Impact of Threats on Vehicular Adhoc Network Security

F. Sabahi

***Abstract*—A vehicular ad-hoc network (VANET) is a new type of ad hoc network that is becoming even more popular than the original ad hoc concept. The structure of a VANET is built on mobile connectivity between car drivers and automobile equipment that informs the drivers about road status or other necessary travel information. The VANET is capable of improving the safety of the roads and reducing traffic congestion. However, VANETs face security issues typical of all networks. For example, some users may try to break into a VANET to use the service without paying for it, or for malicious purposes.**

In this paper, I discuss the security issues available in the VANET. In addition, I prioritize issues and introduce several families of attacks that have migrated from the original ad hoc networks to VANET. These are serious threats that are capable of crashing the VANET.

***Index Terms*—VANET, adhoc, security.**

I. Introduction

VANET is a type of wireless networks which are expected to support a large number of mobile applications in the roads. VANET tries to transmit useful information about road and traffic conditions as well as other information (e.g. traffic problem or accessing to the Internet). There are two main types of VANET:

- V2V (Vehicle to Vehicle): Communication establish between two or more vehicles
- V2R (Vehicle to Roadside): Communication establish between roadside equipment and available vehicles in the range of equipment.

But similar to adhoc which is base technology of VANET, there is no specific protocol which owing good security strategy. As we know, reason of this issue is most of Ad-hoc protocols has suffered from energy consumption problem and the protocols have to focus on reducing resource consumption. Although, it seems VANET has better situation because energy has not critical position as its predecessor. But security has critical situation in VANET similar to adhoc. Using VANET is increasing and security architecture must be carefully designed especially when it becomes a worldwide VANET which give service millions of vehicles in the roads. However, apart from security issues, VANET has noticeable benefits and some of benefits are listed below:

- Warn drivers about road conditions and dangers.
- Better route navigations.
- Accessing to the Internet within his cars.
- Ability of communicating between cars by using VANET.
- All car drivers can request help by using VANET.
- VANET resources are not as critical as adhoc and it help to produce protocols more stable than adhoc.
- In VANET there is ability to use static infrastructure such as roadside stations.

But in VANET there are some Problematic issues that most of them are about security. There are security issues in data integrity, privacy, and confidentiality that inherited from the Ad-hoc. In addition of these issues, there are some issues which can impact performance of VANET such as unpredictable temporary situation (e.g. existence of traffic jam because of an accident).

The security of VANETs is one of the most critical issues because of their transmission information is propagate in open access environments [1]. It is important that all transmitted data cannot be eavesdropped or changed by malicious users. Moreover, the system must be able to detect these malicious users in addition of there is a problem which is legitimate users who do not emphasize their privacy. It seems these problems in VANET are difficult to solve because of increasing network size, speed of the vehicles, their geographic position, and the randomness of the connectivity between them [2].

II. Security of VANET Protocols

In [3] there is a classification of three major group of behavior of attackers: “insider versus outsider”, “malicious versus rational”, and “active versus passive”. Most of protocols use cryptography schemes for authentication. In addition, there are other products for meeting security patterns which are able to use in VANET such as IPsec.

In term of security implementation there are several layers in proposed protocols to ensuring security but often-used way is layer 3 security[3],[4] As said before, one of most popular adhoc protocol which used in VANET is AODV. Unfortunately, AODV doesn’t define special security mechanisms. This problem exists in Ad-hoc previously and this lack of efficiency in security migrates to VANET and can cause occurred impersonation attacks easily [1]. There are a few solution for this problem because AODV is not a source based routing protocol and such a solution would introduce a tremendous overhead [2]. An overview of 802.11 protocol’s Media Access Control layer and location of security sub layer is illustrated in Fig. 1.

III. Privacy

Reflecting the architecture of the VANET, during a long trip at high speeds, a VANET user could pass through multiple VANET zones controlled by various service providers. Under the current access protocols for public wireless networks, this multiplicity of providers poses

Manuscript received June 21, 2012; revised August 7, 2012.

F. Sabahi is with the Azad University, Zanjan, Iran (e-mail: f.sabahi@ieee.org).

challenges for user privacy and network performance [4]. To deal with these challenges, it is necessary to implement a worldwide standard for the privacy policies of VANET service providers. Establishing effective privacy standards will also benefit network performance.

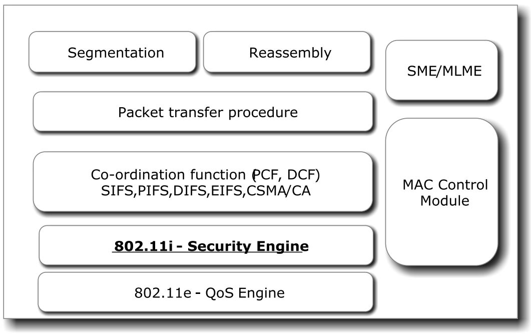
Segmentation
Reassembly
SME/MLME
Packet transfer procedure
Co-ordination function (PCF, DCF)
SIFS,PIFS,DIFS,EIFS,CSMA/CA
MAC Control Module
802.11i - Security Engine
802.11e - QoS Engine

Fig. 1. Magnetization as a function of applied field.

Generally, all drivers want their information be away from unauthorized observers such as trip path, speed or more important such as their identity [1]. There are solutions to achieve this goal if that information is not very important such trip path, for example using temporary keys which will be changed frequently and expires after usage [2], [5]. But if information becomes important such as home addresses the VANET provider must ensure its consumers about privacy. For example if a malicious user can access to home address of typical user of VANET, he will be able to plane a robbery when owner is not at his house.

IV. Threats

Because of the nature of open medium which used in VANET and lack of security in Ad-hoc protocols, VANET is vulnerable against several attacks. Attackers by using these vulnerabilities can reduce performance of the network and cause serious problem for legitimate users.

Similar to other types of networks, in VANET there are several threats which can impact performance and security of it. But VANET has potential to expand to worldwide network such as the Internet. Therefore, threats of VANET become a serious issue and all providers must adopt strong policy against them. Basically, attacks can be broadly categorized into three main groups [2]:

- Threats to availability
- Threats to authenticity
- Threats to driver confidentiality

A. *Threats to Availability*

The following threats are against the availability of V2V and V2R communications (including routing functionality) have been identified [2]:

Black Hole Attack: this threat is formed when nodes refuse to participate in the network or when an established VANET user drops out. When the user drops out, all network traffics are redirected to a specific user which does not exist at all and result is data lost.

Malware: malwares in VANETs can cause disruption to VANET normal operation. Malwares may be injected into the network when the cars' VANET unit and/or roadside station receive updates. Generally, malwares are more likely to be carried out by a malicious insider user rather than an outsider user.

Broadcast Tampering: this type of threats is injecting false safety messages into the network to cause serious problem. For example malicious user can cause an accident by suppressing fake traffic warnings.

Spamming: sending spam messages in VANETs can cause increasing transmission latency and consuming VANET critical resources.

Greedy Drivers: greedy drivers who will try to use network just for their own goals such as using resource more than regular users. These users make serious problem especially in hotspots because they cause overload problem for VANET. This happens because the prediction of condition made by VANET turns out to be wrong and therefore the legitimate users encounter with delayed service [1].

B. *Denial of Service*

There are several attacks in the network world but one of the most important of these threats is Denial of Service (DoS) attacks. This group of attacks has potential of becoming main problem in networks which have limitation in resources such as VANET. There are three types of DoS attacks which have destructive role in VANET that mentioned below [6]:

Overwhelm by consuming resources: The goal of this attack is to overwhelm typical user's resources and then the user cannot perform their necessary tasks because the node becomes continuously busy and have to utilize his resources to verify the messages [1].

Channel Jamming: in this type of DoS attacks, malicious user tries to jamming the channel. If this attack succeeds, it does not allow other users to access the network without its permission.

Distributed Denial of Services (DDoS): Because of the distributive nature of VANET, it seems establishing a DDoS in a VANET environment is simple and very deleterious. If there is a successful attack in a zone of VANET, the attacks propagate several false information in this zone and this cause chained problems appear all over the road.

V. Threats to Authentication

Providing authenticity in VANET involves protecting legitimate users from attackers permeating into the network by using a false identity, identifying attacks that suppress, fabricate, alter or replay legitimate messages, revealing spoofed GPS signals, and impede the introduction of misinformation into the vehicular network [1]. This group of attacks in VANET includes:

Masquerading: The attacker pretends to be another vehicle by using false such as message fabrication, alteration, and replay. For example, an attacker acts as an emergency vehicle to mislead other vehicles to slow down and yield [7].

Replay Attack: This attack happens when an attacker replay the transmission of earlier information to take advantage of the situation of the message at time of sending [8].

Global Positioning System (GPS) Spoofing: In this attack, malicious user tries to deceive legitimate users that they think they are in a different location. This is possible by giving false GPS information to users. This is possible through the use of a GPS satellite simulator to generate signals that are stronger than those generated by the genuine satellite [2].

Tunneling: The attacker connects two distant parts of the Ad-hoc network using an extra communication channel and those nodes suppose that they are neighbors and send data using the tunnel. This attack gives the attacker ability of controlling his attacks outside the victim environment.

Sybil Attack: In this attack type, a node sends multiple messages to other nodes and each message contains a different fabricated source identity in such a way that the originator is not known [1, 2]. The basic goals of the attacker are to provide an illusion to other nodes by sending wrong messages and to enforce other nodes on the road to leave the road for the benefits of the attacker [9].

Message Tampering: This type of attack is against message integrity. Generally in VANET, everyone within the same zone can listen to all the messages which other users is sending. Thus, malicious users can modify the contents of the message before receive it by real destination.

ID Disclosure: Disclose the identity information of users who are existence in the network. With this method of attack, attacker can track the current location of the real his target user.

Sensor tampering: Another easy attack is to deceive the vehicle’s sensors with wrong information such as tampering with the GPS system or temperature sensors [10].

VI. Threats to Confidentiality

Confidentiality of messages exchanged between the users of a typical VANET is vulnerable with malicious techniques such as eavesdropping and also collecting location information available through the broadcast messages. In the case of eavesdropping, attacker can collect information about exist users without their permission and use the information at a time.

VII. Conclusion

The VANET is one of the most exciting technologies and it has ability to make human driving life easier. Adhoc has several security related problem because of it has not infrastructure and centralized control in addition of unstable environment. One of the most important issues in adhoc is security. The VANET is an adhoc-based technology and all the adhoc problems have migrated into VANET. Usage of adhoc usually is in small environment such as universities and it seems the security problem of it can tolerable but in the future VANET will become a network with millions users in the world and if a usable solution doesn’t propose, the security problem which inherit from adhoc, become serious challenge against VANET growth.

In this paper, I try to review all the aspects of VANET security. As shown in this paper, there are other serious threats in VANET in addition of threats which existed in adhoc. For example sensor tampering or GPS spoofing which are not very serious in adhoc. In this paper I try to summarize these threats and showed the lack of centralized control mechanism causes serious problems in VANET. However, it appears centralized control mechanism is not possible in VANET. But it is important to produce a stable distributed control for VANET.

In the near future, VANET become a worldwide base information gathering technology and millions of cars in the all roads of the world become user of it. The experience of security problems of the Internet shows the world that security is everything. But VANET will be a network similar to the Internet but VANET involve with life of people on the roads. It is necessary to solve the security-related issues before VANET become a huge network.

References

[1] F. Sabahi, "Vehicular Ad-hoc Networks Security Analysis," Presented at International Conf. on Computer Engineering and Applications (ICCEA), 2011.

[2] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin, and A. Hassan, *Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges*. 2010.

[3] M. G. Zapata, "Secure Ad hoc On-Demand Distance Vector (SAODV)," *J Routing. Mobile Computing and Communications Review*; vol. 6, pp. 106.

[4] S. Mahajan and A. Jindal, "Security and privacy in VANET to reduce authentication overhead for rapid roaming networks," *International Journal of Computer Applications 2010;* vol. 1.

[5] J. Nzouonta, N. Rajgure, G. Wang, and C. Borcea, *VANET Routing on City Roads using Real-Time Vehicular Traffic Information*. 2008.

[6] H. Hasbullah, I. A. Soomro, J. L. A. Manan, "Denial of service (DoS) attack and its possible solutions in VANET," *J World Academy of Science Engineering and Technology* 2010.

[7] AKK. Aboobaker, "Performance analysis of authentication protocols in vehicular ad hoc networks (VANET)," 2010.

[8] B. Parno and A. Perrig, "Challenges in securing vehicular networks," *The Fourth ACM Workshop on Hot Topics in Networks (HotNets-IV)* 2005.

[9] G. Guett and C. Bryce, "Using TPMs to secure vehicular AD-HOC networks (VANETs)," *Workshop in Information Security Theory and Practices (WISTP)* 2008.

[10] ASK. Pathan, *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*. CRC Press; 2010.

Farzad Sabahi received Bachelor of Science and Master of Science degrees in Computer Engineering from Azad University in 2003 and 2007 respectively, specializing in the computer architecture. His research interests include computer architecture, distributed systems, cloud computing, hypervisor-based security and wireless network security. He is a lecturer in the Department of Electrical and Computer Engineering at the Azad University, Zanjan, Iran. He has published several papers in distributed systems, cloud computing, and wireless network security. He has been an invited reviewer for different international conferences. He has been member of The Institute of Electrical and Electronics Engineers (IEEE) since 2006.