IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Review on various security issues and challenges in VANET

Dr.Prakash Kumar
Associate professor
JRU, Ranchi

Abstract

Vehicular ad hoc networks (VANET) are a class of ad hoc networks in which vehicle communicate with each other to show the traffic scenario and any mishappening on the road. It also ensures the safety on the road. Trust and security remain a major concern in VANET as simple mistake can cause serious problems. A crucial point in VANET is how to trust the information transmitted when the neighbouring vehicles are rapidly changing and moving in and out of range. This obstructs establishing reliable end-to-end communication paths and having efficient data transfer. In a VANET, vehicles will rely on the integrity of received data for deciding when to present alerts to drivers. The communication between vehicle to vehicle and vehicle to roadside unit is done through wireless communication. That is why security is an important concern area for vehicular network application. Also in VANET efficient routing protocols are needed as vehicles are changes their positions very rapidly. In this research paper we are going to analyse and categories various security issues in VANET based on various security requirements. Also we have given the various security challenges faced in VANET that are given in various research papers.

Keywords: Vehicular ad hoc networks, security, attacks, mobility, privacy, threats.

Introduction

The vehicles on the road have increased tremendously in last few decades. This has resulted in increased accident probability and fatalities on the roads. Vehicular Ad-hoc Networks (VANETs) have shown promise of bringing down road accidents and fatalities thereof by enabling communication between vehicles. VANETs also allow the road operators to control and monitor vehicles for rash driving and quick relief [1] .Vehicular ad hoc networks is a technology that has recently emerged. VANET can be used to improve road safety, reduce road traffic, serve interests of its users, and provide emergency services.

Communication architecture of VANET:

Communication Architecture: Communication types in VANETs can be categorized into four types. The category is closely related to VANETs components [2]
In-vehicle communication, which is more and more necessary and important in VANETs research, refers to the in-vehicle domain. In-vehicle communication system can detect a vehicle's performance and especially driver's fatigue and drowsiness, which is critical for driver and public safety.

Vehicle-to-vehicle (V2V) communication can provide a data exchange platform for the drivers to share information and warning messages, so as to expand driver assistance.

Vehicle-to-road infrastructure (V2I) communication enables real-time traffic/weather updates for drivers and provides environmental sensing and monitoring.

Vehicle-to-broadband cloud (V2B) communication means that vehicles may communicate via wireless broadband mechanisms such as 3G/4G. As the broadband cloud may include more traffic information and monitoring data, as well as infotainment this type of communication will be useful for active driver assistance and vehicle tracking.

VANET Structure: In VANET structure three major components are there these are

1. Application Unit: AU is Responsible for providing communication inside vehicle. It helps in monitoring driver as he fatigue, or drowsiness etc. The AU can be connected to the OBU through a wired or wireless connection.

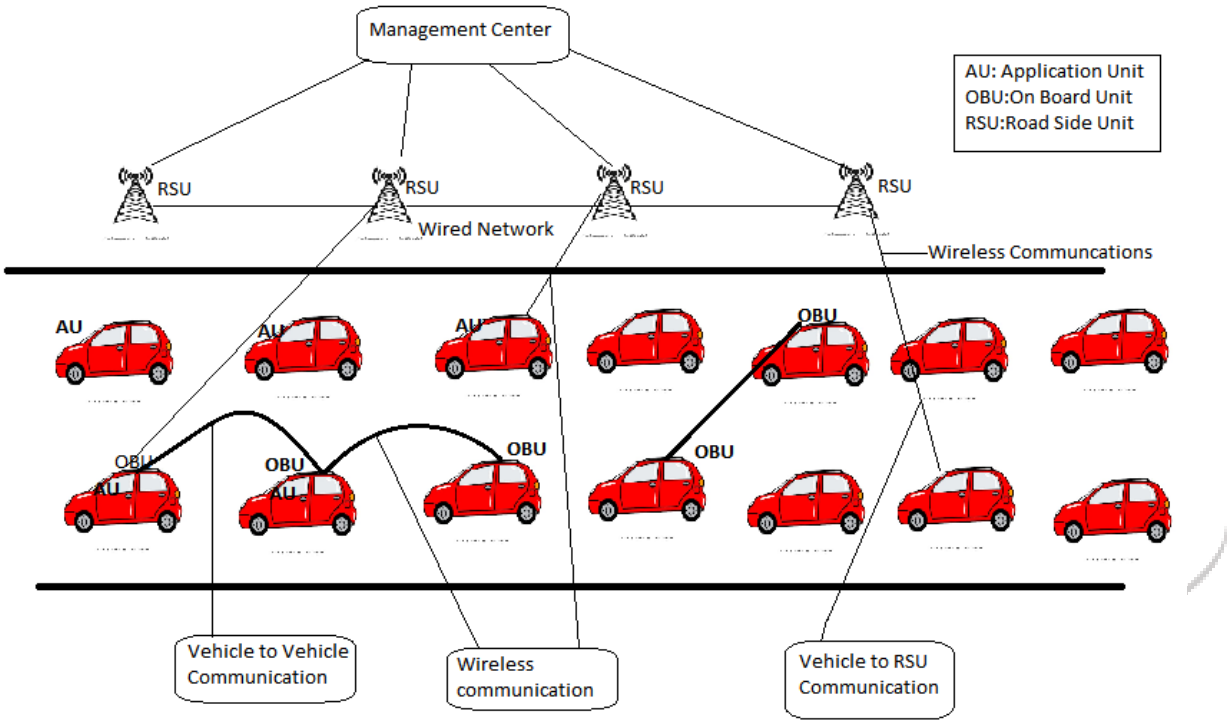

Fig: VANET Architecture.

2. On Board Unit: OBU is Responsible for providing communication between vehicle to vehicle communications. It provides wireless communications between different vehicles.OBU also communicates with RSU through wireless communication medium to provide vehicle to RSU Communication.

3. Road side Unit: The following are the main functionalities of an RSU[3]:
   - Radio frequency, high power, and long-range antenna to access a wireless medium.
   - A network stack to run VANET specific network, link, and physical layer protocols.
   - Forwarding data packets to OBUs in its range and other RSUs.
   - Aggregation of safety information from OBUs through safety applications and alarming incoming OBUs.
   - Working as a gateway to provide Internet connectivity to OBUs.

RSUs support IEEE 802.11p, and all four IEEE 1609 protocols. Along with the wireless channel access protocols, RSUs also supports access to wired channels, such as a coaxial cable or optical fibre cable, with Ethernet like protocols.

4. Management center: The Management center known as central infrastructure domain contains infrastructure management centers such as traffic management centers (TMCs) and vehicle management centers [4].

Security issues: The main security attributes and requirements in VANET are as given below [**5**].

1. Availability
2. Authentication
3. Data Integrity
4. Confidentiality

Availability: Since vehicular networks require real-time responses, they are vulnerable to DoS attacks. In order to remain operational, protocols and services must be resilient against denial of service attacks. The communication channel must be available at all times, it must also be reliable otherwise attackers can launch DoS attacks. Such attacks can disrupt the entire network which will lead to failure in delivering network messages to other vehicles in range. The main attacks related to availability are [6].

1. Denial of service attack: It is the most serious level attack in vehicular network. In this attack attacker jams the main communication medium and network is no more available to legitimate user [7].

2. Blackhole: In Black Hole attack, a malicious node pretends to have an optimum route for the destination node and indicates that packet should route through this node after transmitting the fake routing information. The impact of this attack is that the malicious node can either drop or misuse the intercepted packets without forwarding them [8].

3. Malware: This attack is frequently approved by insiders more than outsiders and when a firmware update is done it can be downloaded into the system [11].

4. Spamming: Spamming attacks aim to consume the network bandwidth and increase the transmission latency. The users are not interested in such messages, like advertisement messages[9]

Authentication: network nodes must be authenticated in order to be able to send messages through the network. Before reacting to messages and events a vehicle must verify the legitimacy of the message and its sender, therefore there is a need for authentication. Without authentication, illegitimate and malicious users can inject false messages into the network and confuse other vehicles by distributing false information. With authentication, vehicles can simply drop messages from unauthenticated users [5].

1. Masquerading: in a masquerade attack, a malicious vehicle changes its identity [41] to be another vehicle, trying to produce different messages, alter, and replay with information to deceive other vehicles. For example, a malicious vehicle can change its identity to be an ambulance and force other vehicles to slow down or change their routes [10].

2. Bogus information: In this case, attackers are insiders, rational, and active. They can send wrong information in the network so that it can affect the behaviour of other drivers. For example, an adversary can inject wrong information about a nonexistent traffic jam or an accident diverting vehicles to other routes and freeing a route for itself [8].

3. GPS Spoofing: A malicious node utilizes the GPS satellite simulator to produce signals which are stronger than the actual satellite signals, tending to deceive vehicles to accept the false position information. This attack is related to physical devices. However, NDN should deal with trust in such data propagation, where collaborative vehicles may detect this information and stop it [10].

1. Monitoring attack:

Data Integrity: This term refers that the data or information among nodes are not altered by attackers [7].

1. Timing attack: In timing attacks, the malicious vehicles do not forward the emergency messages and information at the right time. They received it, by creating an explicit communication delay and adding time slots to the received messages. Their neighbour's vehicles receive these messages too late after the time they need it. The timing attack is a critical issue, especially when dealing with time-constraint applications [10].

2. Social attack: The basic idea of the attack is to confuse and bedazzle the victim by sending unethical and unmoral message so that driver gets disturb. The legitimate user reacts in annoyed manner after getting such kind of messages which is the main objective of the attacker [13]. It effects the driving of the vehicle which indirectly creates the problem in the network.

Privacy and Confidentiality: In VANET's the term confidentiality refers to the confidential communication. In a group no one except the group members are able to decrypt the messages that are broadcasted to every member of the group. Privacy means that that an eavesdropper is impossible to decide whether two different messages come from the same vehicle [7].

1. Impersonation attack: In vehicular network each vehicle has unique identifier which is used to verify the messages whenever the accident occurs by sending the wrong messages to other vehicles [7].

Privacy confidentiality and Integrity:

1. Man in The Middle attack: It happens when a malicious node intercepts or tampers with messages exchanged between legitimate nodes. In these attacks, malicious node (MITM) either eavesdrops or alters the messages exchanged between two legitimate vehicles. The exchanged information may contain sensitive and delay-intolerant information such as steep-curve warning. This results in the dissemination of compromised and incorrect information throughout the network[12]

Authentication and Integrity:

1. Tunnelling: The attackers rapidly insert false positioning information or data in to the committed unit of the node, origin the node to assume that the information received is valid [11].

Authentication and privacy:

1. Sybil attack: It is a critical attack. In this type of attack an attacker transmits multiple messages with different ids to the other vehicles. In this way other vehicles feels that these messages are coming from different vehicles, so there is a jam further and they are enforced to take alternate route. In other words we can say that the main task of the attacker is to provide an illusion of multiple vehicles to other vehicles and to enforce them to choose alternate route and leave the rod for the benefits of the attacker. This task is done by sending multiple messages with different id [13].

Security challenges: The VANET security challenges can be categorised into two types as:

1. **Technical Challenges:** The technical challenges deals with the technical obstacles which should be resolved before the deployment of VANET. Some challenges are given below [14]:

    a) Mobility: Mobility is very high as nodes change their positions very rapidly. Due to this network management becomes very complex.
    b) Topology management: due to high mobility topology is changing very quickly and its management is very difficult.
    c) Congestion and collision Control: The unbounded network size also creates a challenge. The traffic load is low in rural areas and night in even urban areas. Due to this, the network partitions

frequently occurs while in rush hours the traffic load is very high and hence network is congested and collision occurs in the network.

d) MAC Design: VANET generally use the shared medium to communicate hence the MAC design is the key issue. Many approaches have been given like TDMA, SDMA, and CSMA etc. IEEE 802.11 adopted the CSMA based Mac for VANET.

e) Security attacks: There is various security attacks as discussed in this paper are also bigger challenge to VANET.

f) Low tolerance of error: In VANET small error can cause serious harmful effects.

2. **Economical challenges:** Manufactures are interested to build applications that consumer likes most. Very few consumers will agree with a vehicle which automatically reports any traffic rule violation. Hence successful deployment of vehicular networks will require incentives for vehicle manufacturers, consumers and the government is a challenge to implement security in VANET [14].

Conclusion: In this research paper we have highlighted the various security attacks. We have also discussed various security requirements and based on this we have categorised the security attacks in VANET. We have also through some light on various security challenges in VANET.

References:

1. Chaitanya Kumar Karn and Chandra Prakash Gupta,(2016) A Survey on VANETs Security Attacks and Sybil Attack Detection, International Journal of Sensors, Wireless Communications and Control.Vol. 6, 45-62.
2. W. S Manjoro, Brijesh kumar chaursia, Mradul Dhakar, (2017), Traffic congestion detection using data mining in VANET, Internationl conference on electrical, electronics and computer science, pp 23-31, DOI: 10.1109/SCEECS.20167509374.
3. Mukesh Saini, Abdulhameed Alelaiwi, Abdulmotaleb El Saddik, (2015), How Close are We to Realizing a Pragmatic VANET Solution? A Meta-Survey, Article in CM Commuting Survey, pp 1-40, DOI: 10.1145/2817552.
4. Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Shenling Wang, and Rongfang Bie, (2015), Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends, International Journal of Distributed Sensor Networks Volume 2015, pp 11, doi: http://dx.doi.org/10.1155/2015/745303.
5. Parul Tyagi, Dr. Deepak Dambla, (2014), Investigating the Security Threats in Vehicular ad hoc Networks (VANETs): Towards Security Engineering for Safer on-road Transportation, IEEE ICACCI conference at Galgotia Institute of Technlogy, Gr. Noida, DOI: 10.1109/ICACCI.2014.6968313
6. Muawia Abdelmagid Elsadig, Yahia A. Fadlalla , (2016), VANETs Security Issues and Challenges: A Survey, Indian Journal of Science and Technology, Vol 9(28), DOI:10.17485/ijst/2016/v9i28/97782
7. Ujwal Parmar, Sharanjit Singh, (2015), Overview of Various Attacks in VANET, International Journal of Engineering Research and General Science Volume 3, Issue 3,ISSN 2091-2730
8. Namarpreet Kaur, Aman Arora, (2015), A Review on Security Issues in VANET, International Journal of Advanced Research in Computer Science Volume 6, No. 2 pp 161-165.
9. Yousef Al-Rabanah, Ghassan Samara, (2015), Security Issues in Vehicular Ad Hoc Networks (VANET): a survey, International Journal of Science & applied Research, IJSAR, Volume 2(4), pp 50-55.
10. Hakima Khelifi, Senlin Luo, Boubakr Nour, and Sayed Chhattan Shah, (2018), Security and Privacy Issues in Vehicular Named Data Networks, an Overview, Hindawi Mobile Information Systems, Volume(2018),pp 11, doi:org/10.1155/2018/5672154
11. Irshad Ahmed Sumra, P. Sellappan, Azween Abdullah2and Ahmad Ali, (2018), Security issues and Challenges in MANET-VANET-FANET: A Survey, EAI Endorsed Transactions on Energy Web and Information Technology 01 2018 - 04 2018 | Volume 5 | Issue 17 | e16, doi: 10.4108/eai.10-4-2018.155884

12. Farhan Ahmad ,Asma Adnane 2, Virginia N. L. Franqueira , Fatih Kurugollu and Lu Liu, (2018), Man-In-The-Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact ofAttackers' Strategies, MDPI Journal sensor, 2018, 18, 4040; doi:10.3390/s18114040.

13. AJAY RAWAT, SANTOSH SHARMA, RAMA SUSHIL, (2012), VANET: SECURITY ATTACKS AND ITS POSSIBLE SOLUTIONS, Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762 , Volume 3, Issue 1, 2012, pp-301-304.

14. Ram Shringar Raw1, Manish Kumar1, Nanhay Singh, (2013), SECURITY CHALLENGES, ISSUES AND THEIR SOLUTIONS FOR VANET, International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, pp 95-105.

15. Mohammed Ali Hezam Al Junaid1, Syed A. A, Mohd Nazri Mohd Warip, Ku Nurul Fazira Ku Azir1, Nurul Hidayah Romli, (2018), Classification of Security Attacks in VANET: A Review of Requirements and Perspectives**,** MATEC Web of Conferences ,Volume 150, DOI: https://doi.org/10.101051/matecconf/201815006038

16. Abid Khan Jadoon, Qaiser Khan, Asif Tehseen Ilahi, Waseem Iqbal,(2016), A Survey on Security Challenges in VANET, ResearchGate, pp 3.

17. Nirbhay Kumar Chaubey, (2016) Security Analysis of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study, International Journal of Security and Its Applications Vol. 10, No. 5.

18. Jinesh M. K, Bharat Javaraman, Sybil Attack Detection in Vehicular Networks, Security and privacy in internet of things, CRC Press Research gate, pp 35-51.

19. Shivani Kanwar, Sandeep Joshi, Manu Sood,(2014) Detection of Sybil Attack in VANETs by Trust Establishment in Clusters, International Journal of Computer Engineering and Applications, Volume VII, Issue I, pp 51-60.

20. Marvy B. Mansour, Cherif Salama, Hoda K. Mohamed and Sherif A. Hammad, (2018), VANET SECURITY AND PRIVACY – AN OVERVIEW, International Journal of Network Security & Its Applications (IJNSA) Vol. 10, No.2