VANET Security Review: Application Side

[1]Musa Balta, [1]Kevser Ovaz and [1]Ibrahim Ozcelik
[1]Faculty of Computer and Information Sciences, Department of Computer Engineering Sakarya University, Turkey

Abstract

Nowadays, Vehicular ad hoc networks that is a subset of MANET, has become promising research area among car industry and academic environment. It is used to provide communication between vehicle (onboard unit) to vehicle or vehicle to infrastructure (roadside units).The main aim of VANET is enhancing road safety, providing traffic efficiency and also infotainment. But as the other networks, VANET has also challenges about security especially authentication, privacy and attacks against resources. This paper presents a survey that categorizes security issues, challenges and attack types according to different VANET applications.

Key words: VANET, security, DoS attacks, applications

1. Introduction

Vehicle Ad Hoc Network (VANET), subset of Mobile Ad Hoc Network (MANET), is the most promising research field in wireless networks. They have frequent dynamic topology changes and sudden connection loses, therefore they represent significant importance in life threatening circumstances. VANET is usually classified in second generation dedicated short-range communication (DSRC) and use 5.9 GHz band and 75 MHz bandwidth with IEEE 802.11p network interfaces [1-4]. Vehicular networking mainly objected to provide comfort, safety, instant communication between vehicles and their other environments. Road safety, traffic congestion and data dissemination requirements also yielded developments in VANET systems [2-6]. In Figure [1], a general VANET structure is shown.

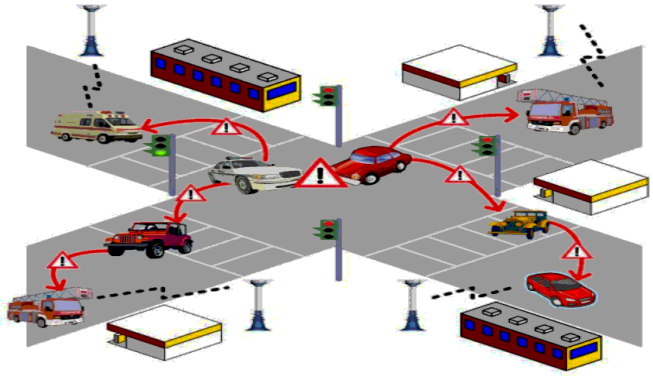

Figure 1. Vehicular Systems [4]

*Corresponding author: Address: Faculty of Computer and Information Science, Department of Computer Engineering, Sakarya University, 54187, Sakarya TURKEY. E-mail address: mbalta@sakarya.edu.tr, Phone: +902642955646

However, instead conventional applications state of art solutions need to be adapted in order to meet with the demands of passengers, vehicle drivers, pedestrians. In this orientation, many applications, architectural models, algorithms are introduced recently. These solutions are mainly traffic safety, traffic efficiency and infotainment directed as they represent major categories in VANET [7,8]. As an example, co-operative merging assistance, emergency warning, lane change assistance, pre-crash sensing are considered in road safety applications. In this category alarms –calling to ambulance, warnings –displaying on HMI (Human Machine Interface) that provides connection to machines and actions –emergency braking could be taken. Traffic efficiency and management applications include speed assistance or navigation based applications [9,10]. This category aims to give comfort during driving. The last group, infotainment is mostly related with social applications such as providing internet services, interest notifications.

VANET systems could be formed of vehicles, drivers, pedestrians, environmental units like road side units (RSU) and remote servers. Each element has numerous hardware or software stack such as wireless adaptors, OBUs, data store or computing units, HMI, microprocessors, bus systems, sensors, actuators and other network components [1,2]. This integration is shaped with architectural models and eventually enables communication with data exchange between VANET nodes. Key point here is presenting a high level of communication with a low error rate since critically state of affairs is existed. To illustrate a communication pattern, imagine sensors placed along the highway detect rain on that area thus gives information to the drivers. Here, RSU receives input from sensors integrated on it and transfers this data to the passing drivers. The first transmission of weather condition and location data completes here and receiving vehicles continue dissemination during their way to other vehicles or RSUs. In all scenarios, transmission quality, scalability, bandwidth optimization, dynamic topology changes, attacks, limited resources, device discovery, incorporation of components are mostly faced issues [11,12].

As mentioned above, plenty of hardware and software integrated additional components may exist in VANETs. They are embedded and eventually work together in harmonic way however, having wide diversity of elements also brings other challenges like security. It is one of the most considering challenge in the last few years since security deficiencies may cause deadly results in VANET systems. There is a conflict that vehicular communication or smart transportation technologies are peaking but simple security holes keep absence. Well-known attacks such as denial of service, man in the middle, spoofing, info manipulation done in other fields can be implemented in these systems as well.

Next section discusses about security requirements in VANET. Third section explains known attack types in VANET and fourth one classifies attacks on application basis with introduced solutions. Finally last section presents open research fields of this area.

2.Security Requirements

Before starting to talk about security issues of VANET, it is important to address the security requirements. As in the other networks, VANET systems also need some security requirements to provide secure communication. The main security requirements are defined as authentication, privacy, availability, integrity and non-repudiation [13-15].

2.1.Authentication

From source to destination node, every message must be authenticated during the communication in VANET. There are several ways to authenticate the message in VANET. One of them is key management. To provide the secure communication, vehicles will assign a private key in every message. After receiving the message by destination vehicle, it is checked for accuracy of key.

The other most known way of providing security via authentication is using digital signature. Signing each message with ECC (Elliptic Curve Cryptography) offers effective solution for vehicular systems. It is used especially against to Sybil attacks [15-21].

2.2. Privacy

During the data transmission between RSU and RSU or RSU and OBU, messages may consist of some specific information besides communication info. These sensitive information may belong to driver's personal information like as driving license, age, name etc. or belongs to car's trip path, speed etc [17-20].

To solve this problem, temporarily keys that is stored in TPD (Tamper Proof Device) could be used. It will be changed periodically. On the other hand, ELP (Electronic License Plate) can be used to hide the real identity of the driver [19].

2.3.Avaliability

Because of being real-time obligation, sometimes the system becomes vulnerable to DoS and Sybil attacks. During the communication process, message cannot be secure enough in order to be fast. Thus an attacker may collapses all data [19,20].

Increasing message size in source node or parsing messages to pieces in middle nodes generally solves this availability problem in VANET. Using an effective routing protocol (like as AODV-Ad hoc on Demand Vector) also can be another solution for availability [17-20].

2.4. Integrity

Integrity controls the message that was changed or not during the communication. False or altered data may cause car crash or traffic density. For example, an attacker changes coordinates of an accident in highway, other cars will set their speed, direction etc. to the fake coordinate and ıt may makes driver in dangerous situation [20,21].

2.5. Non-Repudiation

It will provide an control mechanism to exposure identity of attacker, even after an attack. The main goal of non-repudiation is collecting evidence, maintaining communication and making available area against to VANET crimes. It makes this control via TPD saving vehicle's speed, id, direction etc. in vehicle [19,20].

2.6. Confidentiality

Unlike privacy, confidentiality is used for group communication in VANET. In addition to the privacy, to keep driver's information in secret, this security requirements also uses group signature simultaneously [16-19].

2.7. Real-timeliness

Real-time constraints is most important thing in vehicular systems. Because of node's high mobility, communication between nodes can drop easily. To get response in real-time from destination to source, unfortunately sometimes real-timeliness make security get into second plan [17,18].

3.Well-known Attack Types for VANET

In this section, well-known attack types for VANET will be explained. As the others, VANET systems also can be exposed to the attacks. But unlike the other networks, attack types specialize according to features of VANET like as dynamically topology change, limited bandwidth and real-time constraints etc. Although VANET is a subset of MANET, workout of attacks are not same but similar.

3.1. Denial of Service Attacks

It is the most known damaging attack type in networks. Basically, DoS attacks have two main goal. First goal of DoS attacks is to consume bandwidth of communication medium and the second one is to prevent vehicles to access to network services. In the below, two dangerous types of DoS attacks for VANET in literature will be explained [19-28].

3.1.1.Wormhole attacks

In this kind of attacks, a high speed connection is established between two remote nodes as shown in Figure 2. Legitimate vehicles in transmission range of this two remote nodes (X and Y) use this connection for transferring their data. An attacker can drop the data over the connection [21-29].

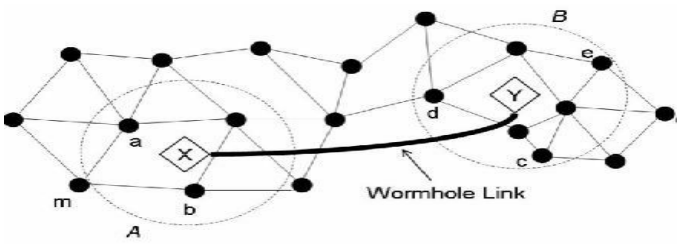

Figure 2. Wormhole attack [22]

3.1.2.Blackhole attacks

In this attack type, a malicious node in the middle of the communication medium present itself as a central node and drops packets [22-27]. In Figure [3], there is a demonstration of Blackhole attacks.

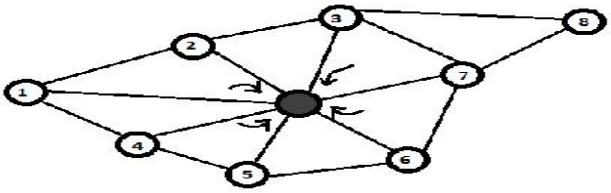

Figure 3. Blackhole attack [22]

3.2.Sybil Attacks

In this attack type, the main goal is to confuse the normal vehicles. Attacker creates a huge number of pseudonymous [22-25]. Towards these fake messages, vehicles are obligated to change their direction or speed, thus undesirable traffic conditions may occur as shown in Figure [4].

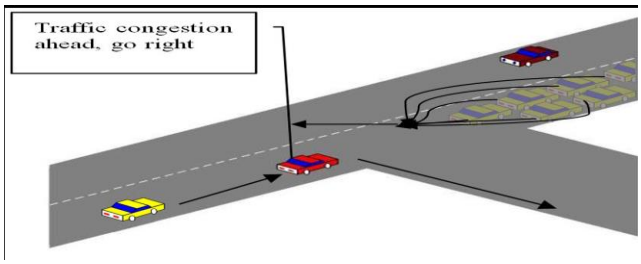

Figure 4. Sybil Attack [21]

3.3.Eavesdropping Attacks

It is an attack type which is used against confidentiality. To success in this kind of attacks, attacker must locate in a vehicle or near RSU and then listen the communication medium and collapse the related data. To prevent eavesdropping attacks, message encryption can be used [20-24].

3.4. Impersonation Attacks

Attackers keep in secret their car id in impersonation attacks and they pretend to be another vehicle. Attacker obtain id of the letigate users by using IP and MAC spoofing. When they success to obtain id, they can send false message for example changing coordinates of traffic cash. With using certificate system, this kind of attacks can be prevented [20-24].

3.5. Alteration Attacks

Attacker listens the communication between vehicles or vehicle-RSU, when he finds available information for himself, he can alter the data as he desires [20-24].

3.6. Replay Attacks

During establishing the connection between two vehicles, attacker obtains beginning packages of transmissions. VANET architecture doesn't prevent this kind of attacks. The main goal of this attacks is to consume bandwidth [21-24].

3.7. Location Falsification

In this attack, attacker changes coordinates of car crash in urban city or highway. When a litigate user see a car accident, he broadcasts fake GPS (Global Positioning System) coordinates and so other vehicles arrange themselves according to the new fake coordinate and traffic jam or accident may occur suddenly [20,21].

Attacks described above are performed by different attacker profiles. These profiles are generally described as follows;

- **Outsider & insider;** outsider attackers are nodes not be authenticated in vehicular system. Generally, they locate near RSU and listen the communication medium continuously to get information. Unlike outsider, insider attacker is an authenticated nodes in vehicular system, they behave a letigate vehicle until attack [17-20].
- **Active & passive;** active attackers send broadcast messages continuously to damage to other nodes. Passive attackers don't sent messages every time, they wait correct time to attack. For example, while a car accident information messages is in the communication, a passive attacker can attack to drop these messages [17,18].
- **Malicious & rational;** malicious attackers can attack any nodes or only communication medium with DoS attacks randomly, they have no specific destination. But rational attacker behaves carefully in their attacks and also they determine a specific victim [18].

4. Classification of Attacks

This section presents us a classification table of attacks according to security requirements and VANET application areas that are mentioned in introduction section of the study. These VANET application areas in Table [1] were prepared by getting information from academic studies, for instance, in study [23], it is mentioned that DoS attacks affects traffic safety. And the Table [1] also gives the most known solutions for these attacks [27-31].

Table 1. Classification of VANET Security Attacks

Nu	Attack Type	Security Requirement	Application Area	Authors and Ref. Nu.	Solution
1	DoS attacks	Authentication Privacy	Traffic safety	Raya et. al [23-31]	A detailed threat analysis and security architecture ▸ Digital signature ▸ Certification authorities ▸ Key management
2	DoS attacks	Authentication	Traffic safety	Frank Karl et.al [32]	Cluster analyzing
3	Alteration attacks	Confidence	Traffic efficiency	Nai-Wei et al. [33]	Dynamics event-based repudiation system
4	Impersonation attacks	Authentication Privacy	Traffic safety	Hung lu et al. [34]	Identity based encryption
5	Sybil attacks	Privacy	Traffic efficiency	QianhongWu etal.[35]	Message linkable group signature
6	Impersonation attacks	Privacy	Traffic efficiency	Sun et al. [36]	Cryptosystem which is identity based
7	Sybil attacks	Non-repudiation Privacy	Traffic safety	X.Wang et al. [37]	Anonymous authentication protocol-based on Certificate-based Cryptography
8	DoS attacks Sybil attacks	Authentication Non-repudiation Privacy	Traffic efficiency	Klaus et al. [38]	Presents a security architecture: ▸ Basic elements of security(PKI) ▸ Single-hop security ▸ Multi-hop security
9	DoS attacks	Integrity	Traffic safety	Dhurandher et al. [39]	Repudiation and plausibility check algorithm
10	Sybil attacks	Privacy	Traffic safety Traffic efficiency	Golle et al. [40]	General approach to assessing the validity

Conclusion

With new developments in the vehicle industry, vehicles need to communicate each other or with road-side units. For this reason, Vehicular ad hoc networks have become promising research area for last decades. Communicating has become a necessity for vehicles to avoid of accidents, increase traffic efficiency and provide infotainment. As in other networks, vehicular networks

also can be exposed to the attacks like as DoS attacks, impersonation attacks etc. Because of this, security has become more important in research studies.

In this study, comprehensive review of VANET security is explained from different aspects like as security requirements and solutions in literature for these requirements, after giving basic information about vehicular networks.

Finally, vehicular networks will hold an important place in our life. So there will be many academic and commercial studies about VANETs. Security routing algorithms and smart cities with VANET are some of the open research areas for vehicular networks.

References

[1]IEEE 802.11, IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std. IEEE 802.11, version 2007, 2007.
[2]IEEE 802.11p, Amendment to Standard for Information Technology- Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications-Amendment 7: Wireless Access in Vehicular En- vironment, IEEE Std. IEEE 802.11p, version 2010, 2010.
[3]IEEE1609.2, "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages," July 2006.
[4] 1609.4-2010 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE)--Multi-channel operation, 1–89.
[5]Aijaz, A., Bochow, B., Dötzer, F., Festag, A., Gerlach, M., Kroh, R., et al. (2006). Attacks on Inter-Vehicle Communication Systems - An Analysis. International Workshop on Intelligent Transportation. Hamburg, Germany: IEEE Communications Society.
[6]Identify intelligent vehicle safety applications enabled by DSRC, US National Highway Traffic Safety Administration 2005.
[7]Morgan Y L (2010). Managing DSRC and WAVE Standards Operations in a V2V Scenario, International Journal of Vehicular Technology, vol 2010.
[8]P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, J.-P. Hubaux, Secure vehicular communications: design and architecture, IEEE Communications Magazine, vol. 46, no. 11, pp. 100-109, November 2008
[9]Grafling S, Mahonen P et al. (2010). Performance evaluation of IEEE 1609 WAVE and IEEE 802.11p for vehicular communications, 2010 Second International Conference in Ubiquitous and Future Networks (ICUFN).
[10]Ludovic Apvrille, Rachid El Khayari, Olaf Henniger, Yves Roudier, Hendrik Schweppe, Herve Seudié, Benjamin Weyl, and Marko Wolf. Secure automotive on-board electronics network architecture. In FISITA'10, World Automotive Congress, 30 May-4 June, 2010, Budapest, Hungary, 2010.

[11]K. Plößl, T. Nowey, C. Mletzko, Towards a security architecture for vehicular ad hoc networks, Proceedings of ARES 2006, IEEE Computer Society, 2006.
[12]Yi Qian; Moayeri, N., "Design of Secure and Application-Oriented VANETs," Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE , vol., no., pp.2794,2799, 11-14 May 2008.
[13]Mershad, K.; Artail, H., "A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks," Vehicular Technology, IEEE Transactions on , vol.62, no.2, pp.536,551, Feb. 2013.
[14] Mehmood, R., Nekovee, M.: Vehicular Ad hoc and Grid Networks: Discussion, Design and Evaluation. In: Proc. of the 14th World Congress on Intelligent Transport Systems, p. 8 (2007)
[15] Karagiannis, G., et al.: Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions. IEEE Communications Surveys & Tutorials
[16] Lee, K.C., Lee, U., Gerla, M.: Survey of Routing Protocols in Vehicular Ad Hoc Networks in Car2Car communication consortium (2010)
[17] http://www.ics.uci.edu/~keldefra/MANET.htm
[18] Gillani, S., Shahzad, F., Qayyum, A., Mehmood, R., A Survey on Security in Vehicular Ad Hoc Networks, Nets4Cars/Nets4Trains 2013, LNCS 7865, pp. 59–74, 2013. Springer-Verlag Berlin Heidelberg 2013
[19] Fuentes, J., Gonzales-Tablas, A., Ribagorda, A., Overview of security issues in Vehicular Ad-hoc Networks, Handbook of Research on Mobility and Computing (2010)
[20] Engoulou, R., Bellaiche, M., Pierre, S., Quintero, A., VANET security surveys, Computer Communications 44 (2014) 1–13, Elsevier
[21] Samara, G., Al-Salihy, W., Sures, R., Security Analysis of Vehicular Ad Hoc Networks (VANET), 2010 Second International Conference on Network Applications, Protocols and Services, DOI 10.1109/NETAPPS.2010.17
[22] Patel, M., Shah, Ms., Glance over VANET, Attacks over VANET and theirIDS approaches, ©2014 IJIRT | Volume 1 Issue 2 | ISSN: 2349-6002, Internatıonal journal of ınnovatıve research ın technology
[23] Raya, M., Hubaux, J.-P.: Securing vehicular ad hoc networks. Journal of Computer Security, 39–68 (2007)
[24] Raya, M., Papadimitratos, P., Hubaux, J.P.: Securing Vehicular Communications. IEEE Wireless Communications 13 (2006)
[25] Raya, M., Pierre Hubaux, J.: The security of VANETs. In: Proceedings of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks (2005)
[26] Raya, M., Papadimitratos, P., Hubaux, J.-P.: Securing vehicular communications. IEEE Wireless Communications Magazine 13(5), 8–15 (2006)
[27]Karami, A., Zapata,M. "A hybrid multiobjective RBF-PSO method for mitigating DoS attacks in Named Data Networking", Neurocomputing 151: 1262-1282 (2015)
[28]Darwish, M., Ouda, A., Capretz, L., "A cloud-based secure authentication (CSA) protocol suite for defense against Denial of Service (DoS) attacks", in press, Journal of Information Security and Applications, Elsevier (2015), http://dx.doi.org/10.1016/j.jisa.2014.12.001.
[29]Özçelik, İ., Brooks, R. "Deceiving entropy based DoS detection", Proceedings of SPIE - The International Society for Optical Engineering, Vol:9091,ISBN: 9781628410280,Jan 1 2014
[30]H. Hasbullah, I.A. Soomro, J.-L. Ab Manan, Denial of service (DOS) attack and its possible solution in VANET, WASET, 2010.

[31]E. Fonseca, A. Festag, A survey of existing approaches for secure ad hoc routing and their applicability to VANETS, NEC Network Laboratories, 2006.
[32] F. Kargl, Z. Ma, E. Schoch, Security engineering for VANETs, in: 4th Workshop on Embedded Security in Cars, 2006.
[33] Nai-Wei, L., Hsiao-Chien, T.: A reputation system for traffic safety event on vehicular ad hoc networks. EURASIP Journal on Wireless Communications and Networking (2009)
[34] Lu, H., Li, J., Guizani, M.: A novel ID-based authentication framework with adaptive privacy preservation for VANETs. In: Computing, Communications and Applications Conference (ComComAp), pp. 345–350. IEEE (2012)
[35] Wu, Q., Domingo-Ferrer, J., Gonz´alez-Nicol´as, U.: Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications. IEEE Transactions on Vehicular Technology 59(2), 559–573 (2010)
[36] Sun, J., et al.: 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)
[37] Wang, X., Liu, T., Xiao, G.: Certificate-based anonymous authentication protocol for vehicular Ad-hoc network. IETE Technical Review 29 (2012)
[38] Klaus, et al.: A privacy aware and efficient security infrastructure for vehicular ad hoc networks. Computer Standards & Interfaces 30, 390–397 (2008)
[39] S.K. Dhurandher, M.S. Obaidat, A. Jaiswal, A. Tiwari, A. Tyagi, Securing vehicular networks: a reputation and plausibility checks-based approach, in: GLOBECOM Workshops (GC Wkshps), IEEE, 2010, pp. 1550–1554.
[40] P. Golle, D. Greene, J. Staddon, Detecting and correcting malicious data in VANETs, in: Presented at the Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, Philadelphia, PA, USA, 2004.