Babylonian Journal of Networking
Vol.2023, **pp**. 105–111
DOI: https://doi.org/10.58496/BJN/2023/014; ISSN: 3006-5372
https://mesopotamian.press/journals/index.php/BJN

Review Article

# Securing Vehicle-to-Vehicle Communications: VANet Challenges

Mahdi Salah Mahdi AL-inizi [1,*], Omar Mohammed NSAIF [2]

[1] *Cybersecurity Science Department, Alfarabi university college, Baghdad, Iraq.*

[2] *Computer Engineering dept, Altinbas üniversitesi, İstanbul, Türkiye.*

**ARTICLE INFO**

Article History

Received 08 Sep 2023
Accepted 07 Nov 2023
Published 28 Nov 2023

Keywords

VANET

V2V

V2I

OBU

RSU

**ABSTRACT**

VANET is a new technology that has both exciting potential and significant obstacles, particularly in the area of security. Three sections make up this paper, all of which are devoted to VANET security frameworks. First, there's a comprehensive review of VANET security features, problems, and prerequisites. Enabling the creation of a secure VANET infrastructure with effective communication between parties requires careful consideration of these needs. Here, you will find information about popular security standards protocols and up-to-date security architectures. In the second, we give special attention to a new way of categorizing the various VANET assaults and the answers to them. In the third, we'll look at some of these solutions side by side using standard VANET security criteria. Afterwards, we highlight some unresolved concerns and technical hurdles concerning VANET security, which can assist researchers in their pursuit of future solutions.

## 1. INTRODUCTION

VANET's primary goal is to lessen the frequency and severity of automobile accidents by facilitating more efficient traffic movement. The second problem can be fixed by giving the driver or the car the right information. There is still a risk that system failure could compromise road safety if this real-time information is tampered with. Securing this information is crucial for its smooth functioning, which is why security experts are focusing on it.

VANETs are a subset of mobile ad hoc networks that use roadways that have already been planned. Its registration and administration are dependent on two distinct entities: on-board units (OBUs) and roadside units (RSUs). While vehicles navigate on VANET, RSUs are installed on the road borders to provide certain services, while OBUs are in the vehicles themselves. The road network is fully operational, and all cars are freely communicating with one another, RSUs, and designated authorities. The communication mode can be V2V (Vehicle-to-Vehicle), V2I (Vehicle-to-Infrastructure), or hybrid, and it can use DSRC (Dedicated Short Range Communication) in either a single or multi-hop configuration. Figure (1) shows that in the near future, the majority of VANET vehicles will have sensors like radar and ladders in addition to onboard wireless devices like GPS and event data recorders. The purpose of this apparatus is to detect traffic jams and their current state. After that, the car will respond autonomously and communicate this data via vehicle-to-vehicle or vehicle-to-infrastructure protocols in the vehicle network. Active road safety, infotainment, and traffic efficiency and management are some of the many useful apps for VANET users. The last category includes tools for cooperative navigation and speed management [1].

Being safe means you are not worried about any potential harm coming your way. Safety and the steps done to ensure one's safety are what we mean when we talk about security. For the parade, for instance, local authorities frequently employ additional security personnel to ensure the safety of the event. Since VANET is a wireless communication, which is inherently insecure, it is essential to prevent misuse and clearly specify the security architecture. Human safety is impacted by security and the assurance of its level of implementation. Security attacks were the focus of much study and investigation a few years ago, with the goal of identifying and mitigating such threats. Some others sought to establish formal standards

*Corresponding author. Email: mehdi.salah@alfarabiuc.edu.iq

and protocols, while others sought to define security infrastructures. However, there is still a lot of room to explore in the direction of node trustworthiness and misbehavior detection [2].

This article provides an overview of VANET security features and conducts an in-depth analysis of the majority of VANET security issues and their current remedies. Presenting and discussing recent frameworks that handle the relevant concerns follows a detailed description of recent security designs and well-known security standards protocols. In this paper, we present a new taxonomy for categorizing the various VANET security threats and their solutions.

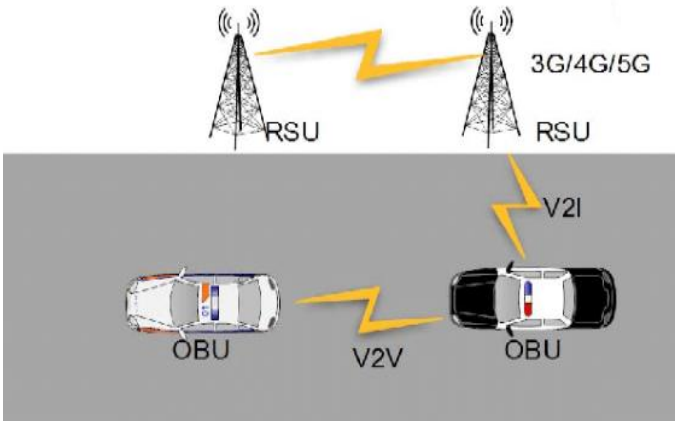


Fig .1. Future vehicle design in VANET

## 2. LITERATURE REVIEW

In this paragraph, the range of research that has been used vanet security below:

When developing a routing protocol for VANETs, it is important to keep in mind the findings of a 2014 survey by Sharef et al. [3] regarding the features and difficulties of VANET routing. In 2014, Engoulou et al. [4] surveyed VANET security concerns and challenges, reviewed VANET security requirements and applications, however they did not address many areas of VANET security. Azees et al. [6] highlighted the privacy and security concerns of VANETs in 2016, while Qu et al. [5] conducted a survey in 2015 that detailed the recent development of numerous experimental tools and simulations. By presenting the most current security architecture with VANET routing protocols, Hasrouny et al. [7] covered the history, current state, and potential future problems with VANET security; however, their thorough review only covers 2017. In their 2018 survey, Lu et al. [8] covered all the bases when it came to VANET architecture, security, privacy, and trust management. Additionally, they touched on integrated simulators and network simulators, however VANET security and privacy were not as extensively covered. When it comes to tackling security risks in vehicle networks, such as VANETs and VANET cloud, Sharma and Kaul [9] provided a comprehensive overview of intrusion detection systems (IDS) and security mechanisms. Using the IDS in VANETs is not without its difficulties, which were covered in this survey. In order to better understand how VANETs handle pseudonym changes, Boualouache et al. [10] conducted a poll. This survey uncovered unanswered questions and compared and contrasted various techniques according to pertinent criteria. By describing performance metrics, classifying and addressing their modeling, needs, and assaults, Ali et al. [11] offered a survey on the authentication and privacy techniques for VANETs. In addition, they went over certain unanswered questions regarding VANET security services.

## 3. VANET ARCHITECTURE

Typically, a wireless protocol known as wireless access in vehicular environment (WAVE) is used for the connection between RSUs and automobiles. The exchange of security messages is described by the WAVE architecture [12], In order to further guarantee the safety of passengers, the WAVE link also updates data about vehicles and traffic patterns. Pedestrian and driver safety are both improved by the program, which also makes the traffic management system more efficient. Many different types of units make up VANETs. These include TAs, RSUs, and OBUs. In example, most RSUs have an app that can communicate with other devices on the network, and every automobile has an OBU installed to record information about the vehicle, such as its speed, acceleration, and fuel consumption. The next step is for the nearby vehicles to receive this information through the wireless network. Each RSU that is talking to another RSU is linked to TA through a wired network. Maintaining the integrity of the VANETs is also TA's responsibility [13].

### *A. Roadside Unit (RSU)*

In order to offer passing vehicles with local connectivity, a computing device called a "roadside unit" is placed alongside the road or in a designated area, like a parking lot or an intersection [14]. Part of the RSU are network nodes that use IEEE

802.11p radio technology for dedicated short-range communication (DSRC). Regarding the various infrastructure networks, RSUs can also communicate with other network devices [14].

*B. Onboard Unit (OBU)*

Typically, every vehicle is equipped with an OBU, which is a tracking device that uses GPS and can interact with both other OBUs and RSUs. A resource command processor (RCP), sensor devices, a user interface, and read/write storage for data retrieval are the various electronic components that comprise an OBU. One of the main functions of an OBU is to connect to other OBUs or a remote service unit (RSU) using an IEEE 802.11p wireless link [15] and exchange messages with them. Furthermore, the OBU is powered by the car's battery, and the vehicle itself has sensors such a global positioning system (GPS), an event data recorder (EDR), with both forward and backward sensors [13].

## 4. VANET SECURITY CHALLENGES

Security in VANET must prevent tampering with or addition to the transmitted messages. Additionally, drivers' culpability is critical for accurately informing the traffic environment within the allotted time. Due to its unique properties, VANET presents unique security challenges. Neglecting these security concerns will result in several limitations. Several of these security threats are detailed below:

Considerations such as network size, geographical relevance, mobility, topology, connection duration, and frequency of disconnections There is no need for a centralized body to regulate the criteria for network size, which means it can be extremely scalable and geographically unlimited.

High mobility causes quick changes in channel conditions and network topology, which in turn necessitates careful network management. As demonstrated in Figure (2), this precludes the usage of structures such as trees, as their setup and maintenance cannot keep up with the rate of topological changes.

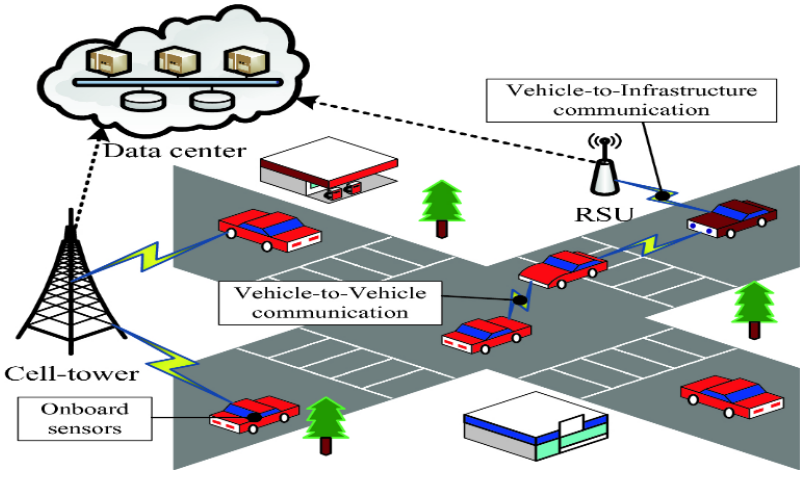


Fig .2. Network Management

Another difficulty that arises from an infinite network size is the control of congestion and collisions. Even in densely populated cities, traffic is light at night and in more rural locations. As illustrated in Figure (3), this causes the network to partition often during peak hours when traffic is heavy, leading to congestion and potential collisions.

Fig .3. Congestion and collision Control.

• Effect on the Environment: VANETs communicate by electromagnetic waves. The environment has an effect on these waves. Therefore, it is necessary to take into account the environmental impact when deploying the VANET, as illustrated in Figure (4).

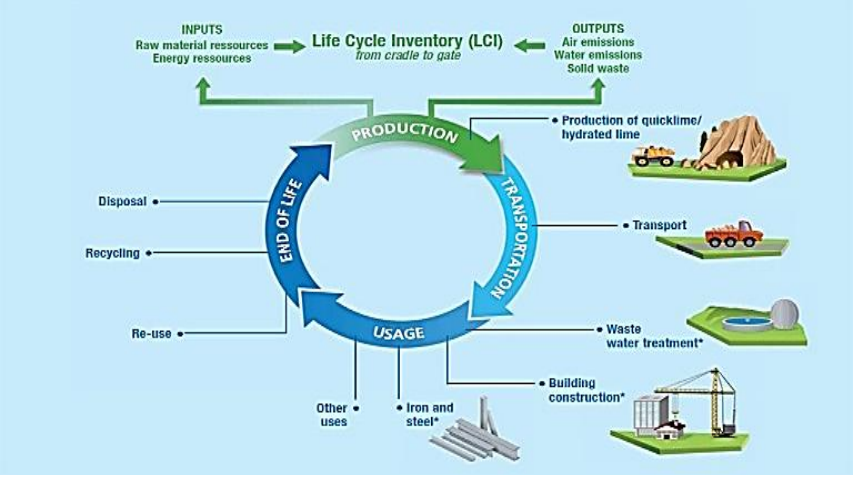


Fig .4. Environmental Impact

• Because VANETs often communicate across a shared media, MAC design is an important consideration. Several methods have been proposed, such as TDMA, SDMA, CSMA, and many more. The CSMA-based Mac for VANET was adopted by IEEE 802.11.

Nodes that receive data must have faith in the sender to provide confidentiality, privacy, and liability. The anonymity of vehicle identifiers guarantees privacy. Even nodes that have been verified as legitimate might occasionally cause problems. Therefore, a compromise between privacy, anonymity, and liability is required.

The ad hoc nature of VANETs encourages nodes to collect information from other vehicles and RSUs, which necessitates trust in order to verify information. Because of the frequency with which this information is sent, its reliability and authenticity must be ensured. It is more important that the data be trustworthy than that the nodes transmitting it be trustworthy.

Key Distribution: Keys are the foundation of all VANET security measures. Decryption of each communication requires the use of either the same key or a different key on the receiver's end. Furthermore, key installation methods can vary across manufacturers, which poses a significant trust issue for public key infrastructure relying on CAs. As can be seen in Figure (5), one of the biggest obstacles to creating security procedures is the distribution of keys across cars.

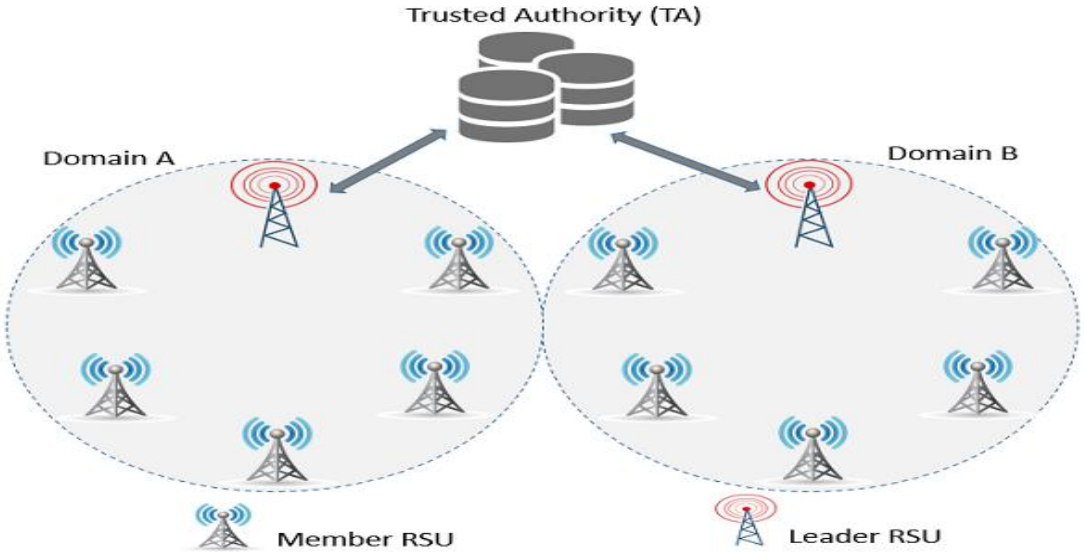


Fig .5. Key Distribution.

Figure (6) shows the various forwarding methods, including unicast, broadcast, V2V, V2I, and hybrid communication, and how difficult it is to determine the optimal amount of transferred packets after determining the best route.

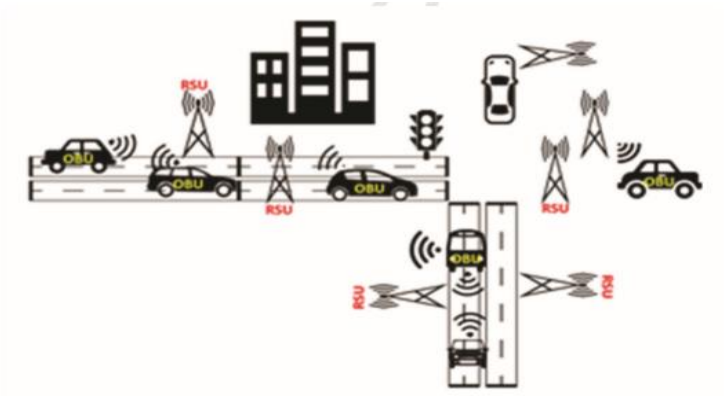


Fig .6. The Forwarding algorithms.

Time is of the essence in VANET, as messages pertaining to safety must be transmitted with a transmission delay of no more than 100 milliseconds. Therefore, a fast cryptographic algorithm is required to meet the real-time limitation. It is critical to authenticate messages and entities promptly.

• Liability for Data Consistency: In VANET, even authenticated nodes are capable of hostile actions that disrupt the network or cause accidents. Therefore, it is necessary to devise a system to prevent this discrepancy. One way to prevent this kind of discrepancy is to ensure that the data collected from each node is adequately correlated with one another.

Some protocols are built around probability, which means there is a low tolerance for error. Actions involving life-critical information are carried out in a flash using VANET. A harm-inducing mistake in a probabilistic algorithm could be rather minor.

To begin with, there are financial incentives for manufacturers to create apps that customers love. The idea of a car that can detect and report violations of traffic laws would be unpopular with most buyers. Implementing security in VANET is a problem, but it is essential for the effective deployment of vehicular networks. Incentives for vehicle makers, consumers, and the government are necessary.

• Great Mobility: Virtual Area Network (VANET) nodes have the same processing power and energy supply as their wired network counterparts, but due to their greater mobility, security protocols executed by VANET nodes take less time to complete the same amount of work as those in wired networks. Security protocol design must so incorporate techniques to decrease execution time. There are two possible ways to fulfill this need.

• Simple security algorithms: Most modern security protocols use public key cryptography based on RSA, including SSL/TLS, DTLS, and WTLS. The NP-Hard integer factorization problem is used by the RSA technique on large prime numbers. Consequently, the RSA method makes decryption a laborious and complicated process. Therefore, different cryptographic algorithms, such as elliptic curve and lattice based cryptosystems, must be put into place. You can use AES to encrypt large amounts of data.

Since DTLS operates across the connectionless transport layer, it should be chosen over TLS as the transport protocol for securing IP transactions. Because it takes too many messages to set up IPsec, which secures IP communication, it should be avoided. Nevertheless, as demonstrated in Figure (7), IPsec and TLS can be employed even when vehicles are not in motion.

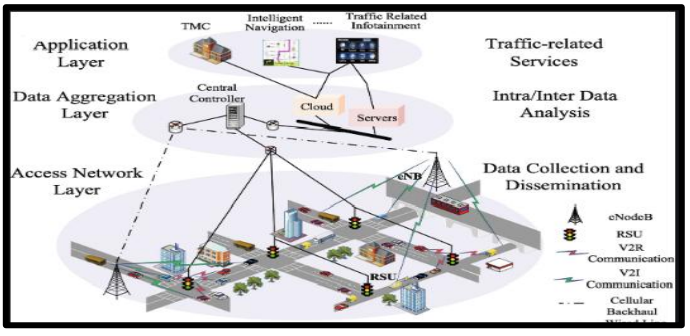


Fig .6. Transport protocol choice.

## 5. CONCLUSION

Due to the high number of persons killed or seriously injured on the road as a result of careless or malicious driving, users are more concerned about their own safety. More work will be needed in the future to overcome these challenges and provide a safe VANET environment. provided a thorough analysis of the majority of VANET security issues, including their origins, current solutions, and potential future developments. We believe that more study is needed to address the security and privacy concerns to the VANET system, and that future research should center on privacy preservation and other related issues. Furthermore, strong authentication methods should be incorporated into the security system to guarantee secure communication in VANETs. In addition, dealing with various security threats calls for an efficient algorithm. Shared traffic data, including vehicle identifiers and locations, as well as weather reports, are becoming increasingly important in ITS through the use of V2X, C-V2X, and LTE-V communications. Due to the sensitive nature of the vast quantities of data and information transferred, both drivers and passengers are seeking assurances of reliability and trustworthiness. This means they need a complex VANET algorithm that safeguards the privacy of their vehicle identifiers and whereabouts while facilitating reliable communication between V2V and V2I.

## Conflicts Of Interest

The author declares no conflict of interest in relation to the research presented in the paper.

## Funding

The author's paper explicitly states that no funding was received from any institution or sponsor.

## Acknowledgment

The author would like to express gratitude to the institution for their invaluable support throughout this research project.

## References

[1] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, T. Weil, “Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions”, published in Communications Surveys & Tutorials, IEEE (Volume:13 , Issue: 4 ), pages 584-616, July 2011.

[2] R.S. Raw, M. Kumar, N. Singh, “Security Challenges, issues and their solutions for VANET”, published in International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013..

[3] M. Azees, L. Jegatha Deborah, and P. Vijayakumar, “Comprehensive survey on security services in vehicular ad-hoc networks,” IET Intelligent Transport Systems, vol. 10, no. 6, pp. 379–388, 2016..

[4] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, “VANET security surveys,” Computer Communications, vol. 44, pp. 1–13, 2014..

[5] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, “VANet security challenges and solutions: a survey,” Vehicular Communications, vol. 7, pp. 7–20, 2017..

[6] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, “Vehicular ad hoc networks (VANETS): status, results, and challenges,” Telecommunication Systems, vol. 50, no. 4, pp. 217–241, 2012.

[7] M. Azeez, L. Jegatha Deborah, and P. Vijayakumar, “Comprehensive survey on security services in vehicular ad-hoc networks,” IET Intelligent Transport Systems, vol. 10, no. 6, pp. 379–388, 2016.View at: Publisher Site | Google Scholar

[8] Z. Lu, G. Qu, and Z. Liu, “A survey on recent advances in vehicular network security, trust, and privacy,” IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 2, pp. 760–776, 2019.

[9] S. Sharma and A. Kaul, “A survey on intrusion detection systems and honeypot based proactive security mechanisms in VANETs and VANET Cloud,” Vehicular Communications, vol. 12, pp. 138–164, 2018.

[10] A. Boualouache, S.-M. Senouci, and S. Moussaoui, “A survey on pseudonym changing strategies for vehicular ad-hoc networks,” IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 770–790, 2018.

[11] Ali, A. Hassan, and F. Li, “Authentication and privacy schemes for vehicular ad hoc networks (VANETs): a survey,” Vehicular Communications, vol. 16, pp. 45–61, 2019.

[12] X. Liang, T. Yan, J. Lee, and G. Wang, “A distributed intersection management protocol for safety, efficiency, and driver’s comfort,” IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1924–1935, 2018. 28. T. Neudecker, N. An, T.

[13] Gauge, and J. Mittag, “Feasibility of virtual traffic lights in non-line-of-sight environments,” in Proceedings of the Ninth ACM International Workshop on Vehicular Inter-Networking, Systems, and Applications—VANET’12, pp. 103–105, Lake District, UK, June 2012.View at: Publisher Site | Google Scholar

[14] Draft guide for wireless access in vehicular environment (WAVE) architecture 2012, http://ieeexplore.ieee.org/servlet/opac?punumber-6320593.
[15] M. Ghosh, A. Varghese, A. A. Kherani, and A. Gupta, “Distributed misbehavior detection in VANETs,” in Proceedings of the IIEEE Wireless Communications and Networking Conference (WCNC), Budapest, Hungary, April 2009.
[16] X. Cheng, C. Chen, W. Zhang, and Y. Yang, “5G-Enabled cooperative intelligent vehicular (5GenCIV) framework: when Benz meets Marconi,” IEEE Intelligent Systems, vol. 32, no. 3, pp. 53–59, 2017.View at: Publisher Site | Google Scholar