BIOINFO Security Informatics
ISSN: 2249-9423 & E-ISSN: 2249-9431, Volume 2, Issue 1, 2012, pp.-28-32.
Available online at http://www.bioinfo.in/contents.php?id=344

VANET SECURITIES AGAINST ATTACKS

CHAVHAN K.L. AND PATIL P.A.

Department of Computer Science and Engineering, Jawaharlal Darda Institute of Engineering and Technology, Yavatmal, MS, India.
*Corresponding Author: Email- kiranlalitccc@gmail.com, meetpallu27@gmail.com

Received: February 21, 2012; Accepted: March 15, 2012

Abstract- A Vehicular Ad-Hoc Network or VANET is a form of Mobile Ad-Hoc Network or MANET which provides communication between vehicles and between vehicles and road-side base stations. A vehicle in VANET is considered to be an intelligent mobile node capable of communicating with its neighbors and other vehicles in the network. VANET is different from MANET due to high mobility of nodes and the large scale of networks. Security and privacy are the two main concerns in designing a VANET. Although there are many proposed solutions for improving securities in VANET but security still remains a delicate research subject. The main objectives of this paper is to improve the security in VANET.The preliminary efforts were focused on the potential applications, possible attacks, security requirement.The long term goal of this paper is to come up with an entirely new solution that can be implemented in designing a VANET .

Citation: Chavhan K.L. and Patil P.A. (2012) VANET Securities Against Attacks, BIOINFO Security Informatics, ISSN: 2249-9423 & E-ISSN: 2249-9431, Volume 2, Issue 1, pp.-23-27.

Introduction

Vehicular ad hoc networks (VANETs) are a subgroup of mobile ad hoc networks (MANETs) with the distinguishing property that the nodes are vehicles like cars, trucks, buses and motorcycles. This implies that node movement is restricted by factors like road course, encompassing traffic and traffic regulations. Because of the restricted node movement it is a feasible assumption that the VANET will be supported by some fixed infrastructure that assists with some services and can provide access to stationary networks. The fixed infrastructure will be deployed at critical locations like slip roads, service stations, dangerous intersections or places well-known for hazardous weather conditions.

The primary VANET's goal is to increase road safety. To achieve this, the vehicles act as sensors and exchange warnings or more generally, telematics information (like current speed, location or ESP activity) that enables the drivers to react early to abnormal and potentially dangerous situations like accidents, traffic jams or glaze. The information provided by other vehicles and stationary infrastructure might also be used for driver assistant systems like adaptive cruise control (ACC) or breaking assistants. In addition, authorized entities like police or firefighters should be able to send alarm signals and instructions e.g. to clear their way or stop other road users. Besides that, the VANET should increase comfort by means of value-added services like location based services or Internet on the road.

This paper focuses on providing the overview of VANET security and dealing effectively with the problems. Firstly, the overview of the network and security requirement will be discussed; it will be followed by the problems associated in VANET security and we will provide effective solutions to those problems that are already available and the basic solution which we have proposed incorporating other solutions and later ending the paper by covering future research directions and conclusion.

VANET Model Overview

There are many entities involved in a VANET settlement and deployment. Although the vast majority of VANET nodes are vehicles, there are other entities that perform basic operations in these networks. Moreover, they can communicate with each other in many different ways. In this Section we will firstly describe the most common entities that appear in VANETs.

Common VANET entities

Several different entities are usually assumed to exist in VANETs. To understand the internals and related security issues of these networks, it is necessary to analyze such entities and their relationships.

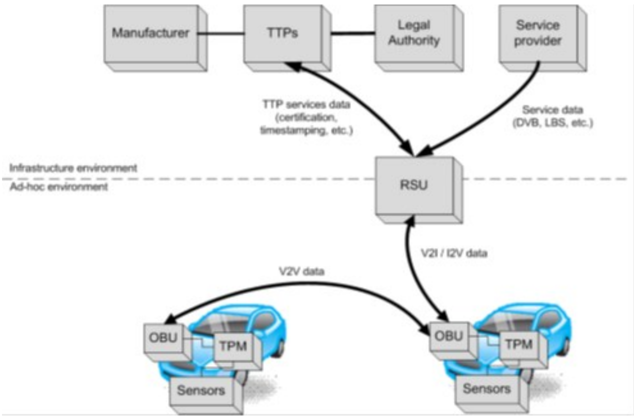

Fig. 1- Simplified VANET model

Infrastructure environment

In this part of the network, entities can be permanently interconnected. It is mainly composed by those entities that manage the traffic or offer an external service. On one hand, manufacturers are sometimes considered within the VANET model. As part of the manufacturing process, they identify uniquely each vehicle. On the other hand, the legal authority is commonly present in VANET models. Despite the different regulations on each country, it is habitually related to two main tasks - *vehicle registration* and *offence reporting*. Every vehicle in an administrative region should get registered once manufactured. As a result of this process, the authority issues a license plate. On the other hand, it also processes traffic reports and fines. Trusted Third Parties (TTP) are also present in this environment. They offer different services like credential management or timestamping. Both manufacturers and the authority are related to TTPs because they eventually need their services (for example, for issuing electronic credentials). Service providers are also considered in VANETs. They offer services that can be accessed through the VANET. Location-Based Services (LBS) or Digital Video Broadcasting (DVB) are two examples of such services.

Ad-hoc environment: In this part of the network, sporadic (ad-hoc) communications are established from vehicles. From the VANET point of view, they are equipped with three different devices. Firstly, they are equipped with a communication unit (OBU, On-Board Unit) that enables Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I, I2V) communications. On the other hand, they have a set of sensors to measure their own status (e.g. fuel consumption) and its environment (e.g. slippery road, safety distance). These sensorial data can be shared with other vehicles to increase their awareness and improve road safety. Finally, a Trusted Platform Module (TPM) is often mounted on vehicles. These devices are especially interesting for security purposes, as they offer reliable storage and computation. They usually have a reliable internal clock and are supposed to be tamper-resistant or at least tamper-evident (Papadimitratos, Buttyan, Hubaux, Kargl, Kung, & Raya, 2007). In this way, sensitive information can be reliably stored.

Application of VANET

A good system design depends on understanding the applications that will be carried in the network. These applications not only call for diverse solutions, such as bandwidth, delay, security, and reliability, but also demonstrate different communication patterns, such as one-to-one, one-to-many, many-to-one, and many-to-many. However, most existing wireless network architectures could not efficiently support such demands. Therefore, it becomes a major challenge to support and enable diverse applications and services. Here we summarize the existing applications and several potential applications that have been proposed for VANET. It is important to note that we also elaborate on the functions of each application that shall be provided in the MAC layer and the network layer, so as to fulfill the requirements of these applications. VANET would support life-critical safety applications, safety warning applications, electronic toll collections, Internet access, group communications, roadside service finder, etc.

Life-Critical Safety Applications- e.g., Intersection Collision Warning/Avoidance, Cooperative Collision

Warning, etc. In the MAC Layer, the Life-Critical Safety Applications can access the DSRC control channel and other channels with the highest priority. The messages can be broadcasted to all the nearby VANET nodes.

Safety Warning Applications- e.g., Work Zone Warning, Transit Vehicle Signal Priority, etc. The differences between Life-Critical Safety Applications and Safety Warning Applications are the allowable latency requirements, while the Life-Critical Safety Applications usually require the messages to be delivered to the nearby nodes within 100 milliseconds, the Safety Warning Applications can afford up to 1000 milliseconds. In the MAC Layer, the Safety Warning Applications can access the DSRC control channel and the other channels with the 2nd highest priority. The messages can be broadcasted to all the nearby VANET nodes.

Possible Attacks in VANET

Due to the nature of open wireless medium used in VANET, there are a number of possible attacks by which the VANET is exposed to. Hence, the chances for possible attacks are so high. The purpose of the attackers is to create problem for legitimate users, and as a result services are not accessible, thus denial of service. Some of the DOS attacks are mentioned below.

Sybil Attack

Douceur[3] is the first author who described 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. 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.

Denial of Service (DOS) Attack

In wireless environment, typically the attacker attacks the communication medium to cause the channel jam or to create some problems for the nodes from accessing the network. The basic purpose is to prevent the authentic nodes from accessing the network services and from using the network resources. The attack may result in devastation and overtiredness of the nodes' and network's resources. Ultimately, the networks are no longer available to legitimate users. In VANET, DOS shall not be allowed to happen, where seamless life critical information must reach its intended destination securely and timely.

Malicious Attack

This kind of attackers deliberately attempt to cause harm via the applications on the vehicular network. Normally, these attackers have specific targets, and they have access to more resources than other attackers. They are more professional. For example, a terrorist might manipulate the deceleration warning system to create gridlock before detonating a bomb. In general, although such kind of attackers will be less than other kinds of attackers, they are probably the most important concern for our security system.

Security requirement in VANET

A. Authentication and location detection

The first issue that we need to address is making sure that the message is really sent from the party that pretends to send it. Therefore, there is a need of using authentication of all vehicles on the road. In the paper the authors introduced the concept of authenticated localization of message origin. This approach is intended to prevent any person sitting on the edge of theroad from pretending that his message originated from a vehicle travelling on the road. Therefore, this will prevent spoofing, in which, pranksters fake their identity to pretend that they are vehicles on the road in order to disturb the order of the traffic. To do this, each vehicle should be kept track of by some authority or infrastructure in some cases, by using authentication. To achieve this public key cryptography authentication is used. In this fashion, each vehicle will broadcast its identity (public key) along with the signature of a current timestamp. This is very important to make sure that the authentication is recent and at the same time have different signatures from the vehicle to ensure its identity. So when each vehicle receives such a broadcast, it signs the other vehicle's ID and rebroadcasts it. Doing this will help vehicles to predict the location of the specific vehicle on the road. For example, if a vehicle A receives a public key of B Kb, it adds its signature {Kb}ka with its private key Ka to its regular broadcast. Therefore, if vehicle B hears C rebroadcast A's identity, before rebroadcasting B's identity, then it knows that A is ahead of him. Further, a vehicle B can get more assurance that vehicle A is ahead of it by getting rebroadcasts of A's identity by vehicles D and E.

B. Preserving Privacy and Anonymization

In VANETs the issue of privacy and preserving the personal information of a driver and vehicle, is raising concerns for both car manufacturers and future potential users. Therefore, there shouldn't be any disclosure on any private information of the driver or vehicles. So a vehicle should not trace the exact identity of other vehicles of the road, but only to verify the connection between the information sent and the vehicle present in the road. In other words, make sure the vehicle it pretends to send the message, is indeed the one who really did. To achieve this, there is a need to include an intermediary service that will map the permanent identity of the driver or/and vehicle and a temporary ID. The authors called this service, anonymization service. This service as mentioned maps between the permanent identity of driver or vehicle and a random ID it provides to that vehicle to keep track of it; it's extremely important that this temporary ID should not be traceable to the driver or vehicle. Therefore, there should be a strong algorithm at the level of the anonymization service to achieve that. Although this technique will create an additional overhead, it will provide the driver with the required privacy and prevent spoofing.

Anonymizers should be placed on a toll booth then there will be reanonymizers on the side of the road on a regular distance difference between them. So when the vehicles approach a reanonymizer, this latter would broadcast a random nonce N, then the vehicle will sign N, and broadcast the new certificate encrypted with the old public key. Then, the reanonymizer will verify the signature and broadcast the new certificate encrypted with the old public key, after that, it will verify the signature and broadcast the new certificate encrypted with the old public key. The certificate contains the new identity of the vehicle and a timestamp as well as the reanonymizer signature. Consequently, every time a vehicle will approach a reanonymizer, it will acquire a new identity, for added security.

C. Secure Aggregation technique:

Using this technique, each vehicle on the road will keep count of the vehicles it passes and authenticate them. Authentication will take place using an infrastructure aid that will deliver as explained above some unique valid IDs that can be understood by all vehicles on the road, and as mentioned above will preserve the privacy.Through this information collected each vehicle will have an estimation of the number of vehicles ahead.

D. Active Position Detection

Position security in VANET is very important to the process of verifying the source of any communication or message through the network. To achieve that, we need to use onboard radars to detect neighboring vehicles and to confirm their coordinates. Based on that data, a history of the vehicles movement is created. Consequently, a check on the history and computing similarity, we can prevent a large number of Sybil attacks and position based attacks.

E. Privacy

This system is used to ensure that the information is not leaked to the unauthorized people who are not allowed to view the information. Third parties should also not be able to track vehicle movements as it is a violation of personal privacy. Therefore, a certain degree of anonymity should be available for messages and transactions of vehicles. However, in liability related cases, specified authorities should be able to trace user identities to determine responsibilities. Location privacy is also important so that no one should be able to learn the past or future locations of vehicles.

Problems

The problems are as follows:

A. Mobility

The basic idea from Ad Hoc Networks is that each node in the network is mobile, and can move from one place to another within the coverage area, but still the mobility is limited, in Vehicular Ad Hoc Networks nodes moving in high mobility, vehicles make connection throw their way with another vehicles that maybe never faced before, and this connection lasts for only few seconds as each vehicle goes in its direction, and these two vehicles may never meet again. So securing mobility challenge is hard problem.

B. Volatility

The connectivity among nodes can be highly ephemeral, and maybe will not happen again, Vehicles traveling throw coverage area and making connection with other vehicles, these connections will be lost as each car has a high mobility, and maybe will travel in opposite direction. Vehicular networks lacks the relatively long life context, so personal contact of users device to a hot spot will require long life password, and this will be impractical for securing VC.

C. Network Scalability

The scale of this network in the world approximately exceeding the 750 million nodes , and this number is growing, another problem arise when we must know that there is no a global authority govern the standards for this network for example: the standards for DSRC in North America is deferent from the DSRC standards in Europe, the standards for the GM Vehicles is deferent from the BMW one

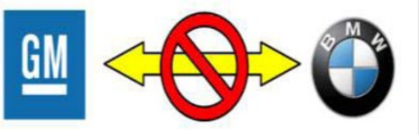

Fig. 2- GM VS BMW Standards

D. Bootstrap

At this moment only few number of cars will be have the equipment required for the DSRC radios, so if we make a communication we have to assume that there is a limited number of cars that will receive the communication, in the future we must concentrate on getting the number higher, to get a financial benefit that will courage the commercial firms to invest in this technology.

VANET Properties supporting Security:

VANET systems have certain properties which make them a unique from other ad hoc network.

A. High processing power and adequate power supply

VANET nodes are the vehicles itself which have their own power in the form of batteries and can have high computing powers. This means that unlike a majority of the ad hoc networks, they do not need power efficient protocols. And high computing power allows the nodes to run complex cryptographic calculations.

B. Central Registration

Usually ad hoc networks are not registered but the good thing is that all the VANET nodes ie., the vehicles are registered with a central authority and already have a unique identity in the form of a license plate. There is an existing infrastructure which maintains records of all vehicles.

C. Existing Law Enforcement Infrastructure

If there is any sort of attacks done by the adversary the law enforcement group can catch the wrong doers although the law enforcement officers.

Security architecture

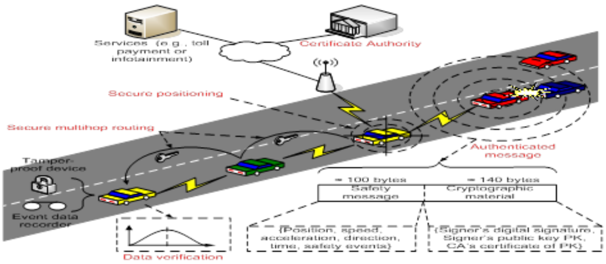

Fig. 3- Security Architecture

The basic idea is that if a user wants to participate in a VANET (the user's vehicle is not required to have a manufacturer's issued certificate), he purchases a payment-processing-device (similar to automatic toll payment devices - sold for tens of dollars). Each device will have an identification and an associated certificate. During initialization the device will be linked/registered with the user's account; user's information will be maintained with the provider and will not be stored in the device.When a user enters a service area and wants to use the service, he makes the payment for the service using onboard payment device. The payment-authorization/service request message will be encrypted using provider's public key, thus hiding the device ID/certificate and services requested from eavesdroppers. The user is issued a pseudonym and other IDs necessary for the service by the provider. The concerned server is also informed of the service purchased and temporary credentials. The temporary credentials can also be used to provide desired security attributes for VANET applications including vehicle to vehicle -V2V communications. As a baseline service, the user can obtain just the temporary credentials, in this case the temporary credentials will not be sent to servers. Certificate, IP address, MAC address etc can all be issued on temporary basis and refreshed several times during a service period. They are encrypted to ensure security and privacy. Initially, they can be encrypted using a random session key sent along the request. Later, they can be encrypted using current public key. The certificate of CA is hard coded in the device, enables other users to check validity of a certificate. Methods can be employed to safeguard against replay, spoofing, man-in-the-middle etc.

Future research direction

A. Cost effectiveness of the system

It should be said that implementing our proposed system will lead to many solutions of the security problems that are encountered in VANET. Even the system is costly. So an imperative solution of this system and an effective cost management analysis of this system can be a great future research issue.

B. Time delay management

VANET is an excellent discovery in terms of safety related information. If the information send later, i.e. after a good amount of time then it will be useless to have such a system. So reducing time delay should be a prime research topic.

C. Using the available technologies such as Wi-Fi, CDMA, GSM

VANET communication uses new protocols. We should think about mixing the communication process with all the existing protocols that are present, such as Wi-fi, CDMA and GSM.

Conclusion

In this paper we proposed a system that can be used for authentication of messages,. Firstly we discussed the overview of the network, applications and system requirements and followed by the problems of the network and properties mitigating these problems. Later we did a survey on many papers and generated an idea that will be helpful to reduce the security issues in VANET.

References

[1] Fay Hui (2005) *A survey on the characterization of Vehicular Ad Hoc Networks routing solutions,* ECS 257.

[2] Zheng Chai. *A Survey of Security in Vehicular Networks*.

[3] Zheng. *Challenges in vehicular networks*.

[4] Wenmao Liu, Hongli Zhang and Weizhe Zhang. *An autonomous road side infrastructure based system in secure VANETs*.

[5] Une Thoing Rosi and Chowdhury Sayeed Hyder. *A Novel Approach for Infrastructure Deployment for VANET*.

[6] Raya M., Jungels D., Papadimitratos P., Aad I., Hubaux J.P. *Certificate Revocation in Vehicular Networks*.

[7] Laboratory for Computer Communications and Applications (LCA)*School of Computer and Communication Sciences*, EPFL, Switzerland, 2006.

[8] Haas J.J., Hu Y.C. and Laberteaux K.P. *Design and analysis of a lightweight certificate revocation mechanism for VANET*.

[9] Lin X., Lu R., Zhang C., Zhu H., Ho P. and Shen X. (2008) *IEEE Communications Magazine*.

[10]Douceur J. (2003) *First International Workshop on Peer-to-Peer Systems*, 1st ed, USA.