

Securing Intelligent Vehicular Ad Hoc Networks: A Survey

Wedad Ahmed and Mourad Elhadeif^(✉)

College of Engineering, Abu Dhabi University, Abu Dhabi, UAE
mourad.elhadeif@adu.ac.ae

Abstract. Vehicular ad hoc networks (VANETs) is an intelligent transportation system that provides wireless communication between vehicles and different objects in the road to increase efficiency and human safety using various applications. However, all this attractive features of VANETs will increase security risks and privacy problems if security attacks is not studied and analyzed thoroughly and completely. This paper discuss VANETs' features, and structures. In addition, it list different security attacks and provide a unique classification for them. Finally, it goes through security architectures and schemes used in VANETs.

Keywords: Vehicular ad hoc networks (VANETs) · Security attacks
Countermeasures

1 Introduction

Vehicular ad hoc network (VANET) is an intelligent transportation system in which vehicles communicate with each other to improve road safety and efficiency. VANET architecture depends on a distributed and autonomous system and is made up of the vehicles themselves without the support of a fixed infrastructure for data routing. Each communicating vehicle act as a wireless router allowing vehicles within a particular range to form a network. In VANET, each vehicle broadcast information about itself and about surrounded road conditions (beacons) to other vehicles. VANET consists of three major components namely, trusted authority, fixed road side unit, and on board units mounted on the moving vehicles. The architecture of VANETs falls within three categories (Fig. 1): WAVE base Wi-Fi, pure ad hoc, and hybrid. WAVE base Wi-Fi structure used for Internet connectivity, collecting vehicle and traffic information, and routing purposes. Ad Hoc Structure: is formed by vehicles themselves and roadside wireless devices communicating with each other to form a network. A hybrid architecture: is a combination of the previous two networks [2, 7, 11]. The objective of this paper is provide a comprehensive survey of security in VANETs, and the various countermeasures that have been developed to solve security threats that are specific to VANETs.

This work is supported by ADEC Award for Research Excellence (A²RE) 2015 and Office of Research and Sponsored Programs (ORSP), Abu Dhabi University.

The rest of the paper is organized as follows. Section 2 discuss a classification of attackers. Security attacks taxonomy is detailed in Sect. 3. In Sect. 4, we present the basic security infrastructure and some algorithms for solving specific attacks in VANETs. Finally, Sect. 5 concludes and presents future research directions.

2 VANETs Security

Due to the ad hoc nature of VANETs, wireless communication is exposed to many attacks targeting data privacy, confidentiality and integrity which limit the applicability of many application in VANETs. Sensitive data information about vehicles and their drivers transmitted over a VANET shows high need of security. This is vital to ensure proper operation of the network and to save human lives. Solving security issues in VANET is challenging due to VANETs' huge and scalable network size that results from instant arrivals and departure of cars, and random speed of the vehicle [9, 14].

In [1], La and Cavalli classified the attackers depending on who they are, their goals of making the attack, their attack impact on VANETs, and whether their attacks have boundaries or not. The following are attackers categorization based in four parameters.

- **Insider vs. Outsider:** Insider is an authenticated member of VANETs while the outsider is an attacker who is not authenticated.
- **Malicious vs. Rational:** Malicious attacker have no personal

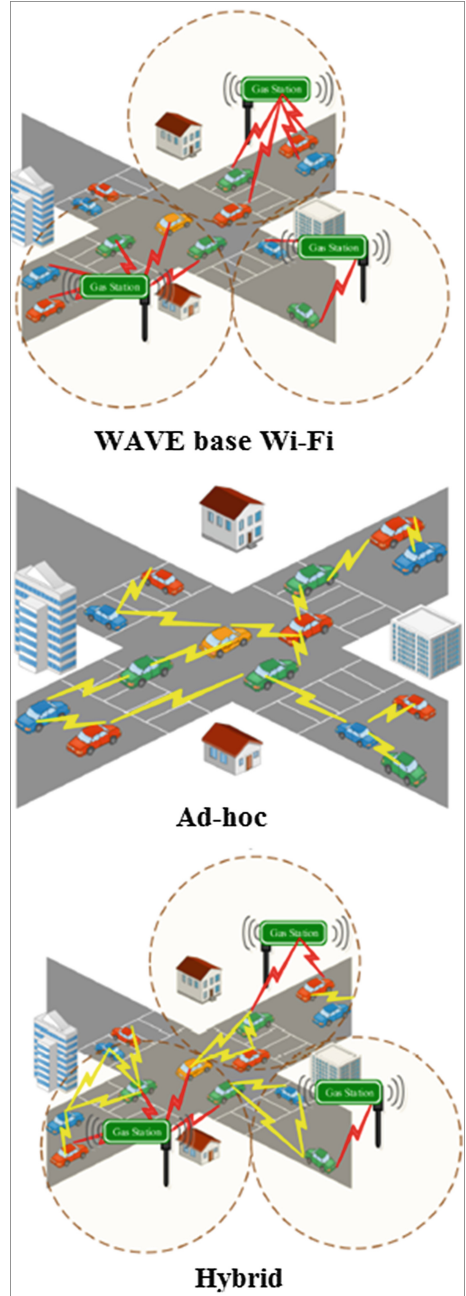


Fig. 1. Communication architectures of VANETs [6].

benefit from the attack and their goal is to make chaos while rational attacker lunches an attack to gain benefits.

- **Active vs. Passive:** Active attack can generate new packets or damage exiting packets in the network while passive attacker only eavesdrop the wireless communication.
- **Local vs. Extended:** Local attackers have a specific scope of their attack range even if they compromise several entities; while extended attackers have several entities that are extended across the network.

3 Security Attacks on VANETs

There are many types of attacks that could happen for different purposes in VANETs. An attacker could use many techniques to perform an attack. Some attacks target packets where attackers drop, delay, or send data packets to unintended destination. Many attacks in VANETs goes under sending falsified or altered data to other vehicles such as illusion attack and bogus information attack. This is done for different purposes either to create chaos in the network or to gain benefit. In addition, attacks could target different technologies used in the network such as tampering with VANETs’ protocols or signal strength. Attacks could merely be an eavesdropping in communication medium to analyze messages transmitted between vehicles or they could be active in which existing data are changed or new data packets are generated.

Many researches have different classification of attacks. Mokhtar and Azab have classified security attacks based on the network layer it target, physical layer, link layer, network layer, transport layer, application layer [4]. Sumra et al. proposed five different classes of attacks [12] namely monitoring attack, social attack, timing attack, application attack, network attack. In this paper, we have our own classification according to five different criteria as shown Fig. 2. The first one is for attackers that use ID in order to lunch their attacks. A malicious node can expose, steal, forge, or duplicate the ID of authentic nodes. Second type are attacks that depends on sending false or modified

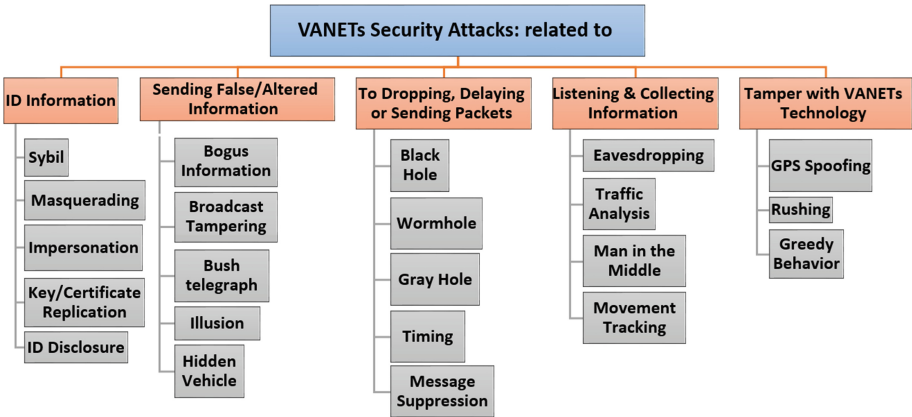


Fig. 2. Attacks taxonomy

messages and information. The third type is all about delaying or dropping packets or send them to different destination. The fourth type is attacks that intercept and/or collect information communicated in the medium channel. The last one is for attacks that corrupt VANET system.

3.1 Attacks Related to ID Information

Various attacks target the ID information, and can be classified as follows.

- **Sybil attack:** A malicious node forges the ID of different vehicles to declare that it is a several vehicles. Then the attacker broadcast numerous messages with different IDs to other vehicles. This result in a deception of having traffic jam [2].
- **Masquerading attack:** The attacker use fake or steal the identity of a valid user. Since it has the privileges of an authenticated user inside VANET, the attacker can do many malicious actions. One scenario is that the attacker pretend to be an emergency vehicle to deceit valid nodes to slow down their speed, or to request priority lane [2].
- **Impersonation attack:** The attacker spoof the MAC and IP addresses of legitimate nodes to gain their benefits. The attacker send fabricated messages on behalf of those nodes to create chaos or accidents [1].
- **Key/Certificate replication:** In this attack, the attacker uses duplicate keys and certificates of other vehicles as its authentication proof to confuse Trusted Authority and to make it hard to identify which vehicle is the legitimate one [2].
- **ID Disclosure:** The attacker goal is to expose the ID of surrounded nodes and use it for multiple purposes. For example, when a malicious node sends a virus to other nodes so that they periodically report their IDs and locations. In addition, these victim nodes could report location information of other surrounded nodes to the attacker [1].

3.2 Attacks Related to Sending False/Altered Information

Other forms of attacks target the information carried by the exchanged messages, and can be classified as follows.

- **Bogus information:** Also called *Message spoofing attack*, is to disseminate bogus information (messages) to deceive and affect the decision of other nodes in the network for example, an attacker may transmit a “Heavy traffic conditions” message so that other vehicles change their route and clear the way. *Message Tampering/Modification/Alteration attack* also can be classified under this category where information is modified to bring about unauthorized effect [1–4].
- **Broadcast tampering attack:** Internal attackers broadcast false or bogus messages about security alerts to cause damage and affect the overall performance of the network. This can lead to severe accidents and threaten human lives [2, 3].
- **Bush telegraph:** is a developed form of the bogus information attack. The difference in this case is that the attacker controls numerous entities across several wireless hops. The attack technique is to send small false errors with the tolerance

margin of a packet. As the packet is transmitted across hops, the error is incremented. Eventually this yields to bogus information [1].

- **Illusion attack:** In this attack, the adversary deceives intentionally the sensors on his own car to produce wrong sensor readings. As a result wrong messages are broadcast in the network and inappropriate decisions and behaviors are taken by vehicles leading to accidents, traffic jams, and other problems [1].
- **Hidden vehicle:** The attacker in this attack sends false position information to near nodes. The attacker persuades neighboring nodes that its location is the best to send safety messages to other vehicles in the area, however, the attacker then keeps silent or may send false information to other nodes [8].

3.3 Attacks Related to Dropping, Delaying or Sending Packets to Unintended Destination

The third class of attacks targets the transmitted messages, and includes the following classes.

- **Black hole attack:** In this attack, the attacker sends data packets to its unintended destination or may drop packets. The Black hole is the area where the network traffic is rerouted. Black holes happen in two cases, either there is no node to redirect the traffic or there is a malicious node that refuse routing that packet. In VANETs, every node is considered a router; a black hole attack could be in the form of dropping the packets whenever it goes to a malicious node or forwarded it to a wrong node [1].
- **Wormhole (tunneling) attack:** In this attack, the attacker sends data packets to its unintended destination. Wormhole attack done by one or more attackers setting in faraway parts in the network. Those attackers capture data packets by overhearing them in the wireless environment and create extra communication channel called a tunnel along existing data routes making a wormhole in-between the legitimate nodes of the network. This tunnel is used to disrupt the data packets' routing, gain unauthorized access, and/or create denial of service attack [1, 2, 4].
- **Gray hole attack:** A misbehaving node deceives the network by agreeing to forward packets but it sometimes drops them for a while and then switches to its normal behavior [1].
- **Message suppression attack:** An attacker selectively drops packets from the network, however, it may use them again when required. Those packets may hold critical information that could prevent collisions [3].
- **Timing attack:** The opponent aims to delay the time critical applications related messages that it should be retransmitted to other vehicles. This may result in accidents for vehicles that receive the message in later time. For example, a malicious node receives a message indicating that there is an accident between car A and car B. A malicious vehicle adds some time slots to the message so that other cars cannot change their route because they received the message when they have already reached the accident position [1].

3.4 Attacks Related to Listening and Collecting Information

Attacks that intercepts the information can be classified as shown below.

- **Eavesdropping attack:** The attacker eavesdrops the wireless communication channel. Through this attack, the protected information is disclosed to unauthorized users in VANETs which leads to information misuse such as identity theft and collection of location data of a target vehicle that can be used for tracking vehicles [2].
- **Traffic analysis attack:** The goal of this attack aims at collecting information by observing and analyzing the frequency, duration of messages being sent in the network. The attacker then tries to utilize this data by extracting knowledge and valuable information from these messages and uses them for its own personal purposes [2].
- **Man in the middle attack (MiMA):** A malicious node intercepts the communication between two nodes by pretending to be each of them and reply to each of them using false information [1].
- **Movement tracking:** This attack done by an attacker that access and expose a vehicle's information such as geographical position and speed. These data are then used by an attacker to track the vehicles, predict their future behavior, and affect their transmission performance [4].

3.5 Attacks that Tamper with VANETs Technology and Infrastructure

Various attacks have been developed to corrupt VANETs infrastructure, and can be classified as follows.

- **GPS spoofing:** A location table is maintained in the GPS satellite, which contains the geographic location information about all the vehicles in the VANETs. An attacker uses GPS satellite simulator to produce signals that are stronger than those produced by the actual satellite system. Nodes read falsified GPS coordinates and position themselves in different locations [2].
- **Rushing attacks:** is an attack used against on-demand ad hoc network routing protocols such as ARAN. Attacking ARAN result in inability to discover routes longer than two hops. This type of attack makes a malicious vehicle have a higher probability of finding routes due to its ability to send route requests more quickly than legitimate users. At the end, this attack results in denial of service (DoS) when used against all on-demand ad hoc network routing protocols [4].
- **Greedy behavior attack:** In this attack, the attacker exploits the weakness of the message authentication code (MAC) technology and gets an access to the wireless medium for getting more bandwidth and shortening its waiting time at the cost of other vehicles. This attack affects the availability requirement and it is considered a common DoS attack and it can be done by an authenticated users who do not respect rules of MAC in VANETs [5].

3.6 Miscellaneous Attacks

Various other forms of attacks can be categorized as follows.

- **Malware and spam attack:** In this attack, a malware can be penetrated into the VANETs via software components installed to operate the OBUs and RSUs. VANETs may get infected when an OBU/RSU performs software updates. Malware may lead to the disruption of ordinary functionality of VANETs [1, 2].
- **Social attack:** This attack targets the emotions of drivers by sending unethical messages. The primary aim of the attacker is to affect the driving performance of the vehicle by making drivers upset and react in an annoyed manner [2].
- **Jamming attack:** A severe DoS where an attacker, or victimized node, emits radio frequency signal and flushes the communication channel with unnecessary packets in order to break down the network and makes its services unavailable to authentic users [10].

4 Security Schemes for VANETs

There are many security techniques being introduced by researchers for the deployment of the security requirements in VANETs. Below we list the basic security infrastructure and some algorithms for solving specific attacks.

4.1 Public Key Infrastructure

Public Key Infrastructure (PKI) provides authentication, encryption and non-repudiation. Authentication is considered to be the first line of defense against any attacks. Authentication insure that nodes are the entities they claim to be. Encryption used to maintain confidentiality and privacy. Furthermore, PKI provides digital signature to ensure non repudiation. However, VANETs have their own special characteristics and ordinary PKI with long confirmation time cannot meet the needs of VANETs security. Digital signature algorithms used to secure VANETs have to meet two standards: (i) fast execution pace of signature generation and verification operation, and (ii) small key size. Elliptic Curve Cryptography (ECC) is asymmetric encryption technique that create faster, shorter, and more efficient key sizes which makes it suitable for VANETs. Furthermore, privacy is a critical issue in VANETs. Many VANETs application require location information, and hence, attackers can gather these information to track movement patterns of vehicles. Those details could be used for malicious purposes. In order to preserve privacy, verification routines and validation processes have to be unknown using pseudonymous confirmation plans [13, 17].

4.2 Hybrid Cryptography Method

Karimireddy and Bakshi in [14] have suggested an approach to secure communication in VANETs based on a combination of public key and private key cryptographic method (hybrid) using RSA and AES (Advanced Encryption Standard) cryptographic algorithms. Their method resolve the limitation of each cryptography type; combining the advantage of symmetric cryptography which is faster and consume less resources as well as asymmetric cryptography that provide strong security in order to ensure

non-repudiation, authentication, and confidentiality. Initially, the private data will be encrypted using the RSA algorithm, then the cipher text will be given as an input to AES algorithm. The cipher text is encrypted twice to increase the difficulty of decrypting the message by an attacker.

4.3 Enhanced Voting Algorithm

Mohamed et al. [15] proposed an enhanced voting algorithm (EVA) for detecting malicious or victimized vehicle(s) that sends jamming messages. In jamming attacks, there could be many collaborating attackers that prevent other vehicles from communicating safety messages and send their own compromised messages. EVA goes through two stages: investigation and voting stage. The first stage distinguishes whether a road vehicle is a victim or a misbehaving node using hybrid jammer detection algorithm (HJDA) as described in [16]. The second stage is voting where only vehicles that pass investigation stage could add their values in the voting set. Thus using EVA, any decisions are based on values that only come from a vehicle that is neither a malicious nor a victim.

5 Conclusion

VANETs is an interesting field that promises to deliver effective solutions to mitigate traffic jam and road accidents. However, due to the high mobility of nodes and the wireless nature of communication, VANETs are subjected to many attacks that need to be examined carefully in order to make it safely applicable in the near future. In this paper, we classified the different security attacks and described various security schemes and algorithms that can detect jamming and data falsification attacks. Future work will focus on DoS attacks and their countermeasures.

References

1. La, V.H., Cavalli, A.R.: Security attacks and solutions in vehicular Ad Hoc networks: a survey. *Int. J. Ad Hoc Netw. Syst.* **4**(2), 1–20 (2014)
2. Azees, M., Vijayakumar, P., Deborah, L.J.: Comprehensive survey on security services in vehicular ad-hoc networks. *IET Intell. Transp. Syst.* **10**(6), 12 (2016)
3. RoselinMary, S., Maheshwari, M., Thamaraiselvan, M.: Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA). In: *IEEE International Conference on Information Communication and Embedded Systems (ICICES)*, p. 4 (2013)
4. Mokhtar, B., Azab, M.: Survey on security issues in vehicular Ad Hoc. *Alexandria Eng. J.* **54**, 12 (2015)
5. Mejri, M., Ben-Othman, J.: GDVAN: a new greedy behavior attack detection algorithm for VANETs. *IEEE Trans. Mob. Comput.* **16**, 13 (2017)
6. Kaiwartya, O., Abdullah, A., Cao, Y., Altameem, A., Prasad, M., Lin, C.-T., Liu, X.: Internet of Vehicles: motivation, layered architecture, network model, challenges, and future aspects. *IEEE Access* **4**, 18 (2016). <https://doi.org/10.1109/ACCESS.2016.2603219>

7. Toor, Y., Mühlethaler, P., Laouiti, I., DE LA Fortelle, A., Mines, E.: Vehicle Ad Hoc networks applications and related technical issues. *IEEE Commun. Surv. Tutorials* **10**(3), 15 (2008)
8. Willke, T., Tientrakool, P., Maxemchuk, N.F.: A survey of inter-vehicle communication protocols and their applications. *IEEE Commun. Surv. Tutorials* **11**(2), 18 (2009)
9. Meraihi, R., Senouci, S.-M., Meddour, D.-E., Jerbi, M.: Vehicle-to-Vehicle communications: applications and perspectives. In: *Wireless Ad Hoc and Sensor Networks* (2010)
10. Verma, K., Hasbullah, H.: Bloom-filter based IP-CHOCK detection scheme for denial of service attacks in VANET (2014). <https://doi.org/10.1002/sec.1043>
11. Kaur, H., Batish, S., Kakaria, A.: An approach to detect the wormhole attack in vehicular Ad hoc networks. *Int. J. Smart Sens. Ad Hoc Netw.* **1**(4), 4 (2012)
12. Sumra, I.A., Ahmad, I., Hasbullah, H., Ab Manan, J.-L.: Classes of attacks in VANET. In: *Tenth International Conference on Wireless and Optical Communications Networks (WOCN)*, pp. 1–5 (2013)
13. Luckshetty, A., Dontal, S., Tangade, S., Manvi, S.S.: A survey: comparative study of applications, attacks, security and privacy in VANETs. In: *International Conference on Communication and Signal Processing*, p. 5. IEEE (2016)
14. Karimireddy, T., Bakshi, A.: A hybrid security framework for the vehicular communications in VANET. In: *IEEE WiSPNET*, p. 6 (2016)
15. Mohamed, M.S., Hussein, S., Krings, A.: An enhanced voting algorithm for hybrid jamming attacks in VANET. *IEEE* (2017)
16. Hussein, S., Mohamed, M.S., Kring, A.: A new hybrid jammer and its impact on DSRC safety application reliability. In: *The 7th IEEE Annual Information Technology, Electronics and Mobile Communication Conference, Vancouver, Canada*, pp. 1–7 (2016)
17. Bariah, L., Shehata, D., Salahat, E., Yeun, C.: Recent advances in VANET security: a survey, p. 7 (2015)

Advances in Computer Science and Ubiquitous
Computing

CSA-CUTE 17

Park, J.J.; Loia, V.; Yi, G.; Sung, Y. (Eds.)

2018, XXXIX, 1482 p. 671 illus. In 2 volumes, not
available separately., Hardcover

ISBN: 978-981-10-7604-6