FUDMA Journal of Engineering and Technology

ISSN: 3092-9385

https://sites.google.com/fudutsinma.edu.ng/fjet

Volume 1, Issue 2, 2025, 436-441

A Review on Vehicular Ad Hoc Network (VANET) Security challenges and Solutions

Lawal B. IDRIS

Department of Computer Science, College of Science and Technology, Hassan Usman Katsina Polytechnic, Katsina, Katsina State, Nigeria

lawal.idris.bagiwa@hukpoly.edu.ng

Abstract

Vehicular Ad Hoc Networks (VANETs), enable communication between moving vehicles called nodes and roadside infrastructures. These communications are meant to increase driver assistance, efficiency, and traffic safety. From a security and privacy perspective, the vehicles in these systems are open to Sybil, DoS or DDoS attacks. The main areas of concern in VANETs are security and privacy of users. This research was aimed at reviewing security issues in Vehicular Ad Hoc Networks (VANETs), taking a closer look at how these networks are struggling with real-world threats. It examined a range of incidents recently reported and various ways attackers get into these networks and identifying vulnerabilities like insider attacks, denial-of-service (DoS), and the challenges of current cryptographic solutions. There is a clear indication that the security frameworks currently rely on are failing; insider attacks, DoS attacks, and weak encryption solutions seem to manifest themselves. However, these networks are key for vehicle communication as well as control and can seriously affect public safety. It is obvious that stronger solutions are needed to keep data and user privacy in a safe manner. Therefore, this study not only identified and explained the vulnerabilities in VANET but also offers some basic recommendations for building strong security frameworks in the networks.

Keywords: *Challenges, review, security, solutions, VANETs.*

1.0 Introduction

The vehicular ad hoc network (VANET) is a subset of mobile ad hoc network (MANET) that is built by moving vehicles called nodes. The nodes communicate wirelessly with each other without the use of established infrastructure. Once the network architecture changes, nodes are free to migrate arbitrarily as the nodes are available to move. Consequently, each node serves as a router by forwarding traffic to nodes it is directed to. VANET is a self-configuring, infrastructure-free network of mobile devices that are connected without the usage of wires. VANETs are employed in intelligent transportation systems (ITS), ITSs are intended to provide passengers and vehicles with road safety services (accident alarm, driver assistance, traffic flow optimization, congestion reduction, and so on) as well as luxury services (Internet access, games, etc.) (Mirza & Bakshi, 2018; Muthukumaran, 2017). This study concentrates on the security challenges facing the VANETs as discussed by different authors.

It also takes a closer look at the current solutions and figured out if they can really handle today's shifting in the security landscape. Researchers often note that the ever-changing nature of VANETs with vehicles constantly joining and leaving the network creating unique challenges for managing and distributing keys "Privacy preservation in VANETs, is a critical concern, as the frequent broadcasting of vehicle locations and other sensitive information can lead to tracking and profiling of individuals (Hayes & Omar, 2019). Balancing privacy with the need for accountability in case of accidents or law enforcement requirements remains a significant challenge (Gupta, Singh, & Tiwari, 2023).

This research is important because it offers value both in theory and in practice. By reviewing the challenges and solutions around VANET security. It discusses the practical guidelines for developers and policymakers working for safer travel systems (HR & Aithal, 2022). A look at related technologies and methods along with some illustrations presented in relevant literature shows that security measures are constantly evolving. It also stands as a key resource meant to provide fresh innovation in VANET security, which is crucial for attaining safer intelligent transportation systems (ITS). Figure 1 describes the Urban transportation system featuring traffic signals and communication infrastructure

Received: 26/08/2025; Revised: 12/09/2025; Accepted: 13/09/2025; Published: 15/09/2025

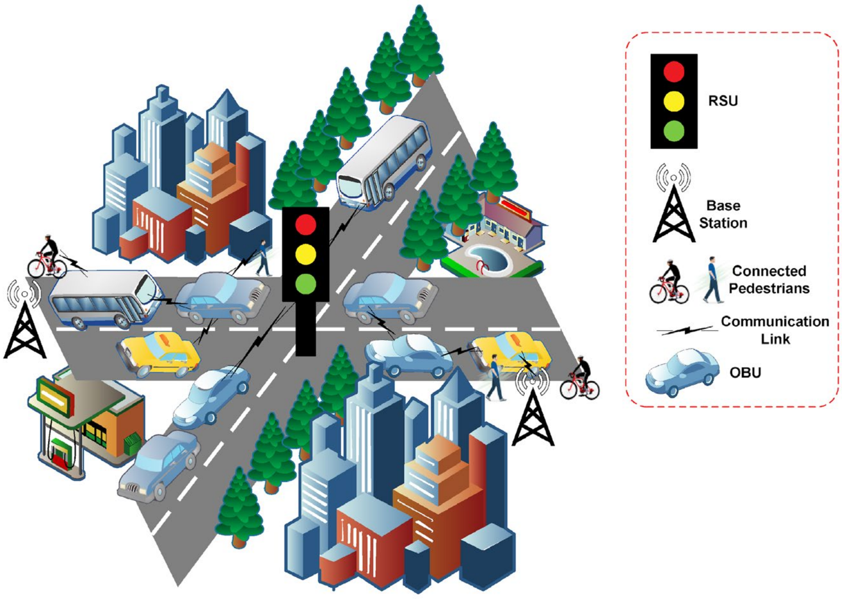

Figure 1: Urban transportation system featuring traffic signals and communication infrastructure (Gayathri & Gomathy, 2022)

2.0 Literature Review

VANETs are formed by extending the principles of mobile ad hoc networks (MANETs) – the spontaneous formation of a wireless network of mobile devices – to the domain of Vehicles (Muthukumaran, 2017). VANETs were initially mentioned and introduced in 2001 as "Vehicle-to-Vehicle ad-hoc mobile communication and networking" applications (Alam & Rababah, 2020), in which networks is built and information transferred among Vehicles. It was demonstrated that vehicle-to-vehicle and vehicle-to-roadside communications architectures coexist in VANETs to provide road safety, navigation, and other roadside services.

VANETs are important component of the intelligent transportation systems (ITS) framework. VANETs are also known as Intelligent Transportation Networks (Patel et al., 2019). They are thought to have grown into a broader "Internet of Vehicles."(Rahim et al., 2021) which is projected to eventually evolve into a "Internet of self-directed vehicles."(Ray, 2018). While VANETs were initially viewed as a one-to-one application of MANET concepts, they have subsequently evolved into a separate field of study. The word VANET had essentially become synonymous with the more generic term Inter-Vehicle Communication (IVC), although the emphasis remained on the feature of spontaneous networking, rather than the utilization of infrastructure such as Road Side Units (RSUs) or cellular networks. However, the vehicles in VANETs are open to Sybil, DoS or DDoS attacks. The main areas of concerns are security and privacy of users

In order to overcome these challenges, Zhang et al. (2008), devised a scheme in which Road Side Unit (RSU) was utilized to aid in message authentication and authorization. When a vehicle reaches the coverage range of a RSU, the vehicle will establish a secret key after mutually authenticating with the RSU and the vehicle will utilize the secret key to create a short Message Authentication Code (MAC) using the secret key. The RSU will conduct an authentication check on the MAC. In this scheme however, when the certificate is made public, it poses the problem of Vehicle being able to be tracked down to their origin by attacker.

Wasef et al. (2009) developed the RSU-aided distributed certificate service (DCS). The scheme provides a method for vehicles to effectively update their certificates from a RSU. A vehicle can update its certificate from any RSU, even if the vehicle is not within the original RSU's coverage range. However, the performance of DCS is affected by the density of RSUs.

Studer et al. (2009) introduced Timed Efficient Synchronous Loss-Tolerant Authentication plus Plus (TESLA++), an improved TESLA version that is more secure and efficient. In TESLA++, the sender broadcasts the MAC first, followed by the entire message and the authentication key after a short delay. However, the scheme uses anonymous authentication and require one-to-one communication between vehicles and the Trusted Authority (TA) which leads to privacy breach, routing challenge and computational overhead (delay in response time).

Gupta et al. (2023), proposed message authentication scheme utilizing proxy vehicles. It can drastically minimize computing overhead for roadside equipment. In this type of message authentication technique, proxy vehicles validate numerous messages at the same time, increasing the computational efficiency of roadside units when there are a significant number of vehicles in their coverage zones. The scheme was termed Proxy-Based Authentication Scheme (PBAS). However, computation overhead is still high in the scheme.

Received: 26/08/2025; Revised: 12/09/2025; Accepted: 13/09/2025; Published: 15/09/2025

In Cheng et al. (2024) Vehicle anonymous credentials were created using a combination of random numbers in the TA and on the vehicle side. The TA provides zero-knowledge proof, which protects the vehicle's privacy during authentication, and facilitates mutual recognition of vehicles and roadside identities. An integrated key generation technique was developed. In this situation, the group key is generated jointly by the TA and the roadside. To maintain security, the roadside obtains the group session key parameter GSPr by calculating the anonymous credentials of all authorized vehicles. This allows for quick updates of the group session key. The TA uses a previously filled quantum key to encrypt the group session key parameter GSPc generated by its quantum random number generator. This approach ensures one-at-a-time encryption while achieving both forward and backward security. Table 1 summarizes the existing VANET Security Challenges and Solutions.

Table 1: VANET security challenges and solutions

S/N	Challenge	Description	**Proposed Solution**	**Effectiveness**	**Year**
1.	Privacy	Protecting sensitive vehicle and driver data	short Message Authentication Code (MAC) schemes	Medium	2008
2.	Authentication	Verifying legitimacy of vehicles and messages	Timed Efficient Synchronous Loss-Tolerant Authentication plus Plus (TESLA++)	High	2009
3.	Integrity	Ensuring data has not been tampered with	Proxy-Based Authentication Scheme (PBAS)	High	2023
4.	Availability	Maintaining network services despite attacks	Intrusion detection systems	Medium	2024
5.	Non-repudiation	Preventing denial of sent messages	Blockchain-based logging	High	2025

Source: (Dalal, 2025)

The security aspect of VANET presents a significant challenge in terms of protecting the network from various authentication, attacks, privacy issues, and data leakage. VANET still has various vulnerabilities that attackers might take advantage of (Ahmad, 2021). Vehicle related accidents, which according to the World Health Organization (WHO) cause around 1.27 million human deaths each year, ranked ninth among the world's causes of human fatalities (WHO, 2020). The cities of both developing and developed countries now face major traffic congestion problems (Kheradmand et al., 2022). There are various solutions to these problems, the most popular being to look at it from the perspective of a smart city. Smart cities incorporate every conceivable end point, including people, households, buildings, and vehicles, into the same network. Academic institutions, vehicle manufacturers, and security agencies have all shown an interest in VANETs (Sasikaladevi & Reddy, 2023, Garba, 2025).

3.0 Methodology

Vehicles using Vehicular Ad Hoc Networks (VANETs) have been getting a lot of attention in these days because they promise to boost road safety and ease traffic. Yet, as this technology advances, a number of security issues manifest (Garba, 2025). VANETs, with their fast movement and constantly changing technology, simply demand high security measures (Dayan & Twitto, 2021). The methodology applied in this research involves reviewing major academic databases, setting out criteria for relevant study, and then using qualitative methods get the required information for the research. This approach was chosen because it is one of the prominent methods that provides evidence-based information (Gayathri & Gomathy, 2022).

4.0 Results

Certain protocols, such as SMT and SEAD, used the hash function or MAC for authentication. When it comes to encryption and decryption, this process is quicker than any others. In addition to conventional mechanisms, researchers are also interested in several more recent approaches. NTRU and Elliptic Curve Cryptography (ECC) are two examples. ECC has been embraced by numerous research teams. Even with a shorter key length, the approach is sufficiently quick and secure thanks to the usage of ECC. The IEEE P1363 working group recently adopted the NTRU cryptosystem. It is an asymmetric cryptosystem that is resistant to quantum computing. In terms of signing and verification, it is quicker than both RSA and ECC.

Asymmetric cryptography has also been used to introduce digital signatures for non-repudiation and authentication. To encrypt, decrypt, and create a signature, this method also uses more processing power. Various protocols have employed PKI (Public Key Infrastructure) as an alternative method for node authentication. With this method, all nodes receive certificates from a central body known as the CA (Certificate Authority). The CA has signed the certificate, which includes details about the keys, certificate number, etc. A node only authenticates the certificate from the CA if it wants to authenticate itself. Maxim Raya et al. demonstrated that this method can be used in VANET; nonetheless, the main obstacle to its application is certificate revocation.

Received: 26/08/2025; Revised: 12/09/2025; Accepted: 13/09/2025; Published: 15/09/2025

Although the primary purposes of these cryptosystems are privacy and authentication, availability is still the fundamental problem that needs to be resolved. This attack is multi-layer, so separate mechanisms should be implemented at the physical and network layers. For example, the physical layer may employ DSSS (Direct Sequence Spread Spectrum) and FHSS (Frequency-Hopping Spread Spectrum), while a secure routing protocol can be employed to prevent DoS attacks.

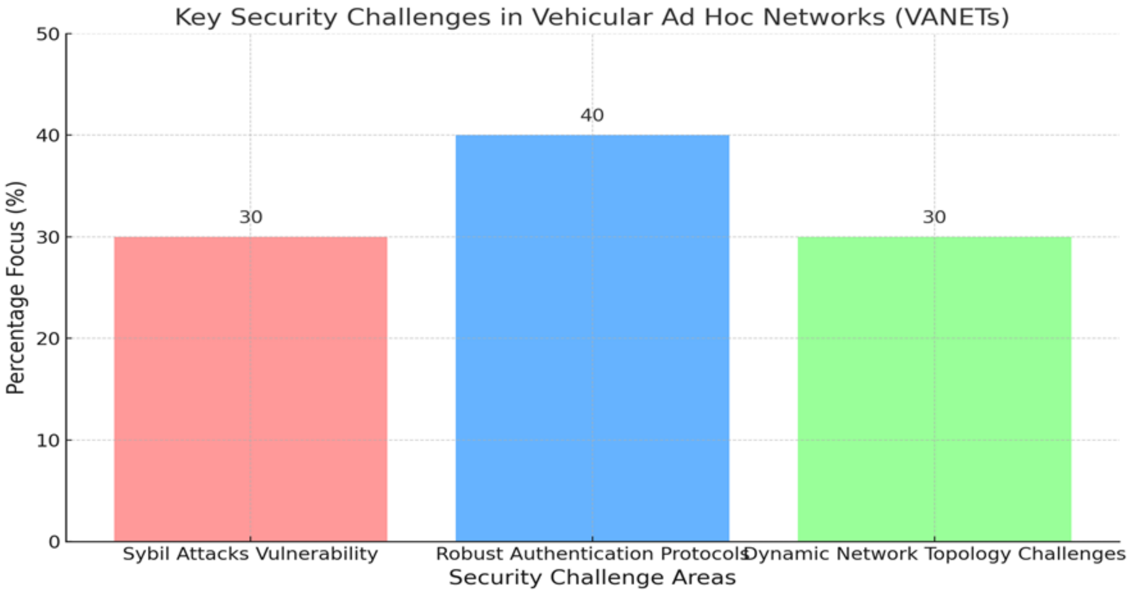

Figure 2: Key security challenges in Vehicular Ad Hoc Networks (VANETs)

Figure 2 described the distribution of key security challenges in Vehicular Ad Hoc Networks (VANETs). Each bar represents the percentage focus on specific challenge areas based on their significance and impact. The chart highlights that "Robust Authentication Protocols" received the highest attention at 40%, while "Sybil Attacks Vulnerability" and "Dynamic Network Topology Challenges" were both at 30%. This representation effectively communicates the emphasis on various security concerns in the context of VANETs. Table 2 provides the overview of VANET Security Challenges and Solutions.

Table 2: VANET Security Challenges and Solutions Overview

S/N	Challenge	Description	Proposed Solution	Effectiveness (%)	Challenge
1.	Authentication	Ensuring legitimate vehicles and messages	Public Key Infrastructure (PKI)	85	Authentication
2.	Privacy	Protecting vehicle and driver information	Pseudonym-based schemes	78	Privacy
3.	Data Integrity	Preventing message tampering	Digital signatures	92	Data Integrity
4.	Availability	Mitigating Denial of Service attacks	Intrusion Detection Systems	70	Availability
5.	Non-repudiation	Ensuring accountability for sent messages	Blockchain-based logging	88	Non-repudiation

5.0 Discussion

In order to address concerns about vehicles continuously broadcasting sensitive information, privacy solutions in VANETs are crucial. By enabling cars to regularly alter their IDs, pseudonym shifting techniques significantly improve privacy by making it more difficult for adversaries to track specific vehicles over time. Furthermore, the use of anonymous authentication procedures and group-based communication can further reduce the possibility of profiling and safeguard user identities. An overview of the mitigating techniques suggested to address privacy issues in VANETs

To maintain security, the roadside obtains the group session key parameter GSPr by calculating the anonymous credentials of all authorized vehicles. This allows for quick updates of the group session key. The TA uses a previously filled quantum key to encrypt the group session key parameter GSPc generated by its quantum random number generator. This approach ensures one-at-a-time encryption while achieving both forward and backward security. Calculations were made of the computing and signaling overheads, with the signaling overhead

Received: 26/08/2025; Revised: 12/09/2025; Accepted: 13/09/2025; Published: 15/09/2025

being cut in half and the group key issuance time was significantly reduced compared with other schemes. However, there is Possibility of privacy breach as shown in Table 3.

Table 3: Summary of security challenges in VANETs

Privacy Challenge/Attack	Description	Effects	Probability of Occurrence
Location Privacy	Manipulation of reported location information.	Misguides other vehicles, compromising traffic flow, safety applications, and coordination mechanism	High
Identity Disclosure	Unauthorized exposure of a user's real identity.	Compromises user privacy, may lead to tracking, profiling, and potential misuse of personal information.	High
Data Minimization	Inadequate efforts to limit the collection of unnecessary data.	Increased risk of privacy breaches, exposure of sensitive information, and potential misuse of collected data.	High
User Consent and Control	Lack of mechanisms for users to control data sharing and provide consent.	Users may be unaware of or unable to manage data sharing, leading to involuntary exposure of personal information	Moderate
Social Engineering Attacks	Manipulation of individuals to disclose sensitive information	Unauthorized access to personal data, compromise of security credentials, and potential misuse of obtained information.	High

Symmetric algorithms are effective and use less CPU time, but their key generation complexity is O(n2), where n is the number of network nodes [14]. The main problem with this strategy is the key distribution as well. The symmetric technique will need more space to store keys that are not used when the network gets sparse as it gets bigger. Since each node only needs one secret and public key pair in an asymmetric architecture, the complexity becomes O (n). Nevertheless, these methods result in a message delay and need extra execution time. This is not a major concern because VANETs have sufficient processing capability to carry out these intricate algorithms. Therefore, VANET can use asymmetric cryptography.

Even though setting up solid communication and security protocols is key, the review also stresses that putting user trust and privacy front and center remains critical. As previous work put it, "trust management in VANETs is crucial for ensuring the reliability of shared information. Developing robust trust models that can quickly adapt to the dynamic nature of vehicular networks while being resilient to various attacks remains an open research focus. Therefore, future studies should focus on how people feel about challenges and how society will accept new solution not only concentrate on the protocols (Kaur et al., 2024). Table 5 displays the Common VANET Security Attacks and Solutions

Table 3: Common VANET security attacks and solutions

S/N	Attack Type	Description	Impact	Proposed Solution	Attack Type
1.	Denial of Service (DoS)	Floods network with fake messages	Disrupts communication	Intrusion detection systems	Denial of Service (DoS)
2.	Sybil Attack	Creates multiple fake identities	Manipulates voting/routing	Position verification	Sybil Attack
3.	Man-in-the-Middle	Intercepts communications	Eavesdrops/alters messages	Encryption and authentication	Man-in-the-Middle
4.	GPS Spoofing	Broadcasts false location data	Causes navigation errors	Plausibility checks	GPS Spoofing
5.	Black Hole	Drops all received packets	Disrupts routing	Watchdog mechanisms	Black Hole

6.0 Conclusion

A vehicle ad hoc network, or VANET, permits communication between moving items and infrastructure along the route. These messages are designed to improve traffic safety, efficiency, and driver aid. The systems' vehicles are vulnerable to attacks in terms of security and privacy. Security and user privacy in VANET are the primary areas for concern. The genuine identity of the message sender must be quickly verified for authenticity and integrity to prevent attacks. Nonetheless, reducing security challenges is essential, especially for signals pertaining to safety. This research reviewed different literature, identified different challenges facing VANETs security and solutions as proposed by various authors. The research suggests more in-depth research of VANET security by using Machine Learning, Internet of Things (IoT) and block cahin technology for building stronger solutions that keep vehicular communications more safer and authentic (HR & Aithal, 2022, Karabulut et al., 2023).

References

Dalal, K. (2025). Ensuring Secure Transmission in VANET: Optimal Clustering and Improved LSTM-Based Intrusion Detection. *International Journal of Communication Systems, 38*(4), e6125.

Dayan, N., & Twitto, M. (2021). *Chucky: A Succinct Cuckoo Filter for LSM-Tree.* Paper presented at the Proceedings of the 2021 International Conference on Management of Data.

Garba, M. (2025). Trust Evaluation in VANETs with Blockchain and Reinforcement Learning.

Gayathri, M., & Gomathy, C. (2022). An Overview of Security Services and Trust-Based Authentication Schemes in VANET. *Micro-Electronics and Telecommunication Engineering*, 193-205.

Gupta, C., Singh, L., & Tiwari, R. (2023). Malicious node detection in vehicular ad-hoc network (vanet) using enhanced beacon trust management with clustering protocol (ebtm-cp). *Wireless Personal Communications, 130*(1), 321-346.

Hayes, M., & Omar, T. (2019). *End to end VANET/IoT communications a 5G smart cities case study approach.* Paper presented at the 2019 IEEE International Symposium on Technologies for Homeland Security (HST).

HR, G., & Aithal, P. (2022). Approaching Research in Different Ways-How to Choose an Appropriate Research Approach/Reasoning During Ph. D. Program in India? *International Journal of Philosophy and Languages (IJPL), 1*(1), 59-74.

Karabulut, M. A., Shah, A. S., Ilhan, H., Pathan, A.-S. K., & Atiquzzaman, M. (2023). Inspecting VANET with various critical aspects–a systematic review. *Ad Hoc Networks*, 103281.

Kaur, U., Mahajan, A. N., Kumar, S., & Dutta, K. (2024). Security Vulnerabilities in VANETs and SDN-based VANETs: A Study of Attacks. *International Journal of Computer Networks and Applications, 11*(6).

Kheradmand, B., Ghaffari, A., Soleimanian Gharehchopogh, F., & Masdari, M. (2022). Clustering-based routing protocol using gray wolf optimization and technique for order of preference by similarity to ideal solution algorithms in the vehicular ad hoc networks. *Concurrency and Computation: Practice and Experience, 34*(23), e7209.

Sasikaladevi, N., & Reddy, M. N. (2023). Energy-Efficient Privacy Preserving Vehicle Registration Protocol for V2x Communication in Vanet *Advanced Computer Science Applications* (pp. 337-349): Apple Academic Press.

Received: 26/08/2025; Revised: 12/09/2025; Accepted: 13/09/2025; Published: 15/09/2025