IJITKM 0973-4414 Volume-9, Number-2 Jan-Jun 2016 pp. 61-64 **Impact Factor 2.8** available online at www.csjournalss.com

Comprehensive Study on security issues and characteristics in Vehicular Adhoc Networks

Divya Shree

Abstract: VANET provides vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. VANETs are the promising approach to provide safety and other applications to the drivers as well as passengers. It becomes a key component of the intelligent transport system. A lot of works have been done towards it but security in VANET got less attention. Due to various kinds of applications including safety driving, parking lot finder, real-time route finder, it is becoming popular in recent years. Safety applications based on vehicular network communication are a major aspect of future innovation. These applications are foreseen to improve traffic safety considerably, and to enable innovative infotainment applications and business models. Security is concerned with protection against malicious manipulation of IT systems and plays an important role when designing and implementing such applications. Safety applications must be protected to avoid malicious manipulation, potentially causing harm to the vehicle driver, and commercial applications must be protected to prevent loss of revenue. In this paper we present Security issues of providing data security in VANET followed by attacker and cryptographic protocols.The research of VANET and development of proposed systems and implementation would increase safety among road users and improve the comfort for the corresponding passengers, drivers and also other road users, and a great improvement in the traffic efficiency would be achieved.
Keywords: VANET, Adhoc Network, Security issues.

Introduction

VANETs are a subset of MANETs (Mobile Ad-hoc Networks) in which communication nodes are mainly vehicles. In the year 1998, the team of engineers from Delphi Delco Electronics System and IBM Corporation proposed a network vehicle concept aimed at providing a wide range of applications. With the advancements in wireless communications technology, the concept of network car has attracted the attention all over the world. In recent years, many new projects have been launched, targeting on realizing the dream of networking car and successful implementation of vehicular networks. The project Network On Wheels (NOW) is a German research project founded by DaimlerChrysler AG, BMW AG, Volkswagen AG, Fraunhofer Institute for Open Communication Systems, NEC Deutschland GmbH and Siemens AG in 2004, The project adopts an IEEE 802.11 standard for wireless access, The main objectives of this project are to solve technical issues related to communication protocols and data security for car-to-car communications. As such, this kind of network should deal with a great number of highly mobile nodes, eventually dispersed in different roads. In VANETs, vehicles can communicate each other (V2V, Vehicle-to-Vehicle communications)[12]. Moreover, they can connect to an infrastructure (V2I, Vehicle-to-Infrastructure) to get some service. This infrastructure is assumed to be located along the roads.VANET will in most situations not have permanent connections to a fixed infrastructure such as Internet.Therefore,critical issues such as privacy and control of the network need to be handled in a different way from PC-based networks.Further,it might be costly to establish the necessary Internet-like organizational aspects in VANET since these traditional approaches cannot simply be reproduced.

State of the Art

VANET are emerging research area, both in academics and in industry. There are many ongoing projects, while the early projects mainly considered the feasibility of VANET, now the security aspects are also added. The vehicle safety communications consortiums worked on security solutions that strongly influenced the IEEE P1609.First a pure wireless ad hoc network where vehicle to vehicle without any support of infrastructure. Second is communication between the road side units (RSU), a fixed infrastructure, and vehicle. Each node in VANET is equipped with two types of unit i.e. On Board Unit and Application Unit (AU). OBU has the communicational capability whereas AU executes the program making OBU‘s communicational capabilities. An RSU can be attached to the infrastructure network which is connected to the InternetCurrently the main industrial projects in USA are performed by the vehicle infrastructure integration initiative as well as by the Vehicle safety communications2 consortium in the vehicle safety communications application project. The standard defines the over-the-air message format for VANET and currently suggests attaching an ECDSA(elliptic curve digital signature algorithm)digital signature to each message. Furthermore, either a certificate or a certificate digest needs to be attached to each message .The standard also defines message content encryption as well as the format of certificate revocation lists.

DOI: 10.141079/IJITKM.2016.917

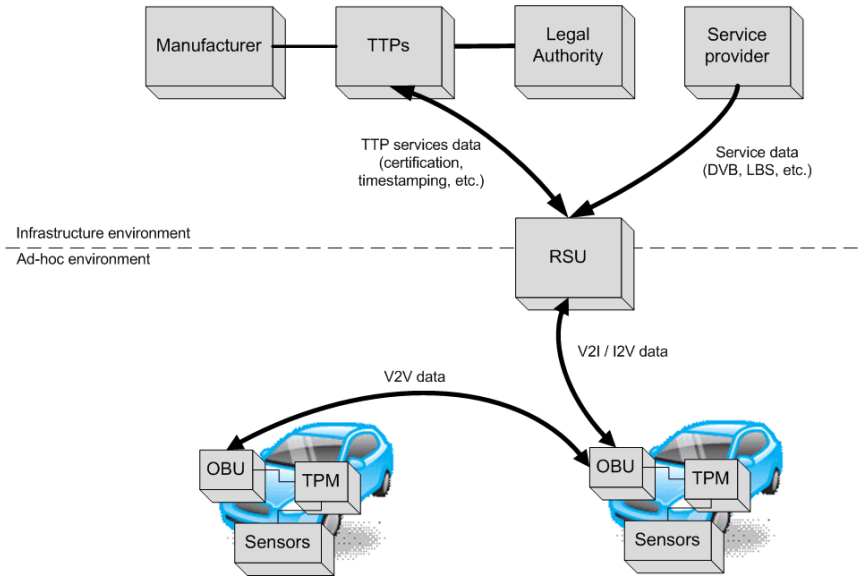

Figure 1: Simplified VANET model

VANET Characteristics

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

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

Data Security Issues in VANET

Data security in the personal computer is well researched, although large scale devastating attacks still occur. Security in vehicular networks poses different security threats and also has different requirements.

A. Privacy: Today, almost all movement patterns of an individual can be traced by tracking their vehicle. Further privacy concerns might be involved in financial transactions carried out on VANET. Privacy is both a technical and an organizational matter.

B. Reliability: Unauthorized software updates can lead to serious safety and liability issues, and to financial loss.

C. Market penetration: Vehicles are expected to be equipped with VANET radios over the next decade. However it is expected to take a considerable time until all vehicles are VANET enabled. It is also unclear to what degree or when there will be supporting infrastructure available in the form of roadside units (RSUs). Therefore, potential security solutions should work with a low penetration rate of radio-enabled vehicles and small number of deployed RSUs.

D. Financial assets: There are a variety of promising applications based on vehicular communication that involve financial aspects, such as digital infotainment content, location based services, and built-in-automotive payment functions (e.g road tolling). Tampering with non-safety applications imposes far less risk of being prose cured than does tampering with safety applications, whereas in the second case, police authorities might heavily pursue any illegal modifications, in the first case, industry needs to defend itself.

E. Cost: In the automotive domain there is little willingness by vehicle buyers to spend money for security. Therefore, security solutions need to be especially cost efficient.

F. Usability: Vehicle driver expects not to deal with electronic issues, and certainly not with a security configuration. If adjustments by external entities are necessary, then they should only be implemented during a workshop visit or by automatic updates via VANET communication channels.

G. Risk Potential: Due to close coupling with the physical environment, the risk involved in vehicular networks can be much larger than the risk in conventional IT applications. The hacking of an automotive safety-critical application system can have far more immediate physical consequences than hard disk data destroyed by a computer virus.

H. Mobility: Contact with other vehicles might be limited to only a few seconds such that establishing a secure channel cannot take too long. Furthermore, the communication quality might be affected by the velocity of vehicles, resulting in packet loss.

I. Legislation: Legislation might requires both technical solutions and organizational mechanisms for the vehicles and for the supporting infrastructure

VANET ATTACKS

In this paper we are concentrating on attacks perpetratedagainst the message itself rather than the vehicle, asphysical security is not in the scope of this paper.

1) Denial of Service attack

This attack happens when the attacker takes control of avehicle's resources or jams the communication channelused by the Vehicular Network, so it prevents criticalinformation from arriving. It also increases the danger to the driver, if it has t depend on the application'sinformation.

2) Alteration Attack

This attack happens when attacker alters an existingdata, it includes delaying the transmission of theinformation, replaying earlier transmission, or alteringthe actual entry of the data transmitted.For instance, an attacker can alter a message tellingother vehicles that the current road is clear while the road is congested.

3) Replay Attack

This attack happens when an attacker replay thetransmission of an earlier information to take advantageof the situation of the message at time of sending.

4) Message Suppression Attack

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

The goal of such an attacker would be to preventregistration and insurance authorities from learningabout collisions involving his vehicle and/or to avoiddelivering collision reports to roadside access points.

For instance, an attacker may suppress a congestionwarning, and use it in another time, so vehicles will notreceive the warning and forced to wait in the traffic.

5) Fabrication Attack

An attacker can make this attack by transmitting falseinformation into the network, the information could befalse or the transmitter could claim that it is somebodyelse.This attack includes fabricate messages, warnings,certificates, identities.

Conclusion

The author has provided an overview of challenges for VANET security, and described various security issues of data security and the characteristics models which describe various requirements for safety and non-safety applications. Vehicular Ad Hoc Networks is promising technology,which gives abundant chances for attackers, who will tryto challenge the network with their malicious attacks.

It is expected that there will be only a few VANET worldwide, but each will be country or even continent-wide and will compromise several hundred million nodes. We believe it is infeasible to design, implement, and deploy a security and application system in vehicles that will run for the entire vehicle lifetime without adaptation. Therefore secure updating of application and security software should be included from initial deployment.

Acknowledgement

The Authors are supported by many books and references and journals as mentioned below. Besides this, we are thankful to some faculties' members from different organization.

References

[1]. Obasuyi, G. and Sari, A. (2015) Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment. International Journal of Communications, Network and System Sciences, 8, 260-273.
[2]. Gerlach, M. (2006) Full Paper: Assessing and Improving Privacy in VANETs.
[3]. Dahiya, A. and Chauhan, R. (2010) A Comparative Study of MANET and VANET Environment. Journal of Computing, 2.
[4]. Sesay, S., Yang, Z. and He, J.H. (2004) A Survey on Mobile Ad Hoc Network. Information Technology Journal, 3, 168-175.
[5]. M. Passino, "Biomimicry of bacterial foraging for distributed optimization and control," IEEE Control Syst Mag. USA, vol. 22, pp. 52- 67, June 2002.
[6]. V. Naumov, R. Baumann, and T. Gross, "An evaluation of inter-vehicle ad hoc networks based on realistic vehicular traces," Proc. ACM the 7th ACM MobiHoc' 06, Florence, Italy, May 22-25, 2006.
[7]. N. Wisitpongphan, F. Bai, P. Mudalige, and O. K. Tonguz, "On the routing problem in disconnected vehicular ad hoc networks," IEEE the 26th INFOCOM'07, Anchorage, Alaska, USA, May 6-12, 2007.
[8]. International journal of Network and Mobile Technologies, Vol. 2 number 1, January-June 2011, ISSN: 2230-8903.
[9]. M. Nekovee, and B. BjarniBogason, "Reliable and efficient information dissemination in intermittently connected vehicular ad hoc networks," IEEE the 65th VTC'07-Spring, Dublin, Ireland, April 22-25, 2007.
[10]. Rahnama, B., Sari, A. and Makvandi, R. (2013) Countering PCIe Gen. 3 Data Transfer Rate Imperfection Using Serial Data Interconnect. 2013 International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), Konya, 9-11 May 2013, 579-582.
[11]. Toor, Y., Muhlethaler, P. and Laouiti, A. (2008) Vehicle Ad Hoc Networks: Applications and Related Technical Issues. IEEE Communications Surveys & Tutorials, 10, 74-88.
[12]. Divyashree (2013) performance evaluation of realistic mobility models using road side units, IJCA October 18,2013.