Received 30 September 2023; accepted 6 March 2024. Date of publication 11 March 2024;
date of current version 4 April 2024. The review of this article was coordinated by Editor Yongdong Wu.

Digital Object Identifier 10.1109/OJVT.2024.3375448

ZSM-Based E2E Security Slice Management for DDoS Attack Protection in MEC-Enabled V2X Environments

RODRIGO ASENSIO-GARRIGA [1], POL ALEMANY [2], ALEJANDRO M. ZARCA [3], ROSHAN SEDAR [2] (Graduate Student Member, IEEE), CHARALAMPOS KALALAS [2] (Member, IEEE), JORDI ORTIZ [3], RICARD VILALTA [2] (Senior Member, IEEE), RAUL MUÑOZ [2] (Senior Member, IEEE), AND ANTONIO SKARMETA [1] (Senior Member, IEEE)

[1]Department of Information and Communications Engineering, University of Murcia, 30100 Murcia, Spain
[2]Centre Tecnològic de Telecomunicacions de Catalunya (CTTC/CERCA), 08860 Castelldefels, Spain
[3]University Center of Defense at the Spanish Air Force Academy, 30720 San Javier, Spain

CORRESPONDING AUTHOR: ALEJANDRO M. ZARCA (e-mail: alejandro.mzarca@cud.upct.es).

This work was supported in part by the ONOFRE-3 under Grant PID2020-112675RB-C44, funded by MCIN/AEI/10.13039/501100011033 and CERBERUS projects, in part by the RELAMPAGO under Grant PID2021-127916OB-I00 funded by MCIN/AEI/10.13039/501100011033, in part by the Department of Information and Communications Engineering (DIIC) of the University of Murcia in part by the "Ministerio de Asuntos Económicos y Transformación Digital " and the European Union-NextGenerationEU in the frameworks of the "Plan de Recuperación, Transformación y Resiliencia " and in part by the "Mecanismo de Recuperación y Resiliencia " under Grant TSI-063000-2021-36, TSI-063000-2021-39, Grant TSI-063000-2021-40, Grant TSI-063000-2021-41, Grant TSI-063000-2021-44, Grant TSI-063000-2021-45, and Grant TSI-063000-2021-62.

ABSTRACT Research on vehicle-to-everything (V2X) is attracting significant attention nowadays, driven by the recent advances in beyond-5G (B5G) networks and the multi-access edge computing (MEC) paradigm. However, the inherent heterogeneity of B5G combined with the security vulnerabilities of MEC infrastructure in dynamic V2X scenarios introduces unprecedented challenges. Efficient resource and security management in multi-domain V2X environments is vital, especially with the growing threat of distributed denial-of-service (DDoS) attacks against critical V2X services within MEC. Our approach employs the zero-touch network and service management (ZSM) standard, integrating autonomous security into end-to-end (E2E) slicing management. We consider an entire 5G network, including vehicular user equipment, radio access networks, MEC, and core components, in the presence of DDoS targeting V2X services. Our framework complies with security service-level agreements (SSLAs) and policies, autonomously deploying and interconnecting security sub-slices across domains. Security requirements are continuously monitored and, upon DDoS detection, our framework reacts with a coordinated E2E strategy. The strategy mitigates DDoS at the MEC and deploys countermeasures in neighboring domains. Performance assessment reveals effective DDoS detection and mitigation with low latency, aligned with the mission-critical nature of certain V2X services. This work is part of ETSI ZSM PoC "security SLA assurance in 5G network slices".

INDEX TERMS Zero-touch network and service management (ZSM), beyond-5G (B5G), vehicle-to-everything (V2X), security, automation, end-to-end (E2E) network slicing, multi-domain, MANO, RAN.

I. INTRODUCTION

A. BACKGROUND

Beyond-5G (B5G) networks are expected to natively integrate intelligent autonomous management of heterogeneous technologies and services. Autonomous management ensures the efficient administration of resources, both virtual and physical, tailored to the requirements of the supported services, the context, and the users. In this regard, network slicing constitutes a key innovation that isolates resources at different network domains, splitting the network into distinct logical segments. This opens up a wide range of possibilities, offering adapted support for autonomous coordination of the deployment of chained services with a multi-domain perspective, thus guaranteeing capabilities such as end-to-end (E2E) network slicing. The coordination of various B5G elements that compose an E2E network slice poses elevated merit when used in conjunction with multi-access edge computing (MEC) nodes, which allow the dynamic instantiation of key computing or network elements and services as close as possible to the user. Latency and traffic congestion gains can thus be attained while increasing the overall quality of service (QoS) and extending security capabilities via real-time task offloading [1].

In B5G networks, vehicle-to-everything (V2X) communication constitutes one of the most attractive verticals, empowered by the growing adoption of MEC-based solutions. Emerging V2X use cases are becoming especially complex given the ubiquitous mobility and criticality of the associated communication and services [2]. The deployment of such on-demand services heavily relies on MEC capabilities to fulfill the stringent V2X requirements in terms of latency and throughput. In this context, MEC nodes can directly benefit from autonomous dynamic management capabilities at the edge, which (i) allocate dedicated resources to ensure the correct deployment and operation of services; (ii) migrate these services seamlessly and with anticipation; (iii) offload the computational load (e.g., delegate computationally intensive functions) [3].

Inevitably, security becomes one of the major concerns, due to the inherent V2X vulnerabilities and breaches, with multi-faceted threat vectors which an adversary may maliciously exploit to intrude the system. On top of this, decentralized MEC deployments render the attack surface sufficiently large and may further exacerbate the V2X security risks. Among various attack types, Denial-of-Service (DoS) attacks constitute one of the salient threats against MEC infrastructure hosting V2X services [4]. In DoS attacks, an attacker tries to prevent legitimate users from accessing the network and services, causing traffic disruption which may destabilize the V2X system and threaten user safety. DoS attackers typically flood the network either with traffic of higher frequency than the system can handle or with high computational requests, resulting in an overload of computational resources. This inevitably causes extensive periods of service unavailability where legitimate users cannot be served. When such attacks are launched from multiple sources, often in spatially distant locations, this results in distributed DoS (DDoS) attack variants [5].

Current technologies that cooperate to offer advanced services with an E2E perspective, could also jointly serve to provide protection against certain DDoS attacks. However, for protecting the entire V2X attack surface, their potential becomes limited without intelligent orchestration engines. The orchestration layer is an essential element in ensuring system automation, abstracting the complexity of the coordination and management of technologies and domains (i.e., RAN, edge, cloud). Moreover, when orchestration processes are combined with (i) policy-based approaches, that provide flexibility in specifying requirements, and (ii) intelligent decision engines, the benefits of abstracting the complexity of the underlying technologies are highly leveraged, enabling B5G V2X use cases with highly diverse requirements in terms of QoS and security [6]. In line with policy-based approaches, it is of utmost importance to ensure that the right security level is properly applied based on the user requirements. Security Service-Level Agreements (SSLAs) [7] are thus employed for this aim, serving as a contract between the customer and the operator.

Recent advances in the areas of 5G, V2X communication and security are also driven by consistent standardization activities from relevant organizations (e.g., 3GPP, ITU, ETSI, and IEEE). Such standardization bodies also define specifications for key enabling technologies, such as Zero-touch network and Service Management (ZSM), E2E slicing, and MEC, to enhance automation and security in future networks [8], [9]. In particular, ZSM represents a visionary next-generation management system with the ultimate goal of achieving complete automation in all operational processes and tasks. These tasks include planning and design, delivery, deployment, provisioning, monitoring, and optimization, all of which are ideally executed without human intervention [10]. In addition, a growing number of standards-developing organizations steer their efforts towards integrating data-empowered solutions for V2X security. Over the next years, network operators are also expected to advance the implementation of automated E2E slicing management and security enforcement functionalities for V2X systems by adopting standards such as ZSM [11].

B. CONTRIBUTIONS

In this work, we demonstrate the feasibility of a ZSM-based framework to autonomously protect V2X services located in the MEC in a B5G infrastructure by effectively mitigating various DDoS attack types. The threefold contribution of this article can be summarized as follows:

- We perform autonomous and ZSM-compliant security management of a real B5G network and services through the deployment and enforcement of E2E B5G security slices. The management involves the dynamic reconfiguration of B5G components (i.e., RAN and V2X aggregator) in order to fulfill the SSLA.
- We incorporate security as a *native* element in the E2E ETSI slice management standard to autonomously manage the E2E B5G security slices, including the E2E logical coordination of different domains to deploy and interconnect per-domain security sub-slices.
- We utilize the V2X aggregator and gNBs as security enforcement points to mitigate DDoS attacks at two levels; firstly, where the attack is detected and, eventually, as close as possible to the source. Adversaries are banned from the domain under attack, while the mitigation countermeasure is shared with neighboring domains to avoid the propagation of malicious information.

To showcase the detection capabilities of our approach at the MEC, we integrate a data-driven DDoS attack detection methodology, originally introduced in [12], based on Reinforcement Learning (RL). By performing experiments using an open-source dataset, our framework is shown to be highly effective in detecting various DDoS attack variants while keeping detection latency at low levels. In line with ongoing standardization activities, our proposed framework has been recently part of the ZSM proof of concept entitled "security SLA assurance in 5G network slices" [13]. It can thus be considered an effective tool to gain meaningful insights into DDoS attack detection and respective mitigation practices/measures to trigger policy actions for V2X security.

C. ORGANIZATION

The material in this manuscript is organized as follows. Section II outlines the related work. Our proposed framework and associated security enablers are described in Section III. Section IV elaborates the working scenario under consideration. Performance outcomes pertaining to the evaluation of the proactive and reactive phases of our framework are presented in Section V. Finally, Section VI is reserved for conclusions.

II. RELATED WORK

A. SECURITY ISSUES FOR MEC-ENABLED V2X SERVICES

In related literature, V2X security has been the focus of attention for several years now, and the implications introduced by MEC-enabled V2X services have been studied by multiple groups. The authors in [14] provide a survey on MEC for V2X architectures, identifying the principal challenge of content delivery in task offloading, and proposing collaborative solutions to limit the induced delay when information required is not cached at the edge servers. Detailed studies of security threats, vulnerabilities, and countermeasures for various MEC-based 5G verticals are presented in [15], [16]. In particular, peculiar MEC characteristics such as network function virtualization, nascent and decentralized deployments, and limited computational capabilities of MEC nodes are highlighted as vulnerable entry points that undermine system security. In addition, ETSI has been involved in standardizing MEC security with various security proposals for MEC applications, such as application programming interfaces over HTTPS with encrypted traffic, application-level authentication and authorization, and use of trusted computing modules [17].

The use of data-driven approaches to secure MEC deployments is also gaining remarkable research interest. In an effort to minimize the risk of eavesdropping in MEC environments, the authors in [18] devise a deep RL algorithm for adaptive computation offloading. In a similar context, a MEC-based intrusion detection scheme is proposed in [19], which comprises deep learning engines for handling malicious vehicular traffic. In our work, the MEC vulnerabilities identified in previous studies are considered in the form of DDoS attack realizations targeting V2X services available at the edge. Our developed security enablers are dynamically deployed at the MEC level, to efficiently detect and react with countermeasure policies against DDoS attack variants in highly volatile V2X environments.

B. ORCHESTRATION

Orchestration forms the basis for zero-touch management of security, services, and infrastructure. The pervasive integration with Artificial Intelligence (AI) engines of agile and self-dynamic capabilities, is expected to increase the level of security management automation towards real-time zero-touch orchestration across multiple domains.

In this regard, the authors in [8] compile relevant AI-based methods applied to orchestration processes (e.g., radio resources or E2E slicing). However, even though network security aspects are discussed, their interrelation with security orchestration is not explored. In [20], convolutional neural networks and genetic algorithms are leveraged to achieve low latency in V2X services migration and to optimize resource utilization. To achieve this, a measurement of pre-established QoS violations with respect to migrated services is performed. The proposed proactive service-migration strategy could be further improved if security was directly applied in the migrated services and the pre-established SSLAs were monitored. In [21], the authors emphasize the importance of effective security modeling, allowing security to be interpreted and interoperated transparently between different parts of the system. The need to have systems capable of reacting to dynamic security environments is also highlighted. In RAN orchestration, C-RAN and O-RAN paradigms have triggered the attention of multiple research groups that leverage orchestration to optimize RAN flexibility [22], [23], [24]. Although some works cover security aspects in the RAN domain, their focus predominantly resides on architectural guidelines [25], [26]. Thus, the potential of utilizing RAN as an enforcement point to apply countermeasures directly on UEs remains rather unexplored.

Even though several works in relevant literature integrate orchestration with AI engines, the complexity of B5G network management requires enhanced modules in charge of providing flexibility, monitoring, and human-in-the-loop [27]. In this context, the ZSM concept has been postulated as an architecture that aims to address such concerns, by providing intent-based E2E management of services and infrastructure, and by abstracting the complexity of underlying domains and technologies through the use of policies. However, increasing the level of management automation comes inadvertently with security risks and compelling attack surfaces that can be exploited for malicious purposes. An in-depth study on ZSM specifications is performed in [28], and the set of security threats introduced by the adoption of ZSM is presented. Key challenges associated with the integration of AI engines in ZSM-based architectures are also discussed in [29]. Although the importance of security is underlined in both surveys, the majority of compiled works focus on E2E slice provisioning and network management; on the contrary, aspects related to security management are often overlooked or neglected. Applicability in V2X scenarios is also not adequately addressed.

Aiming to fill these gaps, we introduce a ZSM-based framework, focusing on security provisioning as the main concern when deploying E2E slices. Security is modeled as an SSLA which is continuously monitored by specialized agents. When a threat or violation is detected, the framework is capable of autonomously enforcing countermeasures, not only in the domain where the threat is detected but also in other potentially affected domains.

C. ADDRESSING DDOS ATTACKS IN MEC-ENABLED V2X SYSTEMS

Given the limited computational resources of MEC nodes, DDoS attacks constitute severe threats as they could shut down or destabilize the entire V2X system and pose perils to V2X user safety [2]. Mature security techniques, such as firewalls to control data traffic and intrusion detection systems, can be applied to the MEC to mitigate DDoS attacks and protect V2X services [30]. However, such approaches may fall short in detecting unknown (i.e., zero-day) DDoS variants and/or in dealing with non-anticipated variability in the malicious behavior of adversaries. Thus, their applicability may be limited to only traditional DDoS vectors. The authors in [31] introduce a hybrid trust establishment scheme to prevent DDoS attacks and eliminate misbehaving vehicles in a distributed manner. Even though accurate detection could be attained, a malicious stealthy attacker may bypass the proposed detection scheme by manipulating trust values, and remain undetected. Various supervised learning algorithms are considered in [32] for DoS/DDoS detection and localization. Although high-accuracy outcomes are attained, such approaches may be impractical in real-time V2X scenarios, as the training and detection of labeled data do not work well when attacks change dynamically. In this context, RL methods can be further explored for context-aware V2X security, by learning new V2X threats and attacks in rapidly changing environments.

A feature-adaption RL approach is proposed in [33], accounting for the spatiotemporal traffic regularities to address unknown DDoS attacks with unlabeled data and limited prior knowledge. However, the enhanced detection comes at the expense of increased time and memory consumption, which may render the scheme insufficient in safety-critical V2X scenarios. In [34], a DDoS attacker could take advantage of automated orchestration procedures by flooding the MEC nodes with task-offloading requests. The authors propose two main actions to mitigate the DDoS attack: (i) maintain a trust score for vehicles connected to the network in order to accept/reject the request; (ii) perform resource orchestration among other available MEC nodes to alleviate overloaded nodes. Although the proposed methodology is shown to be effective in mitigating edge DDoS attacks, it may be susceptible to trust manipulation. In addition, the assumed threat model takes the form of fake service requests by malicious vehicles with variable duration; alternatively, our work considers a broader set of DDoS attack types, where a combination of multiple attacks may occur at once. We further perform attack mitigation as an E2E reaction, where malicious traffic is first prevented from reaching the V2X service and, once the adversary has been identified, radio-level network management ensures proper utilization of radio resources.

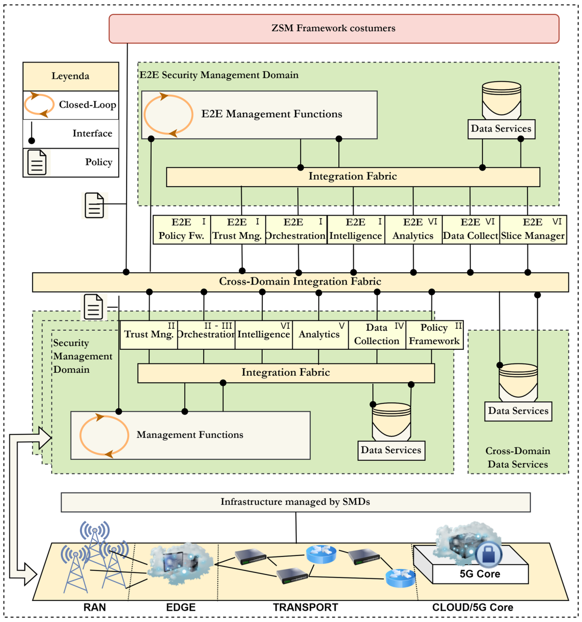


FIGURE 1. ZSM-based architecture of the proposed framework. The Roman numerals on the top right of each entity of the architecture denote the step of the closed loop in which they participate.

III. SECURITY FRAMEWORK OVERVIEW

Our developed framework has adopted the ETSI ZSM architecture, aiming to address the pivotal challenges that network operators and service providers face in heterogeneous V2X environments nowadays. The holistic approach of ZSM to network and service management offers a unified solution that embraces an E2E perspective, ensuring seamless integration of emerging technologies while preserving efficiency and QoS. By using this standardized reference architecture, our security framework not only accelerates the deployment of innovative V2X services but also enhances operational efficiency, minimizes downtime, and improves end-user experience.

The following subsections present our proposed autonomous and technology-agnostic ZSM-based security framework, and the specialized security enablers developed for V2X attack detection, mitigation, and management of 5G components.

A. ZSM-BASED INSPIRE-5GPLUS ARCHITECTURE

Fig. 1 illustrates the framework that was developed in the context of the European INSPIRE-5Gplus project[1] [35]. The framework leverages the innovative ETSI ZSM architecture [36] to support autonomous security and service management features for B5G networks. As shown in Fig. 1,

[1] [Online]. Available: https://www.inspire-5gplus.eu/

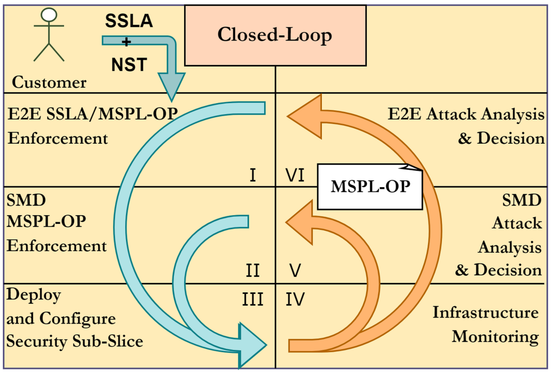

Customer
SSLA
+
NST
Closed-Loop
E2E SSLA/MSPL-OP Enforcement
E2E Attack Analysis & Decision
I
VI
MSPL-OP
SMD MSPL-OP Enforcement
SMD Attack Analysis & Decision
II
V
III
IV
Deploy and Configure Security Sub-Slice
Infrastructure Monitoring

FIGURE 2. Autonomous ZSM-based closed-loop phases.

the framework consists of an E2E Security Management Domain (SMD) and as many independent SMDs as required to manage the underlying physical infrastructure. Although the design is hierarchical, each of these independent SMDs is capable of autonomously managing resources through closed-loop processes such as self-* (observation, analysis, and decision-making). The E2E SMD performs the synchronization of multi-domain tasks. The different steps of the E2E and intra-domain closed loops are explained in the following subsection.

B. SECURITY FRAMEWORK DATA OBJECTS & CLOSED LOOP

In ZSM-based architectures, zero-touch automation is driven by closed loops of different levels. As shown in Fig. 2, the closed loop involves a set of recurring logical steps that enable autonomous management of the infrastructure using policy languages or SLAs.[2] Our framework employs the closed-loop concept to provide autonomous security management through the enforcement and maintenance of SSLAs.

1) DATA OBJECTS

For the closed-loop-driven deployment and management of 5G E2E security slices, the following set of descriptors is defined:

- The SSLA prescribes the set of security capabilities that the end user and service provider agreed to be monitored and ensured. In general, an SSLA is composed of (i) capabilities that define the security threat to be checked (i.e., DDoS protection); (ii) Security Level Objectives (SLOs), that refer to the conceptual objective to verify whether there exists an attack or not (e.g., number of received requests per minute); and (iii) metrics that represent the specific values used as a threshold/objective. An SSLA may have multiple capabilities, with each one focused on a specific threat.
- The Network Slice Template (NST) contains a set of pre-defined service resources along with their logical interconnection. Thus, NSTs aim to fulfill the network resources specification required to deploy the requested services. Each NST may be deployed multiple times with different security and service requirements; for this reason, the NST is a static data object and each associated deployment information is stored in a Network Slice Instance (NSI). An NSI is the data object created to store the information (e.g., domains, characteristics, links) related to the resources (i.e., networking and computing instances) used in a network slice.
- The Medium-level Security Policy Language for Orchestration (MSPL-OP) is the common internal data object model that is used to transform the received secured slice requirements (SSLA + NST) in a homogenized format among the Security Orchestrators (SOs) (E2E and SMD). It has been extended to model E2E B5G security slices as well as sub-slices for each involved SMD.

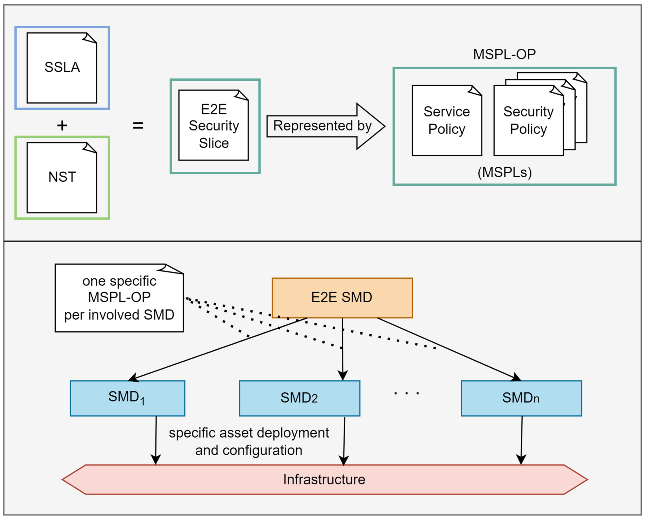


FIGURE 3. E2E policy management.

These three data objects are used by specific components within our framework. The NST and the SSLA are used to interpret which service and security resources are required. As depicted in Fig. 3, at the E2E domain, the combination of the NST and the SSLA allows the creation of the MSPL-OPs used by the E2E SO to orchestrate and distribute multiple actions in the form of MSPL-OP. Such actions need to be managed by each domain SO in order to deploy an E2E B5G security slice. Moreover, the MSPL-OPs delivered to each involved domain will be eventually translated via their Policy Framework (PF) into final asset configurations. Indeed, the same policy could be translated into different asset configurations depending on the domain infrastructure capabilities.

2) CLOSED-LOOP PHASES

The closed-loop of our security framework consists of a *proactive* and a *reactive* phase. In particular, the proactive phase entails the following consecutive steps:

[2] Their specificity can be properly adjusted depending on the point of the closed loop.

1) The framework receives the SSLA and the NST defining the customer's service and security requirements. This information is processed by the E2E SO and, with the aid of other modules, the most suitable domains are selected to enforce the request. Then, a particular MSPL-OP for each of the selected domains is generated and forwarded, which jointly form an E2E security slice.
2) The SO of each SMD orchestrates the received MSPL-OP by selecting the most trustable assets and configurations that can fulfill the corresponding part of the SSLA. The MSPL-OP translation is performed via the PF.
3) The SO, once the policy has been translated into specific asset configurations, selects the Management and Network Orchestration (MANO) available in the domain to deploy the slice containing the selected assets. When the instantiation has been completed,[3] the SO applies the inferred configuration to the assets.

On the other hand, the reactive phase entails the following consecutive steps:

4) Every security requirement specified in the SSLA has one or more associated monitoring probes, that are configured to extract data from the infrastructure related to the SSLA compliance.
5) Extracted data is analyzed and correlated with other infrastructure information. As a result, anomaly detection can be performed, by identifying potential threats and raising alerts to the Decision Engine. In turn, the Decision Engine generates an MSPL-OP that acts as a local countermeasure.
6) If needed, the SMD Decision Engine can escalate the alert to the E2E Decision Engine for further collaboration with other domains in order to jointly mitigate the threat. The E2E Decision Engine generates and forwards an MSPL-OP to the E2E SO which, in turn, initiates the proactive phase of the closed-loop.

C. SECURITY ENABLERS

The security enablers represent the enforcement points of the MSPL-OPs. More specifically, they constitute a set of assets deployed and configured to provide security capabilities, according to the requirements specified by the policies. Security enablers are characterized by a trust value that is dynamically updated depending on their performance. The framework makes use of such trust values to perform trust-based E2E slice orchestration. For the protection of MEC infrastructure against DDoS attacks in V2X scenarios, the following security enablers have been developed and integrated into our framework.

1) V2X AGGREGATOR

The V2X aggregator performs the fusion of vehicular traffic traces at the level of a roadside unit (RSU). RSUs are part of the MEC infrastructure, acting as gateways between the vehicular on-board units and the deployed gNBs. Vehicular traffic, in the form of basic safety messages (BSMs), is streamed from the data plane using 5G vehicular UEs (V-UEs). The V2X data streams are based on an open-source vehicular anomaly-detection dataset (VeReMi [37]). The information contained in each BSM is constantly evolving over time along the vehicle trajectory, while BSMs from neighboring vehicles exhibit high spatial dependency.

2) V2X DDOS DETECTOR

Existing V2X DDoS detection techniques are not designed to dynamically improve their detection performance according to evolving attack patterns in rapidly changing V2X environments. In addition, detection methods relying on anomaly scores or reputation assessment criteria may be applicable only to limited V2X scenarios. To this end, RL is leveraged to consistently improve detection experience over time while interacting with unknown V2X environments. This can be achieved by exploiting the intrinsic temporal and spatial interdependencies of BSMs to detect abnormal DDoS patterns.

Our RL-based DDoS detector, originally introduced in [12], is considered to be deployed in an RSU, acting as an *agent* that interacts with the V2X environment to learn the optimal detection *policy*. The incoming V2X traffic traces are sequentially analyzed based on the mobility patterns of vehicles (i.e., position, velocity, and acceleration) to instruct the RL algorithm for the detection of DDoS patterns. The agent is given a positive reward for correctly identifying the DDoS attack (i.e., true positive) or a normal state (i.e., true negative); otherwise, a negative reward is given to the agent for incorrect identification of a normal state as a DDoS attack (i.e., false positive), or of a DDoS attack as a normal state (i.e., false negative).

3) V2X FILTERING ASSET

Since in DDoS attacks, the BSMs are transmitted at a frequency higher than the limit set by the V2X standard[4], the policy that will be formed to configure the asset will have as its main parameter the inter-arrival BSM time threshold. Upon detection of a DDoS attack, interaction is sought with the SOs to apply the newly formed security policy (i.e., DDoS traffic to be isolated and blocked). In particular, the reactive security policy takes the form of IP traffic filtering of the aggregated DDoS messages at the RSU.

4) 5G CORE & RAN SECURITY AGENTS

Our developed 5G Core (5GC) and RAN security agents enable the enforcement of security policies through the application of determined operations at the 5GC and 5G radio infrastructure (e.g., deploy, re-deploy, start/stop services). Besides, they enable the extraction of useful data on-demand, through the monitoring capabilities of the agents

[3] In case the asset was already instantiated, reconfiguration is also possible.

[4] Frequency threshold values depend on the considered V2X service [38].

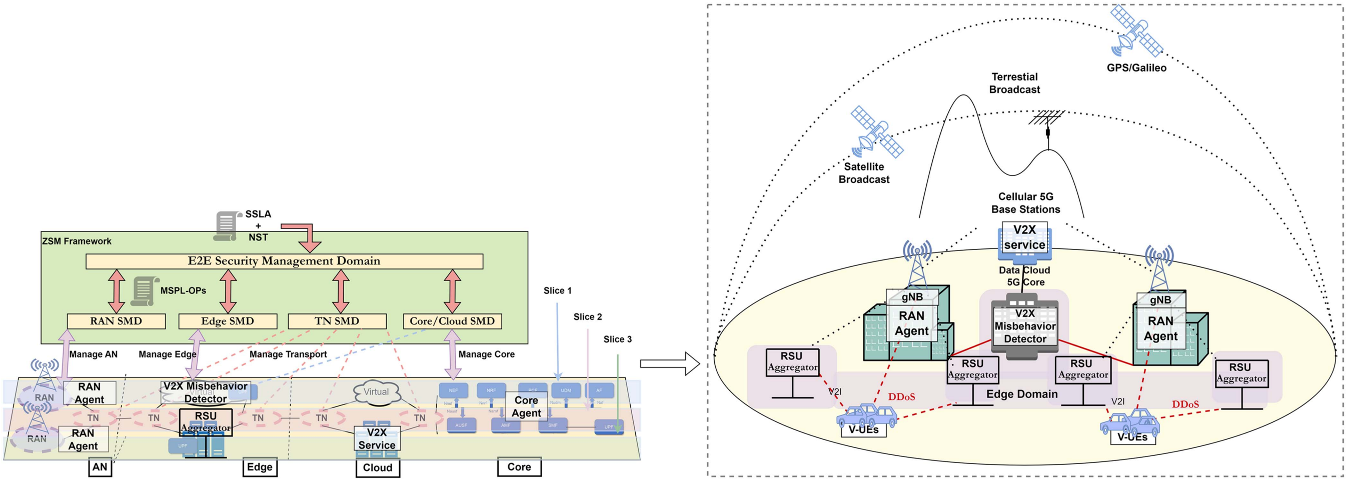


FIGURE 4. ZSM-managed B5G V2X working scenario.

(e.g., get_info operations). Both agents are interconnected as they belong to the same 5G system, and they can exchange information to perform a 5G operation (e.g., new AMF registration). The 5G radio agent provides compatibility with the Amarisoft web socket. Thus, we have implemented a driver to manage the Amarisoft agent dynamically and autonomously. During the enforcement process, the RAN driver evaluates if further exchange of information is required, and whether it can be extracted from another 5G component (e.g., 5GC agent). The 5GC agent is used to retrieve information from the 5GC to enforce or generate policies. For instance, the 5GC agent will retrieve RAN V-UEs specific information by using the IP address to learn the IMSI (from SMF), GUTI from IMSI (from AMF), ID mapping from GUTI, ranuengapID from ID mapping and, finally, the RAN UE ID according to the previously retrieved information. Once the RAN UE ID is acquired, it is possible to request different operations to the 5G RAN for the specific V-UEs. In this case, a handover process to move the malicious V-UEs from the current cell to another with specific restrictions (e.g., upload-link disabled).

IV. WORKING SCENARIO

The scenario under consideration is illustrated in Fig. 4. An E2E B5G security slice is deployed to protect in real-time critical V2X services located at the MEC. The goal resides in preventing the propagation of DDoS attacks that aim to destabilize the system and drain the scarce resources of the MEC. In detail, our scenario comprises (i) dense gNB deployment, to provide a more dedicated service to the same amount of V-UEs; (ii) deployment of RSUs, to support specific vehicular tasks; (iii) MEC nodes, to delegate computational load (e.g., security tasks); and (iv) ZSM-based management of the B5G network that allows the autonomous (re-)instantiation and (re-)configuration of chained services in the form of E2E slice.

Two differentiated phases compose the closed-loop: (i) the *proactive* phase, in which an SSLA with associated NST is requested to be deployed to the ZSM-based framework, and it is translated into an MSPL-OP that will be distributed to the required domains to deploy an E2E security slice; and (ii) the *reactive* phase, which ensures the compliance of the SSLA at any time, mitigating DDoS attacks that compromise the SSLA with an E2E perspective. In particular, we use (i) the V2X filtering asset at the RSU to prevent DDoS traffic from being processed in the V2X aggregator; and (ii) the gNB to penalize malicious V-UEs connected to 5G network, by banning them from the regular radio cell, and then propagate their ban to neighboring cells. The V-UEs are represented by virtual machines connected to an SDR which uses a 5G Amarisoft Simbox radio stack to establish a 5G standalone connection to the gNB.

A. SECURITY SLICE DEPLOYMENT & CONFIGURATION

Fig. 5 shows both proactive and reactive automated workflows. To deploy the V2X services and security slice in the proactive phase, the customer (e.g., V2X service provider) first requests a service based on a set of service and security requirements modeled into an E2E NST and an SSLA (Fig. 5 step 1). Then, the Network Slice Manager (Slice Manager) generates an MSPL-OP by inferring the service from the E2E NST, and the security capabilities from the SSLA (Fig. 5 step 2). Once the policy is ready, the Slice Manager requests the enforcement of the MSPL-OP to the E2E SO (Fig. 5 step 3), which, as part of the orchestration plan, will generate an MSPL-OP per domain to assess the enforcement (Fig. 5 step 4).

The E2E SO requests the slice policy enforcement to the SO deployed in the domain (CTTC SMD) with V2X capabilities (Fig. 5 step 5). The SO retrieves different types of information to prepare the orchestration plan, e.g., trust values (Fig. 5 step 6). In this case, the SO generates a trust-based orchestration plan (Fig. 5 step 7). Once the plan is ready, the SO requests MSPL-OP translations to the PF in order to retrieve the required configurations for those enablers/assets selected during the orchestration plan (Fig. 5 step 8). Since the slice will be composed of a V2X service and a V2X DDoS detector,

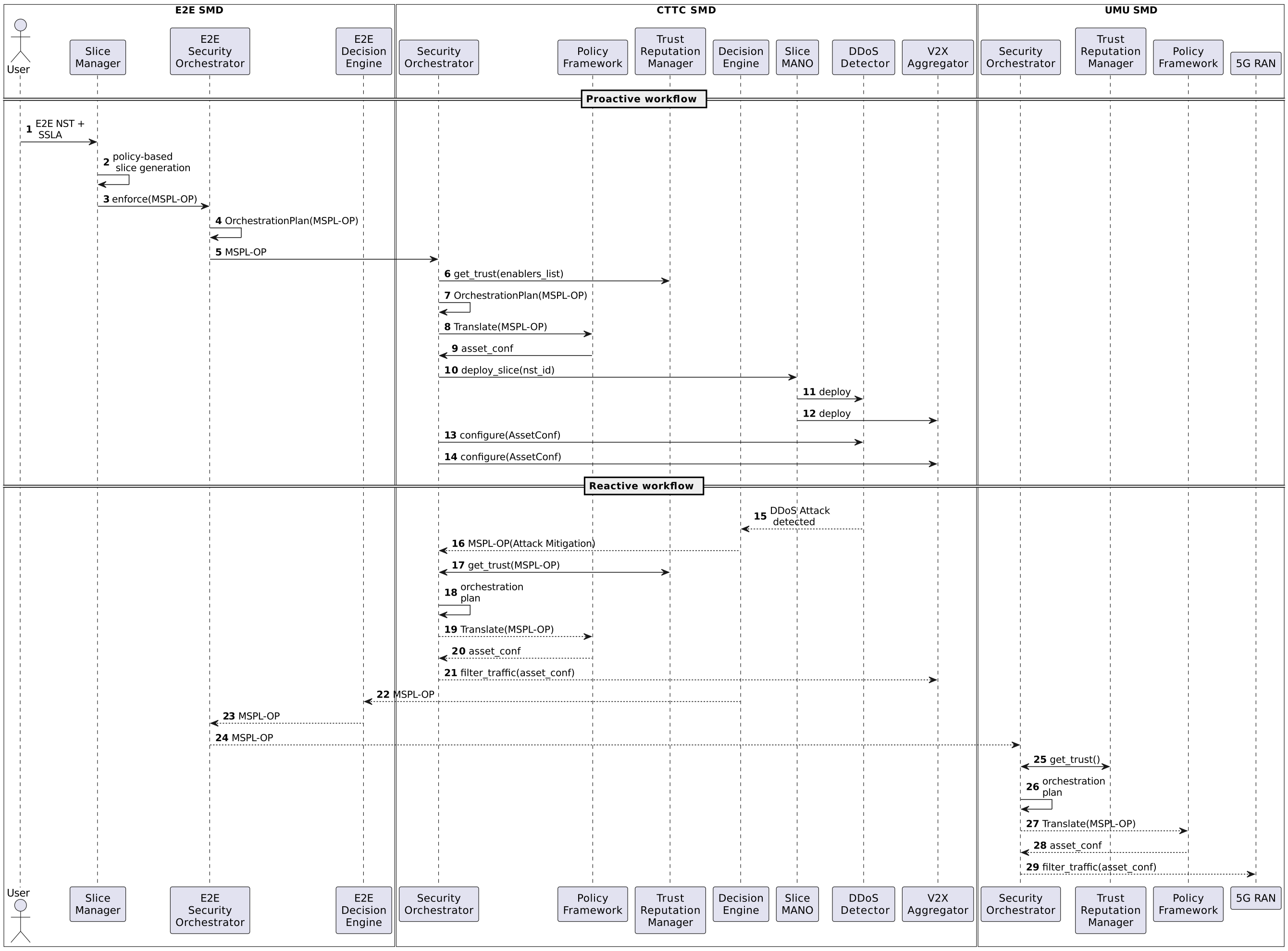


FIGURE 5. ZSM-based proactive E2E security slice deployment and reactive trust-based mitigation across multiple domains.

the SO receives V2X aggregator (service) and DDoS detector configurations (Fig. 5 step 9). As part of the orchestration plan, the specific slice template is identified. This value is used to request the 5G slice deployment to the slice MANO (Fig. 5 step 10). Then, the V2X aggregator and DDoS detector are both deployed as part of the 5G slice (Fig. 5 steps 11–12). Finally, the SO configures both the V2X aggregator and DDoS detector according to the retrieved configurations during the translation stage (Fig. 5 steps 13–14).

B. AUTOMATED SECURITY THREAT REACTION

Fig. 5 also shows the detailed workflow for the automated reaction. In the reactive phase, the DDoS detector first detects the DDoS attack and notifies the Decision Engine (DE) (Fig. 5 step 15). In turn, the DE generates reactive security policies (filtering) and sends the reactive MSPL-OP to the SO (Fig. 5 step 16). The SO retrieves different types of information to prepare the orchestration plan, e.g., trust values (Fig. 5 step 17), generates the orchestration plan (Fig. 5 step 18) and requests MSPL-OP translations to the PF for those enablers/assets selected according to the orchestration plan (Fig. 5 step 19–20). In CTTC SMD, the V2X aggregator provides filtering capabilities, with the aid of the inter-arrival BSM time threshold, as discussed in Section III-C3. Then, the SO enforces the configurations in the V2X filtering asset (Fig. 5 step 21).

In parallel, the DE notifies the reaction to the E2E DE (Fig. 5 step 22), which, in turn, generates new reactive security policies for other SMDs that could also be affected or used as a mitigation point, and requests the E2E policy enforcement to the E2E SO (Fig. 5 step 23). The E2E SO requests the security policy enforcement in the affected SMD (in our scenario, the UMU SMD) in order to apply the same countermeasure, i.e., filter the malicious DDoS traffic, also in that domain (Fig. 5 step 24). The SO deployed in UMU retrieves different types of information to prepare the orchestration plan, e.g., trust values (Fig. 5 step 25), generates the trust-based orchestration plan (Fig. 5 step 26) and requests MSPL-OP translations from the PF for those enablers/assets selected according to the orchestration plan in UMU SMD (Fig. 5 steps 27–28). In this case, the 5G RAN agent is selected. Finally, the SO reconfigures the 5G RAN to filter the DDoS traffic by isolating the malicious V-UE and triggering a handover of the V-UE to an uplink-disabled cell (Fig. 5 step 29).

C. USE CASE DESCRIPTION

In order to evaluate the proposed solution, a V2X use case was defined, implemented, and evaluated. In particular, the E2E SMD and an SMD were implemented in the CTTC laboratory and another SMD in the UMU laboratory. The use case involves the deployment of a 5G service for a V2X scenario, with a 5GC, 5G RAN, 5G security agents (UMU SMD), and a set of V2X security enablers in the edge domain (CTTC SMD) to protect the V-UEs, the RSUs and the V2X service from DDoS attacks. The deployment and configuration of the 5GC and RAN are considered out of the scope of this work. As discussed in Section III-C, the V2X security enablers of the scenario aim at detecting and mitigating different types of DDoS attacks originated by malicious V-UEs in different domains (RAN and edge). Once the attack is detected, a policy is applied to filter the traffic generated by malicious V-UEs.

To generate the set of multiple DDoS attacks, the VeReMi dataset [37] was used in the evaluation phase. The VeReMi dataset comprises the following DDoS attack variants:

1) *DDoS attack:* Malicious V-UEs transmit BSMs at a higher frequency than the acceptable limit set by the standard specifications. The frequency threshold considered in this work is 4 Hz, which is equivalent to an inter-arrival BSM time threshold of 250 ms.
2) *DDoS Random attack:* In this attack, malicious V-UEs set all BSM fields to random values and perform a typical DDoS attack.
3) *DDoS Disruptive attack:* The malicious V-UEs may re-transmit previously transmitted BSMs by other legitimate V-UEs, with the intention of disrupting genuine information from being propagated.
4) *DDoS Random Sybil attack:* The malicious V-UEs change pseudonym identities on every transmitted BSM while performing the DDoS random attack.
5) *DDoS Disruptive Sybil attack:* In this attack, the malicious V-UEs change pseudonyms on every re-transmission of previously received BSMs while performing the DDoS disruptive attack.

V. PERFORMANCE EVALUATION

The evaluation of the proposed framework has been conducted with the aid of several experiments, including both proactive and reactive phases. The proactive phase is validated through the definition of an SSLA and an NST, which requests a V2X service with several security requirements. The ZSM-based framework autonomously deploys and/or configures different assets in order to fulfill the SSLA. The deployments form part of a common E2E B5G security slice, involving multiple SMDs (UMU and CTTC). The evaluation of the proactive phase reflects the different times consumed by each process (Section V-A) at the CTTC domain, for the deployment and configuration of V2X security enablers. On the other hand, the reactive stage is validated through the susceptibility of the framework to the different DDoS attack variants, evaluating for each case the DDoS detection performance (Section V-B). When an attack that compromises an SSLA requirement is detected, the framework raises an alert and ensures, via mitigation security policies, compliance with the SSLA. In order to tackle the threat, mitigation policies are generated both locally and at the E2E level. The evaluation of the reactive phase indicates the time elapsed for the local and E2E processes to mitigate the alert (Section V-C).

A. SECURED V2X SLICE DEPLOYMENT PERFORMANCE

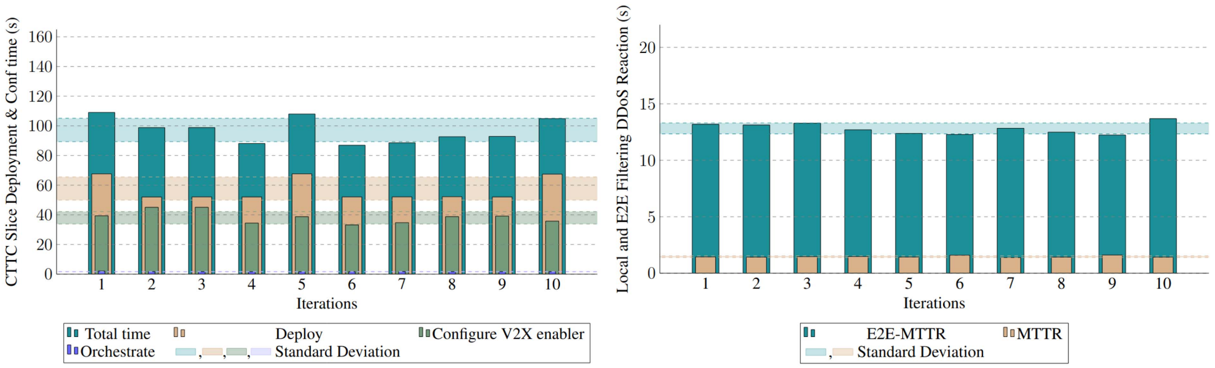
The initial deployment time is an indicator of how long the framework takes from the time the CTTC SMD receives the MSPL-OP until the sub-slice is deployed and configured, and thus the service is ready to be used with all requested capabilities. The distribution of the time consumed by the different processes with respect to the total time can be seen in Fig. 6(a), where the total time has an average of 97.42 s, the deployment represents a 59% of the time with 57.73 s, the configuration of the V2X DDoS detector 38.99% with 37.99 s and the orchestration 1.75% with 1.84 s in average. The orchestration time mainly joins the time spent on the translation (0.17 s avg.) and creation of the enforcement plan (0.97 s avg.) in addition to the load of the different managers and structures. The E2E time is omitted since the other domains do not contain specific V2X enablers. Indeed, the time spent by the E2E SMD is less than 1.8 s on average for constructing all the required MSPL-OPs.

B. DDOS DETECTION PERFORMANCE

In order to evaluate the detection performance of our framework, experiments were performed using the VeReMi dataset with the aid of multiple assessment metrics. Our selected performance indicators are defined as follows:

- Accuracy: The ratio of all correct predictions (i.e., true positives and true negatives) to the total number of considered input samples.
- Precision: The ratio of true positives to the number of true positives plus the number of false positives.
- Recall: The ratio of true positives to the number of true positives plus the number of false negatives.
- F2-score: The weighted harmonic mean between precision and recall metrics. The F2-score weights recall higher than precision,[5] to account for the higher importance of false negatives compared to false positives in safety-threatening V2X scenarios.
- False Positive Rate (FPR): The rate at which a legitimate vehicular behavior is identified as malicious.
- False Negative Rate (FNR): The rate at which a malicious vehicular behavior is identified as legitimate.
- Mean Time to Detect (MTTD): The average time elapsed between the time the DDoS attack takes place and its discovery by the V2X DDoS detector.
- Mean Time to Resolve (MTTR): The average time elapsed between the time the DDoS attack is detected

[5] In contrast, the traditional F1-score weights equally both recall and precision.



(a)

(b)

FIGURE 6. **(a) Proactive ZSM-based E2E B5G security slice deployment (b) Reactive ZSM-aligned trust-based multi-domain mitigation.**

TABLE 1 **Detection Performance Per DDoS Attack Variant**

Attack type	Accuracy (%)	Precision (%)	Recall (%)	F2 (%)	FPR (%)	FNR (%)	MTTD (ms)	MTTR (s)
DDoS	98.90	99.41	98.72	98.86	1.16	1.40	4.2	1.48
DDoS Random	99.78	99.88	99.66	99.70	0.42	0.45		
DDoS Disruptive	97.96	99.01	96.96	97.36	1.23	3.17		
DDoS Random Sybil	94.76	94.68	94.25	94.34	5.03	5.90		
DDoS Disruptive Sybil	92.94	92.98	92.14	92.31	6.57	8.02		

and the enforcement of the mitigation (filtering) policy by the SO.

Table 1 demonstrates the detection performance per DDoS variant, as defined in Section IV-C. Results show that RL-based detection is performed effectively, with an F2-score superior to 92.5% for all five DDoS attack types. Notably, the achieved precision and recall values demonstrate the ability of our detector to accurately differentiate DDoS attack messages from genuine behavior. It can also be observed that when DDoS attacks are launched in Sybil mode, detection performance registers a decline with increased FPR and FNR, albeit not at prohibitive levels. The reported MTTD on average across all DDoS attacks, is in the order of 4 ms, which is effective for many road safety applications, as BSMs usually broadcast with frequency of 1–10 Hz [38]. Such low detection latency levels corroborate the real-time capabilities of our V2X DDoS detector.

C. LOCAL AND E2E REACTION PERFORMANCE

The E2E reaction performance refers to the time elapsed since the alert of the DDoS attack is triggered until the framework has mitigated the attack, both at the local domain by the V2X filtering asset, and at the E2E level by banning the V-UEs from the cells. As shown in Table 1 and Fig. 6(b), the local mitigation time (MTTR) has an average of 1.48 s, which includes the mitigation security policy creation and the enforcement via reconfiguration of the V2X aggregator. Such value is considered acceptable for mitigating the detrimental effects on road users and avoiding the propagation of safety-threatening incorrect information by malicious V-UEs. The E2E reaction time (E2E MTTR) has an average value of 12.82 s which includes (i) the escalation of the alert to the E2E SMD, (ii) the E2E orchestration (creation of the MSPL-OP for the UMU domain), (iii) the extraction of the required information at the UMU domain for the malicious V-UE from the 5GC (as explained in Section III-C4), and (iv) the 5G RAN reconfiguration enforcement to ban the malicious V-UE. Both reactions are executed in parallel, thus the total time is equal to the E2E MTTR.

VI. CONCLUSION

This work demonstrates the feasibility of a ZSM-based security framework to manage the complex V2X characteristics in B5G networks. Our approach reveals how the benefits of policy flexibility are leveraged to deploy slices for V2X services with security requirements and an E2E perspective. Such autonomous management of V2X services, driven by a policy-based closed-loop, allows adaptation to the complex and highly dynamic V2X security landscape. Our proposed framework ensures automated reaction to security attacks, not only in the domain where the attacks are launched but also in other domains that could be affected or used to mitigate the attack more efficiently. We assessed the detection capabilities of our framework in the presence of different DDoS attack variants launched by multiple V-UEs in a multi-domain V2X scenario. Performance evaluation demonstrated that DDoS attacks can be effectively detected and contained with relatively low latency levels.

In the path forward, we will focus on extending the ZSM architecture with infrastructure and service-sharing capabilities, enabling collaboration between large and small stakeholders, as well as integrating blockchain into decision and enforcement processes as an ancillary layer of security. We will also direct our efforts towards incorporating trust of RSU components into collaborative DDoS detection, by leveraging the real-time capabilities of our framework. Finally, the integration of additional attack types from the VeReMi dataset will also be part of our study.

REFERENCES

[1] A. Virdis, G. Nardini, G. Stea, and D. Sabella, "End-to-end performance evaluation of MEC deployments in 5G scenarios," *J. Sensor Actuator Netw.*, vol. 9, no. 4, Dec. 2020, Art. no. 57.

[2] R. Sedar, C. Kalalas, F. Vázquez-Gallego, L. Alonso, and J. Alonso-Zarate, "A comprehensive survey of V2X cybersecurity mechanisms and future research paths," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 325–391, 2023.

[3] M. C. Lucas-Estan et al., "On the scalability of the 5G RAN to support advanced V2X services," in *Proc. IEEE Veh. Netw. Conf.*, 2020, pp. 1–4.

[4] A. Ghosal and M. Conti, "Security issues and challenges in V2X: A survey," *Comput. Netw.*, vol. 169, Jan. 2020, Art. no. 107093.

[5] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Netw.*, vol. 61, pp. 33–50, Mar. 2017.

[6] N. Salhab, R. Langar, and R. Rahim, "5G network slices resource orchestration using machine learning techniques," *Comput. Netw.*, vol. 188, Apr. 2021, Art. no. 107829.

[7] R. Vilalta et al., "Applying security service level agreements in V2X network slices," in *Proc. IEEE Conf. Netw. Funct. Virtualization Softw. Defined Netw.*, 2020, pp. 114–115.

[8] S. Zhang and D. Zhu, "Towards artificial intelligence enabled 6 G: State of the art, challenges, and opportunities," *Comput. Netw.*, vol. 183, Dec. 2020, Art. no. 107556.

[9] N. F. Saraiva de Sousa, D. A. L. Perez, R. V. Rosa, M. A. Santos, and C. E. Rothenberg, "Network service orchestration: A survey," *Comput. Commun.*, vol. 142, pp. 69–94, Jun. 2019.

[10] C. Benzaid and T. Taleb, "AI-driven zero touch network and service management in 5G and beyond: Challenges and research directions," *IEEE Netw.*, vol. 34, no. 2, pp. 186–194, Mar./ Apr. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8994961/

[11] M. M. Sajjad, C. J. Bernardos, D. Jayalath, and Y.-C. Tian, "Inter-slice mobility management in 5G: Motivations, standard principles, challenges, and research directions," *IEEE Commun. Standards Mag.*, vol. 6, no. 1, pp. 93–100, Mar. 2022.

[12] R. Sedar, C. Kalalas, F. Vazquez-Gallego, and J. Alonso-Zarate, "Reinforcement learning based misbehavior detection in vehicular networks," in *Proc. IEEE Int. Conf. Commun.*, 2022, pp. 3550–3555.

[13] ZSM Public Wiki., "PoC 6 Security SLA assurance in 5G network slices," Oct. 2022. [Online]. Available: https://zsmwiki.etsi.org/index.php?title=PoC_6_Security_SLA_assurance_in_5G_network_slices

[14] L. Bréhon–Grataloup, R. Kacimi, and A.-L. Beylot, "Mobile edge computing for V2X architectures and applications: A survey," *Comput. Netw.*, vol. 206, Apr. 2022, Art. no. 108797.

[15] T. W. Nowak et al., "Verticals in 5G MEC-use cases and security challenges," *IEEE Access*, vol. 9, pp. 87251–87298, 2021.

[16] European Union Agency for Cybersecurity, "ENISA threat landscape for 5G networks: Updated threat assessment for the fifth generation of mobile telecommunications networks (5G). Publications Office," 2020. [Online]. Available: https://data.europa.eu/doi/10.2824/802229

[17] ETSI, "MEC security: Status of standards support and future evolutions," Sep. 2022. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP-46-2nd-Ed-MEC-security.pdf

[18] S. Lai, R. Zhao, S. Tang, J. Xia, F. Zhou, and L. Fan, "Intelligent secure mobile edge computing for beyond 5G wireless networks," *Phys. Commun.*, vol. 45, Jan. 2021, Art. no. 101283.

[19] T. Alladi, V. Kohli, V. Chamola, F. R. Yu, and M. Guizani, "Artificial intelligence (AI)-empowered intrusion detection architecture for the internet of vehicles," *IEEE Wireless Commun.*, vol. 28, no. 3, pp. 144–149, Jun. 2021.

[20] A. Dalgkitsis, P.-V. Mekikis, A. Antonopoulos, and C. Verikoukis, "Data driven service orchestration for vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4100–4109, Jul. 2021.

[21] J. Kinyua and L. Awuah, "AI/ML in security orchestration, automation and response: Future research directions," *Intell. Automat. Soft Comput.*, vol. 28, no. 2, pp. 527–545, Jan. 2021.

[22] M. Maule, J. Vardakas, and C. Verikoukis, "5G RAN slicing: Dynamic single tenant radio resource orchestration for eMBB traffic within a multi-slice scenario," *IEEE Commun. Mag.*, vol. 59, no. 3, pp. 110–116, Mar. 2021.

[23] S. Matoussi, I. Fajjari, S. Costanzo, N. Aitsaadi, and R. Langar, "5G RAN: Functional split orchestration optimization," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 7, pp. 1448–1463, Jul. 2020.

[24] F. Rezazadeh, L. Zanzi, F. Devoti, H. Chergui, X. Costa-Pérez, and C. Verikoukis, "On the specialization of FDRL agents for scalable and distributed 6 G RAN slicing orchestration," *IEEE Trans. Veh. Technol.*, vol. 72, no. 3, pp. 3473–3487, Mar. 2023.

[25] M. F. Hossain, A. U. Mahin, T. Debnath, F. B. Mosharrof, and K. Z. Islam, "Recent research in cloud radio access network (C-RAN) for 5G cellular systems-A survey," *J. Netw. Comput. Appl.*, vol. 139, pp. 31–48, Aug. 2019.

[26] M. Liyanage, A. Braeken, S. Shahabuddin, and P. Ranaweera, "Open RAN security: Challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 214, May 2023, Art. no. 103621.

[27] C.-X. Wang, M. D. Renzo, S. Stanczak, S. Wang, and E. G. Larsson, "Artificial intelligence enabled wireless networking for 5G and beyond: Recent advances and future challenges," *IEEE Wireless Commun.*, vol. 27, no. 1, pp. 16–23, Feb. 2020.

[28] M. Liyanage et al., "A survey on zero touch network and service management (ZSM) for 5G and beyond networks," *J. Netw. Comput. Appl.*, vol. 203, Jul. 2022, Art. no. 103362.

[29] J. Gallego-Madrid, R. Sanchez-Iborra, P. M. Ruiz, and A. F. Skarmeta, "Machine learning-based zero-touch network and service management: A survey," *Digit. Commun. Netw.*, vol. 8, no. 2, pp. 105–123, Apr. 2022.

[30] K. Sha, T. A. Yang, W. Wei, and S. Davari, "A survey of edge computing-based designs for IoT security," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 195–202, Jun. 2020.

[31] C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, "TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs," *Veh. Commun.*, vol. 9, pp. 254–267, Sep. 2017.

[32] M. R. Dey, M. Patra, and P. Mishra, "Efficient detection and localization of DoS attacks in heterogeneous vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 5, pp. 5597–5611, May 2023.

[33] Z. Li, Y. Kong, C. Wang, and C. Jiang, "DDoS mitigation based on space-time flow regularities in IoV: A feature adaption reinforcement learning approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2262–2278, Mar. 2022.

[34] Y. Deng et al., "Resource provisioning for mitigating edge DDoS attacks in MEC-enabled SDVN," *IEEE Internet Things J.*, vol. 9, no. 23, pp. 24264–24280, Dec. 2022.

[35] C. Benzaid et al., "White paper: Intelligent security architecture for 5G and beyond networks," Nov. 2020. [Online]. Available: https://doi.org/10.5281/zenodo.4288658

[36] ETSI GS ZSM 002 V1.1.1, "Zero-touch network and Service Management (ZSM); Reference Architecture," European Telecommunications Standards Institute (ETSI), Sophia Antipolis, France, Tech. Specification GS ZSM 002, 2019.

[37] J. Kamel, M. Wolf, R. W. van Der Heijden, A. Kaiser, P. Urien, and F. Kargl, "VeReMi extension: A dataset for comparable evaluation of misbehavior detection in VANETs," in *Proc. IEEE Int. Conf. Commun.*, 2020, pp. 1–6.

[38] ETSI TR 102 638 V1.1.1, "Intelligent transport systems (ITS); vehicular communications; basic set of applications; definitions," European Telecommunications Standards Institute (ETSI), Sophia Antipolis, France, Tech. Rep. TR 102 638 V1.1.1, Jun. 2009.