 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

Vehicular Ad-Hoc Networks (VANETs): A Survey

[1]Er. Archana Phutela, [2]Er.Tulika Mehta
[1]M.Tech, Dept. of CSE, Poornima College of Engineering, Jaipur, Rajasthan, India
[2]Panjab University, UT, Chandigharh, India

Abstract
Wireless networks are gaining popularity now days, as the users require wireless connectivity irrespective of their geographic position. VANETs are the promising approach to provide safety and other applications to the drivers as well as passengers. In this paper we discuss the VANET architecture, security issues, characteristics in VANETs and current solutions to these attacks.

Keywords
VANET, Routing Protocol, Security Issues and Challenges

I. Introduction

With the development in the field of wireless communications, ITS (Intelligent transport system) applications are developed based on car-to-car communication standards such as Wireless Access in Vehicular Environments (WAVE) and Dedicated Short Range Communications (DSRC). WAVE and DSRC standards are defined in IEEE 1609.1-4 and 802.11p respectively. The fact that FCC has allocated dedicated 75 MHz frequency spectrum in the range 5.85 GHz to 5.925 GHz to be used only for Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication. This new application clearly indicates that this is much more than a trend and it is destined to grow into a commercially viable technology.

VANETs can be considered as a subset or special case of Mobile Ad Hoc Networks (MANETs) which have been studied extensively in the literature [1]. The research in this area is relatively new and it essentially spans the last decade. While some significant progress has been made, it is fair to say that several key research and development problems remain open [5]. In terms of V2V communications, the use of both radio (very high frequency (i.e., VHF), micro, and millimeter waves) and infrared waves have been reported in experimental V2V systems [6-8]. While infrared and millimeter waves can support only line-of-sight communications, VHF and microwaves can support broadcast communications as well. VHF can provide long links but at low speed and for this reason the mainstream mode of communications is to use microwaves.

Using vehicular communications, drivers can be well informed of vital traffic information such as treacherous road conditions and accident sites by communicating amongst vehicles and/or with the roadside infrastructure. With the large information of traffic conditions, vehicles will have better knowledge and it is reasonable that the problem of road accidents can be alleviated. Vehicular communications also facilitate traffic monitoring and management in order to raise traffic flow capacity and improve vehicle fuel economy.

A Vehicular Ad hoc Network (VANET) is a kind of wireless ad hoc network to provide communications among vehicles and nearby roadside equipments. VANET consists of vehicles with on-board sensors and roadside units (RSUs) deployed along highways/sidewalks, which provides communications between vehicle-to-vehicle (V2V) and communications between vehicles-to-infrastructure (V2I) as shown in fig. 1. When RSU receives a message from vehicle, it authenticates the message to ensure no malicious message. The Autonomous Server (AS) is responsible for security related issues between vehicle and RSU.

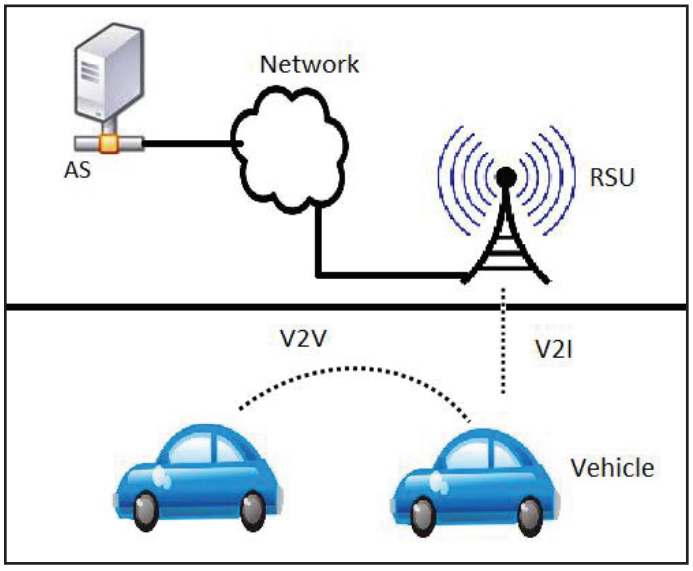

Fig. 1: VANET Architecture

II. Possible Attacks in VANETs

There are a numbers of possible attacks in VANETs. The purpose of these attacks is to create problem for users to access the system or phising some information. Derived are some definition of attacks.

A. Denial of Service Attack

The attacker attacks the communication medium or network's nodes to cause the channel or some problem to networks or nodes. The vehicle is unable to access the networks and result in devastation and overtiredness of the nodes and network's resources. None of the reseachers are focusing on DoS and DDoS attack in VANETs as up to date.

B. Message Suppression Attack

An attacker selectively dropping packets from the packets, these packets may hold critical information for the receiver, the attacker suppress these packets and can use them again in other time [5].

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 [17].

For instance, an attacker may suppress a congestion warning, and use it another time, so vehicles will not receive the warning and forced to wait in traffic.

C. Fabrication Attack

An attacker can make this attack by transmitting wrong information into the network. This attack include fabricate messages, warnings, certificates and identities [5, 7, 17].

D. Alteration Attack

This attack can happens when attacker alters an existing data,

it includes delaying the transmission of information, replaying earlier transmission, or altering the actual entry of data transmitted [5]. For example, an attacker can alter a message telling other vehicles that the current road is clear while the road is congested [17].

E. 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 a jam ahead, and force them to take alternate route [5, 8].

For example, a terrorist can make a claim that there is congestion on road by acting like a hundred of vehicles to divert traffic on other side before detonating a bomb, as shown in fig. 2.

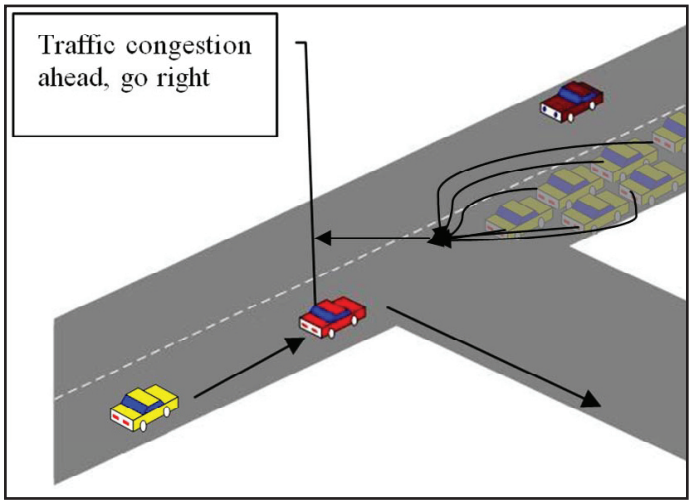

Fig. 2: Sybil Attack

III. Characteristics of VANETs

VANET is an application of MANET but it has its own distinct characteristics which can be summarised as:

A. High Mobility

The nodes in VANETs usually are moving at high speed. This makes harder to predict a node's position and making protection of node privacy [2].

B. Rapidly Changing Network Topology

Due to high node mobility and random speed of vehicles, the position of node changes frequently. As a result of this, network topology in VANETs tends to change frequently.

C. Unbounded Network Size

VANET can be implemented for one city, several cities or for countries. This means that network size in VANET is geographically unbounded.

D. Frequent Exchange of Information

The ad hoc nature of VANET motivates the nodes to gather information from the other vehicles and road side units. Hence the information exchange among node becomes frequent.

E. Wireless Communication

VANET is designed for the wireless environment. Nodes are connected and exchange information via wireless. Therefore some security measure must be considered in communication.

F. Time Critical

The information in VANET must be delivered to the nodes with in time limit so that a decision can be made by the node and perform action accordingly.

G. Sufficient Energy

The VANET nodes have no issue of energy and computation resources. This allows VANET usage of demanding techniques such as RSA, ECDSA implementation and also provides unlimited transmission power.

H. Better Physical Protection

The VANET nodes are physically better protected. Thus, VANET nodes are more difficult to compromise physically and reduce the effect of infrastructure attack.

I. Routing Attack

Routing attacks re the attacks which exploits the vulnerability of network layer routing protocols. In this type of attack the attacker either drops the packet or disturbs the routing process of the network. Following are the most common routing attacks in the VANET:

1. Black Hole Attack

In this type of attack, the attacker firstly attracts the nodes to transmit the packet through itself. It can be done by continuous sending the malicious route reply with fresh route and low hop count. After attracting the node, when the packet is forwarded through this node, it silently drops the packet.

2. Worm Hole Attack

In this attack, an adversary receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. This tunnel between two adversaries are called wormhole. It can be established through a single long-range wireless link or a wired link between the two adversaries. Hence it is simple for the adversary to make the tunnelled packet arrive sooner than other packets transmitted over a normal multi-hop route.

3. Gray Hole Attack

This is the extension of black hole attack. In this type of attack the malicious node behaves like the black node attack but it drops the packet selectively. This selection can be of two type:

- A malicious node can drop the packet of UDP whereas the TCP packet will be forwarded.
- The malicious node can drop the packet on the basis of probabilistic distribution.

IV. Security Issues in VANETs

Among the main cryptographic requirements to solve security issues in VANETs are:

A. Availability

The network must be available at all times in order to send and receive messages. Two possible threats to availability are for example DoS and jamming attacks. Another availability problem might be caused by selfish nodes that do not provide their services for the benefit of other nodes in order to save their own resources like battery power.

B. Confidentiality
Secrecy must be provided to sensitive material being sent over the VANET, like in certain commercial applications.

C. Integrity
Messages sent over the network should not be corrupted. Possible attacks that would compromise their integrity are malicious attacks or signal failures producing errors in the transmission.

D. Authenticity
The identity of the nodes in the network must be ensured. Otherwise, it would be possible for an attacker to masquerade a legitimate node in order to send and receive messages on its behalf.

E. Non-Repudiation
A sender node might try to deny having sent the message in order to avoid its responsibility for its contents. Non repudiation is particularly useful to detect compromised nodes.

V. Current Proposed Solutions
In VANET many security solutions been proposed, and large number of papers were introduced to solve the above problems, the authors in [1] and in [7] suggested the use of VPKI as a solution, where each node will have a public/private key. When a vehicle sends a safety message, it signs it with its own private key and adds the Certificate Authority (CAs) certificate as follows:
V → r: M, SigPrKV [M|T], Certv [7]
Where V is the sending vehicle, r represents the message receivers, M is the message, | is the concatenation operator, and T is the timestamp to ensure message freshness (it can be obtained from the security device).The receivers of the message will obtain the public key of V using the certificate and then verify V's signature using its certified public key. In order to do this, the receiver should have the public key of the CA [12]; this solution is cited in [3], [5], [10], and [11].
Authors in [18]suggested an idea of using the group signature, but this idea has a major drawback that it is causing a great overhead, every time that any vehicle enters the group area, the group public key and the vehicle session key for each vehicle that belongs to the group must be changed and transmitted, another issue must be considered that the mobility of the VANET prevents the network from making a static group, so the group is changing all the time, and the signatures and keys frequently changed and transmitted, group signature is also mentioned in [10, 19], as the authors proposed a protocol for guarantee the requirements of the security and privacy, and to provide the desired traceability and liability, but the result of the study was not quit encouraging, After 9 ms for group signature verification delay, the average message loss ratio was 45%, another result was the loss ratio reaches as high as 68% when the traffic load is 150 vehicles. The other solution been suggested is the use of CA and this requires infrastructure for it. VANET requires a large number of CA to govern it. until now we don't have a real authority that govern the world of VANET, the CA been suggested by [4], [7], [10], [11], [12], [13], all of these researchers mentioned the CA to handle all the operations of certificate : generating, renewing and revoking, and CA must be responsible in initiating keys, storing, managing and broadcasting the CRL. Authors in [1] also discussed how to maintain the authentication for the message, where vehicles will sign each message with their private key and attach the corresponding certificate. Thus, when another vehicle receives this message, it verifies the key used to sign the message and if everything is correct, it verifies the message, and they have proposed the use of ECC to reduce the overhead as mentioned before in section 4.1, while authors in [3] suggested another way to use the keys, by using short term certificates and long term, long term certificates are used for authentication while short term certificates are used for data transmission using public/private key cryptography. Safety messages are not encrypted as they are intended for broadcasting, but their validity must be checked; therefore a source signs a message and sends it without encryption with its certificate; other nodes receiving the message validate it using the certificate and signature and may forward it without modification if it is a valid message, so any adversary can inject false information as a safety message, as it doesn't to be encrypted, it also can steal the certificate from any other safety message and send unencrypted message contains false information along with the stolen certificate claiming that the safety message originated from another vehicle. Using VPKI in VANET accompanied with some challenges, like certificate of an attacker that must be revoked, authors in[1] discussed the Certificate Revocation solution, this solution is used to revoke the expired certificate to make other vehicles aware of their invalidity, and The most common way to revoke certificates is the distribution of CRLs (Certificate Revocation Lists) that contains all revoked certificates, but this method has some drawbacks: First, CRLs can be very long due to the enormous number of vehicles and their high mobility. Second, the short lifetime of certificates still creates a vulnerability window and last one is that there is no infrastructure for the CRL. It is also mentioned some protocols for revocations like RTPD (Revocation Protocol of the Tamper-Proof Device), RCCRL (Revocation protocol using Compressed Certificate Revocation Lists), and DRP (Distributed Revocation Protocol), these protocols also been discussed in details in [4], and been proposed in [11], saying that the use of CRL is not appropriate anymore and these protocols are better, but these methods rely on monitoring, so every vehicle has to monitor and detect all the vehicles around it, but this method didn't consider the reputation system, as it is a possible for number of adversary vehicles to make an accusation and causing of an unnecessary revocation, the best result obtained from DRP simulation is that just 25% if the current road vehicles will receive the warning, which is too low. Authors in [1] mentioned a solution that will help to maintain the privacy by using a set of anonymous keys that change frequently (every couple of minutes) according to the driving speed. Each key can be used only once and expires after its usage; only one key can be used at a time. These keys are preloaded in the vehicle's TPD for a long duration; each key is certified by the issuing CA and has a short lifetime (e.g., a specific week of the year). In addition, it can be traced back to the real identity of the vehicle ELP, the drawback of this solution that the keys need storage. In[3] authors mentioned that In the IEEE WAVE standard vehicles can change their IP addresses and use random MAC addresses to achieve security, IP version 6 has been proposed for use in vehicular networks. Cars should be able to change their IP addresses so that they are not traceable, however it is not clear how this will be achieved. Moreover this can cause inefficiency in address usage since when a new address is assigned the old address cannot be reused immediately. Delayed packets will be dropped when the car changes its IP address which causes unnecessary retransmissions. Authors in [5] added another proposed solution by making regular inspections, where in most U.S. states all vehicles must pass inspection once a year. This yearly trip to the mechanic provides interesting possibilities for security maintenance in addition to the typical maintenance to

be performed.

VI. Conclusion and Future Work

Vehicular Ad Hoc Networks is promising technology, which gives abundant chances for attackers, who will try to challenge the network with their malicious attacks. In this paper we have focussed on VANET architecture, its characteristics, security issues, attacks and some existing solutions to these attacks. As future work new solutions can be made to overcome these attacks in a better way and simulation test can be given to analyse the solutions to these attacks, so that one can easily compare all.

References

[1] M Raya, P Papadimitratos, JP Hubaux,"Securing Vehicular Communications", IEEE Wireless Communications, Vol. 13, October 2006 .

[2] H Fussler, S Schnaufer, M Transier, W Effelsberg, "Vehicular Ad-Hoc Networks: From Vision to Reality and Back", Proc. Of IEEE Wireless on Demand Network Systems and Services, 2007.

[3] GMT Abdalla, SM Senouci,"Current Trends in Vehicular Ad-Hoc Networks", Proceedings of UBIROADS workshop, 2007.

[4] M Raya, D Jungels, P Papadimitratos, I Aad, JP Hubaux, "Certificate Revocation in Vehicular Networks", Laboratory for computer Communications and Applications (LCA) School of Computer and Communication Sciences, EPFL, Switzerland, 2006.

[5] B. Parno, A. Perrig,"Challenges in Securing Vehicular Networks", Proc. of HotNets-IV, 2005.

[6] I Aad, JP Hubaux, EW Knightly,"Impact of Denial of Service Attacks on Ad-Hoc Networks", Networking, IEEE/ACM Transactions on Vol. 16, August, 2008.

[7] M Raya, J Pierre Hubaux,"The security of VANETs", Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks, 2005.

[8] J. Douceur,"The Sybil Attack", First International Workshop on Peer-to-Peer Systems, 1st ed, USA, Springer, 2003.

[9] F. Karnadi, Z. Mo,"Rapid Generation of Realistic Mobility Models for VANET", proc. IEEE Wireless Communications and Networking Conference, 2007.

[10] X Lin, R Lu, C Zhang, H Zhu, P Ho, X Shen,"Security in Vehicular Ad-Hoc Networks", IEEE Communications Magazine, Vol. 4, April 2008.

[11] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, JP Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks", IEEE Magazine, Vol. 10, October 2007.

[12] M Raya, J Pierre Hubaux,"The Security of Vehicular Ad Hoc Networks", Proc. of the 3rd ACM workshop on Security of ad hoc and sensor networks, 2005.

[13] P Papadimitratos, L Buttyan, JP Hubaux, F. Kargl, A. Kung, M. Raya,"Architecture for Secure and Private Vehicular Communications", 7th International Conference on ITS, 2007.

[14] R. Lind et al.,"The network vehicle. A glimpse into the future of mobile multimedia", IEEE Aerosp. Electron. Syst. Mag.,1999.

[15] [Online] Available: http://www.who.int/features/2004/road_safety/en/

[16] Car-to-Car Communications, www.car-2-car.org

[17] Security & Privacy for DSRC-based Automotive Collision Reporting.

[18] W Ren, K Ren, W Lou, Y Zhang,"Efficient user revocation for privacy-aware PKI", Proceedings of the 5th International ICST Conference, 2008.

[19] R Lu, X Lin, H Zhu, PH Ho, X Shen,"ECPP: Efficient conditional privacy preservation protocol for secure vehicular", In proceeding The 27th Conference on Computer Communications, INFOCOM 2008.

Er. Archana Phutela is M.Tech CSE, having three years working experience as Assistant professor, teaching various subjects related to computer science and specialized on Wireless networks. She is presently doing research on mobile Ad hoc networks and look forward and to achieve a mile stone in wireless networks.

Er. Tulika Mehta is an Electronics Engineering professional having worked previously with Telecom Industry. She is presently a young entrepreneur also associated to Panjab University contributing in research and development activities in the field of wireless communications. She is ME MBA from Panjab university Chandigarh and has published several technical research papers.