International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 02 | Feb-2016 www.irjet.net p-ISSN: 2395-0072

Security Requirements for IVC Network

D. V. Jamthe[1], D. B. Khadse[2], Y. B. Malode[3]

[1] Asst. Prof, Computer Science & Engineering Department, PBCOE, M.H., India
[2] Asst. Prof, Computer Science & Engineering Department, PBCOE, M.H., India
[3] Asst. Prof, Information Technology Department, PBCOE, M.H., India

---

Abstract – ***IVC Network will improve in the near future for the safety, comfort of drivers and passengers on the road. In IVC network vehicles are equipped with the necessary transmission Links and embedded systems that will make such type of communication possible using Bluetooth or DSRC. The IVC Network has dynamic topology therefore massage broadcasting should be done in Secure mode. This paper presents security requirements for IVC Network, as the vehicle is broadcasting a message is not a selfish or malicious vehicle. Therefore VAM is needed to ensure the integrity and reliability of the messages exchanged in the network. For this Public Key Infrastructure techniques are the solution for authentication that resides on the idea that each vehicle is assumed to carry out a certain amount of secure operations such as signing and Timestamping. Using PKI encryption technique, there will be no communication delay or overhead.***

Key Words: *IVC, IVCN, VAM, VANET, ITS, PKI, V2V.*

1. INTRODUCTION

IVC networks developed to improve the safety, security and efficiency of the transportation systems and enable new mobile applications and services for the traveling public. The purpose of Vehicular Communication Network (VC) is to create a safer environment and better driving conditions for vehicles on the road. Safety applications are the most important and more urgent to develop, since its matter of saving lives by preventing traffic accidents. VANET consist of Inter Vehicle Communication (IVC) & roadside to vehicle communication (RVC). IVC and RVC applications fall into two categories: Safety-related Information and Infotainment services. Only the security issues of safety-related applications are focused as they are lying at the core of IVC NETWORK concept and bring challenging problems.

In Inter-Vehicular Communication Network, the vehicles regularly broadcast safety-related messages. The idea behind safety application in Inter - Vehicular Communication Network is to have a mechanism in which vehicles on a road can exchange data or information so that to prevent accidents. This exchange of information is going to be through wireless messages between a vehicles and surroundings vehicle on the same road. The surrounding vehicle will use these messages to inform the driver of some dangerous situations happening on the road. [1] Therefore, through these messages the driver of each vehicle will make a better decision regarding a specific situation such as collision, congestion, or construction. Therefore, security and privacy are necessary in Inter - Vehicular communication for a successful acceptance and deployment of this technology, because attackers or pranksters can cause a huge damage in terms of life and road accidents as described in [2]. As a wireless communication technology, VANET is highly vulnerable to abuse and attacks. An adversary may inject a false information in order to mislead the target vehicles or with tampering the on board unit, implement an impersonation attack. He may also, by recording the messages of target vehicle, track the vehicle's location and collect private information about the vehicle.

Therefore it is need to secure the broadcast messages between vehicles on one hand, and each vehicle on the road should be known to be trusted on this other hand. Vehicle authentication on the roads might make the process of implementing Vehicular Communication harder. Each driver on the road should keep user's privacy protected to accept to use this technology which is an issue. Therefore, the authentication process should take place without affecting the privacy of the vehicles. For example, if a vehicle receives any message from a surrounding vehicle, it should test and check if that surrounding vehicle has a valid certification or not, otherwise the message received will be ignored. In this paper we evaluate proposed security mechanisms for Inter - Vehicular Communication Network, most of which haven't been implemented yet for vehicle to vehicle.

The Inter-Vehicle Communication systems are a new paradigm of networking. Largely related to mobile ad hoc networks and their distributed, self-organizing structure, they also introduce new threats [3]. Vehicle to Vehicle Communication is one of the most promising technologies to make traffic in future safer and efficient. The number of possible use cases is immense; the technology development is in progress [4]. In Intelligent Transport Systems (ITS), it has exchange necessity information between vehicles such as position and speeds in order to

guarantee an efficient trip and insurance. Through the Inter-Vehicular Communication Network, each vehicle can exchange information such as position, speed, acceleration, direction of the vehicle with its neighbours as shown in Figure1. Therefore this transfer of messages should be in secure mode.

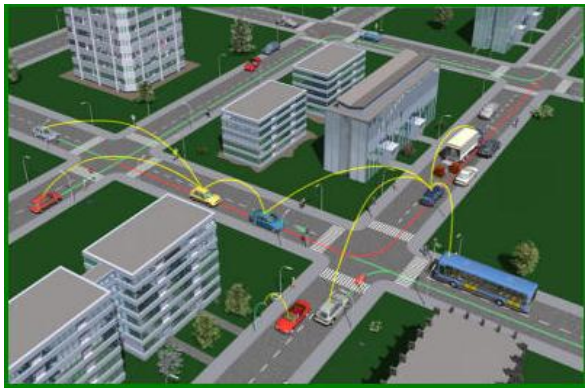

Figure1. Inter – Vehicular Communication Network

In the next section, the Adversaries, Threats and Attacks are discussed. Section III discussed security challenges in IVC Networks. Section IV states the security requirement for IVC Networks. Section V and VI discussed Security Solutions for IVC Network and Public Key Infrastructure Technique respectively. Section VII states the result of response time for encrypted communication. Finally the paper concludes and discuses a future work to provide a security for collision avoidance in IVC Network.

2. ADVERSARIES, THREATS AND ATTACKS ON IVC NETWORK

In IVC Network, V2V communication is done through the wireless network, which in some cases can be fatal for different attacks. Therefore, it should be noticed that any wireless device that runs on the same communication protocol stack can be a threat to the network. The list of adversaries that should be aware of is very long, and the methods are very different. [5] Here are some types of adversaries:

Greedy Drivers:

Try to convince the vehicle around user that there is a congested road ahead so that they will choose alternate routes and allow user a clear path to destination.

Snoops:

Everyone who wants to get maximum information about other drivers. After collecting the information probably harm the user.

Hackers:

Teenagers or hackers probing for vulnerability and seeking fame. It could also abuse the security vulnerability to DoS attacks to disable applications or prevent critical information from reaching another vehicle.

Industrial Insiders:

Attacks by insiders are particularly insidious, and the extent to which vehicular networks are vulnerable will depend on other security design decisions.

Malicious Attacker:

Malicious attackers deliberately attempt to cause harm via the applications available on the vehicular network.

Now the most important thing is vulnerabilities and its impact on IVC Network users.

A. *Denial of Service (DoS):* in which the attacker will overwhelm a vehicle with messages in order to congest the communication channel.
B. *Message Suppression Attack:* In a more subtle attack, the adversary may use one or more vehicles to launch a suppression attack by selectively dropping packets from the network.
C. *Fabrication Attacks:* An adversary can initiate a fabrication attack by broadcasting false information into the network. These attackers are diffuse wrong information in the network to affect the behavior of other drivers (e.g., to divert traffic from a given road and thus free it for themselves) as shown in Figure2.
D. *Spoofing Attacks:* Very common in regular or wired attacks is spoofing, which basically means impersonating somebody you are not, and therefore, send messages to other nodes, which you are not supposed to send. So, combining spoofing with message fabrication can lead to very dangerous results.
E. *Eavesdropping:* In this an intruder will can interfere into the conversation of two drivers in two vehicles and get message in which there might be some important information critical to a driver's privacy, or will violate her/his privacy.
F. *Alteration of Data:* It consists of attacking a network in order to alter the data inside the message exchanged on the road. The attacker will access the content of a certain message in the network and change it as wished. Again this can cause very serious consequences, in the case the hacker changes the message from a regular message to a warning which will affect the traffic on the road or even create incidents.
G. *Masquerading*: In masquerade attacks, an entity poses as another entity. It is caused when an unauthorized vehicle pretends to be another vehicle by using false

identities and can be motivated by malicious or rational objectives.

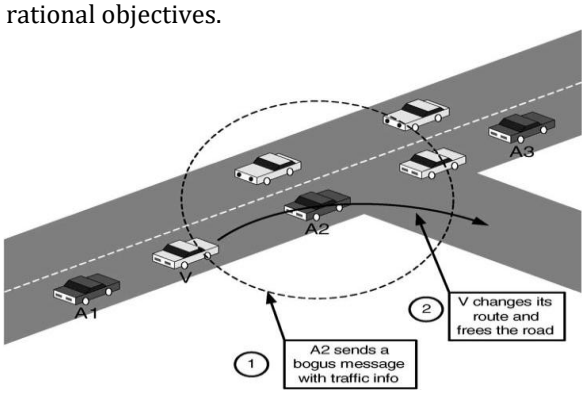

Figure2. In this example *bogus information* attack, colluding attackers (A2 and A3) disseminate false information to affect the decisions of other vehicles (V) and thus clear the way of attacker A1.

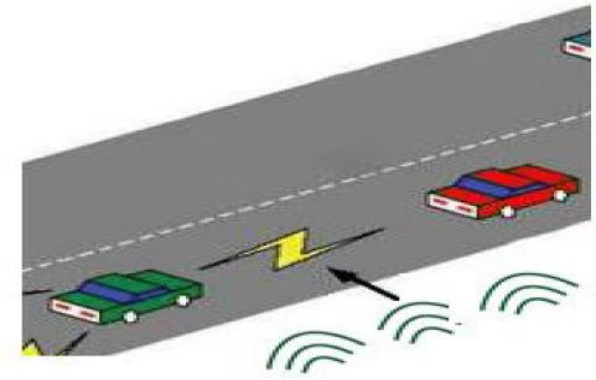

Figure 3: Signal Interruption of V2V Communication

3. SECURITY CHALLENGES IN IVC NETWORK

Inter – Vehicular Communication Network is a new concept in VANET that will change roads and vehicles. However, implementing this technology will not be as easy as it looks. There are many challenges which prevent the implementation of such system. Vehicle to vehicle communication will need some degree of authentication mechanism in order to secure the communication. Therefore, the authentication mechanism needs to have some degree of information about the vehicle and the driver. It's totally understandable that most drivers on the road want their identity to be kept private, that's why this issue of privacy versus authentication, will be one of the main issues in implementing IVC NETWORK worldwide.

Another IVC NETWORK security challenge is the forwarding of event-related messages on very large ad hoc networks of highly mobile nodes in such a way that the information can be trusted by receiving nodes because by doing so we improve traffic safety and mobility [6]. One of the most reasonable ones was to use the vehicle information instead of driver's information. That is, including the license plate information (number) of the vehicle, this actually constitutes a unique id, in the authentication message that will be used in communicating with other vehicles. The other main issue facing the implementation of IVC NETWORK on the road is availability. Meaning that all the system should be available to send and receive message all the time, and in real time. For example if a vehicle has an accident, it should send a warning messages to all the neighboring vehicles in real time or near real time so that the drivers of the other vehicles can avoid that accident, the figure 4 below show how that works. However, if there is a delay of broadcasting that message, the message will be meaningless since the other vehicles will not benefit from it. Conversely, implementing a system whose response time is real time or near real time, will make it more vulnerable many different types of hackers' attacks, but DoS attack will have the most impact on the system. It will easily overwhelm the system with a huge number of meaningless messages and makes it crash easier.

Another challenge for VANET is the range of coverage of the broadcasting a message. A message can be lost in the case of too few vehicles on the road, because there will be no vehicle to work as relay to that specific message and can be lost. Through some experiments conducted in [7] only 50% to 60% of vehicle on the road will receive a message that was intended to be sent to them. Another challenge is the error tolerance as mentioned in [8].

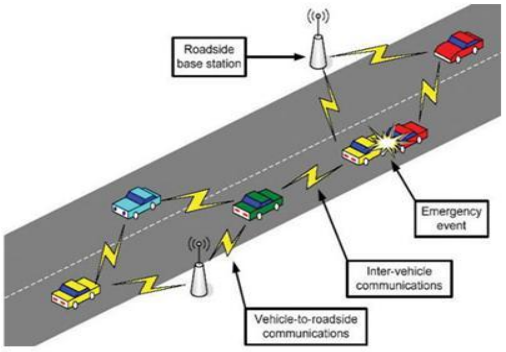

Figure 4: V2V and V2I in the case of an accident on the road

Inter – Vehicular Communication Network is intended to reduce the number accidents and save lives. Therefore, the applications that should be used should have a very low rate of failure, otherwise, it can cause to disastrous results. Therefore, the applications to be deployed and used should have a very low margin of error in order for them to be deployed in vehicles. Mobility is another concern to

IVC NETWORK developers, since vehicle network is so random and mobile. It's clear that the dynamic topology of the network will create the problem of the connectivity, so that, if there is a few numbers of vehicles on the road, some of them will not receive the message, if this vehicle is outside the transmission range of the closest vehicle on the road.

4. SECURITY IMPLEMENTATION REQUIREMENT FOR IVC NETWORK

In Inter-Vehicular Communication Network, the vehicles form a mobile ad-hoc network which consists of a collection of mobile hosts that communicate via radio transmission. There is a challenge in balancing security and privacy needs. On the one hand, the receivers want to make sure that they can trust the source of information. On the other hand, the availability of such trust might contradict the privacy requirements of a sender. The implementing security applications in IVC NETWORK, vehicle can't be achieved without a regular maintenance of the equipment that VANET provides. Actually, a regular check on the software and hardware will allow the authorities to ensure that vehicle's software hasn't been changed or modified for the sake of impairing the Inter-Vehicular Adhoc Network on the road.

In any cryptographic system, the confidentiality and the integrity of the private keys are essential while vehicles by their nature are highly vulnerable for tampering. Security and reliability of VANET relies on the tamper resistant Hardware Security Modules (HSM) in which the cryptographic keys are stored. Also cryptographic operations, such as digital signatures and encryption, are performed. For that every vehicle should be registered with an authority that provides VANET technology. For securing IVC NETWORKs communication possible, most of the drivers of the road are considered, or at least, most likely to be honest. Meaning that most of the users of the technology will attempt to modify or change the software or the configuration they are given.

5. SECURITY SOLUTIONS FOR IVC NETWORK

For successfully deploy of Inter-Vehicular Communication Network on roads, we need to face the problem of potential security threats presented above. Some of these solutions were worth considering and present in this section.

- 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. 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. [9], [13]

- Preserving Privacy and Anonymization

In IVC NETWORKs the issue of privacy and preserving the personal information of a driver and vehicle, is raising concerns for both vehicle 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 earlier 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. [10]

- 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. [11] Consequently, a check on the history and computing similarity, we can prevent a large number of Sybil attacks and position based attacks

- Secure Aggregation

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. [13]

6. PUBLIC KEY INFRASTRUCTURE TECHNIQUE

At the basic level, PKI (Public Key Infrastructure) can be described as a technique that enables users on a network to securely exchange data. This is achieved by the use of public key/ private key pair that are generated and exchanged through a certified authority. A PKI is an arrangement that binds public keys with users' identities through a certificate authority (CA). CA uniquely identifies user identities individually. To achieve that, each user must be individually registered with a CA. After registration the CA adds this user to a list and updates its list of users' identities and their assigned public keys. In addition to the registered users, CA will keep another list of the users with revoked certification. Meaning, the ones who were registered before, and for a reason, they should not trusted anymore.

The technique PKI allows two network vehicle users to authenticate each other to exchange using encryption. Therefore, password exchange mechanism can avoided, which can be very dangerous wireless medium. Since nobody can guarantee that a network is completely secure. Due to smooth and easy logic PKI infrastructure is advantageous. In this sender will sign a message, encrypt it using his private key. Similarly the receiver decrypts with the public key of the sender. It is also feasible for the sender to encrypt something the sender encrypts the message with the public key of the receiver. Then only the receiver can decrypt the message using his private key.

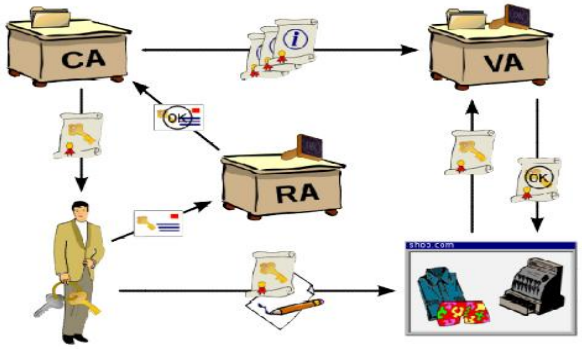

Figure 5: Illustration of Public Key Infrastructure [12]

7. SIMULATIONS

All the vehicles on the roads should broadcast their relative information to the surrounding nodes. For secure and reliable communication in IVC NETWORK, the proposed solution in this study is implemented. The simulation is done on the simulator taking two types of vehicles, one which is broadcasting the information without encryption and another is broadcasting the messages with encryption as shown in following Figure6.

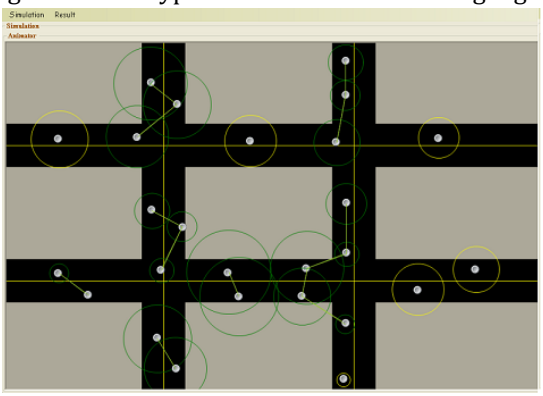

Figure6: Vehicles Broadcasting Information

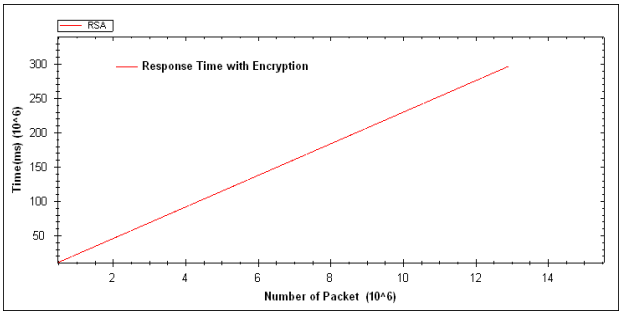

Figure7: Response time Simulation Result

Figure7 shows the response time of ready vehicles in the presence and absence of PKI encryption. The results obviously show that the response time in the case of encrypted communication is higher than in the regular communication (without encryption).

8. CONCLUSION

Securing Inter Vehicular Communication Network (IVC NETWORK) is a crucial and serious issue, since failure to do so will delay the deployment of this technology on the road. All vehicles' drivers want to make sure that their and vehicles identity is preserved while exchanging messages with the other entities on the road. Using PKI encryption technique, Vehicle authentication is ensures the integrity and reliability of the messages exchanged in the network. In future research directions, optimal inter-vehicular collision avoidance secure technique to the dynamic clustering mechanism will be taken an issue of IVC NETWORK. This is to ensure that the vehicles perform safety communication with each other, by defining a critical "inter-vehicular distance" to be maintained between any two vehicles.

REFERENCES

[1] Increasing Broadcast Reliability In Vehicular Ad Hoc Networks Nathan Balon And Jinhua Guo University Of Michigan – Dearborn 2006.
[2] U.S. Department Of Transportation, Bureau Of Transportation Statistics. Transportation Statistics Annual Report, 2003.
[3] Attacks On Inter Vehicle Communication Systems – An Analysis By Amer Aijaz, Bernd Bochow, Florian Dotzer, Andreas Festag, Matthias Gerlach, Rainer Kroh, Tim Leinmuller Proceedings Of The 3rd International Workshop On Intelligent Transportation Wit(2006).
[4] Inter-Vehicle Communication Systems: A Survey Mihail L. Sichitiu, North Carolina State University Maria Kihl, Lund University Ieee Communications Surveys & Tutorials 2nd Quarter 2008.
[5] A Survey Of Security In Vehicular Networks Antonios Stampoulis, Zheng Chai.
[6] Florian D., Lars F., Przemyslaw M.: 'Vars: A Vehicle Ad Hoc Network Reputation System'. Int. Conf. On A World Of Wireless, Mobile And Multimedia Networks (Wowmom 2005), 2005, Pp. 454–456.
[7] J. Yin, T. Elbatt, G. Yeung, B. Ryu, S. Habermas, H. Krishnan, And T. Talty. Performance Evaluation Of Safety Applications Over Dsrc Vehicular Ad Hoc Networks. In Proc. Of Acm Workshop On Vehicular Ad Hoc Networks (Vanet), 2004.
[8] Jean-Pierre Hubaux, , The Security And Privacy Of Smart Vehicles, Ieee Security And Privacy Magazine, 2(3):49-55, May-June 2004.
[9] Maxim Raya, Adel Aziz And Jean-Pierre Hubaux, Efficient Secure Aggregation In Vanets, Vanet'06, September 29, 2006, Los Angeles, California, Usa
[10] G. Yan, S. Olariu, and M.C. Weigle, Providing Vanet Security through Active Position Detection. Computer Communications, Volume 31, Issue 12, 30 July 2008, Pages 2883-2897
[11] Public Key Infrastructure. (2009, November 2009). In Wikipedia, the Free Encyclopedia. Retrieved October 10, 2009.
[12] Bryan Parno and Adrian Perrig. Challenges in Securing Vehicular Networks, HotNets 2005.

BIOGRAPHIES

The author1**, D. V. Jamthe** received the B.E. Degree in Information Technology from Rashtrasant Tukadoji Maharaj University of Nagpur, India, in 2005. He has received Master of Engineering (M.E.) Degree in Wireless Communication and Computing from G. H. Raisoni College of Engineering, Nagpur, Maharashtra, India. His research area includes Wireless Network, Computer Network, Computer Security, Adhoc Network, and VANET.

The author2**, D. B. Khadse** received the B.E. Degree in Information Technology from Rashtrasant Tukadoji Maharaj University of Nagpur, India, in 2007. He has received Master of Engineering (M.E.) Degree in Wireless Communication and Computing from G. H. Raisoni College of Engineering, Nagpur, Maharashtra, India.

The author3, **Y. B. Malode** received his B.E. degree in information technology from the Rashtrasant Tukadoji Maharaj University of Nagpur, India, in 2006. He has received his Master's Degree in Computer Science and Engineering from Rajiv Gandhi College of Engineering, Research and Technology, Chandrapur, Maharashtra. He is majoring in computer Science and is familiar with Data Mining. His research area includes Data Mining, Periodicity mining and Image processing.