JOURNAL OF EDUCATION: RABINDRA BHARATI UNIVERSITY
ISSN : 0972-7175

A REVIEW ON VANET SECURITY, THREATS AND DESIGNS

Reena G.Bhati Department of Computer Science Tilak Maharashtra Vidyapeeth, Pune, India
reena4bhati@gmail.com

Abstract:
Vehicular Ad hoc Network (VANET) is a new type of Mobile Ad hoc Network (MANET) which refer to a set of smart vehicles used on the road. Based on wireless Local Area Network (LAN) technology, these cars deliver communication services to each other and to Road Side Infrastructure (RSU). Road accidents and related sequences are becoming more common over the world, necessitating the development of methods that include road safety and regulation. Even vehicles with short-range networks can successfully use VANET to construct an intelligent transportation system (ITS). Travelers will benefit from VANET since it will improve road safety and convenience. However, such technology is already subject to a number of vulnerabilities, posing a slew of security issues that must be addressed before VANET technology can be used realistically and securely. The key advantages of VANETs are such that they improve traffic safety and vehicle protection while also safeguarding drivers' privacy from malicious attacks. Because the information communicated is dispersed in a freely accessible environment, safety is among the most important challenges associated to VANETs. This paper offers a summary of security concerns and the challenges they provide. The various types of VANET applications are discussed, as well as certain security needs, threats, and designs for addressing the security issue.

Introduction:

MANET has a subset called VANET. Each node in a VANET is a vehicle or RSU (Road Side Unit) that may freely travel within the subnet while remaining connected. Each node interacts with other nodes either in a single hop or multiple hop fashion. Drivers can choose between safe and non-safe services provided by VANET. Each node connects with the rest of the network. Via one or more hops. VANET offers two types of services to drivers: safe and non-safe.

Vehicular Ad hoc networks are made up of network nodes (sensor-equipped automobiles), stationary equipment (Road Side Access Point), and mobile networks that allow them to communicate with one another. Driving safety is the most critical service supplied by these networks. Road accidents claim the lives of around 1.3 million people worldwide, with another 20-50 million injured. Traffic collisions were ranked as the 9th biggest cause of death [1]. According to one study [2], 60 percent of incidents can be stopped if the motorist receives the alert even quarter a minute before the collision. This significant rise in car accidents can be mitigated by using cutting-edge technology to provide real-time information to drivers regarding vehicle health parameters, road conditions, traffic bottlenecks, and weather forecasting. With the growth of Intelligent Transportation Systems (ITS), the internet of vehicles, also known as the (IoV),[3] the basic of interaction required communicating data on crises and changing traffic patterns have been enhanced.

According to a recent estimate by the IoT tracker service, the connected auto industry will grow by an additional 270 percent by 2022, encompassing more than 125 million vehicles [4]. This significantly increases the scale and complexity of currently operational vehicle ad hoc networks, often known as VANETs. Aside from operational problems, the rapid growth of vehicle connectivity has resulted in major security and data confidentiality concerns about the development and extension of VANETs design.

VANET technology has a variety of benefits, including a decrease in the number of accidents, a more joyful driving and travelling experience, and the simplicity of different payment methods for tolls,

parking, and gasoline, among others. Users on the road use a variety of applications for quality and reliability, traffic control, navigation system, caution, comfort, maintenance, musical exchange, and network gaming [5].

These applications send and receive messages including such emergency information transmission, traffic collisions, and road surface warnings to improve traffic safety and travel efficiency. These applications necessitate node-to-node data transfer. . The message's content can influence driving behavior. This may modify the network topology, and security may be jeopardized if a hostile user modifies the message [6]. A few possible attacks include Denial-of-Service (DoS) attacks, in-transit traffic malicious attacks, impersonation, and hardware tampering, as well as causing traffic jams, spreading bogus information, cheating positioning information, disclosing IDs, replaying, masquerading, or forging data, violating privacy, or causing wormholes[7].

Literature Survey:

This section contains a research report on the most recent prospective options for protecting the VANET network. This paper's [8] goal is to provide a summary of security issues and the challenges they provide. There includes discussion of the many types of VANET applications, as well as some specific security, hazards, and designs to deal with the security challenge.

This article [9] provides a brief summary of all the most challenging VANET challenges, and even some well-known solutions. Later, author discussed the latest research and our long-term goals. By reading this article, researchers and academics will gain a better grasp of VANET and existing research in this new area.

This article [10] focuses on examining important VANET threats and discussing feasible solutions, with a focus on Block chain Technology-based solutions. This study [11] is unique in that it investigates privacy protection in VANETs from the aspect of safety and dependability. It also presents a critical evaluation of numerous attacks, identity fraud, manipulation, and other strategies employed in cutting-edge VANET solutions for location privacy protection.

Author [12] study examines the state of the art in vehicular trust management, focusing on the variables studied such as weight quantification, threshold quantification, misbehavior detection, and so on. Furthermore, an overall IoV architecture, constituents under the notion of trust, and IoV-related assaults have been provided, as well as open research problems in the subject domain.

Challenges of VANET

Authentication: Authentication is required for all messages sent from one vehicle to another. Each car in the network will be authenticated by the central authority [13].

Security and trust: Security issues are occasionally addressed in travel applications, particularly in terms of the passenger's comfort, and this is due to the fact that everyone works together. Customers will not embrace warning systems if privacy & safety are not assured. Among the most important concerns in VANET security is trust and reliable software. Security maps for VANET algorithms might also cause message delivery delays [14].

Environmental impact: VANETs use electromagnetic radiation for connectivity. These waves have an impact on the ecosystem. As a result, the ecological damage of deploying VANET must be examined [15].

Reliability: The information you get in interaction should be accurate and complete. Periodic system verification is carried out to ensure that that factually incorrect material is removed.

Availability: These systems deal with sensitive information, therefore it should be accessible to all authenticated persons quickly and simply**.**

Volatility: The time it takes for two nodes to link can fluctuate, and also an event like this may only happen once. Because each vehicle is mobile, the connections between them would be lost and might remain thus for a short amount of time within a few wireless hops [16, 17].

ATTACKS IN VANET

Denial of service (DOS) attacks: Among the most popular VANET attacks is DoS. Vehicles attacked in the VANET network, either internally or outside [18]. The attacker essentially precludes any feasible kind of activity by blocking vehicle connection. This assault, called as a distributed denial of service, can be carried out by a large number of attackers at the same time (DDoS) [19].

Jamming attack: A heavily generated signal of an equivalent frequency disrupts the VANET channel of communication. It is the most dangerous security application assault because a genuine security warning was not followed. If the jamming attempt is effective, the valuable signal will be disrupted at the same moment as an occurrence [20].

Black hole attack: It's one of the VANET's security threats. The attacking node refuses to take part in the attack and even drops the data packet [21]. As a result, this form of attack has a greater impact on the vehicle network.

Gray hole attack: It occurs when autonomous cars seek to send certain data packets while removing another without being traced [22].

Spamming: Spam assaults are aimed at consuming bandwidth and delaying transmission. Users are uninterested in spam messages, which are similar to advertising messages [23].

Tunneling attack: This is similar to the wormhole assault. Using the same connection, starting a private chat on a channel known as the tunnel. The attacker connected to the VANETs from two different locations. As a result, nodes that are far away can connect as neighbors [21].

Masquerading: One attacker is defined in this attack by some other vehicle's fake identity and appearance as a valid node. As all cars interact, the attacker imitates a man in the centre middle and spoofs them as the second vehicle. This is also a calculated attempt to influence the outcome [24].

Replay attack: By repeatedly giving authentic data and inserting signals and answers obtained by the VANET network, the hacker seeks to repeat or postpone false transmission. It can be difficult for traffic police to identify automobiles in the event of an accident [25].

Table 1.Summary of various attacks in VANET

Property	**Possible attack**	**Attack effects**	**Ease of attack**
Authentication	Dos	Users are unable to connect with one another due to a denial of channel service in the network.	High
	Replay attack	Every packet was received by the rogue node, which transmitted them to all nodes at various times.	Medium
	Message spoofing	The inaccurate location information has led you in the wrong way.	Medium
	Bogus information	Attackers disseminate false information to all other vehicles at the same time, as well as across all wireless networks.	Medium
	Sybil attack	Multiple identities can be assumed by a single compromised node.	High
Confidentiality	Eavesdropping	Take the car's owner's (or driver's) critical and personal information.	High

	Blackhole & Grey hole	Instead of spreading across the network, the information has been prevented.	Moderate
	Man- in the middle	It occurs when a rogue node disrupts the relay (or) tampers with the genuine messages sent between legitimate nodes.	High
	Timing attacks	The process of creating real-time material has evolved.	High
	Injection attack	The attackers provide incorrect data to the automobile bus system.	High
	Location tracking	For tracking attacks, attackers can gather and change location tracking data.	High
	Brute force	The attacker cracks the key in cryptography with the help of the approach.	High
	Id disclosure	Obtain the vehicle's ID and follow the vehicle's path.	High
Availability	Flooding attack	A large number of packets fall on a node, causing it to become unavailable.	High
	Jamming attack	The attacker jams the channel with the jammer signal.	Medium
	Amalgamation attacks	A group of rogue nodes banded together to launch harmful attacks such as isolating the legal node.	Low
Integrity	Alter the Real message	The information obtained by the compromised node is modified and distributed by the compromised node.	High
	Forgery attacks	The hacked node alters the correct time and location.	High
	Illusion attack	The exploited node deceives a car's sensors and sends neighbors false traffic warning alerts.	High
	Masquerading	The attackers steal the authentic identity in order to get sensitive information.	High
	Broadcast tampering	The attackers exploit the car maintenance time to interfere with the vehicle's hardware.	High

Application:

The emergence of smart automobiles opens up a plethora of new potential VANET applications. These applications are divided into two categories: Intelligent Transportation Applications (ITA) and Comfort Applications (CA) [7]. The ITA is organized into two subgroups: Transport Safety Applications (TSA) and Transport Efficiency Applications (TEA) (TEA). The primary goal of ITA is to avoid and prevent traffic accidents [26]. TSAs are individuals who deal with emergency circumstances, whereas TEAs are

more concerned with avoidance. Comfort Applications, whose objective is to make the driving experience even better for both travelers, will be utilized largely for news and entertainment [27].
Eight applications were recognized by the Vehicle Safety Communication (VSC) Consortium, which was founded by the government and the private sector [28]: (1) Traffic Signal Violation Warning: The purpose of Traffic Signal Violation Warning is to alert drivers when they are going to break a traffic signal that allows a halt (a red light, a flashing red light, a stop sign, a railroad crossing, etc.), and (2) Curve Speed Warnings: RSUs send out alerts to approaching vehicles in this application. Curve position, curve speed limits, curvature level, information about the road banks, and road surface conditions are all examples of information that can be transmitted. As a result, drivers can be alerted to possible hazards ahead of time [29]. (3) Emergency Electronic Brake Lights: The EEBL app is part of a Collaborative Adaptive Cruise Control (CACC) system that leverages network data to immediately brake the automobile if the driver does not respond to the warning [30]. (4) Pre-Crash Warning: If a collision is necessary, the car involved will send a pre-crash warning signal to other vehicles, giving them more time to respond and potentially avoiding a fatal pileup [31]. (5) Cooperative Forward Collision Warning: It developed to help drivers prevent or lessen rear-end crashes with vehicles front by alerting them to a potential collision. (6) Left Turn Assistant: It provides real-time traffic information to help drivers make a left turn at a signalized intersection where there is no left-turn arrow. . (7) Lane Change Warning: This software alerts the driver if a planned lane change might result in a collision with another car. (8) Stop Sign Movement Assistance: This programmer issues a caution to a vehicle approaching an intersection after coming to a complete stop at a stop sign.
The TEA seems to be more intriguing because of its involvement in accident prevention. The most important application in this division is traffic control. This application's special scenario could be traffic surveillance programs, in which nodes are alerted about the traffic problem forward. They can then offer an alternative route depending on the info they've gathered [32]. Furthermore, the on-the-fly real - time traffic analysis will aid in the avoidance and reduction of road congestion. If a node becomes aware of a line ahead or a specific scenario that may generate congestion, it will adjust the route if possible. Several other applications, such as on-board guidance, location-based solutions within the vehicle, traffic violation applications, and cooperative driving for VANETs, might be anticipated in smart vehicles and VANETs [33, 34].
The goal of comfort programs, which are sometimes known as infotainment apps, is to improve the user's driving experience. There are numerous applications that can be used. The goal is to have a connection that allows access to all online applications, including music, streaming video, email, games, and adverts. Other comfort programs, on the other hand, can be used even if you don't have access to the Internet. These apps provide weather data, interactive communications, gaming networks, information about hotels, gas stations, restaurants, payment systems, and other location-based services. Drivers who have mechanical emergencies can use maintenance apps to get remote aid from a technician service through a wireless diagnosis and intervention [7, 35].

Discussion:
Table 2. A Review on Security Aspects in VANET

Author	**Objective**	**Drawbacks**
R.Waghmode et al [36]	To keep your vehicle safe, use group-based V2V communication. This approach can be used to	This approach entails a one-time group authentication process, after which only V2V communication is conducted

	track down a malicious vehicle that sends out a bogus message. System has improved, as has the cost of calculation.	within the group using the symmetric key mechanism.
M. Raya et al [37]	Various Revocation protocols were discussed (RTPD, RCCRL, and DRP). The LEAVE protocol is used to secure the system's functioning.MDS can be used to identify faulty nodes.	Only monitoring is used in these strategies. Not suitable for a reputation system. Bloom filters have a high rate of false positives.
Zhang et al [38]	The use of a group signature is a good idea.	Mobility keeps a group alive and protects it from becoming stagnant.
Kenneth et al. [39]	CRLs are distributed in an epidemic way using cars. Increases the speed of dissemination.	Constraints in terms of bandwidth and hardware. Performs only RSU distribution points-based techniques.
Jasson et al. [40]	For exchanging CRL updates, a simple approach was used. Reduction in the number of certificates revoked.	Due to the large number of cars, CRLs are long. In a high-traffic area, performance is poor.
Zhang et al [41]	To achieve security principles, signcryption and group signature mechanisms were discussed. Physical road limits can be exploited efficiently and correctly dispersed RSUs using this protocol particular feature such as mobility.	If one of the RSUs fails, the network's operation is disrupted. The performance rate falls as the load increases.

Conclusion:

VANET requires a safe and protected atmosphere because it is a means for sharing safety information. Due to its extremely dynamic nature, wireless method of communication, and regularly changing topology, VANET presents a large attack surface. Furthermore, VANET's distinct technique raises new security risks, such as location finding, illegal tracking, and jamming. Because of its enhanced capabilities of delivering safe, secure, and comfortable driving, VANET is now widely used. VANET, its characteristics, and the necessity for VANET security are all hot subjects in the current context. On this work, we conducted a literature analysis on various forms of assaults, their applications, and different sorts of attackers in the VANET.

References:

[1] Road Crash Statistics- Association for Safe International Road Travel. Available: http://asirt.org/initiatives/informing-road-users/road-safety-facts/roadcrash-statistics

[2] Maxim Raya et al., “The Security of Vehicular Ad Hoc Networks”, SASN’05, Nov 7 2005, Alexandria, Virginia, USA, pp. 11-21
[3] Alam, M.; Ferreira, J.; Fonseca, J. Introduction to intelligent transportation systems. In Intelligent Transportation Systems; Springer: Berlin/Heidelberg, Germany, 2016; pp. 1–17.
[4] Bhatia, H. 125 Million+ Connected Cars Shipments by 2022; 5G Cars by 2020; Available online: https://www.counterpointresearch.
com/125-million-connected-cars-shipments-2022-5g-cars-2020/ (accessed on 15 February 2020).
[5] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, A. Hassan, Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges, Springer Science, 2010.
[6] T. Leinmuller, R.K. Schmidt, E. Schoch, A. Held, G. Schafer, Modeling roadside attacker behavior in VANETs, in: GLOBECOM Workshops, IEEE, New Orleans, LO, 2008, pp. 1–10.
[7] Y. Wang, F. Li, Vehicular Ad Hoc Networks, Springer-Verlag, London, 2009.
[8] Richard Gilles Engoulou, Martine Bellaïche, Samuel Pierre, Alejandro Quintero,VANET security surveys, Computer Communications, Volume 44, 2014, Pages 1-13, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2014.02.020.
[9] Hemalatha, R. "A survey: security challenges of VANET and their current solution." *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 12.2 (2021): 1239-1244.
[10] N. Ravi and C. Kapoor, "Block Chain Techniques to Detect Attacks on VANET System: A Survey," 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), 2021, pp. 160-165, doi: 10.1109/ICIEM51511.2021.9445311.
[11] Khan, Shawal, et al. "Security Challenges of Location Privacy in VANETs and State-of-The Art Solutions: A Survey." Future Internet 13.4 (2021): 96.
[12] Siddiqui, S.A.; Mahmood, A.; Sheng, Q.Z.; Suzuki, H.; Ni, W. A Survey of Trust Management in the Internet of Vehicles. Electronics 2021, 10, 2223. https://doi.org/10.3390
[13] S. K. Bhoi and P. M. Khilar, "Vehicular communication: a survey," IET networks, vol. 3, no. 3, pp. 204-217, 2013, doi: 10.1049/iet-net.2013.0065.
[14] A. Quyoom, A. A. Mir, and A. Sarwar, "Security Attacks and Challenges of VANETs: A Literature Survey," Journal of Multimedia Information System, vol. 7, no. 1, pp. 45-54, 2020, doi: 10.33851/JMIS.2020.7.1.45.
[15] M. M. Hamdi, L. Audah, S. A. Rashid, and S. Alani, "VANET-based traffic monitoring and incident detection system: A review," International Journal of Electrical & Computer Engineering (2088-8708), vol. 11, no. 4, 2021, doi: 10.11591/ijece.v11i4.pp3193-3200.
[16] M. Raya, P. Papadimitratos, J.P. Hubaux, Securing vehicular communications, IEEE Wirel. Commun. 13 (2006) 8–15.
[17] B. Parno, A. Perrig, Challenges in securing vehicular networks, in: Workshop on Hot Topics in Networks (HotNets-IV), 2005.
[18] A. Daeinabi and A. G. Rahbar, "Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks," Multimedia tools and applications, vol. 66, no. 2, pp. 325-338, 2013, doi: 10.1007/s11042-011-0789-y.
[19] A. F. Femi, "Perception of performance appraisal and workers’ performance in Wema Bank Headquarters, Lagos," Global Journal of Arts, Humanities and Social Sciences, vol. 1, no. 4, pp. 89-101, 2013.
[20] A. Y. Dak, S. Yahya, and M. Kassim, "A literature survey on security challenges in VANETs," International Journal of Computer Theory and Engineering, vol. 4, no. 6, p. 1007, 2012.
[21] 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, doi: 10.1007/s11235-010-9400-5.
[22] M. S. Sheikh, J. Liang, and W. Wang, "A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets)," Sensors, vol. 19, no. 16, p. 3589, 2019.

[23] C. Sun, J. Liu, X. Xu, and J. Ma, "A privacy-preserving mutual authentication resisting DoS attacks in VANETs," IEEE Access, vol. 5, pp. 24012-24022, 2017, doi: 10.1109/ACCESS.2017.2768499.
[24] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Review of prevention schemes for modification attack in vehicular ad hoc networks," International Journal of Engineering and Management Research, vol. 10, 2020, doi: 10.2139/ssrn.3662927.
[25] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in Workshop on hot topics in networks (HotNets-IV), 2005, pp. 1-6: Maryland, USA.
[26] Yasser Toor, P. Muhlethaler, A. Laouiti, A.D.L. Fortelle, Vehicle ad hoc networks: applications and related technical issues, IEEE Commun. 10 (2008).
[27] H. Hartenstein, Kenneth P. Laberteaux, A tutorial survey on vehicular ad hoc networks, IEEE Commun. Mag. (2008).
[28] Identify intelligent vehicle safety applications enabled by DSRC, US National Highway Traffic Safety Administration 2005.
[29] H.T. Cheng, H. Shan, W. Zhuang, Infotainment and road safety service support in vehicular networking: from a communication perspective, Mech. Syst. Signal Process. (2010).
[30] M. Segata, R. Lo Cigno, Automatic emergency braking: Realistic analysis of car dynamics and network performance, IEEE T. Veh. Technol. 62 (9) (2013) 4150–4161.
[31] K.V.N. Kavitha, A. Bagubali, L. Shalini, V2V wireless communication protocol for rear-end collision avoidance on highways with stringent propagation delay, in: International Conference on Advances in Recent Technologies in Communication and Computing, ARTCom '09, 2009, pp. 661–663.
[32] K. Dresner, P. Stone, A multiagent approach to autonomous intersection management, J. Artif. Int. Res. 31 (2008) 591–656.
[33] G. Jyoti, M.S. Gaur, in: S. Auerbach (Ed.), Security of Self-organizing Networks MANET, WSN, WMN, VANET, CRC Press, 2010.
[34] V.S. Yadav, S. Misra, M. Afaque, Security of Wireless and Self-Organizing Networks: Security in Vehicular Ad Hoc Networks, CRC Press, 2010, pp. 227–250.
[35] A. Stampoulis, Z. Chai, A Survey of Security in Vehicular Networks, Project CPSC 534, 2007.
[36] R. Waghmode, R. Gonsalve, " Security enhancement in group based authentication for VANET",International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), IEEE, January 2017.
[37] M Raya, P Papadimitratos, JP Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, Vol 13, October 2006.
[38] Vengatesan, K., Kumar, A., Subandh, T., Vincent, R., Sayyad, S., Singhal, A., & Wani, S. (2019). Secure Data Transmission Through Steganography with Blowfish Algorithm. In International Conference on Emerging Current Trends in Computing and Expert Technology (pp. 568–575).
[39] X Lin, R Lu, C Zhang, H Zhu, PH Ho, "Security in Vehicular Ad Hoc Networks", IEEE Communications Magazine, April 2008.
[40] I Aad, JP Hubaux, EW Knightly, "Impact of Denial of Service Attacks on Ad Hoc Networks", Networking, IEEE/ ACM Transactions on Volume 16, August, 2008.
[41] W Ren, K Ren, W Lou, Y Zhang, "Efficient user revocation for privacy-aware PKI", In Proceedings of the 5th International ICST Conference, 2008.