IEEE Open Journal of the Communications Society

Received XX Month, 2024; revised XX Month, 2024; accepted XX Month, XXXX; Date of publication XX Month, XXXX; date of current version XX Month, XXXX.

Digital Object Identifier 10.1109/OJCOMS.2024.1234567

Access-Side DDoS Defense for Space-Air-Ground Integrated 6G V2X Networks

Xu Chen[1], **Wei Feng**[1,2], ***Senior Member, IEEE***, **Yunfei Chen**[3] ***Senior Member, IEEE***, **Ning Ge**[1,2], ***Member, IEEE***, **You He**[1]

[1]Department of Electronic Engineering, Tsinghua University, Beijing, China
[2]State Key Laboratory of Space Network and Communications, Beijing, China
[3]Department of Engineering, University of Durham, Durham DH1 3LE, U.K.

CORRESPONDING AUTHOR: Wei Feng (e-mail: fengwei@tsinghua.edu.cn).

ABSTRACT Distributed Denial of Service (DDoS) attacks pose a significant threat to the Internet of Vehicles, causing delays in driving operations and risking personal safety. With the emerging of Space-Air-Ground Integrated Sixth-Generation (6G) networks, DDoS defense faces new challenges, especially in open and complex Vehicle-to-Everything (V2X) connections. In this study, we reviewed the requisites and challenges of DDoS defense in V2X and introduced a tailored access-side defense architecture for Space-Air-Ground Integrated 6G V2X. The objective is to provide ultra-low latency and privacy-assured services despite limited communication resources. Our architecture uses access-side control points (CPs) for rapid attack responses, collaborating with local controllers to create a seamless defense perimeter at the network edge. This prevents malicious traffic infiltration. Incorporating proactive defense strategies and lightweight detection methods, our approach ensures high attack detection rates with low defense costs. Simulation results confirm its efficacy and advantages in defense and network efficiency. We also discuss open issues for future research to facilitate practical applications.

INDEX TERMS access-side defense architecture, distributed denial of service (DDoS), defense efficiency, sixth generation (6G), vehicle-to-everything (V2X).

I. INTRODUCTION

WITH the rapid development of driving assistance technologies, vehicles have begun to transform from a single transportation platform to a networked intelligent terminal. The vehicle-to-everything (V2X) communication network has become a key infrastructure for supporting future autonomous driving applications [1]. Moreover, the development of sixth-generation (6G) mobile communication, especially low earth orbit (LEO) satellite communication technology, is expected to further expand the coverage of V2X networks to remote areas. The vision of 6G is to establish a space-air-ground integrated network that supports global wide area access [2]. A large collaborative network made of trillions of interconnected vehicles, roadside infrastructure, sensors, and pedestrians is on the way [3]. However, in such a heterogeneous network, the risks of vehicle operation safety, data privacy and network security complicate the security of V2X communication. Network security is the basic premise for ensuring the operational safety of vehicles and an important fulcrum for realizing data privacy, making network security a top priority for ensuring V2X security [4]. Unfortunately, the ultra-large scale of the 6G V2X network further expands the attack surface of traditional mobile networks. Potential attackers can launch more damaging attacks by compromising more network devices and causing more serious damage.

In connected vehicle systems, denial of service (DoS) attacks are a category of traditional security threats [5]. As the number of intelligent vehicles and on-board devices connected to the network increases, the ways to launch DoS attacks against vehicles are rapidly diversifying. Among such threats, distributed denial of service (DDoS) attacks, which involve the launching of malicious traffic from a large number of compromised devices can directly destroy the availability of connected vehicles, infrastructure and network services and seriously threaten driving safety [6]. However, DDoS defense is much more difficult than ever before. On the one hand, the high complexity and heterogeneity of 6G

V2X networks make it more difficult to achieve distributed collaboration among different control domains. Traditional defense methods based on centralized control strategies (such as SDN-based methods) have difficulty achieving effective defenses across different network domains and face the difficulty of scalability and integration of heterogeneous network devices [7]. DDoS defense methods based on uniformly allocating network-wide resources are infeasible [8], [9]. It is necessary to develop a new distributed DDoS malicious traffic defense mechanism.

On the other hand, the unprecedented scale of attack traffic in 6G V2X will make traditional defense methods (such as traffic scrubbing) on the server side unsustainable [10]. The server-side mitigation methods adopted by most enterprises require investment in very expensive infrastructure and network bandwidth. The repeated construction of security infrastructure leads to a great deal of resource waste and is not affordable for small and medium-sized enterprises (SMEs). In addition, server-side defense methods allow malicious traffic to consume excessive communication resources after entering a data network (DN). To overcome both challenges and improve the effectiveness of DDoS defense in V2X, it is necessary to push the defense surface from the server side to the edge, i.e., the access side of V2X. Therefore, developing an access-side DDoS defense mechanism in 6G V2X networks is urgently needed to ensure the driving safety of intelligent vehicles and support the rapid development of the vehicle industry [11].

Fortunately, the development of new technologies has also provided many opportunities for DDoS defense. Blockchain and advanced authentication technologies in 6G will provide a unique and reliable identity for all network elements in V2X [12], [13]. This approach enables trust evaluation-based DDoS detection. The deployment of multiaccess edge computing (MEC) will provide the necessary computing infrastructures for edge intelligence [14]. This makes it viable to deploy traffic control points (CPs) on the network access side to defend against DDoS attacks. Such access-side CPs usually refer to software modules that are deployed on edge computing servers in the access network. They actively extract necessary information from the passing traffic, detect potential attack behaviors and implement predefined security strategies, thus improving the network security performance. On this basis, federated learning techniques can avoid excessive communication overhead and provide privacy-preservation [15]. The detection accuracy of malicious traffic at access-side CPs can therefore be significantly improved [16]. Digital twin technology enables the network controller to monitor the working status of network devices in real time and detect abnormal statuses to prevent intrusions [17], [18]. In addition, the development of integrated spatial-terrestrial network technology in 6G will also bring new opportunities for DDoS defense [19]. For example, space-ground collaboration provides a more efficient method for defense strategy distribution and attack information sharing [20]. The simplified network topology of long-distance communication can also support a wider range of collaborative defenses.

Motivated by the above observations, this article aims to improve the DDoS defense efficiency in V2X by taking advantage of new 6G technologies. The main contributions of this work are as follows.

- We explore the requirements and challenges associated with implementing DDoS defense in 6G V2X at the network layer and identify the design goals of the corresponding security architecture.
- We propose a comprehensive access-side defense architecture against DDoS traffic. This architecture promotes horizontal collaboration among CPs at the access side to deter potential attackers and establish long-term defense strategies.
- We detail four key technologies that need to be considered when implementing this architecture. These technologies involve formulating a unified strategy coordination mechanism among CPs by combining proactive and reactive defense methods, enabling efficient DDoS detection through multi-domain collaboration and reducing detection costs through packet sampling.
- We implement a set of simulations and verify the effectiveness and efficiency of the proposed access-side DDoS defense architecture through comparative analysis. To the best of our knowledge, this article is the first attempt to systematically discuss the DDoS defense requirements in 6G V2X and provide a comprehensive defense architecture at the access side.

The remainder of this article is organized as follows. We analyze the requirements and challenges in DDoS defense in Section II. In Section III, we introduce the access-side DDoS defense architecture in terms of its components, collaboration mechanism and security performance. We discuss the key technologies involved in the proposed access-side defense architecture in Section IV. Numerical results on the defense performance are illustrated in Section V. We present some open issues for further research in Section VI. Section VII concludes the article.

II. Requirements and Challenges

A. 6G V2X ARCHITECTURE

To improve road safety and traffic efficiency, connected vehicles need to communicate frequently with other vehicles, roadside units (RSUs), pedestrians, remote control centers, global navigation satellite systems (GNSSs), and other cloud services via an in-vehicle communication unit, a.k.a, an on-board unit (OBU). The ubiquitous connectivity of 6G spawns a large collaborative network. A typical space-air-ground integrated 6G V2X architecture is shown in Fig. 1.

The architecture can be divided into four layers. The bottom layer is the access layer, which consists of vehicles, pedestrians, and various intelligent transportation devices,

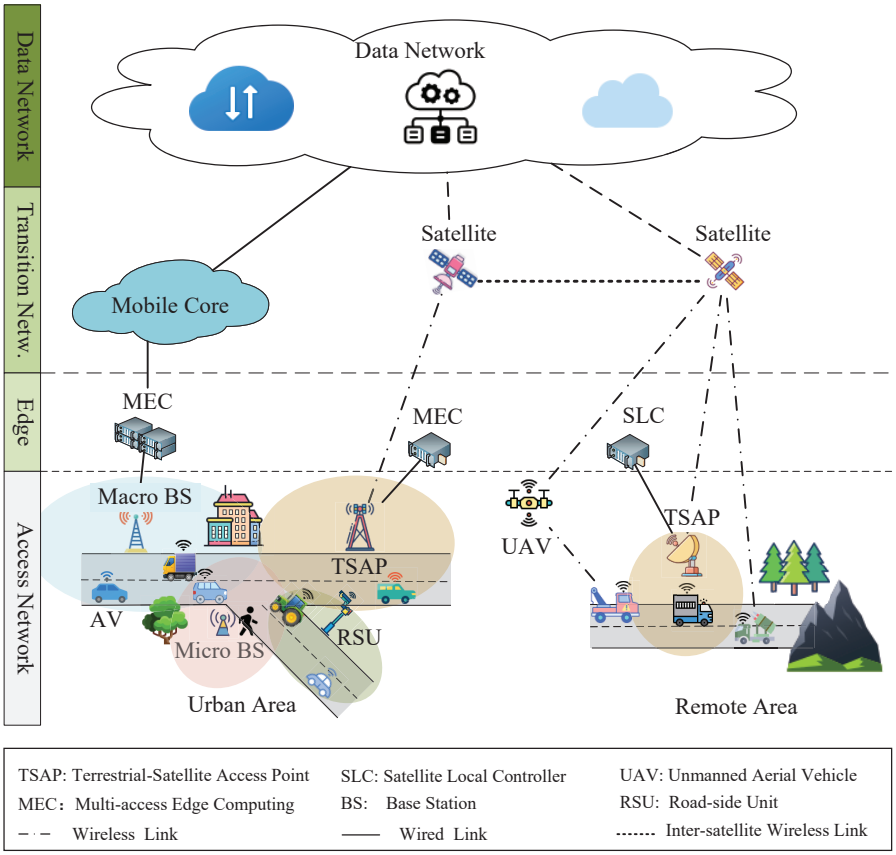

FIGURE 1. **A typical scenario of the space-air-ground integrated 6G V2X architecture.**

such as traffic lights, cameras, and other environmental sensing devices. The access equipment includes base stations, terrestrial satellite access points (TSAPs) and RSUs. Vehicles in remote areas can connect to satellite networks via TSAPs or relayed by unmanned aerial vehicles (UAVs) [21]. The second layer is the edge. Edge nodes can be servers or edge devices with enough computing power, such as macro base stations and satellite local controllers (SLCs). Due to the low propagation latency, edge computing is widely used to support latency-sensitive services for computational offloading and data caching in V2X applications. The third layer is the transition network, which consists of the terrestrial 6G core network and satellites in space. The efficiency of the transition network has a significant impact on the quality of service (QoS) in the cloud. The last layer is the data network which provides cloud-based services, such as remote control, weather forecasting, and entertainment systems.

B. DDOS DEFENSE REQUIREMENTS IN 6G V2X

Information exchange in V2X has enabled a large variety of applications, including remote driving, platooning, map sharing, cooperative awareness, cooperative sensing, and cooperative collision avoidance. The new security requirements of the V2X can be investigated in terms of confidentiality, authenticity, integrity, and availability. There have been some research efforts on the security requirements of 6G networks, including V2X networks. Hafi et al. discussed the requirements, solutions, challenges, and application scenarios of deploying Split Federated Learning in 6G networks [22]. Li et al. proposed a security reference architecture named SecCDV for Cybertwin-Driven 6G V2X, primarily focusing on data security and privacy at the application layer [23]. However, these works did not delve deeply into DDoS attacks at the network layer in V2X or address access-side security. In this work, we concentrate on network domain security, comprehensively analyzing the characteristics of various DDoS attacks in V2X and the challenges faced by access-side defense. Among the many kinds of security requirements, the availability of V2X services is essential for road safety and is directly related to the personal and property safety of passengers. DDoS attacks that seriously hinder the availability of V2X services should be given priority in the security design of 6G V2X. According to the type of victim, DDoS attacks in V2X can be divided into the following categories.

(1) DDoS attacks in access networks

Vehicles in the existing Internet of Vehicles (IoT) can communicate with each other directly via 802.11p-based

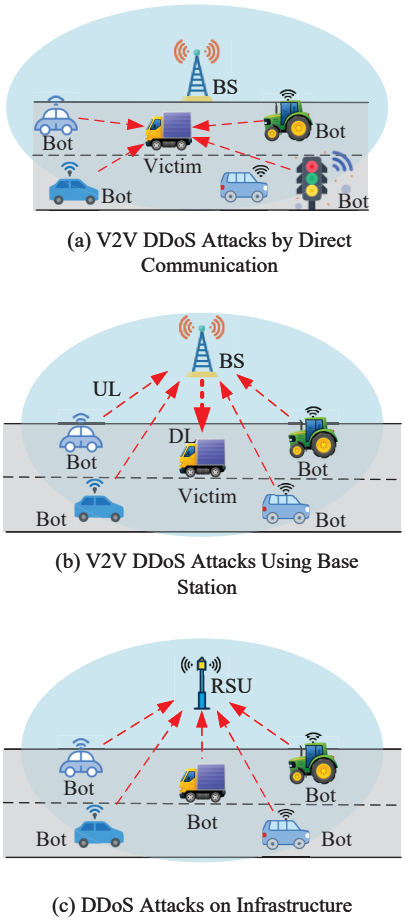

FIGURE 2. **DDoS attacks in access networks.**

technologies, LTE PC5 [24], the 5G New Radio (NR) Sidelink interface [25], or base stations using interfaces such as LTE-Uu. Vehicle-to-vehicle (V2V) communication enhances information collaboration between vehicles. However, they also allow DDoS attackers to directly orchestrate compromised V2X devices to launch attacks against targets in the access network. According to whether the attack traffic passes through the base station, DDoS attacks in the access network can be divided into two categories, as shown in Fig. 2(a) and Fig. 2(b). The red arrows indicate the attack traffic.

V2V direct communication is feasible only in the short range. The DDoS attack traffic relay by the base stations is limited by the coverage of the base stations. The number of available bots within this range is limited. The defense strategy of such DDoS attacks has been fully studied in vehicle ad hoc networks (VANETs) by previous researchers [26]–[29]. In addition, the victims of DDoS attacks in the access network can also be RSUs or base stations, as shown in Fig. 2(c). The attack distance is limited by the physical signal coverage of the victim. The base stations and RSUs

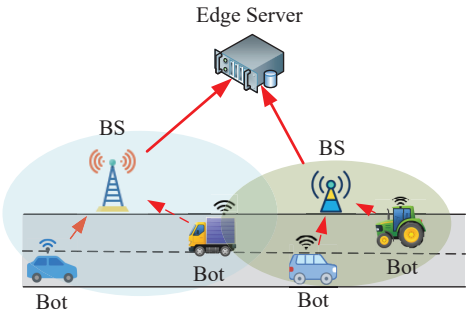

FIGURE 3. **DDoS attacks on an edge server.**

have sufficient service capabilities for connected vehicles, so such attacks should not paralyze them.

(2) DDoS attacks on network edges

Edge servers provide low-latency services for vehicle users. Because edge servers are resource restricted, they are more vulnerable to DDoS attacks than cloud servers. DDoS attacks on network edges are illustrated in Fig. 3. The coordinated bots concurrently send service requests to the edge server through the base stations. The server is overloaded and unable to provide services. Such DDoS attacks will significantly increase service delays over a wide range and seriously affect driving safety. These conditions are most harmful to the security of V2X communication systems.

(3) DDoS attacks on transition networks

The 6G core network is envisioned to follow the service-based architecture (SBA) of 5G networks. The SBA introduces vulnerabilities in network function registration, discovery and authorization. Network function services and interfaces can easily become the target of DDoS attacks. In addition, hybrid software-defined networking (SDN) may be a key enabler for 6G [30]. The SDN controller can be an important target for DDoS attacks. Furthermore, satellite-ground links and intersatellite links will also become targets of DDoS attacks. A DDoS attack scenario on transition networks of 6G V2X is shown in Fig. 4. In V2X, bot nodes may move at high speed, and their access points may change rapidly, making defense against them much more difficult.

(4) DDoS attacks on data networks

Since most digital assets on the Internet are concentrated in data centers, cloud platforms have long been an important target for DDoS attacks. Cloud platforms also possess most of the DDoS defense resources in the existing network. Edge devices can share the workload of clouds, but their role as critical infrastructures of information and communication technology (ICT) will not change over the next decade. In this situation, DDoS attacks will continue to proliferate in 6G V2X.

Based on the requirement analysis, we are motivated to make great efforts to seek a long-term, efficient and

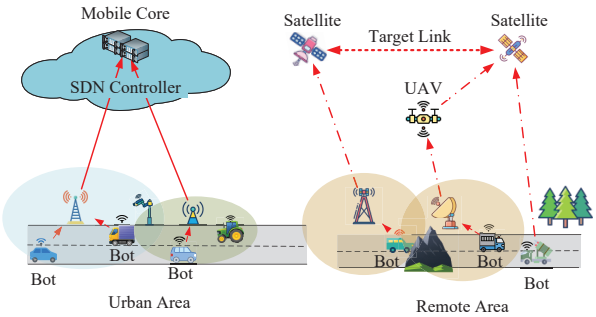

FIGURE 4. **DDoS attacks on transition networks in 6G V2X.**

systematic solution to address potential DDoS attack threats. For DDoS attacks in access networks and edges, centralized local detection and mitigation can be performed based on the existing DDoS defense methods. In this article we focus on DDoS attacks on transition networks and data networks that involve collaboration among multiple entities.

C. NEW DDOS DEFENSE CHALLENGES IN 6G V2X

There are still few studies on DDoS defense methods for V2X. The existing methods can be categorized into two kinds. One kind includes DDoS defense mechanisms in traditional VANETs. The attack scenarios in such methods are usually simple. Only V2V and Vehicle-to-Infrastructure (V2I) communications are considered [30]. The customized defense methods for VANETs cannot meet the DDoS defense requirements in 6G V2X since they cannot adapt to highly complex attack scenarios. The other kind of approach involves transplanting traditional DDoS defense methods in centrally controlled networks (e.g., SDN), to V2X through adaptive improvement [27]. These methods usually lack consideration of the special characteristics of V2Xs, such as bot mobility. Especially in satellite-terrestrial integrated networks (STINs), in-depth and detailed research on overcoming the topological dynamics and heterogeneity of V2Xs is still lacking. New DDoS defense challenges in 6G V2X are summarized as follows.

(1) Limited commutation resources

An intelligent vehicle is a complex system. There are various types of in-vehicle devices that require considerable communication resources, such as access infrastructures, link bandwidths, and power. The majority of V2X services are accessed through wireless communication channels [31]. Although the communication resources in 6G mobile networks will be further enriched, the applications of V2X will be more diversified and resource-consuming. 6G V2X applications involve not only urban areas with sufficient communication resources but also rural areas, mountains and even deserts with limited communication resources. An uneven distribution of communication resources will continue to exist [32]. This limitation puts forward two major challenges for the DDoS defense architecture. First, the defense architecture must work with limited network resources. In security architectures based on traditional machine learning methods, the model training process requires the transmission of a large amount of traffic data and historical information. This consumes considerable network bandwidth. Due to the rapid changes in security situations, continuous model updating will result in considerable communication resource consumption. How to apply traditional DDoS defense methods in resource-constrained scenarios has become an open problem [33].

Second, traditional server-side DDoS defense methods, such as the next generation firewall (NGFW) and intrusion detection system (IDS), cannot detect attack traffic until they reach the target network. DDoS attack traffic consumes a large amount of communication resources in transmission. To improve defense efficiency, the defense architecture must block malicious traffic at the network entrance to preserve downstream network resources. The selection of access-side CPs and their collaboration mechanism have become additional open problems. Therefore, the defense architecture in V2X communication should reduce additional resource consumption as much as possible, and block malicious traffic at the access side to save communication resources.

(2) Ultralow latency

Different kinds of services carried by V2X communication have different delay requirements. In particular, automatic driving decision-making, vehicle-road coordination, vehicle-vehicle coordination, and satellite-terrestrial coordination are sensitive to delays. The development of services requires the entire communication network to achieve millisecond (ms)-level delays. For example, a new radio vehicle aims to achieve 3 ms or lower latency and 99.999% reliability [30]. The duration of new types of DDoS, such as pulse attacks, can usually be shortened to a few seconds for each round. However, traditional defense mechanisms fail to respond quickly. In addition, due to the high-speed mobility of vehicles, the frequent switching of network access points and local network environments also brings challenges to the delivery delay of services. Existing security architectures face the following difficulties in meeting ultralow latency requirements. 1) Propagation delay of the defense policy. In existing security architectures, even if countermeasures are deployed at the network edge, remote cloud centers usually make defense decisions and then forward them to the edge. Round-trip propagation results in significant delays and affects the timeliness of defense decision implementation. 2) Processing delay of the traffic data. For attack traffic detection, intensive computing power is necessary to process a large amount of network raw traffic data. At the edge, the delay of high-throughput traffic processing will greatly increase due to the limited computing power. Online processing is therefore difficult to achieve. Alternatively, the offline processing mode of mirrored traffic in clouds will affect the real-time performance of the defense system. Therefore, the defense architecture of the 6G V2X must make distributed

decisions at the access side. Defense decisions need to adopt lightweight detection methods to achieve online processing of large-scale traffic and meet the requirements of delay-sensitive applications.

(3) Privacy-preserving requirements

Data processing in V2X involves sensitive information such as passengers' locations, personal preferences, and even identities, which requires high privacy-preserving performance. The existing security architecture of V2X usually adopts pseudonym, anonymity, or data aggregation-based obfuscation operations to improve user privacy in the cloud [34]. However, it is still difficult to prevent malicious users from probing users' privacy through data mining. Moreover, it is usually necessary to use information such as the Vehicle Identification Number or International Mobile Equipment Identity (IMEI) in attack traffic tracing or trust management-based DDoS detection methods. Moreover, users' privacy is difficult to preserve. To address this dilemma, user identity-related information can be kept at the edge for processing instead of in the cloud. By taking advantage of this approach, the access-side defense architecture is promising for preventing privacy data leakage.

To this end, defense against DDoS attacks at the access side needs to solve two problems. First, we need to construct a distributed collaborative defense architecture. It is necessary to deploy many CPs in different network domains for DDoS detection at the access layer of V2X. These CPs must collaborate horizontally via a feasible cross-domain collaboration mechanism. When no attack incident is reported, these CPs perform routine collaborative defense strategies to form a seamless defense surface to jointly deter potential attackers. When an attack event is reported, the relevant CPs activate the emergency response mechanism to quickly detect and efficiently block attack traffic in collaboration. To reduce bandwidth consumption, collaboration should avoid large-scale information exchange. Therefore, the collaborative mechanism among CPs is the primary problem.

Second, access-side defense methods must be lightweight and adaptive. These devices should be able to flexibly adapt to heterogeneous edge computing devices. Since the computing power at the edge nodes is limited, defense methods cannot consume too much computing resources. Low-latency V2X applications also require that the defense architecture respond quickly, which limits the time complexity of DDoS detection methods. On this basis, considering that the packet throughput of the access-side network node may be large, the task load of packet processing should be reduced as much as possible to avoid excessive processing delay.

Therefore, the tradeoff between detection accuracy and response delay is the second problem to be solved. Moreover, privacy protection requirements should be implemented throughout architectural design. The information exchange in the collaborative strategy should not transmit sensitive user information, and the information used for attack traffic detection should also be limited to local storage to avoid uploading to the cloud or spreading it in a large area.

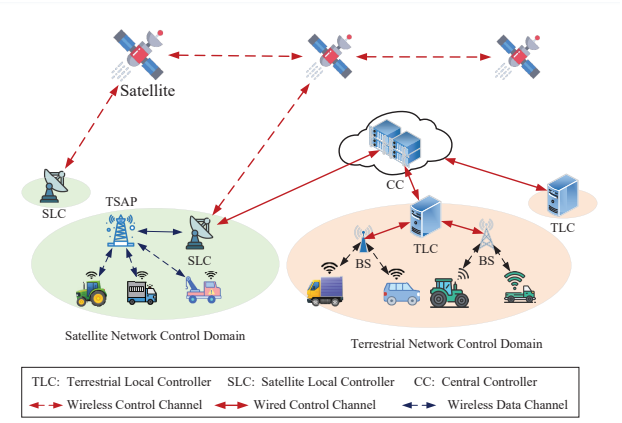

FIGURE 5. Control architecture of space-air-ground integrated 6G V2X.

III. Access-side DDoS Defense Architecture in 6G V2X

Due to the heterogeneity of user equipment (UE) in 6G V2X, it is difficult to construct a unified application layer security architecture based on UE resources. We pay attention to the network layer, specifically the edge, to defend against DDoS attacks. Access-side defense measures can be deployed to the nearest computing nodes from UEs, such as the RSUs, base stations, TSAPs, or edge servers. Note that the security architecture of the 6G networks is envisioned to perform strict UE identity authentication. Unauthorized UEs will be identified and sent out before network sessions are established to suppress DDoS attack traffic. Therefore, we assume that DDoS in V2X is initiated by legitimate UEs.

A. ANALYSIS OF EXISTING DDOS DEFENSE ARCHITECTURES

The access-side DDoS defense aims to detect attacks as early as possible, thereby minimizing potential damage. However, three challenges hinder the detection of DDoS attack traffic at the access side. Firstly, parsing application layer information is challenging due to source encryption and other factors, resulting in limited available information for detection. Secondly, attack traffic is often dispersed and small in scale, making it difficult to detect before causing harm. Thirdly, security modules at the access side typically operate under constraints of limited communication and computing resources, complicating the execution of complex security operations like traffic scrubbing.

Existing DDoS defense architectures based on edge computing can be classified into three categories: passive mitigation, online detection, and proactive defense. Passive mitigation methods mitigate DDoS attack damage through optimized task offloading or resource allocation [16], [35]. This typically involves transferring some service requests to neighboring edge servers [36] or coordinating traffic

scrubbing [37]. Based on available defense resources, these schemes can mostly be implemented through software-level settings and configurations, offering advantages in deployability and compatibility. However, their defense efficiency is constrained by the total amount and distribution of edge resources, and the scalability is also limited.

In online detection methods, detection modules based on machine learning (ML) are used to detect and defend against malicious traffic [38]. The advantages of such methods include high detection accuracy and promoted security performance. However, additional training costs and computational requirements are introduced, which reduce their compatibility and deployability. In addition, some online ML methods need to inspect all packets forwarded by the edge server, which is expensive and non-scalable [38], [39]. The application of federated learning (FL) technology could reduce the computing and communication overhead at a single node [40], [41]. However, due to the differences in traffic components and distributions among edge detection nodes, the model aggregation of FL models may deteriorate the detection performance of the local models. Both kind of methods mentioned above are effective against known attacks but may falter against potential or unknown attacks.

Proactive defense methods are mostly based on game models and Moving target Defense (MTD). By flexibly deploying potential targets and dynamically changing system configurations, the MTD method can create cognitive barriers for attackers, increasing the difficulty of launching attacks or reducing attack effectiveness. This architecture is often effective, especially for zero-day attacks and advanced persistent threats (APTs) [42]. However, the cost of hardware and software deployment and target migration is usually high, requiring special security design. Alternatively, the game model-based methods usually derive the optimal defense strategy [43]. The disadvantage of this method is that the defense efficiency is limited by the modeling accuracy and parameter settings. The tradeoff between modeling complexity and practical feasibility should be carefully balanced.

Different from the above work, we build a novel DDoS defense architecture for 6G V2X with the following characteristics. (1) Low cost. It is deployable and can be implemented only through software configuration, without introducing additional hardware or excessive computing/communication overhead. (2) Scalable. It can be applied to different types of DDoS attacks and can be deployed on large-scale networks. (3) Proactive. It can distinguish different defense requirements, flexibly adjust defense strategies, and actively deter potential attackers.

B. OVERVIEW OF THE NEW ARCHITECTURES

We first explain the control architecture of the 6G V2X network. As a space-air-ground-sea integrated network, 6G is envisioned to adopt an SDN-based hierarchical control architecture to facilitate efficient operation and management in the integrated network [30]. SDN controllers in urban/remote scenarios should be organized hierarchically for scalability considerations, as shown in Fig. 5. The entire network is logically divided into multiple nonoverlapping control domains. An SDN local controller (LC) is deployed in each control domain. The central controller (CC) performs network-wide resource management for service delivery and seamless coverage even in high mobility situations as a coordinator for local controllers. We build a collaborative defense architecture based on the control domains of SDN LCs.

In industrial applications, satellite Local Controllers (SLCs) are deployed in various configurations, utilizing different hardware platforms such as GEO satellites, LEO satellites, ground stations, Network Control Centers (NCCs), Network Management Centers (NMCs), and even terrestrial cloud centers. GEO satellite-based controllers provide stable connections with ground stations but have limited coverage, especially in polar areas. Additionally, their computing resources constrain network scale. LEO satellite-based controllers communicate with terrestrial access points only when flying over stations, resulting in increased signaling delay for network state collection and control message distribution. Limited onboard resources also pose scalability challenges. NCC/NMC-based controllers face similar limitations. In our paper, we assume that the SLC is deployed at a ground station or network control center to minimize transmission delay in space-ground link for transmitting attack information and distributing security strategies.

According to the defense objectives of the V2X, we distinguish between two different defense scenarios: routine defense and emergency defense. Routine defense means that when the LC does not receive an attack event report, the CPs randomly inspect the traffic forwarded by their associated edge servers to detect potential attacks based on the security strategies provided by the LC. The primary goal of routine defense is to deter potential attackers while minimizing the cost of defense. In emergency defense, when an attack incident is reported, the LC instructs the CPs to quickly activate the defense countermeasures, detect and block attack traffic as soon as possible, and minimize defense costs.

As shown in Fig. 6, the entire defense architecture has three layers. The bottom layer consists of UEs, which include vehicles, cameras, traffic lights and other roadside sensors. Some of these devices are compromised by attackers. Attack traffic originates from these compromised UEs, passes through the CP, and enters the downstream network. The defense surface is deployed in the middle as the second layer, which consists of all the CPs. All upstream traffic passes through this layer, including both normal and attack traffic. The attack traffic detection module is deployed on each control point. The forwarded traffic can be detected according to the defense strategy distributed by the upper-layer LC. CPs are the main entities of defense strategy execution in this architecture, and they are also the core components of the defense surface. DDoS attacks targeting

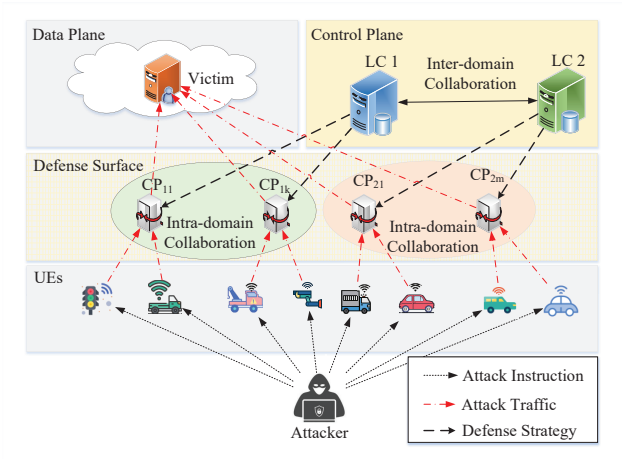

FIGURE 6. Access-side collaborative DDoS defense architecture in 6G V2X.

devices in the access network and edge can be detected and mitigated by each CP, which is consistent with the traditional DDoS defense architecture and does not involve collaboration issues. The top layer is divided into two parts: the control plane and the data plane. The control plane consists of all the LCs and the CC. The LC is the decision maker for defense strategies and the mediator of CPs in each control domain. The CC is the coordination medium of LCs for facilitating interdomain collaboration. The data plane refers to the network elements in the transition network and the DNs in which the potential victims reside. It is usually the destination domain of attack traffic.

Note that Fig. 6 only illustrates the logical division of the defense architecture. The physical network domain division may be slightly different. For example, the victim, LC and CPs may all be located in the same SDN control domain. In addition, this article considers attacks on only upper-layer victims through the uplink and does not consider attacks on edge nodes or UEs through the downlink. This is because the attack traffic in V2X mainly comes from UEs. Edge nodes mostly use intranet addresses or randomly allocated addresses from the IP address pool. These addresses are unknown to public users. The mobility of UEs may lead to address switching, which makes them difficult to target. It is unfeasible for attackers to control malicious UEs to send attack traffic, uplink through the core network/DN, and then downlink to attack edge nodes/UEs.

To clearly explain the operation mechanism and demonstrate the advantages of this new architecture, we compare it with the traditional server-side DDoS defense methods in Table 1.

(1) Computing support devices. As mentioned above, server-side defense methods are deployed at border gateways, firewalls, or cloud centers in the target network. These devices are usually rich in computing resources. Access-side defense methods can be deployed only on access points or edge servers. Their resources are mostly poor. Therefore, lightweight defense methods need to be developed.

(2) Available information. Server-side defense methods can directly use application layer and network layer information. The application layer information cannot be used due to traffic encryption. High-precision detection requires mining information from other sources. Multi-domain information mining and fusion are necessary.

(3) Points of defense. The attack traffic on the server side is aggregated in DDoS attacks. Defense countermeasures can be deployed at a single point. On the access side, the attack traffic is spread over multiple access points and is small in scale. At each point, defensive measures need to be deployed and collaborate with each other. Therefore, multi-point collaboration mechanisms are highly important for access side defense architecture.

(4) Communication efficiency. When the defense point is deployed on the server side, the attack traffic consumes a large amount of communication resources in the forwarding path. The communication efficiency of the defense is low. The access-side defense system blocks attack traffic at the access point, avoiding the consumption of downstream communication resources. In the access-side defense system, attack information aggregation, defense strategy distribution, and trust value sharing introduce numeric data exchange in collaboration. However, the communication overhead is quite low. Therefore, the communication efficiency is high.

(5) System latency. In DDoS defense systems, the response latency is determined by three factors: the feature extraction time, the time complexity of the algorithms, and the scale of the data processing. To achieve a high detection rate, server-side defenses usually adopt a high-complexity detection method. A very large amount of traffic data must be processed. The state-of-the-art machine learning-based detection methods introduce a high time delay in flow-level feature extraction. The system latency is inevitably high. The data scale on a single defense point at the access side is relatively small. By combining packet sampling and lightweight detection methods, the system delay can be reduced to a very low level. Therefore, real-time online processing can be achieved.

(6) Privacy preservation. Privacy issues are caused mainly by the utilization of application layer information and large-scale data pooling. Therefore, it is difficult to protect privacy in server-side defense. The access side defense architecture can avoid these two problems. The only elements involved in privacy are user identity and trust value. User identifiers (such as SUCIs) are inherent information of Internet service providers (ISPs), and their use is limited to the control plane of the ISP network and is not uploaded to cloud centers or other network elements. The trust value evaluation and transmission process are carried out using blockchain-based encrypted identity, which is only converted into user identity on the control plane of the ISP network. Therefore, the privacy of user trust values and identities can be ensured.

TABLE 1. Comparison of access-side defense and server-side defense characteristics.

Defense mechanism	Access-side defense	Server-side defense
Computing support devices	Edge servers, access points	Border gateways, firewalls, cloud servers
Available information	Network layer information, other sources	Network & application layer information
Points of defense	Single point, centralized	Multiple points, distributed, collaborative
Communication efficiency	Low	High
System latency	High	Low after optimization
Privacy preservation	Weak	Strong

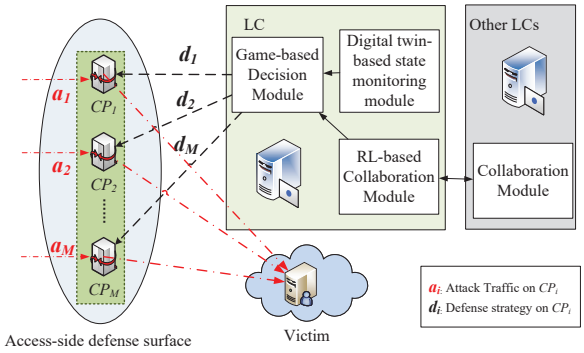

FIGURE 7. Security game and collaboration framework in routine DDoS defense.

IV. Key technologies for access-side defense

A. DISTRIBUTED COLLABORATION MECHANISM

The collaboration relationships in the proposed DDoS defense structure can be divided into two modes: intradomain collaboration between CPs and cross-domain collaboration between LCs. In different defense scenarios, the collaboration mechanism of the DDoS defense architecture is different. We introduce them separately below.

1) Collaboration in routine defense

In routine defense, the defense objective is to deter potential attackers. We define the LC as the defender of a network control domain in V2X. The formulation of a defensive strategy requires fine-grained modeling and analysis of decision-making elements, including the action space and utility function of both players. This problem can be modeled using game theory. A typical DDoS security game scenario in V2X is illustrated in Fig. 7. The DDoS detection methods are deployed at the CPs. The security function of the LC has three modules: a game-based decision module, a collaboration module with other LCs and a state monitoring module for CPs.

- Game-based decision module. To make an optimal defense decision, a multipoint collaborative security game model can be formulated in the LC of each control domain. By analyzing the victim's characteristics and the attacker's equilibrium strategy, the defender can derive a dominant strategy so that the attacker cannot benefit from launching an attack as expected. A specific defense action can be a countermeasure that directly affects the detection rate of attack behaviors, such as the packet inspection rate. For the detailed modeling methods and theoretical analysis, please refer to our earlier work [43]. On this basis, it is sufficient for the CPs in each control domain to collaborate with each other according to the derived dominant defense strategy broadcasted by the LC.
- Reinforcement learning-based collaboration module. Considering that the parameters of the DDoS security game model may change over time, a single LC cannot perceive such changes in a timely and accurate manner due to its small sample size of strategic interactions. This module is used to establish an information collaboration mechanism between LCs to adjust and optimize the equilibrium defense strategy. LCs can share their defense strategies and game results as training samples with other LCs. The shared information should consist of the state, action, reward, and strategy. Among them, reward information is the most important and can provide feedback from the environment (i.e., attackers) for recipients to improve their strategies. This interdomain information sharing does not require high timeliness and can be achieved through terrestrial backbone networks or satellite networks in 6G. Then, classical reinforcement learning methods such as the Q-learning algorithm can be adopted to update the local game model and defense strategy [44]. We will not discuss the implementation details of the learning models here.
- Digital twin-based state monitoring module. This module is designed for privacy-preserving purposes. Along with the widespread use of open radio access network (O-RAN) technology, heterogeneous access devices may introduce a large number of vulnerabilities, putting CPs at risk. A CP state monitoring mechanism must be established. Digital twin technology has provided a

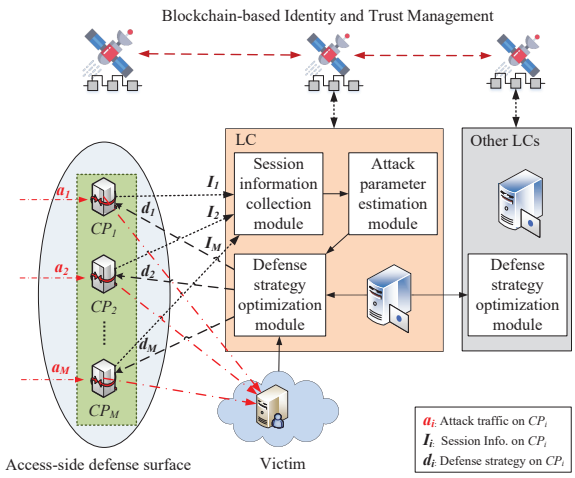

FIGURE 8. The collaboration framework in emergency DDoS defense.

solution to this problem [45]. By accurately mapping the physical state of the access-side devices to the digital space, the LC can monitor and diagnose all the CPs in its control domain in real time to detect abnormal devices and eliminate their security risks. Therefore, this module can avoid CP-led attacks and privacy issues.

In summary, collaboration in routine defense mainly includes two parts: strategic collaboration among the CPs in the control domain and interdomain information collaboration among LCs. The former establishes a local defense surface based on a proactive strategy, and the latter expands the local collaboration network-wide and realizes strategy evolution. The integration of both can realize a long-term proactive defense architecture.

2) Collaboration in emergency defense

In an emergency defense, the defense objective is to block attack traffic as soon as possible. We take a session as the basic unit of attack detection. Each attack session can be blocked immediately after being detected, instead of inspecting every packet in the session. This setting can help reduce costs and improve defense efficiency. To this end, LCs need to derive their defense strategies to detect attack sessions with the required detection rate. The collaboration framework for emergency DDoS defense is shown in Fig. 8. The CPs are deployed with the detectors of attack traffic. The LC still serves as the defender and decision maker for a single control domain, but its functions are different from those of routine defense.

The LC hosts three functional modules: the session information collection module, the attack parameter estimation module and the defense strategy optimization module. The CPs implement attack session detection and periodically report the newly collected attack session information to the LC. The attack session information can be customized by LC according to the input parameters of the detection method, which usually include the session 5-tuple (i.e., the allocated source IP address, the destination IP address, the source/destination port and the layer 4 protocol), the session ID, the identifier of the source UE (such as the Subscription Concealed Identifier, a.k.a. SUCI in 5G), the transmitted length (bits), the number of packets, etc.

The session information collection module runs continuously in the system, whether in an emergency or not. The collected information is aggregated and reported to the attack parameter estimation module. Then, the attack parameter estimation module estimates the key characteristic parameters of the attack behavior according to the decision-making requirements. The parameters that need to be estimated may be the size of the attack session (total number of packets/bits), the average duration, the packet arrival rate, etc. At the beginning of an emergency defense, the defender may not have knowledge of the characteristics of the attack behavior, so this module is critical for optimizing the defense strategy. In DDoS attacks, the attack behavior of bots is usually similar under the unified instructions of the command and control (C & C) server. This fact is reflected in the similarity of attack session characteristics. Therefore, it is feasible to rapidly estimate attack behavior parameters using dense sampling over a large number of concurrent attack sessions. Finally, the defense strategy optimization module optimizes the defense strategy by integrating the information obtained from various sources, including the estimated attack parameters, the feedback from the victim and the trust values from the trust management infrastructure deployed in the satellite network. The updated defense strategy can be redistributed to the CPs for execution. This process results in the formation of a complete optimization loop from observation and orientation to decision and action. Since the estimation of attack parameters is usually inaccurate due to the limitation of the number of observations in the beginning, this closed-loop optimization process is very important for improving decision-making efficiency.

Note that we have introduced a blockchain-based identity and trust management infrastructure in the proposed architecture. The blockchain is deployed at satellites and is used to record the historical malicious communication behaviors of each UE. This infrastructure provides real-time trust values of suspicious UEs to LCs based on a trust evaluation algorithm. Considering that a trust management system must be established based on the unique digital identity of each UE, the infrastructure will also maintain a digital identity system. Accordingly, each LC deploys a mapping list from the subscriber identity to the digital identity of the accessed UE to request the trust values of suspicious UE devices from the blockchain for attack detection. Rapid movement of vehicle bots may lead to changes in the access network domain. Deploying a trust management system on a satellite network can facilitate access to trust values anytime and

anywhere while avoiding delay and privacy issues that may be caused by cross-domain handovers.

Considering that the attack may be launched from multiple control domains simultaneously, horizontal strategy collaboration is also required between LCs. This collaboration is achieved through the sharing of defensive strategies. Strategy sharing can enable LCs that have just switched to an emergency defense state to quickly execute optimized defense strategies rather than starting from scratch. LC can also speed up its strategy optimization process by directly adopting more convincing defensive policies based on more observations of attack sessions. In summary, in emergency defense, intradomain collaboration among CPs can be achieved through attack information sharing, and collaboration among LCs is enabled by both trust information sharing and defensive strategy sharing.

The frequency of defensive strategy sharing can be determined by the defender based on the actual security requirements. In fact, the communication costs associated with such strategy interactions between LCs are low (which will be evaluated in detail below), so a higher frequency of strategy sharing means faster strategy optimization. However, if it is less than the arrival interval of attack packets, the LC does not collect enough new information, and strategy sharing becomes meaningless. Therefore, in practical applications, we recommend referring to the attack packet arrival interval to determine the strategy information sharing frequency.

Aiming at the DDoS defense requirements in 6G V2X, the architecture deploys detection algorithms based on access-side control points and optimizes local defense strategies for LCs to realize horizontal collaboration among CPs. The LCs can switch their working states between routine defense and emergency defense to meet defense objectives in different scenarios. By means of information exchange among LCs, global information sharing and wide-area security defense are realized.

B. PROACTIVE DEFENSE DECISION-MAKING METHOD

Proactive defense decision-making in routine scenarios relies on detailed characterization and cost–benefit analysis of the behavioral models of both the attacker and the defender. The traditional security game model (TSGM) cannot meet this demand for the following three reasons [43]. First, DDoS attack defense at the access side is accomplished by the collaboration of multiple CPs, and the TSGM lacks accurate characteristics of the multiagent collaboration effect. Second, the players' action space is high-dimensional and even continuous, and the attacker's action is constrained by the geographical distribution of the bots. However, TSGMs lack these considerations. Different from those of the TSGM, the utility functions of the DDoS game are not simple summations of the utilities on each CP but piecewise and nonlinear functions with respect to the total volume of traffic that reaches the target. Therefore, developing a new multiagent collaborative DDoS game model is the basis of for proactive defense decision-making.

To solve this problem, four main issues need to be considered.

(1) Model selection. Game theory was developed nearly a century ago, and researchers have developed a wide variety of models based on the diverse needs of solving practical problems. Determining which model is best for modeling this decision problem requires careful consideration. Considering that the defender has limited security resources that preclude full security coverage of important potential targets at all times, optimizing the allocation of limited security resources to maximize defensive utility is the ultimate goal of the defender. Usually, the defender develops a defensive strategy first, after which the attacker responds to it. This is in line with the framework of Stackelberg games [46]. Therefore, we believe that the Stackelberg game model is one of the best choices in this scenario. First, this model can give the defender (leader) the initiative of equilibrium selection so that the dominant strategy for the defender can be selected to achieve the goal of deterring the attacker. Second, the equilibrium utility of the Stackelberg game is not inferior to the Nash equilibrium and is even better in some cases [47]. Third, the solution to this model has been well studied, which can guarantee that the established model can be solved, especially when the action space and utility functions are complex.

(2) Model formulation. After the model is selected, it is necessary to formulate the problem in combination with the actual defense scenario. The parameters that need to be formalized include the action space, strategy, and utility functions. The formulation of utility functions is the most difficult. We need to model the effect of defense measures at each CP and model the arrival behaviors of both normal traffic and attack traffic at the victim. The effect of defensive measures varies according to the detection method, and a simpler approach is probabilistic modeling. Assuming that the detection rate of attack traffic is stable or follows a certain distribution, the packet pass rate of attack traffic can be analyzed and modeled. The packet pass rate of the attack traffic is the proportion of packets that successfully reach the victim in the total number of attack packets. There are many modeling methods for the continuous-time packet arrival process. The most commonly used model is the Poisson process [48]. Note that the traffic arriving at the target includes both normal traffic and attack traffic. The packet arrival process characteristics of the two are different and cannot be modeled by the same model. On this basis, the equilibrium strategy solving problem can be transformed into a conventional optimization problem.

(3) Model solution. The solution of strong Stackelberg equilibria has been shown to be NP-hard [49]. There are many sophisticated polynomial time solution methods for the TSGM, but most of them employ the Harsanyi transformation in discrete action spaces, consequently, these methods

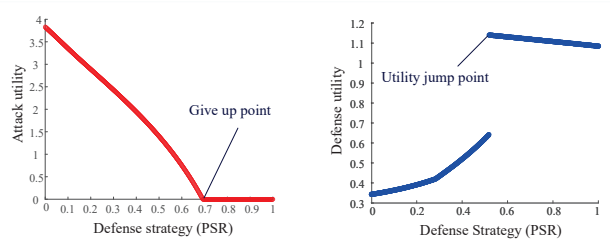

FIGURE 9. An example of the utility functions for attackers and defenders. For the setting of relevant parameters, please refer to Section V-C and reference [43].

cannot be applied to DDoS game scenarios. In recent years, several researchers have attempted to use new technical tools, such as neural networks, to solve the leader's strategy of Stackelberg games in a continuous action space [50]. However, when training a neural network, a large number of training samples need to be collected in advance, and the convergence of the equilibrium strategy is relatively slow, consequently, the trained network cannot quickly adapt to dynamic changes in the security situation. In fact, the solution of DDoS game equilibrium is expected to be achieved by a heuristic algorithm. Since the investment of both attack and defense resources obeys the law of diminishing marginal utility, the utility functions are convex in the nonlinear part with respect to the component of the action profile on each CP. Based on this observation, a heuristic algorithm can be designed to quickly solve this equilibrium [43]. The equilibrium we expect is the threshold of defense resource investment that the attacker gives up because the attack is unprofitable. If the defender detects DDoS traffic regardless of the cost, the attack traffic will be detected and blocked with probability 1, and the attacker will certainly suffer losses. Therefore, the equilibrium we expect must exist in theory. Fig. 9 shows an example of the utility functions at a control point. The left panel shows the change in the attack utility (under the optimal strategy), and the right panel shows the defense utility. As shown in the figure, around $PSR = 0.69$, the payoff of the attacker launching the optimal attack reaches 0, where the attacker has better to give up the attack. At the same point, the defender achieves a gain in efficiency because the attacker gives up. This point is the ideal equilibrium that we pursue.

(4) Model generalization. When constructing the Stackelberg game model, we assumed a specific attack and defense scenario. That is, the attacker has a specific target and resource distribution, and the victim has a certain ability to mitigate redundant traffic. However, in practical applications, the resource endowments of each potential participant are not the same. The defender must consider the unspecified ability of the attacker and the victim. This requires the generalization of the model to remove or relax some specific assumptions. After generalization, the model may become simpler and may enable an analytical solution. Executing the equilibrium strategy of the generalized model may cause the defender to lose some defense utilities in some specific scenarios, but it can cope with a wider range of game settings and ensure that the defense utility is always maintained at a high level. Therefore, model generalization is a critical step from mathematical conclusions to practical strategies in DDoS defense.

C. MULTIDOMAIN COLLABORATIVE DDOS DETECTION FRAMEWORK

To achieve efficient defense against DDoS attacks in V2X, we should seriously consider cost–benefit issues. Theoretically, the existing malicious traffic detection algorithms based on edge AI can detect the vast majority of current DDoS attacks with extremely high accuracy and sufficient resources. We need to consider the computational, storage and time costs of these methods. The computational cost determines the deployability of the defense architecture, which involves two main aspects: the computational complexity of the detection algorithms and the scale of the data processing. The time cost, namely, the delay, directly affects the availability of V2X services, especially delay-sensitive services. Corresponding to the calculation cost, the delay also comes from two aspects, i.e., the calculation delay of the detection algorithm and the processing delay of the streaming data. Due to the development of storage technology, the storage cost usually does not impose significant restrictions on the performance of detection algorithms. Therefore, we design a real-time detection framework that considers the optimizations of both computational complexity and the data processing scale.

To ensure real-time performance, we make efforts from the following two aspects. One is to design a lightweight attack traffic detection algorithm, and the other is to reduce the workload of packet processing. The anomaly detection methods based on machine learning are state-of-the-art DDoS detection algorithms. With respect to 6G V2X, the development of edge intelligence is expected to deploy FL models as infrastructure at CPs to perform attack detection tasks [48]. However, real-time detection based on FL still faces the following challenges. First, flow-level features cannot be used due to the feature extraction delay, which limits the detection accuracy of the model. A round of DDoS attacks usually persists for one flow. The flow-level features cannot be extracted until the flow is complete, making the detection meaningless. Therefore, more fine-grained features, such as features based on packets, flowcells [51], or time windows, must be used. However, the semantic information about the behavior that fine-grained features can reflect is much less than that of flows, and the accuracy of attack traffic detection based on such features may also be limited.

To compensate for the information loss caused by the above limitations, additional sources of information must be used, and lightweight detection methods should be developed to ensure the accuracy of DDoS detection at the access side. We propose a multidomain collaborative DDoS detection

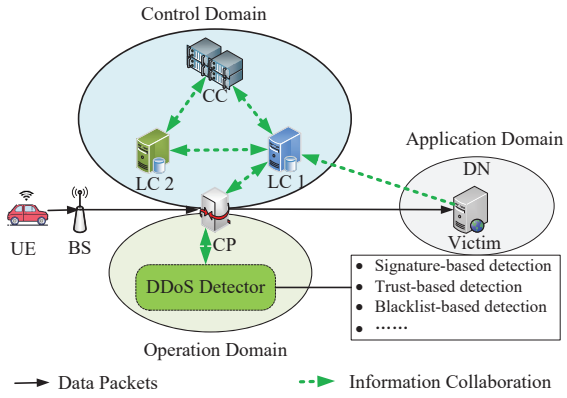

FIGURE 10. **Multidomain collaborative DDoS detection framework.**

framework to integrate multidomain information [52]. In fact, the sources of information at the access side are not fully utilized. We divide the information sources available at the access side into the control domain, operation domain and application domain, as shown in Fig. 10 [52].

The control domain mainly refers to the control plane of the ISP network. Due to their proximity to UEs, the access and movement behavior of UEs can be recorded in the control domain. The LCs can also make full use of the signaling of the ISP network to implement operations such as source address verification.

The operation domain refers to the data plane of the ISP network. Because it directly performs packet forwarding operations, it can extract and record the packet-level features of the session for further detection and can also use other information collection methods, such as packet counters, to estimate the parameters of the attack sessions.

The application domain refers to the data network in which the victims reside. Victims can decrypt attack traffic to obtain more application-layer information about the attack. This information can be fed back to the LCs, helping to improve the detection accuracy. In addition, victims may have some preferences or priorities for DDoS defense, which can also be used as guidelines for access-side defense.

The fusion of multidomain information requires the synthesis of various methods. We recommend considering the following lightweight methods.

(1) Signature-based detection methods use packet-level features only. Although the signature-based algorithm is traditional, it is very efficient at detecting certain known attacks [53]. Many known attack types have anomalies at the packet level. For example, source address spoofing, empty packets, oversized packets, and specific vulnerable port numbers. Through deep packet inspection (DPI), a large number of features at the packet level can be extracted to effectively detect such DDoS attacks. The most harmful reflective DDoS attacks have source address spoofing features, and this method can be used for fast filtering.

(2) Trust-based detection methods. Trust management was first introduced as a kind of malicious behavior detection method in peer-to-peer (P2P) networks. This method requires that the behavior pattern of the object be simple enough to carry out trust evaluation. In recent years, it has been widely used in the IoT, and V2X scenarios are also applicable [54]. The main advantage of using the trust value as an attack traffic detection metric is that it is lightweight. Since trust is a relatively stable trait, it can be computed offline on a back-end server and requested on demand during application. The trust value cannot be used as the only evaluation criterion, and the evaluation results of the current behavior should also be considered.

(3) Blacklist/whitelist-based packet filtering. The blacklist/whitelist technology seems slightly outdated, but it is very practical and efficient to implement. The configuration is simple and flexible. In particular, this approach can support the diversified defense preferences of victims and simplify the calculation process of trust management methods. In recent years, this technology has also been developed and is worthy of being advocated because of limited computing resources at the access side [55], [56].

The three methods presented above are all of linear complexity and can support online detection and collaboration. In practice, to maximize the defense utility, we need to integrate the workflows of various methods into a unified detection framework to ensure the detection efficiency of DDoS attack traffic.

D. SELF-OPTIMIZING PACKET SAMPLING STRATEGY

Packet feature extraction based on DPI is an important information source for online DDoS detection. The packet processing workload of the DDoS defense architecture is an important factor affecting the overall delay of the architecture and directly determines the defense cost. Due to the limited computing power and large traffic scale at the access side, the cost of detecting all inbound packets is too high, and the resulting delay is often intolerable. Therefore, packet sampling becomes a key way to reduce the cost of data processing in the DDoS defense architecture.

There are many packet sampling strategies that can be roughly divided into two categories: probability-based and time-based. For the former, the packet sampling rate (PSR) is a very important index. For the latter, the sampling interval is more important. The specific sampling strategy selection depends on the type of DDoS attacks to be detected. Considering the decreasing trend of DDoS attack duration, some attack sessions may be missed by time-based sampling, and the probabilistic sampling strategy can ensure a sufficiently high detection rate of attack sessions. Therefore, determining the optimal PSR has become the primary issue in optimizing the defense costs.

The optimal PSR is related to the size of the attack session, that is, the number of packets transmitted during the session's lifetime. In the emergency defense scenario,

the defender cannot determine the attack session length at the very beginning. When an attack session is detected, the defender immediately blocks the session to reduce damage, so the session size cannot be directly observed. To solve this problem, we need to realize accurate estimation of the attack session size during the packet sampling detection process. This can be done by setting a packet counter for each session on the CP, marking which packet of the session is being forwarded. When the attack session is sampled, the current value of its packet counter is recorded. Because in most cases, DDoS attack sessions are usually the same size and predetermined by the attack instructions [1], and the arrival time to the CP is independent due to route differences, the counter's reading of detected attack sessions can be approximated as random samplings from multiple discrete uniformly distributed populations. We need to estimate the bounds of the discrete uniform distribution based on the results of multiple independent and identically distributed random samples. This statistical problem can be solved using standard statistical methods. We have discussed this in detail in our recent work [52]. The minimum-variance unbiased estimator (MVUE) of the session size (denoted by $\hat{L}$) based on the observations from packet counters of attack sessions can be formulated as

$$\hat{L} = X(t) + \left[\frac{1}{\left(1 + \frac{1}{X(t)-1}\right)^{t} - 1} \right], \tag{1}$$

where t is the number of sampled sessions, $X(t)$ is the maximum order statistic of the readings from packet counters, and $[\cdot]$ is the round operator to ensure that the output result is an integer.

Since the second term in (1) is mostly 0 when t is large, we usually use the asymptotically unbiased estimator $\hat{L} \approx X(t)$ for simplicity. Let us analyze the confidence interval for this estimator. The distribution function of $X(t)$ is

$$F(X(t) = k) = \frac{(k-1)^t}{L^t} \tag{2}$$

where L is the true value of the attack session size, and $1 \leq k \leq L$ is an arbitrary integer. We assume that the required confidence level is $1 - \alpha$, then the upper and lower bounds of a symmetric confidence interval can be formulated as

$$CI_u = \left[\frac{X(t) - 1}{\sqrt[t]{\alpha/2}} \right] + 1, \tag{3}$$

and

$$CI_l = \left[\frac{X(t) - 1}{\sqrt[t]{1 - \alpha/2)}} \right], \tag{4}$$

where CI_u is the upper bound and CI_l is the lower bound.

[1] If a sophisticated attacker changes the attack mode such that the size of attack sessions follows a certain distribution, we need to estimate the distribution function. See [57], [58] for more details.

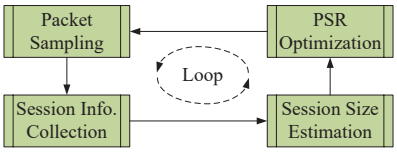

FIGURE 11. Loop of packet sampling strategy optimization.

Based on the estimation of the attack session size L, the optimal PSR can be formulated as [52]

$$p_0 = 1 - (1 - \alpha)^{1/\hat{L}}, \tag{5}$$

where α is the expected detection rate of attack sessions.

Based on the estimation of the attack session size, the optimal PSR can be derived to optimize the defense cost. However, estimations can be biased which may affect the cost minimization. To solve this problem, the estimated session size can be further optimized using re-estimation based on the new observations after each round of sampling, and ultimately converges to the optimal value. Since attack sessions are immediately blocked after being sampled, the newly collected samples and historical samples are also independent of each other, so the convergence process of this PSR can be guaranteed by the law of large numbers. This method forms a self-optimizing procedure for the packet sampling strategy, as shown in Fig. 11.

To start the optimization loop, the initial sampling rate can be initialized as the proactive defense sampling strategy in the routine defense scenario. Since the self-optimization procedure usually converges quickly, the defender has the flexibility to choose an appropriate initial sampling rate, such as 5%, based on the amount of remaining computing resources. In applications, to detect attack sessions as early as possible, we recommend that the initial sampling rate be appropriately increased as long as the resources are affordable. To stop the loop after PSR convergence, it is necessary to detect the change in the PSR in each strategy update. If the improvement is negligible in several successive updates, the strategy optimization process can be terminated.

This section provides examples of a quick start and optimized defense strategy in an emergency defense scenario. In a real defense scenario, the optimized target quantity may not be the PSR. However, the methodology of rapidly estimating attack parameters by observing a large number of attack sessions is still applicable and is an important example of time-for-space engineering thinking.

V. Performance Evaluation

To verify the performance of the proposed access-side DDoS defense architecture, we present a set of simulation results. We verify the performance of our proposed architecture in three aspects, namely, computational cost, communication efficiency, and detection performance. The software simulation platform used in this study is Matlab 2016a. The performance parameters of the hardware platform are:

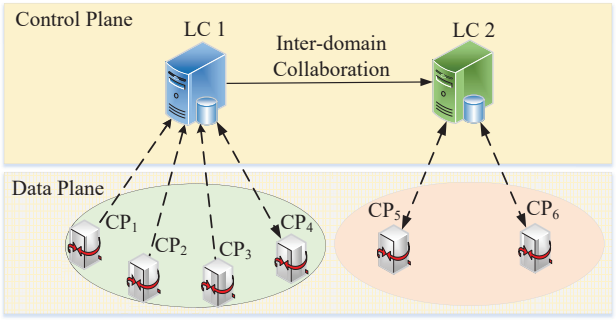

FIGURE 12. Network topology employed in the simulations.

Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz, 16.0 GB of RAM and Windows 10 64 bit operating system.

The network topology employed in the simulations is shown in Fig. 12. We set 2 local controllers in the network, which are denoted as LC1 and LC2. In LC1, there are 4 CPs, namely CP1, CP2, CP3 and CP4. In LC2, CP5 and CP6 are deployed. There are communication links between CPs in the same local control domain (not marked in the figure), and LC1 and LC2 collaborate through inter-domain links. The software simulation platform used in this study is Matlab 2016a. The performance parameters of the hardware platform are: Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz, 16.0 GB RAM and Windows 10 (64 bits) Operating system.

We set a set of concurrent DDoS attack sessions passing through the control points, including 1000 continuous normal sessions and 10 attack sessions when the simulation began. To simulate the actual attack scenario, we assume that the packet counters of the 10 attack sessions are set randomly at the beginning when the defense process is activated. Assuming that the vehicular bots are sending attack packets at an average rate of 10 packets per second (pps) and the total session size is set to 50 packets by the attacker, thus the total duration of an attack session is 5 seconds. During the first 3 seconds of the simulation, a new batch of attack sessions is launched every 0.1 seconds. The number of new attack sessions in each batch is determined according to a Poisson process with a parameter of 5. Thus, all attack sessions ended in 8 seconds. We assume that our defensive goal is to detect the attack with a 99% probability before the session ends. The initial PSR at each CP was set to 0.05. The defense strategy we use in this simulation is detailed in Sections III and IV for emergency defense scenarios. We estimate the attack session size and determine the optimal PSR based on the packet inspection results in previous sampling periods. We take the average number of packets that need to be inspected to detect an attack session as the metric for evaluation. This metric well reflects the balance of defensive costs and benefits.

A. COMPUTATIONAL COST

To evaluate the computational cost of the proposed architecture, we first analyze its computational complexity, and then distinguish two types of scenarios including intra-domain collaboration and inter-domain collaboration to measure the computational cost of emergency DDoS traffic detection by simulations.

1) Computational cost analysis

In an emergency defense scenario, the computational cost of the access-side defense architecture mainly comes from the DPI and defense strategy calculations. Since the strategy calculation mostly uses information from IP headers, which can be extracted in conjunction with packet parsing by the associated network element during the packet forwarding process, the defense architecture does not need to introduce additional computational overhead.

The DPI to a single packet can be completed in constant time, so the complexity of DPI is $O(pN)$, where p is the PSR and N is the total number of packets forwarded in each sampling period. The time complexity of the attack session size estimation and sampling strategy calculation is $O(1)$ according to (1) and (5). Since trust values of UEs can be calculated offline on remote cloud centers, the calculation of packet filtering strategies based on trust values and blacklists involves only a retrieval process in a given list, and its time complexity is sub-linear. If a machine learning-based approach is used to make packet filtering decisions, the complexity of policy generation is determined by the learning algorithm itself, which has nothing to do with the architecture proposed in this paper. Therefore, the computational cost of our proposed access-side defense architecture is linear in complexity.

In a routine defense scenario, calculating the defensive strategy requires solving the game equilibrium, but the strategy can be calculated offline in advance and does not need to be adjusted in the short term, so its complexity is not considered here to evaluate the computational cost of the security architecture [43].

2) Intra-domain collaboration

Next, we evaluate the computational cost of using DPI to detect malicious traffic at the access side. Since the cost of implementing DPI for a single packet is constant, we evaluate the computational cost of detection by the total number of packets inspected, and reveal the important role of collaboration in optimizing inspection costs from both intra-domain and inter-domain perspectives.

First, we investigate the collaboration effect on defense efficiency using intra-domain collaboration. We take LC1 as an example. In the simulations, CP1, CP2 and CP3 work independently to detect and optimize the defense strategy, while CP4 (which we denote as Co-CP) executes the collaborative defense strategy derived from their public LCs. We calculate the average detection cost (i.e., the number of inspected packets) of one attack session in the simulations.

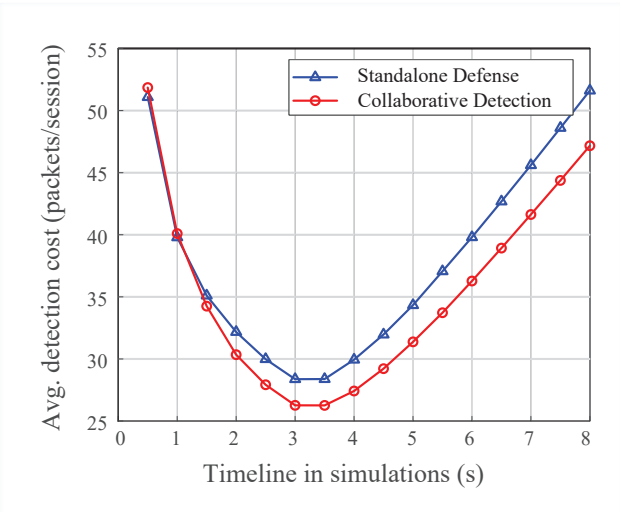

FIGURE 13. Average detection costs of attack sessions in intra-domain collaboration.

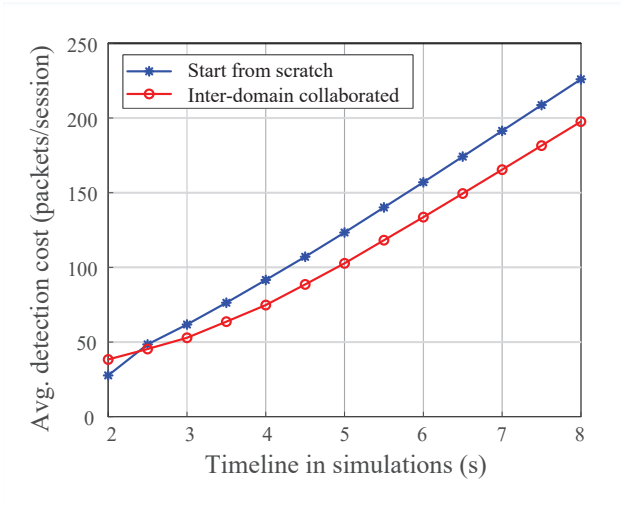

FIGURE 14. Average detection costs of attack sessions in inter-domain collaboration.

The results obtained by averaging 100 random simulations are shown in Fig. 13. The red curve illustrates the average detection cost of CP4 implementing the collaboration strategy and the blue curve refers to the average detection cost of other standalone CPs. The costs of attack detection first decrease and then increase.

In the first 3 s, because new attack sessions continue to arrive, the proportion of total attack sessions in the traffic continues to increase so that the cost of detecting attack sessions continues to decrease. After 3 s, as the attack sessions are gradually detected and blocked, the number of attack sessions remaining in the traffic continues to decline without new arrivals, and the detection cost of a single session increases. From a numeric perspective, the average detection cost in the first 1 s in collaborative mode (CP4) is comparable to that in standalone mode (CP1-CP3), or even slightly greater, because the PSR at CP4 has converged and is significantly lower. The rapid optimization convergence of the defense strategy makes the cost advantage increasingly significant, while the standalone mode leads to a higher detection cost due to oversampling before the defense strategy converges. This result verifies the importance of intra-domain collaboration in reducing defense costs.

3) Inter-domain collaboration

To verify the effect of inter-domain strategy collaboration on the computational cost, we designed another set of simulations. This time we focused on LC2. The background traffic settings are the same as those of the CPs in LC1. Due to the mobility of vehicle bots, we assume that at t=2 s, 60 active bots move from LC1 to LC2 while continuing to send attack traffic. Among them, 30 bots access CP5, and the other 30 bots access CP6. The 6G handover system transfers the corresponding session information to the new CPs. For CP5, we set its initial defense strategy as the optimal value of LC1 at time t=2 s through the inter-domain collaboration mechanism and then carry out its own strategy optimization loop. CP6 does not adopt an inter-domain collaborative optimization strategy but directly starts from scratch. We also examine the average session detection cost of CPs in both scenarios. Fig. 14 shows the average results of 100 simulations.

The defense cost of CP5 is slightly greater than that of CP6 in the initial stage because the PSR at CP5 converges more quickly due to inter-domain collaboration, making its detection rate slightly lower than that of CP6 in the first 2.5 s. From $t = 2.5$ s on, inter-domain collaboration has a significant cost advantage. CP5 has a lower average detection cost for sessions due to the use of a more optimized defense strategy. The cost advantage even increases further as the number of attack sessions decreases. These results show that inter-domain collaboration can better cope with bot mobility in V2X during emergency defense against attack events and prevent newly involved CPs from learning defense strategies from scratch, thus further improving defense efficiency.

B. COMMUNICATION EFFICIENCY

To demonstrate the bandwidth efficiency of the new architecture, we designed two sets of simulations. The first set evaluates the bandwidth resource consumption introduced by the defense architecture, which reflects the communication cost of defense. The second set evaluates the total network bandwidth consumption caused by attack traffic propagation after the defense architecture is deployed, which reflects the benefits of access-side defense.

We take LC1 as an example. We assume that IPv6 is used as the network layer protocol in collaboration. The length of the attack session information description is 248 bits each [52], including 232 bits for basic information and 16 bits for the packet counter. We take the PSR as the defense strategy, and the message length is set to 8 bits. The trust value is

set to 8 bits per UE. The blacklist provided by the victim consists of 1000 IPv6 addresses with 128 bits each, which are first sent to the LC and then distributed by the LC to the CPs. The attack packet length was 1 kb. Other parameters of our simulation are set as described above.

1) Bandwidth cost

The bandwidth consumption of the proposed architecture comes from two aspects: one is session information collection, that is, the CPs send description information of attack sessions to LC1, and each attack session has a triplet [52]; The second is defense strategy distribution, that is, LC1 sends defense strategy related information to the CPs, including the optimal PSR, blacklist, and trust value of the accessed vehicles.

We use the online ML-based architecture for comparison. One representative example of such methods is [39]. In line with our ideas in this paper, LEDEM proposed in [39] takes the switches as the control points in SDN and the LC as the defense strategy engine. The switches periodically send the captured network traffic data to the LC. The LC performs online machine learning methods, generates defense strategies, and then sends them back to the corresponding switches in terms of flow entries to perform traffic control actions. This architecture is similar to ours, except that our CPs are deployed at the access side, while the CPs in LEDEM are spread across the network. As we will show below, the bandwidth overhead of these two architectures is quite different.

For ease of comparison, we consider the 4 CPs of LC1 as switches in LEDEM and let LEDEM take the same packet sampling strategy as our architecture in data capture. The packet length of session description information is set to be 568 bits, including 248 bits of session information and 40bytes (320 bits) of IPv6 packet header. In LEDEM, the length of flow entries distributed by LC is set to 98 bytes according to Openflow v1.3 or newer, including the Match Field 32bits, Priority 4bytes, Counters 8 bytes, Timeout 8 bytes, Instruction 2 bytes, Cookies 8 bytes and IPv6 header 40 bytes. Other parameter settings and the attack traffic generation method remains the same as above, except that the number of benign sessions increases from 1000 to 10000, increments by 1000. We collected the total bandwidth consumption of the two architectures in the data/feature collection and defense strategy distribution processes in 100 random simulations, and the average results are shown in Fig. 15.

In general, the bandwidth overhead of by our proposed architecture is much lower than that of online ML-based approaches. As the scale of background traffic increases, the bandwidth resources consumed by online ML generally increase linearly, because the detector forwards all the sampled packets to LC1 for further detection. In our architecture, the function of malicious traffic detection is moved forward to

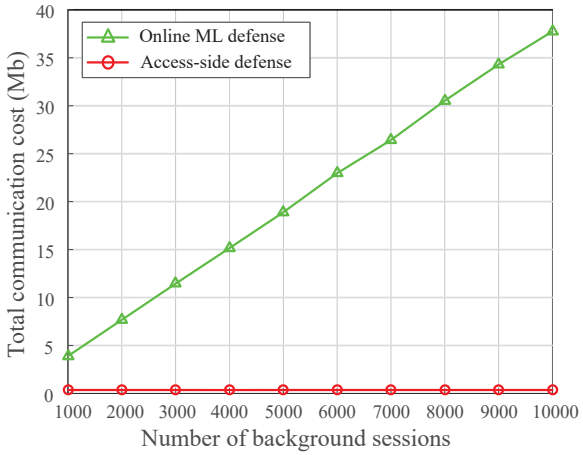

FIGURE 15. The bandwidth consumption under our defense architecture and online ML-based architecture.

CPs, and CPs only need to transmit the detected malicious session information to LC1 for defense strategy optimization. Therefore, the communication overhead for data forwarding in our architecture is related only to the number of malicious sessions, not the size of the background traffic. This observation is important because the vast majority of sessions are benign in real network traffic, while forwarding packets of benign sessions is an unnecessary consumption of bandwidth resources. Our architecture avoids this expense, which greatly saves bandwidth resources. It should be noted that the curves in Fig. 15 show slight fluctuations due to randomness and changes in the number of defense strategies from LC1 to CPs. Due to the magnitude difference in the values between the two sets of results, such fluctuations are subtle in the figure. In summary, compared with online ML, our architecture not only saves significant bandwidth resources, but is also robust to the background traffic scale.

2) Bandwidth benefits

In this set of simulations, we count the total bandwidth consumed by the attack traffic under the proposed architecture and the traditional server-side defense architecture in LC1. We increase the number of route hops between the bot and the victim from 2 to 10 to adapt to different attack paths. In the access-side defense, the bandwidth consumption comes from three parts: collaborative information exchange, strategies provided by the LC, and missed attack packets. In the server-side defense, the bandwidth cost is caused by the attack traffic propagation. The average results of 100 random simulations are shown in Fig. 16.

In both defense architectures, the total bandwidth consumed by the attack increases linearly with the average hop count. The bandwidth consumption under server-side defense increases rapidly with the number of routing hops of attack traffic. In contrast, the bandwidth consumption increases

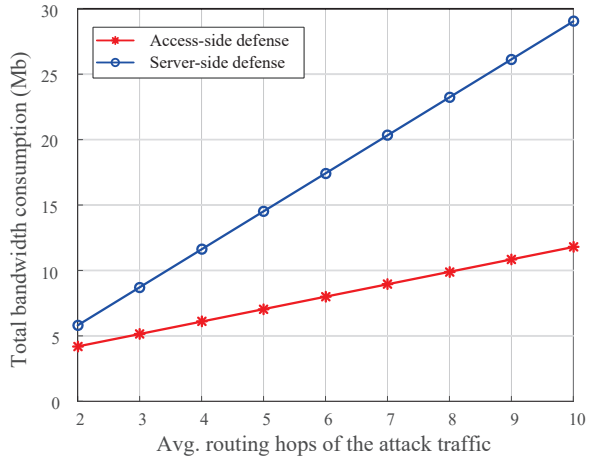

FIGURE 16. The bandwidth consumption of attack traffic after deploying access-side defense and server-side defense.

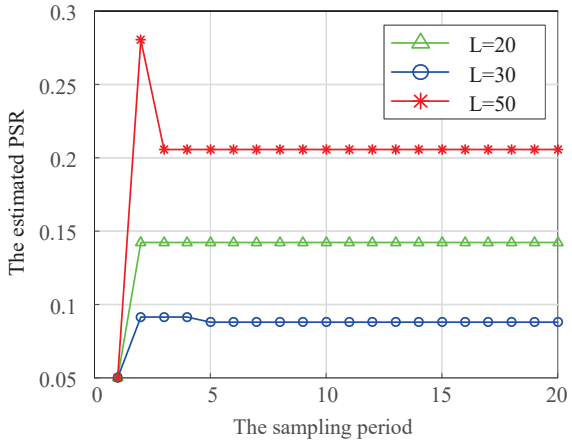

FIGURE 17. The convergence of PSR in the defense strategy optimization.

very slowly under the access-side defense architecture. The reason is that the communication overhead caused by black-list transmission and missed attack packet propagation is positively linear with respect to the hop count. In general, the total bandwidth consumption under the access-side defense architecture is much lower than that under the server-side defense architecture, because our architecture blocks the vast majority of attack traffic at the network entrance, while the introduced cost is very low. These results further verify the great advantages of the access-side defense architecture.

C. DEFENSIVE PERFORMANCE

We first examine the convergence of the optimal defensive strategy, and then distinguish between routine defense and emergency defense scenarios to evaluate the performance of the proposed access-side defense architecture.

We follow the previous defense scenario settings and consider three attack session sizes, namely $L = 20$, $L = 30$ and $L = 50$. We use Eq. (1) to estimate the session size and examine the convergence of the PSR with the sampling process. The initial PSR is set to 0.05. The average results of 100 random simulations are shown in Fig. 17.

It can be seen from the results that although the initial value of PSR is small, the convergence speed is fast. For all three typical session sizes, the PSR generally converges to its optimal value within about 5 sampling periods. This is due to the large number of DDoS attack sessions, even if the PSR is low, a significant number of attack sessions can be sampled in each sampling period, which provides new information for session size estimation and can quickly optimize the PSR. These results show that our proposed optimization loop for defense strategies has high efficiency. Detailed discussions can also be found in our recent work in [52].

1) Routine defense

In the routine defense scenario, the goal of defense is to deter the attacker with the maximum defense utility. Our proposed architecture adopts a security game model to derive the optimal defense strategy at the equilibria, and then executes the strategy statically. Therefore, the defense utility is the most important metric of defensive performance.

To verify the superiority of access-side defense, we compared it to centralized defense deployed at the server side. For details on the game model adopted by the access side defense architecture, please refer to our previous work [43]. For server-side defense, we adopt the traditional Stackelberg security game (SSG) model, as described in [46]. This model deploys CPs around the victim server, and the defense strategy is also random sampling and packet inspection. The difference with our model is the lack of collaboration among multiple CPs. We denote our new model "D-SSG" and the server-side model "C-SSG". We consider LC1 and set the background traffic load on the four CPs as $n_1 = 1\times10^8$ pps, $n_2 = 6\times10^7$ pps, $n_3 = 4.8\times10^7$ pps and $n_4 = 3\times10^7$ pps. Moreover, we set the number of attack sessions forwarded by these CPs as $A_1 = 4,000$, $A_2 = 3,000$, $A_3 = 5,000$ and $A_4 = 2,000$. We take the distributed reflection denial of service (DRDoS) attack as an example and increase the reflection factor from 1 to 10. The length of the attack packets is set to 1 kb. The other model parameters are set the same as [43]. After implementing 100 random attack simulations, we compared the average defensive utilities as shown in Fig. 18.

The results show that the defensive utilities of both models decrease as the reflection factor increases. The overall utility of the D-SSG model is significantly better than that of the C-SSG. This is because the D-SSG model can flexibly adjust the defense strategy at each CP at the access side according to the scale of attack traffic and background traffic, to maximize the overall defense utility. However, C-SSG does not have this flexibility. In other words, D-SSG has

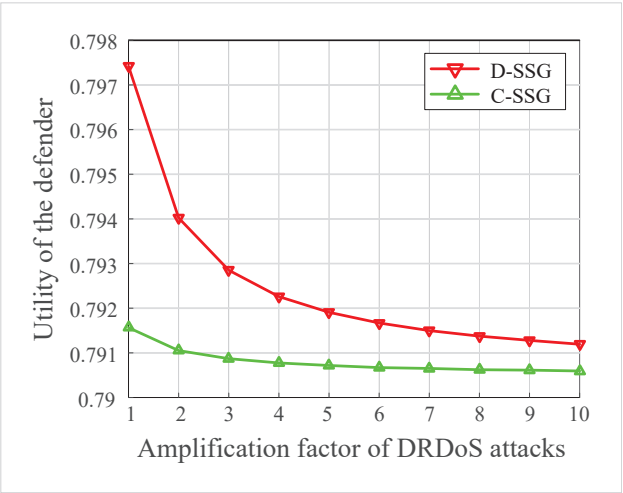

FIGURE 18. **Average defense utilities under centralized and distributed security game models.**

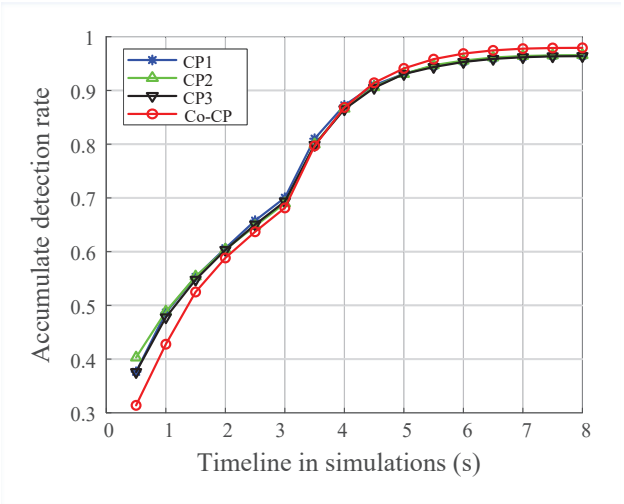

FIGURE 19. **Accumulate detection rates of attack sessions on CPs.**

a higher dimension of defensive action space that enables a more flexible strategy configuration. This advantage is due to the access-side deployment of CPs. Moreover, with increasing of the reflection factor, the advantage of D-SSG gradually decreases. This is because the damage caused by a single attack packet after breaking through the defense line increases dramatically, making the attack packet pass rate dominate the defense utility, thus weakening the importance of defense strategy optimization.

2) Emergency defense

In the emergency defense scenario, the goal of defense is to reduce the communication and computational costs while ensuring the expected detection rate of attack sessions. In previous simulations, we have demonstrated that optimizing defense strategies through collaboration can reduce defense costs. Now we examine whether this detection cost reduction comes at the expense of detection performance. Note that we set a target detection rate of 99% and developed a defense strategy accordingly. The simulation settings are the same as those in Section A. The average results of 100 random simulations are shown in Fig. 19.

The detection rate curves of CP1, CP2 and CP3 almost overlap with each other after eliminating the influence of random errors using the average. With an attack session size of $L = 50$, the converged optimal packet sampling strategy of the defender is $PSR = 0.088$, i.e., 8.8%, which is sufficiently low compared to full sampling. At CP4, since the PSR converges more quickly due to collaboration for the same reasons as in Fig. 14, the accumulated detection rate is slightly lower than those of the other CPs in the first 3 s. The four curves all jump around $t = 3$ s because there are new arrivals of attack sessions every 0.1 s in the first 3 s, so that the total number of attack sessions reaches the peak at $t = 3$ s. Subsequently, no new attack sessions arrive, and the curve tends to be flat. The detection rates of attack sessions at the four CPs ultimately reached 98.5% or more, which is slightly lower than 99%. This is because the target detection rate is set for full sessions, while at the beginning of the simulations we set 10 initial sessions in progress whose actual sizes are less than 50 packets. In general, the accumulative detection rate at CP4 reached or even exceeded the average level of the other three CPs. These results indicate that collaboration does not lead to a loss in detection performance while reducing costs.

In summary, a series of simulation results show that the proposed architecture can greatly reduce the defense cost while ensuring the detection rate. In particular, the defense cost can be further optimized through intra-domain and inter-domain collaboration. Moreover, due to the location advantage of access-side defense, the network bandwidth efficiency of access-side defense is significantly better than that of traditional server-side defense.

VI. Open Issues

In this article, a high-level architecture, collaboration mechanism and key technologies of an access-side DDoS defense architecture are proposed. There are still some open issues to be studied in the implementation of access-side DDoS defense. Some of them are listed below.

- Security of edge AI. With improvements in the intelligence of in-vehicle systems, many AI models have been integrated, and new technologies such as few-shot learning and transfer learning will be further applied. To speed up the training process, the required training samples are greatly reduced, while the quality requirements of the training data increase. The access-side defense architecture focuses on network layer security, and the semantic information of packets in the application layer is not inspected. Therefore, the current access-side defense architecture cannot distinguish abnormal

training data samples from normal ones. Therefore,it cannot defend against attacks such as data pollution and poisoning that specifically target AI models, as well as against backdoor attacks [59]. How to integrate the defense capabilities of application-layer AI models under the premise of privacy preservation is another issue that needs to be discussed. Fortunately, the application of adversarial machine learning and federated learning techniques in edge computing scenarios has achieved many remarkable results [41], and it is expected to become a key way to solve these problems in the future.

- In-vehicle DDoS attacks. With the increase in the computing power of vehicles, the demand for long-distance communication will gradually weaken. Autonomous driving can be achieved through local environmental awareness, small-scale collaboration and satellite navigation systems. DDoS attacks on sensors, operating systems and control systems in vehicles could become the main threats to road safety [60]. On the other hand, the number of on-board terminals and sensors is likely to increase further, making it possible for attackers to launch DDoS attacks using intra-vehicle devices only. Therefore, the battlefield of DDoS attacks may move from the data network to vehicles or even vehicle components. How to defend against such attacks in vehicles and maintain collaboration performance without overloading signaling channels is an open problem. In such cases, it may be necessary to deploy a simpler local controller into the vehicle, which is responsible for overall vehicle safety management. Vehicle-vehicle collaboration can be achieved through edge nodes to share attack information and defensive strategies.
- Interoperability and inter-domain access. As applications based on vehicle intelligence flourish, platoons of connected vehicles can communicate with each other through a dedicated short range communication (DSRC) network, and realize cooperative adaptive cruise control (CACC) and other intelligent applications [61]. In these scenarios, frequent interoperability among intelligent vehicles increases the risk of DDoS attacks within platoons, bypassing the access network's defense structure. Hence, complementary security mechanisms are necessary. Strengthening mutual certification and establishing a trust management system between vehicles is a common approach [23]. In large-scale 6G networks with distributed control architectures, controllers may not promptly perceive and receive attack information, especially in cross-control domain access. This delay in emergency defense reactions can be exploited by attackers for short-term, high-frequency attacks. Strengthening network layer access management and adopting a zero-trust architecture for wide area networks are viable solutions [33]. In addition, Additionally, blockchain-based cross-domain information sharing services will play a vital role in facilitating inter-domain collaboration.

VII. Conclusion

The rapid advancement of 6G communication technology will expand traditional V2X communication scenarios and introduce more sensors and new terminals. While these additions broaden the V2X network scale, they also increase the potential for severe DDoS attacks. Consequently, DDoS attacks will emerge as a major threat to V2X security in the 6G era. To effectively counter DDoS attacks in 6G V2X, we have proposed an access-side DDoS defense architecture based on a thorough analysis of defense requirements and challenges. By deploying multiple control points at the network edge and establishing distributed collaboration among them, our architecture establishes a seamless defense surface to block attack traffic from infiltrating V2X. To enhance defense efficiency, we have addressed key technical issues such as proactive defense decision-making, multi-domain collaborative detection methods, and self-optimized packet sampling strategies, proposing several potential solutions. We have validated the advantages of our architecture in terms of computational cost, communication efficiency and defensive performance, demonstrating its superiority compared to traditional solutions. We have also discussed open issues for future application of our proposed architecture.

ACKNOWLEDGMENT

This work was supported in part by the National Key R&D Program of China under Grant 2020YFA0711301, in part by the National Natural Science Foundation of China (Grant No. 62201605, U22A2002, 62341110), in part by the Suzhou Science and Technology Project, and in part by the King Abdullah University of Science and Technology Research Funding (KRF) under Award ORA-2021-CRG10-4696.

REFERENCES

[1] J. He, K. Yang, and H. H. Chen, "6G Cellular Networks and Connected Autonomous Vehicles," *IEEE Netw.*, vol. 35, no. 4, pp. 255–261, 2021.
[2] W. Feng, Y. Wang, Y. Chen, N. Ge, and C.-X. Wang, "Structured satellite-UAV-terrestrial networks for 6G Internet of Things," *IEEE Netw.*, pp. 1–8, 2024.
[3] M. Noor-A-Rahim, Z. Liu, H. Lee, M. O. Khyam, J. He, D. Pesch, K. Moessner, W. Saad, and H. V. Poor, "6G for Vehicle-to-Everything (V2X) Communications: Enabling Technologies, Challenges, and Opportunities," *Proc. IEEE*, vol. 110, no. 6, pp. 712–734, 2022.
[4] H. Mun, M. Seo, and D. H. Lee, "Secure Privacy-Preserving V2V Communication in 5G-V2X Supporting Network Slicing," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 14 439–14 455, 2022.
[5] Z. A. Biron, S. Dey, and P. Pisu, "Real-Time Detection and Estimation of Denial of Service Attack in Connected Vehicle Systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3893–3902, Dec. 2018.
[6] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems VANETs and IoV," *Ad Hoc Netw.*, vol. 61, no. 2017, pp. 33–50, 2017.
[7] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," *Proc. IEEE*, vol. 103, no. 1, pp. 14–76, 2015.
[8] S. Simpson, S. N. Shirazi, A. Marnerides, S. Jouet, D. Pezaros, and D. Hutchison, "An Inter-Domain Collaboration Scheme to Remedy DDoS Attacks in Computer Networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 15, no. 3, pp. 879–893, 2018.

[9] B. Rashidi, C. Fung, and E. Bertino, "A collaborative ddos defence framework using network function virtualization," *IEEE Trans. Inf. Forensic Secur.*, vol. 12, no. 10, pp. 2483–2497, 2017.

[10] Y. Zhou, G. Cheng, and S. Yu, "An SDN-Enabled Proactive Defense Framework for DDoS Mitigation in IoT Networks," *IEEE Trans. Inf. Forensic Secur.*, vol. 16, pp. 5366–5380, 2021.

[11] D. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, D. Niyato, O. Dobre, and H. V. Poor, "6G Internet of Things: A Comprehensive Survey," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 359–383, 2022.

[12] J. Meijers *et al.*, "Blockchain for V2X: Applications and Architectures," *IEEE Open J. Veh. Technol.*, vol. 3, pp. 193–209, 2022.

[13] H. Liu, Y. Zhang, and T. Yang, "Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing," *IEEE Netw.*, vol. 32, no. 3, pp. 78–83, 2018.

[14] C. Liu, W. Feng, X. Tao, and N. Ge, "MEC-Empowered Non-Terrestrial Network for 6G Wide-Area Time-Sensitive Internet of Things," *Engineering*, vol. 8, pp. 96–107, 2022.

[15] Z. Yang, M. Chen, K. K. Wong, H. V. Poor, and S. G. Cui, "Federated Learning for 6G: Applications, Challenges, and Opportunities," *Engineering*, vol. 8, pp. 33–41, Jan. 2022.

[16] Y. Deng *et al.*, "Resource Provisioning for Mitigating Edge DDoS Attacks in MEC-Enabled SDVN," *IEEE Internet Things J.*, vol. 9, no. 23, pp. 24 264–24 280, Dec. 2022.

[17] H. Chai, S. Leng, J. He, K. Zhang, and B. Cheng, "CyberChain: Cybertwin Empowered Blockchain for Lightweight and Privacy-Preserving Authentication in Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 4620–4631, May 2022.

[18] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Communication-Efficient Federated Learning for Digital Twin Edge Networks in Industrial IoT," *IEEE Trans. Ind. Inform.*, vol. 17, no. 8, pp. 5709–5718, Aug. 2021.

[19] W. Guo, J. Xu, Y. Pei, L. Yin, C. Jiang, and N. Ge, "A Distributed Collaborative Entrance Defense Framework Against DDoS Attacks on Satellite Internet," *IEEE Internet Things J.*, vol. 9, no. 17, pp. 15 497–15 510, Sept. 2022.

[20] K. Bian, G. Zhang, and L. Song, "Towards Secure Crowd Sensing in Vehicle-to-everything Networks," *IEEE Netw.*, vol. 32, no. 2, pp. 126–131, March 2018.

[21] W. Feng, Y. Lin, Y. Wang, J. Wang, Y. Chen, N. Ge, S. Jin, and H. Zhu, "Radio Map-Based Cognitive Satellite-UAV Networks Towards 6G On-Demand Coverage," *IEEE Trans. Cogn. Commun. Netw.*, pp. 1–10, 2023.

[22] 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.

[23] G. Li, C. Lai, R. Lu, and D. Zheng, "SecCDV: A Security Reference Architecture for Cybertwin-Driven 6G V2X," *IEEE Trans. Veh. Techno.*, vol. 71, no. 5, pp. 4535–4550, 2022.

[24] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing Vehicle-to-Everything (V2X) Communication Platforms," *IEEE Trans. Intell. Veh.*, vol. 5, no. 4, pp. 693–713, Dec. 2020.

[25] H. Bagheri *et al.*, "5G NR-V2X: Toward Connected and Cooperative Autonomous Driving," *IEEE Commun. Stand. Mag.*, vol. 5, no. 1, pp. 48–54, Mar. 2021.

[26] M. Poongodi, M. Hamdi, A. Sharma, M. Ma, and P. K. Singh, "DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET," *IEEE Access*, vol. 7, pp. 183 532–183 544, 2019.

[27] G. O. Anyanwu, C. I. Nwakanma, J. M. Lee, and D. S. Kim, "Optimization of RBF-SVM Kernel Using Grid Search Algorithm for DDoS Attack Detection in SDN-Based VANET," *IEEE Internet of Things J.*, vol. 10, no. 10, pp. 8477–8490, May 2023.

[28] S. Biswas, J. Mišić, and V. Mišić, "DDoS attack on WAVE-enabled VANET through synchronization," in *IEEE Global Commun. Conf. (GLOBECOM)*, Anaheim, CA, USA, Dec. 2012, pp. 1079–1084.

[29] A. M. Alrehan and F. A. Alhaidari, "Machine Learning Techniques to Detect DDoS Attacks on VANET System: A Survey," in *Int. Conf. Comp. Appl. & Inform. Secur. (ICCAIS)*, vol. 2, Riyadh, Saudi Arabia, May 2019, pp. 1–6.

[30] X. You *et al.*, "Toward 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts," *Sci China-Inf Sci.*, vol. 64, no. 110301, pp. 1–74, 2021.

[31] Z. Zhou, A. Gaurav, B. B. Gupta, M. D. Lytras, and I. Razzak, "A Fine-Grained Access Control and Security Approach for Intelligent Vehicular Transport in 6G Communication System," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 9726–9735, Jul. 2022.

[32] S. Chen, "Dynamic spectrum access and cognitive radio for vehicular communication networks," in *Vehicular Communications and Networks*. Woodhead Publishing, 2015, pp. 127–150.

[33] X. Chen, W. Feng, N. Ge, and Y. Zhang, "Zero Trust Architecture for 6G Security," *IEEE Netw.*, vol. early access, Oct. 2023.

[34] Z. Lu, G. Qu, and Z. Liu, "A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2019.

[35] L. Chen, H. Tang, W. You, and Y. Bai, "A resource-based pricing collaborative approach for mitigating DDoS attack in mobile edge computing," *China Commun.*, vol. 19, no. 12, pp. 160–175, 2022.

[36] Q. He, C. Wang, G. Cui, B. Li, R. Zhou, Q. Zhou, Y. Xiang, H. Jin, and Y. Yang, "A Game-Theoretical Approach for Mitigating Edge DDoS Attack," *IEEE Trans. Depend. Secure Comput.*, vol. 19, no. 4, pp. 2333–2348, 2022.

[37] R. Zhou, Y. Zeng, L. Jiao, Y. Zhong, and L. Song, "Online and Predictive Coordinated Cloud-Edge Scrubbing for DDoS Mitigation," *IEEE Transactions on Mobile Computing*, pp. 1–15, 2024.

[38] Y. Jia, F. Zhong, A. Alrawais, B. Gong, and X. Cheng, "FlowGuard: An Intelligent Edge Defense Mechanism Against IoT DDoS Attacks," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9552–9562, 2020.

[39] N. Ravi and S. M. Shalinie, "Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3559–3570, 2020.

[40] J. Li, L. Lyu, X. Liu, X. Zhang, and X. Lyu, "FLEAM: A Federated Learning Empowered Architecture to Mitigate DDoS in Industrial IoT," *IEEE Trans. Indust. Inform.*, vol. 18, no. 6, pp. 4059–4068, 2022.

[41] Y. Song, T. Liu, T. Wei, X. Wang, Z. Tao, and M. Chen, "FDA^3: Federated Defense Against Adversarial Attacks for Cloud-Based IIoT Applications," *IEEE Trans. Indust. Inform.*, vol. 17, no. 11, pp. 7830–7838, 2021.

[42] Y. Zhou, G. Cheng, Y. Zhao, Z. Chen, and S. Jiang, "Toward Proactive and Efficient DDoS Mitigation in IIoT Systems: A Moving Target Defense Approach," *IEEE Trans. Indust. Inform.*, vol. 18, no. 4, pp. 2734–2744, 2022.

[43] X. Chen, L. Xiao, W. Feng, N. Ge, and X. Wang, "DDoS Defense for IoT: A Stackelberg Game Model-Enabled Collaborative Framework," *IEEE Internet of Things J.*, vol. 9, no. 12, pp. 9659–9674, Jun. 2022.

[44] M. Abdoos, "A Cooperative Multiagent System for Traffic Signal Control Using Game Theory and Reinforcement Learning," *IEEE Intell. Transp. Syst. Mag*, vol. 13, no. 4, pp. 6–16, 2021.

[45] K. Zhang, J. Cao, and Y. Zhang, "Adaptive Digital Twin and Multiagent Deep Reinforcement Learning for Vehicular Edge Computing and Networks," *IEEE Trans. Indus. Inform.*, vol. 18, no. 2, pp. 1405–1413, Feb. 2022.

[46] A. Sinha, F. Fang, B. An, C. Kiekintveld, and M. Tambe, "Stackelberg Security Games: Looking Beyond a Decade of Success," in *Proc. 27th Int. Joint Conf. Artif. Intell. (IJCAI-18)*, Jul. 2018, pp. 5494–5501.

[47] Z. Han, D. Niyato, W. Saad, T. Baar, and A. Hjrungnes, *Game Theory in Wireless and Communication Networks: Theory, Models and Applications*. Cambridge University Press, UK, 2011.

[48] F. Gebali, *Analysis of Computer and Communication Networks*. Springer, 2008.

[49] V. Conitzer and T. Sandholm, "Computing the optimal strategy to commit to," in *Proc. 7th ACM conf. Electr. Comm.*, vol. 7, 2006, pp. 82–90.

[50] N. Kamra, U. Gupta, F. Fang, Y. Liu, and M. Tambe, "Policy Learning for Continuous Space Security Games Using Neural Networks," in *Proc. AAAI Conf. Artif. Intell.*, vol. 32, no. 1, 2018, pp. 1103–1112.

[51] K. He, E. Rozner, K. Agarwal *et al.*, "Presto: Edge-based Load Balancing for Fast Datacenter Networks," *ACM SIGCOMM Comp. Commun. Rev.*, vol. 45, no. 4, pp. 465–478, 2015.

[52] X. Chen, Y. Chen, W. Feng, L. Xiao, X. Li, J. Zhang, and N. Ge, "Real-Time DDoS Defense in 5G-Enabled IoT: A Multidomain Collaboration Perspective," *IEEE Internet of Things J.*, vol. 10, no. 5, pp. 4490–4505, Mar. 2023.

[53] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Commun. Surv. Tutor*, vol. 18, no. 2, pp. 1153–1176, 2016.

[54] B. Pourghebleh, K. Wakil, and N. J. Navimipour, "A Comprehensive Study on the Trust Management Techniques in the Internet of Things," *IEEE Internet of Things J.*, vol. 6, no. 6, pp. 9326–9337, Dec. 2019.
[55] B. Coskun, "(Un)wisdom of Crowds: Accurately Spotting Malicious IP Clusters Using Not-So-Accurate IP Blacklists," *IEEE Trans. Inf. Forensic Secur.*, vol. 12, no. 6, pp. 1406–1417, June 2017.
[56] L. Melis, A. Pyrgelis, and E. D. Cristofaro, "On collaborative predictive blacklisting," *ACM SIGCOMM Comp. Commun. Rev.*, vol. 48, no. 5, pp. 9–20, 2018.
[57] D. Veitch and P. Tune, "Optimal Skampling for the Flow Size Distribution," *IEEE Transactions on Information Theory*, vol. 61, no. 6, pp. 3075–3099, 2015.
[58] F. Murai, B. Ribeiro, D. Towsley, and P. Wang, "On Set Size Distribution Estimation and the Characterization of Large Networks via Sampling," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 6, pp. 1017–1025, 2013.
[59] A. Qayyum, M. Usama, J. Qadir, and A. Al-Fuqaha, "Securing Connected & Autonomous Vehicles: Challenges Posed by Adversarial Machine Learning and the Way Forward," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 2, pp. 998–1026, 2020.
[60] S. Liu, L. Liu, J. Tang, B. Yu, Y. Wang, and W. Shi, "Edge Computing for Autonomous Driving: Opportunities and Challenges," *Proc. IEEE*, vol. 107, no. 8, pp. 1697–1716, Aug. 2019.
[61] Z. Abdollahi Biron, S. Dey, and P. Pisu, "Real-Time Detection and Estimation of Denial of Service Attack in Connected Vehicle Systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3893–3902, 2018.

Xu Chen received his B.S. and M.S. degrees in School of Mathematical Sciences from Peking University in 2009 and 2013, respectively, and the Ph.D. degree in the Department of Electronic Engineering from Tsinghua University in 2022. He has worked as an assistant research fellow for several years. He is now a postdoctoral researcher at Tsinghua University. His research interests include game theory, network management and security.

Wei Feng (Senior Member, IEEE) received the B.S. and Ph.D. degrees from the Department of Electronic Engineering, Tsinghua University, Beijing, China, in 2005 and 2010, respectively. He is currently a Professor with the Department of Electronic Engineering, Tsinghua University. His research interests include maritime communication networks, large-scale distributed antenna systems, and coordinated satellite-UAV-terrestrial networks. He serves as the Assistant to the Editor-in-Chief of CHINA COMMUNICATIONS and an Editor of IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING.

Yunfei Chen (Senior Member, IEEE) received the B.E. and M.E. degrees in electronics engineering from Shanghai Jiaotong University, Shanghai, China, in 1998 and 2001, respectively, and the Ph.D. degree from the University of Alberta in 2006. He is currently a Professor with the Department of Engineering, University of Durham, U.K. His research interests include wireless communications, cognitive radios, wireless relaying, and energy harvesting.

Ning Ge (Member, IEEE) received the B.S. and Ph.D. degrees from Tsinghua University, Beijing, China, in 1993 and 1997, respectively. From 1998 to 2000, he was with ADC Telecommunications, Dallas, TX, USA, where he researched the development of ATM switch fabric ASIC. Since 2000, he has been with the Department of Electronics Engineering, Tsinghua University, where he is currently a Professor and also serves as the Director of Communication Institute. He has published over 100 papers. His current research interests include communication ASIC design, short range wireless communication, and wireless communications. Dr. Ge is a senior member of the China Institute of Communications and the Chinese Institute of Electronics.

You He received the Ph.D. degree from Tsinghua University, Beijing, China, in 1997. He was selected as the Chinese Academy of Engineering Academician in 2013. He is currently a Professor with the Department of Electronic Engineering, Tsinghua University. His main research interests include information fusion, computer vision, and big data technology. Dr. He is a fellow of IET. He won four Second Prizes of the National Science and Technology Progress.