SECURITY ISSUES IN VANET

Rizwanul Karim Sakib
Student ID: 06210003
Bisway Reza
Student ID-06210013

Department of Electronics and Communication Engineering
April 16, 2010

BRAC University, Dhaka, Bangladesh

DECLARATION

We hereby declare that this thesis report is based on the results of the papers that we have studied so far .This type of report has not been submitted before and is entirely a new one .

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 issues in VANET.The preliminary efforts were focused on the potential applications, possible attacks, security requirements and the literature review. The long term goal of this project is to come up with an entirely new solution that can be implemented in designing a VANET..

ACKNOWLEDGEMENT

We would like to thank our thesis supervisor Dr, AL SAKIB KHAN PATHAN for his guidance, patience and support, for making us familiar with this very new topic called “VANET” and for providing us with lots of important resources that has helped us understand what VANET is all about. Thanks to our co-supervisor Mr. Nazmus Sakib for providing papers regarding MANET.

TABLE OF CONTENTS

PAGE

Chapter-1
Introduction

With an immense improvement in technological innovations, we find Vehicular Communication (VC) as a solution to many problems of our modern day communication system in roads. VC involves the use of short range radios in each vehicle, which would allow various vehicles to communicate with each other which is also known as (V-V) communication and with road side infrastructure(V-I) communication. These vehicles would then form an instantiation of ad hoc networks in vehicles, popularly known as **Vehicular Ad Hoc Networks (VANET)**. It is a subset of Mobile Ad Hoc Networks (MANET) [1]. The similarity between these two networks is characterized by the movement and self organization of nodes. Also the difference between these ad hoc networks is that MANET nodes cannot recharge their battery power where as VANET nodes are able to recharge them frequently. [2]

VANET is mainly designed to provide safety related information, traffic management, and infotainment services. Safety and traffic management require real time information and this conveyed information can affect life or death decisions. Simple and effective security mechanism is the major problem of deploying VANET in public. Without security, a Vehicular Ad Hoc Network (VANET) system is wide open to a number of attacks such as propagation of false warning messages as well as suppression of actual warning messages, thereby causing accidents. This makes security a factor of major concern in building such networks. VANET are of prime importance, as they are likely to be amongst the first commercial application of ad hoc network technology. Vehicles are the majority of all the nodes, which are capable of forming self organizing networks with no prior knowledge of each other, whose security level is very low and they are the most vulnerable part of the network which can be attacked easily. The capacity of VANET technology is high with a wide range of

applications being deployed in aid of consumers, commercial establishments such as toll plazas, entertainment companies as well as law enforcement authorities. However, without securing these networks, damage to life and property can be done at a greater extent. [1]

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.

CHAPTER-2

Network Overview, Applications and Security Requirements for VANET

Overview of VANET

It is stated earlier that in VANET, the connectivity is done among vehicle to vehicle and vehicle to road side infrastructure (RSU) and vehicle or road side infrastructures to the central authority responsible for the network maintenance. The basic tool for communication is the short range radios that are being installed in any of the nodes. Vehicular node has the shortest transmission range. RSU's are spread sporadically or regularly depending on the deployment of the network in any particular region. In real life RSU's are spread sporadically. They act as an intermediary node between the Central Authority (CA) and Vehicular Node (VN) [1].

In 1999, the FCC has allocated a frequency band of 5.850- 5.925 GHz in the US specifically for the purpose of vehicular networks. Similar bands exist in Japan and Europe. The emerging de facto standard for VC is the Dedicated Short Range Communications (DSRC). DSRC has a MAC Layer that is either a modified version of 802.11WLAN or the 3G protocol extended for decentralized access. Since the current 802.11 protocol is not suitable for VANET due to the high mobility and highly dynamic topology, a special version of it, called 802.11p is being developed by the IEEE. Also, the current 3G protocol is designed for centralized cellular networks, but in VANET centralized infrastructure is not always present. [3] The IEEE standards propose each 10 MHz channels capable of carrying 27Mbps data, which will lead to at least 1 channel for safety related information and the remaining 6 dedicated channels for data transmission. [1]

A number of organizations and industry consortiums are involved in developing standards for VANET. For example, the IEEE is involved in standards development related to the physical, medium access and security issues as well as in defining higher layer services and interfaces for intelligent transportation. By the end of 2006, the IEEE P1609 standards for wireless access in vehicular environments (WAVE) had specified the application layer and message formats for operation in the 5.9 GHz DSRC communications. The IEEE 802.11p standard which is a modification of the popular IEEE 802.11 (Wi-Fi) standard, looks at issues related to the highly dynamic environment and the extremely short time durations, during which communications must be completed due to the high speed of the communicating vehicles. Several consortiums with industry and/or public participation are also working on furthering the development and deployment of vehicular networks. Some examples include the Car-2-Car Consortium, which has as one of its primary objectives, the creation and establishment of an open and interoperable standard for V2V communications in Europe using Wi-Fi like components. Some communication protocols are being developed by the Network-on-Wheels (NOW) group, which is associated with the Car-2-Car Consortium. Ford and General Motors created a Crash Avoidance Metrics Partnership (CAMP) and with the National Highway Transportation Safety Administration, this partnership is working on projects such as enhanced digital maps for safety, driver workload metrics and forward crash warning requirements . Other VC projects being implemented include the Berkeley PATH and the Fleetnet projects in USA and Germany respectively. [1]

APPLICATIONS

Major applications of VANET include **providing safety information, traffic management, toll services, location based services and infotainment. One** of the major applications of VANET include providing safety related information to avoid collisions, reducing pile up of vehicles after an accident and offering warnings related to state of roads and intersections. Affixed with the safety related information are the liability related messages, which would determine which vehicles are present at the site of the accident and later help in fixing responsibility for the accident.

Collision Avoidance

V-V and V-I Communications can save many lives and prevent injuries. In this application, if a vehicle reduces its speed significantly after observing an accident or experiencing an accident, it will broadcast its location to its neighbor vehicles. And other receivers will try to relay the message further and the vehicle in question will emit some kind of alarm to its drivers and other drivers behind. In this way, more drivers far behind will get an alarm signal before they see the accident and can take any decision for his betterment.

Cooperative Driving

The drivers play the leading part in this application. Like violation warning, turn conflict warning, curve warning, lane merging warning etc. These services may greatly reduce the life-endangering accidents. In fact, many of the accidents come from the lack of cooperation between drivers. Given more information about the possible conflicts, we can prevent many accidents.

Traffic Optimization

In this application the vehicles could serve as data collectors and transmit the traffic condition information for the vehicular network. To be more specific, in this application, vehicles could detect if the number of neighboring vehicles is too

many and or the speed of vehicles is too slow, and then relay this information to vehicles approaching the location. To make it work better, the information can be relayed by vehicles traveling in the other direction so that it may be propagated faster to the vehicles toward the congestion location. In this way, the vehicles approaching the congestion location will have enough time to choose alternate routes.

Payment Services

This application is very suitable for toll collection without even decelerating the car or waiting in line.

Location-based Services

Finding the closest fuel station, restaurant, lodge etc can be done effectively using location based service. Although, GPS systems have such kinds of services already present in it but it can also be achieved using VANET.

SECURITY REQUIREMENTS FOR VANET

Authentication

Authentication is a major requirement in VANET as it ensures that the messages are sent by the actual nodes and hence attacks done by the greedy drivers or the other adversaries can be reduced to a greater extent. Authentication, however, raises privacy concerns, as a basic authentication scheme of attaching the identity of the sender with the message would allow tracking of vehicles. It, therefore, is absolutely essential to authenticate that a sending vehicle has a certain property which provides authentication as per the application. For example, in location based services this property could be that a vehicle is in a particular location from where it claims to be. [3]

Message Integrity

This is very much requires as this ensures the message is not changes in transit that the messages the driver receives are not false. [1]

Message Non-Repudiation

In this security based system a sender cannot deny the fact having sent the message. But that doesn't mean that everyone can identify the sender only specific authorities should be allowed to identify a vehicle from the authenticated messages it sends. [3]

Entity authentication

It ensures that the sender who has generated the message is still inside the network and that the driver can be assured that the sender has send the message within a very short period. [3]

Access control

It is required to ensure that all nodes function according to the roles and privileges authorized to them in the network. Towards access control, Authorization specifies what each node can do in the network and what messages can be generated by it. [1]

Message confidentiality

It is a system which is required when certain nodes wants to communicate in private. But anybody cannot do that. This can only be done by the law enforcement authority vehicles to communicate with each other to convey private information. An example would be, to find the location of a criminal or a terrorist. [1]

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. [3]

Real time guarantees

It is essential in a VANET, as many safety related applications depend on strict time guarantees. This can be built into protocols to ensure that the time sensitivity of safety related applications such as collision avoidance is met. [1]

CHAPTER- 3

Problems and Properties associated in VANET Security

The problems can be classified into tree distinct parts which are **challenges** that are faced while implementing the system, **adversaries** that can attack the system and the **type of attacks** that can be encountered in VANET. The latter two parts are explained together. Later the chapter will illustrate the existing **properties** that support **security issues**, i.e. which will mitigate some security situation.

CHALLENGES

Tradeoff between authentication and privacy

For authentication of all message transmission, it is required to track the vehicles for the identification of vehicles from the message they send which most consumers will not like others to know about their personal identification therefore this has to come in equilibrium. Therefore a system needs to be introduced which enables message to be anonymous to the general nodes but also enables identification by central authorities in cases like accidents. [1,4]

High Mobility

Due to high mobility the protocol cannot be handshake based and most of the communications are between nodes that have never interacted before therefore learning based scheme should be introduced so that they learn to know about each others behaviors.

Real-time guarantees

As the major VANET applications are used for collision avoidance, hazard warning and accident warning information, so applications require strict deadlines for message delivery.

Location Awareness

Certain location based service is essential for most VANET applications to be truly effective, so that reliance of the VANET system on GPS or other specific location based instruments can be increased as any error in these is likely to effect in the VANET applications.

ADVERSARIES and their attacks

Greedy Drivers

It can be thought that most of the drivers in the road is honest and will follow all the rules and regulations but there can be greedy drivers as well who will try to attack for their own benefit and we cannot deny the fact. For example, in our congestion avoidance system, a greedy driver might try to convince his neighbors that there is congestion ahead, and if his neighbors choose other routes, our greedy driver will get a terrific driving condition. Message Falsification is a type of attack usually done by the greedy drivers. An attacker can send false messages in a VANET network such as false hazard warnings to divert traffic from a route for freeing up resources for it. Message delay is also another type of attacks where in case of road traffic accident the driver will not pass the message to its neighboring cars in appropriate time so as to create road traffic congestion

Snoops/Eavesdropper

These people are those who try to collect information about you. While data mining is acceptable over aggregate data, but for identifying information for an individual, that raises serious privacy concerns and is not acceptable. Impersonation is a type of attack done by the snoops. An attacker may take on someone else's identity and gain certain advantages or cause damage to other vehicles. Privacy Violation is also done by the snoops and is done by using a simple mechanism which is to associate the identity of vehicles with the messages they send using asymmetric key cryptography. However, this lends itself to people being able to identify the sender of the message. Thus, vehicles can be tracked and anyone can identify a vehicle's owner. This raises some serious privacy issues as in all applications like safety, traffic management and toll access the messages would reveal the driver's identity, his location, his

actions and preferences. Consumers would not like to adopt a technology which violates their privacy.

Pranksters

Pranksters are especially the bored teenagers who will attempt things for fun. For example, a prankster targeting a collision-avoidance might sit by the road and convince one vehicle to slow down while convincing the vehicle behind to speed up. A prankster could also abuse the security vulnerability to Denial of Service (DoS) attacks to disable applications or prevent critical information from reaching another vehicle. Message Alteration is a form of attack that is done by the pranksters by changing a hazard warning to a no hazard warning to cause road traffic accidents.

Industrial Insiders

Industrial insiders are those who stays inside the car manufacturing company Attacks from insiders can be very harmful, and the extent to which vehicular networks are vulnerable will depend on other security design decisions. For example, if mechanics can update the firmware of a vehicle, they also have an opportunity to load malicious firmware. If we allow vehicle manufacturers to distribute keys, then a insider at one manufacturer could create keys that would be accepted by all other vehicles. Hardware Tampering is usually done by the industrial insiders. Attackers can tamper with the security hardware of a vehicle to steal identities as well as extract cryptographic keys. Therefore, specific mechanism like tamper proof hardware needs to be implemented to ensure such attacks cannot be easily accomplished. Sensors tampering are also another easy attack done by the insiders If the main system is tamper proof it is easy to fool the vehicle’s sensors with wrong information by simulating false conditions. Examples include tampering with the GPS system and temperature sensors.

Malicious Attackers

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.

VANET Properties supporting Security

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

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.

Known Time and Position

The location of a node with time would be available for the implementation of various security purposes as it is thought that most vehicles will be equipped with the GPS system.

Periodic Maintenance & Inspection

In most cases, cars receive periodic maintenance, which can be used for regular checks and updates of firmware and software. In case public key cryptography is implemented, it can also be used for updating certificates and keys, along with provision of fresh Certificate Revocation Lists (CRLs).

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.

Honest Majority

Usually it is thought that majority of the drivers in the system are honest and there are few vehicles or nodes which will try to attack in some ways If anything wrong happens then the set of good drivers will help the law enforcement to find the adversary with the help of polling and voting system.

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

CHAPTER- 4

Related Works

Although handling security issues in VANET is very tough, because handling security issues will increase the overhead cost and also the functional cost. VANET will be executed when cost management and security handling issues, both will be reduced or compromised so that the system becomes effective from both the point of views. While going through all the papers each and every paper gave us certain information. VANET follows a simple security architecture which is underlined below [1, 3].

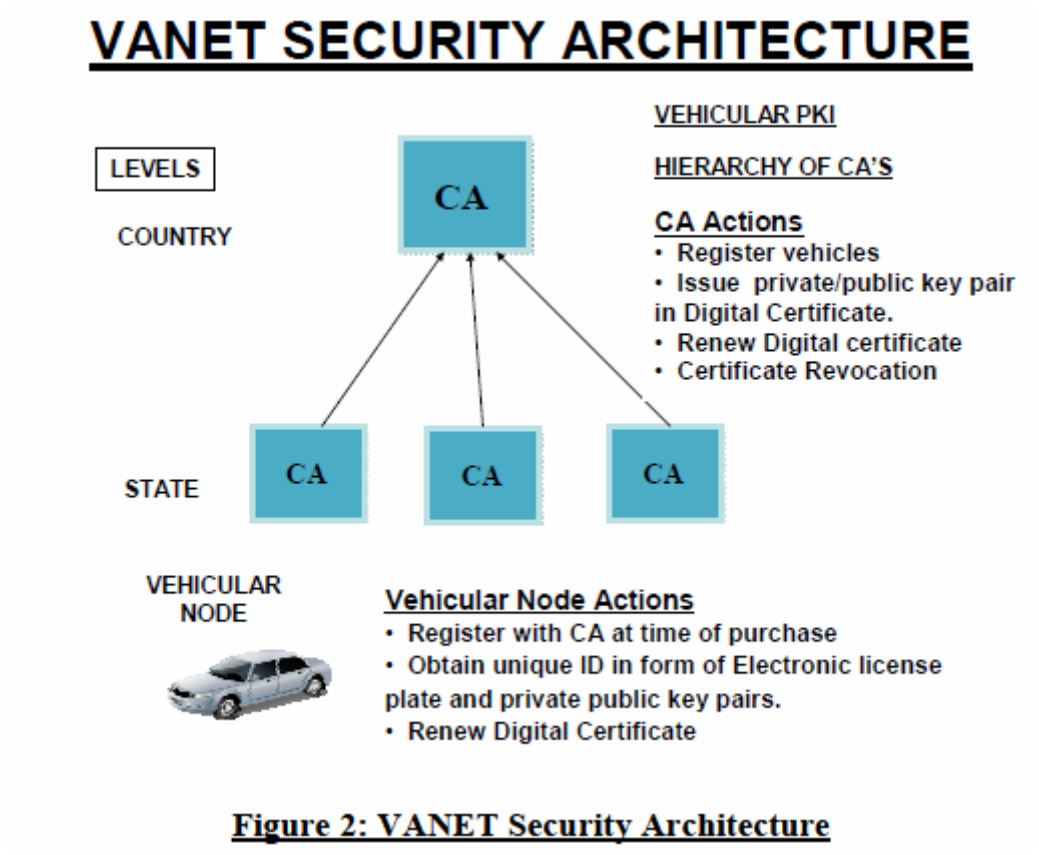

Figure 2: VANET Security Architecture

The basic architecture consists of Network nodes which can be either Vehicles or Road Side Infrastructure and existing Registration Authorities for vehicle registration and record maintenance.

These nodes will be installed with required sensors for gaining information, processing units for processing the collected or received information and communication system for disseminating information to and receiving information from other nodes. A secure system, besides the basic network nodes, will consist of a Vehicular Public Key infrastructure (PKI), a Secure Computing platform and various security mechanisms. Secure mechanisms comprise identity management using Electronic License Plates with certified public and private keys attached to the owner, Authentication and Integrity using Digital Signatures, Privacy using Pseudonyms, Pseudonym handling and Certification Revocation mechanisms.

A Vehicular PKI will consist of the national and state level registration authorities acting as Certification Authorities (CAs) which will issue certified public/private key pairs to vehicles. A Secure Computing platform on a vehicle will consist of tamper resistant hardware and firmware. Its job is to store cryptographic material (private keys) and a trusted (tamper proof) clock.

Digital Signatures will provide the required authentication and integrity along with non-repudiation using timestamps.

Privacy is introduced by using Pseudonyms in the form of additional set of public/private keys which are given to the user. These keys are used for a short period of time and changed frequently. These keys do not contain identity related information but can be traced back to the owner in liability related cases with the help of central authorities. The aim in using pseudonyms is to ensure that a vehicle cannot be tracked and a message cannot be attributed to it’s sender by other vehicles

Finally, when a vehicle becomes faulty or is detected as an illegitimate or malicious vehicle, Certificate Revocation mechanisms are required to revoke

both long term certificates and set of Pseudonyms currently being used by the vehicle.

The security architecture developed by the Vehicle Safety Communications Consortium (VSCC) and subsequently submitted to IEEE P1609.2 can be seen as the only approach for a security architecture in vehicular networks that is under standardization so far. It defines a public-key-infrastructure (PKI)-based approach for securing messages sent in a vehicle-to-vehicle and vehicle-to-infrastructure fashion.

The Daimler Chrysler group also published security architecture in the form of a layered structure with multiple views of the system. The security architecture of the system discussed in this paper contains the Vehicle Manufacturer and the Registration Authority for registration of nodes and assigning node identifiers, the Inspection site for test and certification of nodes, an Escrow entity with authority to identify and revoke certification of nodes and finally the communication infrastructure consisting of communication systems, processing and databases necessary to carry out online testing, pseudonym provision for nodes and infrastructure based data assessment and intrusion handling.

There are also some papers which dealt with the entire environment that how the communication process will be like [6], its result showed that effective communication between nodes depends on the density of vehicular nodes, there velocities and the number of lanes, i.e. width of the road.

Papers such as, [2, 7,8 and 9] dealt with routing protocols and gave effective solutions so that the communication between the nodes is computational effective and leading to less congestion of network traffic.

There are security solutions that are related with the deployment of RSU’s. In [11] CA cluster in different regions comply with corresponding scalability strategy

and regional policy. A distributed IDS system integrated with the CA database provide further security protection from malicious vehicles with legal certificates. The certificate caching and forwarding schema accelerates authentication. Where as in [12] usage of DSRC mainly gives a flawed solution in deployment of RSU, but it gave a simple mathematical approach of getting the position of a vehicular node without the help of GPS.

In [10] a solution of group formation combined with RSU is illustrated, which resulted in easy revocation of malicious vehicle, location privacy protection is improved and the system maintenance becomes flexible.

In [4], the paper has made use of syntactic aggregation and cryptographic aggregation techniques to dramatically reduce the transmission cost, and adopt batch verification technique for efficient emergency messages verification. This made the authentication of the emergency events easier.

Chapter-5
SECURITY FRAMEWORK

The proposed solution is based on transferring authenticated messages with the help of base stations, monitoring center and road side situated camera. The message authentication is monitored by the Central Authority (CA), i.e. monitoring center and at the same time, spreading proper messages to all the vehicle is also monitored by CA.

There are certain assumptions which are considered beforehand, i.e. deploying the whole proposed system. It will be discussed through out, while describing the system.

There will be **a monitoring center** beside the road which will have quite a good number of **base stations** under its centers supervision, which will perform the monitoring duty. These base stations will be set beside roads on such a way that it does not collide with any other form of interfering signals. These base stations will be a node of the network, which is able to communicate with other nodes. Base station will have a secured computer platform and various security mechanisms and a simple form of identity, unlike vehicular nodes which can be easily addressed by the monitoring center. When vehicles will pass the base stations then it will communicate with the help of a ***hello message*** with the base station, thus the base station will be able to notify the vehicle, by getting the identification of that vehicle. [12] There will also be road side cameras situated at a specific gap, which is computer controlled and which will be highly maintained. The cameras will have quite a good number of functionality, such as quick image processing, tamper proof and most importantly climatic behavior proof.

Now the whole communication process will be explained here-

Let there is an emergency event, then a message will be generated by a vehicle (who is a part of the situation or viewer of the situation**) to the nearby base station,** the message will be generated by the vehicle's uplink communication system. It will be proposed that there will always be a two way communication. Now the base station will receive the message and transfer it to the monitoring center. The monitoring center always needs to be extremely active, because VANET will be the biggest deployment of technical contribution in maintaining road situation. Now the monitoring center will identify the location of the event via camera and GPS or else a position method [12] will help us to get the location of the vehicle. Monitoring center will verify the information by the help of the base stations present near the emergency situation. Triangulation method can be used by the base stations to verify the exact situation. Also it is assumed that a base station can monitor a 500m radius circular region.

If the situation is true then, monitoring center will instruct the base station to transmit the message using the group formation rule; it will choose a group leader and ask him to convey the emergency message to the whole group. Then the question of authentication of these messages can be asked by any other vehicle in the group. It will be instructed to vehicular nodes that for authenticating a message's reliability send a message back to the nearby base station. The base station will wait for a certain percentage; let *K* out of *L* number of vehicles present in the group. Later it will stop receiving the message. It will generate a yes message by singly using binary system, i.e. 0 for a wrong message generated (no) and 1 for a correct message generated (yes).

If the situation is false then, monitoring center will directly revoke the nodes licensed certificate by sending a message to the falsified vehicle. It will cancel its public/private pair of keys. Then the car will be put in Certificate Revocation List

and the list will be delivered to other vehicles by the base station using group formation.

Model hardware in vehicular nodes, there will be a device which has short range radio devices (DSRC). It will have two buttons- one for receiving data and other for sending data. When the node is communicating with base stations it will use its uplink channel and when it receive data, then base station will use the downlink channel.

Now there a few shortcomings of this system such as it will have network overheads as there will be lot of redundant networks roaming around in the system. Also road side cameras need to be maintained and monitoring center should have accountability of there actions. Last and above all, time delay is present in the system.

Now the expected return of the system is much higher in long run. There will be a message transfer system that is monitored entirely by a monitoring center. No adversaries can attack the system, if the devices are properly protected. Also TPD should be present in vehicular nodes which will make sure that vehicular communication is done smoothly, i.e. malicious attackers cannot have access to manipulate it. There will be less (negligible) damage to life and property of state. Time delay is a major problem in this system. DSRC has been modified in recent years, which is done to reduce the time latency. [7] Over here DSRC is used everywhere. For meeting up security problems in VANET this could be a solution.

It is an effective system in terms of security issue handling but not entirely a cost effective solution. But in the long run the cost will be accumulated with the savings that will be achieved due to the efficiency of this system, i.e. less accidents and proper traffic management. A study shows that every year around 43,000 people die and around 1,200,000 people gets injured due to road

accidents in Europe [12]. So calculating these fatal injuries will have much higher cost than implementing the proposed system!!

CHAPTER-6

Future research direction and Conclusion

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.

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

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. Al Sakib Khan Pathan: A book: where a chapter is Security in VANET- YEet to yet be published.

2. Fay Hui: **A survey on the characterization of Vehicular Ad Hoc Networks routing solutions**
ECS 257 Winter 2005
Date: 01/28/2005

3. Antonios Stampoulis (antonios.stampoulis@yale.edu),Zheng Chai: **A Survey of Security in Vehicular Networks**

4. Haojin Zhu, Xiaodong Lin, Rongxing Lu, Pin-Han Ho, Xuemin (Sherman) Shen: **AEMA: An Aggregated Emergency Message Authentication Scheme for Enhancing the Security of Vehicular Ad Hoc Networks**

5. Zheng: Challenges in vehicular networks

6. Maen M. Artimy, William Robertson, and **William J. Phillips: CONNECTIVITY IN INTER-VEHICLE AD HOC NETWORKS**

7. Jijun Yin Tamer ElBatt Gavin Yeung Bo Ryu: **Performance Evaluation of Safety Applications over DSRC Vehicular Ad Hoc Networks**

8. **S.Y.** Wang: **Predicting the Lifetime of Repairable Unicast Routing Paths in Vehicle-Formed Mobile Ad Hoc Networks on Highways**

9.Linda Briesemeister
Role-Based Multicast in Highly Mobile
but Sparsely Connected Ad Hoc Networks

10. Yong Hao, Yu Cheng, and Kui Ren
Distributed Key Management with
Protection Against RSU Compromise in
Group Signature Based VANETs

11. Wenmao Liu, Hongli Zhang and Weizhe Zhang
An autonomous road side infrastructure based
system in secure VANETs

12. Une Thoing Rosi and Chowdhury Sayeed Hyder
A Novel Approach for Infrastructure Deployment for VANET