nepal, "End-to-End Evaluation of Federated Learning and Split Learning for Internet of Things," *Proceedings of the IEEE Symposium on Reliable Distributed Systems*, vol. 2020-September, pp. 91–100, 3 2020.
- [36] H. Hafi, B. Brik, P. A. Frangoudis, A. Ksentini, and M. Bagaa, "Split Federated Learning for 6G Enabled-Networks: Requirements, Challenges, and Future Directions," *IEEE Access*, vol. 12, pp. 9890–9930, 2024.
- [37] H. Alavizadeh, D. S. Kim, and J. Jang-Jaccard, "Model-based evaluation of combinations of Shuffle and Diversity MTD techniques on the cloud," *Future Generation Computer Systems*, vol. 111, pp. 507–522, 10 2020.
- [38] N. M. Yungaicela-Naula, C. Vargas-Rosales, and J. A. Pérez-Díaz, "SDN/NFV-based framework for autonomous defense against slow-rate DDoS attacks by using reinforcement learning," *Future Generation Computer Systems*, vol. 149, pp. 637–649, 12 2023.
- [39] A. Javadpour, F. Ja'Fari, T. Taleb, and M. Shojafar, "A Cost-Effective MTD Approach for DDoS Attacks in Software-Defined Networks," *2022 IEEE Global Communications Conference, GLOBECOM 2022 - Proceedings*, pp. 4173–4178, 2022.
- [40] A. Javadpour, F. Ja'fari, T. Taleb, M. Shojafar, and B. Yang, "SCEMA: An SDN-Oriented Cost-Effective Edge-Based MTD Approach," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 667–682, 2023.
- [41] Y. Zhou, G. Cheng, S. Jiang, Y. Zhao, and Z. Chen, "Cost-effective moving target defense against DDoS attacks using trilateral game and multi-objective Markov decision processes," *Computers & Security*, vol. 97, p. 101976, 10 2020.
- [42] H. Wang, F. Li, and S. Chen, "Towards cost-effective moving target defense against DDoS and covert channel attacks," *MTD 2016 - Proceedings of the 2016 ACM Workshop on Moving Target Defense, co-located with CCS 2016*, pp. 15–25, 10 2016.
- [43] Y. Zhou, G. Cheng, S. Jiang, Y. Hu, Y. Zhao, and Z. Chen, "A Cost-effective Shuffling Method against DDoS Attacks using Moving Target Defense," *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 57–66, 3 2019.
- [44] W. Soussi, M. Christopoulou, G. Gur, and B. Stiller, "MERLINS - Moving Target Defense Enhanced with Deep-RL for NFV In-Depth Security," *2023 IEEE Conference on Network Function Virtualization and Software Defined Networks, NFV-SDN 2023 - Proceedings*, pp. 65–71, 2023.
- [45] W. Soussi, M. Christopoulou, G. Xilouris, and G. Gur, "Moving Target Defense as a Proactive Defense Element for beyond 5G," *IEEE Communications Standards Magazine*, vol. 5, no. 3, pp. 72–79, 9 2021.
- [46] P. Escalera, V. A. Cunha, D. Gomes, J. P. Barraca, and R. L. Aguiar, "Moving Target Defense for the cloud/edge Telco environments," *Internet of Things*, vol. 24, p. 100916, 12 2023.
- [47] Z. Abdelhay, Y. Bello, and A. Refaey, "Towards Zero-Trust 6GC: A Software Defined Perimeter Approach with Dynamic Moving Target Defense Mechanism," 12 2023.
- [48] N. P. Palma, S. N. Matheu-Garcia, A. M. Zarca, J. Ortiz, and A. Skarmeta, "Enhancing trust and liability assisted mechanisms for ZSM 5G architectures," *Proceedings - 2021 IEEE 4th 5G World Forum, 5GWF 2021*, pp. 362–367, 2021.
- [49] A. Alotaibi and A. Barnawi, "LightFIDS: Lightweight and Hierarchical Federated IDS for Massive IoT in 6G Network," *Arabian Journal for Science and Engineering*, pp. 1–17, 11 2023.
- [50] C. Thapa, P. C. M. Arachchige, S. Camtepe, and L. Sun, "SplitFed: When Federated Learning Meets Split Learning," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 36, no. 8, pp. 8485–8493, 6 2022.
- [51] X. Chen, J. Li, and C. Chakrabarti, "Communication and Computation Reduction for Split Learning using Asynchronous Training," *IEEE Workshop on Signal Processing Systems, SiPS: Design and Implementation*, vol. 2021-October, pp. 76–81, 7 2021.