ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

SECURITY ANALYSIS OF VEHICULAR AD HOC NETWORKS

Dr Vidhya PM
vidhya@sngce.ac.in
Associate Professor, Dept. of CSE, Sree Narayana Gurukulam College of Engineering,
Kadayiruppu, Kerala, India.

ABSTRACT
Vehicular Ad Hoc Network (VANET) is receiving more attention today, however the available methods to make VANET secure and to defend the network against threats and attacks are still insufficient. This intelligent vehicle communication with one another and the roadside unit (RSU) create safer roadways, improve driving efficiency, and provide security against intruders. Since VANET messages are transmitted through open wireless channels, security is its most pressing problem. VANET is subject to numerous attacks. In this work, many VANET security concerns and issues have been, addressed, and solutions have been proposed to address these issues and challenges.
Key Words: Wireless Technologies, Vehicle communication, Intelligent transport system

INTRODUCTION
A VANET is an ad hoc network which connects various moving vehicle and other connecting devices so they can communicate with one another and share relevant information. The vehicle and other equipment act as node in the network at the same time, forming a tiny network. All other nodes receive the information that each node possesses. Similar to this, after sending their own set of data, each node receives the data being sent by the other nodes. After gathering all of this data, nodes work to extract information that is useful from it and retransmit it to other devices [4]. Now new vehicles are being introduced to the market, they come with on-board sensor that makes it simple for the vehicles to join and merge in the network and profit from VANET. Vehicular Ad-hoc Networks are a part of the Intelligent Transportation Systems [26]. (ITS). Network topology, unrestricted network size, frequent information interchange, unlimited power and storage, and on-board sensors are the major features of a VANET. There are three domains in the VANET architecture.

- Mobile domain: There are two components to the mobile domain. The first is the vehicle domain, which includes all continuously moving vehicles including buses, cars, trucks, and so forth. The second section is the mobile device domain, which includes all portable handy gadgets including PDAs, laptops, GPS, and smart phones, among others.
- Infrastructure domain: It has two parts as well. Traffic lights, poles, and other stationary roadside elements make up the roadside infrastructure domains. Central managing centres, like the traffic management centres and vehicle management centres, are included in the central infrastructure domains.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

- Generic domain: It consists of both private and public infrastructure. Generic domain includes various nodes, servers, and other computational resources that are used directly or indirectly by a VANET.

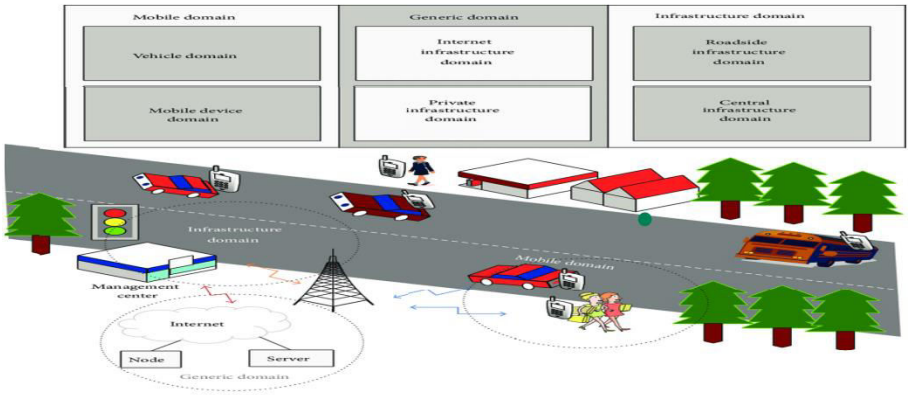

Figure 1 Vanet Architecture Domains

The efficient and effective use of the road by the users is a result of the data flow between the stationary and mobile resources [28]. Figure 1 shows the three components of the VANET's architecture domains. There are mainly three communication modes in VANET.

- Communication between vehicles: Vehicle or a group of vehicles interact and communicate with each another in a point-to-point manner. When driving with others, it works out to be really beneficial.
- Communication from vehicles to infrastructure: For the purpose of providing upload or download data to and from the vehicles, sufficient number of base station must be placed near to the roads and having a fixed infrastructure. A cluster is covered by each infrastructure access point.
- Communication between clusters: In VANETs, the networks are divided into autonomous groupings of vehicles called clusters. Communications between the clusters are made possible via the Base Station Manager Agent (BSMA). One cluster's BSMA can communicate with another cluster's BSMA.

The figure2 shows three modes of communications in VANET. Each vehicle can communicate with other vehicles using short radio signals DSRC (5.9 GHz), for range can reach 1 KM, and this communication is an Ad Hoc communication, meaning each connected node can move freely, no wires required; the routers used are called Road Side Unit (RSU), the number of vehicles in the world today exceeding 750 million [23], and these vehicles will need an authority to govern it.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

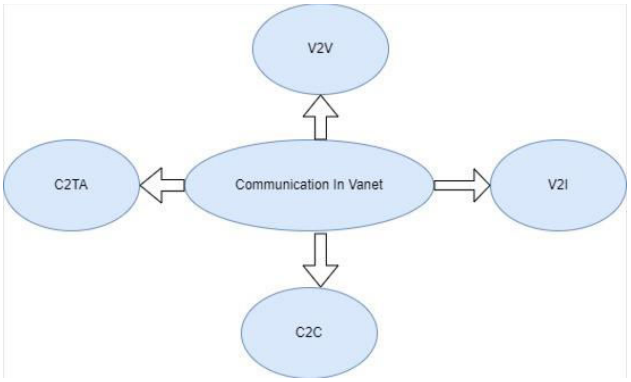

Figure 2 Vanet Communication Types

LITERATURE REVIEW

[11] Provides a short overview of VANET. VANET's system and communication architecture is discussed, as well as the several kinds of protocols that VANET employs also described VANET's application areas. By foreseeing and assisting drivers and other persons with regard to road safety and other crucial conditions, VANET, which is regarded as a different sort of Mobile Ad Hoc Networks, possesses the potential to influence decisions that could determine a person's life or death. The security and privacy features of VANET networks discussed in [6] are crucial to their need for robustness. A variety of VANET security issue and challenge has been examined.

VANET have largely captured today's interest, despite the fact that the present technologies to secure VANET and defend the network from attacks are still insufficient. In [2,] a variety of security challenges, demands, attacks, and attackers in VANET are discussed. The benefits and drawbacks of a few recent solutions to the security issues have also been examined. Since VANET messages are transmitted through open wireless channels, security is its most critical matter. [31] Suggests the use of the AATMS anti-attack trust management method in VANET to assess the reliability of vehicles. Vehicles on the VANET can interact with trusted vehicles and avoid malevolent vehicles with the use of AATMS. The Trust Rank algorithm, which is employed to prevent web spam, served as the primary inspiration for AATMS. Additionally calculated in this area are local and global trusts, which represent the relationships between vehicles' local and worldwide trusts. In order to determine the local trust of vehicles based on previous contacts, Bayesian inference is used first. Based on neighbourhood trust and a few other social characteristics, the authors choose a limited group of seed vehicles. The local trust connection structure of vehicles is used to assess the global trust of all vehicles after they have determined the reliable seed vehicles. The simulation results demonstrate that AATMS can successfully distinguish between reliable and unreliable vehicles in VANET even in the face of malicious attacks.

Security is becoming a bigger concern as intelligent transportation systems (ITS) evolve. In [18] a trust-based collaborative intrusion detection system (TBICDS) is proposed. In order to determine their previous pattern of network behaviour, each vehicle in the network keeps a score table of the other vehicles. The vehicles also collect real-time network data that may be analysed using a local IDS agent that has k-nearest-neighbor kNN nonlinear classifiers. Additionally,

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

vehicles can work with other nearby vehicles to update the score tables, which can then be used to anticipate the future and identify intruders in real-time.

The latest VANET approaches are summed up in [17] VANET security by tackling security challenges. The authors go over these potential dangers and strategies for identifying literature. The attack and their effect are finally identified and explained, and the response is discussed at once. Tasks, barriers, system architecture, and operation are different in VANETs compared to MANETs. RSUs and smart vehicles communicate using risky wireless technologies. They are predisposed to being threatened, which can result in dangerous situations. Security procedures are required to identify these VANET assaults due to the potential for negative effects. The taxonomy for authentication systems in VANET has been covered in full in [3]. The security, privacy, and scalability requirements have been compared with the authentication techniques. It has been debated how to develop authentication systems with low cost, low communication overhead, and minimal computing overhead using contemporary technologies like 5G, 5G-SDN, and Blockchain. Also described were the current difficulties with VANET authentication. The number of linked vehicles is anticipated to skyrocket, and with it, the volume of safety- and non-safety-related messages that could pose a security and privacy risk. VANET must provide an authentication mechanism to prevent the attack and protect user privacy in order to ensure safe communication.

[10] Discussed many security and privacy concerns that can arise in the next-generation VANET environment and also provides a basic solution for both problems. A group signature-based technique is also suggested as a solution to the VANET network's privacy issues. It frequently experiences numerous security challenges as a result of developments of the intelligent transportation systems. The authors describe PKI as the most prevalent and practical remedy for security issues.

The advantages of both group signature-based and pseudonym-based techniques are combined in a hybrid approach [21]. The strategy forbids vehicles from engaging in group management or requiring them to manage a list of certificates that have been revoked. In order to achieve conditional anonymity, the system makes use of effective and lightweight pseudonyms that are not only employed for message authentication but also act as a trapdoor. The authors' descriptions of several assault scenarios demonstrate how resistant the suggested strategy is to various security and privacy risks. To demonstrate the effectiveness of suggested techniques, they also offer a study of the computational and communication overhead. Moreover, run a comprehensive simulation to offer a thorough network performance study. The security requirements for VANETs lead to the competing design goals of maintaining member privacy while simultaneously ensuring non-repudiation because of their high speed, mobility, and exposure to the environment.

[5] Offers a group signature technique that has been altered to eliminate pairing procedures through the caching of computed data, while still upholding the crucial criterion of conditional privacy. In order to avoid creating keys that are only ever used once or infrequently, as well as to lessen the system's dual burdens of excessive key recalculation and key redistribution, this study also makes a case for abandoning perfect forward and backward secrecy in VANET schemes. [15] Describe the vehicular networks' communication patterns, it assesses and contrasts the answer with similar works. In comparison to similar schemes, our group signature system is

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

more effective and secure throughout both the signing and verification phases. [20] Uses identity-based group signatures (IBGS) to establish accountability in vehicle communications while protecting privacy, and to partition a large-scale VANET into manageable groups. No further certificate is needed because each party's publicly accessible identification serves as its public key. This effectively gets around traditional protocols' convoluted certificate management. We look into selfish verification strategy further in order to speed up message processing in VANET. In [8], an anonymous authentication technique (AAAS) for VANETs is proposed.
The authors in [30] present a novel authentication protocol scheme based on the concept of group signatures, by utilising the entire sub-tree method to achieve membership revocation, which guarantees forward security. The plan also uses a decentralised group model, which divides the entire domain of VANETs into smaller regions. Any vehicle must update its non-revoked token on a regular basis from the regional group manager who oversees the region where it resides.

Table 1 Comparison of related work On VANET

Related work	Advantages	Disadvantages
Vehicular public key infrastructure[25,6,26]	Secure the exchange of data between the network Provide confidentiality, integrity and authenticity of messages	Cannot ensure sender of public key is really who claims he is. Cannot preserve conditional privacy of drivers.
VPKI with Digital signature[27,28]	Provide the confidentiality, integrity, non-repudiation and authentication requirements.	Verification time is too long. Increases storage requirements as the size of message increases due to certificates and keys.
Identity based framework[11,12]	Does need to store public keys of all the vehicles reduce the storage. Also reduces impersonification attack.	If TTP gets compromised keys also gets compromised.
Certification Authority(CA)[28,3]	Much more scalable. Need to trust only on single Certification authority (CA).	Requires a public key Infrastructure. Cost of initial deployment increases when compared to public-key authentication
Group signature based scheme[13,5]	Allows member of any group to sign a message on behalf of a group which can be verified by a single group key (i.e. reduces storage of keys) Provides privacy of messages.	If a vehicle leaves a group or joins a new group the Trusted-Authority needs to compute whole group keys which puts extra burden on TA

[7] Covered in three parts with a focus on VANET security framework. The first gives a thorough review of the requirement, difficulty, and characteristic of VANET security. Certain needs should be taken into account to create a secure VANET infrastructure with effective party

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

communication. [16] In addition to presenting the communication architecture of VANETs and outlining the privacy and security concerns that must be resolved in order to make such networks safe to use in practice, this section gives a synopsis of most current state of VANETs'. It lists all security issues that are currently present in VANETs and categorises them from a cryptographic standpoint. It gathers research, examines the several cryptographic algorithms that have been independently proposed for VANETs, and assesses the effectiveness of the solutions.

[29] introduced an effective Conditional Privacy-Preserving authentication system (ECPB) for vehicle ad hoc networks based on group signature (VANETs). Despite the fact that group signatures are frequently employed in VANETs for security purposes, the existing group signature-based techniques have inferior verification efficiency due to greater computational delays during certificates revocation list checking and signature verification procedure. The costs associated with verifying the signatures will significantly drop if the CRL checks are neglected. Additionally, batch verification is supported by the technique. According to experimental investigation, the method is more efficient than the ones in use in terms of verification delay and average latency.

VANET Security Concerns

Denial of Service attack

It happens when a vehicle's resources are hijacked or the Vehicular Network's communication channel is jammed, preventing the delivery of vital information. If the driver must rely on the information provided by the programme, it also raises the risk to the driver. For example, if someone is malicious and wants to cause a huge pileup on the road, they can cause an accident and launch a DoS attack to stop the warning from being sent to the coming vehicles [24].

Message Suppression Attack

Such an attacker would want to conceal information about incidents involving his vehicle from registration and insurance authorities and avoid collision report to roadside access point. For instance, an attacker might suppress a congestion warning and use it later, forcing vehicles to wait in traffic because they won't receive the alert.

Fabrication Attack

By sending fake information into the network, an attacker can launch this attack. The information could be fraudulent or the transmitter could pose as someone else. This attack uses fake identities, certificates, messages, and warnings [19].

Alteration Attack

It occurs when an attacker modifies already available data. It involves postponing transmission of information, an earlier transmission replay, or changing the entry of the delivered data itself. For instance, when the route is clogged, an attacker could change a message indicating to other vehicles that the current path is clean.

Replay Attack

It occurs when attackers send previous messages again to exploit the context of the message at the time of transmission. Such an assault would be intended to confound law enforcement and perhaps hinder the identifications of automobiles in hit-and-run incident.

Sybil Attack

To warn other vehicle that there is a traffic jam up ahead and force them to take another way, the attacker generates a huge number of pseudonymous automobile and pretends or acts as though

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

they are more than a hundred vehicles. For instance, an attacker may behave and pretend to be 100 vehicles in order to get other cars on the road to take another route and let the road clear up.

Selfish Driver

The road can be made clear for it by a selfless driver informing other vehicle that there is traffic and that they should take another way,

Malicious Attacker

Through the usage of the applications accessible on the vehicular network, this type of attacker attempts to cause harm. These attackers frequently have predetermined targets in mind and have access to the network's resources [23]. A terrorist may issue a deceleration warning, for example, in order to create traffic before setting off a bomb.

Pranksters

Include disinterested individuals searching for security holes and hackers looking to get notoriety through their harm [19].

VANET Networks Challenges

Mobility

According to the basic Ad Hoc Networks theory each node in the network can move from one location to another within the coverage area. However, this mobility is still limited. For example, in Vehicular Ad Hoc Network, where node is moving quickly, vehicle may make connections with other vehicles they have never encountered before, but these connections may only last a few second as each vehicle proceeds in its own directions. These two vehicles may never cross paths again. Secure mobility is therefore a difficult issue.

Volatility

Communication between nodes can be very transient and may never arise again. Due to each car's great mobility and potential for travelling in the other direction, connections made by vehicles travelling outside the coverage region will be lost. Since vehicular networks lack a context with a comparatively long life, connecting a user device directly to hotspot would requires a long-lasting password, which would be impracticable for securing VC.

Privacy VS Authentication

In VANET, authentication is crucial to preventing the previously stated Sybil attack. We can give each vehicle a unique identity to prevent this issue, but most drivers prefer to keep their information secure and private, so they won't be comfortable with this option.

Network Scalability

Given that there are currently more than 750 million nodes in this network worldwide [24] and that number is expected to increase, it becomes problematic since there is no global body that sets the rules for this network. For instance, the DSRC standards in North America differ from those in Europe, and those for GM vehicles differ from those for BMW.

VANET Security Requirements

Authentication

In VANET, each message must be authenticated in order to establish its authenticity and regulate the level of vehicle authorization. To accomplish this, vehicle will give each message their private keys and certificates. The receiver will then receive the message and verify it after confirming the key and certificate are present.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

Availability

A delay of even a few seconds in some applications might render the message worthless and perhaps have disastrous effects. Vehicular networks must be available constantly. Many applications call for real-time performance from sensor networks or even ad hoc networks.

Non-repudiation

It will make it easier to track down the attacker after the attack has already taken place. This keeps cheaters from trying to cover up their wrong doing. Any official side possessing authorization can get any data related to the vehicle, including the journey routes, speed, time, and any violations.

Privacy

Temporary keys are for achieving privacy; it will be often changed because each key can only be used once before expiring.

Integrity

To prevent attackers from tampering with communications and to ensure that message contents can be trusted, integrity for all messages should be safeguarded.

Confidentiality

The messages should be encrypted to prevent accessing the drivers' information from outsiders, and each driver's privacy must be safeguarded.

CURRENT SOLUTIONS

The authors of [25] proposed the use of a group signature, but this idea has the significant drawback that it is generating a significant amount of overhead. The group public key and the vehicle session key must be changed and transmitted as each time a vehicle enters the group area. Group signature is also discussed in [14], where the authors offered a protocol to fulfill the security and privacy criteria, as well as to give the needed traceability and liability, although the study's findings were not particularly positive. The average message loss ratio was 45% after a group signature verification delay of 9 ms, and when there are 150 vehicles on the road, the loss ratio can reach 68%.

The usage of CA has also been proposed as a solution, although this requires infrastructure. For VANET to be governed, a lot of CA is needed. The CA has been proposed by [22], and all of these researchers mentioned the CA to manage all certificate operations including generating, renewing, and revoking certificates. In addition, the CA must be in charge of starting keys and storing, managing, and broadcasting the CRL.

The authors of [24] also explored how to keep the message's authentication up to date, in which each message is signed by the vehicles using their private keys and the relevant certificates is attached. In order to reduce the overhead, they have suggested using ECC. Long term certificates are used for authentication whereas short term certificates are used for data transmission utilising public or private key cryptography, contrary to what the authors of [1] indicated as alternative way to use the keys. As they are intended for broadcasting, safety messages are not encrypted, but their validity must be verified. However, any adversary can inject false information as safety messages because it is not encrypted, and it can also steal the certificate. In order to address issues associated with using VPKI in VANET such as the need to revoke an attacker's certificate, writers in [24] explored the Certificate Revocation solution. First, because there are so many

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

vehicles and they are so mobile, CRLs can be very long. Second, there is still a vulnerability window due to certificates' short lifespan, and third, there is no infrastructure for CRLs.
Other revocation protocols addressed include Distributed Revocation Protocol, RTPD Revocation Protocol of the Tamper-Proof Device, and RCCRL Revocation protocol utilising Compressed Certificate Revocation Lists. These protocols are also covered in detail in [23].
The technique described by the authors in [24] utilising a set of anonymous keys that vary often (every few minutes) in accordance with the driving pace. Only one key may be used at a time, and each key may only be used once before it expires. These keys have a short lifetime and are certified by the issuing CA. The disadvantage of this system, that the keys need storage, can also be linked to the true identity of the car ELP.
IP version 6 has been suggested for usage in automotive networks, according to the authors of [1], who also noted that in the IEEE WAVE standard, vehicles can change their IP addresses and utilize random MAC addresses to achieve security. It should be possible for vehicles to change their IP addresses in order to become untraceable, although it is unclear how this will be done. Additionally, since the old address cannot be instantly used when a new one is assigned, this may result in inefficient address usage. When the automobile changes its IP address, delayed packets will be discarded, resulting in needless retransmissions. Another remedy was provided by the authors in [19] by instituting routine inspections, where in the majority of U.S. states all vehicles are required to pass inspection once a year.

CONCLUSION

For enhancing information services and road safety VANET is a convincing wireless communication system. The fundamental overview of a VANET is provided in this work. It's a promising technology that offers lots of opportunities for hacker to attempts to attack the networks with their malicious attack. After outlining characteristics and design, this study provides an in-depth analysis of VANET security. Then, threats and assaults on VANET were introduced, along with the security issues. Additionally, various security-related topics have been brought up, including the need for security, attacker profiles, and attacks, as well as potential solutions and their benefits and drawbacks. However, there are still a number of challenges to overcome before VANETs' beneficial effects on traffic efficiency and safety achieved. The fundamental concepts of authentications are also explained in terms of message transmissions among vehicles.

REFERENCE

1. Abdalla, G. M., Abu-Rgheff, M. A., & Senouci, S. M. (2007). Current trends in vehicular ad hoc networks. Ubiquitous Computing and Communication Journal, 1-9.
2. Afzal, Z., & Kumar, M. (2020). Security of vehicular ad-hoc networks (VANET): a survey. In Journal of Physics: Conference Series (Vol. 1427, No. 1, p. 012015). IOP Publishing.
3. Azam, F., Yadav, S. K., Priyadarshi, N., Padmanaban, S., & Bansal, R. C. (2021). A comprehensive review of authentication schemes in vehicular ad-hoc network. IEEE access, 9, 31309-31321.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

4. Bako, B., & Weber, M. (2011). Efficient information dissemination in VANETs. In Advances in Vehicular Networking Technologies. IntechOpen.
5. Funderburg, L. E., & Lee, I. Y. (2021). Efficient short group signatures for conditional privacy in vehicular ad hoc networks via ID caching and timed revocation. IEEE Access, 9, 118065-118076
6. Ghassan, S., Al-Salihy, W. A., & Sures, R. (2010). Security analysis of vehicular ad hoc networks (VANET). In 2010 second international conference on network applications, protocols and services, national advanced IPv6 center. Universiti Sains Malaysia Penang, Malaysia.
7. Hasrouny, H., Samhat, A. E., Bassil, C., & Laouiti, A. (2017). VANet security challenges and solutions: A survey. Vehicular Communications, 7, 7-20.
8. Jiang, Y., Ge, S., & Shen, X. (2020). AAAS: an anonymous authentication scheme based on group signature in VANETs. IEEE Access, 8, 98986-98998.
9. Kamini, K., & Kumar, R. (2010). VANET parameters and applications: A review. Global Journal of Computer Science and Technology.
10. Kohli, P., Painuly, S., Matta, P., & Sharma, S. (2020, December). Future trends of security and privacy in next generation VANET. In 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS) (pp. 1372-1375). IEEE.
11. Kugali, S., & Kadadevar, S. (2020). Vehicular ADHOC Network (VANET): A Brief Knowledge. International Journal of Engineering and Technical Research, (9), 6.
12. Kumar, R., & Dave, M. (2011). A comparative study of various routing protocols in VANET. arXiv preprint arXiv:1108.2094.
13. Kumar, R., & Dave, M. (2012). A review of various vanet data dissemination protocols. International Journal of u-and e-Service, Science and Technology, 5(3), 27-44.
14. Lu, R., Lin, X., Zhu, H., Ho, P. H., & Shen, X. (2008, April). ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. In IEEE INFOCOM 2008-The 27th Conference on Computer Communications (pp. 1229-1237). IEEE.
15. Malina, L., Vives-Guasch, A., Castellà-Roca, J., Viejo, A., & Hajny, J. (2015). Efficient group signatures for privacy-preserving vehicular networks. Telecommunication Systems, 58(4), 293-311
16. Mejri, M. N., Ben-Othman, J., & Hamdi, M. (2014). Survey on VANET security challenges and possible cryptographic solutions. Vehicular Communications, 1(2), 53-66.
17. Mustafa, A. S., Hamdi, M. M., Mahdi, H. F., & Abood, M. S. (2020, November). VANET: towards security issues review. In 2020 IEEE 5th international symposium on telecommunication technologies (ISTT) (pp. 151-156). IEEE.
18. Nandy, T., Noor, R. M., Idris, M. Y. I. B., & Bhattacharyya, S. (2020, February). T-BCIDS: Trust-based collaborative intrusion detection system for VANET. In 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA) (pp. 1-5). IEEE.
19. Parno, B., & Perrig, A. (2005, November). Challenges in securing vehicular networks. In Workshop on hot topics in networks (HotNets-IV) (pp. 1-6).

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

20. Qin, B., Wu, Q., Domingo-Ferrer, J., & Zhang, L. (2011, November). Preserving security and privacy in large-scale VANETs. In International Conference on Information and Communications Security (pp. 121-135). Springer, Berlin, Heidelberg.
21. Rajput, U., Abbas, F., Eun, H., & Oh, H. (2017). A hybrid approach for efficient privacy-preserving authentication in VANET. IEEE Access, 5, 12014-12030.
22. Raya, M., & Hubaux, J. P. (2005, November). The security of vehicular ad hoc networks. In Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (pp. 11-21).
23. Raya, M., Jungels, D., Papadimitratos, P., Aad, I., & Hubaux, J. P. (2006). Certificate revocation in vehicular networks. Laboratory for computer Communications and Applications (LCA) School of Computer and Communication Sciences, EPFL, Switzerland, 1-10.
24. Raya, M., Papadimitratos, P., & Hubaux, J. P. (2006). Securing vehicular communications. IEEE wireless communications, 13(5), 8-15.
25. Ren, W., Ren, K., Lou, W., & Zhang, Y. (2010, May). Efficient user revocation for privacy-aware PKI. In 5th International ICST Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness.
26. Saha, A. K., & Johnson, D. B. (2004, October). Modeling mobility for vehicular ad-hoc networks. In Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks (pp. 91-92).
27. Saini, M., & Singh, H. (2016). VANET its characteristics attacks and routing techniques: a survey. International Journal of Science and Research, 5(5), 1595-1599.
28. Tomar, R., Prateek, M., & Sastry, G. H. (2016). Vehicular adhoc network (vanet)-an introduction. International Journal of Control Theory and Applications, 9(18), 8883-8888.
29. Wang, Y., Zhong, H., Xu, Y., & Cui, J. (2016). ECPB: efficient conditional privacy-preserving authentication scheme supporting batch verification for VANETs. Int. J. Netw. Secur., 18(2), 374-382.
30. Yue, X., Chen, B., Wang, X., Duan, Y., Gao, M., & He, Y. (2018). An efficient and secure anonymous authentication scheme for VANETs based on the framework of group signatures. IEEE Access, 6, 62584-62600.
31. Zhang, J., Zheng, K., Zhang, D., & Yan, B. (2020). AATMS: An anti-attack trust management scheme in VANET. IEEE Access, 8, 21077-21090.