DISTRIBUTED DENIAL OF SERVICE ATTACK: A SERIOUS CONCERN IN VANET

Naramalli Jayakrishna
School of Computer Science and Engineering
Vellore Institute of Technology Vellore, Tamilnadu, India
jayakrishna.n@vit.ac.in

Narayanan Prasanth
School of Computer Science and Engineering
Vellore Institute of Technology Vellore, Tamilnadu, India
n.prasanth@vit.ac.in

DOI: doi.org/10.34293/shanlax.9789361631474.ch016

Abstract

VANETs (Vehicular Ad hoc Networks) have a lot of potential for improving road safety and passenger comfort in Vehicles. On the other hand, since they communicate over an open medium, they are vulnerable to a number of attacks that compromise the reliability of these features. VANET's are gaining more popularity in short time due to the wide variety of services it offers to the modern day vehicular users. In the last few years, VANETs have been an emerging research topic and therefore they are attracting a lot of interest from academia and industry researchers. This is because of their unique characteristics including high dynamic topology and predictable mobility. On the other hand, VANET communication is vulnerable to a variety of security threats including Distributed Denial of Service (DDoS) attacks. As the Denial of Service attacks are intended in restricting the access of existing resources and services by the legitimate users such that it has a drastic impact on the network's performance. The majority of the current DDoS detection techniques is inaccurate and has a high computational overhead. In this paper, we discuss the key aspects of VANETs architecture, and its different forms of networks. The paper further discusses about the VANET security with respect to different services. It also reviews the various solutions to combat the DoS attack and its challenges and limitations.

Keywords: *VANET; Security Attacks; DDoS; Road Safety*

1. Introduction

VANET is a technology in which moving vehicles act as nodes to create a mobile network. In VANET every involved vehicle node is turned into a wireless router. In this type of network, cars in the range of approximately 300 to 500 meters are allowed to connect and exchange information. Thus a network of wider range is created. As initial cars/vehicles move out of the communication range and gets disconnected with the network, other cars will join the network and thereby creating a mobile Internet. Probably fire and police vehicles will become the foremost systems to integrate this technology and communicate amongst themselves for safety purposes [1].

Mobile communication is consistently developing department. While dealing with vehicles, the implementation of telecommunications is done on motorized production in no time. The

ideology of VANET stands applicable in such communications. We can connect one vehicle with the other through wireless technology and the desired information can be replicated to facilitate simple and secure road transport. Such a methodology will drastically update the transportation in an efficient way by ensuring safety to the users and improving the air quality. As the count of cars increases, need of VANET technology for connection between vehicles and communication of vehicles with infrastructure will also increase. To ensure high end safety and efficiency in transportation, it is important to involve all participants of the traffic within the communication by step-wise development of this mechanism. VANET has been pulling in a great deal of consideration in remote correspondence and vehicle enterprises in the on-going years. It supports the communication between ad hoc devices and infrastructure networks. Design and deployment of VANET based solutions are quite complex and is also hard to assure the quality of service, secure data transmission, fair channel allocation due to high mobile environment [2]. In spite of the fact that the measure of research has been given to the different steering issues in VANET yet at the same time there are a few territories that need more consideration.

VANET is one of the categorical features of mobile Ad Hoc network (MANET) that represents a self-governing system of nodes interlinked with various mobile stations through wireless links. A network is created on purely ad hoc basis by connecting all these nodes without wires. Each node can play the roles of a furtherer, receiver, and a router. As nodes are portable at any time and to any direction hence mobility of nodes is the key benefit in such networks. VANET when compared with MANET the primary variance noticed is the dynamic variable network topology. Nodes as cars can spontaneously take part otherwise withdraw from the network topology. Initially it was a WLAN technology with dynamic connection launch, which allows inaugurating a transitory network connection with nodes. In road transport, each vehicle can act as an information carrier. Based on vehicle speed, it forms a bridge among diverse topologies [3]. The idea of the VANET networks involves networking of all traffic participants and possibly, also exterior participants similar to MANET. The VANET brings them the total environment where these vehicles are operated with the individual challenges and requirements. Presently vehicles records huge amount of data that is generated which is applicable for only local management. The primary goal of VANET communication is sharing the data with the neighbouring vehicle to facilitate them with better road information.

VANET integrates ad hoc network, wireless local area network (WLAN) and cellular technology. It represents a variant of Mobile Ad Hoc Networks

(MANETs) in which vehicles communicate amongst themselves and with the road side units (RSUs). VANETs are distributed and self-organizing in nature and forms the primary constituent of Intelligent Transportation System (ITS) [4]. They make transportation safer by enabling efficient intercommunication between vehicles so that safety and critical messages are instantly disseminated. Some of the unique features of VANETs are high mobility of vehicle nodes, varying density of vehicle nodes and limitless range of the network [5].

VANETs are self-distributed and have the capability to move between vehicles. These are specially designed with wireless features sort of communication devices. ITS management system is used for this purpose which is referred as ITS [7]. It has the ability to cause certain changes in the performances of transportation systems. This system has specific aims and objectives that could improve the level of safety for roads. It also helps to cut down increased level of traffic, fuel consumption and improve waiting time. The process of integration of devices with special navigation systems (GPS) and other related features like digital maps have the potential to serve various applications. They can play a vital role to improve road security systems. One way is to integrate all these systems so as to provide latest information to the drivers that could keep them updated with the latest proceedings on the road. A vehicular network can have certain mobile nodes. These nodes have On Board Units and some other types of nodes that are basically referred as Road Side Units. These devices are composed of various communications networks and can perform required operations in an ad-hoc fashion [9]. Such networks are commonly known as Vehicle-to-RSU and Vehicle-to Vehicle networks [10]. There are different network channels where RSU operates and is shown in Fig. 1. Here are several wireless technologies that have their role to play for VANET environment [11]. Here, a Dedicated Short Range Communications are used to support the process of data transfer in the variety of communication environments that will change with respect to time [13]. VANET communication is vulnerable to a variety of security threats and a most disastrous one is Distributed Denial of Service (DDoS) attacks. This is because it is hard to manage and can leads to a worst possible situation in a no man's time. It is important to address this attack as early as possible for the safe passage of vehicular users. In this paper, we discuss the concept of VANET and the impact of DOS attack. Section 2 discusses about the VANET architecture and its components. Section 3 discusses about the VANET security issues.

2. Components of VANET Architecture

The architecture of VANET is shown in Fig. 1 and its main system components are:

1. **On Board Unit (OBU)**: OBU is a Global Positioning System (GPS)-

based backup that regularly shares RSU and other OBU with vehicle data for all vehicles. The OBU is responsible for setting up communications with RSU or other OBUs via the IEEE 802.11p remote connection and transmission as messages with other OBUs or RSUs. The OBU also uses input power, where each VU has GPS and OBU input and opposite input sensors.

2. **Application Unit (AU)**: The AU is an in-vehicle device that uses the services provided by the provider using OBU communication capabilities. AU can be a dedicated device for security applications or a common device such as a personal digital assistant (PDA) to use the Internet, the AU can be connected to the OBU via a wired or wireless connection and can stay with the OBU locally. One body unit the difference between the AU and the OBU makes sense.
3. **Road Side Unit (RSU)**: RSU is a computer unit, located at a specific location to provide local connections to vehicles passing through road sections. The road unit is a computer machine. RSU is a network device based on IEEE 802.11p Dedicated Short-Range Communication (DSRC) radio technology. In particular, RSUs can also be used to connect to other infrastructure networks and other network devices.

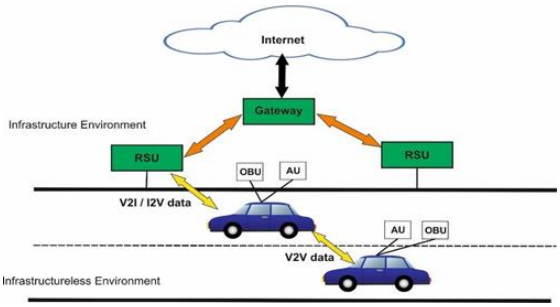

Figure 1. VANET Architecture

2.1 Challenges and Requirements in VANET

There are many issues concerned with the gathering of data regarding vehicular networks of ad hoc features. These are done to provide an enhanced driver behaviour that has the goal of minimizing the fatalities which are resulted by car accidents [14]. So, here are certain challenges about VANET and other technological environmental challenges presented below:

Signal Fading: The challenges those are often associated with signal fading are these objects that create troubles for the communication between vehicles with the capacity to impact the work efficiency for VANETs. Some of these cars and buildings are a crime on the streets of these cities. In addition, coordinator centrally attached in VANET has some Bandwidth limitations [15]. It controls the process of communication among several nodes that could responsibly manage the operation of contention and bandwidth.

Connectivity: One needs to understand the fact that there are some factors like changes in topology along with the mobility can cause

fragmentation in a variety of networks. Therefore, one must ensure that the time that is needed for this purpose of communication should be elongated [16]. One can accomplish this task by maximizing the power of transmission that could result in a degradation process. Thus, for VANET, connectivity surely is a big issue that can play a role for the communication of nodes.

Security and Privacy: Security protects the privacy, integrity and access to information, while privacy is clear about privacy rights regarding personal information. During this process, one also needs to make sure that certain challenges exist in the privacy and security processes. It is necessary to obtain reliable information that can be obtained from other sources.

3. VANET Security Requirements

3.1. Security Services

Security services are very much important for applications in ad hoc networks which are sensitive in nature. To create an ad hoc network, one must focus on ensuring security attributes such as reliability, confidentiality, authenticity, and confirmation.

Availability

Network services include bandwidth and network access due to all the complexity of dealing with product surplus, block chain and identification using group signatures [This method is intended to solve both product overload and creation]. These approaches seek to find ways to bring RSU access to automotive communications. If the attack disrupts the RST, the connection, the proposed strategy will still exist due to the network connection of the vehicle to the vehicle**.**

Authentication

Authentication ensures that vehicles are connected and validates the information sharing process as it provides additional benefits; also ensures that all vehicles are able to connect to the entire network. Whereas it is proposed to allow vehicles, RSUs, and keys to be integrated to create a public or private links. On the other hand, users have to enter their password in order to gain access to RSU again as authentication.

Integrity

Data integrity promises the message's data which is shared among nodes, Butt, and sources. Integrated protection requires both a password and a digital signature has been employed.

Confidentiality

Unidentified individuals inside the network should never reveal confidential information additionally; it ensures that only approved users have access to information such as plate number, name, and location information. To protect the privacy of vehicle networks, each vehicle will have several master keys, each of which will be encrypted. For signing, messages use different 'pseudo' encryption and "Pseudo" does not have access to the car, however relevant can. Vehicle needs to buy pseudo that has reached the earlier expiry date before they have to apply for new licenses.

Non-Repudiation

Non-Repudiation is important security primitive which should be considered to ensure that any parties involved in the VANET connection (V2I and V2V) cannot deny the connection / acquisition that took place.

3.2. Attacks in VANET

Obstacles that because many malicious activities on VANET are listed as multi-layer attacks such as jumping, flooding, etc., can cause serious problems, such attacks on network layers cause many problems.

The attacks were categorized as shown in table 1 based on threat to VANET security requirement.

Table 1. VANET Security services

Authenticity	Sybil and Replay attacks, GPS Spoofing, Position faking
Integrity	Replay, Message Suppression/Fabrication/Alteration, Masquerade.
Confidentiality	Eavesdropping. Information gathering, Traffic analysis.
Availability	DoS, Jamming, Black Hole attack, broadcast tampering.
Non-Repudiation	Loss of event traceability

DoS affect the availability service in a VANET and hence it requires protection at the network layer. It is considered as the primary threat to the lifespan, rate and time of users in VANET. DoS attacks are mainly aimed at exhausting both node and communication resources such as computing power, memory and bandwidth, which leads to an overload. Subsequent DoS attacks are highlighted according to [12] and [22].

1. Flooding Attack
2. Jamming Attack
3. Broadcast Tampering/Spamming
4. Malware Attack
5. Black Hole Attack
6. Sybil attack

To establish VANET as a secure, effective and most efficient road traffic management system, vehicular networks must be designed in such a way that it is safeguarded from these attacks. DoS are done on the network to slow down its work by introducing useless traffic. It makes the network temporarily unavailable or interrupts the services of a host connected to the Internet. In a DoS attack, the failed node transmits a large number of unnecessary messages and requests the network to validate these requests with incorrect return addresses.

In a DDoS attack, the malicious party uses many vehicles to generate large amounts of network traffic in order to damage the integrity of the network. The vehicles used in a DDoS attack do not know that they are being used by the malicious user. Because of this, the

computers used in DDoS attacks are often referred to as zombies. Blocking the vehicle's communication systems could result in a vehicle accident and, in the worst case, loss of life. This attack can be difficult to detect due to the use of zombie vehicles. An extensive review has been done on DoS, and each technique is thoroughly discussed in the next section.

4. DOS/DDOS attacks in VANET

Currently, the detection of the DoS-JSA (jamming signal attack) signal for the VANET, which has so far only been identified in these tests, is in accordance with IEEE 802.11, the incorrect behaviour of certain vehicles and nodes in the MAC layer violates the IEEE 802.11 rules. In order to access the channel more frequently than other nodes, small polling counters were chosen. However, their success was hampered by that. In these investigations, identification of all types of attacks, including HDSA (Hybrid DoS Attacks), was a challenge. Furthermore, the examination was focused solely on a DoS JSA assault. In detecting DoS JSA only in VANET, a prior revision [15] proposed a system that used a unicast traffic method based on the regression model. However, the suggested approach did not take into account the node's trustworthiness inquiry. Another study [16] also proposed instantaneous identification of DoS attacks in the IEEE 802.11p vehicular network system. This took into account beacons transmitted on a daily basis in IEEE 802.11p broadcast mode itself, with no re-transmission. This approach also included a backup jamming detector for solitary detection of DoS JSA attacks in a VANET subdivision. The inquiry, however, uncovered shortcomings in the protocol's trustworthiness. Upon the examination of these approaches, we may confirm that the DoS attacks investigated in VANET were solely grounded on DoS JSA. Additional attacks, such as HDSA, are common in VANET. The identification of all other attacks and HDSA remains the most difficult problem in the implementation of VANET protection applications.

There are other types of denial of service attack, such as PD (packet drop), RCO (Resources consumption), and some form of them even include perpetrator DoS attacks like DoS resilience attacker (DRA). Together, these attacks have contributed to RSU overutilization, however all the above plans neglected the fact that HDSA will be part of the investigation as well. Additionally, the researchers' investigations on these schemes have proven only [17] restricted recommendations and hardware/ software-based security techniques. The authors reported DoS attacks based on their proposed network monitoring schemes. Because of the goals of this project, we are including DDoS (Distributed Denial of Service) attacks. As a consequence, it is important to have a thoughtful study design process [18]. This new strategy would be able to detect all types of Distributed Denial of Service

(DDoS) attacks, including High DDoS (real-time) Attacks.

Vehicular computing includes both vehicular cloud and fog computing (VFC). In addition, VFC provides reliable and resource-efficient computing, and out-of-network availability. Additionally, optimization algorithms such as ABC (basic Cuckoo image optimization) and Firefly (extended Cuckoo image optimization) and the firefly neural algorithm (FNO) are able to contribute to swarm intelligence. To the extent that they depend on algorithm or process, the OAs (Optimization algorithms) may or may not have problem cracking skills. Lastly, they pose the option to change their DoS JSA and HDSAs (which include everything else, such as DoS JSA, PDRCO, and abuse), which allows for a better overall experience OAs for short-range communications has been used in real-time data collection, which utilizes IEEE 802.11p for dedicated communications [19]. Deploying digital rights management rights management in a safe and stable manner Integration with OAs and verification of VANET trust, which also includes KDE, will enable us to appropriately secure the VANET. This security approach for IEEE 802.11p adds the DSR (Dedicated short range) compatibility. This contributes to the protection of road and highway design on the basis that the use of intelligent transportation systems is anticipated. To reliably detect real-time DDoS JSA and HDSA attacks, which is based on IEEE 802.11p, it is important to perform end-to-end delay & jitter evaluation within VANET.

This type of surveillance research was conducted to explore DDoS attacks, but also used vehicle electronics telematics. However, following the Cuckoo/CSA (ABC) inquiry, it was found that it had no bearings on VFC [20]. There is thus no emphasis on bimodily (as opposed to bierly, which is just the combination of unicast and multicast) schemes for schemes in schemes' investigations. Nonetheless, this methodology did not earn it confidence in the group. The authors have performed an enquiry on Firefly (VANET: a long-E will be a key enabler of future ITS), and leverage the firefly principle of future ITS by using a combination of real-time protection from DoS. The authors caused the unruly nodes to imprint upon the vehicles that were delayed in VANET. In addition, they have used the DSRC and Multicast technology however, his research was somewhat constrained due to the absence of real data[21] There are several types of attacks included in the network analysis, like DoS JSA and RCO, but these are not included in the investigation since the focus is on DDoS attacks only. The other main disadvantage of the VFC approach was that it was noticed in all of the schemes. Thus, it can be inferred that VANET is an unreliable. It's always the biggest obstacle.

To counteract these issues, we describe all types of DoS, as well as DoS attacks in VANET, which includes DoS

JSA, and HDSA, in this paper. In addition, we recommend that VFCs be placed in OA configurations where possible and we also use the complete KDE (key distribution establishment) authentication/integrity mechanism in the VANET. These will be used to examine the end-to-to-end IEEE 802.11p data transmission delay and jitter in real-time in this paper, we clarify how we expect to use VFC to locate DDoS attacks in the IEEE 802.11p environment.11p spectrum in real time.

Table-2 provides an outline of all DoS handling mechanisms with their methodology, attainment and all their pros and cons along with the concerned metrics.

Table 2 A summary of several DoS remedies in VANET

Technique	Methodology
Prediction Based Authentication[1][25]	Predict future Merkle tree building beacon, sign the message
Fast Authentication[9][26][27]	Creates the hash tree Merkle and predicts the authentication of beacon messages.
VANET Authentication using Signature [10][28][29]	TESLA++ authenticates messages and uses ECDSA signatures to provide non-repudiation.
Timed Efficient Stream Loss-tolerant Authentication [10][30]	Similar to TESLA but only re-MACs are saved to reduce the memory constraint
TESLA broadcast authentication protocol[11][32][33]	Uses symmetric key encryption with delayed key release.
Elliptic Curve Digital signature algorithm[17][34][35]	Using asymmetric key encryption, a message has public keys and private key
Ant Colony Optimization [24][36][37]	Applies trust and pheromone value to drive down malicious vehicles.
Technology/ Frequency- Hop/ Channel Switching [12][38]	When an attack is detected, it transfers to other free technology, frequency or channel to send message to destinations safely.
Pre- Authentication Technique[20][39][40]	They create a hash-chain by using the original identity as a seed.

Attainment	Advantages	Disadvantages
Quick beacon messages authentication	Resist computer and memory based DoS, as well as packet loss-resistant in the loss environment.	In the loss setting, signature processing leading to overhead computation is essential.
Prevents floodingsignature	Fast authentication with short signatures.	Difficult to authenticate when a packet is misplaced.
Authentication of the message and non- repudiation with multi-hopcontact	Resist overhead computing and connectivity.	In a low-density area only signatures leading to calculation are used.
Text authorship and less overhead memory	No computer and memory overhead	Does not accept repudiation, multi-hopand packet loss.
Authentication of message with simpleMACs	Removes signature that does not contribute to overhead computation	Save Macs includes memory that leads tomemory-based DoS.
Provides goodmessage authentication.	Supports authenticationand non-rejection of messages.	Computer-based DoSfails when flooding happens.
Chooses the safest route without malicious cars.	Optimized route selection for reliable message delivery.	Trust and pheromone updates are overhead.
Secure Messagedelivery.	No classified information isneeded and there are no additional criteria to use current features.	The OBU processor isoverhead. Uses Hash Chain tosearch users beforehand.
The hash value is appended to any message to verify user	To authenticate the message, verification time is reduced	Simple and quick check Not able to withstand externalattacks.

5. Challenges and Future Perspectives

Given the difficulties and characteristics of VANETs, the following should be considered in some potential perspectives for the creation of new efficient communication approaches:

Network Management

The network topology and channel state change rapidly because of high mobility. This makes it impossible to use tree-like structures since these structures cannot be set up and maintained as fast as the topology changes.

Collision control

The unbounded scale of the network is often difficult. Traffic is poor in rural areas and also in urban areas at night. As a result, network partitions occur sometimes when the traffic load is very high in rush-hours and the network is therefore congested and a network collision occurs.

Environmental Impact

Electromagnetic waves are used by VANETs for communication. These waves are environmentally influenced. The environmental effects must also be taken into account to deploy the VANET.

MAC Design

VANET usually uses the shared media to communicate, so the main problem is the MAC design. Many methods such as TDMA, SDMA, and CSMA have been adopted, etc. IEEE 802.11 implemented VANET's CSMA-based Mac.

Protection

Because VANET offers life-critical road safety applications, security of these messages must therefore be fulfilled.

Real time Conditions

VANET is time-critical for delivering a safety message with 100ms transmission delay. A fast cryptographic algorithm should be used to achieve real-time constraints. Authentication of message and person must be completed in time.

Responsibility for Data Consistency

In the VANET authentication node, malicious activities may trigger accidents or interrupt the network. A mechanism should therefore be established to prevent this incoherence. Correlation between the received data on specific information from different nodes can prevent this type of incompatibility.

Low error tolerance

Some protocols are based on chance. VANET uses crucial knowledge about the action in a very short period of time. A minor mistake in the probabilistic algorithm may be damaging [22].

Key Distribution

All the key-dependent protection mechanisms implemented in VANET. Each message is encrypted and must be decrypted with either the same key or different key at the end of the recipient. Different manufacturers can also mount keys in many ways and I have big public infrastructure trust in CA.

6. Conclusion

Vehicle ad Hoc networks are now common as they are built to provide road safety and passenger comfort services. Given its importance and its open communication environment, vehicles are vulnerable to a variety of attacks especially during the network routing. Therefore, securing VANETs and its communication is a great challenge. This paper surveys all the aspects of VANET, including design, standardisation and features, and shows all the VANET safety leaks and their effects. The attacks were classified according to the layers and specifications of the protocol. Finally, we draw up the most suitable authentication schemes and traffic regulatory schemes to ensure better performance against any form of Denial of Service attacks.

References

1. Setia, H. et al. (2024). Securing the road ahead: machine learning-driven DDoS attack detection in VANET cloud environments. Cyber Security Appl. 1(2), 100037.
2. Malnar, M., & Jevtić, N. (2020). A Framework for Performance Evaluation of VANETs Using NS-3 Simulator. Promet-Traffic & Transportation, 32(2), 255-268.
3. Quyoom, A., Mir, A. A., & Sarwar, A. (2020). Security Attacks and Challenges of VANETs : A literature survey. *Journal of Multimedia Information System*, *7*(1), 45–54. https://doi.org/10.33851/jmis.2020.7.1.45
4. Kumar, S., & Mann, K. S. (2019). Prevention of DoS Attacks by Detection of Multiple Malicious Nodes in VANETs. *2019 International Conference on Automation, Computational and Technology Management (ICACTM)*, 89–94. https://doi.org/10.1109/icactm.2019.8776846
5. Sumra, I. A., Hasbullah, H. B., & AbManan, J. L. B. (2015). Attacks on security goals (confidentiality, integrity, availability) in VANET: a survey. In Vehicular Ad-Hoc Networks for Smart Cities (pp. 51-61). Springer, Singapore.
6. Sonker, A., & Gupta, R. K. (2021). A new procedure for misbehavior detection in vehicular ad-hoc networks using machine learning. *International Journal of Power Electronics and Drive Systems/ International Journal of Electrical and Computer Engineering*, *11*(3), 2535. https://doi.org/10.11591/ijece.v11i3.pp2535-2547
7. Lyu, C., Gu, D., Zhang, X., Sun, S., & Tang, Y. (2013, April). Efficient, fast and scalable authentication for vanets. In 2013 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1768-1773). IEEE.
8. Farman, H., Jan, B., Talha, M., Zar, A., Javed, H., Khan, M., Din, A. U., & Han, K. (2018). Multicriteria-Based location privacy preservation in vehicular ad hoc networks. *Complexity*, *2018*(1). https://doi.org/10.1155/2018/7697324
9. Sheikh, M. S., & Liang, J. (2019). A Comprehensive survey on VANET Security Services in traffic Management system. *Wireless Communications and Mobile Computing*, *2019*, 1–23. https://doi.org/10.1155/2019/2423915
10. Eledlebi, K., Yeun, C. Y., Damiani, E., & Al-Hammadi, Y. (2022). Empirical studies of TESLA Protocol: Properties, Implementations, and replacement of public cryptography using biometric authentication. IEEE Access, 10, 21941–21954. https://doi.org/10.1109/access.2022.3152895
11. Mahmood, J., Duan, Z., Yang, Y., Wang, Q., Nebhen, J., & Bhutta, M. N. M. (2021). Security in vehicular ad hoc networks: challenges and

countermeasures. *Security and Communication Networks*, *2021*, 1–20. https://doi.org/10.1155/2021/9997771

12. Bae, J., Park, M., Yang, E., & Seo, D. (2020). Implementation and performance evaluation for DSRC-Based Vehicular Communication System. *IEEE Access*, *9*, 6878–6887. https://doi.org/10.1109/access.2020.3044358
13. Islam, M. N. U., Fahmin, A., Hossain, M. S., & Atiquzzaman, M. (2020). Denial-of-Service attacks on wireless sensor network and defense techniques. *Wireless Personal Communications*, *116*(3), 1993–2021. https://doi.org/10.1007/s11277-020-07776-3
14. Zeadally, S., Hunt, R., Chen, Y. S., Irwin, A., & Hassan, A. (2012). Vehicular ad hoc networks (VANETS): status, results, and challenges. Telecommunication Systems, 50(4), 217-241.
15. Al-Kahtani, M. S. (2012, December). Survey on security attacks in vehicular ad hoc networks (VANETs). In 2012 6th international conference on signal processing and communication systems (pp. 1-9). IEEE.
16. Imghoure, A., El-Yahyaoui, A., & Omary, F. (2022). ECDSA-based certificateless conditional privacy-preserving authentication scheme in Vehicular Ad Hoc Network. *Vehicular Communications*, *37*, 100504. https://doi.org/10.1016/j.vehcom.2022.100504
17. Ai, Y., deFigueiredo, F. a. P., Kong, L., Cheffena, M., Chatzinotas, S., & Ottersten, B. (2021). Secure vehicular communications through reconfigurable intelligent surfaces. *IEEE Transactions on Vehicular Technology*, *70*(7), 7272–7276. https://doi.org/10.1109/tvt.2021.3088441
18. Trullols, O., Fiore, M., Casetti, C., Chiasserini, C. F., & Ordinas, J. B. (2010). Planning roadside infrastructure for information dissemination in intelligent transportation systems. Computer Communications, 33(4), 432-442.
19. He, L., & Zhu, W. T. (2012, May). Mitigating DoS attacks against signature-based authentication in VANETs. In 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE) (Vol. 3, pp. 261-265). IEEE.
20. De Fuentes, J. M., González-Tablas, A. I., & Ribagorda, A. (2011). Overview of security issues in vehicular ad-hoc networks. In Handbook of research on mobility and computing: Evolving technologies and ubiquitous impacts (pp. 894-911). IGI global.
21. Gillani, S., Shahzad, F., Qayyum, A., & Mehmood, R. (2013, May). A survey on security in vehicular ad hoc networks. In International Workshop on Communication Technologies for Vehicles (pp. 59-74). Springer, Berlin, Heidelberg.

22. Vegni, A. M., Biagi, M., & Cusani, R. (2013). Smart vehicles, technologies and main applications in vehicular ad hoc networks. Vehicular technologies-deployment and applications, 3-20.
23. Patel, K. N., & Jhaveri, R. H. (2015). Isolating packet dropping misbehavior in VANET using Ant Colony Optimization. International Journal of Computer Applications, 120(24).
24. Luo, G., Shi, M., Zhao, C., & Shi, Z. (2020). Hash-Chain-Based Cross-Regional Safety Authentication for Space-Air-GroundIntegrated VANETs. Applied Sciences, 10(12), 4206.
25. Zhou, Z., Zhang, H., & Sun, Z. (2017). An improved privacy-aware handoff authentication protocol for VANETs. Wireless personal communications, 97(3), 3601-3618.
26. Rehman, M. U., Ahmed, S., Khan, S. U., Begum, S., & Ishtiaq, A. (2018, March). ARV2V: Attack resistant vehicle to vehicle algorithm, performance in term of end-to-end delay and trust computation error in VANETs. In 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) (pp. 1-6). IEEE.
27. Bagga, P., Das, A. K., Wazid, M., Rodrigues, J. J., & Park, Y. (2020). Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges. IEEE Access, 8, 54314-54344.
28. Chauhan, R. K., & Dahiya, A. (2012). AODV extension using ant colony optimization for scalable routing in VANETs. Journal of Emerging Trends in Computing and Information Sciences, 3(2), 241-244.
29. Patel, K. N., & Jhaveri, R. H. (2015). Isolating packet dropping misbehavior in VANET using Ant Colony Optimization. International Journal of Computer Applications, 120(24).
30. Wahab, O. A., Otrok, H., & Mourad, A. (2013). VANET QoS-OLSR: QoS-based clustering protocol for vehicular ad hoc networks. Computer Communications, 36(13), 1422-1435.
31. Thilak, K. D., & Amuthan, A. (2016, February). DoS attack on VANET routing and possible defending solutions-A survey. In 2016 International Conference on Information Communication and Embedded Systems (ICICES) (pp. 1-7). IEEE.
32. Mishra, B., Panigrahy, S. K., Tripathy, T. C., Jena, D., & Jena, S. K. (2011, December). A secure and efficient message authentication protocol for VANETs with privacy preservation. In 2011 World Congress on Information and Communication Technologies (pp. 880-885). IEEE.
33. Sheikh, M. S., & Liang, J. (2019b). A Comprehensive survey on VANET Security Services in traffic Management system. *Wireless Communications and Mobile Computing*,

2019, 1–23. https://doi.org/10.1155/2019/2423915

34. Manvi, S. S., & Tangade, S. (2017). A survey on authentication schemes in VANETs for secured communication. Vehicular Communications, 9, 19-30.
35. Vaibhav, A., Shukla, D., Das, S., Sahana, S., & Johri, P. (2017). Security Challenges, Authentication, application and trust Models for Vehicular Ad hoc Network- a survey. *International Journal of Wireless and Microwave Technologies*, *7*(3), 36–48. https://doi.org/10.5815/ijwmt.2017.03.04
36. Zhou, X., Luo, M., Vijayakumar, P., Peng, C., & He, D. (2022). Efficient certificateless conditional Privacy-Preserving authentication for VANETs. *IEEE Transactions on Vehicular Technology*, *71*(7), 7863–7875. https://doi.org/10.1109/tvt.2022.3169948
37. Xie, Y., Wu, L., Shen, J., & Alelaiwi, A. (2017). EIAS-CP: new efficient identity-based authentication scheme with conditional privacy-preserving for VANETs. Telecommunication Systems, 65(2), 229-240.
38. Shao, J., Lin, X., Lu, R., & Zuo, C. (2015). A threshold anonymous authentication protocol for VANETs. IEEE Transactions on vehicular technology, 65(3), 1711-1720.
39. Chen, C. M., Xiang, B., Liu, Y., & Wang, K. H. (2019). A secure authentication protocol for internet of vehicles. Ieee Access, 7, 12047-12057.