Analysis of Security Challenges in Vehicular Adhoc Network

Nazish Siddiqui[1], Mohd Shahid Husain[2], Mohammad Akbar[3]

Department of Computer Science & Engineering, Integral University, Lucknow, India

***Abstract*- Vehicular Adhoc Network (VANET) is one among the latest emerging and promising technologies of our near future that provides Network on Wheels (NOW). Providing security to VANET is important and essential in terms of having efficient and secure communication. Vehicular ad hoc networks are receiving increasing attentions from the field of academics and industry, due to various applications and tremendous benefits they offer. Safety information exchange enables life-critical applications. Vehicles will rely on the integrity and authenticity of received data. That is why security is an important area of concern and moreover a challenge for vehicular network applications. The main aim of this paper is to explore the various security issues and challenges in vehicular communication.**

I. INTRODUCTION

With the rapid development of wireless technologies, people have started to enjoy wireless access everywhere, even in vehicles on the move. Today, car manufacturers and telecommunications industries have teamed up together to equip vehicles with wireless technologies which not only bring various information technology services to vehicles but also improve the safety on the road and traffic efficiency. Vehicles together with the road side infrastructure can form a huge self-organized communication network called vehicular adhoc network (VANET). More specifically, a VANET is a collection of vehicles in a network that are dynamic in nature and communicate with each other and/or with nearby Road Side Units (RSUs), using a technique called, Dedicated Short Range Communication (DSRC)[5]. These vehicles are equipped with wireless On-Board Unit (OBU), which perform this communication. The VANET provides a complete computing environment to its users and enables numerous services through a variety of applications. For example, each vehicle may periodically broadcast its traffic information to others, to avoid traffic jams and accidents. Moreover, vehicles can make themselves more comfortable and knowledgeable during their journeys by sharing specific information with each other, such as tourism information, road conditions, media files (music & movie files), or hotel information etc. Due to high impact and enormous potential, VANETs have drawn considerable research attention and many prototype applications have already been developed. However, before implementing these applications, particularly safety related ones, security problems related to vanet must be addressed and resolved.

II. OVERVIEW OF VANET

A Vehicular Adhoc Network is a form of Mobile Adhoc Network (MANET), that provides communication among the vehicles. The communication involves the communication between the nearby vehicles, and between the vehicles and the nearby fixed equipments called Road Side Units (RSUs). Every node whether it is a vehicle or RSU communicates with the other nodes in single hop or multi hop. VANETs are designed with the primary goal to improve driving safety and provide comfort to passengers. A VANET has the following types of communication:

- Inter-Vehicular or Vehicle to Vehicle (V-V) Communication
- Vehicle to Roadside or Vehicle to Infrastructure (V-I) Communication
- Inter Roadside Communication.

Dedicated Short Range Communication (DSRC) is the radio used for the communication. DSRC/WAVE is part of the initiative by Vehicle Infrastructure Integration (VII) of the Federal Highway Authority and supports vehicle-to-vehicle and vehicle-to-infrastructure communication for the emerging Intelligent Transportation Systems (ITS)[8]. DSRC/WAVE systems remove the drawbacks that exist in the wireless infrastructure by facilitating low latency, geographically local, high data rate, and high mobility communications[8][1]. IEEE 802.11p [8][1] is an improvement of the IEEE 802.11 standard to add Wireless Access in Vehicular Environments (WAVE). It defines enhancements to 802.11 and supports the applications of ITS. This includes data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure in the licensed ITS band of 5.9 GHz (5.85-5.925 GHz). Another higher layer standard based on the IEEE 802.11p is IEEE 1609[4].

A. *Characteristics Of Vanet*

VANET has its own distinct characteristics that are summarized as:

1) *High Mobility:* The nodes in VANETs are vehicles which are usually moving at very high speed. Hence, they

remain in the communication range of each other for few seconds, and links are established and broken fast.

2) *Rapidly changing network topology:* High mobility and random speed of vehicles, causes the position of nodes to vary frequently. As a result of this, there is a frequent change in the network topology.

3) *Unbounded network size:* VANET can be implemented for one or more cities or even for countries that results in geographically unbounded size of the network.

4) *Frequent exchange of information:* VANET's ad hoc nature motivates the nodes to gather information from the neighbouring vehicles and RSUs. Hence the exchange of information among the nodes become frequent.

5) *Wireless Communication:* VANET is designed for the wireless environment. Nodes are connected and exchange their information through a wireless medium.

6) *Mobility modeling and predication:* The nodes in vanet are generally constrained by prebuilt highways, streets and roads. So provided the speed and the street map, vehicle's future position could be predicated.

7) *Time Critical:* The delivery of information to the nodes in VANET must be done within time limit so that it can perform the action accordingly. High data rates is not required in vanet; however it does have hard delay constraints.

8) *Geographic position available:* Accurate positioning systems like GPS with integrated electronic maps are quite popular in cars, as vehicles equipped with these tools, provide location information for routing purposes.

9) *No power constraint:* The nodes in VANET do not have much issue concerning the energy of computational resources. Thanks to always recharging batteries of the nodes which are cars instead of small handheld devices, so power constraint could be neglected.

III. Security Requirements In Vanets

To ensure security in VANET, we need to consider certain attributes which includes

1) *Authentication:* Authentication refers to the verification of identity between the infrastructure units (RSUs) and the vehicles and the integrity validation of information exchange. It ensures that the message is transmitted by the actual node and hence reduces the attacks done by the attackers or the adversaries to a greater extent. It is the major security requirement in VANET.

2) *Integrity:* Integrity of message is very much required as it ensures that the message is not altered or changed during its transmission. Data integrity gives the assurance that the received data, is exactly the same as what has been generated originally. Digital signature integrated with password access[9][10] are used in order to protect the integrity of the message.

3) *Non-Repudiation:* In this security based system a sender cannot deny the fact of having sent the message. But that doesn't mean that everyone can identify the sender. Only specific authorities with complete authorization are allowed to identify a vehicle. The attackers could be identified even after the attack happened. This prevents cheaters from denying their crimes.

4) *Confidentiality:* It is a system which is required when certain nodes wish to communicate in private. But anybody cannot do that. It can only be done by the vehicles of the law enforcement authority to convey private information and communicate with each other. An appropriate example would be, to find the location of any criminal or a terrorist.

5) *Privacy:* Privacy ensures that the information is not leaked to the people who are not allowed to view the information i.e unauthorized users. Location privacy is also important so that past or future locations of the vehicles could not be traced. However specified authorities must be allowed to trace the identity of the user in some liability related cases.

6) *Real time guarantees:* Many safety related applications in VANET depend on strict time guarantees. It ensures that the time constraint is met in case of safety related applications like collision avoidance.

7) *Availability:* The term availability deals with the services, like bandwidth and connectivity [9][13] provided by the network for all the nodes. Prevention and detection techniques using group signatures[9][10] has been introduced in order to deal with the issue of availability.

8) *Access control:* It ensures that all the nodes in the network perform their functions according to the roles and privileges authorized to them. Authorization, in access control, specifies what each node could do in the network and what sort of messages could be generated by it.

IV. Security Vulnerabilities of VANETs

Following are some of the major threats to security goals that could affect the security in Vehicular Network:

1) *Snooping:* Snooping is a passive attack in which the attacker only monitors or accesses the information without modifying the data. When a vehicle in the network sends information to another vehicle then the attacker intercepts and accesses the contents of the information and uses it for its own benefit.

2) *Traffic analysis*: It is another passive attack in which no modification of data is performed by the attacker. In this attack, an attacker analyses the traffic and collects the information by monitoring the vehicular network constantly and perform the attack by a guessing strategy.

3) *Data modification:* It is an active attack in which the data is intercepted and modified or altered by the attacker. When a vehicle in the network sends an important information say warning message to another vehicle, then the attacker may modify the data, delete the data or make some delay in its delivery.

4) *Replay attack:* In this attack, the attacker saves a copy of the message by intercepting and later uses it for replaying. In the VANET systems, when a vehicle sends some message to another vehicle, the attacker keeps a copy of the message and later uses it for its own benefit. It is an active attack.

5) *Masquerading:* It is another active attack where the data can be modified. In this attack, an attacker impersonates some other vehicle by providing false ID and advertises as a legal node.

6) *Repudiation*: In this attack, an attacker denies that he/she has sent the message. In the VANET systems, a sender vehicle or a receiver vehicle can create this attack by denying that it has sent or received a message, respectively.

7) *Sybil attack:* In this attack, an attacker generates multiple identities and cheats with false identities. A malicious vehicle in the network acts as multiple vehicle nodes and joins the network and after joining the network it behaves maliciously. This attack is an active attack which degrades the systems performance.

8) *Tunneling:* In tunneling attack, an attacker injects false data into the network. When a vehicle in the network is going to receive the location information it suddenly injects faulty location information which creates a problem for the receiver vehicle.

9) *Spamming:* In this attack, an attacker increases the flooding effect in the network by which traffic congestion occurs. It reduces the efficiency of the request/response scheme by creating a delay in the network. The attacker tries to jam the network by transmitting signals to interfere by which the network performance degrades[5][17].

10) *GPS spoofing:* In this attack, the attacker transmits false robust signals which are powerful than the GPS signals. By performing this action, the attacker jams the network and the receiver obtains false position signals of itself. This creates a problem in obtaining a correct position and the receiver deviates from the right position and broadcasts its false position to other vehicles.

V. Challenges In Vanet

1) *Tradeoff between authentication and privacy:* For the authentication of the messages that are to be transmitted, it is required to track the vehicles for their identification. This is not feasible as most consumers will not like others to know about their personal identification. Therefore this has to come in equilibrium and a tradeoff must be maintained between the authentication and privacy of the nodes.

2) *High Mobility & Volatility:* The network in Vanet is highly volatile. Due to high mobility most of the communication occur between nodes that never interacted before. These nodes are in continuous motion in their own directions and due to this the connection between them lasts for very small amount of time. Therefore a learning based scheme should be introduced so that they learn to know about each others behavior.

3) *Location Awareness:* Most VANET applications require certain effective location based services. The increased reliance of VANET on GPS or other specific location based instruments may effect its applications in case of occurrence of any error.

4) *Real-time guarantees:* Most of the applications in VANET requires time critical messages, like collision avoidance, hazard warning and accident warning information etc. Hence strict deadlines for the delivery of messages must be met.

5) Liability v/s Privacy: Liability offers the opportunity for legal investigation. In some specific cases, this data can’t be denied, when required. On the other hand each driver must have the ability to keep his personal information protected from others. Hence privacy must not be violated.

6) Network Scalability

The scale of the vehicular network in the world is exceeding continuously and as this number is growing, another problem is arising. As we know that there is no global authority to govern the standards for this network in the world. For example: DSRC standards in North America are different from that in Europe.

VI. Conclusion

Vehicular Adhoc Networks have gained a lot of attention for various applications that they offer. The wide variety of services that they provide include- applications ranging from safety and crash avoidance to Internet access and multimedia In this paper various aspects of VANET like its architecture and various characteristics have been listed which distinguishes it from other networks like MANET ; furthermore various attacks and challenges have been discussed. In this paper, I have briefly introduced Vehicular Ad Hoc Network and various challenges associated with its security services. VANET is an emerging research area with a promising future along with some great challenges in its security.

REFERENCES

[2] Ankita Agrawal, Aditi Garg, Niharika Chaudhiri, Shivanshu Gupta, Devesh Pandey, Tumpa Roy, "Security on Vehicular Ad Hoc Networks (VANET) : A Review Paper", International Journal of Emerging Technology and Advanced Engineering , 3(1), (pp. 231-235), January 2013.

[3] Megha Nema, Prof. Shalini Stalin, Prof. Vijay Lokhande, "Analysis of Attacks and Challenges in VANET", International Journal of Emerging Technology and Advanced Engineering, 4(5), (pp. 831-835), July 2014.

[4] Sherali Zeadally · Ray Hunt · Yuh-Shyan Chen · Angela Irwin · Aamir Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges", ©Springer Science + Business Media LLC, (pp. 217-241), December 2010.

[5] Sourav Kumar Bhoi, Pabitra Mohan Khilar, "Vehicular communication: a survey", ©The Institution of Engineering and Technology, 3(3), (pp. 204-217), August 2013.

[6] Rizwanul Karim Sakib, Bisway Reza, "Security issues in VANET", Department of Electronics and Communication Engineering, BRAC University, Dhaka Bangladesh, (pp. 1-31), April 2010.

[7] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures, "Security Analysis of Vehicular Ad Hoc Networks (VANET)" ,Proceedings of Second International Conference on Network Applications, Protocols and Services, (pp. 55-60), 2010.

[8] Maria Elsa Mathew, Arun Raj Kumar P., "Threat Analysis and Defence Mechanisms in VANET", International Journal of Advanced Research in Computer Science and Software Engineering, 3(1), (pp. 47-53), January 2013.

[9] Ahmad Yusri Dak, Saadiah Yahya, and Murizah Kassim, "A Literature Survey on Security Challenges in VANETs", International Journal of Computer Theory and Engineering, 4(6), (pp. 1007-1010), December 2012

[1] Jose Maria de Fuentes, Ana Isabel Gonzalez- Tablas, Arturo Ribagorda, "Overview of security issues in Vehicular Ad-hoc Networks", Handbook of research on Mobility and Computing, 2010.