A Study of Vanet Security Issues and Protocols

Ronak Juneja , Mona Sharma

1,2 Dronacharya College of Engineering,Farrukh Nagar,Gurgaon, India

Abstract-
Vehicular Ad Hoc Networks (VANET) is a subclass of Mobile Ad Hoc networks. In VANET, Wireless device sends information to nearby vehicles, and messages can be transmitted from one vehicle to another vehicle or roadside infrastructure. So, using VANET we can increase safety and traffic optimization. Similar to other technologies, in VANET there are some important and noticeable issues. One of the most important of them is Security. Since the network is open and accessible from everywhere in the VANET radio range, it is expected to be an easy target for malicious users. Therefore, the survey of the security protocols in VANET is important. This paper discusses VANET related security issues, attacks and protocols. Finally, a comparison of the various VANET security protocols is shown.

Keywords-Swarm intelligence,Wi-Fi,WiMax,Zigbee,DSRC

I.INTRODUCTION

A Vehicular Ad Hoc network(VANET) is a form of Mobile Ad Hoc network which provide communication among nearby vehicles and between vehicles and nearby fixed equipment like the roadside equipment. The main goal of VANET is to provide safety and comfort for passengers. Each vehicle equipped with VANET device will be a node in the Ad-hoc network and can receive and relay other messages through wireless network[6]. With the sharp increase of vehicles on roads in the recent years, driving has become more challenging and dangerous. Now a days, roads are saturated, therefore, the safety distance and reasonable speeds are highly valued. The leading car manufacturers have decided to jointly work with government agencies to develop a solution which aimed at helping drivers on the roads by anticipating hazardous events or bad traffic areas. One of the outcomes is a novel type of wireless access called wireless access for vehicular environment (WAVE) used for vehicle to vehicle and vehicle to road side communication[1]. VANET integrates multiple Ad-Hoc networking technologies such as WiFi IEEE 802.11 b/g, WiMAX 802.16, Bluetooth, IRA, Zigbee for accurate, effective and simple communication between vehicles on dynamic mobility[2].

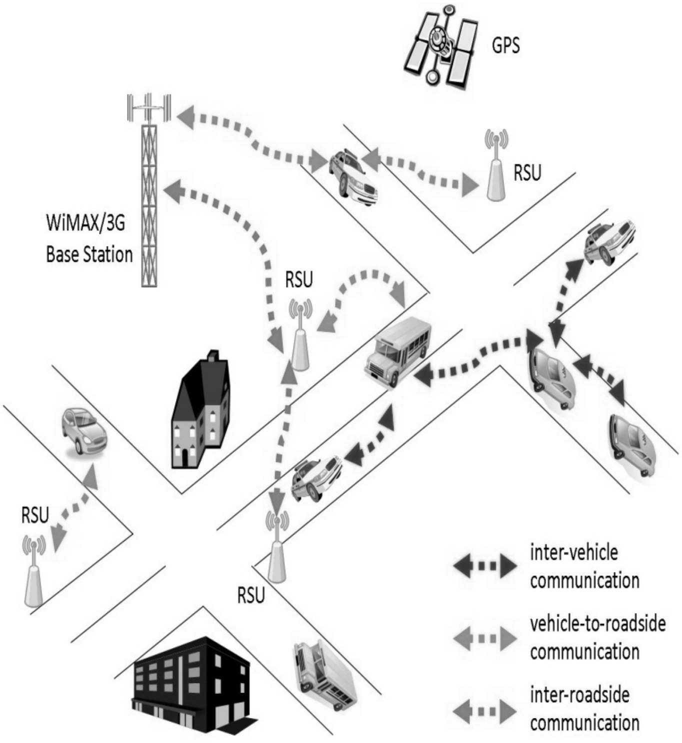
GPS
WiMAX/3G
Base Station
RSU
RSU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

Fig 1.Vanet Structure

II. SECURITY REQUIREMENTS IN VANET

The issue of security in VANETs is particularly challenging due to it’s unique features, such as high-speed mobility of the network nodes or vehicles and the sheer size of the network. Specifically, it is essential to make sure that "life critical safety" information cannot be inserted or modified by an attacker[6]. While the system should be capable of establishing the liability of drivers, it should protect their privacy as much as possible. Any type of malicious user behavior, such as a modification and replay attack of the disseminated messages, will be fatal to other users. In the past few years, considerable effort has been spent in research on VANET networking protocols and applications[3]. However, research on security ,threats and reliability of VANETs has started only recently. VANET security should satisfy the requirements which are mentioned below.

A.Entity Authentication

The receiver is not only ensured that the sender send the message, but in addition has evidence that the sender is a network node.

B.Liability Identification

Users of vehicles should be held responsible for their deliberate or accidental actions that disrupt the operation of other nodes in the transportation system. As part of the "conditional privacy" requirement, the authorities should be able to determine the identities of message senders in the case of a dispute[6].

C.Access Control

Local policies determine access to specific services provided by the infrastructure node and other node.

D.Message Confidentiality

The content of a particular message is kept secret from those nodes that don't have the right to access it.

E.Message Authentication and Integrity

Messages must be protected from any modification and the receiver of the message must confirm the sender of the message.

F.Availability

The network and nodes should remain available even in the presence of faults or malicious conditions. This requires not only secure but also a fault-tolerant design, survivable protocols, which resume their normal operations after the removal of the faulty conditions.

G.Privacy and Anonymity

Conditional privacy must be achieved in the way that the user-related information has to be protected from unauthorized access, but on the other hand, authorities should be able to access such information to look for witnesses in case a of dispute such as a crime or a car accident scene investigation. The user-related information includes the driver name, license plate, speed, position, and travelling routes[4].

H.Message Non-Repudiation

The sender of a message cannot deny having sent the message[6].

I.Real-time constraints

Vehicles move in high speed, this will require a real-time response in some situation, or the result will be devastating [7]. Current plans for vehicular networks rely on the emerging standard for dedicated short-range communications (DSRC), based on an extension to the IEEE 802.11 technology.

III.ATTACKS IN VANET

In this paper we are mainly concentrating on attacks against the message itself rather than the vehicle, as physical security is not in the scope of this paper.

A.Denial of Service attack

This attack happens when the attacker prevents critical information from arriving by taking control of a vehicle's resources or jams the communication channel used by the Vehicular Network. It also increases the danger to the driver, if it depends on the application's information. For instance, if a malicious user wants to create a massive pile up on the highway, it can make an accident and use the DoS attack to prevent the warning from reaching to the approaching vehicles [8], [7], [9], and [10]. Authors in [8] discussed a solution for DoS problem and according to them the existing solutions such as hopping do not completely solve the problem, the use of multiple radio transceivers, operating in disjoint frequency bands, could be a feasible approach but even this solution will require adding new, better and more equipments to the vehicles, and this will need more funds and more space in the vehicle. The authors in [12], proposed a solution by switching between different channels or even communication technologies like DSRC, UTRA-TDD, or even Bluetooth for very short ranges if they are available, when one of them is brought down.

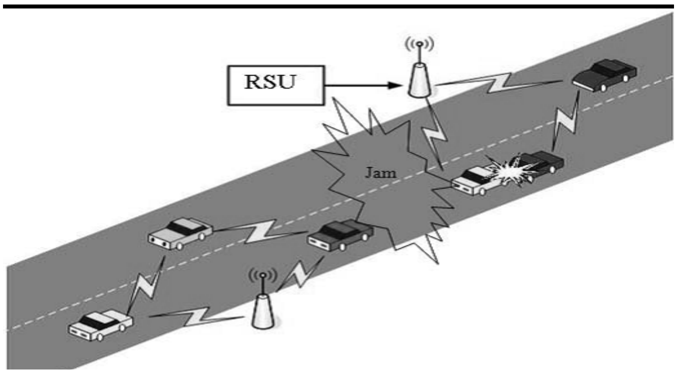

Fig 2.DOS attack

B.Message Suppression Attack

An attacker selectively dropping packets from the network, these packets may hold critical information for the receiver, the attacker suppress these packets and can use them again in other time[7]. The goal of such an attacker would be to prevent registration and insurance authorities from learning about collisions involving his vehicle and/or to avoid delivering collision reports to roadside access points [11]. For example, an attacker may suppress a congestion warning, and use it in some another time, so vehicles will not receive the warning and will be forced to wait in the traffic.

C.Fabrication Attack

An attacker can make this attack by transmitting false information into the network, the information could be false or the transmitter could claim that it is somebody else. This attack includes fabricate messages, warnings, certificates, identities [7], [10] [11].

D.Alteration Attack

This attack happens when attacker alters an existing data, it includes delaying the transmission of the information, replaying earlier transmission, or altering the actual entry of the data transmitted [7]. For instance, an attacker can alter a message telling other vehicles that the current road is clear while the road is congested [11].

E.Replay Attack

This attack happens when an attacker replay the transmission of an earlier information to take advantage of the situation of the message at time of sending [7]. Basic 802.11 security provides no protection against replay. It does not contain sequence numbers or timestamps. Because of keys can be reused, it is possible to replay stored messages with the same key without detection to insert false messages into the system. Individual packets must be authenticated, not just encrypted. Packets must have timestamps. The goal of such an attack would be to confuse the authorities and possibly prevent identification of vehicles in hit-and-run incidents [11].

F.Sybil Attack

This attack happens when an attacker creates large number of pseudonymous, and claims or acts like it is more than a hundred vehicles, to tell other vehicles that there is jam ahead, and force them to take alternate route[7],[12]. Sybil attack depends on how cheaply identities can be generated, the degree to which the system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the system treats all entities identically. For example an attacker can pretend and act like a hundred vehicle to convince other vehicles in the road that there is congestion, so that they take another road and that road will be clear.

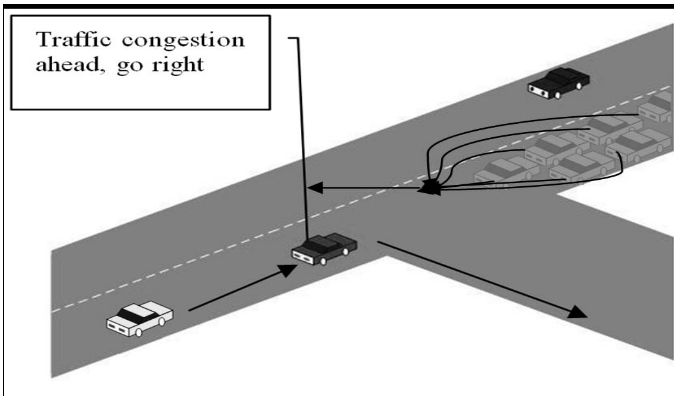

Fig 3.Sybil attack

IV.OVERVIEW OF SECURITY PROTOCOLS

In VANET, the following security protocols have been proposed:

A. A Security Protocol distributed systems for Vehicular

This protocol guarantees that the content of messages remains intact against possible attacks. Because privacy of the passengers must be preserved in VANET, this security protocol is designed to not to rely on the driver's identity. The protocol also proves the time and location when a message was sent[6]. The security protocol considers the particular characteristics of VANETs. It ensures data integrity, reliability, non-repudiation, preserves privacy and links a message to a particular time and place when the message was generated. The security protocol is implemented in VANET simulator and the evaluation result shows its capability to handle a wide range of attacks that are characteristic to such environments[5].

B.A Secure VANET MAC Protocol for DSRC applications

A secure MAC protocol for VANETs assigns priorities to message for different types of applications to access DSRC channels. The MAC protocol can provide secure communications and at the same time guarantee the reliability and latency requirements of safety related DSRC applications for VANETs. The secure communication protocol is designed to guarantee the freshness of the message, message authentication and integrity, message non- repudiation, and privacy and anonymity of the senders.

C. Cognitive security protocol for sensor based VANET using swarm intelligence

The cognitive security protocol distributes information using distributed sensor technology while prioritizing prevention of data aging, efficient quality of service (QoS) and robustness against denial-of-service (DoS) attack. The reliability and optimality of the protocol is computed based on current mission response time and thus maintaining message authentication, integrity, confidentiality and non-repudiation. DoS, is an act by adversary to reduce the reliability of the application. The DOS attacks leads to packet loss, localization error and loss of integrity of information transmitted. Due to the varied design constraints and missions in VANET, a nature inspired framework and optimization technique is applied to the protocol. The process of identifying an intrusion is based on agent's performance matrices i.e., PDR energy, BER, distance, hop stored in the tubulise form[6]. When the agent senses a sudden change in PDR from its previous tour, it flags the node and updates globally.

D. Real-World VANET security protocol

Real-world VANET security protocol used recordings of actual vehicle movements on various roadways. The simulation of the protocol used as input, traces of vehicles movements that have been generated by traffic simulators which are based on traffic theory models[3]. In order to enable analysis on this scale, a new VANET simulator is developed, which can handle many more vehicles than NS-2[6]. To use this simulator, the researcher presented results of a cross-validation between NS-2 and their simulator, showing that both simulators produce results that are statistically the same. The evaluations are performed using real vehicle mobility, which is the first simulation using real vehicle mobility[5].

E. A secure fire truck communication protocol for VANET

A secure fire truck communication protocol is a secure emergency vehicle transmission protocol to ensure the messages will not be revealed or stolen. The protocol combines symmetric encryption and digital signature mechanism[2].The protocol can achieve the mutual authentication, session key security, known-key security and prevent the known attacks. This protocol mainly works efficiently in urban environment.

Table 1: Comparison of various VANET protocols[6]

Protocols	**A Security Protocol distributed systems f or Vehicular**	**A Secure VANET MAC Protocol for DSRC applications**	**Cognitive security protocol for sensor based VANET using swarm intelligence**	**Real-World VANET security protocol**	**A secure fire truck communication protocol for VANET**
Data integrity	Yes	Yes	Yes	No	Yes
Reliability	Yes	Yes	Yes	Less reliable	Less reliable
Non-repudiation	Yes	Yes	Yes	Yes	Yes
Authentication	Yes	Yes	Yes	Yes	Yes
Scenario	Urban	Urban	Urban	Urban	Urban
Realistic traffic flow	No	No	No	Yes	No

V. CONCLUSION

This paper provided a brief idea about vehicular ad hoc network ,various attacks on it and security requirements for vanet. It also analyzed and compared various vanet security related protocols. All the protocols discussed above provide data integrity except the real-world VANET security protocol .All the security protocols discussed above ensure message non-repudiation. Entity Authentication ensures that the receiver is not only ensured that the sender generated the message, but in addition has evidence that the sender is a network node. The future perspectives for VANET security protocols should include firstly a major challenge in protocol design in VANET is to improve reliability of Protocols and to reduce delivery delay time and the number of packet retransmission. And secondly to design and implement the protocols for rural environments as well.

VI.REFERENCES

[1] Catalin Gosman, Ciprian Dobre, Valentin Cristea, "A Security Protocol for vehicular distributed systems", 12th international conference on symbolic and numeric algorithms for scientific computing (SYNASC), pp. 321-327, 2010,IEEE digital library.

[2] Jason J. Haas and Yih-Chun Hu, Kenneth P.Laberteaux, "Real-World VANET Security Protocols Performance",

Globecom, pp. 1-7,2009, IEEE digital library.

[3] Rajani Muraleedharan and Lisa Ann Osadciw, "Cognitive Security Protocol for Sensor Based VANET Using Swarm Intelligence", Asilmore, pp. 288-290, 2009.

[4] Shankar Yanamandram, Hamid Shahnasser, "Analysis of DSRC based MAC protocols for VANETs", International conference on ultra modern telecommunications and workshop,

2009.

[5] Chin-Ling Chen, Chun-Hsin Chang, "A Secure fire truck communication protocol for VANET", Department of Computer Science and Information Engineering, Chaoyang University of

Technology, Taiwan.

[6]Simple Nain and Sandeep Tayal, A comparative study of the Security Protocols in VANET , International Conference on Emerging Trends in Engineering and Management

[7] B. Parno and A. Perrig, “Challenges in Securing Vehicular Networks”, Proc. of HotNets-IV, 2005.

[8]M Raya, P Papadimitratos, JP Hubaux, “Securing Vehicular Communications”, IEEE Wireless Communications, Vol 13, October 2006 . [9] I Aad, JP Hubaux, EW Knightly, ”Impact of Denial of Service Attacks on Ad Hoc Networks”, Networking, IEEE/ACM Transactions on Volume 16, August, 2008.

[10] Raya, J Pierre Hubaux,” The security of VANETs”, Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks, 2005. [11]security & Privacy for DSRC-based Automotive Collision Reporting

[12] J. Douceur,” the Sybil Attack”, First International Workshop on

Peer-to-Peer Systems, 1st ed, USA, Springer, 2003.