Computer Networks 185 (2021) 107658

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Survey paper

Truck platoon security: State-of-the-art and road ahead

Amrita Ghosal [a,*], Sang Uk Sagong [b,c], Subir Halder [a], Kalana Sahabandu [b], Mauro Conti [a], Radha Poovendran [b], Linda Bushnell [b]

[a] Department of Mathematics, University of Padua, Padua 35121, Italy
[b] Department of Electrical and Computer Engineering, University of Washington, Seattle, USA
[c] Hyundai Motor Group, Republic of Korea

ARTICLE INFO

Keywords:
Truck platoon
Security
Adaptive cruise control
Truck-to-truck communication
Attack surfaces
Defense

ABSTRACT

Trucks form a platoon, where they align in a lane on freeways, in order to save fuel. The trucks positioned behind the first truck in the platoon can save fuel because their air drag reduces. In a truck platoon, various technologies such as Adaptive Cruise Control (ACC) system and Vehicle-to-Vehicle (V2V) communication protocol are exploited to control the trucks in the platoon effectively. The camera sensors measure distance between contiguous trucks in the platoon and these sensor measurements are provided to the ACC system. By using these sensor measurement, the ACC system controls the truck speed via in-vehicle network protocols such as the controller area network, which does not encrypt data or authenticate messages. Also, the V2V communication protocol is vulnerable to cyber attacks that disable the wireless channels among the trucks in the platoon. As a result, the ACC system and V2V communication protocol may introduce attack surfaces in a truck platoon. In this survey, we analyze the attack surfaces of a truck platoon under different perspectives. Then, we summarize the defense systems corresponding to the discussed attacks in terms of detection mechanisms, response countermeasures, and proactive defenses. Finally, we provide the research issues that need to be addressed in future.

1. Introduction

Truck platoon, in which trucks align in a lane on freeways and runs as a group, will be an indispensable functionality of future intelligent transportation systems, mainly due to the fact that fuel can be saved significantly [2–7]. An air drag coefficient of the trucks behind the first truck of the platoon decreases when the distance between the trucks in the platoon is smaller than a certain threshold. Due to the decrease in the air drag coefficient, the trucks behind the first one can save fuel. In addition to saving of fuel, the freeways can be effectively utilized for preventing road accidents [8–11]. A truck platoon is composed of a Platoon Leader (PL) and a Platoon Member (PM) in a leader-follower structure as illustrated in Fig. 1 [1]. A PL provides permission to trucks for entering or leaving the platoon, controls the speed of the platoon, and tracks the number of trucks in the platoon. A PM follows the commands from the PL and reports its status to the PL or other PMs.

Adaptive Cruise Control (ACC) system and Vehicle-to-Vehicle (V2V) communication protocols are indispensable technologies for establishing a truck platoon in freeways. By exploiting different types of sensors, such as radio detection and ranging (RADAR), light detection and ranging (LIDAR), and visible light cameras, the distance between the trucks can be measured, and the measurements from these sensors are transmitted to the ACC system via in-vehicle networks. The ACC system sends control messages to the engine control module and brake module in order to control the truck speed. A truck platoon also exploits the V2V communication protocol because the PL and PMs need to exchange data for maintaining the platoon. For instance, a PL sends a command for changing the speed to all PMs through the V2V communication protocol, such as Dedicated Short Range Communication (DSRC) and Wireless Access in Vehicular Environment (WAVE). A Cooperative ACC (CACC) system [12] is introduced, in which the ACC system and V2V communication are combined together [13].

Due to the increasing number of trucks on roads and more complicated road conditions, trucks in a platoon are equipped with more Electronic Control Units (ECUs) with outward-facing interfaces, such as cellular networks, WiFi, and Bluetooth to provide higher safety and more accurate control of the trucks. Data for the ACC system is

* Corresponding author.
E-mail addresses: amrita.ghosal@math.unipd.it (A. Ghosal), sagong@uw.edu (S.U. Sagong), subir.halder@math.unipd.it (S. Halder), ksahaban@uw.edu (K. Sahabandu), conti@math.unipd.it (M. Conti), rp3@uw.edu (R. Poovendran), lb2@uw.edu (L. Bushnell).

[1] Many papers considered vehicle platoons, not limited to truck platoons [1]. Since a truck platoon is a special case of a vehicle platoon, results of these existing papers on vehicle platoons can be applied to truck platoons. Without loss of generality, we focus on truck platoons in this paper.

https://doi.org/10.1016/j.comnet.2020.107658
Received 14 April 2020; Received in revised form 3 August 2020; Accepted 27 October 2020
Available online 6 November 2020

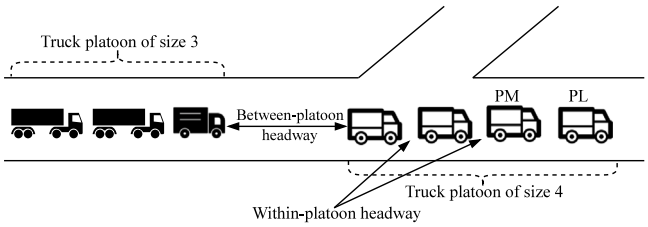


Fig. 1. An illustration of a truck platoon on freeways.

exchanged among the ECUs through in-vehicle network protocols, such as the Controller Area Network (CAN) and Local Interconnect Network (LIN) [14–17]. The in-vehicle network protocols do not encrypt data or authenticate messages [18,19]. An adversary may take full control of a truck in a platoon once the ECUs with outward-facing interfaces are compromised. Consequently, the ECUs with outward-facing interfaces may introduce attack surfaces in a truck platoon [1,20,21]. By using these attack surfaces, the adversary may prevent a truck platoon from saving fuel. There are extensive works that explore attack surfaces of truck platoons and many works proposed defense systems for the truck platoons [1].[1]

1.1. Existing work

There exist many research works on truck platoons [22–26]. We categorize these works with respect to network architecture, communication protocols, stability analysis, and traffic models. The authors in [22] summarize the fundamental technologies used for establishing truck platoons, such as, network architecture, standard, and traffic dynamics. The authors of [22] discussed issues on platoon management, CACC system, and Inter-Vehicle Communication (IVC) protocols for truck platoons. Also, simulation tools that may be used to emulate truck platoons are introduced in relation with traffic dynamics and behavior of vehicular ad-hoc networks.

The authors of [23] provided a technical overview of truck platoons which includes vector field for autonomous navigation, spring dynamics for leader and follower models, and a proportional controller design for inter-platoon dynamics. In [23], obstacle detection and collision avoidance are categorized and extended to CACC systems. Stability of a truck platoon is also modeled and theoretically analyzed using the string stability theory. The security issues of IVC protocols, however, are not discussed.

In [24], a taxonomy for communication protocols of truck platoons is constructed, which is categorized as general information services, information services for truck safety, individual motion control using IVC protocols, and group motion control using inter-vehicle communication. Communication requirements for each category are discussed, and a representative set of protocols are classified according to their architecture and applicability. Attributes of IVC protocols, such as low latency, high reliability, high scaling, and membership service, are summarized according to the application of each protocol. Although the authors of [24] categorized the existing protocols that can be used in truck platoons, they have not discussed the attack surfaces of truck platoons or defense systems that can mitigate the attack surfaces.

The authors of [25] categorized the existing IVC protocols based on the protocols' discussion from the physical layer to the transport layer. They discussed the security and privacy issues of the protocols in each layer. This work also summarizes the road model, wireless channel model and the network simulator for the IVC protocols. Attack surfaces of truck platoons and attack models are not discussed in detail with respect to network architectures and IVC protocols. Defense systems of truck platoons are not discussed in this work.

A survey paper on vulnerabilities and security of truck platoons was published in 2017 [1]. The authors of [1] discussed a truck platoon in an adversarial environment with respect to the stability of the truck platoon. Although the attack model and defense mechanism are discussed in [1], only two papers (one for an attack on the truck platoon and one for a defense mechanism) are surveyed, which did not incorporate various attack surfaces of truck platoons in terms of stability, in-vehicle network protocols, and IVC protocols.

In [26], the author first analyzed the vulnerability in the platooning control system and found new destabilizing and modification attacks. Next, the author proposed an anomaly detection method which is the combination of the system identification method and machine learning technique to locate the attacker(s) in the platoon. Further, a mitigation scheme is proposed based on fractional order calculus to suppress the malicious behavior of the attacker.

1.2. Comparison with our survey

The existing survey papers have their advantages and significance in truck platoons. In [22,23,26], the authors modeled the traffic dynamics of a truck in a platoon using spring dynamics and proportional controller design. Based on the traffic model, stability of a truck platoon is formulated using string stability theory. Also, the IVC protocols for truck platoons are reviewed. These papers do not discuss security issues in the IVC protocols and truck platoon, and as a consequence, defense mechanisms for truck platoons are not reviewed. Although some survey papers categorize the IVC protocols and discuss their security issues [24,25], they contain limited discussion on security issues of the truck platoons and do not discuss defense mechanisms to secure the truck platoons.

In contrast to the existing papers, our survey provides the most recent research on security analysis of the truck platoons, and we provide security requirements and comprehensive categorization of attack surfaces in truck platoons. Moreover, a taxonomy of defense systems is discussed with respect to fundamental techniques for mitigating attacks on truck platoons. Table 1 compares the existing papers and our work.

1.3. Contribution and organization of the paper

The contributions in this paper are as follows.

- We summarize the background of truck platoons, which includes network architectures of truck platoons and communication protocols for truck platoons.
- We provide a comprehensive analysis of attack surfaces of truck platoons in various aspects such as network topology.
- We summarize defense systems corresponding to the previously discussed attacks and identify attacks for which a defense system is not proposed yet.
- We provide research issues that might be studied in order to make truck platoons more resilient to attacks with respect to the network protocols, PL, PM, and sensor perspectives.

We organize the rest of the paper as follows. Section 2 presents the background on truck platoons. In Section 3, we present the security challenges and requirements in truck platoons. Section 4 categorizes the existing defense mechanisms that can secure truck platoons. In Section 5, we put forward lessons learned from both attacks and defenses in truck platoons. Section 6 discusses future research issues. Finally, we wrap up the paper in Section 7.

2. Background on truck platoon

In this section, we describe the background of truck platoons. Particularly, Section 2.1 presents the fundamentals of truck platoons. In Section 2.2, we discuss the major benefits of truck platoons. Section 2.3 illustrates various types of communication topologies used in existing truck platoons. Finally, we present various communication protocols used in truck platoons.

Table 1
Comparison with other survey works on truck platoon.

	Traffic dynamics modeling	Stability issue	IVC protocol	Security issues of IVC	Security issues of truck platoon	Defenses	Paper covered
[1]	ND	✓	ND	ND	LD	LD	1994–2015
[22]	✓	✓	✓	LD	ND	ND	2004–2015
[23]	LD	✓	✓	ND	ND	ND	1994–2010
[24]	ND	ND	✓	✓	LD	ND	1999–2006
[25]	✓	ND	✓	✓	LD	ND	1993–2006
[26]	LD	✓	✓	ND	✓	✓	2000–2018
Ours	✓	✓	✓	✓	✓	✓	2010–2019

✓—Detailed Discussion; LD—Limited Discussion; ND—No Discussion.

2.1. Concept

A truck platoon, supporting trucks to travel through road as a group, is headed by a truck called PL and a number of other trucks called PMs. The PL continuously provides necessary information to the PMs, including highway conditions and maneuvers that the platoon is going to perform. In [27], the authors have defined a truck platoon as a *tightly spaced string of trucks, where the inter-truck distances are appropriately maintained as low as three to one meter at highway speeds depending on what sensors and communication devices are applied*. Generally, in truck platoon, a platoon or group of trucks move in fine-grain co-ordination with completely automated longitudinal speed and lateral steering control. The trucks in a platoon usually maintain short pre-defined gaps between themselves, irrespective of speed called headway-truck spacing. Due to the small headway-truck spacing, the truck carrying capacity of highway increases immensely. In addition, because of fine-grain co-ordination and automation between trucks, the road safety increases significantly. In fact, as the relative speed between the trucks is very small, life-threatening accelerations and decelerations cannot cause havoc impacts on the trucks.

A platoon is a complex system that integrates various technologies like communication, sensing and control [28]. Every individual truck in the platoon contributes to the greater stability of the platoon by exchanging various information, e.g., present kinematics status and projected maneuvers, data from on-board sensors like camera, radar with other trucks. In order to form a truck platoon, the travel speeds, departure times and routes of the trucks should be synchronized. To join a truck platoon, a truck needs to adjusts its speed, route and even make a small detour. However, such restrictions are not applicable during leaving a truck platoon.

2.2. Benefits

There are several benefits of truck platoons. In this section, we discuss the major benefits of truck platoons.

2.2.1. Fuel efficiency

One of the major benefits of truck platoons is the enhancement in fuel efficiency. In [29], Liang et al. show that a truck platoon is beneficial if the platoon is long enough, specifically, platooning distance is significantly bigger than the catch-up distance. It is mainly due to the fact that when platoon size is bigger than the catch-up distance, the air drag force that acts against a running truck, reduces significantly. Here, it is worth mentioning that for a truck of typical 40 ton weight, air drag force is 23% of the total force that acts against a running truck [30]. Since longer platoons reduces air drag force, thus, it significantly enhances fuel efficiency and subsequently reduces emissions [31].

2.2.2. Road safety

Another major benefit of truck platoon is the enhancement of road safety. In conventional system, around 90% of all road accidents are due to human (or driver) errors. It is mainly due to the high reaction time of driver and significant concentration required from the driver while driving. In truck platoon, the acceleration and the braking of the platoon trucks are autonomous in nature. Particularly, in a tightly-coupled truck platoon, an actual human driver controls the lead truck all the time. Various actions of the lead truck are communicated via CACC to the trailing autonomous trucks, who follow the lead and manage the inter-truck distance. Because of this fact, in truck platoon, the reaction time is almost zero compared to human braking. For example, usually, the average human reaction time is 0.25 s, whereas, the reaction time of a truck platoon is 0.1 s [32], resulting in reduction of a number of accidents, including rear-end collision [33].

2.2.3. Road capacity

Truck platoons significantly increases the road capacity by spacing trucks as tightly as possible. Typically, CACC maintains the suitable inter-vehicle or inter-platoon distance. In a truck platoon, CACC usually maintains a 8–10 m gap, end-to-end, in contrast to standard 50 m gap presently used on our roads [32]. Due to the tight coupling among the trucks in a platoon, large number of trucks participate in a truck platoon, resulting in significant increase in road capacity [34].

2.2.4. Green environment

Typically, a truck (non-platoon) has an average CO_2 emission of 2.6 kg per litre of fuel [32]. However, truck platoon has the potential to reduce CO_2 emission considerably. This is because trucks are coupled tightly in platoons and ideally seem to move at constant speed, with minimum braking and acceleration. All these factors result in significant fuel saving of up to as much as 10% less CO_2 emission [35]. In fact, truck platoon is now a days a part of automobile company's integrated approach to reduce CO_2 emission significantly [36].

2.2.5. Business profit

Truck platoons have a great potential of transforming logistic processes to be more efficient and safe [36]. Induction of truck platoon can reduce the overall direct and indirect operating costs of transport industries up to 30%, as platoons not only decrease fuel consumption significantly but also reduce maintenance cost of the trucks.

2.3. Communication topology

In this section, we discuss the various types of communication topologies used in truck platoon. We categorize the communication topologies into three categories, namely, centralized, distributed and hybrid. In Section 2.3.1, we present a brief discussion on centralized communication topology. While Section 2.3.2 illustrates the distributed communication topology, we finally discuss the hybrid communication topology in Section 2.3.3.

2.3.1. Centralized communication topology

We present a typical centralized truck platoon architecture in Fig. 2(a). In a centralized architecture, the PL and PM communicate with each other directly through either ACC or CACC [37]. Therefore, as the length of the platoon increases, the communication distance between the PL and the PM increases proportionally. To maintain the platoon, the PL collects every PM's information like location, velocity at regular intervals. Based on the collected information, the PL calculates the velocity of each PM and informs them accordingly. There are a number of drawbacks in the centralized architecture. First, to maintain the platoon, the PL exchanges a significant number of packets with the PMs. Also, as the PM directly communicates with the PL at some particular time slot, hence, communication incurs significant transmission delay. Because of significant computation and communication overheads, the PL often fails to notify the PMs about their velocities within a tolerable time limit.

2.3.2. Decentralized communication topology

In the decentralized truck platoon architecture, each truck (irrespective of the leader and follower) directly communicates with its succeeding truck [37] as shown in Fig. 2(b). To maintain the platoon, each truck shares its own current location and velocity with the succeeding truck at regular intervals. Based on the received information, both PL and PMs decide their respective velocities. One of the major limitations of the decentralized architecture is that, if the preceding truck leaves the platoon, it creates a connectivity hole inside the truck platoon. Further, if any truck leaves or joins the platoon, then the succeeding truck has to adjust its relative velocity based on the collision distance and connection loss in a very quick manner to stabilize the platoon [37].

2.3.3. Hybrid communication topology

In general, hybrid communication topology is a combination of various communications among PL and PMs. There are a number of categories, however, for conciseness, we present here the following topologies: (a) predecessor-leader following, (b) bidirectional, (c) directional-leader, and (d) two-predecessors [38] as shown in Figs. 2(c), 2(d), 2(e) and 2(f), respectively. Among these four categories, predecessor-leader following and bidirectional communication topologies has been devised by leveraging CACC systems. CACC systems usually collect velocity information from the immediate successor or predecessor through the on-board sensors, e.g., radar. Recently, with the advent of V2V communication, CACC systems are now capable of collecting wider range of information.

2.4. Communication protocol

We present the major communication protocols used in truck platoons in this section. Particularly, Section 2.4.1 discusses DSRC communication standard. We then present WAVE communication standard in Section 2.4.2. Finally, Section 2.4.3 illustrates recently developed Long Term Evolution (LTE) cellular system.

2.4.1. Dedicated short range communications

In the context of truck platoon communication, the DSRC technology has broad range applications, particularly, in the safety of truck platoon. Based on the IEEE 802.x family [39,40], the USA Federal Communication Commission has developed and standardized the DSRC technology in 1999. The DSRC technology supports Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communication by following the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism [41].

DSRC operates at the spectrum from 5.850 GHz to 5.925 GHz, i.e., 5.9 GHz band and supports channel switching, defined in IEEE 1609.4 [42]. The DSRC spectrum comprises of seven channels, one central Control Channel (CCH) and six Service CHannels (SCHs). In DSRC, channel switching allows simultaneous access of CCH and SCHs. This is achieved by dividing the spectrum band into seven 10 MHz channels, each followed by a 5 MHz guard band [43]. In DSRC, CCH is used to transmit safety messages, e.g., control and collision alarms, whereas, SCHs are used to transmit data in various applications.

In Fig. 3, we present a classic communication stack for DSRC that comprises of a data plane and a management plane. The data plane in the communication stack typically performs data processing tasks, like addition and deletion of frame headers. In a data plane, layer 4 is comprised of the WAVE Short Message Protocol (WSMP) as shown in Fig. 3. WSMP implements security policies along with responding to probable attacks and monitoring traffic patterns [44]. On the contrary, the management plane mainly performs synchronization. The WAVE Management Entity (WME) plays an important role in the management plane. In particular, WME is responsible for defining the transmission channel in addition with the quality of service priorities during the time when data frames are scheduled. Eventually, these priorities support the capability of transmitting urgent safety related messages with minimum delay. Further, the WME does the work of managing safety messages, priority channels and frame queuing. In WAVE, the key management and data encryption techniques are handled by the WAVE Security Entity (WSE). In addition to WME, the management plane consists of two important entities, i.e., MAC Layer Management Entity (MLME) and Physical Layer Management Entity (PLME). In addition to data and management planes, there are a number of points, which help in the proper functioning of the DSRC technology. Particularly, Data Service Access Points (DSAP) designate accurate interfaces among various data stacks. Whereas, Standardizing Service Access Points (SAPs) supports plugging of different units. Additionally, a part of the DSRC technology is dedicated on describing Management Service Access Point (MSAP) with respect to every entity. It is worth mentioning that the applications of DSRC exploit the Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) stack.

Although DSRC communication technology has several benefits, with respect to truck platoons, it has a number of limitations too. For example, in an ideal environment, DSRC achieves almost 100% data delivery if inter-truck distances in a platoon is at most 78 m [42]. Further, the truck platoon highly depends on real time data which hardly supports DSRC due to the multi-channel method makes a uniform share of available channels to all messages [40]. Furthermore, DSRC uses CSMA/CA technique as MAC protocol. Due to the use of CSMA/CA, in a high dense scenario, the channel contention increases significantly, resulting in considerable performance degradation of IEEE 802.11. To overcome the limitations, several measures were undertaken by governments, industrial organizations, research and academic institutes, and standardization bodies. For example, if the road is hilly, to improve data delivery, the researchers have proposed to use both side antennas [42].

2.4.2. Wireless access in vehicular environment

To overcome the limited applications of DSRC in truck platoons, the American Society for Testing and Materials (ASTM) working group, ASTM 2313, transferred the DSRC to IEEE802.11p WAVE by integrating both the physical and MAC layers [45]. Two classes of devices are defined in WAVE: Road Side Unit (RSU) and On-Board Unit (OBU). The RSU is primarily used as a movable device, whereas, the OBU is mainly used as a static device.

The WAVE architecture is developed on the IEEE 802.11 standard [46,47] as shown in Fig. 4. The distinguishing factors in the operating environment of an IEEE 802.11 wireless local area network and a vehicular network led to the development of another standard, called as IEEE 802.11p [48]. Development of the physical and data link layers already exists in the IEEE 802.11p standard, while the development in the upper layers are done by IEEE P1609 [49]. The architecture of WAVE is composed of the primary components of resource manager, multichannel operation, WAVE short message protocol at the network

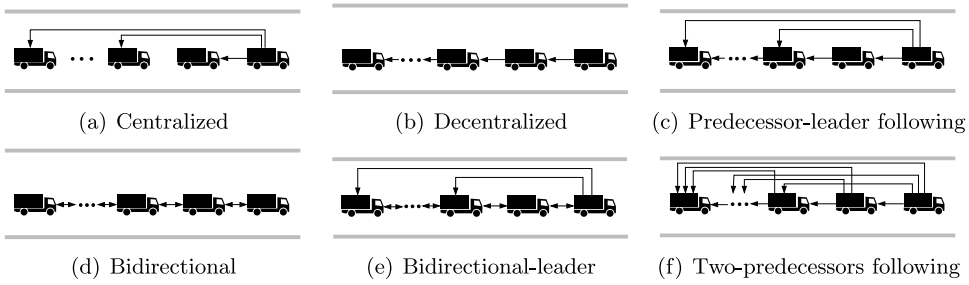


Fig. 2. Various communication topologies for truck platoon.

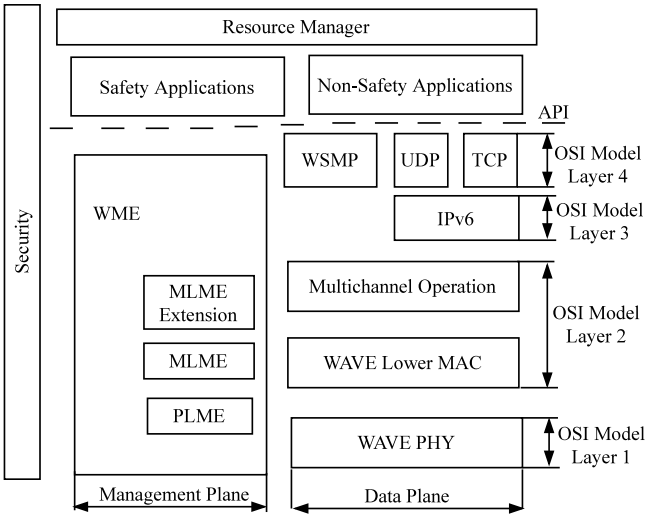


Fig. 3. DSRC communication stack.

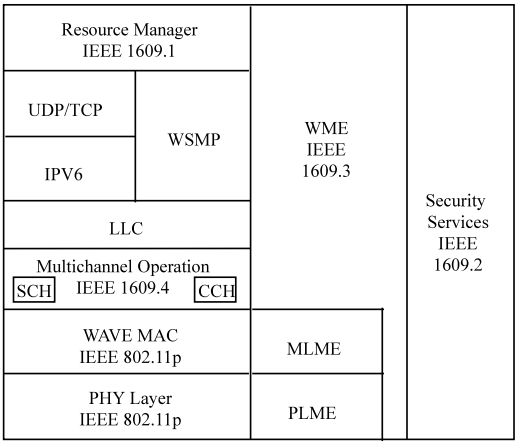


Fig. 4. WAVE protocol stack.

layer and IEEE 802.11p at the underlying layers. WAVE supports both IP and non-IP applications. The applications control the physical properties of the transmission channel using the WSMP protocol in non-IP applications. The two device topologies required by WAVE are OBUs and RSUs. RSUs are static entities by the road side, while OBUs are placed inside trucks and capable of communicating with other RSUs and OBUs. Both the RSU and OBUs possess the capability of organizing themselves to form smaller networks referred to as Wave Basic Service Set (WBSS). The WBSS comprises of either only OBUs, or combination of RSUs and OBUs.

IEEE 802.11p defines the data transmission of the protocols along with the management functions of physical and data link layers. The WAVE units may need division of their time between the Service Channel (SCH) and the CCH. This necessitates the inclusion of a sublayer at the level of the OSI layer 2 in the WAVE protocol stack, for dedicated control of the multichannel operation that IEEE 1609.4 specifies for this sublayer. The IEEE 802.2 standard is followed by the logical link control layer, that is the remaining part of OSI layer 2. For the level of OSI layers 3 and 4, the standard IEEE 1609.3 [44] is responsible for specifying WSMP and defines inclusions of UDP, TCP, and IPv6 in the systems. The defined set of management functions is utilized for providing networking services. The standards IEEE 1609.1 and IEEE 1609.2 [50] support the resource manager and security service block, respectively. Certain advantages of the 802.11 standard makes it suitable for usage in the vehicular domain. IEEE 802.11 is a stable standard, and therefore supports interoperability between trucks of various companies as well as the various road side infrastructures placed at diverse locations. In spite of the efforts invested for the improvement of the WAVE functions, a recent study in [51] have identified different challenges that need attention in future research.

2.4.3. LTE

The standardization process of LTE-based Vehicle-to-Everything (V2X), which provides support for solutions related to V2X communications in truck platoons, was undertaken by the 3rd Generation Partnership Project (3GPP) [40]. The standardization of LTE also benefited from deployment of LTE system worldwide and its rapid commercialization. The 3GPP standardization progress redefined the LTE-based V2X as LTE-V2X. The LTE release 14 [52] contains more than 30 studies which includes LTE-V2X. Presently, researchers and industries are given preference to LTE mobile networks for communication between the road side infrastructure and trucks.

The advantages of LTE in relation with V2X communication in truck platoon include providing greater mobility support, high network capacity and enhanced coverage when compared with IEEE 802.11p. The drawback in LTE occurs due to higher latency under the influence of increased network load [53,54]. To overcome this limitation, V2X communication is facilitated using the micro-cells over LTE-enable smart phones or vehicular on-board units [53]. The Qualcomm's Snap-dragon X5 LTE modem is an example of LTE OBU. With the standardization of LTE-V2X, the V2X communication is also being aided with the LTE device-to-device. In [55], the authors cited that hybrid approaches which combine LTE and IEEE 802.11p, are also appropriate for V2X communication.

The standardization required for supporting LTE-V2X communication in truck platoon is planned to be completed soon for obtaining improved system performance and responding to upcoming market potential [56,57]. Recently, some research projects and field tests are being conducted in some countries based on the development of LTE-V2X standardization in 3GPP. For example, in China, official allocation of 20 MHz frequency is done for validation of LTE-V2X in six pilot areas. The LTE stakeholders and automotive industry are cooperating with each other for promoting V2X solutions based on new directions in truck platoons.

3. Security challenges and requirements in truck platoons

In this section, we discuss the security challenges and requirements in truck platoons. Particularly, in Section 3.1, we discuss the security challenges for truck platoons. In Section 3.2, we put forward the functional requirements for truck platoons. We present the security requirements for truck platoons in Section 3.3. Finally, we provide attack classification in various network layers of truck platoons in Section 3.4.

3.1. Security challenges

We list below the primary security challenges for truck platoons.

3.1.1. Attack prevention

Future vehicular communication including trucks is foreseen to support applications of various kinds and allied services. For enabling these activities, trucks will need to transmit critical data, for example, truck identity, that requires maximum security for acceptance from the perspective of the total communication system.

3.1.2. Forward-compatible security architecture

The truck platoon technology and security architecture should be commensurable with the latest and future vehicular technologies. Integration of security and privacy features is facilitated by the hooking concept that preserves the compatibility factor. The hooking concept places inter-layer proxies at different points of the communication stack. This restricts only the need for the configuration of the intermediate layers, if there are any requirements for transferring the security features to new platforms.

3.1.3. Users' trust and privacy

As any system may be exposed to threats, ensuring the users' trust is a major challenge to overcome. It is not at all desired that trucks are vulnerable to privacy issues or traffic rules violations. Therefore, effective measures for protecting users' privacy need to be developed.

3.2. Functional requirements

In this section, we present the major functional requirements for secure truck platooning.

3.2.1. Network topology

The network topology in truck platoons is highly dynamic in nature, mainly due to its mobile nature. This aspect results in a difficult challenge to face, specifically considering the security frameworks. Generally, trucks move with high velocity, resulting in connections for shorter duration. Therefore, imbibing the security specifications with the quality of communication that depends on the high velocity trucks, comes as a big task.

3.2.2. Heterogeneity

The heterogeneity of future truck platoon networks is the outcome of implementation of different network infrastructures globally. So, the truck manufacturers will focus their technicalities based on their respective country's security and privacy policies. Therefore, appropriate synchronization between the adopted security features by the manufacturers and the truck platoon technology is hard to achieve.

3.2.3. Communication latency

Latency in platoon communication can be due to issues such as, understanding the methods of collecting correct information and disregarding the rest, data that needs to be processed, and the ones that should be transmitted and received. So, communication latency should be addressed in truck platoons in such a manner that safety and security critical situations can be handled in real time.

3.2.4. Data priority

The truck platoon network should have the ability to prioritize data received from different sources. Data processing should take into consideration prioritization, buffering and queuing techniques for ensuring a robust and efficient data communication link. The data received from security critical sectors must be allocated the highest priority, so as to prevent collateral damage in the network.

3.2.5. Insider attacks

The platoon is vulnerable to insider as well as outsider attacks. An example of insider attacks in truck platoons can be when an attacker uses either a malignant control law or provides false reports about its behavior. Such attacks may result in causing unusual circumstances in truck platoons and finally lead to fatal accidents. Another example can be of an attacker exploiting the platoon controller for causing a high speed accident with the truck following it.

3.3. Security requirements

Data exchange among trucks in a truck platoon deals with communication related to both V2I and V2V. Example of an attack scenario can be an attacker compromising a truck and triggering false hazard warnings. False warnings impact all the trucks connected together in the communication stream. Likewise, there is a possibility of forging of the transmitted messages with the intention of misleading other trucks in the network. Also, truck platoons will depend on information obtained from inter-vehicle communication channels and on-board sensors to make driving decisions and achieve platooning. But such dependence may generate an opportunity for attacks related to safety violation, motivated for disruption of platoon creation and resulting in accidents [58]. All the previous examples demonstrate the significance of achieving the security requirements in truck platoons. Considering the broader perspectives that platoon communication handles, it is very true that attack exploitation is possible in a large scale. The major challenge lies in designing secure protocols for the correct detection and defense mechanisms against the attackers.

To enhance the users' trust in platoon technology, there is a need to develop trustworthy systems. These systems must be capable of satisfying the needs of the system users with respect to security, privacy, reliability, and integrity. The first major step in achieving trustworthiness is appropriate acquiring of the security requirements. The security requirements vary, depending on the different attack approaches. In the context of truck platoon security requirements, we reviewed several state-of-the-art works that dealt with various attacks (see Section 3.4) and identified the following major security requirements.

- **Authentication.** It implies that the receiver is sure that the messages received are from a genuine sender [59]. Basically, it permits the receiver to validate the source of the message, and whether the source is actually the one that it claims to be.
- **Integrity of system and communication.** The integrity of system and communication is validated, if the transmission of messages from source to destination occurs without any interference and tampering of the system, and reliability and accuracy of message communication can be guaranteed at the destination [60, 61].
- **Security property authorization.** It serves for granting access to specific services for the various network entities. The property of access control authorizes a truck for performing actions in the network that are allowed, e.g., the network protocols that the truck can execute [62].
- **Confidentiality of system and communication.** This requirement ensures non-disclosure of certain resources to unauthorized users [63]. Generally, confidentiality is achieved by involving a set of rules that limits access to certain resources.

- **Availability.** The availability requirement guarantees secure, fault tolerant protocols that are able to restabilize themselves after fault elimination [64].
- **Privacy and anonymity.** Communication in truck platoon should ensure protection of the privacy of network users. Therefore, in the context of a broader area, privacy refers to information/data hiding, while anonymity is considered as a subset of privacy in platoons.
- **Data verification.** This requirement is for eliminating false messaging. In general, the verification of data consistency with similar messages is used for detecting data correctness [65], particularly between neighboring trucks.
- **Non-repudiation.** Non-repudiation ensures that when a recipient identifies the source of message, the source takes complete responsibility and cannot deny later of its role [65]. One can retrieve the information about the source from the tamper proof device located in OBU even after any crash or accident.
- **Traceability and revocability.** Generally, due to security reasons, the real identity of the trucks might be hidden from third parties. This requirement ensures the ability to retrieve trucks' real identity even if the real identity of that truck is hidden from others [65].

3.4. Taxonomy of attacks in network architectural layer

In this section, we present a taxonomy of attacks in every network architectural layer of truck platoon. In this work, we classified the attacks according to network architectural stack or layer. However, other classifications are also possible like composite and atomic attacks, active and passive attacks.

3.4.1. Application layer attacks

The application layer of network architecture layer of truck platoon directly interacts with the application and provides common application services. Therefore, to launch attacks, an attacker exploits some applications to capture and analyze application specific information, e.g., acceleration, location and packet loss characteristics of trucks. All these information helps the attacker in detecting future behaviors of other trusted trucks in the platoon. The major attacks in application layer are as follows: illusion attacks, false position attacks, impersonation attacks, and repudiation attack [66]. A brief discussion on the application layer attacks is provided below.

Illusion attack. In illusion attack, the attacker broadcasts false traffic warning messages depending on the current road situation, that mislead other trucks in the platoon. Initially, the attacker creates or realizes a suitable traffic scenario by capturing and analyzing the application specific information to prepare the current road situation. Therefore, when other trucks receive corresponding false information message, they are more likely to believe in them. These illusionary messages can lead to traffic jams, accidents and can decrease the performance of the platoon.

False position attack. In this type of attack, the attacker circulates error messages containing incorrect locations of the trucks. This type of attack has a significant impact on platooning, as the major part of the security depends on the truck location. Misleading information about the truck's position can lead to reduction in packet delivery, as the intended recipients may not receive the packets. Overall, communicating incorrect messages leads to a decrease in performance, reliability and security.

Impersonation attack. In this attack, the attacker convinces the victim trucks that it is the genuine truck which has sent the messages, that are actually corrupted. To carry out this attack, an attacker captures and analyzes application services. Every truck has an unique identity, with which it is recognized in the platoon environment. The attacker truck changes its identity, posing as the original truck, leading to circulation of falsified information in the network.

Repudiation attack. The attacker denies or attempts to deny its participation in communication. It results in common identity of two or more trucks, thus making it almost impossible to distinguish the actual truck from the attacker one.

3.4.2. Transport layer attacks

The transport layer of network architecture layer of truck platoon deals with several security aspects like authentication, end-to-end secure communication through data encryption, packet corruptions and loss. By leveraging the weaknesses in security aspects, an attacker can carry out the following attacks: man-in-the-middle attack, GPS spoofing attack, session hijacking attack, covert channel attack [66]. A brief discussion about these attacks are given below.

Man-in-the-middle attack. Truck platoon is highly susceptible to this attack in different contexts. The attacker positions itself between the two communicating pair of trucks, i.e., between the sender and the receiver. Also, the attacker takes over the control of the communication between the two communicating trucks. The man in the middle attack [67] violates integrity, authenticity and non-repudiation issues in the truck platoons.

GPS spoofing attack. This attack is also known as tunnel attack. The attacker overrides a GPS simulator for transmitting false information to the trucks by exploiting weaknesses in the existing security mechanisms, e.g., authentication, data encryption. The signals that are produced by the GPS simulator are stronger than the ones produced by the GPS, leading to ignoring of the correct GPS signals by the drivers [68].

Session hijacking attack. Generally, at the beginning of every new session, authentication is done. However, at the beginning of the session establishment, an attacker spoofs IP address of a legitimate truck and inserts the correct sequence number to block other trusted trucks. Consequently, the genuine truck whose IP address was used, becomes unavailable for a session. Later the attacker controls the session among the trucks, resulting in what is known as the session hijacking attack [68].

Covert channel attack. Generally, a covert channel is defined as any communication channel that can be exploited by a process to transfer information in a way that violates the system's security policy [69]. In truck platoon, a covert channel attack maliciously (or, without authentication) transfers packets between two possibly malicious trucks by exploiting the communication channels that are not intended for data transfer. Due to the bypassing of authentication procedure, this attack destroys the topology-based communication cooperation and algorithms. Broadly, there are two types of covert channel attacks, (i) timing-based, and (ii) storage-based [70]. In timing-based covert channel attack, an attacker modifies only the timing of packets, e.g., inter-arrival time or jitter to transfer bits of data covertly, however, the data contents remain intact. On the contrary, in storage-based covert channel attack, an attacker hides data in shared resource, e.g., a storage location.

3.4.3. Network layer attacks

The transport layer of network architecture layer of truck platoon is responsible for establishing an optimal and efficient route to broadcast information easily and quickly to other trucks in the platoon. Therefore, any attack during routing might interrupt the overall communication and paralyze the platoon. The most prominent attacks in this layer are worm hole attack, black hole attack, flooding attack, packet dropping attack, location disclosure attack, DoS attack and sybil attack, we now discuss each of these.

Worm hole attack. In this attack [40], the attackers make use of tunnels that are responsible for transmission of the major network traffic. This makes it easier for attackers to gather important information. Also, it may result in the attackers having the ability of controlling the traffic using the collected data and launching serious attacks by analyzing the collected information. The detection of this type of attack is difficult, as it usually has no effect on the normal network performance.

Black hole attack. In this attack [40], the attacker receives packets from the network, but denies participation in routing of the received data. This causes updating of the routing tables in an untimely manner. Therefore, legitimate users are prevented from receiving important information, mainly due to the fact that the attacker declares itself to be a part of the network, though in reality it is not so [71].

Flooding attack. In such type of attacks, the attacker generates network traffic with the motivation of exhausting network resources such as bandwidth, power and other similar resources. Flooding attacks can be categorized into two types: data flooding and routing control packets flooding. The consequences of each type of flooding attack are the same. The legitimate users do not have access to the network resources. For a data flooding type of attack, the attacker generates bogus data packets and transmits them to each truck. For a route request flooding attack, the attacker performs the task of broadcasting the route request control packets to all trucks that do not form the platoon network [72].

Packet dropping attack. In this type of attack, the attackers act as forwarders for dropping packets. The attackers either drop all packets, referred to as black hole attack or drop packets selectively, which is known as gray hole attack [73].

Location disclosure attack. The attackers have an impact on the message confidentiality transmitted between the trucks in a platoon. The attacker gathers the location information of a truck using broadcast message. For the drivers, location privacy and anonymity are important issues that need protection. The attackers launch this attack to retrieve the location of a truck and gather privacy related information of the truck drivers [72].

Denial of Service (DoS) attack. DoS attacks comprise of a group of attacks that target the network service availability. These attacks may have serious impacts on the performance of applications in the truck platoon. Here, the attackers can be either internal or external. The primary objective of the attackers lie in disrupting the means of communication as well as disturbing normal services, such that they are unavailable to legitimate users [71].

Sybil attack. The attacker here generates several trucks on the road with identical identity. Thus, the other trucks on the road are duped and thereby, end up sending messages to false recipients, resulting in the benefit of the attacker [74].

3.4.4. Medium Access Control (MAC) layer attacks

The MAC layer of network architecture layer of truck platoon maintains one-hop connectivity among the trucks. The attacks in this layer mainly disrupt the cooperation of the various MAC protocols. The prime attacks in the MAC layer are as follows: illusion attack, impersonation attack, jamming attack and collision attack. We briefly discuss each of these attacks below.

Illusion attack. Similar to the application layer, the illusion attack has severe impact on the MAC layer. In the MAC layer, this attack mainly affects the integrity and data trust for vehicular communication. Here, false data is generated by the attackers to disrupt the cooperation of MAC protocols. The false data generated by the attackers have free access in the network and rely on interaction with drivers for taking decisions. The attacker gets attached with the network in an authentic manner, resulting in difficulty in tracking it [75].

Impersonation attack. Similar to the application layer, this attack has considerable impact on MAC layer as the attacker changes its identity and poses as the genuine sender of a message [76]. Therefore, fabricated messages are transmitted to the trucks, thereby compromising the integrity of the platoon network.

Jamming attack. The attacker acts as a jammer and sends radio signals in a continuous manner to interfere with the communication between the trucks. This results in the transmitter or the receiver of the message to assume that the status of the communicating channels are busy for transmission or reception. Therefore, the recipient truck inside the jammed area is unable to receive legitimate messages sent by the sender truck [77].

Collision attack. This attack is responsible for causing packet loss, localization error and integrity violation of the information transmitted [78, 79].

3.4.5. Physical layer attacks

In the physical layer, the attacker intercepts or disrupts link characteristics to carry out several attacks. The most prominent attacks in the physical layer are eavesdropping attack, GPS spoofing attack, jamming attack and message altering attack. Here is the brief discussion about these attacks.

Eavesdropping attack. This is a passive form of attack, where the attacker only listens to the communication medium without the victim being aware of it. The confidentiality of the transmitted messages is compromised in this attack. This attack facilitates in collection of certain useful information that may aid in truck tracking.

GPS spoofing attack. Similar to the transport layer, the GPS spoofing attack has significant impact on the physical layer. In this attack, the attacker supersedes the communication link/signal generated by the genuine truck to send GPS information. As a result, an attacker successfully injects false position information to other truck(s) in the platoon by using GPS signals [80].

Jamming attack. Similar to the MAC layer, this attack has severe effect in the physical layer. Basically, in the physical layer, jamming of radio signal by the attacker causes packets to be dropped. In order to jam the radio signal, an attacker generates a stronger signal to supersede the target signal.

Message altering attack. This attack takes place when an attacker performs modifications in existing data [81]. This attack results in delaying the transmission of the information, replaying previous transmissions, as well as modifying the actual entry of the transmitted data.

In summary, Fig. 5 presents all of the aforementioned attacks and the respective layers in which they operate. It is worth noting that there are several attacks which have significant impacts on several layers. For example, both illusion and impersonation attacks has impacts on both application and MAC layers. Similarly, GPS spoofing attack has considerable impact on both transport and physical layers. Although, several attacks exists in different layers, however, it is not possible to realize such attacks for a particular layer independently of the others. It means that GPS spoofing attack cannot be realized only for transport layer. Alternately, GPS spoofing attack has always impacts on both transport and physical layers.

After presenting the network architectural layer with attacks in truck platoon, we now discuss about the different attacks that affect the communication security in truck platoon. The basic security properties such as availability, confidentiality, authentication and data integrity are affected due to attacks during the communication of truck platoons. Availability in truck platoon is affected by jamming and DoS attacks. Likewise, the confidentiality in truck platoons gets affected due to eavesdropping and main in the middle attack. The attacks such as GPS spoofing, masquerading, impersonation and message tampering have an impact on the authentication of truck platoon. Data integrity suffers due to replay attack and message modification attack. The modifications of the control algorithm happen when the truck platoon is under the influence of destabilizing attack, high-speed collision induction attack and traffic flow instability attack. The tampering of sensor reading occurs because of false data injection attack and efficiency motivated attack.

<table>
<tr><th colspan="2">Layers</th><th colspan="2">Protocols</th><th>Attacks</th><th rowspan="7">Message Tampering Attack, Replay Attack</th><th rowspan="7">Sybil Attack</th><th rowspan="7">DoS Attack, DDoS Attack</th></tr>
<tr><td colspan="2">Application Layer</td><td colspan="2">Resource Manager (IEEE 1609.1)
Security Services for Application (IEEE 1609.2)</td><td>Illusion Attack
Impersonation Attack
False Position Attack
Repudiation Attack</td></tr>
<tr><td colspan="2">Transport Layer</td><td colspan="2">UDP/TCP (IEEE 1609.3)
Wave Short Message Protocol WSMP (IEEE 1609.3)</td><td>Man-in-the-middle Attack
Session Hijacking Attack
Tunnel Attack
Covert Channel Attack</td></tr>
<tr><td colspan="2">Network Layer</td><td colspan="2">Security Services (IEEE 1609.2)
Networking Services IPv6 (IEEE 1609.3)</td><td>Worm Hole Attack
Flooding Attack
Black Hole Attack
Location Disclosure Attack
Packet Dropping Attack</td></tr>
<tr><td rowspan="2">MAC Layer</td><td>MAC Layer</td><td>Multi-Channel Operation (IEEE 1609.4)</td><td>MLME Extension (IEEE 1609.4)</td><td rowspan="2">Illusion Attack
Jamming Attack
Impersonation Attack
Collision Attack</td></tr>
<tr><td>MAC Sub Layer</td><td>WAVE MAC (IEEE 802.11p)</td><td>MLME (IEEE 802.11p)</td></tr>
<tr><td colspan="2">Physical Layer</td><td>WAVE Physical Layer Single Channel Operation (IEEE 802.11p)</td><td>PLME (IEEE 802.11p)</td><td>Eavesdropping Attack
Jamming Attack
GPS Spoofing Attack
Message Altering Attack</td></tr>
</table>

Fig. 5. Network architectural layer with attacks in truck platoon.

4. Defense mechanisms for truck platoon

In this section, we discuss the defense mechanisms that are developed or can be used in order to provide security assurance to truck platoons. We first discuss Detection Mechanism (DM). Then, we present defense mechanisms that can mitigate the detected attacks, i.e., Response Countermeasure (RC), and also prevent the attacks in truck platoons, i.e., Proactive Defense (PD).

Fig. 6 shows the categorization of the defense systems for a truck platoon and examples for each category.

4.1. Detection mechanisms

An intrusion in a truck platoon can be detected by tracking abnormal deviation in the physical properties of trucks or network. Packet Delivery Ratio (PDR) is exploited as an indicator of an attack in a truck platoon in [82] and [83]. Detecting Jamming Attacks in Vehicular Ad hoc Network (DJAVAN) scheme proposed in [82] is based on the rapid change of PDR in the MAC layer and observes the presence of a jamming attack by constantly calculating the PDR and by measuring the variation of the calculated value of PDR during a given window of time. According to the authors, a truck is considered to be jammed if at least one of the following conditions are satisfied.

- When PDR rate decrease is greater than or equal to a decrease rate threshold.
- When the PDR value is less than or equals to the PDR threshold.
- When the rate of PDR decrease is strictly positive until the PDR value is equal to zero.

When a particular truck in a platoon is considered to be jammed, it will broadcast a warning message to other trucks with its current state, direction, jammed time and jammed position. As claimed by the authors, a truck leaves the jamming region when the PDR value is greater than the threshold value and the PDR decreasing rate is less than or equals to zero or the previous value of PDR is zero and PDR decreasing rate is negative. Once a truck leaves the jamming region, it will broadcast a warning message to other trucks in the platoon which contains position, direction and time. To conclude, DJAVAN provides necessary tools for each truck in the platoon to detect a jamming attack.

A centralized PDR based DoS detection scheme is proposed in [83]. This scheme utilizes the concept of “Protection Node” where one node on the Vehicular Ad hoc Network (VANET) will be selected based on its importance and then divided into multiple levels using a hierarchical architecture. The centralized PDR based DoS detection scheme works in four steps, which are Local Protection Node (LPN) selection, appointment of LPN, detection, and behavior-based profile creation. In the LPN selection, higher level nodes send a LPN Request (LPNREQ) to lower level nodes, and the lower level nodes transmit LPN acknowledgment (LPNACK) back to the appropriate higher level sender nodes (i.e., protected higher level nodes). Then, the protected higher level nodes confirm with the lower level nodes. In the appointment of LPN, lower level nodes are used to protect LPNs. During detection, LPNs alert that there is a DoS attack in the VANET. Profiles are created by monitoring the characteristics of each node’s activities such as bandwidth consumption, speed and packet sending rate in the VANET in the last step.

The authors of [84] proposed a data mining based detection scheme to detect faulty or malicious vehicle in a VANET. As stated by the authors, the scheme is called VANET Association Rules Mining (VARM) which collects data from a single node regarding each neighbor transmission and obtain temporal correlation rules between truck nodes involved in the range in order to detect faulty or malicious truck nodes. In order to accomplish this task, each truck node in the VANET stores the information received from the route messages in a database known as temporary transaction database. VARM can derive generic bases of association rules regarding an event that can be produced by a truck node which is achieved by using itemset-tree to enhance storage compression. In the final step, divide and conquer algorithm is utilized to extract frequently closed itemsets with their associated minimal generators, as a result, VARM is able to differentiate malicious truck nodes from legitimate truck nodes.

Table 2 summarizes the detection mechanisms that detect attacks in truck platoons.

4.2. Response countermeasures

Response countermeasures can both detect and mitigate attacks in a truck platoon while detection mechanisms can only detect an attack [85]. An attack on a truck platoon, which is launched via wireless channels such as a jamming attack, can be mitigated by using additional wireless communication channels, since the legitimate data and information can be transmitted through other wireless channels

Table 2
A comparative summary on detection mechanisms.

Work	Methodology	Attack	Strength	Weakness
[82]	Compare rapid changes in PDR to a predefined threshold	Jamming	Trucks leaving the jammed area can warn other trucks about the jamming	Verification and validation on actual hardware is not completed
[83]	Based on LPN scheme	DoS	Ability to create behavior-based profiles for each truck in the VANET	Additional hardware is required
[84]	Based on Data mining scheme (i.e., Temporal Correlation between truck data)	Impersonation	Can locate the malicious trucks	Verification and validation on actual hardware is not completed; Accuracy of events correlation extraction is not verified

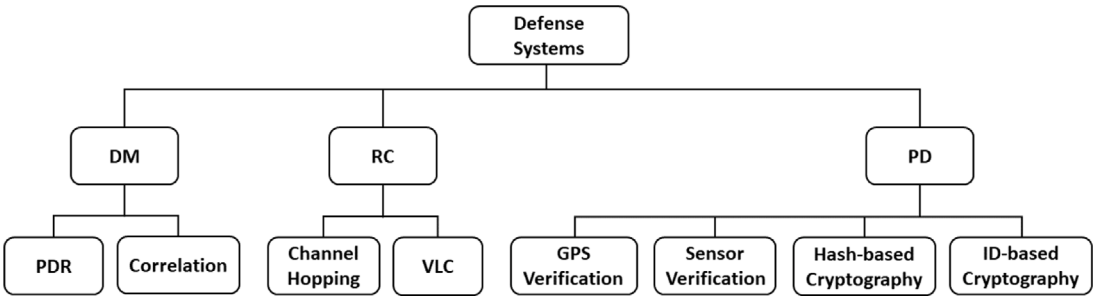


Fig. 6. Categorization of defense systems for a truck platoon.

once a channel is attacked. We focus on the mechanisms that can mitigate the detected attack and consider two cases: (1) channel hopping and (2) heterogeneous channels.

4.2.1. Channel hopping

Channel hopping is the process where communicating nodes hop to another channel and try to synchronize with other nodes in the network. When a certain node cannot initiate communication with other nodes for a certain period of time, it starts to sense other channels to find out whether neighboring nodes have hopped due to the presence of a jammer [86]. Various research works have been proposed which utilize channel hopping in the context of wireless sensor networks and Mobile Ad Hoc Networks. However, no applications to VANETs were found. According to the authors of [87], the VANETs channels are pre-assigned and fixed in their spectrum according to the IEEE 802.11p standard.

4.2.2. IEEE 802.11p and Visible Light Communication (VLC) hybrid communication

In addition to using just RF signals with multiple channels, the authors of [88,89] opted VLC as a secondary transmission medium. The underlying idea of using VLC in both cases is to shorten the message delivery delay under RF jamming attacks by forwarding control messages from the leader using both IEEE 802.11p wireless communication and VLC interfaces. While the authors of [88] utilize VLC mainly as an alternative communication medium to maintain platoon stability under jamming attacks, the authors of [89] decided to use VLC not only as a mitigation strategy against jamming attacks but also against attacks such as data packet injection, channel overhearing and platoon maneuver attacks.

In [88], the protocol of radio and visible light hybrid communication is exploited under a jamming attack. A platoon leader sends control messages by utilizing both radio and multi-hop VLC interfaces on the assumption that even if a platoon member fails to receive a message through wireless radio interface, it will be able to receive an exact message via VLC interface as illustrated in Fig. 7. Once a platoon member receives a control message from the platoon leader, it forwards the message via both VLC and radio interfaces. Additionally, a particular platoon member checks the control message's timestamp to ensure that it is not forwarding any older messages, which could lead the platoon to an unstable state. However, forwarding messages

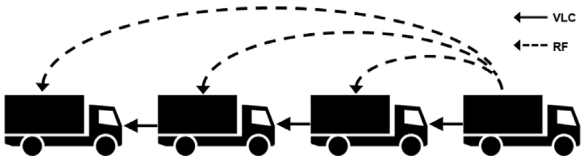


Fig. 7. Hybrid communication method exploits both RF and VLC communication channels.

through radio interface could increase the congestion in radio channels even under jamming attacks. Therefore, the authors have adopted the following two strategies to avoid the frequency that the platoon members use for forwarding messages received via the radio interface.

On the other hand, [89] detects platoon jamming by periodically checking the reception of messages from following and preceding members in the platoon. If there are no messages received in a given window of time through the IEEE 802.11p radio channel, the truck decides that there is a jamming attack in progress. Therefore, the platoon will switch to VLC only communication until trucks in the platoon sense that the IEEE 802.11p radio channel is idle again. The authors have adopted the Diffie–Hellman key exchange method to securely construct the initial secret key in order for the communication between a truck that intends to join the platoon and one of the members already in the platoon or a truck which recently joined the platoon and its preceding/succeeding platoon member. This secret key establishment provides protection against jamming and platoon maneuvering attacks. Authentication of the message is fulfilled by employing block Cipher-based Message Authentication Code (CMAC) algorithm, where both authenticity and the integrity of the message are verified. This ensures that the message has been recently generated by a legitimate platoon member.

Table 3 summarizes the response countermeasure mechanisms that detect and mitigates attacks to truck platoon.

4.3. Proactive defenses

An attack on a truck platoon can be prevented if a secure and reliable defense mechanism is implemented in a truck platoon in advance, which includes verification and cryptography. We first discuss two verification-based mechanisms and cryptography-based mechanisms,

Table 3
A comparative summary of response countermeasure mechanisms.

Work	Methodology	Attack	Strength	Weakness
[86]	Channel hopping	Jamming	Finding the hopping pattern is nearly impossible for adversary	Requires sometime to get synchronized with the other nodes in the network once hopped to a new channel; The channels are pre-assigned
[87]	Channel hopping	Jamming	Finding the hopping pattern is nearly impossible for adversary	The channels are pre-assigned
[88]	Hybrid communication (IEEE 802.11p and VLC)	Jamming	Trucks can still receive messages through VLC channel during a jamming attack	The Functionality of VLC is limited to maintaining the stability of the truck platoon; VLC has to be established in line-of-sight
[89]	Hybrid communication (IEEE 802.11p and VLC)	Jamming Eavesdropping Illusion	Can verify both authenticity and integrity of a message using CMAC algorithm	The functionality of VLC is limited to maintaining the stability of the truck platoon; VLC has to be established in line-of-sight

respectively. The first verification-based mechanism cross-checks GPS data with the map data, and the second mechanism exploits the fact that the sensor data in a truck platoon is correlated. The cryptography-based mechanisms include hash-based cryptography, which uses algorithms such as elliptic curve digital signature algorithm, and ID-based cryptography, which proposed new protocols for a truck platoon.

4.3.1. GPS verification

The authors of [90] have introduced GPS verification which utilizes data from GPS module and map data to detect deviation of platoon members from the expected course during a jamming attack via error corrections and warnings, delivering an independent system which could monitor the state of the truck that is not subjected to similar type of interference as the inter-truck communication medium. During the process of GPS verification, the acceleration data recorded by the corresponding sensors of the truck are compared with the values which are typically expected to give the current location of the truck on the map. In addition, the authors have conducted extensive simulations with activated and deactivated GPS verification. The authors have revealed that with disabled GPS verification, the truck will immediately accept any acceleration input since the truck is unable to deduce if the acceleration data is valid or erroneous due to network error that can destabilize the truck platoon in the worst case. However, when GPS verification is activated, even a single change in the course that is not in agreement with the map data will be voted off since the truck assumes this is due to erroneous data and ignores the change, which will preserve the stability of the platoon in the long run.

4.3.2. On-board sensor verification

Research works summarized in this section capture capabilities of on-board sensors such as cameras, integrated sensors in Lane Departure Warning System (LDWS) and CACC to detect and/or mitigate sybil, jamming and GPS spoofing attacks respectively. As one of the earliest mitigation strategies for sybil attacks, the authors of [91] have developed a sensor-driven heuristic approach, (i.e., Adversarial Parsimony) which in simplest terms translates to finding the best possible explanation for inconsistent data received to identify the source nodes with high probability in order to detect and mitigate sybil attacks. To improve the node's ability to verify whether a particular node's claimed position is true, the authors have adopted cameras and visible as well as infrared spectrum allowing legitimate nodes in the VANET to exchange data. Once the data exchanging phase has been concluded, the heuristic engine detects inconsistencies in data by contrasting received data to a VANET model maintained in each node in order to distinguish malicious nodes from legitimate nodes. However, the introduced detection mechanism is neither supported by simulations nor with test-bed setup.

The authors of [90] have derived a jamming detection mechanism by utilizing LDWS since this technology was developed aiming at truck monitoring and it is widely offered with many modern trucks currently offered by manufacturers. With this mechanism, the data (information from truck sensors such as video, laser or infrared) from the LDWS and acceleration data is compared with the data received from the preceding truck to detect interference in inter-truck communication medium due to the presence of jamming attack.

The proposed GPS spoofing detection and mitigation system utilize CACC systems commonly used in truck platoon for data sharing and inter-truck ranging [92]. As per spoof detection scheme, the measurement of the radar range is compared with the difference between two GPS locations for the two receivers to compute the GPS range. Once the appropriate thresholds are calculated using deviations of ranges, the algorithm compares GPS range and radar range with the threshold values computed in the previous stage and inspects if GPS and radar range exceed threshold values of the algorithm proceeds by assessing the newer measurements. However, if the algorithm discovers the GPS and radar range do not exceed the threshold, it will fall back to the first step of the process where it calculates GPS range. While assessing succeeding measurements during the next decision-taking step, if the detection algorithm learns that the multiple succeeding measurements exceed the threshold value, the user is acknowledged via an alert and the system moves to its next phase, where the suppression algorithm is used to analyze and remove spoofing signal. According to the authors, at the end of the detection algorithm, the proposed system is aware of which parameters it needs to remove in order to recover the incoming data stream. Therefore, as the first step of the suppression algorithm, designated tracking loops [92] calculate spoofing signals parameters (e.g., estimated signal amplitude, navigation signal, and Doppler frequency). Utilizing these parameters, the proposed replica spoofing signal generator creates a replica signal such that it can be subtracted from the raw intermediate frequency data, yielding cleaned authentic GPS signal. Once the recovery process in the prior step has concluded, in the final step, acquisition and tracking are performed.

4.3.3. Hash-based cryptography

The summary of papers presented in this section leverage hash-based cryptography to detect and/or mitigate message eavesdropping, message modification, replay, impersonation, and sybil attacks. While the authors of [93] proposed a defense mechanism which is lightweight, scalable, does not require additional hardware and contains an unique pool of pseudonyms provided by the Department of Motor Vehicles (DMV), the authors of [94] proposed a novel defense mechanism derived from elliptic curve cryptography, named elliptic curve digital signature algorithm.

The lightweight scalable framework proposed in [93] is a privacy-preserving scheme which do not require vehicles in the VANET to disclose their identities to other entities in the network. The DMV assigns vehicles with a pool of pseudonyms instead of assigning each vehicle with an unique single ID and the unique pseudonyms provided for each truck is then hashed to a common value allowing vehicles in the VANET to use any of the pseudonyms to preserve its identity. It is then stored at RSUs and the DMV. According to the authors, RSUs have the ability to check whether a received pseudonym belongs to the same pool or not. Upon inspection, when a RSU is suspicious of

a sybil attack, it sends the pseudonyms and the hash values to the DMV for further inspection by cross-checking whether the suspicious pseudonyms have been assigned to the same vehicle or not. In case a RSU is compromised by an attacker, the proposed system allows the attacked RSU to be revoked.

The novel Elliptic Curve Digital Signature Algorithm (ECDSA) proposed in [94] is a Hash-based message authentication mechanism which provides strong security for messages exchanged between nodes in the VANET and strong authentication for the destination nodes. As per functionality of this mechanism, the source node generates private and public key pairs, where the public key is available for all the vehicles in the VANET. Then the source node hashes the message using a secured hash algorithm. The message is encrypted using the source node's private key and sent to the destination node. Upon receiving the encrypted message at the destination node, the message is decrypted using the public key yielding the hash of the message. Finally, the destination node will take the message, hash it using a secured hash algorithm and compare the two hashes to check the authenticity of the received message, since a minor changes to the message will result in changing the message hash.

4.3.4. ID-based cryptography

In [95], a Detection Technique against Sybil Attack (DTSA) protocol is introduced, which employs Session Key based Certificate (SKC) to verify the identities among the trucks in the VANET and detect the presence of a sybil attack. On the other hand, the authors of [96] proposed a novel certificate revocation protocol, specifically tailored towards secured VANETs against jamming, data forgery, impersonation and privacy violation attacks.

The authors of [95] proposed a novel DTSA protocol capable of detecting the presence of a sybil attack in a VANET. In addition to sybil attack detection, the authors of [95] claimed that DTSA is capable of protecting the privacy of the truck participating in the VANET using commitment ID as well as verifying the integrity of a message using hash functions and XOR operations. The proposed DTSA protocol assumes that all the trucks are equipped with a hash function, Elliptic Curve Cryptography (ECC), Advanced Encryption Standard (AES) algorithm, a master key and an unique ID. During the execution of the first step of the DTSA protocol, each truck participating in the VANET transmits its unique ID and the master key to a VANET server such that it can be registered. Upon completion, truck A produces an anonymous ID and transmits it to a local VANET server that truck A belongs to. With the help of the VANET server mentioned in the initial step, the local VANET server validates the anonymous ID of truck A. Then truck A and local VANET server work hand in hand to generate a session key and a local certificate to truck A with a session key. In the next step, truck A sends its local certificate based on the session key, road number, message along with the message's hash value to truck B. Upon receiving of the truck A's local certificate at truck B, it validates truck A's ID. If the authentication of the truck A's local certificate based on the session key is not correct, it is suspected that a certain truck in the VANET is trying to attack truck B after stealing truck A's ID (sybil attack). If truck B detects a sybil attack, it will send information to the local VANET server regarding the detected truck. But if the truck A's ID is validated, truck B will take the truck A's message and compute the hash value of the message. The integrity of the A's message will be verified by comparing the computed hash value and received hash value from A. Finally, truck B validates the road number received by the truck A. If the roads are overlapped on a boundary line then it will be selected as the direction they are heading to.

Due to current limitations of Certificate Revocation Lists (CRLs) in VANET, authors of [96] have designed a specific solution which revolves around three revocation protocols namely, Revocation Protocol of Tamper-Proof Device (RTPD), Revocation Protocol using Compressed Certificate Revocation List (RCCRL) and Distributed Revocation Protocol (DRP) to maintain the secured nature of the VANET from the attacks

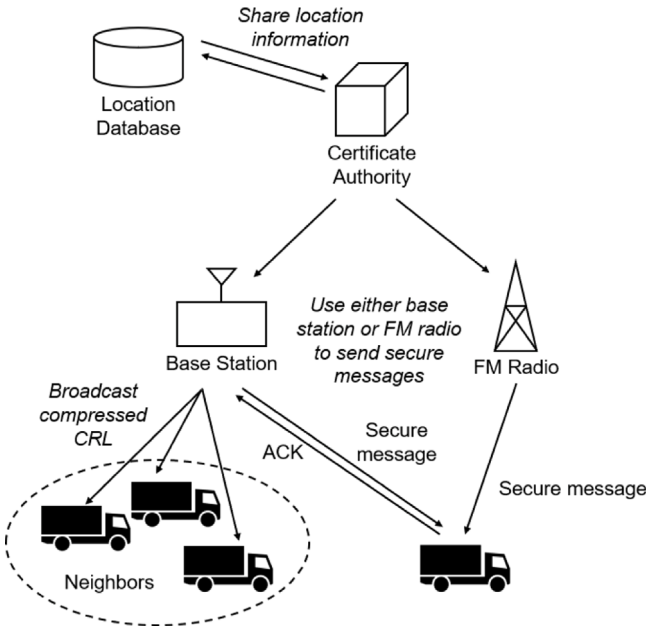


Fig. 8. Illustration of RTPD.

mentioned in the opening paragraph of this section. As illustrated in Fig. 8, once the Certificate Authority (CA) decides to revoke all the certificates of a specific truck in a VANET, the CA sends a revocation message encrypted with that truck's public key. Upon receiving this message, the specific truck decrypts this message and removes all the currently stored keys. It also stops signing safety messages and sends an acknowledgment (ACK) to the CA to inform that the message has been successfully received. The RCCRL protocol is utilized, when a CA wants to revoke a subset of the truck's keys or when the specific truck in the VANET is unreachable. However, compared to RTPD, RCCRL has the ability to warn the neighboring nodes regarding a revoked truck. The DRP protocol which functions purely on ad-hoc mode, is utilized to acquire accusations against malicious trucks in a VANET. Once, these accusations are made, using a reputation system these accusations are evaluated and misbehavior is detected and finally reported to CA by the DRP protocol. In comparison to RCCRL and RTPD, the revocation of DRP is triggered by the misbehaving neighboring trucks. On a surface level, the proposed protocols introduced by the authors eliminate the probability of joining of malicious trucks in a VANET by frequently checking with CA using RTPD and RCCRL protocols, and frequently tagging and reporting misbehaving potential malicious trucks to the CA.

Table 4 summarizes the proactive defensive mechanisms discussed in Section 4.3.

5. Evaluation and lessons learned

In this section, we first summarize (in Section 5.1) the lessons learned for each attack and the respective defense mechanisms as mentioned in Sections 3 and 4 respectively. We next summarize the methodologies of evaluating the performance of a truck platoon in adversarial environments and with the defense system, which includes the software tools and known data sets in Section 5.2.

5.1. Lessons learned

This section discusses the lessons learnt after analyzing the practical scenario of the truck platoons, mostly from the security perspective. We divide the lessons learned on the basis of practical implications of attacks on truck platoons and the defense mechanisms adapted for detection, mitigation and prevention of such attacks on truck platoons.

Table 4
A comparative summary of proactive defensive mechanisms.

Work	Methodology	Attack	Strength	Weakness
[90]	GPS verification	Jamming	Detection of deviations in the location of trucks in a platoon	GPS is based on reception of signals from GPS satellites which can be jammed
	LDWS and acceleration data		Detection of interference in inter-truck communication	Verification and validation on a simulator or testbed is not completed
[91]	Sensor-driven heuristic approach	Sybil	Inconsistency in sensor data is exploited as an attack indicator	Verification and validation on a testbed is not completed
[92]	Sensor-driven Approach	GPS spoofing	GPS data and RADAR data are compared to prevent an attack	GPS is based on reception of signals from GPS satellites which can be jammed
[93]	Cryptography	Eavesdropping Message altering Impersonation sybil	Lightweight hash-based cryptography is implemented for truck platoon	Additional module or hardware is required
[94]	Cryptography	Eavesdropping Message altering Impersonation Sybil	Elliptic Curve Digital Signature Algorithm provides strong authentication and security for message exchange between trucks	Additional module or hardware is required
[95]	Cryptography	Sybil	All members of a truck platoon are identified using session key-based certificate	Additional module or hardware is required
[96]	Cryptography	Jamming Impersonation Message altering	Certificate Revocation protocols for truck platoon	Additional module or hardware is required

5.1.1. Practical implications of attacks

In this section, we analyze and summarize the impacts of attacks on the different security issues in truck platoons. The vulnerabilities in truck platoons are induced as they are exposed to several attack vectors and due to the inherent challenges. We briefly discuss the different attacks that are prevalent in truck platoons and how the truck platoons behave under such attack scenarios or what are the consequences in platoon behavior under such circumstances.

Recent studies verified that attacks on platoons may lead to physical damages and as a result hamper the normal functions of the components of the platoon. Research works have mainly investigated the drawbacks in controls and tried to work on the vulnerabilities, like modification of control law, so that attacker is capable of creating catastrophic impacts on the platoon. This type of impact includes collision in high relative velocity to maximize the damage or oscillation to cause passenger discomfort and increase fuel consumption [26,97,98]. In [99,100], the authors create a scenario in which a group of malicious trucks on a highway perform a cooperative attack for creating undesirable wave effects among other trucks. Mathematical analysis is done for choosing the undesirable wave. This investigation helps to understand the effect of drivers behavior on traffic formation. In [97], the attacker modifies its gains in such a manner that the system becomes unstable and the authors also briefly introduce the controllability of attacker over platoon. To explore this idea further, the authors in [101] studied the reachability of the platoon in presence of an attacker. This study enables the understanding of the attacker's capability in affecting position and velocity of other trucks in the platoon, with its own motion involving acceleration or deceleration. Finally, the authors conclude that the attacker has a very limited capability to disrupt the platoon, by only utilizing acceleration and deceleration when all trucks in the platoon follow normal control law. Additionally, the authors found out that the attacker's attempt would not result in severe damage and current control law has proven to be robust to such attacks. On the other hand, when the attacker combines the motion modification and control law alteration, it can result in this type of attack being more disruptive and causing collisions between one to all trucks.

5.1.2. Defenses

In this section, we analyze and summarize the defense systems that can detect, mitigate, and prevent attacks in truck platoons. We also discuss the implementation of these defense systems in a practical environment. We first categorize the defense systems into three categories, i.e., DM, RC, and PD depending on capabilities of the defense systems. DM can only detect an attack, so a system operator has to remove a detected attack. However, a RC can both detect and mitigate an attack. Consequently, the system operator does not need to act to remove the detected attack. Finally, a PD protects a truck platoon by using preemptive mechanisms, which prevents an adversary from launching attacks.

Recently, many DMs for truck platoons are developed, which detect an attack by tracking abnormal deviations in PDR and correlation between truck data [82–84]. By exploiting a sudden drop in PDR, a DM claims that an attack has occurred and is unable to detect which truck in the platoon launches the attack. A DM that exploits a temporal correlation of the truck data can detect an attack and locate the compromised truck as well. A DM is designed to detect a certain type of attack as shown in [82,83]. For instance, in [82], DM can only detect a jamming attack while in [83], DM detects a DoS attack. As a result, multiple DMs, which detect different types of attacks, might need to be implemented in a truck platoon in order to provide higher resilience to many possible attacks.

Increasing robustness of the wireless channel is a good method that mitigates attack in a truck platoon [86,88,89]. Channel hopping method, which keeps switching frequency of the wireless communication channel according to a predetermined pattern, is considered to be one method that can mitigate an attack in truck platoons. Channel hopping method can be disabled if all the wireless channel is damaged by a jamming attack. Hence, other works developed mitigation methods that exploit another wireless channel that is independent to the RF wireless channel. In [88] and [89], VLC is used as an extra wireless channel complementary to a RF wireless channel. These papers indicate that more number of complementary wireless channels may detect and mitigate attacks in truck platoons.

PDs that exploit GPS data or sensor data were also proposed in recent papers [90–92]. The underlying assumption for these PDs is that these GPS data and sensor data are not spoofed. Hence, many works developed PDs that are based on cryptography [93–96]. Although these PDs use many different cryptography systems to provide security assurance in truck platoon, additional module or hardware is required, which may increase the cost of trucks.

In summary, we present the various state-of-the-art mechanisms designed for defending different attacks of network architectural layers in Table 5. We notice from Table 5 that there no state-of-the-art defensive solutions for a number of attacks, including false position, repudiation, man-in-the-middle, session hijacking, covert channel, worm hole, black hole, flooding, packet dropping, location disclosure and collision attacks in the context of truck platoon.

5.2. Methodologies for performance evaluation

We introduce existing methods that are used for evaluating the performance of attacks on truck platoons and defenses for truck platoons. Commonly exploited methodologies are running of computer

Table 5
Summary of defenses corresponding to attacks in OSI layer.

Work	Defensive mechanism	Methodology	Attack	Ease of attack	Detection probability	OSI layer
[82]	DM	Compare rapid change of PDR to a predefined threshold	Jamming	High	High	MAC layer Physical layer
[83]	DM	Based on LPN scheme	DoS	High	High	All layers
[84]	DM	Based on Data mining scheme (i.e. Temporal Correlation between truck Data)	Impersonation	Low	High	Application layer MAC layer
[86]	RC	Wireless Channel hopping	Jamming	High	High	MAC layer Physical layer
[87]	RC	Wireless Channel hopping	Jamming	High	High	MAC layer Physical layer
[88]	RC	Hybrid communication (802.11p and VLC)	Jamming	High	Moderate	MAC layer Physical layer
[89]	RC	Hybrid communication (802.11p and VLC)	Jamming Eavesdropping Illusion	Moderate	Moderate	Application layer MAC layer Physical layer
[90]	PD	GPS verification utilizing data from GPS module and map data Data from LDWS and acceleration data are compared with data from preceding truck	Jamming	High	Moderate	MAC layer Physical layer
[91]	PD	Sensor driven heuristic approach (i.e., Adversarial Parsimony)	Sybil	High	Moderate	Application to MAC layers
[92]	PD	Comparing GPS range and radar range with computed threshold value	GPS spoofing	High	Low	Physical layer
[93]	PD	Hash-based cryptography utilizing DMV provided unique pseudonyms	Eavesdropping Message altering Impersonation Sybil	Moderate	Moderate	All layers
[94]	PD	Based on ECDSA	Eavesdropping Message altering Impersonation Sybil	Moderate	Moderate	All layers
[95]	PD	Based on DTSA protocol	Sybil	High	Moderate	Application to MAC layers
[96]	PD	Based on RTPD, RCCRL and DRP protocols	Jamming Impersonation Message altering	Moderate	High	Application layer MAC layer Physical layer

simulation in which human is in the loop, implementing a testbed that may prove the concept of attack and defense, and testing attack and defense on a real truck.

5.2.1. Computer simulation

Vehicular Network Open Simulator (VENTOS) is a widely used simulation tool for truck platoons [89,102]. VENTOS is a simulator based on C++, which emulates the flow of trucks, collaborating driving, and interactions between trucks and road side infrastructures. VENTOS can be used to design a truck platoon protocol that supports many different cases of trucks in the platoon, which includes merging multiple platoons, splitting a platoon, entry of a truck, and exit of a truck to/from a platoon. In addition, VENTOS provides an adversary module that can emulate attacks in a collaborative driving [13,103] environment.

Simulation of Urban Mobility (SUMO) is another open source road traffic simulation tool that is developed by the Institute of Transportation Systems at German Aerospace Center [104]. SUMO provides a microscopic simulation, where each truck is explicitly modeled. (i.e., a truck has its own route and moves independently). A routing algorithm can be assigned to each truck to emulate different dynamics of traffic flow.

In order to emulate a discrete event in a generic network, Objective Modular Network Testbed in C++ (OMNet++) can be used, which is a C++-based simulation framework for network protocols [105]. Vehicles in Network Simulation (VEINS) is an open source framework for vehicle network simulations and is implemented based on OMNet++ and SUMO [20,106]. In VEINS, SUMO simulates the road traffic and OMNet++ performs a network simulation using a physical layer modeling package MiXiM. VEINS provides comprehensive models of IEEE 802.11p, IEEE 1609.4 DSRC/WAVE network layers, and cellular network such as LTE, which include multi-channel operation, interference effects, and noise effects.

Many different types of network architectures for truck platoons can be emulated in computer simulation because it is less expensive to change the topology and protocol of the network. Also, a response of a truck platoon to an attack and performance of defense mechanism can be verified under various traffic conditions. When an updated version of a protocol is released, the truck platoon based on the new protocol can be validated and checked for the compatibility with the legacy systems. Despite the benefits of using computer simulation, the models for trucks, traffics, and network are not exactly same as the real world. This gap between the model and real world might result in an inaccurate prediction of a truck platoon, which might cause accidents in real world circumstances.

5.2.2. Computer simulation with human in the loop

The authors of [6] used a computer simulation where human interacts with truck platoons online while the simulation runs. The evaluation of their proposed algorithm for controlling a truck platoon is reinforced by introducing human reaction in the simulation. An action space of the human reaction, however, is limited to the fact that human may only decide when to intercept in a truck platoon. An unexpected adversarial behavior of a compromised truck can easily be emulated and defense mechanisms for a truck platoon are analyzed. Although an attack and defense mechanism on a truck platoon can be verified in a more realistic environment by including human in the loop, different types of human behaviors need to be incorporated in the evaluation.

5.2.3. Real truck testbed

Attacks and defense mechanisms for a truck platoon can be demonstrated using real trucks [4,107]. The authors of [4] collected data from

a real truck while the truck is driven on the road for 280km. They did not implement a truck platoon using multiple trucks. In [107], many existing papers on truck platoons are summarized. For this evaluation method, the trucks need to be modified with additional hardware such as GPS antenna, Inertia Measurement Unit (IMU), cameras, and LIDAR in order to implement a truck platoon. By using real truck testbeds, feasibility of attacks and defense mechanisms can be demonstrated in a real road environment. However, verifying proposed attacks and defense mechanisms on a real truck platoon are costly with respect to money and time. Also, experiments of attacks and defense mechanisms have to be conducted in a safe and controlled environment to avoid any unexpected and unwanted circumstances during the experiments. Table 6 compares three different evaluation methods with respect to benefits, limitations, and examples of tools.

6. Open research issues and future direction

The real life implementation of truck platoon heavily depends on the safety, security and reliability of services provided by such systems. We discussed various existing techniques leveraged from physical properties, communication channel, etc. to safeguard truck platoons from numerous attacks. In this section, based on the literature survey presented in Section 4, we summarize some open research issues, and illustrate them in terms of research problem, current solutions and future research direction.

6.1. Truck platoon protocol perspective

Research problem: In the recent past, cyber attacks has come up as a considerable threat on truck platoons. Particularly, communication protocols associated with the cooperative driving of truck platoon are more vulnerable to numerous attacks, e.g., man in the middle attack, flooding attack, which might lead to traffic chaos, even truck crash on road. Further, a truck in a platoon might suffer major attacks from the road side infrastructure. One such typical attack is the poisoning of navigation map stored on the truck's database. Furthermore, in truck platoons, we notice that there are no security mechanisms during V2V communication, as any truck can join the platoon dynamically. By exploiting this weakness, an adversary can launch various attacks, e.g., jamming attack, impersonation attack, collision attack which may lead to large scale truck crashes.

Preliminary solution: To secure V2V communication, currently trucks use long-term and short-term certificates, i.e, pseudonyms. Basically, trucks use these two types of certificates to sign the messages for preserving authenticity and integrity. In the process of signing, trucks include 108 bytes to the cooperative awareness message and decentralized environmental notification message as a header [108]. Due to such large header size, the computation overhead increases significantly on both sender and receiver trucks in the platoon [109]. Further, such large header size introduces additional communication latency which has severe impact on time sensitive applications under dense scenario.

Future research directions: In our opinion, misbehavior detection mechanism can be one of the research directions to identify malicious truck(s), which launch various attacks leveraging weaknesses in communication protocols. The proposed misbehavior detection technique might work in two levels. In the first level, we can embed misbehavior detection technique into the truck to monitor message exchange for any possible attack. In the second level, we may analyze the messages, that are exchanged in a truck platoon and stored in the cloud, to identify the adversary truck(s).

6.2. Platoon controllers perspective security issue

Research problem: In truck platoons, leader truck mainly coordinates the stable movement of a platoon. Usually, a stable coordinated movement is designated as string stability, traffic flow stability and sensitivity, which guarantee reduction in range error as they propagate along the truck streams to obtain uniform inter-truck gap. A number of platoon coordination techniques have been proposed to gain stable movement of a platoon [110,111]. Nevertheless, these existing platoon coordination techniques are mainly designed and analyzed under ideal scenario, where no malicious truck interferes the normal performance of a leader executing platoon coordination which may result in intelligent collision. It is worth noting that several potential attacks might occur due to the underlying platoon coordination technique. Therefore, it is crucial to thoroughly access the security vulnerabilities in autonomous truck platoons by identifying the issues that might directly or indirectly hinder the coordinated movement of truck platoons.

Preliminary solution: Nowadays, CACC technologies, especially Cruise Control (CC) and ACC, are used for platoon coordination. There are only a handful number of solutions that exist to protect data related to the platoon coordination. For example, Golle et al. proposed a secure platoon coordination mechanism to defend Sybill attack [91]. Particularly, the authors developed a sensor-driven heuristic approach to identify the adversary. On the contrary, Patounas et al. proposed a jamming attack defensive mechanism by exploiting LDWS [90]. In [92], the authors proposed GPS spoofing detection and mitigation system for platoon coordination. However, none of these works have been tested under realistic scenarios. In fact, in most of the cases, the proposed solutions are neither validated through simulation nor test-bed setup.

Future research directions: As far as the security of platoon controller is concerned, we must emphasize on more complex attacks and study their defensive mechanisms. In fact, defensive mechanism alone is likely insufficient to tackle complex attacks. Therefore, we must focus on attack prevention mechanisms by designing resilient platoon controllers on one side, and effective attack detection and mitigation techniques on the other side. Another more interesting aspect of platoon controller security is that, not all attack detection mechanisms are compatible with truck platoons, since the corresponding platoon behavior is distinct. Therefore, one of the possible research direction is to design dedicated misbehavior detection mechanisms specially for a CACC scenario.

6.3. Platoon leader perspective security issue

Research problem: The PL in a truck platoon performs the task of setting the trajectory and speed to the trucks behind it. When the scenario is a distributed control algorithm, the adjustment of the truck movements depends on the knowledge of the preceding truck and the PL truck determines the next movement. The information about the preceding truck is generally obtained from direct hearing and further verification is possible through in-truck sensor data. But the information of the leading truck maybe second hand information, where in case, the truck may not be in the transmission range of the PL. In such cases, the truck receives the status information of the PL indirectly from proceeding trucks. The authenticity of the messages generated by the PL need to be protected as well as the PL, thus preventing the platoon from leader impersonation attack. Identification of the correct leader is more prominent when a new truck joins the platoon.

Preliminary solution: Many research works have been conducted that look into the problem of message authentication [112–114]. Also, implementing an endorsement mechanism might protect the leadership of the leader from impersonation by the use of efficient cryptographic primitives. The establishment of the leadership is achieved through the endorsement of the trucks that are part of the platoon. A truck who endorses the leader cannot deny its establishment. Therefore, the adversary is unable to alter the endorsement even under the circumstance

Table 6
Comparison of methodologies for evaluating performance of attack and defense algorithms.

	Strength	Weakness	Tool	Work
Computer simulation	Various types of truck platoon network architecture can be emulated; various dynamics and conditions of traffic flow can be considered; compatibility of a new protocol can be validated easily	There exists a gap between the model and real world	VENTOS, SUMO, OMNet++, VEINS	[13], [20], [89], [102], [103], [104], [105], [106]
Computer simulation with human in the loop	Algorithms are verified in a more realistic environment	Human action space is limited	Not Applicable	[6]
Real truck testbed	Algorithms are verified and validated in a real environment (Most realistic evaluation)	Implementing testbeds and testing are costly respect to money and time	Not Applicable	[4], [107]

when it is one of the endorsers. One possible cryptographic primitive that may be used for protection of the leadership is through aggregate signature scheme that permits co-signing of one document by multiple entities.

Future research directions: In the context of authentication of messages generated by the leader, many privacy preserving schemes have been proposed by exploiting pseudonyms [115,116] and group signature [117,118]. However, most of the pseudonyms based techniques use public key infrastructure and corresponding certificates, which ultimately increases the computational overhead and communication overhead of the leader truck. Therefore, as a future work, it is the need of the hour to design some advance authentication mechanisms which are not only lightweight in terms of computational overhead but also robust to defend complex security attacks. Another possible future direction could be to design authentication scheme by leveraging fingerprints of leader truck , e.g., received signal strength.

6.4. Platoon member perspective security issue

Research problem: The control and protection algorithms for the follower trucks are to some extent different from the leader truck. The follower trucks are unable to use their camera sensors which possess maximum resistance against cyber security attacks. They are dependent mainly on the received wireless messages which have minimum reliability with respect to cyber security. Further, some malicious leader trucks may jeopardize the entire truck platoon by providing low quality services to the follower trucks. Another major issue with respect to platoon security is the dynamic joining of the platoon member. Specifically, in the truck platoon, a member truck can join or leave at any time. Therefore, how to securely join the member truck for creating and maintaining the truck platoon is a big challenge. Further, ensuring anonymity of platoon members is another critical problem.

Preliminary solution: The control algorithms used by the follower trucks need to revisited and refined to make them more robust against cyber attacks. On the contrary, to overcome the issue of low quality services to follower trucks, Hu et al. [119,120] proposed a promising approach which is based on trust. The proposed scheme integrates a number of realistic factors,e.g., location, destination in order to deliver high quality services. As far as secure joining of member in a platoon is concerned, Lai et al. [121] proposed two authentication protocols. The first protocol exploits attribute-based encryption to authenticate all trucks simultaneously in the platoon. Whereas, the second protocol exploits contributory key agreement technique to ensure anonymous authentication with traceability.

Future research directions: Due to the advent of complex and sophisticated cyber attacks, designing security solutions for platoon members is a non-trivial task. As a future research direction, trust based truck platoon security could be a promising research direction — that can provide strong foundation for forming a secure and reliable truck platoon. Another promising research direction could be to integrate data mining technique to automate the trust model building procedure in truck platoons.

6.5. Sensor perspective security issue

Research problem: Most researchers believe that for successful platoon implementation, wireless communication is essential for coordination among the trucks [22]. But the wireless link is associated with the disadvantage that it is the weakest sensor of the automated truck. Compared to the wireless link, radar, camera and LIDAR are much more robust against attacks. The wireless link is very much vulnerable to attackers. Therefore, relying on wireless communication is not a feasible option if it impacts the control algorithms of the trucks. Recently, it has been found out that attackers are now able to forge radar and LIDAR sensors using a modulated laser [122].

Preliminary solution: The present requirement is of strategies that allow fusing sensor input and is able to detect forged individual input. One possible solution can be assigning confidence levels to sensors and correct sensor input [123], provided the individual sensors demonstrate unreasonable inputs based on the confidence levels. Another promising solution is to design of collaborative control strategy [124,125] in order to improve the protection level of sensors in truck platoons.

Future research directions: Future works may consider more complex strategies to thwart an attacker that has the capability of forging multiple sensors in parallel. Also, different kinds of heuristic mechanisms such as machine learning can be applied for detecting anomalous sensor input. Furthermore, the designing of safe and secure truck platoons require robustness to various attacks on sensors. The possible future research direction could be to design adversarial deep reinforcement learning technique for enhancement of robustness to various attacks on sensors in truck platoons.

7. Conclusion

Platooning trucks on freeways is envisaged as the first step towards automated driving in the truck ecosystem. Truck platoons has the potential of providing cost efficient driving through decrease in fuel consumption as well as providing higher safety to truck drivers. For proper utilization of the benefits of platooning, requires thorough planning of the platoon system. This survey outlines the various security aspects that truck platoons are exposed to, together with the different defense mechanisms that can be used to thwart off such vulnerabilities. This survey primarily provides a brief overview about the truck platoon, their network architecture and the communication protocols. Further, a comprehensive analysis is provided for the attacks that take place in the layers of the network architecture. Furthermore, a classification is achieved for defining the existing defense systems against the attacks that strike the truck platoons. Also, performance evaluation of the truck platoons is done, considering all the lessons learnt along the way. Finally, the survey wraps up with conclusive remarks on the prospective future research directions.

CRediT authorship contribution statement

Amrita Ghosal: Conceptualization, Data curation, Formal analysis, Investigation, Resources, Writing - original draft. **Sang Uk Sagong:** Conceptualization, Data curation, Investigation, Resources, Writing - original draft. **Subir Halder:** Conceptualization, Formal analysis, Methodology, Validation, Writing - original draft. **Kalana Sahabandu:** Data curation, Investigation, Resources, Writing - original draft. **Mauro Conti:** Funding acquisition, Supervision, Writing - review & editing. **Radha Poovendran:** Funding acquisition, Supervision, Writing - review & editing. **Linda Bushnell:** Funding acquisition, Supervision, Writing - review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This work is partially supported by ONR SOTERIA, USA with grant number N00014-20-1-2636.

References

[1] S.W. Lee, S.J. Lee, D.H. Lee, Attack on vehicular platooning and mitigation strategy: A survey, in: Applied Mechanics and Materials, 2017, Vol. 865, 2017, pp. 423–428.
[2] A. Alipour-Fanid, M. Dabaghchian, K. Zeng, Platoon stability and safety analysis of cooperative adaptive cruise control under wireless rician fading channels and jamming attacks, 2017, ArXiv abs/1710.08476.
[3] S. van de Hoef, K.H. Johansson, D.V. Dimarogonas, Fuel-efficient en route formation of truck platoons, IEEE Trans. Intell. Transp. Syst. 19 (1) (2018) 102–112.
[4] K.-Y. Liang, J. Mårtensson, K. Johansson, Heavy-duty vehicle platoon formation for fuel efficiency, IEEE Trans. Intell. Transp. Syst. 17 (2016) 1051–1061.
[5] M. Saeednia, M. Menendez, A consensus-based algorithm for truck platooning, IEEE Trans. Intell. Transp. Syst. 18 (2) (2017) 404–415.
[6] E. Stefansson, J.F. Fisac, D. Sadigh, S.S. Sastry, K.H. Johansson, Human-robot interaction for truck platooning using hierarchical dynamic games, in: Proc. of 18th European Control Conference (ECC), 2019, pp. 3165–3172.
[7] C. Bonnet, H. Fritz, Fuel consumption reduction in a platoon: Experimental results with two electronically coupled trucks at close spacing, in: SAE Technical Paper, 2000, 2000.
[8] M. Segata, S. Joerer, B. Bloessl, C. Sommer, F. Dressler, R.L. Cigno, Plexe: A platooning extension for Veins, in: Proc. of IEEE Vehicular Networking Conference (VNC), 2014, pp. 53–60.
[9] J. Lioris, R. Pedarsani, F.Y. Tascikaraoglu, P. Varaiya, Platoons of connected vehicles can double throughput in urban roads, Transp. Res. C 77 (2017) 292–305.
[10] D. Chen, S. Ahn, M. Chitturi, D. Noyce, Towards vehicle automation: Roadway capacity formulation for traffic mixed with regular and automated vehicles, Transp. Res. B 100 (2017) 196–221.
[11] T.-S. Dao, C.M. Clark, J.P. Huissoon, Distributed platoon assignment and lane selection for traffic flow optimization, in: Proc. of IEEE Intelligent Vehicles Symposium, 2008, pp. 739–744.
[12] E. Talavera, A.D. Álvarez, J.E. Naranjo, A review of security aspects in vehicular ad-hoc networks, IEEE Access 7 (2019) 41981–41988.
[13] P.K. Singh, G.S. Tabjul, M. Imran, S.K. Nandi, S. Nandi, Impact of security attacks on cooperative driving use case: CACC platooning, in: Proc. of TENCON, 2018, pp. 0138–0143.
[14] Bosch, CAN specification version 2.0, 1991.
[15] International standard ISO 17987 road vehicles-local Interconnect Network (LIN), Part 1 general information and use case definition, 2016.
[16] R. Kumar, R. Pathak, Adaptive cruise control-towards a safer driving experience, Int. J. Sci. Eng. Res. 3 (8) (2012) 3–7.
[17] T. Herpel, B. Kloiber, R. German, S. Fey, Routing of safety-relevant messages in automotive ECU networks, in: Proc. of IEEE 70th Vehicular Technology Conference Fall, 2009, pp. 1–5.
[18] C. Miller, C. Valasek, Adventures in automotive networks and control units, in: DEF CON21, 2013, 2013.
[19] C. Miller, C. Valasek, Remote exploitation of an unaltered passenger vehicle, Black Hat USA 2015 (2015) 91.
[20] R. van der Heijden, T. Lukaseder, F. Kargl, Analyzing attacks on cooperative adaptive cruise control (CACC), in: Proc. of IEEE Vehicular Networking Conference (VNC), 2017, pp. 45–52.
[21] N. Jahanshahi, R.M. Ferrari, Attack detection and estimation in cooperative vehicles platoons: A sliding mode observer approach, IFAC-PapersOnLine 51 (23) (2018) 212–217.
[22] D. Jia, K. Lu, J. Wang, X. Zhang, X. Shen, A survey on platoon-based vehicular cyber-physical systems, IEEE Commun. Surv. Tutor. 18 (1) (2016) 263–284.
[23] P. Kavathekar, Y. Chen, Vehicle platooning: A brief survey and categorization, in: Proc. of International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, 2012, pp. 829–845.
[24] T.L. Willke, P. Tientrakool, N.F. Maxemchuk, A survey of inter-vehicle communication protocols and their applications, IEEE Commun. Surv. Tutor. 11 (2) (2009) 3–20.
[25] M.L. Sichitiu, M. Kihl, Inter-vehicle communication systems: a survey, IEEE Commun. Surv. Tutor. 10 (2) (2008) 88–105.
[26] S. Dadras, Security of Vehicular Platooning (Ph.D. thesis), Utah State University, 2019, [Online]: https://digitalcommons.usu.edu/etd/7445.
[27] L. Li, F.-Y. Wang, Advanced Motion Control and Sensing for Intelligent Vehicles, Springer Science & Business Media, 2007.
[28] G. Nardini, A. Virdis, C. Campolo, A. Molinaro, G. Stea, Cellular-v2x communications for platooning: Design and evaluation, Sensors 18 (5) (2018) 1527.
[29] K.-Y. Liang, J. Mårtensson, K.H. Johansson, When is it fuel efficient for a heavy duty vehicle to catch up with a platoon?, IFAC Proc. Vol. 46 (21) (2013) 738–743.
[30] T. Sandberg, Heavy Truck Modeling for Fuel Consumption Simulations and Measurements (Licentiate Thesis), Linkoping University, 2001.
[31] G. Scora, M. Barth, Comprehensive Modal Emissions Model (Cmem), Version 3.01, Vol. 1070, User guide, Centre for Environmental Research and Technology, University of California, Riverside, 2006.
[32] CACI, Truck platoons – the road ahead, 2020, Accessed on July 6, [Online]: https://www.truckstopsrouting.com/truck-platoons/.
[33] A. Kesting, M. Treiber, How reaction time, update time, and adaptation time influence the stability of traffic flow, Comput.-Aided Civ. Infrastruct. Eng. 23 (2) (2008) 125–137.
[34] M. Wang, S. van Maarseveen, R. Happee, O. Tool, B. van Arem, Benefits and risks of truck platooning on freeway operations near entrance ramp, Transp. Res. Rec. 2673 (8) (2019) 588–602.
[35] N. Harwood, N. Reed, Modelling the impact of platooning on motorway capacity, in: Proc. of Road Transport Information and Control Conference, 2014, pp. 1–6.
[36] R. Heilweil, Networks of self-driving trucks are becoming a reality in the US, 2020, Accessed on July 6, [Online]: https://www.vox.com/recode/2020/7/1/21308539/self-driving-autonomous-trucks-ups-freight-network.
[37] A. Sarker, C. Qiu, H. Shen, Quick and autonomous platoon maintenance in vehicle dynamics for distributed vehicle platoon networks, in: Proc. of 2nd International Conference on Internet-of-Things Design and Implementation, 2017, pp. 203–208.
[38] Z. Wang, G. Wu, M.J. Barth, A review on cooperative adaptive cruise control (CACC) systems: Architectures, controls, and applications, in: Proc. of 21st International Conference on Intelligent Transportation Systems (ITSC), 2018, pp. 2884–2891.
[39] K. Abboud, H.A. Omar, W. Zhuang, Interworking of dsrc and cellular network technologies for v2x communications: a survey, IEEE Trans. Veh. Technol. 65 (12) (2016) 9457–9470.
[40] A. Ghosal, M. Conti, Security issues and challenges in v2x: A survey, Comput. Netw. 169 (2020) 107093.
[41] K. Lim, D. Manivannan, An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks, Veh. Commun. 4 (2016) 30–37.
[42] S. Gao, A. Lim, D. Bevly, An empirical study of dsrc v2v performance in truck platooning scenarios, Digit. Commun. Netw. 2 (4) (2016) 233–244.
[43] J. Wang, J. Liu, N. Kato, Networking and communications in autonomous driving: A survey, IEEE Commun. Surv. Tutor. 21 (2) (2019) 1243–1274.
[44] IEEE P1609.3, Wireless access in vehicular environments (WAVE) networking services, 2009, IEEE P1609.3 D1.2.
[45] S. Zeadally, R. Hunt, Y.S. Chen, A. Irwin, A. Hassan, Vehicular ad hoc networks (vanets): status, results, and challenges, Telecommun. Syst. 50 (4) (2012) 217–241.
[46] IEEE Computer Society LAN/MAN Standards Committee, IEEE standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks- specific requirements-part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, 2007, IEEE Std 802.11.
[47] R. Uzcategui, G. Acosta-Marum, Wave: a tutorial, IEEE Commun. Mag. 47 (5) (2009) 126–133.
[48] ASTM E2213-03, Conversion of ASTM E2213-03 to IEEE 802.11x Format, 2004, Doc. IEEE 802.11-04-0363-00-WAVE.
[49] Y.J. Li, An overview of the DSRC/WAVE technology, in: Proc. of International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, volume LNICST-74, 2010, pp. 544–558.

[50] IEEE P1609.2, IEEE P1609.2 trial-use standard for wireless access in vehicular environments - security services for applications and management messages, 2009, IEEE P1609.2 D07.

[51] N.K. Chaubey, Security analysis of vehicular ad hoc networks (vanets): a comprehensive study, Int. J. Secur. Appl. 10 (5) (2016) 261–274.

[52] 3GPP, LTE release 14, 2018, Accessed on October 15, [Online]: http://www.3gpp.org/release-14.

[53] G. Remy, S.M. Senouci, F. Jan, Y. Gourhant, LTE4V2X: LTE for a centralized VANET organization, in: Proc. of IEEE Global Telecommunications Conference (GLOBECOM), 2011, pp. 1–6.

[54] A. Vinel, 3gpp lte versus ieee 802.11p/wave: Which technology is able to support cooperative vehicular safety applications?, IEEE Wirel. Commun. Lett. 1 (2) (2012) 125–128.

[55] Y. Shi, LTE-v: a cellular-assisted v2x communication technology, in: Proc. of ITU Workshop, 2015, Huawei, China, 2015, pp. 1–16.

[56] H. Seo, K.D. Lee, S. Yasukawa, Y. Peng, P. Sartori, LTE evolution for vehicle-to-everything services, IEEE Commun. Mag. 54 (6) (2016) 22–28.

[57] S. Chen, J. Hu, Y. Shi, L. Zhao, LTE evolution for vehicle-to-everything services, IEEE Internet Things J. 3 (6) (2016) 997–1005.

[58] M. Sun, A. Al-Hashimi, M. Li, R. Gerdes, Impacts of constrained sensing and communication based attacks on vehicular platoons, IEEE Trans. Veh. Technol. 69 (5) (2020) 4773–4787.

[59] R.V.D. Heijden, Security architectures in V2V and V2I communication, in: Proc. 20th Student Conference on IT, 2010, pp. 1–10.

[60] A.Y. Dak, S. Yahya, M. Kassim, A literature survey on security challenges in vanets, Int. J. Comput. Theory Eng. 4 (6) (2012) 1–4.

[61] G. Samara, W.A. Al-Salihy, R. Sures, Security analysis of vehicular ad hoc networks (VANET), in: Proc. of International Conference on Network Applications Protocols and Services, 2010, pp. 55–60.

[62] R.K. Sakib, Security Issues in Vanet (Ph.D. thesis), Department of Electronics and Communication Engineering, BRAC University, 2010.

[63] V.L. Hoa, A. Cavalli, Security attacks and solutions in vehicular ad hoc net-works: a survey, Int. J. AdHoc Netw. Syst. 4 (2) (2014) 1–20.

[64] M.N. Mejri, J. Ben-Othman, M. Hamdi, Survey on vanet security challenges and possible cryptographic solutions, Veh. Commun. 1 (2) (2014) 53–66.

[65] H. Hasrouny, A.E. Samhat, C. Bassil, A. Laouiti, Vanet security challenges and solutions: A survey, Veh. Commun. 7 (2017) 7–20.

[66] M. Arif, G. Wang, M.Z.A. Bhuiyan, T. Wang, J. Chen, A survey on security attacks in vanets: Communication, applications and challenges, Veh. Commun. 19 (2019) 100179.

[67] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain, F. Hussain, Marine: Man-in-the-middle attack resistant trust model in connected vehicles, IEEE Internet Things J. 7 (4) (2020) 3310–3322.

[68] F. Sakiz, S. Sen, A survey of attacks and detection mechanisms on intelligent transportation systems: Vanets and iov, Ad Hoc Netw. 61 (2017) 33–50.

[69] D.C. Latham, Trusted Computer System Evaluation Criteria (Orange Book), United States Department of Defense Standard, 1985, pp. 1–116.

[70] A. Cornelissen, Covert Channel Data Leakage Protection (MSc Thesis), University of Twente, 2012, [Online]: https://www.ru.nl/publish/pages/769526/acornelissen.pdf.

[71] J. Liu, S. Zhang, W. Sun, Y. Shi, In-vehicle network attacks and countermeasures: Challenges and future directions, IEEE Netw. 31 (5) (2017) 50–58.

[72] W. Zeng, M.A. Khalid, S. Chowdhury, In-vehicle networks outlook: Achievements and challenges, IEEE Commun. Surv. Tutor. 18 (3) (2016) 1552–1571.

[73] V.L. Thing, J. Wu, Autonomous vehicle security: A taxonomy of attacks and defences, in: 2016 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2016, pp. 164–170.

[74] B. Yu, C.-Z. Xu, B. Xiao, Detecting sybil attacks in vanets, J. Parallel Distrib. Comput. 73 (6) (2013) 746–756.

[75] L. Liu, C. Chen, Q. Pei, S. Maharjan, Y. Zhang, Vehicular edge computing and networking: A survey, 2019, arXiv preprint arXiv:1908.06849.

[76] P. Wang, X. Wu, X. He, Modeling and analyzing cyberattack effects on connected automated vehicular platoons, Transp. Res. C 115 (2020) 102625.

[77] H. Peng, L. Liang, X. Shen, G.Y. Li, Vehicular communications: A network layer perspective, IEEE Trans. Veh. Technol. 68 (2) (2018) 1064–1078.

[78] R. Hussain, S. Zeadally, Autonomous cars: Research results, issues, and future challenges, IEEE Commun. Surv. Tutor. 21 (2) (2018) 1275–1313.

[79] S. Zeadally, J. Guerrero, J. Contreras, A tutorial survey on vehicle-to-vehicle communications, Telecommun. Syst. 73 (3) (2020) 469–489.

[80] A. Chattopadhyay, K.-Y. Lam, Y. Tavva, Autonomous vehicle: Security by design, IEEE Trans. Intell. Transp. Syst. (2020) 1–15, http://dx.doi.org/10.1109/TITS.2020.3000797.

[81] M.Y. Gadkari, N.B. Sambre, VANET: routing protocols, security issues and simulation tools, IOSR J. Comput. Eng. 3 (3) (2012) 28–38.

[82] L. Mokdad, J. Ben-Othman, A.T. Nguyen, DJAVAN: Detecting jamming attacks in vehicle ad hoc networks, Perform. Eval. 87 (2015) 47–59.

[83] P. Bansal, S. Sharma, A. Prakash, A novel approach for detection of distributed denial of service attack in vanet, Int. J. Comput. Appl. 120 (5) (2015) 28–32.

[84] J. Rezgui, S. Cherkaoui, Detecting faulty and malicious vehicles using rule-based communications data mining, in: Proc. of 36th IEEE Conference on Local Computer Networks, 2011, pp. 827–834.

[85] G. Loukas, E. Karapistoli, E. Panaousis, P. Sarigiannidis, A. Bezemskij, T. Vuong, A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles, Ad Hoc Netw. 84 (2019) 124–147.

[86] F. Ahsan, A. Zahir, S. Mohsin, K. Hussain, Survey on survival approaches in wireless network against jamming attack, J. Theor. Appl. Inf. Technol. 30 (1) (2011) 55–67.

[87] H. Alturkostani, A. Chitrakar, R. Rinker, A. Krings, On the design of jamming-aware safety applications in vanets, in: Proc. of 10th Annual Cyber and Information Security Research Conference, 2015, pp. 1–7.

[88] S. Ishihara, R.V. Rabsatt, M. Gerla, Improving reliability of platooning control messages using radio and visible light hybrid communication, in: Proc. of IEEE Vehicular Networking Conference (VNC), 2015, pp. 96–103.

[89] S. Ucar, S.C. Ergen, O. Ozkasap, IEEE 802.11p and visible light hybrid communication based secure autonomous platoon, IEEE Trans. Veh. Technol. 67 (9) (2018) 8667–8681.

[90] G. Patounas, Y. Zhang, S. Gjessing, Evaluating defence schemes against jamming in vehicle platoon networks, in: Proc. of 18th International Conference on Intelligent Transportation Systems, 2015, pp. 2153–2158.

[91] P. Golle, D. Greene, J. Staddon, Detecting and correcting malicious data in VANETs, in: Proc. of 1st ACM International Workshop on Vehicular Ad Hoc Networks, 2004, pp. 29–37.

[92] N. Carson, S.M. Martin, J. Starling, D.M. Bevly, Gps spoofing detection and mitigation using cooperative adaptive cruise control system, in: Proc. of IEEE Intelligent Vehicles Symposium (IV), 2016, pp. 1091–1096.

[93] T. Zhou, R.R. Choudhury, P. Ning, K. Chakrabarty, Privacy-preserving detection of sybil attacks in vehicular ad hoc networks, in: Proc. of 4th Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services (MobiQuitous), 2007, pp. 1–8.

[94] S.S. Manvi, M.S. Kakkasageri, D. Adiga, Message authentication in vehicular ad hoc networks: Ecdsa based approach, in: Proc. of International Conference on Future Computer and Communication, 2009, pp. 16–20.

[95] B. Lee, E. Jeong, I. Jung, A DTSA (detection technique against a sybil attack) protocol using SKC (session key based certificate) on VANET, Int. J. Secur. Appl. 7 (3) (2013) 1–10.

[96] M. Raya, P. Papadimitratos, J.-P. Hubaux, Securing vehicular communications, IEEE Wirel. Commun. 13 (5) (2006) 8–15.

[97] S. Dadras, R.M. Gerdes, R. Sharma, Vehicular platooning in an adversarial environment, in: Proc. of 10th ACM Symposium on Information, Computer and Communications Security, 2015, pp. 167–178.

[98] B. DeBruhl, S. Weerakkody, B. Sinopoli, P. Tague, Is your commute driving you crazy?: A study of misbehavior in vehicular platoons, in: Proc. of 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks, 2015, p. 22.

[99] M. Ghanavati, A. Chakravarthy, P. Menon, Pde-based analysis of automotive cyber-attacks on highways, in: Proc. of American Control Conference (ACC), 2017, pp. 1833–1838.

[100] M. Ghanavati, A. Chakravarthy, P.P. Menon, Analysis of automotive cyber-attacks on highways using partial differential equation models, IEEE Trans. Control Netw. Syst. 5 (4) (2017) 1775–1786.

[101] S. Dadras, S. Dadras, C. Winstead, Reachable set analysis of vehicular platooning in adversarial environment, in: Proc. of Annual American Control Conference (ACC), 2018, pp. 5568–5575.

[102] VEhicular network open simulator, 2019, https://maniam.github.io/VENTOS/, Accessed on November 2, 2019.

[103] M. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, H.M. Zhang, J. Rowe, K. Levitt, Security vulnerabilities of connected vehicle streams and their impact on cooperative driving, IEEE Commun. Mag. 53 (6) (2015) 126–132.

[104] D. Krajzewicz, J. Erdmann, M. Behrisch, L. Bieker, Recent development and applications of SUMO - simulation of urban mobility, Int. J. Adv. Syst. Meas. 5 (3&4) (2012) 128–138.

[105] OMNet++ discrete event simulator, 2019, https://omnetpp.org/, Accessed: 2019-11-06.

[106] C. Sommer, R. German, F. Dressler, Bidirectionally coupled network and road traffic simulation for improved IVC analysis, IEEE Trans. Mob. Comput. 10 (1) (2011) 3–15.

[107] S. Tsugawa, S. Jeschke, S.E. Shladover, A review of truck platooning projects for energy savings, IEEE Trans. Intell. Veh. 1 (1) (2016) 68–77.

[108] Document ETSI TS 103 097 V1.3.1, Intelligent transport systems (ITS); security; security header and certificate formats, 2019, Accessed on October 15, 2019. [Online]: https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.03.01_60/ts_103097v010301p.pdf.

[109] M.B. Brahim, E.B. Hamida, F. Filali, N. Hamdi, Performance impact of security on cooperative awareness in dense urban vehicular networks, in: Proc. of 11th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2015, pp. 268–274.

[110] F. Farokhi, I. Shames, K.H. Johansson, Private and secure coordination of match-making for heavy-duty vehicle platooning, IFAC-PapersOnLine 50 (1) (2017) 7345–7350.

[111] K. Kogiso, T. Fujita, Cyber-security enhancement of networked control systems using homomorphic encryption, in: Proc. of 54th IEEE Conference on Decision and Control (CDC), 2015, pp. 6836–6843.

[112] J. Petit, S.E. Shladover, Potential cyberattacks on automated vehicles, IEEE Trans. Intell. Transp. Syst. 16 (2) (2014) 546–556.

[113] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, Z. Zhang, Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles, IEEE Trans. Intell. Transp. Syst. 19 (7) (2018) 2204–2220.

[114] M. Muhammad, G.A. Safdar, Survey on existing authentication issues for cellular-assisted v2x communication, Veh. Commun. 12 (2018) 50–65.

[115] R. Lu, X. Lin, H. Zhu, P.-H. Ho, X. Shen, ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications, in: Proc. of 27th IEEE Conference on Computer Communications (INFOCOM), 2008, pp. 1229–1237.

[116] Y. Sun, R. Lu, X. Lin, X. Shen, J. Su, An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications, IEEE Trans. Veh. Technol. 59 (7) (2010) 3589–3603.

[117] J.Y. Hwang, L. Chen, H.S. Cho, D. Nyang, Short dynamic group signature scheme supporting controllable linkability, IEEE Trans. Inf. Forensics Secur. 10 (6) (2015) 1109–1124.

[118] A. Wasef, X. Shen, Efficient group signature scheme supporting batch verification for securing vehicular networks, in: Proc. of IEEE International Conference on Communications, 2010, pp. 1–5.

[119] H. Hu, R. Lu, Z. Zhang, TPSQ: Trust-based platoon service query via vehicular communications, Peer-to-Peer Netw. Appl. 10 (1) (2017) 262–277.

[120] H. Hu, R. Lu, Z. Zhang, J. Shao, Replace: A reliable trust-based platoon service recommendation scheme in vanet, IEEE Trans. Veh. Technol. 66 (2) (2016) 1786–1797.

[121] C. Lai, R. Lu, D. Zheng, SPGS: a secure and privacy-preserving group setup framework for platoon-based vehicular cyber-physical systems, Secur. Commun. Netw. 9 (16) (2016) 3854–3867.

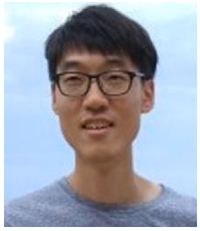
[122] J. Liu, D. Ma, A. Weimerskirch, H. Zhu, Secure and safe automated vehicle platooning, IEEE Reliab. Soc. (2016).

[123] J. Erickson, S. Chen, M. Savich, S. Hu, Z.M. Mao, CommPact: Evaluating the feasibility of autonomous vehicle contracts, in: Proc. of IEEE Vehicular Networking Conference (VNC), 2018, pp. 1–8.

[124] A. Petrillo, A. Pescapé, S. Santini, A collaborative approach for improving the security of vehicular scenarios: The case of platooning, Comput. Commun. 122 (2018) 59–75.

[125] A. Ferdowsi, U. Challita, W. Saad, N.B. Mandayam, Robust deep reinforcement learning for security and safety in autonomous vehicle systems, in: Proc. of 21st International Conference on Intelligent Transportation Systems (ITSC), 2018, pp. 307–312.

Amrita Ghosal obtained her Ph.D. degree in Computer Science and Engineering from Indian Institute of Engineering Science and Technology, India in 2015. She received her Master of Technology degree in computer science and engineering from Kalyani Government Engineering College, India in 2006. She is currently a Postdoctoral Researcher at University of Padua, Italy. Prior to that, she was Assistant Professor in the Department of Computer Science and Engineering, Dr. B. C. Roy Engineering College, India. Her current research interests include security and privacy in wireless resource-constrained mobile device and smart grid, network modeling and analysis. She has published research works in reputed conference proceedings and journals in her field. She also has co-authored a number of book chapters.



Sang Uk Sagong is a researcher at Hyundai Motor Group. He received the B.S. degree and the M.S. degree in Electrical Engineering from Yonsei University — Korea in 2009 and 2011, respectively. He received the Ph.D. degree in Electrical Engineering from the University of Washington — Seattle in 2019. His research interests include standards of the Controller Area Network (CAN) protocol, security of automobiles, and secure control of systems.

Subir Halder received his Master of Technology and Ph.D. degrees in Computer Science and Engineering from Kalyani Government Engineering College and Indian Institute of Engineering Science and Technology, India in 2006 and 2015, respectively. He is currently a Postdoctoral Researcher at University of Padua, Italy. Prior to that, he was Assistant Professor in the Department of Computer Science and Engineering, Dr. B. C. Roy Engineering College, India. He has co-authored more than 30 papers in international peer-reviewed conferences and journals in his field. He has also co-authored 5 book chapters. His research interests include security and privacy in next generation networking including WSN, IoT, network modeling and analysis, and performance evaluation and optimization.

Kalana Sahabandu is a M.S. candidate in the Department of Electrical and Computer Engineering at the University of Washington — Seattle. He received the B.S degree in Computer Science from the Washington State University — Pullman in 2019. His research interests includes autonomous vehicle security and systems security.

Mauro Conti is Full Professor at the University of Padua, Italy, and Affiliate Professor at the University of Washington, Seattle, USA. He obtained his Ph.D. from Sapienza University of Rome, Italy, in 2009. After his Ph.D., he was a Post-Doc Researcher at Vrije Universiteit Amsterdam, The Netherlands In 2011 he joined as Assistant Professor the University of Padua, where he became Associate Professor in 2015, and Full Professor in 2018. He has been Visiting Researcher at GMU (2008, 2016), UCLA (2010), UCI (2012, 2013, 2014, 2017), TU Darmstadt (2013), UF (2015), and FIU (2015, 2016, 2018). He has been awarded with a Marie Curie Fellowship (2012) by the European Commission, and with a Fellowship by the German DAAD (2013). His research is also funded by companies, including Cisco, Intel and Huawei. His main research interest is in the area of security and privacy. In this area, he published more than 250 papers in topmost international peer-reviewed journals and conferences. He is Area Editor-in-Chief for IEEE Communications Surveys Tutorials, and Associate Editor for several journals, including IEEE Communications Surveys Tutorials, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Dependable and Secure Computing, and IEEE Transactions on Network and Service Management. He was Program Chair for TRUST 2015, ICISS 2016, WiSec 2017, and General Chair for SecureComm 2012 and ACM SACMAT 2013. He is Senior Member of the IEEE.

Radha Poovendran received the B.S. degree in electrical engineering from IIT Bombay in 1982, the M.S. degree in electrical and computer engineering from the University of Michigan, Ann Arbor, in 1992, and the Ph.D. degree in electrical and computer engineering from the University of Maryland at College Park, College Park, in 1999. He is currently a Professor and the Chair of the Electrical and Computer Engineering Department, University of Washington (UW). He is also the Director of the Network Security Lab, University of Washington. He is also the Associate Director of Research of the UW Center for Excellence in Information Assurance Research and Education. He holds eight patents in wireless and aviation security. His research interests are in the areas of wireless and sensor network security, control and security of cyber–physical systems, adversarial modeling, smart connected communities, control-security, games-security, and information theoretic security in the context of wireless mobile networks. He is a Fellow of the IEEE for his contributions to security in cyber–physical systems. He was a recipient of the NSA LUCITE Rising Star Award in 1999, National Science Foundation CAREER in 2001, ARO YIP in 2002, ONR YIP in 2004, and PECASE in 2005 for his research contributions to multi-user wireless security. He was also a recipient of the Outstanding Teaching Award and Outstanding Research Advisor Award from UW EE in 2002, the Graduate Mentor Award from Office of the Chancellor at the University of California

at San Diego, San Diego, in 2006, and the University of Maryland ECE Distinguished Alumni Award in 2016. He was co-author of award-winning papers, including the IEEE/IFIP William C. Carter Award Paper in 2010 and the WiOpt Best Paper Award in 2012. He is Fellow of the IEEE.

Linda Bushnell is a Research Professor in the Department of Electrical and Computer Engineering at the University of Washington — Seattle. She received her Ph.D. in Electrical Engineering from University of California — Berkeley in 1994, her M.A. in Mathematics from University of California — Berkeley in 1989, her M.S. in Electrical Engineering from University of Connecticut — Storrs in 1987, and her B.S. in Electrical Engineering from University of Connecticut — Storrs in 1985. She also received her MBA from the University of Washington Foster School of Business in 2010. Her research interests include networked control systems and secure-control. She is a Fellow of the IEEE for contributions to networked control systems. She is a Fellow of IFAC for contributions to the analysis and design of networked control systems. She is a recipient of the US Army Superior Civilian Service Award, NSF ADVANCE Fellowship, and IEEE Control Systems Society Distinguished Member Award. She has been a member of the IEEE since 1985, and a member of the IEEE CSS since 1990. She is currently the Treasurer of the American Automatic Control Council, Member of the Technical Board for the International Federation on Automatic Control, Associate Editor for Automatica, and Associate Editor for the IEEE Transactions on Control of Network Systems.