Archives available at journals.mriindia.com

International Journal on Advanced Computer Theory and Engineering

ISSN: 2319 - 2526

Volume 15 Issue 01s, 2026

A Guide to Safe Vehicle Ad Hoc Networks: Perspectives and Analogies

[1]Mayur J. Patil [0009-0000-0540-8783], [2]Dr. K. P. Adhiya[0000-0002-3925-0213]

[1] Research Scholar, SSBTs COET Bambhori, Jalgaon, Maharashtra, India

[2] Professor, Department of Computer Engineering, SSBTs COET Bambhori, Jalgaon, Maharashtra, India

Email: [1]mayurpatil.rcpit@gmail.com, [2]kpadhiya@yahoo.com

Peer Review Information

Submission: 08 Dec 2025

Revision: 25 Dec 2025

Acceptance: 10 Jan 2026

Keywords

VANETs, Security, Authentication, Privacy, Attacks.

Abstract

Concerningly, traffic accidents have been on the rise globally, resulting in significant human and material losses. This highlights the critical need for creative and effective solutions to address this issue. A new wireless communication technology called Vehicular Ad Hoc Networks (VANETs) has recently gained a lot of attention from researchers because of its potential to improve traffic management and road safety. Nevertheless, in spite of these advantages, VANETs have considerable security concerns. Their essentially open and dynamic traits make them especially susceptible to numerous harmful threats, endangering the network's reliability and the users' safety. Establishing robust security mechanisms is essential for developing resilient and reliable VANET systems that can effectively mitigate threats and safeguard network integrity. An overview of vehicle ad hoc networks (VANETs), together including its design and salient features, is given in this study. It explores the primary security issues VANETs face and underlines the essential need of a safe network environment. The study investigates important security concerns and how they impact VANET integrity in order to underline the shortcomings threatening this integrity. Viewing these hazards, this work looks at and assesses some possible countermeasures. Organizing several security solutions into groups and carefully evaluating them helps one to determine which ones are most appropriate for particular security issues.

Introduction

Rapid advancements in wireless communication have piqued interest in exploring potential new areas of use. Since more and more manufacturers are installing wireless communication devices into their automobiles, this trend has had a disproportionate impact on the automotive sector. Since this is happening, the idea of "smart cars" is moving closer to becoming a reality. With the proliferation of smart, connected vehicles, we can anticipate an improvement in connectivity and an expansion of intelligent transportation systems [1]. Vehicular Ad Hoc Networks (VANETs), a unique network paradigm, are set to transform transportation by facilitating seamless communication among themselves. By enabling real-time data transmission between vehicles, this cutting-edge technology has the potential to revolutionize traffic systems by enhancing traffic flow and lowering congestion. We expect VANETs to significantly improve road safety because they enable sophisticated warning systems, accident prevention techniques, and effective route planning. Further development of this technology will redefine the future of transportation, ushering in a new era of safer, smarter, and more effective roads [2].

Vehicular Ad Hoc Network is an amazing technological evolution of the network which might prove to change the course of transportation. VANETs can communicate in real time with the car so as to increase the chances for improved

traffic circulation and reduce tailbacks on busy roads. They will do so by introducing advanced security features such as early warning systems, accident prevention strategies, and intelligent routing, and will eventually transform the future of VANET's development, rehabilitating the transport domain for improved safety, smarter connectivity, and more effectiveness to envision a new way road can be used for vehicular movements. [3]. As road safety directly and indirectly affects lives, that is, more than one million deaths and over 50 million injuries - as reported by alarming facts - it continues to be high on the agenda of traffic management. Alarmingly, several reports have stated that unless prompt and effective measures are taken, road accidents are expected to rise by about 60% in the next couple of years. The gruesome reality thus highlights the urgent need for comprehensive plans and creative solutions to address the underlying causes of traffic crashes and to improve safety for all road users. Besides the horrific toll on human life, traffic congestion entails a huge wastage of time and an economic cost. The annual losses due to loss of time, productivity, and wastage of fuel run into several hundreds of millions. These inefficiencies affect the quality of life of people and communities as well as place a drain on the economy: hence, innovative approaches need to be devised to tackle these problems of optimizing road transportation, reducing congestion, and dealing with its attendant social economic problems [4].

Vehicular Ad hoc networks (VANETs) offer a suitable way to improve the traffic environment and lessen road-related problems. By means of integrated wireless and processing technologies, VANETs-a specific and special subset of the Mobile Ad-hoc Network (MANETs)-enable vehicles to communicate with infrastructure and with other vehicles. These new advancements allow information exchange between different units of a road and vehicles. The possibilities for synergistic, sophisticated transportation systems are extravagant in providing a safer way of commutation. Such a system can open a new age for road transport with reduced congestion and accidents to allow smarter mobility platforms. [2]. VANETs come from a different school of thought than other types of MANETs with nature that assigns operating constraints to vehicles on a predetermined road infrastructure and traffic laws like signs and signals. VANET nodes exclusively operate on controlled movement patterns within the bounds of road networks, unlike free-moving networks. They are vehicles capable of wirelessly communicating with one another and sharing information on real-time traffic and roads. Under this overarching context, VANETs intend to promote road safety, efficient traffic management, and improved driver experiences [5] [6].

With vehicle technology becoming more complex, a great number of applications in the sphere of VANET can be outlined on the cline of safety/non-safety. While safety applications mainly prioritize human lives and danger avoidance, they include emergency alarms and warnings of hazardous road conditions. In this respect, they provide timely, life-saving information, which reduces the possibilities of road accidents. Non-safety applications, however, involve the transfer of infotainment, navigation aid, and real-time traffic information in favour of user comfort and productivity. Over the whole picture, these applications indicate what VANETs can do in terms of revolutionizing present-day transportation [7] [8]. Safety applications in VANETs are aimed at putting road safety first by reducing the chances of collision and immediately responding to any possible threats. This software includes a wide range of utilities, from traffic management tools, collision avoidance systems, to alerts on emergency vehicles, signal infractions, sharp curves, work zones, and adverse road conditions. The ultimate goal, however, is to reduce fatal accidents by informing drivers quickly and reliably, thus saving lives. Meanwhile, non-safety applications focus on the overall experience of a journey by adding convenience and enjoyment. They facilitate things such as online gaming, audio and video sharing, internet access, and weather updates, in addition to providing useful features like payment systems, parking aids, and guidance to nearby venues. Together, these two groups of applications will work toward changing the way transportation systems work on the rating scale in the near future [4] [7] [8].

The ability to convey messages easily among the nodes of the VANETs is pertinent for both safety and non-safety applications. These applications are based on the exchange of messages which rely on two important factors: validity of the message contents and security of the transmitters. Any degradation of the integrity of information or authenticated identity of senders would cause failure of the network, causing inefficiencies and potentially creating safety hazards. Thus, it is vitally important for the roles of communication to be established reliably and to share validated data safely so as to ensure uninterrupted and safe functioning of the applications [9]. Due to their special features, namely great mobility and open communication routes, VANETs are especially subject to a range of cyber-attacks. A successful breach of the network may incur catastrophic consequences, ranging from costly traffic snarls or fraudulent activities to the loss of human lives

due to safety applications being compromised. Therefore, one top priority in VANET development is ensuring that preventive measures are robust. By remedying any weak spots or vulnerabilities and putting into place robust protections, VANETs will provide a reliable and trusted platform to develop secure and efficient transportation systems [10].

This study mainly intends to supply readers and researchers much fond of the security aspects of VANETs with a refined foundational source. In looking at issues like general architecture of VANETs, specific problems they face, basic security requirements for reliable operation, and different types of possible attack that could strike at the network level, it aims to provide foundational background knowledge. By covering such topics, the paper serves as a springboard for more research and development in this area and provides a guide for enhancing understanding and resolution of the intricacies of VANET security.

Table 1. Section wise Content Covered

Section No.	Content Covered
2	Gives information about the components and operational layout of VANET's structural framework.
3	Outlines the main obstacles that VANET must overcome, including as security, environmental, and technical problems.
4	Describes the fundamental security needs to create a dependable and safe VANET.
5	Explains and evaluates the main assault types that target VANET and the possible consequences of each.
6	Explains possible defences against the aforementioned attacks, including how to categorize and compare them.
7	Ends the paper by summarizing the outcomes and offering some concluding remarks on VANET security.

VANETs Structure

Multiple wireless communication technologies are used to ensure reliable and efficient data sharing within vehicular networks. An important technology specifically designed to accommodate extreme dynamicity in vehicular situations is Dedicated Short-Range Communications (DSRC), which operates within the 5.9-GHz band. DSRC allows for fast data transfer; thus, infrastructure and vehicles can communicate in case of emergency. DSRC supports signal ranges extending to 1000 m, allowing the timely dissemination of critical information such as traffic updates and safety warnings, thus boosting network reliability and performance with a keen eye toward safety [2] [11].

Vehicular networks exploit DSRC combined with several other wireless communication technologies overall in order to give an efficient and adaptable connectivity. Wi-MAX can let people get very high internet speeds over the long distance which means the service is very widespread. Using fast and unbroken cellular networks like 4G and 5G, users may continue to stay connected and share data while they are on the go. Wireless Fidelity (Wi-Fi) enables uninterrupted internet access for leisure and convenience applications, whilst Wireless Local Area Network (WLAN) provides localized connectivity, suitable for short-range interactions. These technologies work together to establish a unified environment that improves the functionality and performance of vehicle networks [7].

Any vehicle form that is part of the VANET has specialized device hardware that enables radio communication with the rest of the nodes to deliver data efficiently within the network. The node may be a host or a router, depending on which specific task it performs. The host's action is to send data requests while the router's action is to move data to other nodes. Even if the network has a decentralized structure, this feature allows the network to be adaptable and capable of taking dynamic data and consequently everywhere around the network will get access to it. The mobile node is usually of two types, one is more to master the data request and the other is the one that distances the data [12].

Vehicles:

VANETs are wireless networks that involve mobile nodes representing dynamic vehicles connected to the network. An On-Board Unit (OBU) is a technical tool that nodes have to make communication more effective. To enable a proper data exchange with the network nodes, the OBU is processed with wireless transmitter and receiver modules. The OBU is designed to be a facilitating factor for uninterrupted and real-time communication among the vehicles on the network by letting a vehicle communicate with the rest of the network and receive necessary data, including traffic updates, road condition, and safety alarms. The operation and effectiveness of VANETs totally rely on this technology [13].

Nowadays, the vehicles in VANET are instrumented with a wide number of other devices in addition to the On-Board Unit (OBU) for safety improvement and data acquired. Among the devices is an Event Data Recorder (EDR), which acts like the black box in an airplane. The EDR records key vehicle data, namely speed, position, time

and transmission parameters, as well as travel data and incoming messages. This stored info plays a key role in analyzing accidents after they happen. It gives a full picture of what occurred before during, and after a crash helping to pinpoint the cause. Cars also have a Tamper Proof Device (TPD) in addition to the EDR. The TPD guards private data, including encryption keys and driver details. It helps keep communications secure by processing, signing, and checking messages between network nodes. To make sure the network runs well and, cars also have various sensors to collect data. This data then gets processed and shared based on how important it is [4].

RSU:

Roadside units (RSUs) are fixed infrastructure nodes in a VANET, and are crucial to support communication between automobiles and the outside world such as the internet. RSUs are gateways or routers, extending the reach of the network, and aid in bridging the communication gap between vehicles. In this manner, RSUs help overcome the limitations of short-range ad hoc networks by dispersing information to carry it to further On-Board Units (OBUs) so that there is continuous data flow. These RSUs are placed appropriately on roads, are often attached to backbone networks, and, in turn, deliver a plethora of network services and applications for things like emergency alerts, traffic management, and real-time navigation-all of which work to make the vehicular network perform well overall [7] [13].

The two primary communication channels Vehicular Ad Hoc Networks (VANETs) use are Vehicular to Infrastructure (V2I) and Vehicular to Vehicular (V2V)—which also covers Infrastructure to Vehicle (I2V) communication. V2V communication allows direct information sharing between vehicles and makes possible technologies including cooperative driving, real-time traffic updates, and collision avoidance. Roadside units (RSU), traffic signals, and through road signals, V2I communication - it is communication between cars and roadside features - access to outer networks, direction aid and traffic control. Together, these two channels of communication provide a smooth and efficient automotive network designed to promote road safety and driving bliss [14] [15].

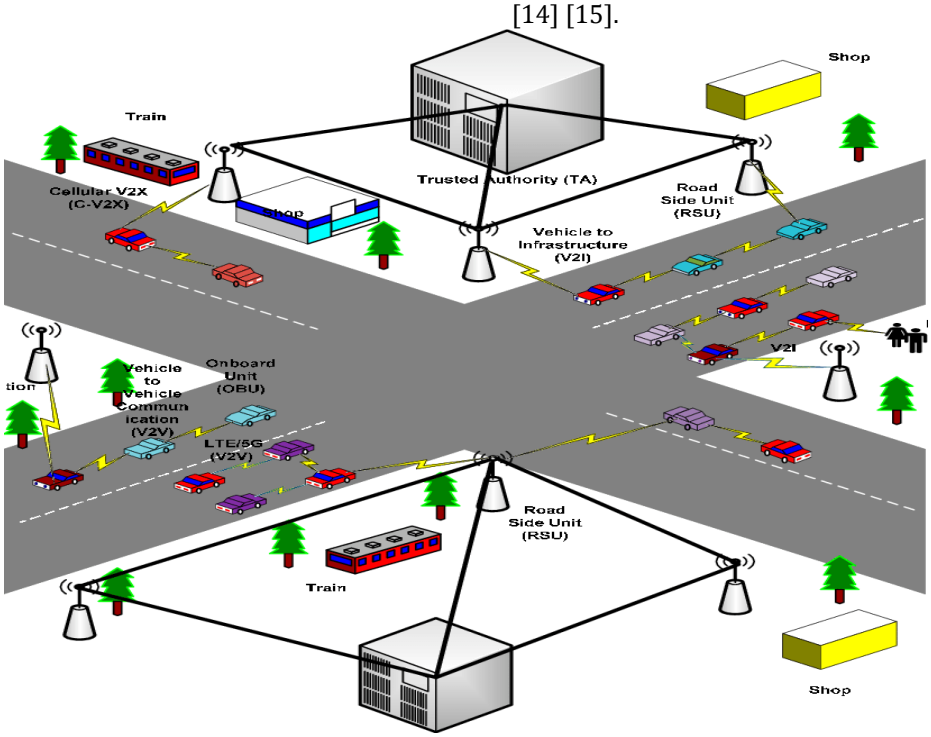

Fig. 1. VANETs ARCHITECTURE [37]

VANET Challenges

Due to their high dynamics, dynamic topology, and vehicle-to-vehicle and vehicle-to-infrastructure dependence on communication, waves are according to a separate definition from the traditional network. These specific features especially create difficulties that need to be removed to guarantee the development of a reliable and efficient network. The complexity of VANETS requires a constructive solution for everything from addressing problems with network scalability and delay to ensure safe communication in constraints constantly changing environments. The main issues to be solved to be effective of vent deployment and operation will be discussed and this will be investigated in this part. [16].

Table 2. Challenges in VANET

Challenges	Description
Volatility	Because of their great mobility, vehicles in VANETs frequently have erratic and transient connectivity with other vehicles. The connection between automobiles is short-lived since they travel quickly and can change directions, like in separate lanes. Because there is no long-lived context, it is challenging to safeguard communications using password-based methods. Furthermore, the short length of connections makes multi-phase or collaboration-heavy procedures like voting impracticable [4 17 18].
Scalability	VANETs have to handle millions of nodes that connect to the network sporadically, given that there are more than a billion cars on the road globally. Due to regional variations in vehicle equipment and protocols such as the different DSRC standards in North America and Europe the absence of a global regulatory organization for network standards makes issues more difficult. Additionally, only a tiny subset of vehicles can communicate with VANETs because many automobiles do not currently have the required technology [2 19].
Time Constraints	Safety and emergency alerts are among the communications in VANETs that must be delivered right away since they are time-sensitive. Delays in these messages could have catastrophic results. High priority, quick processing, and fast transmission are required for these messages. Efficient methods such as quick cryptography, quick message verification, and authentication algorithms must be used to overcome this difficulty and guarantee prompt communication [9 20].
Mobility	High-speed vehicle movement in VANETs produces extremely dynamic network topologies. Network stability is a problem since cars frequently establish fleeting connections with nodes they might never see again. It is difficult to secure communications in such dynamic circumstances, necessitating effective algorithms that maximize bandwidth and route management. Furthermore, the network density varies by region; for example, freeways with faster-moving vehicles may have sparser connections, while locations with low vehicle speeds or substantial traffic will have a larger density. It becomes even more difficult to establish consistent communication because of this fluctuation [2 5 21]
Liability	Especially when it comes to post-accident analysis, vehicle communications provide useful information that can support legal investigations. This calls for the ability to track the origin of communications in addition to other information like the driver's identification and trip specifics. But it's important to strike a balance between this requirement and privacy issues. Ensuring message traceability aids in preventing attackers from posing as cars, but protecting the message originator's anonymity and drivers' private data is just as crucial. Sensitive information, such as biometric data, which could be used to regulate and grant access to vehicles, should be kept extremely private and safe. Thus, it is crucial to find a balance between the necessity to protect privacy and anonymity and the legal requirements of culpability [4 18].

Security Requirements

Strict security guidelines are followed in the building process of such a network. Such specifications lay the foundation for the protection of privacy, integrity of data, and the general stability of the network. Without giving importance to these security guidelines, it may also damage the dependability of the network and create vulnerabilities that could be exploited by the wrong individuals. Since users and companies want secure settings for their communications, such weaknesses not only jeopardize the functioning of the network but also limit its potential for widespread deployment. Thus, successful operation and expansion of the network depend on adhering to and implementing these security principles [9].

It is essential to ensure the integrity and authenticity of network communications, especially with safety messages. Nodes should only receive

messages created by authorized parties and malicious actors must not be able to tamper with or censor them. It will, therefore, be correct information about things like traffic updates or safety alerts that may prove disastrous if wrong. The system has to maintain its safety and trust while at the same time creating a balance between privacy and accountability, so the nodes are not only accountable for their network activities but also are protected from access to their private information [20].

Basic requirements for security, needed for VANETs to function, will be discussed in the following sections. These are privacy, non-repudiation, integrity, availability, and authentication; all of these are essential for safety aspects and to ensure that the network remains secure. Availability ensures that the network keeps functioning, even when disturbed by unfavorable conditions, while authentication approves the nodes' authenticity and stops unauthorized access. Integrity does not allow manipulation of data; hence, the data will always be correct. Non-repudiation ensures that no party is capable of withdrawing their acts. As a result, the element of privacy avoids access to private information. As a whole, these requirements form the basis for evaluating and maintaining VANET security, and they are designed to be secure, dependable, and trustworthy in operation.

Table 3. Security Concern in VANET

Security Requirement	Description	Advantages
Authentication	By confirming their identity before allowing access, authentication makes guarantee that only valid nodes are permitted to take part in the network	1] Keeps malevolent entities and illegal access at bay. 2] Increases the network's dependability and confidence. 3] Keeps identity faking at bay.
Availability	Through constant access to vital services and data, availability guarantees that the network will continue to function even in the face of difficult circumstances.	1] Ensures continuous contact, which is essential for messages pertaining to safety. 2] Strengthens the network's resistance against failure or denial-of-service attacks. 3] Guarantees dependability in urgent circumstances.
Integrity	Integrity prevents information from being tampered with or corrupted during transmission by ensuring that the data transferred inside the network stays unchanged.	1] Guarantees the consistency and correctness of the data. 2] Prevents data modification, which is crucial for applications that depend on safety. 3] Increases the communication's believability.
Non-repudiation	By ensuring that the sender cannot retract their involvement once a message has been sent, non-repudiation serves as evidence of the activity committed.	1] Increases accountability by holding nodes accountable for their deeds. 2] Minimizes disagreements over decisions or activities taken inside the network. 3] Makes precise post-event analysis easier.
Privacy	Sensitive information, including a driver's name or car specifications, is shielded from illegal access and surveillance thanks to privacy.	1] Prevents the exposure of users' personal information. 2] Keeps tracking and illegal profiling at bay. 3] Guarantees adherence to data protection laws.

Attacks on VANET

Though still in the developing stages, vehicular ad hoc networks, or VANETs, are projected to encounter quite a number of security challenges. VANETs are vulnerable to potential attacks because of the inherent flaws in wireless transmission that can be exploited by malicious actors to weaken the network's security [9]. This section

elaborates on significant security threats encountered by VANETs, covers hypothetical scenarios indicating these threats, and lists important security countermeasures that have to be executed to address those attacks.

Table 4. Attacks on VANET with Impact and Solution

Attack Type	Description	Scenarios	Impact	Solution
Denial of Service (DoS)	By flooding or obstructing communication channels with dummy messages, it stops valid nodes from using network resources or services.	1] The network is overloaded by an attacker, which uses bandwidth and decreases effectiveness. 2] Access to other nodes is blocked when one node has exclusive control over its resources.	1] The availability of the network is jeopardized. 2] Effective communication is impossible for nodes.	1] Put in place reliable intrusion detection (IDS) systems. 2] To avoid too much traffic, use rate-limiting devices.
Sybil Attacks	In order to influence network behavior and disseminate misleading information, an attacker creates many fictitious identities and poses as various nodes.	1] Using fictitious congestion alerts to maliciously reroute traffic. 2] Posing as several nodes in order to compromise the integrity of data.	1] There are issues with availability and authentication. 2] Inefficiency is caused by congestion or inaccurate routing information.	1] Make use of identity verification tools, such digital signatures. 2] Install certificate authorities so that nodes may be verified.
Information Disclosure	This includes employing nefarious methods, including spreading viruses or malicious code to neighboring nodes, to get private information about a target node.	1] By infecting nearby nodes, a virus gathers data such as geo-location and individuality. 2] Systems for tracking vehicles are used maliciously.	1] This compromises the node owner's privacy. 2] Private information, like location or personal information, is made public.	1] Use encryption techniques for private information. 2] Make use of safe authentication procedures. 3] Update software frequently to avoid vulnerabilities.
Message Suppression/Alteration	Attacks that reuse, alter, distort, or conceal the contents of messages in order to obtain a competitive edge or interfere with communication.	1] Ignoring congestion alerts, which causes delays in transportation. 2] To confuse nodes, crucial signals are delayed or replayed.	1] There is a compromise in the communications' integrity. 2] Missing or changed messages impair network availability.	1] For content verification, use message authentication codes (MACs). 2] Implement redundancy measures for important communications.

				3] To stop messages from replaying, use time-stamping.
Impersonation/Masquerading	To interfere with network operations or obtain unauthorized access to resources, an attacker impersonates or steals a lawful node.	1] Posing as an ambulance in order to command other cars to yield and obtain lane priority. 2] Asking RSUs to change traffic signals.	1] There is a breach in the network's trust and authentication. 2] Traffic flow disruption and possible misuse of resources.	1] Use strong identity verification techniques, such as digital certificates. 2] To keep an eye out for irregularities, use intrusion detection systems.

Analyzing And Comparing Defensive Techniques For Vanet Security

Several solutions have been developed in recent years to address the security issues that VANETs face. This section provides a comprehensive review and discussion of several countermeasures that have recently been presented in the literature. The discussion is particularly more on solutions that are appropriate to the previously identified security threats, offering data on their effectiveness and applicability in order to stay coherent and concentrated.

Sophisticated Defenses Against DoS Attacks

Table 5. Defenses against DoS Attacks

Proposed Approach	Description	Mechanism	Advantages	Limitations
OBU-Based Switching Options [29]	Four switching techniques are used to mitigate DoS attacks: numerous radio transceivers, frequency hopping spread spectrum, technology switching, and channel switching.	1] After evaluating harmful messages, OBUs choose a switching option. 2] The selected option spreads to nearby OBUs.	1] Enhances network accessibility in the event of an assault. 2] Gives you options when dealing with malicious activities.	1] Perhaps sophisticated hardware is needed. 2] In certain situations, switching may result in higher latency.
Attacked Packet Detection Algorithm (APDA) [26]	Uses an algorithm that integrates with RSUs to evaluate and validate messages based on velocity (rate of positional change) and frequency (packets per second) in order to detect DoS attempts.	1] A database of verified nodes is kept up to date by RSUs. 2] Early detection of attacked packets and tracking of hostile nodes.	1] Filters invalidate requests to cut down on overhead delays. 2] Increases the precision of detection and security.	1] Depends on RSUs, which reduces efficacy in regions where RSU deployment is sparse.
Request Response Detection Algorithm (RRDA) [30]	An APDA extension that grants or denies node access by comparing new network requests to a validated database.	1] Checks requests against the validated database that is currently in place.	1] Improves security and response speed. 2] Guarantees that only verified nodes are	1] Reliance on the APDA database may cause delays if it is huge or not updated in a timely manner.

		2] Rejects requests that aren't verified or handles those that are.	added to the network.	
Bloom Filter-Based IP-Chock Detection [31]	Uses Bloom filters to monitor and filter IP addresses using both proactive and reactive techniques in order to detect DoS assaults.	1] Collects and analyses traffic and IP data in stages. 2] Raises warnings and uses hash functions to find rogue IP addresses.	1] Economical in terms of compute, storage, and detection time. 2] Blends proactive and reactive tactics.	1] Only IP-based attack detection is available; other possible DoS attack vectors are not addressed.

Sophisticated Defenses Against Sybil Attacks:

Table 6. Defenses against Sybil Attack

Proposed Approach	Description	Mechanism	Advantages	Limitations
Signal Strength-Based Sybil Attack Detection [27]	This method confirms a node's location in VANETs by using the received signal strength (RSS). Nodes alternately act as witnesses, claimers, and verifiers. While the verifier gathers signal strength measurements from witnesses to determine the claimer's position, the claimer broadcasts its position.	1] Using the intensity of the received signal, nodes verify positions by acting as claimers, verifiers, or witnesses. To find suspicious nodes, the verifier compares the estimated position with the declared position.	1] Economical, effective in preventing Sybil attacks, and efficient in terms of detection time.	1] Exposes private information such node position and identification, which is a violation of privacy.
Footprint-Based Sybil Attack Detection [32]	This approach involves nodes gathering permitted communications from Road-Side Units (RSUs) at various points along the way. Each node's trajectory is formed by these messages. The method makes the assumption that each node's trajectory is distinct. Similar trajectories are identified as Sybil assaults if they are found. By not disclosing node identities, this technique prioritizes privacy.	1] In order to create a trajectory, nodes gather permitted messages from RSUs while traveling. Given that there is little chance of identical pathways for distinct nodes, similar trajectories are identified as Sybil attacks.	1] Effectively detects Sybil attacks while protecting node privacy.	1] The assumption that all RSUs are reliable can be exploited by attackers in the event that single RSU is compromised.
Neighbor Resemblance-Based Sybil Attack Detection [33]	Every so often, nodes send out beacon signals with information about their nearby nodes. Within communication range, nodes share these records with one another. Nodes are flagged as Sybil	1] To exchange information with nearby nodes, nodes send out beacon messages. By using com-	1] Communication overhead is decreased by the high detection rate, cheap computing cost, and	1] Needs more research to determine how successful it is in high-density situations like traffic bottlenecks.

	attackers if they identify identical groupings of surrounding nodes for longer than a predetermined threshold. This method takes advantage of an attacker's fictitious identities' shared neighbors.	mon fake identities among attackers, nodes that have identical nearby sets after a threshold period are identified as Sybil nodes.	lack of RSU infrastructure.	

Sophisticated Defenses Against Suppression/Alteration Attacks:

Table 7. Sophisticated Defences against Suppression/Alteration Attacks

Proposed Approach	Description	Mechanism	Advantages	Limitations
Protecting Location Privacy with Clustering Anonymization (PLPCA) [34]	In order to protect nodes' location privacy in VANETs from location-based services, the PLPCA technique turns vehicular networks into edge cluster graphs. Road and traffic information is obscured using a cloaking method, making location data indistinguishable within clusters.	1] Converts car networks into edge cluster graphs and uses cloaking algorithms using privacy metrics like l-diversity and K-Anonymity.	1] Maintains a high degree of location privacy by successfully concealing traffic and road information.	1] The cloaking and graph transformation operations could result in additional computing overhead.
Lightweight and Efficient Strong Privacy Preserving (LESPP) [35]	The purpose of the privacy-preserving LESPP method is to protect vehicle communications on VANETs. It is effective for real-time applications because it uses lightweight cryptographic algorithms for message signing and verification, generates pseudo identities, and ensures conditional traceability and privacy preservation.	1] Makes use of lightweight message authentication code (MAC) regeneration for verification, symmetric encryption for message signing, and pseudo identities.	1] Minimizes communication overhead, lowers computing costs, and protects privacy by limiting identity exposure to those who are permitted.	1] Depends on reliable authorities; the privacy and traceability features may be compromised if these organizations are compromised.

Conclusion

At the forefront of innovative research, VANETs promise safer and more intelligent mobility in the future. VANETs can completely transform current transportation systems by increasing passenger comfort, road safety, and traffic efficiency. However, these networks face several obstacles and are susceptible to various security risks, which prevents their widespread adoption despite their vital role in protecting lives. This essay delves into the basics of VANET technology, including its structure, major obstacles, and security requirements. In addition to a detailed summary of the many attacks that target VANETs, an analysis of how these risks compromise essential security requirements is presented. The study further looks into several remedies that try to mitigate such risks, hence giving insight on how to build stronger VANETs against future threats. This research paper would serve as a great tool for readers and researchers who are interested in the security of VANET and opens a door to even more durable and resilient vehicular networks by letting light into all important factors of security as well as making helpful recommendations. Through this contribution, the work stimulates innovation within the domain of intelligent transportation systems and brings forward a giant step toward developing robust and secure architectures for VANETs.

References

[1] Firooz, M.H. and Roy, S. (2012) Collaborative Downloading in VANET Using Network Coding.

Proceedings of IEEE International Conference on Communications (ICC), Ottawa, 10-15 June 2012, 4584-4588.

[2] Samara, G., Al-Salihy, W. and Sures, R. (2010) Security Analysis of Vehicular Ad Hoc Nerworks (VANET). Proceedings of Second International Conference on Network Applications Protocols and Services (NETAPPS), IEEE, Kedah, 22-23 September 2010, 55-60. https://doi.org/10.1109/netapps.2010.17.

[3] World Health Organization (WHO) http://apps.who.int/gho/data/node.main.A995

[4] Raya, M., Papadimitratos, P. and Hubaux, J.P. (2006) Securing Vehicular Communications. IEEE Wireless Communications, 13, 8-15. https://doi.org/10.1109/WC-M.2006.250352.

[5] Al-Raba'nah, Y. and Samara, G. (2015) Security Issues in Vehicular Ad Hoc Networks (VANET): A Survey. International Journal of Sciences & Applied Research (IJSAR), 2, 50-55.

[6] Srikanth Kavuri. (2023). Self-Healing Test Automation Framework Using Autonomous ML Agents for Real-Time Test Maintenance and Failure Recovery. International Journal of Intelligent Systems and Applications in Engineering, 11(4), 1089–1098.

[7] Al-Sultan, S., Al-Doori, M.M., Al-Bayatti, A.H. and Zedan, H. (2014) A Comprehensive Survey on Vehicular Ad Hoc Network. Journal of Network and Computer Applications, 37, 380-392. https://doi.org/10.1016/j.jnca.2013.02.036.

[8] Eze, E.C., Zhang, S.J., Liu, E.J. and Eze, J.C. (2016) Advances in Vehicular Ad-Hoc Networks (VANETs): Challenges and Road-Map for Future Development. International Journal of Automation and Computing, 13, 1-18. https://doi.org/10.1007/s11633-015-0913-y.

[9] Engoulou, R.G., Bellaïche, M., Pierre, S. and Quintero, A. (2014) VANET Security Surveys. Computer Communications, 44, 1-13. https://doi.org/10.1016/j.comcom.2014.02.020

[10] Deshpande, S.G. (2013) Classification of Security attack in Vehicular Ad hoc network: A survey. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 2, 371-377.

[11] Zeadally, S., Hunt, R., Chen, Y.S., Irwin, A. and Hassan, A. (2012) Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges. Telecommunication Systems, 50, 217-241. https://doi.org/10.1007/s11235-010-9400-5

[12] La Vinh, H. and Cavalli, A.R. (2014) Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey. International Journal on Ad Hoc Networking Systems (IJANS), 4, 1-20. https://doi.org/10.5121/ijans.2014.4201

[13] CAR 2 CAR Communication Consortium Manifesto (C2C-CC). https://www.car-2-car.org/index.php?id=31

[14] Alam, M., Ferreira, J. and Fonseca, J. (2016) Introduction to Intelligent Transportation Systems. In: Alam, M., Ferreira, J. and Fonseca, J., Eds., Intelligent Transportation Systems, Springer International Publishing, Switzerland, 1-17. https://doi.org/10.1007/978-3-319-28183-4_1

[15] Mere, M.N., Ben-Othman, J. and Hamdi, M. (2014) Survey on VANET Security Challenges and Possible Cryptographic Solutions. Vehicular Communications, 1, 53-66. https://doi.org/10.1016/j.vehcom.2014.05.001

[16] Gillani, S., Shahzad, F., Qayyum, A. and Mehmood, R. (2013) A Survey on Security in Vehicular Ad Hoc Networks. In: Berbineau, M., Ed., Communication Technologies for Vehicles, Springer, Berlin Heidelberg, 59-74. https://doi.org/10.1007/978-3-642-37974-1_5

[17] Mokhtar, B. and Azab, M. (2015) Survey on Security Issues in Vehicular Ad Hoc Net-Works. Alexandria Engineering Journal, 54, 1115-1126. https://doi.org/10.1016/j.aej.2015.07.011

[18] Qin, B., Wu, Q., Domingo-Ferrer, J. and Zhang, L. (2011) Preserving Security and Privacy in Large-Scale VANETs. In: Qing, S., Susilo, W., Wang, G. and Liu, D., Eds., Information and Communications Security, Springer, Berlin Heidelberg, 121-135. https://doi.org/10.1007/978-3-642-25243-3_10

[19] World Health Organization (WHO). http://www.who.int/features/2004/road_safety/en/

[20] Razzaque, M.A., Salehi, A. and Cheraghi, S.M. (2013) Security and Privacy in Vehicular Ad-Hoc Networks: Survey and the Road Ahead. In: Khan, S. and Khan Pathan, A.-S., Eds., Wireless Networks and Security, Springer, Berlin Heidelberg, 107-132. https://doi.org/10.1007/978-3-642-36169-2_4

[21] Toor, Y., Muhlethaler, P., Laouiti, A. and De La Fortelle, A. (2008) Vehicle ad Hoc Networks: Applications and Related Technical Issues. IEEE Communications Surveys & Tutorials, 10, 74-88. https://doi.org/10.1109/COMST.2008.4625806

[22] Raya, M. and Hubaux, J.P. (2007) Securing Vehicular Ad Hoc Networks. Journal of Computer Security, 15, 39-68. https://doi.org/10.3233/jcs-2007-15103

[23] Mejri, M.N. and Hamdi, M. (2015) Recent Advances in Cryptographic Solutions for Vehicular Networks. IEEE Proceedings of International Symposium on Networks, Computers and Communications (ISNCC), Hammamet, 13-15 May 2015, 1-7.

[24] Kaushik, S.S. (2013) Review of Different Approaches for Privacy Scheme in VANETs. International Journal of Advances in Engineering & Technology (IJAET), 5, 356-363.

[25] Kim, Y. and Kim, I. (2013) Security Issues in Vehicular Networks. IEEE Proceedings of the International Conference on Information Networking (ICOIN), Bangkok, 28-30 January 2013, 468-472.

[26] Roselin, M.S., Maheshwari, M. and Thamaraiselvan, M. (2013) Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA). IEEE Proceedings ofInternational Conference on Information Communication and Embedded Systems (ICICES), Chennai, 21-22 February 2013, 237-240.

[27] Yu, B., Xu, C.Z. and Xiao, B. (2013) Detecting Sybil Attacks in VANETs. Journal of Parallel and Distributed Computing, 73, 746-756. https://doi.org/10.1016/j.jpdc.2013.02.001.

[28] Fuentes, J.M.D., González-Tablas, A.I. and Ribagorda, A. (2010) Overview of Security Issues in Vehicular Ad Hoc Networks. In: Cruz-Cunha, M.M. and Moreira, F., Eds., Handbook of Research on Mobility and Computing, Hershey, New York.

[29] Hasbullah, H., Soomro, I.A. and Manan, J.A. (2010) Denial of Service (Dos) Attack and Its Possible Solutions in VANET. International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, 4, 813-817.

[30] Gandhi, U.D. and Keerthana, R.M. (2014) Request Response Detection Algorithm for Detecting DOS Attack in VANET. IEEE Proceedings of International Conference on Optimization, Reliabilty, and In-Formation Technology (ICROIT), Faridabad, 6-8 February 2014, 192-194.

[31] Verma, K. and Hasbullah, H. (2014) IP-CHOCK (Filter)-Based Detection Scheme for Denial of Service (DOS) Attacks in VANET. IEEE Proceedings of International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, 3-5 June 2014, 1-6. https://doi.org/10.1109/ic-coins.2014.6868377

[32] Chang, S., Qi, Y., Zhu, H., Zhao, J. and Shen, X. (2012) Footprint: Detecting Sybil Attacks in Urban Vehicular Networks. IEEE Transactions on Parallel and Distributed Systems, 23, 1103-1114. https://doi.org/10.1109/tpds.2011.263

[33] Grover, J., Laxmi, V. and Gaur, M.S. (2014) Sybil Attack Detection in VANET Using Neighboring Vehicles. International Journal of Security and Networks, 9, 222-233. https://doi.org/10.1504/IJSN.2014.066178

[34] Ying, B. and Makrakis, D. (2014) Protecting Location Privacy with Clustering Anonymization in Vehicular Networks. Proceedings of IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, and 27 April-2 May 2014, 305-310.

[35] Wang, M., Liu, D., Zhu, L., Xu, Y. and Wang, F. (2016) LESPP: Lightweight and Efficient Strong Privacy Preserving Authentication Scheme for Secure VANET Communication. Computing, 98, 685-708.

[36] Khan, U., Agrawal, S. and Silakari, S. (2014) Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks. Proceedings the International Conference on Information and Communication Technologies (ICICT), Kochi, 3-5 December 2014, 965-972.

[37] Sheikh, M.S., Liang, J.: A comprehensive survey on VANET security services in traffic management system. Hindawi Wirel. Commun. Mob. Comput. (2019). https://doi.org/10.

[38] 1155/2423915