Sybil Attack - The most threatening Security Attack in Ad hoc VANET

Nishtha

Department of Computer Science, Rajiv Gandhi Govt. Degree College, Chaura Maidan, Shimla, India

Abstract : A vehicular ad hoc network (VANET) can be deployed using Vehicle to Infrastructure (V2I) or Vehicle to Vehicle (V2V) modes of communication. In ad hoc deployment of VANET where vehicles arrange in a one-to-one manner in order to communicate from the host vehicle to the target vehicle. This is the most defenseless deployment of VANET and is inclined to attacks. Various types of attacks are possible in this ad hoc deployment of VANET. In this paper discussing various attacks, we have found that the Sybil Attack is one of the prominent attacks.

Index Terms **- Sybil Attack**, **Denial of Service Attack, Grey-Hole Attack, Black-Hole Attack.**

I. Introduction

The enclosure of communication technology in vehicles was initiated long ago when vehicles used car phones with Internet access or Bluetooth adapters. But its standardization started with the initial development of specifications by Federal Communications Commission (FCC), the Dedicated Short-Range Communication (DSRC) in the USA, and a similar communication consortium in Europe [1], [2]. DSRC is the collection of protocols and standards designed for single-hop communication in the vehicular network. The prominent standard on adaptation of this technology supporting Inter Vehicular Communication (IVC) is 802.11p [1], [2], [3], [4].

This on-the-spot formation of a wireless ad hoc network where nodes are vehicles for achieving precise vehicular communication-related tasks is specifically termed a Vehicular Ad hoc Network (VANET). It is a kind of communication network formed among ubiquitous vehicles that cooperate with other vehicles to make a safe, and convenient with a reduction in travel time [1], [3].

The deployment of VANET among moving vehicles is attainable because every vehicle participating in VANET has a fabricated intelligent unit termed an On-Board Unit (OBU). Communication among vehicles in VANET also takes place using radio signals in their specified radio range. When vehicles with OBUs move into the radio transmission range of each other, VANET formation is said to have occurred [2], [3], [4]. These OBUs have processors, sensors, Global Positioning System (GPS) units, memory, and radio interfaces, and these OBUs generate high computational, communication, and sensing capabilities in vehicles [5], [6]. Vehicles existing in each other communication range can directly communicate with one another [2], [3]. In contrast, for vehicles falling outside communication range message is delivered using a multi-hop communication technique where each intermediate vehicle act as a router that forwards the message using the carry forward approach. These OBUs make every vehicle participating in VANET act as a packet sender, router, and receiver, depending on the data forwarded for communication [1], [3], [6].

Some critical issues of concern inherent in VANETs are a very high movement of vehicles in a specific direction**,** a variety of vehicles existing over a geographic location, time-critical applications utilizing a distinct message transmission mode**,** and three distinct architectures for its deployment with a peer to peer communication without a central authority in the V2V communication, self-configuring nature, lack of proper vehicle authentication method, and topographical complexities [2], [6]. As a result, there is a likelihood that these vehicles function in a physically insecure environment as these intrinsic challenges throw VANETs open to various types of attacks.

VANET is a kind of communication network where its sustainability depends entirely upon the on-time information delivery of its multifarious applications. Besides the time criticality of information delivery that is of prime importance in VANET, the information delivered essentially follows some other specific characteristics related to security, preserving privacy, unaltered, precise, and reliable with QoS [1].

High speed of vehicles, broadcast transmission, and multi-hop data forwarding is a few inherent issues among many others that restrict VANETs to achieve on-time information delivery along with other required information parameters and make VANETs vulnerable to several types of attacks [1], [2], [6], [7].

With wireless communication media, such deployments do not possess many security mechanisms to authenticate the vehicles before entering the VANET [1]. As a result, many security breaches are there in VANET that make an adversary quickly come into the VANET and carry out various kinds of attacks [8]. Consequently, VANETs are likely to be influenced by multiple types of attacks. These attacks cover impersonation attacks based on the identity of a vehicle, traffic jamming by supplying false warning messages, violation of privacy, or on-board tempering by stopping the sensors or tampering with GPS units to provide false value [9].

Depending on the categorization of attacks in MANETs, attacks on VANETs may also be grouped into active and passive attacks. In active attacks, an intruder by actively participating in VANET performs malicious activities on data traffic and routing

traffic. In comparison, the passive attack is hard to detect, where the attacker indirectly involves malicious tasks and eavesdrops on the data [8], [10]. In this way, the attacker reveals the location information or movement patterns of the vehicles.

Further sections of this paper are divided with section II discussing various attacks in VANET, an analysis of security attacks is discussed in section III, and the conclusion in section IV.

II. Various Attacks in VANET

The most prominent attacks to which VANETs are exposed are as follows:

2.1 Denial of Service Attack

In Denial of Service (DoS) attack is a widespread attack in traditional wired networks. Wireless Ad hoc Networks such as VANETs because of their deployment in areas of prime importance such as in war fields, are vulnerable to attacks by intruders [7] [9],[11]. As the name suggests, DoS is an attack where the intruder makes sure that the network access or services of a genuine user are disrupted in the network. The DoS attack in history was reported in the year 1996 when the third-largest ISP Panix in the world was its first target, which brought down its services for many days [12]. In the DoS attack, a malicious user generates congestion in the network traffic by repeatedly sending the messages in the network, and this prevents other legitimate users from communicating in the network or utilizing the network services. In a DoS attack, depending on the type of destruction the malicious user needs, it may specifically damage a specific vehicle or may try to deteriorate the performance of the entire network [11].

2.2 Distributed Denial of Service Attack

The DDoS attack is initiated simultaneously by more than one malicious user present in VANET. This malevolent user (s) relentlessly sends messages one after the other in a distributed manner may be from different locations and/or at different points of time. Repetition of messages collectively by the number of malicious users creates congestion and jamming of network traffic, preventing genuine users from communicating or acquiring network services [9]-[13]. This attack is relevant in today's scenario and was recently reported in June 2019 during the Hong Kong anti-extradition protests. The messaging app Telegram was under the DDoS attack, and the protesters were left with no other option but not to use this App. In the same manner, Wikipedia users in Germany and some other parts of Europe were denied access to Wikipedia on the 6th and 7th of September 2019. Under DDoS attacks, the Wikipedia services were stopped for two days [11].

2.3 Black Hole Attack

The black hole in networking is the place where incoming or outgoing traffic drops automatically without providing any acknowledgment about the delivery of messages to the source. In this attack, the black hole is an empty region without having any vehicles or where the existing vehicles deny participation in VANET. A malicious vehicle existing in the network (as per the requirements of a predefined routing protocol) announces having the shortest path to the destination and consequently becomes successful in accessing the packets. The malicious vehicle then drops every received packet [7], [9], [13],[14].

2.4 Grey-Hole Attack

A Grey hole attack is analogous to the Blackhole attack with a disparity that the malevolent vehicle on receiving packets drops the packets and, after that, starts behaving in a usual way. As a result, none of the packets reach the destination, and it becomes challenging to locate the malicious user in this type of attack [7], [9], [13], [15].

2.5 Wormhole Attack

A wormhole attack in the network occurs when two or more malicious users take control of the network by forming a tunnel. The malicious users place themselves at the endpoints of the tunnel. Moreover, the malicious vehicle creates a tunnel for all the packets, including the ones not addressed to it. The malevolent user at the other end becomes a primary vehicle in the network that possesses all the diverted packets in the network. The malicious vehicle, controlling all the transmitted packets, may threaten the security of the network [7], [9], [13], [15].

2.6 Illusion Attack

In an illusion attack, to create an illusion for its neighboring vehicles, the malicious user deceives the sensors present in her/his own vehicle. Closing the sensor produces incorrect sensor readings and traffic information and can cause traffic jams, and accidents, and deteriorates the network performance [7], [9], [13],[15].

2.7 Sybil Attack

Sybil attack is also possible in peer-to-peer networks without centralized management, where the attacker creates numerous virtual identities from a single one and tries to control the network in various ways. Douceur initially introduced this attack in the year (2002) [16]. This attack was subsequently named after a book titled Sybil, containing documentation of a woman identified with Dissociative Identity Disorder (DID). A person suffering from this disorder has a dual personality

disorder, where the single person undergoes two different personality states [17]. In the same manner, in a Sybil attack, a malicious vehicle illegitimately launches one or more virtual/ superficial vehicles that do not exist in reality but disrupts the normal functioning of VANET in several ways. These unnatural/virtual/superficial vehicles are known as Sybil nodes/vehicles, and the malevolent vehicle from where these Sybil vehicles originate is known as Sybil attacker/ Sybil launcher [11], [7], [9], [12], [15].

2.8 Impersonation Attack and Masquerade

In VANET, the only method for vehicle identification is by their IP and MAC addresses. This way of vehicle identification is inappropriate as these methods cannot authenticate a user/sender purely on the basis of this information, and IP and MAC addresses can be spoofed easily. In the impersonation attack, a malicious vehicle, by stealing the identity of another vehicle, can forward messages on its behalf. In this way, the malicious vehicle by hiding itself in the network may create chaos in the network in various ways such as i) traffic jams, ii) accidents, and iii) transmitting false messages. Impersonation is accomplished by the malicious vehicle by using masquerade identity, message fabrication, and replay [9], [15].

2.9 Timing Attack

The majority of applications framed for VANET, like safety-related applications, are time-critical, and these applications require information to reach within a specific time frame. In the timing attack, the malicious vehicle present in the network creates a delay in message forwarding. Therefore, the adjacent vehicles do not receive the message in the required time frame, thereby deteriorating the performance of VANET [9], [15].

2.10 Man-in-the-Middle Attack

In the Man-in-the-Middle (MiMA) attack, a malicious user in VANET eavesdrops the communication between two legitimate vehicles. When these two vehicles try to communicate, the malicious vehicle acts as the other vehicle and delivers false information with the reply. In this way, the malicious vehicle disrupts the communication between legitimate vehicles [9], [15].

2.11 ID Disclosure

In an ID disclosure attack, a malicious vehicle reveals the identity or location of its neighbor vehicles and utilizes this information for various malevolent motives [15].

2.12 Bogus Information Attack and Bush Telegraph

In a Bogus information attack, the attacker may be an intruder or a legitimate vehicle with malicious intentions, and transmits bogus or false information for personal benefit in the network [9], [15]. A more complicated type of bogus information is the Bush Telegraph. In the bush telegraph attack, the attacker owns many identities distributed over numerous wireless hops. When a packet is received in a hop, error checking is carried out. The packet is forwarded only if the error is small and is within a tolerance limit. The attacker adds incremental errors lower than the tolerance level in the packet at each hop. After traversing many hops, the accumulated error ultimately leads to bogus information [15].

2.13 Malware and Spam Attack

In Malware and Spam attacks, a malicious user present in VANET transmits virus-infected and spam messages to create severe disruption in the normal functioning of VANET. These messages ultimately consume a lot of network bandwidth. In infrastructure-less VANETs, without the use of centralized control, this attack is complicated to be prevented. On software updates, the OBUs and RSUs usually get infected by these attacks [15].

2.14 Global Positioning System (GPS) Spoofing, Tunnel Attack, and Global Positioning System (GPS) Jamming

The OBU of every vehicle participating in VANET is equipped with GPS. This GPS unit provides the geographic location of all vehicles. But it is always possible to spoof the GPS signals. In a GPS spoofing attack, the attacker avails a GPS Satellite simulator that produces more powerful signals than the real satellite to spoof the original GPS signals. The spoofing of GPS signals enables the attacker to create a false location on the GPS. In this way, GPS spoofing misleads the user, and the user assumes the incorrect position to be the real one [9], [15].

In GPS jamming, one can block the GPS signals in a specific region by using GPS jamming devices. GPS jamming area varies from a few meters to approximately six kilometers [17]. The other method to spoof GPS signals is when a vehicle comes across an obstacle or moves in a tunnel (Tunnel attack). At this time, the vehicle does not receive GPS signals. Taking advantage of this situation, the attacker may replace the real information about that vehicle available with other vehicles with fabricated information [15].

III. Analysis of Security Attack

Author	Significant Attacks in VANET											
	Denial of Service Attack	Replay Attack	Black Hole Attack	Grey Hole Attack	Worm hole Attack	Illusion Attack	Sybil Attack	Man-in-the-Middle Attack	Impersonation Attack and Masquerade Attack	Timing Attack	Malware and Spam Attack	Global Positioning System Spoofing Tunnel Attack
J.T. Isaac et al. (2009) [18]						✓	✓					✓
G. Samara et al. (2010) [7]	✓	✓					✓					
J.M. Fuentes et al. (2011) [19]	✓						✓		✓			
M. S. Al-kahtani (2012) [9]	✓		✓		✓	✓	✓	✓	✓	✓	✓	✓
I. A. Sumra et al. (2013) [20]	✓		✓	✓		✓	✓		✓	✓		✓
S. Gillani et al. (2013) [13]	✓	✓	✓				✓		✓		✓	✓
V. H. LA et al. (2014) [15]	✓		✓		✓	✓	✓	✓	✓	✓	✓	✓
M. A. Elsadig et al. (2016) [21]	✓		✓		✓	✓	✓	✓	✓	✓	✓	✓
S. Sharma et al. (2016) [22]	✓		✓	✓	✓		✓		✓			
F. Sakiz et al. (2017) [23]	✓	✓	✓		✓	✓	✓					✓
H. Hasrouny et al. (2017) [8]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
T. Zaidi et al. (2018) [24]	✓		✓		✓	✓	✓	✓		✓		✓
Z. Lu et al. (2018) [25]	✓	✓	✓	✓			✓				✓	✓
M. A. Hezam et al. (2018) [26]	✓	✓	✓		✓		✓		✓		✓	✓
K. Singh et al. (2019) [27]		✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
M. S. Sheikh et al. (2019) [28]	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓
M. S. Sheikh et al. (2020) [29]	✓	✓	✓	✓		✓	✓		✓			✓

The most common security attacks to which VANETs are easily prone: Denial of Service (DoS), Black Hole**,** Grey Hole**,** Wormhole**,** Illusion**,** Sybil**,** Man-in-the-Middle (MiMA), Impersonation, Masquerade, Timing, Malware, Spam, Global Positioning System (GPS) Spoofing, Tunnel, Replay attacks [14], [18]-[29]. In the literature, several researchers have highlighted various types of security attacks on VANET. Based on the literature review on all these major security attacks on VANET, an author-specific summary of various attacks is displayed in Table 1.

Among these, one of the crucial attacks that may affect ad hoc networks to a large extent and the one that has been discussed specifically for VANETs in every research paper is the Sybil Attack as shown in Table 1.

IV. Conclusion

This shows that one of the crucial attacks that may affect ad hoc networks to a large extent. Thus, a malevolent vehicle in VANET illegitimately produces virtual vehicle(s) and disrupts or breakdown the network services. Thus, Sybil Attack is the deadliest attack that is to be prevented in ad hoc VANETs.

REFRENCES

[1] R. D. Pietro, S. Guarino, N. V. Verde and J. Domingo-Ferrer. Security in Wireless Ad-Hoc Networks – A Survey. Computer Communications. vol. 51. 2014.

[2] W. Liang, Z. Li, H. Zhang, S. Wang and, R. Bie. Vehicular Ad Hoc Networks: Architectures, Research Issues. Challenges and Trends. International Journal of Distributed Sensor Networks. vol. 11. pp. 1–11. 2015.

[3] F. Li and Y. Wang, Y. Routing in Vehicular Ad Hoc Networks: A Survey. IEEE Vehicular Technology Magazine. vol. 2. no.2, pp. 12-22, 2007.

[4] C. M. Silva, B.M. Masini. G. Ferrari and I. Thibault. Survey on Infrastructure-Based Vehicular Networks. Hindawi Mobile Information Systems. 2017.

[5] P. Papadimitratos, A D. L. Fortelle, K. Evenssen, R. Brignolo and S. Cosenza.Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation. Communications Magazine. IEEE. vol. 47. no.11. pp. 84-95. 2009.

[6] E. C. Eze, S. Zhang, E. Liu, J.C. Eze. Advances in Vehicular Ad-Hoc Networks (VANETs): Challenges and Road-map for Future Development. International Journal of Automation and Computing. vol. 13. no.1. pp. 1-18. 2016.

[7] G. Samara, W. A. H. Al-Salihy and R. Sures. Security Analysis of Vehicular Ad Hoc Networks (VANET). in Second International Conference on Network Applications, Protocols and Service. IEEE. Malaysia. 2010.

[8] H. Hasrouny, A. E. Samhat, C. Basil and A. Laouitui. VANET Security Challenges and Solutions: A Survey. Vehicular Communications. vol. 7. pp. 7-20. 2017.

[9] M. S. Al-kahtani. Survey on Security Attacks in Vehicular Ad Hoc Networks. in 6th International Conference on Signal Processing and Communication Systems. IEEE. Gold Coast. QLD Australia. 2012.

[10] J. Sen. Security and Privacy Issues in Wireless Mesh Networks: A Survey. Wireless Networks and Security and Communication Technology, S. Khan, A.S. Khan Pathan (eds). Springer. Berlin. Heidelberg. 2013.

[11] V. Gupta, S. Krishnamurthy and M. Faloutsos. Denial of Service Attack at the MAC Layer in Wireless Ad Hoc Networks. vol.2. pp. 1118 – 1123. 2002. (online) Available: 10.1109/MILCOM.2002.1179634

[12] wiki: https://en.wikipedia.org/wiki/Denial-of-service_attack.

[13] S. Gillani, F. Shahzad, A. Qayyum and R. Mehmood. A Survey on Security in Vehicular Ad Hoc Networks. in International Workshop on Communication Technologies for Vehicles. pp. 59-74. 2013.

[14] B. Sun, Y. Guan, J. Chen, and U. W. Pooch. Detecting Black-hole Attack in Mobile Ad Hoc Networks. in 5th European Personal Mobile Communications Conference, Glasgow. UK. 2003.
[15] V. H. LA and A. Cavalli. Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey. International Journal on Ad Hoc Networking Systems. vol. 4. no. 2. 2014.
[16] J. R. Douceur. Sybil Attack. in First International Workshop on Peer-to-Peer Systems. P. Druschel, M.F. Kaashoek, A.I.T. Rowstron (eds). Springer-Verlag. London. UK. pp. 251-260. 2002.
[17] R. H. Mitch, R. C. Dougherty, M. L. Psiaki, S. P. Powell, B. W. O'Hanlon, J. A. Bhatti and T. E. Humphreys. Signal Characteristics of Civil GPS Jammers. in 24th International Technical Meeting of the Satellite Division of the Institute of Navigation, ION GNSS, vol. 3. pp. 1907–1919. Portland. 2011.
[18] J.T. Isaac, S. Zeadally, J.S. Camara. Security Attacks and Solutions for Vehicular Ad Hoc Networks. IEEE Communications. vol.4. pp. 894-903. 2009.
[19] J. M. Fuentes, A. I. Gonzalez-Tablas Ferreres, A. Ribagorda. Overview of Security Issues in Vehicular Ad-Hoc Networks In: M.M. Cruz-Cunha, F. Moreira (eds.). Handbook of Research on Mobility and Computing, IGI Global, 2010.
[20] I.A. Sumra, H. BinHasbullah, J. A. Manan, I. Ahmad. Classification of Attacks in Vehicular Ad hoc Network (VANET). Information –An International. Interdisciplinary Journal. vol. 16. pp.2995-3004. 2013.
[21] M.A. Elsadig, Y.A. Fadlalla. NETs Security Issues and Challenges: A Survey. Indian Journal of Science and Technology. vol. 9. 2016.
[22] S. Sharma, S. Sharma. A Review: Analysis of Various Attacks in VANET. International Journal of Advance Research in Computer Science, vol. 7. pp. 249-253. 2016.
[23] F. Sakiz, S. Sen. Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV. Ad Hoc Networks. vol. 61. pp. 33-50. 2017.
[24] T. Zaidi, S. Faisal. An Overview: Various Attacks in VANET. 4th International Conference on Computing Communication and Automation (ICCCA). IEEE, Greater Noida, India.2018, Doi:10.1109/CCAA.2018.8777538.
[25] Z. Lu, G. Qu, Z. Liu. A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy. IEEE Transactions on Intelligent Transportation Systems, vol. 20. pp. 760-776. 2018.
[26] M. Al Junaid, A. Syed, M. Warip, K.N.F. Ku Azir, N. Romli. Classification of Security Attacks in VANET: A Review of Requirements and Perspectives. MATEC Web of Conferences, vol. 150, pp. 06038-06044, 2018.
[27] M. Jain, R. Saxena. VANET: Security Attacks, Solution and Simulation. Proceedings of the Second International Conference on Computational Intelligence and Informatics (ICCII). 2107.
[28] Deeksha, A. Kumar, M. Bansal. A review on VANET security attacks and their countermeasure. 4th International Conference on Signal Processing, Computing and Control (ISPCC), 2017, 580-585, doi: 10.1109/ISPCC.2017.8269745..
[29] M. A. Hezam A. Junaid, Syed A. A, M. N. M. Warip, K. N. F. K.Azir, N. H. Romli. Classification of Security Attacks in VANET: A Review of Requirements and Perspectives. MATEC Web of Conferences 150, MUCET. 2017.