Survey Security Issues in Vehicular Ad-Hoc Network(VANET)

Sandip Kumar Shaw IHC2017008
Neeraj Kumar IHC2017009
Ankit Kumar IHC2017011
Mangesh Matke IWC2017003
Praveen Chaudhary IWC2017004

***Abstract*—Vehicular Ad-hoc Networks (VANETs) are becoming new research are for the researchers. As in VANET the vehicles are connected through each other ,there are a lot of security issues that need to be taken care of.Thus, designing security mechanisms to authenticate and validate transmitted message among vehicles and remove adversaries from the network are significantly important in VANETs. The communication between car to car, car to roadside unit done through wireless communication. That is why security is an important concern area for vehicular network application. For authentication purpose so many bandwidth is consumed and the performance becomes low. In this paper we have discussed about several security attacks on VANET and there approaches to defend against them**

I. Introduction

Vehicular Ad hoc Networks(VANET) are special case of ad hoc networks that, besides lacking infrastructure, communicating entities move with various accelerations.VANETs have achieved widespread applicability in different application domains related to transportation systems such as providing public safety and assistance, driving improvement, toll collection, roadside service finders, traffic monitoring and control, highway Internet access and enhancing safety and efficiency of highway systems.VANET shave different applications which can be applied by Peer-to-Peer (P2P) communication or via multi-hop communication. VANETs are called Inter-Vehicle Communications(IVC) or Vehicle-to-Vehicle communications (V2V); its applications are like cooperative traffic monitoring, optimization of a route to a destination, collision prevention, weather forecasting, and broadcasting information like advertisements for some goods, commodity and online services.VANETs are considered a subclass of MANETs (Mobile Ad Hoc Networks); but there some differences like topology change frequently with high speeds, high probability of network fragmentation since there are speedy vehicles,no strict limitations of power consumption, operation at large scales inside cities and their edges and high ways,and depending on vehicles behaviors in response or re-action for delivered messages [2]. Vehicles have specific units which make them communicate with other vehicles.These units are called Survey on Security Issues in Vehicular Ad Hoc Networks On-Board Units (OBUs).In addition, the architecture of VANETs can take different styles which are cellular/WLAN (Wireless Local Area Network), ad hoc, and hybrid. For the first architecture, the vehicles receive and exchange data with base stations (also know by Road-Side Units (RSUs)) or fixed remote entities (V2R Communications). In the second one, the vehicles exchange messages directly together without intermediate entities (V2V communications). Finally, the hybrid architecture combines the last two architectures [1]. Furthermore, vehicles in VANET transmit self-information to fixed remote nodes such as their speed, direction, acceleration and traffic conditions.In this survey, we provide in the first section, an overview of VANETs, security requirements, their challenges and security attacks. Then, a classification of attacks in VANETs due to different network layers will be presented in the second section. Finally, conclusions and some recommended future issues will be discussed. Fig. 1 shows the structure of our survey.

II. How VANET works?

VANETs are special case of ad-hoc networks that the communicating entities are vehicles, and have unfixed or no infrastructure.
In VANETs, there are two types of communications:
(1)Vehicle to vehicle (V2V)
(2)Vehicle to infrastructure(V2I).
Vehicles have On Board Units (O BUs), which consist of Omni directional antennas, processors, GPS unit, and sensors for V2V communications. Vehicles also perform V2I communications with roadside infrastructures, which are placed within a fixed distance of each other depending upon the communication range of the roadside devices, also known as Road Side Units (RSUs)
RSUs communicate each other through wireless medium or wired connections. They can also be mobile. The V2I communications can be further extended to provide applications such as Internet since RSUs can be connected to a network.
The V2V communications can be used to send emergency and real-time information such as an accident or road traffic information so that other vehicles can take alternative routes to prevent traffic congestion. The communications between nodes done through using radio signals, range of these signals can reach up to 1 KM. Communications between nodes that have distance exceeds the signal range demand messages to hop across multiple nodes.

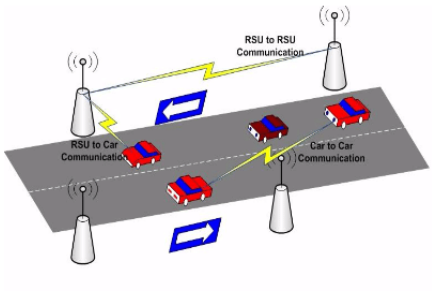

Fig. 1. VANET Structure

III. Security Requirements

1.) Vehicle Privacy and Anonymity: The transferred messages have to be accessed by authorized vehicles and remote nodes, and not to be exposure by misbehaved vehicles.
2.) Vehicle ID Trace ability: the ability to retrieve real identities of vehicles which sent messages.
3.) Anti-Jamming: malicious vehicles send interfering messages to drop communication between legitimate vehicles.
4.) Resistance against In-Transit Traffic and On-Board Tampering: In-transit traffic tampering is that a malicious vehicle can corrupt or capture data of other vehicles when it is an intermediate node (in multi-hop communication). In on-board tampering, a vehicle can know specific information about a certain vehicle such as velocity and location.
5.) Access Control: vehicles should have the capability of accessing available services offered by remote nodes.

IV. Security Attacks

In this section, we present several security attacks on Vehicular Ad-hoc Networks (VANETs).

A. Denial of Service (DoS)

Attackers may transmit dummy messages to jam the channel and thus, reduce the efficiency and performance of the network Figure 3 illustrates that a malicious black car transmits a dummy message Lane close Ahead to legitimate car behind it and also to an RSU to create a jam in the network.Denial of Service(DoS) attack can be done by the network insiders and outsiders

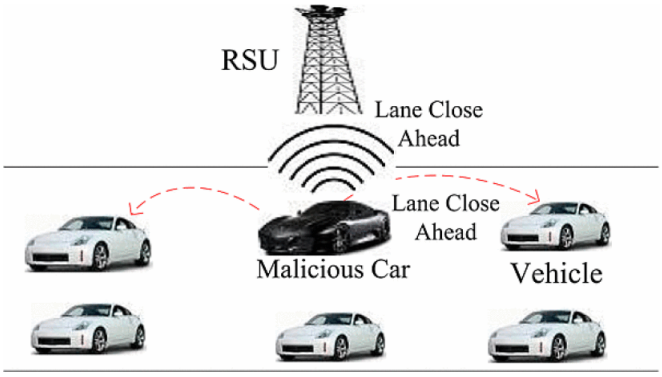

Fig. 2. DOS Attack

B. Black Hole Attack

A black hole is an area of the network where the network traffic is redirected.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.Existing solutions to black hole attacks consider designing protocols having more than one route to the destination, which imposes processing overload to the network.

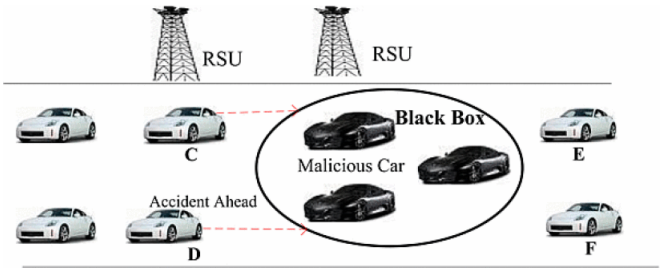

Fig. 3. Black Hole Attack

C. Wormhole Attack

In this attack, two or more malicious nodes create a tunnel to transmit data packets from one end of the network to another. The malicious nodes take the control of such a short network connection or link, threatens the security of transmitting data packets and delete them. The malicious nodes or wormholes can gain unauthorized access to perform Denial of Service (DoS) attacks.

D. Global Positioning System (GPS) Spoofing

This kind of attack allows the attacker to manipulate the received GPS signal inside the attacked area in an arbitrary way. Thus, receivers report time and location information as controlled by the attacker.In VANETs, the position information is must be accurate and authentic. This attack Spoofing or PFA (Position Faking Attack) transmitting to the neighbors node a information.

E. Sybil Attack

It this various messages are sent from one node with polymorphic identities. Except for various ultimate circumstances and hypothesis of chances of resource parity and organization among various entities , Sybil attack is possible.It creates turmoil in network when any node creates various copies of itself. All the forbidden and artificial ids and permit are claimed. This could smash the system creating crash in the network. This type of situation in network is called Sybil attack. Both internal and external attacks are possible in this system,in which the external attacks are possibly controlled by authentication but it cannot be done in internal attacks. Sybil attacks can be detected through resource testing. This approach assumes that all physical entities are limited to some resources.

F. Man in the Middle Attack (MiMA)

The man in the middle attack, attack in which an attacker between the main connection between the host and the client and Causing the attacker to impersonate the client as the default host to send information to an attacker ,The attacker to forge customer information it communicates with connect to the host.In MiMA attacker listen the communication between the vehicles and inject false or modified message between the vehicles.

G. Masquerade

A vehicle fakes its identity and pretends to be another vehicle for its own advantage. It is achieved using message fabrication, alteration, and replay. For instance, a malicious vehicle or attacker can pretend to be an ambulance to defraud other vehicles to slow down and yield.

H. 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. Basic 802.11 security has no protection against replay. In this attack, the attacker reinsert packets that have been previously used by nodes into the network, this can poison a nodes location table by replaying bacons. The goal of such an attack would be to confuse the authorities and possibly prevent identification of vehicles in hit-and-run incidents.

V. SECURITY SOLUTIONS

To provide secure VANET, many researchers introduced set of solutions to solve different security problems in VANET, researchers in, and proposed the using of Vehicular Public Key. Infrastructure (VPKI), here every node sends safety message, it signs that message with its private key,and attaches it with Certificate Authority (CA).

The receiver party of the message, will get the public keyof the sending party by using the certificate, and check the signature of that sender, using its certified public key, but this solution requires that the CA public key be known by the receiver party. He sham et al. proposes a dynamic key distribution protocol that handles key management without the need to store a large number of keys for PKI support and thus, reduces the usages of Tamper Proof Device (TPD).

Gazder proposes efficient dynamic cluster-based architecture of the Public Key infrastructure (PKI) for Vehicular Ad hoc Networks (VANETs) based on a trust model. Each vehicle will have a trust value in the range [0], [1] where anew vehicle in the network starts with 0.1. The vehicle with trust value 1 is the most authentic and confident vehicle.

Public Key Infrastructure (PKI) and symmetric key cryptography are not the best schemes to provide security in VANETs since they are infrastructure-less. Hence, ID-based cryptography that covers the best features of other security schemes is also being explored by the research community.For instance, ID-based cryptography reduces the computational cost in the ID-based

VI. CONCLUSION

In this paper we have discussed about different security issues for Vehicular Ad-hoc Network and different security solution for particular security attacks.This survey gave us a wide analysis for the current challenges and solutions, and critics for these solution, This paper gave a wide analysis for the current challenges and solutions, and critics for these solution.

VII. ACKNOWLEDGMENTS

The authors would like to thank all the teaching assistants, Dr. Soumyadev Maity for their valuable suggestions and for his teachings in the class from where we got the ideas of most of the concepts whenever needed to improve the report.

VIII. FUTURE WORK

Distributing certificates securely, validating them very fast and computationally efficient way should be given more attention while designing secured routing protocols for VANETs. Determining the mobility pattern of vehicles and linking the mobility pattern with malicious vehicles could be considered as a potential research in providing security and privacy in VANETs. Determining and assigning trust values to vehicles and establishing trust among vehicles are significantly important to provide the integrity and reliability of applications in VANETs.

REFERENCES

[1] Bassem Mokhtar, Mohamed Azab, Survey on Security Issues in Vehicular Ad Hoc Networks, Alexandria Engineering Journal (2015) 54, 11151126, accepted 22 July 2015

[2] Mohammed Saeed Al-kahtani, Survey on security attacks in Vehicular Ad hoc Networks (VANETs), 12-14 Dec. 2012, Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference.

[3] Arif Sari, Murat Akkaya, Review of the Security Issues in Vehicular Ad-Hoc Networks (VANET), Int. J. Communications, Network and System Sciences, 2015, 8, 552-566 , Published Online December 2015 in SciRes.