Indian Journal of Science and Technology, Vol 9(28), DOI:10.17485/ijst/2016/v9i28/97782, July 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

VANETs Security Issues and Challenges: A Survey

Muawia Abdelmagid Elsadig[1*] and Yahia A. Fadlalla[2]

[1]College of Computer Science and Technology, Sudan University of Science and Technology – SUST, Khartoum, Sudan; Muawiasadig@Yahoo.Com
[2]Infosec Consulting, Hamilton, Ontario, Canada; Trusted_Software@Usa.Net

Abstract

Vehicular Ad-hoc Networks (VANETs) are sought to control traffic, avoid accidents, and control other aspects of traffic. It (VANET) is a piece of critical infrastructure that bolsters traffic management efficiency and road safety. Nowadays, VANET applications have received a great deal of attention by the research community due to the important role that such networks can play. However, security in VANETs still remains a big challenge due to its nature. This survey paper sheds some light on VANETs' vulnerabilities and attacks. It surveys and examines some recent security solutions along with their achievements and limitations. As a result, we conclude that security is the key to success for VANET applications, but still some critical challenges remain. Moreover, when designing a sufficient security solution; privacy preservation, productivity, and usability should be taken into account. Therefore, the door for future research is open for a lot more contributions in this filed.

Keywords: Attacks, Privacy, Security, Threats, VANETs, Vulnerabilities

1. Introduction

VANETs – Vehicular Ad Hoc Networks are created by applying the principles of a Mobile Ad Hoc Network (MANET). Therefore, it is considered as a subset of a MANET. It incorporates the capabilities of new generation wireless networks into vehicle[1]. These types of networks are highly dynamic in nature[2]. VANETS can autonomously organize networks without infrastructure and lack of guaranteed connectivity[3].

In Wireless Access in Vehicular Environments (WAVEs), two standards are defining the communication methods. These two standards are Vehicle-to-Vehicle communication (V2V) and Vehicle-to-Roadside (V2R) communication[4]. In VANETs, Inter Vehicle Communication (IVC) refers to communication between moving vehicles[2]. A VANET is considered as a different form of a MANET. In which every participating vehicle is turned into a wireless router or node, and allows vehicles in a range of 300 meters to connect to each other[5].

Vehicular Ad Hoc Networks (VANETs) have been receiving potential attention from the research community as well as from general populace due to its important role in many applications. These applications may include: Alert signal functionality on lane merging and intersection, value added services (i.e., providing appropriate Internet access to improve drivers' traveling experience), toll payment services, congestion avoidance warning messages, navigation, road conditions, alarm signals circulated by emergency vehicles, detour notification, etc[6].

VANET is a promising approach that can facilitate traffic management, road safety, and infotainment dissemination for both, passengers and drivers[7]. VANETs have a potential role in maintaining road safety based on alerts being given to drivers in adequate time. So they can react accordingly to dangerous situations. Therefore, in order to prevent abuse of VANETs, an infrastructure to satisfy all security requirements in VANETS is needed. Authors in[8] give a comprehensive detail on VANETs' security requirements and propose a security infrastructure.

A review study that demonstrates some methods of facilitating security services and maintaining privacy in Vehicular applications is given in[7]. In addition, the authors pointed out two essential issues making the standards practical: Conditional privacy preservation

*Author for correspondence

and certificate revocation. Therefore, preserving privacy and securing certificate revocation are considered great challenges in VANETs.

The characteristic of the highly dynamic topology in VANET makes security in such a type of network a real challenge. It is pointed out in[9] that in order to protect consistency and integrity, VANET needs a series of security mechanisms.

The issue of security is a major challenge of VANETs and should be taken seriously prior to deployment of any applications based on such types of networks. In order to understand how important security is, try to imagine that a safety message initiated by a VANET system has been modified, delayed, or discarded due to any type of attack that caused by an intruder or an attacker, intentionally or accidentally. As such, serious consequences could happen such as injuries, deaths, infrastructure damage, etc. Consequently, researchers are still seeking to develop adequate security architecture that is able to maintain a secure VANET[10]. On the other hand, one of the important challenges that addressed by[11] is to maintain a reasonable balance between the security and privacy in VANETs; it is important for any receiver to get reliable or trustworthy information from its source. However, this trusted information can violate the sender's privacy.

In[12], a security attack on a Cooperative Adaptive Cruise Control (CACC) vehicle has been grouped into four categories: Network layer, application layer, privacy leakage, and system level attacks. These attacks can be caused by insider or outsider attackers. In addition, they pointed out that all of the mentioned attacks have potential impact on the string stability of the system and can compromise the safety and privacy of CACC vehicle stream passengers. A comprehensive discussion on these attacks is covered in[12].

In this section we introduce VANET systems and some issues concerning them. The rest of the paper is organized as follows; Section 2 points out security goals by defining security requirements and what to achieve after satisfying them. Section 3 demonstrates VANET attacks and vulnerabilities from various aspects and classifications. A comprehensive study and discussions on related work are given in Section 4. Achievements and limitations of many approaches and methods that have been given by recent previous work have been presented. Conclusions are given in Section 5.

2. Goals

A secure VANET system should fulfill fundamental security requirements which involve confidentiality, authentication, nonrepudiation, integrity, and accountability. Maintaining all of these can aim at protecting the system against denial of service, unauthorized-message injection, eavesdropping, message alteration, etc[10].

3. VANETs Attacks and Vulnerabilities

VANET is envisioned to control traffic, avoid accidents, enhance driving experience, and control other aspects of traffic. It is a critical infrastructure for traffic management efficiency and road safety. However, with the rapid development in VANET, security concerns have continued to strengthen as well. VANET architecture is vulnerable to unauthorized access, illegal use, eavesdropping, protocol tunneling, etc. Authors in[13] give a comprehensive investigation and discussion on VANET vulnerabilities and Attacks and they classify VANET attacks into many categories. Table 1 below shows a summary of their attacks classification, whereby it has been noticed that their classification of attack types is based on insiders, outsiders, maliciousness, networks, and monitoring attacks.

In[20] the following attack types are discussed: Bogus Information, Cheating with Sensor Information, ID Disclosure, Denial of Service (DoS), Replaying and Dropping Packets, Hidden Vehicle, Worm Hole Attack, and Sybil Attack. In addition, a comprehensive discussion and analysis on Bogus Information, DoS, impersonation, eavesdropping, message suspension, and hardware tampering has been listed in[21].

According to their object of action, the authors in[22] have classified VANET security threats into two categories: data threats and threats to the VANET system. Data threat refers to VANET information loss having incurred in the following aspects either intentionally or accidentally: Confidentiality, integrity, availability, authenticity, and non-repudiation. Meanwhile, threats to the VANET system include software, hardware, users, etc. (i.e., theft, destruction, malicious analysis to OBU and RSU, viruses, spyware, illegal access that evade system certification, user privacy leakage, etc). Figure 1 below shows the classifications in which the threats are classified according to their object of action. Comprehensive details on these classifications can be seen in[22]

Table 1. Classifications of attacks

Attack Name	Attack Type	Attack Effects
Impersonation attack	Insider attack	Privacy and confidentiality
DoS [14–16]	Malicious, active, insider, network attack	Availability
Masquerading	Insider, active attack	Authentication
Wormhole/ tunneling	Outsider, malicious, monitoring attack	Authentication and confidentiality
Bogus Information	Insider attack	Authentication
Black Hole[17]	Outsider, passive attack	Availability
Social attack	Insider attack	Integrity
Malware	Insider attack, malicious	Availability
Man-in-the-middle	Insider attack, monitoring attack	Confidentiality, privacy and integrity
Monitoring attack	Monitors road activity	Authenticity and privacy
Spamming	Insider attack, malicious	Availability
Illusion Attack	Insider, outsider attack	Authenticity and data integrity
Timing Attack	Insider attack, malicious	Integrity
Sybil Attack[18–20]	Insider, network attack	Authentication and privacy
GPS Spoofing	Outsider attack	Authentication

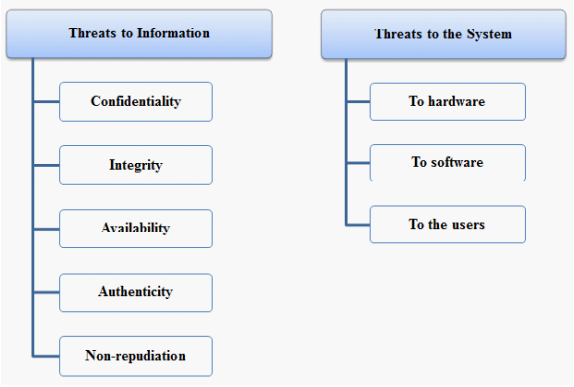

Figure 1. VANET Threat classifications based on their object of action[22]

The authors in[23] classify attacks into five classes; each class further describes different types of attack, its priority, and threat level. Theses classifications seek to better identify attacks; they include Network Attack, Social Attack, Application Attack, Monitoring Attack, and Timing Attack. Comprehensive details on these classifications were given in[23]. We recommend[24] and[25] for further readings on these attacks.

4. Related Work

VANETs offer countless services and benefits to users, but attack and misuse in such networks can defiantly cause considerable damage. The importance of taking into consideration security requirements in VANETs' design is illustrated in[10]. Authors in[10] have proposed security system for VANETs that mainly focuses on achieving privacy, non-frame ability, traceability, and privacy preserving defense against misbehavior. Their secure VANET system mainly attempts to resolve the conflicts of traceability and privacy (privacy is vehicles' desire while traceability is required by law enforcement authorities). Moreover, their system seeks to satisfy the requirements of authentication, confidentiality and message integrity. Their proposed system employs an ID-based cryptosystem where authentication doesn't need to rely on certificates. However, as the authors state, their system is yet to be simulated and experimented using real VANETs. So, more simulations and experiments are required to verify the efficiency of their proposed system especially to measure how much their system can satisfy the security requirements with fewer overheads.

In[26], the authors have proposed a Cluster based Medium Access Control Protocol (CMAC). This was proposed to handle communication between vehicles in VANETs. They claimed the proposed CMAC can deliver the message with low delay and high reliability. In addition, the aforementioned protocol can overcome hidden or exposed terminals problem. However their proposal is mainly based on the presence of the Road Side Unit (RSU). Therefore, in areas not equipped with RSUs, the protocol will function less[2].

Authors in[20] have presented a method to detect Sybil attacks in VANETs. Their approach is based on key infrastructure for detection such an attack. A Sybil attack has a significant effect on network performance and thus will lead to a large amount of damage. Based on their simulation, the authors claim that their proposed method faces

low delay in detecting a Sybil attack due to the fact that most operations are done in the Certification Authority. However the limitation here is concerned with the inability of this algorithm to identify the malicious node that causes this type of attack. The authors left that as a future work.

Due to the safety concerns about human lives on roads, the automotive industry has paid a lot of attention to VANET security. One of the important security aspects is to maintain availability. When services provided by VANET become unavailable, a considerable damage will happen. Therefore Denial of Service (DoS) is considered to be one of the important attacks that potentially affect VANETs. Adequate security approaches to fight against this type of attack should be presented. Just imagine the damage when one node sends life critical message but a DoS attack prevents it from reaching its destination.

In[14], DoS severity level in VANET environment has been elaborated as well as they have developed a model to keep VANETs secure against DoS attacks. In addition, they discussed some possible solutions. However, they came up with a model that needs to be deployed and evaluated with real scenarios; so still more work is needed in this direction.

The increasing number of traffic accidents has motivated the authors in[27] to try to improve road safety and passenger comfort. They have suggested a solution based on integration of cloud computing with VANETs. Cloud computing has the potential to enhance road safety and the travelling experience. It delivers flexible solutions such as traffic lights synchronization and alternative routes. Consequently, the authors proposed a cloud computing model (where the VANET-Cloud is applied to vehicular ad hoc networks). Their model provides numerous transportation services. However, their model has not taken into account issues such as security and privacy which will be considered in future work, as the authors stated.

Authors in[5] have proposed a novel authentication framework with conditional privacy-preservation and non-repudiation (ACPN) to be used for VANETs. For authentication, they used two schemes: ID-based Online/Offline Signature (IBOOS) and ID-based Signature (IBS). To maintain privacy preservation, the authors used the pseudonym-based scheme while utilizing the PKC-based system for the pseudonym generation. They claimed that ACPN achieved the desired requirements and is sufficient for Urban Vehicular Communications (UVC). However, using of the Public Key Cryptography (PKC) may cause more overheads; therefore, the efficiency over a large scale network needs to be approved.

Authentication in VANET is still a challenge because we do not need only to look at an adequate authentication mechanism, but we also need to pay close attention to preserve privacy while designing that mechanism. Therefore this balance should be obtained in order to attain an effective authentication mechanism. In[28], the authors have proposed a Lightweight and Efficient Strong Privacy Preserving authentication scheme (LESPP) that uses symmetric operations for message signing and verification. LESPP uses self-generated pseudo identity to ensure conditional traceability and privacy preservation. In addition, it uses symmetric encryption and Message Authentication Code (MAC) generation. Their proposal can reduce the overheads of computation and communication. The simulation performed to determine feasibility demonstrates that the proposed model works successfully in terms of network delay, message loss ratio, and message signing or verification. However, if any limitation is to be addressed, it concerns the use of symmetric algorithms. In addition, more simulations are needed to verify the result. Also, LESPP needs to be tested by deploying it on real scenarios.

In[29], the authors have demonstrated how using aggregation in VANETs is important and meaningful and pointed out some unique security issues in comparison with those happen to other VANET scenarios. Because of the limitations of the wireless bandwidth medium, scalability is a success factor. Data aggregation has great contribution on achieving and enhancing scalability. However, the verification of aggregated information integrity is not an easy task. So, an attack is defiantly possible to take place[29].

The authors in[29] presented security mechanisms for semantic data aggregation that are suitable for use in VANETs. Based on their evaluation, they demonstrate the effectiveness of their mechanisms. Their scheme is capable to be incorporated with many existing aggregation approaches, as they have stated. However, the authors in[30] have pointed out that, the scheme in[29] produces a high dissemination delay.

The MobiMix approach presented in[31] enhances attack resilience by taking into consideration numerous factors such as user moving patterns, traffic density, etc. However, the authors in[32] have stated that this approach does not work appropriately against continuous query attacks. It is able to deliver user-level protection against attacks such

Table 2. Summary of related work

Paper Title	Achievements	Limitations	Year	Reference
"CMAC: A cluster-based MAC protocol for VANETs"	(CMAC) can safely deliver the message with low delay and high reliability. Overcome hidden/exposed problem.	This protocol works only in the presence of RSU[2].	2010	[26]
"Efficient detection of sybil attack based on cryptography in VANET"	Ability to detect Sybil attack in VANETS, with low delay.	Inability to identify malicious node that causing this type of attack	2011	[20]
"VANET-cloud: a generic cloud computing model for vehicular Ad Hoc Networks"	Their Model has facilitated the passenger comfort and improved the road safety	No attentions have been paid to the security and privacy issues in their model.	2015	[27]
"ACPN: a novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs"	They proposed ACPN frame work, which achieved efficient privacy-preserving authentication with non-repudiation. In addition, it capable to be used with other new schemes.	Using PKC may cause more overheads, thus the efficiency over a large scale network need to be approved.	2015	[5]
"LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication"	LESPP has achieved high performance in terms of network delay, message loss ratio and message signing/ verification.	They used symmetric algorithms in encryption.	2014	[28]
"Resilient secure aggregation for vehicular networks"	Presented security mechanisms for semantic data aggregation that are suitable for use in VANET	High dissemination delay [30]	2010	[29]
"Mobimix: Protecting location privacy with mix-zones over road networks"	Enhanced attack resilience by taken into consideration numerous factors.	It does not work appropriately against continuous query attacks. It doesn't able to attain the desired privacy protection [32]	2011	[31]
"A novel mechanism of detection of denial of service attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA)"	The MIPDA approach can reduce delay overhead and thus, enhance communication speed and security in VANETs.	They are not verifying their result through actual deployment or simulation of the environment.	2015	[16]
"Secure Data Downloading with Privacy Preservation in Vehicular Ad Hoc Networks"	Their proposal warranties vehicles exclusive access to their requested data	It is not sufficient to be used in real time applications.[36]	2010	[35]
"Bayesian-based model for a reputation system in vehicular networks"	Their model is capable to differentiate between trustworthy and untrustworthy vehicles	More simulations are needed to discover weaknesses and optimize the model to different scenarios as stated by the model's authors.	2015	[37]
"Location-based Security Authentication Mechanism for Ad hoc Network"	Security authentication mechanism is that resists against some common attacks	Digital signature may cause in revealing the node identity (i.e. privacy and position information)[9].	2012	[38]

as timing and transition attacks, but it does not maintain the desired privacy protection.

The authors in[16] shed some light in common attacks such as Jamming attacks, Sybil attacks, Selfish Driver attack, and misbehaving nodes that generate false information and wrong vehicle position information. They have paid special attention to DoS attacks, which are considered as a major threat that has impactful effect. They proposed a Malicious and Irrelevant Packet Detection Algorithm (MIPDA) to be used for analyzing and detecting the DoS attacks. They claim that their approach reduces delays overhead and thus enhance communication speed and security in VANETs. However, the authors do not show any experiments that reflect the efficiency of this algorithm in a simulated environment or real one.

The deployment of VANETs arise serious and new threats, as stated in[33]. Standardization of the VANET communication and railway communication systems has not adequately covered many security issues (i.e., Denial of Service attack and jamming attack). Anti-jamming approaches that presented to be used in conventional wireless networks are not adequate to be applied in VANET systems. A new anti-jamming strategy for VANET is proposed in[33]. Some security metrics are defined in[33] to measure how the defense mechanisms are effective and sufficient against jamming attacks. They have proved their claim through performing a simulation study.

Commonly, encryption techniques are used for the purpose of protecting information. The authors in[9] point out that the elliptic curve encryption algorithm (with 256 bits length) that was presented by[34], is more effective and sufficient than the Rivest-Shamir-Adleman encryption algorithm (RSA). However, their proposed algorithm is slow when used in signature authentication and encryption. Their Algorithm will cause considerable delay if used in applications that utilize a large scale network. Therefore, it is not sufficient for VANET systems.

Authors in[35] propose a secure data downloading protocol with privacy preservation for VANETs. They claim that their proposal allows a vehicle to get exclusive access to its requested data. Meanwhile, if an eavesdropper was able to compromise some RSUs, he would never be able to get any vehicles' private information. Therefore, privacy preservation will be achieved. The authors also demonstrated their proposal performance. However, as stated in[36], the proposal in[35] uses a single authority to authenticate the vehicles and issue private/public key pairs for them. Hence, the system has the bottleneck of generating all vehicles keys. In addition, the protocol proposed in[35] needs five rounds of communication to download the data. Therefore, it is not sufficient to be used in real-time applications.

A distributed detection system has been presented in[37]. Bayesian filter is used in this approach to sort out any malicious node (a vehicle). Their approach differentiates between trusted and distrusted vehicles. Their model performance is presented in terms of error rate and accuracy. However, as they have stated, further simulations have to be performed for discovering weaknesses and optimization. Moreover, it is highlighted that the change caused by merging new vehicles was not taking into account in their simulation environment.

In[9], intrusion detection system, security authentication, and data encryption have been discussed along with their limitations and challenges. A security authentication mechanism that resists against some common attacks is proposed in[38]. It is claimed that the digital signature technique is reasonable for security authentication processes. However, it can cause the node identity to be revealed. Seeking to solve such a problem, an anonymous signature authentication approach based on group/alias was proposed for VANET networks. But, still some limitations regarding communication and authentication costs and revocation of certificate are present[9].

Table 2 shows a summary of the related work section:

5. Conclusion

Intelligent transportation systems will become more widely used as a result of the rapid development in VANET systems. This kind of network has received potential attention in recent years due to their huge impact in enhancing traffic management systems and road safety. A significant amount of research is conducted to enhance numerous aspects of VANETs such as protocols, coverage, and other related aspects. Security in VANETs is given important attention, but the nature of this kind of networks seems to stand against reaching adequate and effective security. In this paper many proposals on how to enhance security in VANETs are surveyed and discussed. Although much development has taken place, security still lags behind. Up to date, there are no security standards that sufficiently meet all security requirements with fewer overheads. Furthermore, seeking to preserve privacy would add much more complications to achieving an adequate security model. Therefore, the research

door is wide open for further developments of sufficient security standards. The current major challenge is how to attain a balance between security, privacy, and usability while ensuring a fewer overheads. As a future work, it is suggested that research would focus on developing a security framework that take into consideration all or most of the aforementioned observations in order to come up with a sufficient security solution that attains or satisfies VANETs requirements.

6. References

1. Jabbarpour MR, Marefat A, Jalooli A, Noor RM, Khokhar RH, Lloret J. Performance analysis of V2V dynamic anchor position-based routing protocols. Wireless Networks. 2015; 21(3):911–29.
2. Malik V, Bishnoi S. Security threats in VANETS: A review; 2014.
3. Wu D, Cao J, Ling Y, Liu J, Sun L. Routing algorithm based on multi-community evolutionary game for VANET. Journal of Networks. 2012; 7(7):1106–15.
4. Mauri JL, Ghafoor KZ, Rawat DB, Perez JMA. Cognitive networks: Applications and deployments. CRC Press; 2014.
5. Li J, Lu H, Guizani M. ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. IEEE Transactions on Parallel and Distributed Systems. 2015; 26(4):938–48.
6. Sun J, Fang Y. Defense against misbehavior in anonymous vehicular ad hoc networks. Ad Hoc Networks. 2009; 7(8):1515–25.
7. Lin X, Lu R, Zhang C, Zhu H, Ho P-H, Shen X. Security in vehicular ad hoc networks. IEEE Communications Magazine. 2008; 46(4):88–95.
8. Ploßl K, Federrath H. A privacy aware and efficient security infrastructure for vehicular ad hoc networks. Computer Standards and Interfaces. 2008; 30(6):390–7.
9. Lu C, Hongbo T, Junfei W, editors. Analysis of VANET security based on routing protocol information. 2013 4th International Conference on Intelligent Control and Information Processing (ICICIP); 2013 Jun 9-11.
10. Jinyuan S, Chi Z, Yanchao Z, Yuguang F. An identity-based security system for user privacy in vehicular ad hoc networks. IEEE Transactions on Parallel and Distributed Systems. 2010; 21(9):1227–39.
11. Al-Sultan S, Al-Doori MM, Al-Bayatti AH, Zedan H. A comprehensive survey on vehicular ad hoc network. Journal of network and computer applications. 2014; 37:380–92.
12. Amoozadeh M, Raghuramu A, Chuah C-N, Ghosal D, Zhang HM, Rowe J, et al. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. IEEE Communications Magazine. 2015; 53(6):126–32.
13. Tyagi P, Dembla D, editors. Investigating the security threats in Vehicular ad hoc Networks (VANETs): Towards security engineering for safer on-road transportation. 2014 International Conference on Advances in Computing, Communications and Informatics ICACCI; 2014 Sep 24-27.
14. Soomro IA, Hasbullah H, Ab Manan J-l. Denial of Service (DOS) attack and its possible solution in VANET; 2010.
15. Mary SR, Maheshwari M, Thamaraiselvan M, editors. Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA). 2013 International Conference on Information Communication and Embedded Systems (ICICES); 2013 Feb 21-22.
16. Quyoom A, Ali R, Gouttam DN, Sharma H, editors. A novel mechanism of detection of Denial of Service attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA). 2015 International Conference on Computing, Communication and Automation (ICCCA); 2015 May 15-16.
17. Bibhu V, Roshan K, Singh KB, Singh DK. Performance analysis of black hole attack in VANET. International Journal of Computer Network and Information Security (IJCNIS). 2012; 4(11):47.
18. Najafabadi SG, Naji HR, Mahani A, editors. Sybil attack detection: Improving security of WSNs for smart power grid application. Smart Grid Conference (SGC); 2013 Dec 17-18.
19. Xiao B, Yu B, Gao C, editors. Detection and localization of sybil nodes in VANETs. Proceedings of the 2006 Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks; 2006.
20. Rahbari M, Jamali MAJ. Efficient detection of sybil attack based on cryptography in vanet. arXiv preprint arXiv:11122257; 2011.
21. Qu F, Wu Z, Wang F-Y, Cho W. A security and privacy review of VANETs; 2015.
22. Qingzi L, Qiwu W, Li Y, editors. A hierarchical security architecture of VANET. International Conference on Cyberspace Technology (CCT 2013); 2013 Nov 23-23.
23. Sumra IA, Ahmad I, Hasbullah H, Manan J-lBA, editors. Classes of Attacks in VANET. IEEE 2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC); 2011.
24. Rawat A, Sharma S, Sushil R. VANET: Security attacks and its possible solutions. Journal of Information and Operations Management. 2012; 3(1):301–4.
25. Sumra IA, Ahmad I, Hasbullah H, bin Ab Manan JL, editors. Behavior of attacker and some new possible attacks in

Vehicular Ad hoc Network (VANET). 2011 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT); 2011 Oct 5-7.
26. Rathore NC, Verma S, Tomar GS, editors. CMAC: A cluster based MAC protocol for VANETs. International Conference on Computer Information Systems and Industrial Management Applications (CISIM); 2010 Oct 8-10.
27. Bitam S, Mellouk A, Zeadally S. VANET-cloud: A generic cloud computing model for vehicular Ad Hoc networks. IEEE Wireless Communications. 2015; 22(1):96–102.
28. Wang M, Liu D, Zhu L, Xu Y, Wang F. LESPP: Lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication. Computing. 2014:1–24.
29. Dietzel S, Schoch E, Konings B, Weber M, Kargl F. Resilient secure aggregation for vehicular networks. IEEE Network. 2010; 24(1):26–31.
30. Molina-Gil J, Caballero-Gil P, Caballero-Gil C. Aggregation and probabilistic verification for data authentication in VANETs. Information Sciences. 2014; 262:172–89.
31. Palanisamy B, Liu L, editors. Mobimix: Protecting location privacy with mix-zones over road networks. 2011 IEEE 27th International Conference on Data Engineering (ICDE); 2011.
32. Tyagi AK, Sreenath N, editors. Location privacy preserving techniques for location based services over road networks. 2015 International Conference on Communications and Signal Processing (ICCSP); 2015 Apr 2-4.
33. Azogu IK, Ferreira MT, Larcom JA, Hong L, editors. A new anti-jamming strategy for VANET metrics-directed security defense. IEEE Globecom Workshops (GC Wkshps), 2013; 2013 Dec 9-13.
34. Enge A. Elliptic curve cryptographic systems. Handbook of Finite Fields; 2013. p. 784–96.
35. Yong H, Jin T, Yu C, Chi Z, editors. Secure data downloading with privacy preservation in vehicular ad hoc networks. 2010 IEEE International Conference on Communications (ICC); 2010 May 23-27.
36. Zhang L, Wu Q, Qin B, Domingo-Ferrer J, Liu B. Practical secure and privacy-preserving scheme for value-added applications in VANETs. Computer Communications. 2015; 71:50–60.
37. Begriche Y, Khatoun R, Khoukhi L, Chen X, editors. Bayesian-based model for a reputation system in vehicular networks. 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC); 2015 Aug 5-7.
38. Li C, Wang Z. Location-based security authentication mechanism for ad hoc network. Parameters. 2012; 1:2.