IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 7, July 2019

VANET: Attacks and Privacy Preserving Protocols

Ritika Yaduvanshi[1], Shashank Shekhar Tiwari[2], Kumkum Dubey[2], Prince Rajpoot[2,] Shivendu Mishra[2]

Department of Computer Science and Engineering, Mahamaya College of Agricultural
Engineering and Technology, Akbarpur, Ambedkar Nagar (U.P), India[1]

Department of Information Technology, Rajkiya Engineering College Ambedkar Nagar (U.P), India[2]

Abstract: Now days, it is seen that VANET are widely spread in the world of vehicular transportation. It is different from the other networks because of its features and working. Main function of Vehicular Ad-hoc Network is to provide safety, increases driving experiences, and good management of the traffic. Further, VANET focuses on private data transferring from one vehicle to other with threat less data management. In this paper, we will discuss about the various features of VANET's with possible attacks, and security requirements in VANET. Moreover, some of the privacy preserving protocols are also describe with their advantages and disadvantages.

Keywords: Vehicular Ad-hoc Network (VANET), Trusted Authorities (TA), Security, Privacy, Message Authentication Code (MAC).

I. INTRODUCTION

Vehicular ad-hoc network is the combination of dynamic and mobile nodes for unstable networks without any help of fixed infrastucture. Mobile ad-hoc networks' principles are the basis for vehicular ad-hoc network. It is based on wireless network technology for exchanging data from vehicle to vehicle within the domain of vehicles.VANET have three most important elementsie. Roadside Units (RSUs), Trusted Authority (TA), and a vehicle with embedded On-Board Units (OBUs). Trusted authority (TA) is responsible for maintenance and storage capabilty of the whole system TA is used to register each RSUs at the road side and OBUs attached with vehicle.RSUs are storage database they have storing information coming from TA and OBUs. RSUs works between TA and OBUs, RSUs also helps to track the harmful vehicle[2].OBUs are used to collect, share traffic information, andto communicate with other vehicles, and increases careful driving environment.There are three kinds of communication exists in VANETs i.e. Vehicle to Vehicle Communication (V2V), Vehicle to Infrastructure Communication (V2I), and Infrastructure to Vehicle communication (I2V)[1].

A. *Features of VANET*

VANET has defferent features which are following-:

- **High Mobilty:** In VANETs nodes which are basically the vehicles generally move at high speed. Thus it is difficult to find the position of nodes hence making security and privacy of node.
- **Dynamic Topology:** Because of the dynamic infrastucture of nodes,It is very difficult to calculate all the nodes position. Thus networks topology in Vehicular ad-hoc netwoks changes on a frequent interval. Further More, The link connections between the vehicles in VANETs has regularly not stable connection due to dynamically nodes position in the environment.
- **Wireless Communication:**Nodescommunication are wireless in VANETs hence security measures must have been taken while communication.
- **Unbounded network size:**In VANETs the size of Network is geographically unbounded. Therefore, VANETs can be implemented at any place i.e. for any city, country and other geaographical areas.
- **Time Critical:**The sending and the receiving of the information to the nodes in VANETs must have been within time interval. So all nodes in VANETs are updating regularly and exchange informaton very fast to each other, critical medical emergency messages must have been delivered on time so save human lives.
- **No Power limitation:**As in MANET there is concerned energy and computation resaurces, the VANET doesn't have the same. That can be further utilized in efficient processing of complex and computational hungry routing and security mechanism.

DOI 10.17148/IJARCCE.2019.8705

- **Geographic position available:**In VANETs, We calculate the corrrect position of vehicle with the help of GPS. Moreover, electronic maps are completely popular in cars and other vehicles, and also providing location information for routing purposes of vehicles in VANETs environment.

II. VANET ARCHITECTURE

VANET can use for communicating real time traffic and safety information among VANET units. In VANET, there are three kinds of entities, which are TA, RSUs, OBUs environment. OBUs communicate with other devices by sharing the data and related information. TA is the government-trusted authority that is used to register each RSU at the roadside and OBUs are attached with the vehicle. If vehicle got involved in any kind of harmful activity then the TA can reveal the real identity of the vehicle since it has the authority. RSUs are assistant by TA since it has a storage unit that stores the information coming from TA and OBUs. RSUs play the role of inter-mediator between TA and OBUs. RSUs provides anonymous key and certificate to the OBUs, it also helps in tracking the harmful vehicles. OBUs are located on each vehicle in VANET in order to improve the safety of driving.

III.SECURITY ATTACKS

VANET generally uses wireless medium for data transmission. There are some possible security attacks, which we enlisted in this paper:

- **Sybil Attack:** In this attacker, create illusion to different vehicle. Here different source used to put attack on culprit. Further, Attacker creates illusion of crossing so victim vehicle uses another path.
- **Denial of Service attack (DoS**): Such attacks used to jam the connectivity between vehicles. In this attacker uses programs to persist the modular wave of data, so it creates hindrances in the networking. Bandwidth of required channel is mostly in use that is channel jam condition of victim vehicle will occur.
- **Replay attack:** In such attack, attacker creates conflicts between RSUs and OBUs. In this information gather by attacker replayed repeatedly to acquire the benefit of situation and create perplexing to authorities in order to deceive them what is actually going on.
- **Privacy attack:** In this attacker acquires sensitive and important information about vehicle user. Attacker creates vehicle profile by using his identity information and tracks vehicle. Therefore, attacker can illegally leak the information related to vehicle use that can access by any user that will detrimental for any vehicle user.
- **Spamming:** In such type of attack, the attacker sends many spam messages in the network so that the bandwidth of network is decreased and transmission latency increased. This type of attack is hard to manage [6].
- **Bogus Information:** In such type of attack, the attacker broadcast wrong or false information in the network. For example announcement of "intense traffic" although there is no traffic in the network.
- **Black Hole:** In such type of attack, the attacker distract all the traffic of the network towards an area where no node exists or non (participated) interested nodes exists and hence result in loss of information [7].
- **Grey hole:** This type of attack is deviation of Black Hole attack. In this, the attacker sometimes misleads the network but it from time to time drops the packets and then switches to its usual behaviour.
- **Warm hole:** This type of attack is also a deviation of Black Hole attack. In this the attacker creates a subway to transmit confidential information from one (attacker) end of tunnel to other end (attacker).
- **Masquerade:** In such type of attack, the attacker makes believe to other to itself as legitimate user. The attacker does this by IP and MAC addresses spoofing.
- **Timing Attack:** In such type of attack, the attacker forward received message after some delay in the network. Hence, the other nodes receive the required information in late that cause them to struck into traffic, choose wrong path etc.
- **Location Tracking:** In such type of attack, the attacker somehow tracks the location of a particular vehicle.
- **Identity Disclosure:** In such type of attack, the attacker somehow discloses the identity of neighbouring nodes. This information can be use by various purposes. For ex. The car owner can track their car driver path using this attack.
- **Malware Attack:** Such type of attack is perform by viruses to gain the information of infected vehicle.
- **Man in the Middle Attack:** In such type of attack, the attacker somehow makes a connection in between two communicating vehicle and make believe them no one is in between them. In this the attacker modify the information or only read the information for own interest.

DOI 10.17148/IJARCCE.2019.8705

IV. REQUIREMENTS OF SECURITY

There are following requirements which will be considered under security-

- **Authentication:** In VANET every vehicle and each RSUs should certified using certification i.e. there is a proper identity provided to individual vehicle to differentiate between good and faulty vehicles. Further, in VANET source as well as Message authentication both required.
- **Data Integrity:** In VANET, modified and tampered data creates traffic security and data altering safety problem. So data integrity must be provide.
- **Availability:** In this, Bandwidth of channel will provided for vehicle to prevent from DoS attack because it has proper identity channel so attacker cannot do multiple request on vehicle for messaging.
- **Anonymity:** In this actual identity of each vehicle, owner is hide from other users and authorities too. To prevent from the malicious activities only trustable higher committee like TA knows all the information.
- **Unlinkability:** To prevent from the data hijacking of identity from the attacker in unpredictable manner.
- **Traceability and revocability:** Even though, the vehicle real identity should be conceal from other vehicles, there should be an entity (e.x. Manager) that has the ability to obtain vehicles' real identities and to invalidate them from future usage.
- **Non-repudiation:** It ensures that any vehicle must not be able to refuse the broadcast of the information.
- **Privacy:** VANET is designed in such a way that none of the crucial information will be access by any unauthorized user and committee even none of the user can locate the user's information i.e. Proper anonymous identity should be maintained in VANET.

V. PRIVACY PRESERVING STRATEGY

The privacy preserving strategy broadly classified into following four categories as shown in Figure 1:

1. Pseudonymous based privacy strategy
2. Group signature based privacy strategy
3. Identity based privacy strategy
4. Hybrid strategy

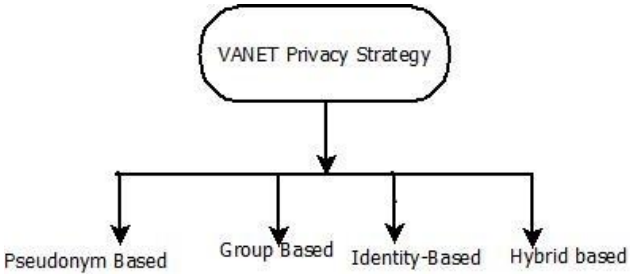

Figure 1: Privacy Preserving Strategy

1. Pseudonymous based privacy strategy: Chum introduced the concept of pseudonym (Alternate or false name) based privacy-preserving technique [8]. In this strategy pseudonym are usedfor anonymously communication among vehicle. Hence, it can insure privacy and identity secrecy. These pseudonyms generated in such a way that no one except trusted authority (TA) can link pseudonyms with real vehicle identity. Thus using pseudonym vehicle real identity is anonymous to other vehicle (un-likability) and in case of any dispute; TA reveals the real identity of vehicle and thus providing conditional privacy. There are many schemes developed until date based on this strategy. Some of them shown in the following Table1 with advantages and disadvantages of each.

TABLE 1: PSEUDONYM BASED STRATEGY

S.No	Protocol	Advantages	Disadvantages
1	PASS[10] Year	Efficient Certificate Updation, Distributed certificate updation, CRL size is linear to revoked vehicles.	computation Overhead, communication overhead, certificate managements
2	EPPKI[11]	Certificate traceability and revocation	Computation overhead, verification delay
3	RH[12]	Hierarchical pseudonym, blind signature,	Verification delay, computation overhead, no security proof
4	LSVN[13]	Navigation based, low computation and delay	Overhead over RSU and OBU due to key sharing process.

DOI 10.17148/IJARCCE.2019.8705

5	Mohanty et al.[14]	Certificateless aggregate signature, batch verification, scalability, bandwidth utilization, low communication overhead	More overhead on RSU
6	He et. al[15]	Batch verification, low transmission over head.	No traceability
7	Kang et.al.[16]	Batch verification, fast authentication	No traceability

2. **Group signature based privacy strategy:** In this strategy group signature used to maintain vehicle privacy. In-group signature there are two main entities i.e. Group Manager and second Group Members. The ability of group signature is that no one either in-group or outside of the group knows which member sign the message and thus provides un-traceability. In-group signature each member has their own private key and the public key is common for all and is known as system public key. It constructed with four algorithms, which is setup phase, signature phase, verification phase and open phase. In the setup phase, the system public parameter is generated. In signature phase, each member using their private key and system public parameter generates signature on any information without revealing their identity. In verification phase, anyone can verify that the signature is from the same group without revealing sender of signature. In open phase, manage reveal the identity of signer in case of dispute. Hence, it provides conditional privacy. There are many schemes developed until date based on this strategy. Some of them shown in the following Table2 with advantages and disadvantages of each.

TABLE 2: GROUP BASED STRATEGY

S.No	Protocol	Advantages	Disadvantages
1	Guo et. al.[17]	Access control list, access control based role scheme, traceability	No implementation
2	Tiwari et.al.[18]	ECDSA, low cost, only authorized access.	No implementation, security, and verification delay discussion.
3	kim et al.[19]	No signature process, low computation	Communication overhead, message loss, no performance discussion
4	Hasrouny et.al.[20]	Fast verification, reduce latency, delay.	No conditional privacy and batch verification.
5	Shao et. al.[21]	Batch signature verification, threshold authentication, low computation cost.	Communication overhead, slow verification, more end to end delay
6	WASEF et al.[22]	Batch signature verification, low verification delay, signature size, and message lost ratio.	Design fault
7	Lim et. Al.[23]	Efficient key distribution, reduced message signature and verification time, scalability.	Congestion can happen in VANET,
8	Alimohammadi et.al. [24]	Fast verification, reduced overhead	End to end delay

1. **Identity based privacy strategy:** Shamir [9] introduced the concept of identity based encryption and signature scheme, in 1984. This concept removes the needs of certificates and provides more secure and efficient schemes. In identity-based system, the user's unique identity are used bytrusted third party known as private key generator (PKG) to computes user's public key and user's private key. There are many schemes developed until date based on this strategy. Some of them shown in the following Table3 with advantages and disadvantages of each.

TABLE 3: GROUP BASED STRATEGY

S.No	Protocol	Advantages	Disadvantages
1	Zhang et. al.[25]	Hierarchical aggregation, batch verification, reduced cost for certificate management, low latency,and fast response.	Overall, slow operation, likability, less security.
2	Sun et.al. [26]	Average computation overhead, less communication and computation cost.	likability, less security, and no identity anonymity

DOI 10.17148/IJARCCE.2019.8705

3	Jiang et al.[27]	Signature size small, low computation cost, low communication cost.	Repudiation, likability, less security, and no identity anonymity

2. Hybrid strategy: This strategy uses combination of above strategy i.e. uses Pseudonymous based privacy strategy, Group signature based privacy strategy, and Identity based privacy strategy for better result in term of security, cost, efficiency etc. some of the schemes using hybrid strategy described in the Table 4 [10].

Table 4: Hybrid Based Strategy

S.No	Protocol	Advantages	Disadvantages
1	Liu et al.[65]	Distributed computing service, batch verification, Low communication overhead	Dos, Sybil attack and location tracking possible
2	Rabieh et.al.[70]	Future routes privacy, average computation and communication overhead.	No identity anonymity, no traceability
3	Wazid et.al.[69]	Efficient key sharing, small message size, better performance.	More end to end delay, no conditional privacy.

VI. CONCLUSION

VANET is a good & upcoming technologies still improve day by day. In this paper, we conclude that VANET has architecture attractive application, training & problem solving of attacks and required features to sort out the attacks. It is also design for vehicle communication and better way of travel safe from tracking. In addition privacy preservation protocols classified for the privacy of messages convey from one vehicle to other.

REFRENCES

[1]. Biswas, S., & Misic, J to Privacy-preser, "A Cross-layer Approach ving Authentication in WAVE-enabled VANETs." Vehicular Technology, IEEE Transactions on 62(5): 2182 – 2192 (2013).
[2]. Pradweap, R. V., & Hansdah, R. C, “A Novel RSU-Aided Hybrid Architecture for Anonymous Authentication (RAHAA) in VANET”, In Information Systems Security (pp. 314-328). Springer, (2013).
[3]. Verma, K.; Hasbullah, H.; Kumar, A., "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," Advance Computing Conference (IACC), 2013 IEEE 3rd International, vol., no., pp.550, 555, 22-23 Feb. 2013.
[4]. Grzybek, A.; Seredynski, M.; Danoy, G.; Bouvry, P., "Aspects and trend sin realistic VANET simulations, Wireless, Mobile and Multimedia Network, 2012 IEEE International Symposium on a, vol., no., pp.1,6, 25-28 June 2012.
[5]. Xie, Y., Wu, L., Shen, J. et al.“EIAS-CP: new efficient identity-based authentication scheme with conditional privacy-preserving for VANETs”, Telecommun Syst 65: 229, (2017).
[6]. Rawat, Ajay & Sharma, Santosh & Sushil, Rama,“VANET: Security attacks and its possible solutions”, Journal of Information and Operations Management, (2012).
[7]. Vinh Hoa LA, Ana CAVALLI,”SECURITY ATTACKS AND SOLUTIONS IN VEHICULAR AD HOC NETWORKS: A SURVEY”, International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 2, April (2014).
[8]. D. Chaum, Security without identification: transaction systems to make big brother obsolete, Communications of the ACM, 28 1030-1044, (1985).
[9]. A. Shamir, Identity-based cryptosystems and signature schemes, Advances in Cryptology-Crypto, pp. 47-53, (1984).
[10]. Ali, Ikram & Hassan, Alzubair & Li, Fagen. “Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey”. Vehicular Communications, (2019).
[11]. Y. Sun, R. Lu, X. Lin, X. Shen, J. Su, “An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications”, IEEE Transactions on Vehicular Technology, 59 (7) (2010).
[12]. C. I. Fan, R. H. Hsu, C. H. Tseng, “Pairing-based message authentication scheme with privacy protection in vehicular ad hoc networks”, in: The International Conference on Mobile Technology, Applications & Systems 2008 (Mobility Conference) , pp. 1-7, (2008).
[13]. E. R. Agustina, A. R. Hakim, “Secure VANET protocol using hierarchical pseudonyms with blind signature”, in: 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, pp. 1-4,(2017).
[14]. G. Li, M. Ma, C. Liu, Y. Shu, A lightweight secure VANET-based navigation system, in 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, pp. 1-6,(2015).
[15]. S. Mohanty, D. Jena, S. K. Panigrahy, “A secure RSU-aided aggregation and batch-verification scheme for vehicular networks”, in: International Conference on Soft Computing and its Applications(ICSCA’2012), Kuala Lumpur, pp. 174-178, (2012).
[16]. D. He, S. Zeadally, B. Xu, X. Huang, “An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks”, IEEE Transactions on Information Forensics and Security, 10, (12) 2681-2691, (2015).
[17]. J. Guo, J. P. Baugh, S. Wang, “A group signature based secure and privacy-preserving vehicular communication framework”, in: 2007 Mobile Networking for Vehicular Environments, Anchorage, AK, pp. 103-108, (2007).
[18]. D. Tiwari, M. Bhushan, A. Yadav, S. Jain, “A novel secure authentication scheme for VANETs”, in: 2016 Second International Conference on Computational Intelligence & Communication Technology (CICT), Ghaziabad, pp. 287-297, (2016).
[19]. D. Kim, J. Choi, S. Jung, “Mutual identification and key exchange scheme in secure VANETs based on group signature”, in: 2010 7th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, pp. 1-2, (2010).

[20]. H. Hasrouny, C. Bassil, A. E. Samhat, A. Laouiti, "Group-based authentication in V2V communications", in: 2015 Fifth International Conference on Digital Information and Communication Technology and its Applications (DICTAP), Beirut, pp. 173-177, (2015).

[21]. J. Shao, X. Lin, R. Lu, C. Zuo, "A threshold anonymous authentication protocol for VANETs", IEEE Transactions on Vehicular Technology, 65 (3) 1711-1720, (2016).

[22]. A. Wasef, X. Shen, Efficient group signature scheme supporting batch verification for securing vehicular networks, in: 2010 IEEE International Conference on Communications, Cape Town, pp. 1-5,(2010).

[23]. L. Wei, J. Liu, T. Zhu, "on a group signature scheme supporting batch verification for vehicular networks", in: 2011 Third International Conference on Multimedia Information Networking and Security, Shanghai, pp. 436-440,(2011).

[24]. M. Alimohammadi, A. A. Pouyan, "Sybil attack detection using a low cost short group signature in VANET", in: 2015 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC), Rasht, pp. 23-28, (2015).

[25]. L. Zhang, C. Hu, Q. Wu, J. D. Ferrer, B. Qin, "Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response", IEEE Transactions on Computers, 65 (8) 2562-2574, (2016).

[26]. J. Sun, C. Zhang, Y. Zhang, Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks", IEEE Transactions on Parallel and Distributed Systems, 21 (9), 1227-1239 (2010).

[27]. Y. Jiang, M. Shi, X. Shen, C. Lin, BAT: "A robust signature scheme for vehicular networks using binary authentication tree", IEEE Transactions on Wireless Communications, 8 (4), pp 1974-1983, (2009).

[28]. Y. Liu, L. Wang, H. H. Chen, "Message authentication using proxy vehicles in vehicular ad hoc networks", IEEE Transactions on Vehicular Technology, 64 (8), pp 3697-3710, (2015).

[29]. K. Rabieh, M. M. E. A. Mahmoud, M. Younis, "Privacy-preserving route reporting schemes for traffic management systems", IEEE Transactions on Vehicular Technology, 66 (3), pp 2703-2713, (2017).

[30]. M. Wazid, A. K. Das, N. Kumar, V. Odelu, A.G. Reddy, K. Park, Y. Park, "Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks", IEEE Access, 5, pp 14966-14980, (2017).

DOI 10.17148/IJARCCE.2019.8705