Computers, Materials & Continua
DOI: 10.32604/cmc.2023.032694
Article

Tech Science Press

Central Aggregator Intrusion Detection System for Denial of Service Attacks

Sajjad Ahmad[1], Imran Raza[1], M. Hasan Jamal[1], Sirojiddin Djuraev[2], Soojung Hur[3] and Imran Ashraf[3,*]

[1]Department of Computer Science, COMSATS University Islamabad, Lahore Campus, Lahore, 54000, Pakistan
[2]Department of Software Engineering, New Uzbekistan University, Tashkent, 100007, Uzbekistan
[3]Department of Information and Communication Engineering, Yeungnam University, Gyeongsan-si, 38541, Korea
*Corresponding Author: Imran Ashraf. Email: imranashraf@ynu.ac.kr

Received: 26 May 2022; Accepted: 29 June 2022

Abstract: Vehicle-to-grid technology is an emerging field that allows unused power from Electric Vehicles (EVs) to be used by the smart grid through the central aggregator. Since the central aggregator is connected to the smart grid through a wireless network, it is prone to cyber-attacks that can be detected and mitigated using an intrusion detection system. However, existing intrusion detection systems cannot be used in the vehicle-to-grid network because of the special requirements and characteristics of the vehicle-to-grid network. In this paper, the effect of denial-of-service attacks of malicious electric vehicles on the central aggregator of the vehicle-to-grid network is investigated and an intrusion detection system for the vehicle-to-grid network is proposed. The proposed system, central aggregator–intrusion detection system (CA-IDS), works as a security gateway for EVs to analyze and monitor incoming traffic for possible DoS attacks. EVs are registered with a Central Aggregator (CAG) to exchange authenticated messages, and malicious EVs are added to a blacklist for violating a set of predefined policies to limit their interaction with the CAG. A denial of service (DoS) attack is simulated at CAG in a vehicle-to-grid (V2G) network manipulating various network parameters such as transmission overhead, receiving capacity of destination, average packet size, and channel availability. The proposed system is compared with existing intrusion detection systems using different parameters such as throughput, jitter, and accuracy. The analysis shows that the proposed system has a higher throughput, lower jitter, and higher accuracy as compared to the existing schemes.

Keywords: Denial of service attack; vehicle to grid network; network security; network throughput

1 Introduction

A Vehicular Ad hoc network (VANET) is a network of movable smart vehicles, fixed Infrastructures, and cloud environments [1]. A vehicle is the key entity of VANETs that is equipped with various electronic devices such as an on-board unit (OBU), global positioning system (GPS) unit, electronic license plate (ELP), etc. In VANET, there are various types of communication models that include vehicle-to-infrastructure (V2I), vehicle-to-vehicle (V2V), infrastructure-to-infrastructure (I2I), and vehicle-to-everything (V2X), etc. [2]. In V2I, a vehicle and the infrastructure send or receive messages to each other. Two vehicles communicate with each other in V2V communication and similarly, two infrastructures exchange massages in I2I communication. V2X communication includes many other kinds of communication such as vehicle-to-grid (V2G), vehicle-to-pedestrian (V2P), and vehicle-to-network (V2N) [3,4]. From the above-mentioned infrastructure, V2G is a special type of V2X, in which an electric vehicle (EV) also called the battery vehicle (BV) communicates with the smart grid (SG) for charging its batteries. SG is a combination of different electronic devices such as advanced metering infrastructure (AMI), aggregators, smart meters (SM), data collectors (DC), etc. It provides the power (electrical energy) to the EVs or BVs through aggregators which is a bridge between SG and EVs. First, EVs are connected to an aggregator. There are two types of connection between the aggregator and the EV i.e., power and communication connection. Similarly, this aggregator connects with SG through the same type of connections [5]. For connection, the SG uses an open network that poses various types of security challenges in the V2G network that can degrade the performance and efficiency of the system. Denial of service (DoS) is one of the common types of attacks in the V2G network in which an attacker sends a large amount of data to any node i.e., an aggregator that blocks the V2G network bandwidth resulting in congestion. An intrusion detection system (IDS) is used to detect and mitigate the DoS attack automatically by first defining the abnormal/malicious activity and then comparing the user behavior against the defined abnormal activity for attack detection [6]. Upon detection, the malicious node is blacklisted and all nodes in the system are informed accordingly.

Comparative analysis shows that each IDS is different in terms of functionality for different network scenarios and various mechanisms and techniques have been developed to detect and mitigate the cybersecurity attacks in different networks but the detection and mitigation mechanism of DoS attack on the V2G network is yet to be explored. From this perspective, this study proposes a novel approach and makes the following contributions.

- A novel intrusion detection approach, central aggregator-intrusion detection system (CA-IDS), is proposed for the detection and mitigation of DoS attacks on the V2G network.
- The proposed IDS approach is deployed at the central aggregator (CAG) using wireless access vehicular environment (WAVE) protocol in the V2G network. The CA-IDS detects the DoS attack and generates an alert to inform other entities in the system about the attacker's entity.
- The performance is analyzed using several parameters like throughput, packet delivery rate, and jitter. Similarly, DoS attack detection accuracy is used for performance comparison with existing works including real-time attack detection, Cuckoo, and genetic algorithm.

The rest of the paper is structured as follows. The literature review is presented in Section 2. Section 3 discusses the proposed approach, simulation setup, and parameters used for simulations. Results are given in Section 4 while Section 5 concludes this study.

2 Related Work

This section summarizes the techniques used for DoS detection and its mitigation and classifies various models of IDS and the techniques used. The discussed research works are categorized concerning the use of the model for intrusion detection, privacy-preserving, etc.

2.1 Intrusion Detection Systems

In [7,8] authors propose a distributed grid-based intrusion detection system (GIDS) in the SG environment that protects against various attacks in VANETS. In [7], GIDS works as an administrator in this system. Each GIDS collects and analyses the data and identifies the attack by comparing the behaviors of the different hosts. However, in [8], the vehicle initially connects with the charging or discharging station through an authentication scheme called anonymous and fine-grained access control authentication. An authentication server authenticates the vehicle's identity. After that, an aggregator and the vehicle communicate with each other. The communication server does the communication between different entities and the control center (CC) controls all activities of this system. Pooja et al. [9] propose a two-phase scheme that provides a solution for DoS attacks in the vehicular environment. In the first phase (also called the entity phase), it calculates the Hash identity (HMAC) of every vehicle after which it generates a message in their timestamp called Ti. If Ti and received massage time is the same or less than the threshold value, it means that the DoS attack did not occur. In the second phase, the system creates the two tables called detection and blacklist tables. The detection table comprises two values i.e., the identity of vehicles and threshold values. The blacklist table maintains the list of blacklist vehicles. If any vehicle identification (ID) exists in the detection table, the system compares this value with the threshold. If this value is greater than the threshold, it means that the DoS attack has occurred, after which the vehicle ID is added to the blacklist table.

In [10], the authors propose an IDS based on analyses of data to mitigate the black hole attack (a type of DoS attack) in the SG environment using IDS, AMI, and DC entities. DC collects the data from the SG network and gives it to IDS. IDS and DC can easily communicate with each other using an ad hoc on-demand distance vector (AODV) routing protocol. An IDS observes and analyses the data activities such as the flow of data etc. After analyses, it takes necessary action against the malicious nodes. If there is any problem in the SG environment, it generates a signal for alarm. In [11], the authors propose a reliable and lightweight IDS based on monitoring in the vehicular network. This system is used as a greedy forward protocol for communication between different vehicles. Firstly, a vehicle finds its neighboring vehicles in its radio link range. After that, IDS monitors all other links in their radio link range. This vehicle (IDS installed on this vehicle) works as a guard vehicle. A guard vehicle must exist in every radio link range which detects the Intrusions and generates an alert to other vehicles. In [12] and [13] authors propose an IDS to detect intrusions in the vehicular environment. It is a two-step process, i.e., a detection phase and a prevention phase. The system in [12] uses a model to analyze the data. Two types of models are used in this system called system analyses model and the signal analyses model also called signal-based IDS. In [13], the detection system receives the packet from the sender and checks the status of the packet (blacklisted packet or not). If the packet is blacklisted, it sends this packet to the prevention system and if the packet is normal, it is passed through the classifier.

Islam et al. [14] propose a distributed DoS (DDoS) attack detection and prevention scheme called CVGuard in a V2I environment that uses a software-defined network (SDN), network functions virtualization (NFV), and edge computing. There are two parts of this scheme called micro box and CVGuard controller. The micro box is a smart security module that is installed at each road side unit (RSU). It acts as a gateway for all vehicles. It can capture the malicious packets sent by the attackers. CVGuard controller resides in the cloud environment and is a centralized system that monitors the whole network (e.g., V2I communication, vehicles, and infrastructure or RSU). CVGuard is more flexible, reliable, and quick as it uses NFV and SDN. Aloqaily et al. [15] propose a three-phase hybrid Intrusion detection system for VANETs that is used to detect the DoS attack. The main principle is to detect and identify the behaviors of different attackers and analyses and monitors the network. This system is divided into three layers called trusted third party (TTP), vehicle, and cluster heads. The main responsibility of the cluster head is the collection of data in a cluster. Each vehicle sends the data to its cluster head and the cluster head sends this data to the TTP that takes the decision. After receiving data (normal and abnormal), it detects the intrusion by a malicious vehicle and generates an alert for the administrator that sends this alert to other parts of the system. In [16], the authors propose a real-time detection mechanism for DoS attacks based on the proposed system architecture (PSAM) for VANETs. PSAM uses the attacked packet detection algorithm (APDA) to detect the malicious packet. APDA is deployed at every RSU and RSU works as a gateway in VANETs. This mechanism works based on the frequency, velocity, and position of the vehicles. It works on unicast, multicast, and broadcast transmission modes of data. For reliability, PSAM is integrated with the atypical segment area transmission range model (ESATRM). ESATRM can mitigate the hybrid attacks in VANETs. The integration of PSAM and ESATRM provides the authentication and key distribution for the vehicles. This makes VANETs more reliable and secure leading to higher throughput and lower jitter.

Nasim et al. [17] propose a hybrid IDS that detects the wormhole attack based on the location of SMs in the neighboring area network (NAN) in the SG environment. NAN is the part of SG that has some SMs or nodes. The authors select a collector in every NAN that analyzes and monitors the nodes. The system uses an analytical approach that computes the hop count between the collector and SMs. A collector takes the data from the SM, decrypts it, and sends it to the analytical engine. The analytical engine works based on the location of the nodes. A static SM's location is compared with the mobile ad hoc node. A GPS is used to get the location of nodes. All nodes must be registered with the collector. This makes it easier to know the shortest path. So, this technique is much better for the detection of wormhole attacks in NAN in the SG environment.

2.2 Authentication Systems

Sun [18] propose an authentication scheme that prevents the attacker to connect to the V2G network. Five entities are involved i.e., trusted authority (TA), charging or discharging station (ST), local aggregator (LAG), CAG, and vehicles. To communicate with the V2G, the vehicle first connects with the TA by sending its identity information and the TA generates the keys (both public and private) to authenticate the vehicle. These keys are forwarded to all other entities i.e., ST, CAG and LAG, etc. Upon verification of the keys, TA issues a certificate to the legal vehicle, and only those vehicles that are granted a certificate can communicate with the LAG (which is part of ST). A vehicle can only join the V2G network through the ST. The vehicle sends the message to the ST and after verification, it joins the V2G network.

Tseng [19] propose an authentication scheme where each vehicle has given time intervals, granted by LAG, to authenticate communicating vehicles. A distributed system is used for the registration of the vehicles that generate the keys and sends these keys to the vehicle. Firstly, LAG registers a vehicle and upon verification of the keys, it grants a certificate to the vehicle. LAG sends the information to CAG which sends this information to the TA. When a vehicle is registered, LAG sends its identity information to all other entities in the system. Whenever a vehicle wants to join the V2G network for charging or discharging, LAG verifies its' authenticity and upon verification sends a confirmation message back to the vehicle using the Boneh group signature scheme. After the verification process, the vehicle connects with the V2G network. Liu et al. [20], propose a secure communication scheme in the vehicular network where a vehicle registers with the TA and is issued a smart card that is inserted into the vehicle to connect to the network and secure communication between vehicles.

Hoang et al. [21] propose a plug-in electric vehicles (PVES) scheme for a V2G environment for charging or discharging authenticated EVs. It is a centralized scheme comprising TA, ST, CAG, LAG, and EV. An EV is connected to the LAG which is connected to the CAG. Firstly, an EV registers with the TA by sending its identity information. TA grants permission to EV by issuing a membership certificate. Only EVs that are issued membership certificates can connect to the V2G network through ST to charge or discharge their batteries securely. Yi et al. [22] and Verma et al. [23] purpose a similar two-step approach that uses a mechanism for detection and prevention of denial of service attacks based on the monitoring of the network traffic. However, in [22], the detection and prevention techniques are only applicable in the AMI environment, which uses network mash topology and distance short range (DSR) protocol for communication.

Kumar et al. [24] propose an efficient detection and prevention algorithm based on frequency (f) and velocity (v) fixed range values (upper and lower) in the VANETs environment. The algorithm detects the malicious vehicle and drops its packets considering it a DoS attack. The main advantage of this algorithm is that the network is always free for all other vehicles. When a vehicle wants to send the packet to the RSU, it compares the packet's f and v values with the RSU fixed range values (f and v). If the packet's frequency and velocity and fix range values (f and v) are the same, the packet has been sent, otherwise, it becomes the cause of the DoS attack. So, the proposed algorithm efficiently detects and prevents the attacker packet and drops it.

2.3 Privacy Preserving Systems

Yang et al. [25] propose a secure privacy-preserving scheme against different types of cybersecurity attacks in the V2G network using CAG, LAG, and TA, entities. Each vehicle communicates with the LAG and the LAG communicates with the CAG and TA communicates with all entities. Each LAG monitors and manages all vehicles in its range. Firstly, each vehicle registers with the CAG which grants permission to the vehicle. LAG can only communicate with vehicles that are granted permission from the CAG. Therefore, this scheme provides a secure mechanism against different attacks (i.e., DoS attacks) as no malicious vehicle can access the V2G network. Mohamed et al. [26] propose a host-based intrusion detection system (HIDS) based on a time slot to mitigate the DoS attack in the SG environment. HIDS is installed at each LAG that works based on the behavior of the vehicles. Each vehicle communicates with LAG for charging or discharging purposes. A vehicle can only send or receive the packet in its fixed time slot. If a packet takes time more than a fixed time slot, it is considered a malicious packet sent by an attacker. Every vehicle in the system also checks its neighboring vehicles' behavior in their time slot. After checking, it takes the decision and generates a message that is sent to the CC. However, if any vehicle's behavior is malicious, CC sends an alarm message to all other entities in the system.

Another important problem for an intelligent transportation system is vehicle re-identification where the image features can be utilized. Study [27] presents a multi-feature model with enhanced local attention (MELA) that combines local and global features to enhance the performance of vehicle re-identification. Similarly, for vehicle type classification, [28] presents a lightweight convolutional neural network along with feature optimization to reduce the computational complexity for real-time solutions. In addition, a joint learning strategy is introduced where the softmax loss is combined with a contrastive-center loss to improve the classification performance of the model. The comparison of the existing approaches for DoS attack detection and mitigation is shown in Tab. 1.

Table 1: Summary of literature review

Ref.	Type of network			Detection/Mitigation system			Detection system deployed on			
	V2G	VANETS	SG	IDS	Scheme	Other schemes	CAG/LAG	SG	RSU	Vehicle or EV
[5]	✓	✗	✗	✗	✓	✗	✗	✓	✗	✗
[6]	✓	✗	✗	✗	✓	✗	✗	✓	✗	✗
[7]	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
[8]	✗	✓	✗	✗	✗	✓	✗	✗	✓	✗
[9]	✗	✓	✗	✓	✗	✗	✗	✗	✓	✗
[10]	✗	✓	✗	✓	✗	✗	✗	✓	✓	✗
[11]	✓	✗	✗	✓	✗	✗	✗	✓	✗	✗
[12]	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗
[13]	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓
[14]	✓	✗	✗	✗	✗	✓	✗	✗	✓	✗
[15]	✗	✗	✓	✓	✗	✗	✗	✓	✗	✗
[16]	✗	✓	✗	✗	✗	✓	✗	✗	✓	✗
[17]	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓
[18]	✗	✓	✗	✗	✓	✗	✗	✗	✗	✓
[19]	✓	✓	✗	✗	✓	✗	✗	✗	✗	✓
[20]	✗	✗	✓	✓	✗	✗	✗	✓	✗	✗
[21]	✗	✓	✗	✗	✗	✓	✗	✗	✓	✗
[22]	✗	✓	✗	✗	✗	✓	✗	✓	✓	✗
[23]	✗	✓	✓	✗	✗	✓	✗	✓	✓	✗
[24]	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
[25]	✗	✓	✗	✓	✗	✗	✓	✗	✗	✗
[26]	✗	✓	✗	✓	✗	✗	✗	✗	✓	✗
[29]	✗	✓	✗	✗	✗	✓	✗	✗	✓	✗

3 Central Aggregator Intrusion Detection System

A V2G network is comprised of a group of EVs that communicate with the ST for charging and discharging batteries. EVs are mostly in motion and periodically broadcast important information such as alerts, state of the battery, distance, etc. using a wireless communication medium. CAG is a central component of the V2G network as EVs can only communicate with other EVs and entities in the network through the CAG and a DoS attack on the CAG can bring down the whole V2G network. A CAG can send or receive the data to/from EVs that are in its accessible range. In this paper, we present CA-IDS, an IDS system that works as a security gateway for all EVs in the V2G network that not only detects the DoS attack but also mitigates it. CA-IDS is a centralized security system deployed at the CAG that monitors and analyses the incoming network traffic from all EVs. CA-IDS ensures efficient and reliable use of the V2G network. Fig. 1 shows the V2G architecture and the deployment of the proposed CA-IDS while Fig. 2 shows the system architecture of the proposed CA-IDS.

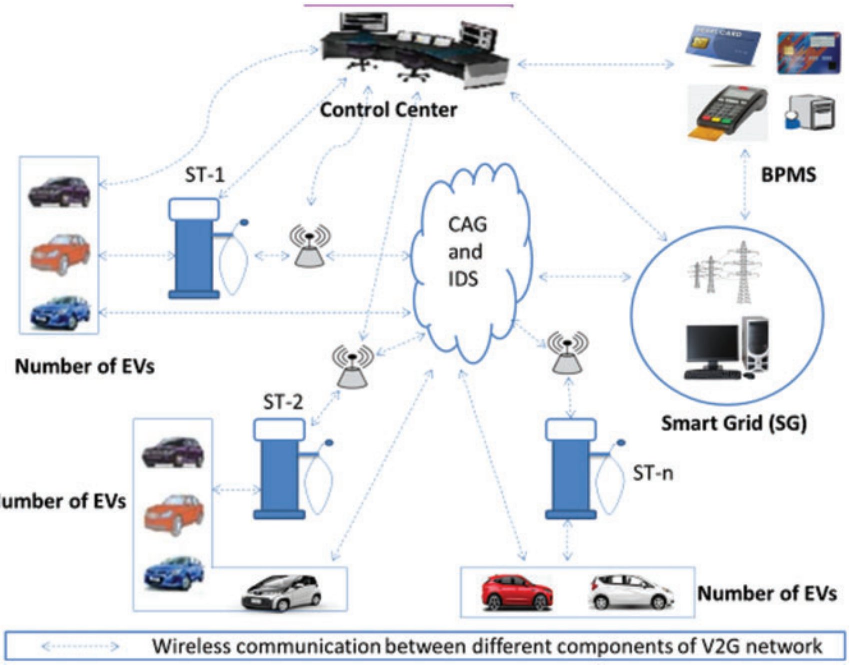

Figure 1: Architecture of V2G network with CA-IDS

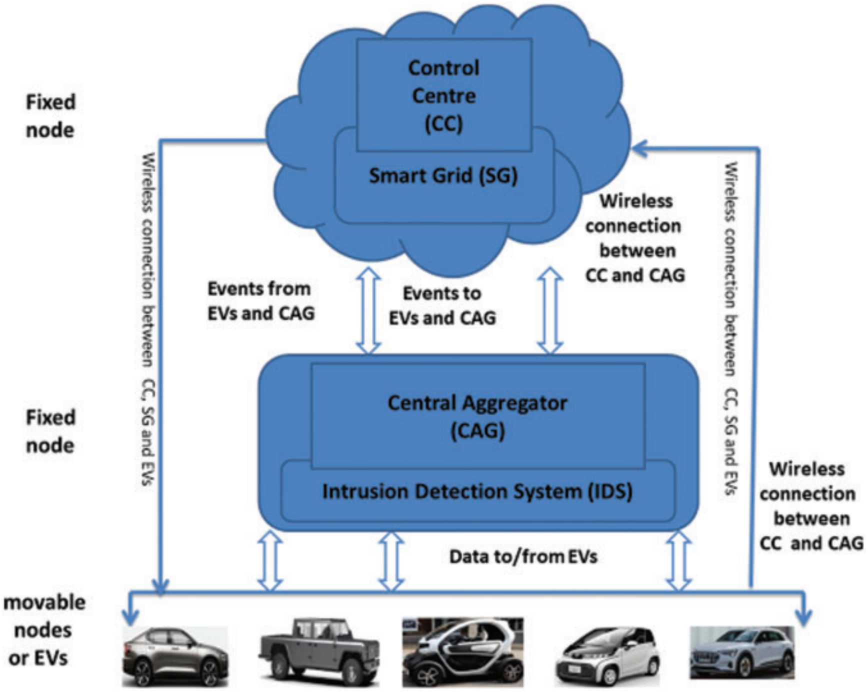
Fixed node
Control Centre (CC)
Smart Grid (SG)
Wireless connection between CC, SG and EVs
Wireless connection between CC and CAG
Events from EVs and CAG
Events to EVs and CAG
Wireless connection between CC, SG and EVs
Fixed node
Central Aggregator (CAG)
Intrusion Detection System (IDS)
Wireless connection between CC and CAG
Data to/from EVs
movable nodes or EVs

Figure 2: Security architecture of the proposed CA-IDS

When an EV needs to connect to the ST to charge/discharge, it sends a message to the CAG. CA-IDS, which is deployed at the CAG, checks to determine if it is a malicious or normal EV. If EV is normal, a message is sent to the CC for authentication and after identity verification, the EV is connected to the ST for charging or discharging. ST charges or discharges an EV and debits or credits the payment through the billing payment and management system (BPMS). For malicious EVs, a message is sent to the CC which adds the source address of the malicious EV to the blacklist (if not already on the blacklist), and the alert is propagated to all other entities of the V2G network. All packets of malicious EV are dropped. The communication process flowchart of the proposed system is shown in Fig. 3.

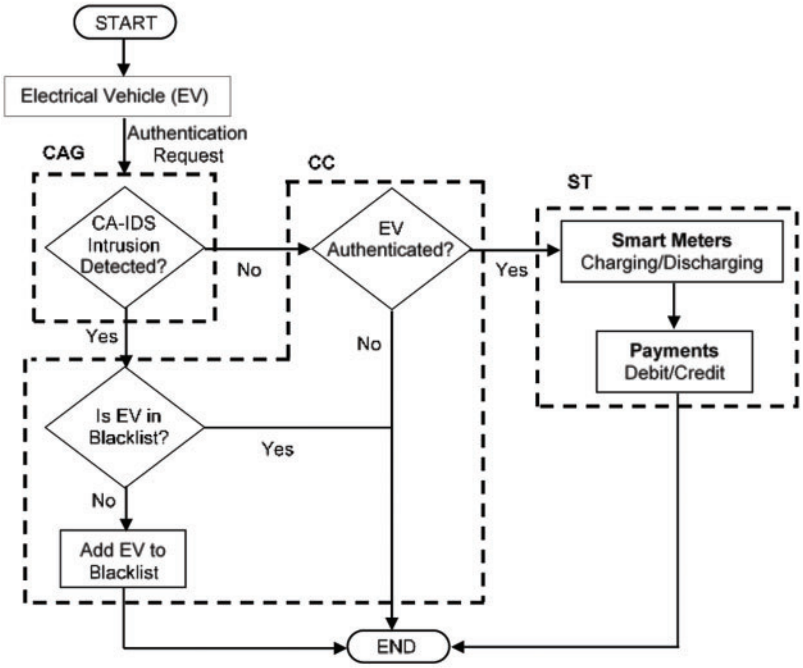

Figure 3: Flow chart of the proposed CA-IDS

The predefined policies of the V2G network and the attack detection rules of CA-IDS that identify the behavior of malicious EVs and mitigate the DoS attack are formulated as follows.

i. Each CAG has a specific communication range depending on the communication medium used (range of WAVE is up to 300 to 400 m), hence, a CAG can communicate with only those EVs that are in its WAVE communication range. For that, a CAG contains the geometry information of road locations (e.g., maps) within its communication range. Therefore, EV_i can only send the authentication request to CAG if

$$|L_i(a,b) - L_{CAG}(a,b)| < R_{CAG} \quad (1)$$

where $L_i(a,b)$ is the location (latitude and longitude) of EV_i and R_{CAG} is the communication range of the CAG. Eq. (1) helps determine if the EV_i is in the WAVE communication range of CAG.

ii. CAG maintains a registration table keeping the record of all registered EVs in the V2G network. Only registered EVs can communicate to the CAG and charge or discharge the batteries. CAG also maintains the entry and exit time of each EV as it enters within the range of the CAG.

iii. CAG maintains a blacklist table keeping a record of all malicious EVs. A blacklisted EV's connection request is denied by the CAG.

iv. CAG can provide services to a fixed number of EVs denoted by N.

v. An EV sends or transmits data at a fixed rate Tx_i and a CAG receives data at a certain rate Rx_{CAG}. The combined transmission rate of all EVs should be less than the receiving rate of the CAG, as shown in Eq. (2) so that CAG can receive all the packets transmitted by the EVs in the communication range of CAG.

$$\sum_{i=1}^{N} Tx_i < Rx_{CAG} \tag{2}$$

vi. CAG can receive data from an individual EV at a rate of less than the defined threshold T, as shown in Eq. (3) so that the condition in Eq. (2) is not violated.

$$Tx_i < T < Rx_{CAG} \tag{3}$$

vii. For an EV to communicate with the CAG and get services, it must maintain a speed S within a specified range, as shown in Eq. (4).

$$S_{min} < S < S_{max} \tag{4}$$

vii. The time complexity of CA-IDS in detecting a malicious EV is O(1). The intrusion detection in the CAG is done in constant time, and by implementing the blacklist as a hashmap in the CC, the status of the malicious EV can also be checked from the blacklist in constant time.

3.1 Formulation of DoS Attack

A malicious EV launches a DoS attack by sending a large amount of data to CAG to utilize the full capacity and block the V2G network. For that, the malicious EV needs to transmit data at a rate higher than Rx_{CAG} to breakdown the V2G network security, i.e., $Tx_c > Rx_{CAG}$, where Tx_c is the transmission rate of the attacker EV. When an attack occurs at the CAG in the V2G network, the CAG is unable to receive messages from other verified EVs and these EVs cannot get services from CAG (e.g., charging or discharging, authentication, alerts, etc.). A successful DoS attack is dependent on Rx_{CAG}, Tx_c, network transmission overhead (d), receiving capacity of the receiver (a), the average size of the packet (b), and channel availability (ρ). DoS attack can be launched in the V2G network on CAG using these parameters as shown in Eq. (5).

$$N \geq \rho(Tx_c * \frac{1}{a} + \alpha * \frac{10^6}{b} * d) \tag{5}$$

3.2 Detection of DoS Attack Using CA-IDS

As discussed earlier, CA-IDS monitors the EVs and when a malicious EV violates the pre-defined policies, an abnormal activity occurs which is not only detected but also mitigated using the detection rules defined previously. Due to the DoS attack, the transmission rate of the malicious EV will increase and the transmission rate of other legitimate EVs will decrease leading to the blockage of the V2G network. Using Eq. (3), CA-IDS will detect the malicious EV and send its source address to CC which will add this source address to the blacklist, block the transmission of data of the malicious EV and drop this EV from the network.

3.3 *Simulation Environment*

To test and evaluate CA-IDS, we simulate a DoS attack on the V2G network using an NS-3 simulator by implementing the predefined policies and rules. In the simulation scenario, different entities are wirelessly connected and communicate with each other. Our simulation environment consists of one LAG, one CC, one SG, one BPMS, one CAG, and ten EVs, nine of which are normal EVs, and one EV is malicious. The area of simulation is 300 m^2. The simulated environment is shown in Fig. 4.

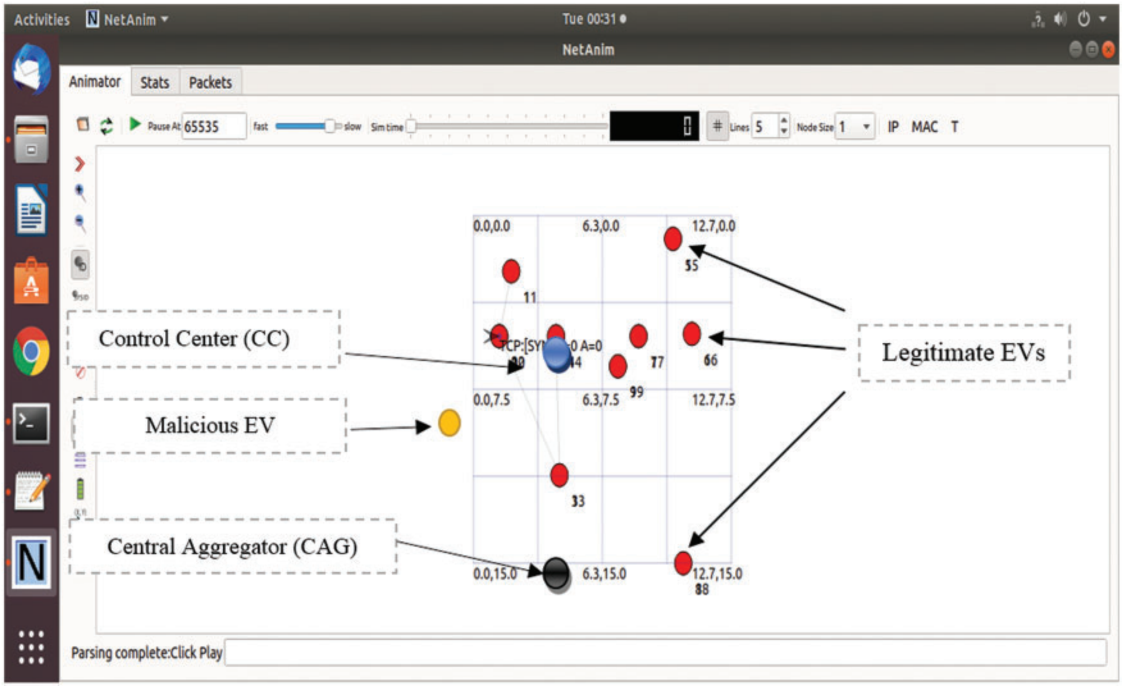

Figure 4: Simulation environment of V2G network

Tab. 2 shows the simulation parameters used in the experiments. This study uses Network Simulator (NS) V3.30 for simulation. The simulation is run for the 30 s while the simulation area is 300 m^2. The simulation includes 10 EVs where 9 EVs are legitimate while 1 is malicious. TCP is the traffic type used with wireless channels and WAVE protocol. Transmission and receiving rates are 100 and 1.5 Mbps respectively. Delay is 1 ms while packet size is 1000.

Table 2: Summary of literature review

Parameters	Measurements
Simulator	NS-3 (V3.30)
Simulation area	300 m^2
Simulation time	30 s
No of CAG	1
Number of malicious EVs	1
Number of legitimate EVs	9

(Continued)

Table 2: Continued

Parameters	Measurements
Control Center (CC)	1
Protocol	WAVE
Chanel type	Wireless
Traffic type	TCP
Transmission rate	100 Mbps
Receiving rate	1.5 Mbps
Delay	1 ms
Packet size	1000

4 Results and Discussions

This section presents the results of the simulation performed for the proposed approach. Besides discussing important parameters like throughput, jitter, and packet delivery rate (PDR) of the proposed approach, its performance is compared with existing approaches including real-time detection [29], CUCKOO [30], and Genetic algorithm [31].

4.1 Packet Delivery Ratio

In our simulation setup, a malicious EV transmits data at the rate of 100 Mbps to CAG. Due to the large inflow of packets to the CAG, the packet deliver ratio (PDR) of the V2G network is decreased. Upon detection of the DoS attack by CA-IDS, the attack is mitigated and the PDR of the V2G network is increased. With the increases in the number of nodes, the PDR of the V2G network is decreased, which is shown in Fig. 5.

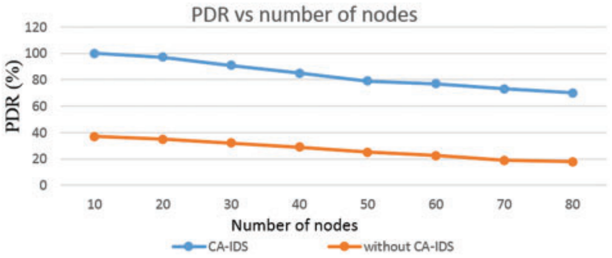

Figure 5: PDR *vs.* number of nodes

4.2 End-to-End Delay

Fig. 6 shows the performance of end-to-end delay using CA-IDS. The result shows that end-to-end delay is slightly increased when the total number of EVs is increased. Delay is an amount of time that takes a packet to transmit from one node to another node and delay variance means the variation of delay in the V2G network. CA-IDS has improved end-to-end delay as malicious vehicles with high data rates are added to a blocklist minimizing traffic and delay at CAG. In our experiment, delay variance is 22 ms when a malicious EV transmits at a higher data rate than CAG.

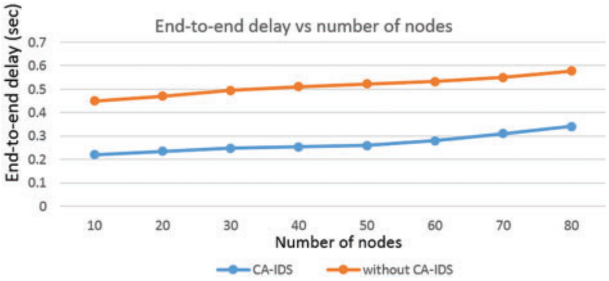

Figure 6: End-to-end delay *vs.* the number of nodes

In the following figures, we compare the proposed CA-IDS with existing systems (e.g., real-time detection [29], Cuckoo [30], and Genetic algorithm [31]) based on the average jitter, accuracy, and throughput.

4.3 Throughput, Detection Rate, and Jitter

Fig. 7 illustrates the performance of throughput as the number of attackers increases. When an attack occurs on CAG, the throughput of the V2G network is decreased. Upon detection of DoS attack by CA-IDS, the throughput continuously increases as malicious vehicles with high data rates are added to a blocklist. With the increase in the number of attackers, the throughput is slightly decreased.

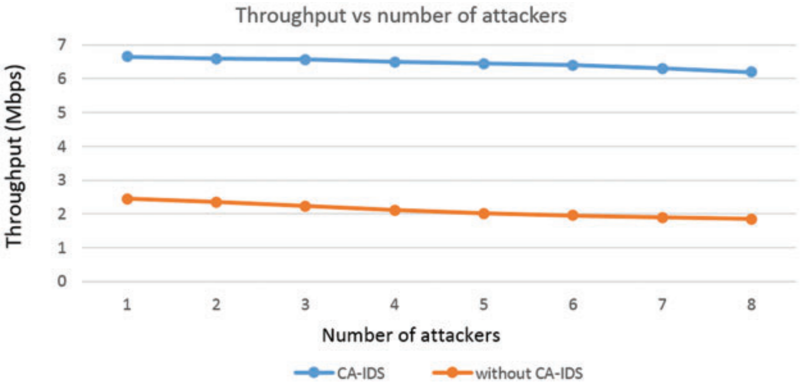

Figure 7: Throughput *vs.* the number of attackers

Fig. 8 shows the result of the detection rate as the transmission rate of the attacker is increased. At the attacker's sending data rate of 100 Mbps, the detection rate is around 100 percent. Similarly, the detection rates at a transmission rate of 200, 500, 700, and 1000 Mbps are 99.9, 99.8, 99.67, and 99.6 percent.

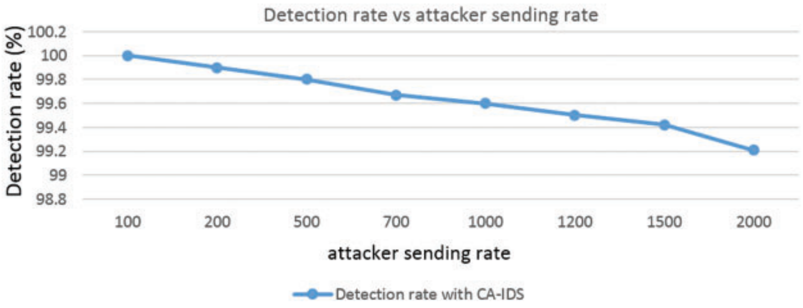

Figure 8: Detection rate *vs.* the number of attacker sending rate

4.4 Performance Comparison with Existing Studies

The comparison of the jitter of CA-IDS and existing systems including real-time detection [29], CUCKOO [30], and Genetic algorithm [31] is shown in Tab. 3. The delay is measured in the V2G network, and the system is evaluated based on this delay. The jitter of CA-IDS is less than 12, while for existing systems, the delay is higher. CA-IDS has less delay as CAG is more responsive in relaying the information between EVs due to isolated malicious EVs and control over unnecessary traffic. The jitter is calculated using Eq. (6).

$$Average\ Jitter = \frac{Maximum\ Jitter - Minimum\ Jitter1}{2} \tag{6}$$

The throughput comparison of CA-IDS and existing systems is shown in Tab. 3. CA-IDS has higher throughput as compared to the existing systems as CAG handles actual traffic volume ignoring traffic from malicious EVs.

The accuracy of CA-IDS is compared with the existing systems and the accuracy of CA-IDS is higher compared to the existing systems as shown in Tab. 3.

Table 3: Performance comparison with existing studies

System	Jitter (ms)	Throughput (Mpbs)	Accuracy (%)
CA-IDS	22.0	6.7	100
Realtime detection [29]	24.0	5.2	92
Cuckoo [30]	33.0	3.8	63.89
Genetic algorithm [31]	33.5	2.3	62

5 Conclusion

In the V2G network, EVs are connected with CAG for charging and discharging purposes. Therefore, CAG is an important component of the V2G network, and a cybersecurity protection mechanism is needed for CAG. Cybersecurity mechanisms can be hardware-based or software-based. Hardware-based security or hardware security module is not suitable due to maintenance and cost issues. A software-based cybersecurity mechanism is more suitable because it is configurable and inexpensive. It is very difficult to select a cyber-security mechanism that is more suitable. This study proposes a software-based cybersecurity mechanism called a central aggregator intrusion detection system (CA-IDS) which is more reliable and secured. CA-IDS detects and mitigates the DoS attack in the V2G network. The proposed CA-IDS is implemented in NS-3 (v-3.30) simulator to measure the efficiency and performance by using various parameters such as jitter, throughput, and accuracy. First, a case study is conducted, a DoS attack is launched and its effect on the V2G network has been analyzed. After that, the cybersecurity mechanism is deployed on CAG which is capable to detect and mitigate the DoS attack and dropping the malicious packets. These results are compared with existing schemes which prove that the proposed CA-IDS is better and increases the efficiency. Simulations include 1 malicious node in comparison to 9 legitimate nodes and the influence of the number of malicious nodes is not analyzed in this study and is left for the future.

Funding Statement: This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2021R1A6A1A03039493).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. U. Rehman, M. A. Khan, T. A. Zia and L. Zheng, "Vehicular ad-hoc networks (VANETs)-An overview and challenges," *Journal of Wireless Networking and Communications*, vol. 3, no. 3, pp. 29–38, 2013.

[2] C. Corchero and M. Sanmarti, "Vehicle- to- everything (V2X): Benefits and barriers," in *Proc. Int. Conf. on the European Energy Market*, Poland, pp. 1–4, 2018.

[3] I. Kabashkin, "Reliable v2x communications for safety-critical intelligent transport systems," in *Proc. Advances in Wireless and Optical Communications*, Riga, Lativia, pp. 251–255, 2017.

[4] I. Ivanov, C. Maple, T. Watson and S. Lee, "Cyber security standards and issues in V2X communications for internet of vehicles," in *Proc. Living in the Internet of Things: Cyber Security of the IoT*, Germany, pp. 46–62, 2018.

[5] G. Brusaglino, "Integration of road electric vehicles into the smart grid system," in *Proc. Int. Conf. on Clean Electrical Power*, Ischia, Italy, pp. 177–182, 2011.

[6] C. Guo, Y. Ping, N. Liu and S. S. Luo, "A two-level hybrid approach for intrusion detection," *Neurocomputing*, vol. 214, pp. 391–400, 2016.

[7] A. Schulter, J. A. Reis, F. Koch and C. B. Westphall, "A grid-based intrusion detection system," in *Proc. Int. Conf. on Networking, Int. Conf. on Systems and Int. Conf. on Mobile Communications and Learning Technologies*, Mauritius, pp. 187, 2006.

[8] N. Saxena, S. Grijalva, V. Chukwuka and A. V. Vasilakos, "Network security and privacy challenges in smart vehicle-to-grid," *IEEE Wireless Communications*, vol. 24, no. 4, pp. 88–98, 2017.

[9] B. Pooja, M. M. M. Pai, R. M. Pai, N. Ajam and J. Mouzna, "Mitigation of insider and outsider DoS attack against signature-based authentication in VANETs," in *Proc. Asia-Pacific Conf. on Computer Aided System Engineering*, Bali, Indonesia, pp. 152–157, 2014.

[10] N. Boumkheld, M. Ghogho and M. El Koutbi, "Intrusion detection system for the detection of black hole attacks in a smart grid," in *Proc. Int. Symp. on Computational and Business Intelligence*, Olten, Switzerland, pp. 108–111, 2016.

[11] H. Sedjelmaci, S. M. Senouci and M. A. Abu-Rgheff, "An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks," *IEEE Internet of Things Journal*, vol. 1, no. 6, pp. 570–577, 2014.

[12] M. Aloqaily, S. Otoum, I. A. Ridhawi and Y. Jaraweh, "An intrusion detection system for connected vehicles in smart cities," *Ad Hoc Networks*, vol. 90, no. 4, pp. 101842, 2019.

[13] A. Sahi, D. Lai, Y. Li and M. Diykh, "An efficient DDoS TCP flood attack detection and prevention system in a cloud environment," *IEEE Access*, vol. 5, pp. 6036–6048, 2017.

[14] M. Islam, M. Chowdhury, H. Li and H. Hu, "Cyber security attacks in vehicle-to-infrastructure," *Transportation Research Record*, vol. 2672, no. 19, pp. 66–78, 2017.

[15] M. Aloqaily, S. Otoum, I. Al Ridhawi and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," *Ad Hoc Networks*, vol. 90, no. 4, pp. 101842, 2019.

[16] D. Kosmanos, A. Pappas, L. Maglaras, S. Moschoyiannis, F. Aparicio-Navarro *et al.,* "A novel intrusion detection system against spoofing attacks in connected electric vehicles," *Arrays*, vol. 5, no. 1, pp. 100013, 2020.

[17] B. M. Nasim, M. Jelena, K. Hamzeh and B. M. Vojislav, "An intrusion detection system for smart grid neighborhood area network," in *Proc. Int. Conf. on Communications*, Sydney, Australia, pp. 4125–4130, 2014.

[18] Z. Sun, "An anonymous authentication scheme for vehicle-to-grid networks," *Int. Journal of Communications, Network and System Sciences*, vol. 10, no. 8, pp. 316–323, 2017.

[19] H. Tseng, "On the security of a unique batch authentication protocol for vehicle-to-grid communications," in *Proc. Int. Conf. on ITS Telecommunications*, Taipei, Taiwan, pp. 280–283, 2012.

[20] C. Liu, K. T. Chau, D. Wu and S. Gao, "Opportunities and challenges of vehicle-to-home, vehicle-to-vehicle, and vehicle-to-grid technologies," *Proceedings of the IEEE*, vol. 101, no. 11, pp. 2409–2427, 2013.

[21] D. T. Hoang, P. Wang, D. Niyato and E. Hossain, "Charging and discharging of plug-In electric vehicles (PEVs) in vehicle-to-grid (V2G) systems: A cyber insurance-based model," *IEEE Access*, vol. 5, pp. 732–754, 2017.

[22] P. Yi, T. Zhu, Q. Zhang, Y. Wu and L. Pan, "Puppet attack: A denial of service attack in advanced metering infrastructure network," *Journal of Network and Computer Applications*, vol. 59, pp. 325–332, 2016.

[23] K. Verma and H. Hasbullah, "IP-CHOCK (filter)-Based detection scheme for denial of service (DoS) attacks in VANET," in *Proc. Int. Conf. on Computer and Information Sciences*, Taiyuan, China, pp. 1–6, 2014.

[24] S. Kumar and K. S. Mann, "Prevention of DoS attacks by detection of multiple malicious nodes in VANETs," in *Proc. Int. Conf. on Automation, Computational and Technology Management*, London, UK, pp. 89–94, 2019.

[25] Z. Yang, S. Yu, W. Lou and C. Liu, "P^2: Privacy-preserving communication and precise reward architecture for V2G networks in smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 697–706, 2011.

[26] A. Mohamed, S. M. Senouci, H. Sedjelmaci, E. H. Aglzim and D. Chrenko, "An efficient intrusion detection system against cyber-physical attacks in the smart grid," *Computers & Electrical Engineering*, vol. 68, pp. 499–512, 2018.

[27] W. Sun, G. C. Zhang, X. R. Zhang, X. Zhang and N. N. Ge, "Fine-grained vehicle type classification using lightweight convolutional neural network with feature optimization and joint learning strategy," *Multimedia Tools and Applications*, vol. 80, no. 20, pp. 30803–30816, 2021.

[28] W. Sun, X. Chen, X. R. Zhang, G. Z. Dai, P. S. Chang *et al.,* "A multi-feature learning model with enhanced local attention for vehicle re-identification," *Computers, Materials & Continua*, vol. 69, no. 3, pp. 3549–3560, 2021.

[29] A. Haydari and Y. Yasin, "Real-time detection and mitigation of ddos attacks in intelligent transportation systems," in *Proc. Int. Conf. on Intelligent Transportation Systems*, Hawaii, US, pp. 157–163, 2018.

[30] M. E. A. Fekair, A. Lakas and A. Korichi, "CBQoS-Vanet: Cluster-based artificial bee colony algorithm for QoS routing protocol in VANET," in *Proc. Int. Conf. on Selected Topics in Mobile & Wireless Networking*, Cairo, Egypt, pp. 1–8, 2016.

[31] G. Kaur, "A preventive approach to mitigate the effect of gray hole using genetic algorithm," in *Proc. Int. Conf. on Advanced in Computing, Communication, Automation*, Bareilly, India, pp. 8–9, 2016.