ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.3, Issue 11, November 2014

Multiple channels in Vehicular Ad-Hoc Network to Enhance Security.

Nitish Shukla[1], Pranjal Katiyar[1], Aarti Gautam Dinker[2]

Student, Dept. of ECE, Gautam Buddha University, Greater Noida, Uttar Pradesh, India [1]

Faculty Associate, Dept. of ECE, Gautam Buddha University, Greater Noida, Uttar Pradesh, India [2]

ABSTRACT*:* VANET refers to vehicular ad-hoc network. In this network vehicles communicate with each other and with the roadside units to get the information of scenarios in their path ahead. As no. of vehicles have increased tremendously in the past few years security threats have also increased correspondingly so proper attention needs to be given on the security issues so that a comprehensive level of security can be attained.

Considering the different security issues, few new solutions have been proposed in this paper which is likely to improve the security aspects nevertheless only security issues have been considered to priority.

KEYWORDS*:* Attacks, RSU, OBU, authentication, directional antennas, multiple channels.

I.INTRODUCTION

An Ad-Hoc network is defined as a group of dynamically forming nodes forming a network without any centralized infrastructure.

VANET refers to vehicular ad hoc network which can be acknowledged as one of the special type of mobile ad hoc network or application of ad hoc network. In this network moving vehicles communicate with each other to gather information. The vehicles have OBUs i.e. on board units and the partial infrastructure that is created to assist these nodes is the RSUs i.e. road side units. So the OBUs and the RSUs communicate with each other gather information. Security in these networks is the area of research now days. Our paper firstly discusses the issues regarding the network security and then tries to explain the concepts of multiple channels, frequency reuse, directional antennas etc. to overcome the dominant issues that persists in the network.

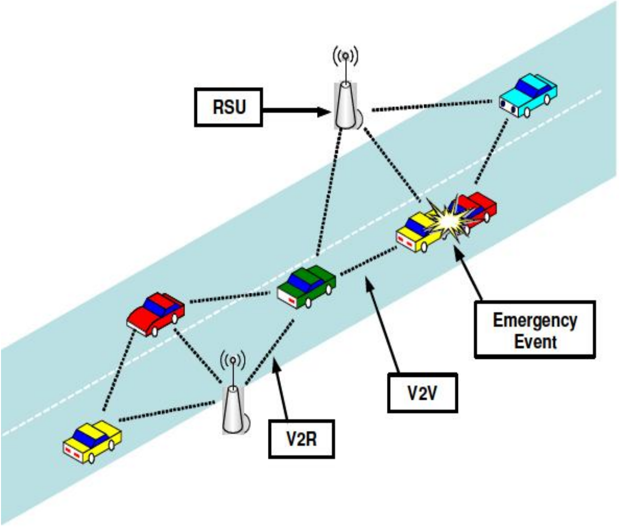

Fig 1: Example of a VANET [17].

10.15662/ijareeie.2014.0311067

II. RELATED WORK

1. Message suppression attacks

In this attack, the attacker selectively drops the packet from the network, these packets might hold the critical information for the receiver, and the attacker can then suppress these packets and can use them again in other time. The goal of such an attacker is to prevent concern authorities to from learning about collisions of vehicles and spreading the report for other vehicles as well. For instance, an attacker may suppress a congestion warning; this will make vehicles not to receive the warning and to wait in the traffic.

2. Replay Attack

This attack takes place when attacker replays the transmission of earlier information to take the advantage of the situation of the message at time of sending. Basic 802.11 securities have no protection against this attack. It does not contain sequence number or timestamps of the messages. Because of keys can be reused, it is possible to replay stored messages with the same key without detection to insert bogus messages into the systems. Individual packets must be authenticated, not just encrypted. Packets must have timestamps.

The goal of such an attack would be to confuse the authorities and possibly prevent identification of hit-an-run incidents.

3. Sybil attacks

This attack takes place when an attacker creates a large number of pseudonymous, and claims or acts like it is more than a hundred vehicles, to tell other vehicles that there is jam ahead, and force them to take alternate route. A Sybil attack depends on how cheaply identities can be generated, the degree to which the system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the system treats all entities identically.

4. Black-hole attack

In this type of attacks, malicious node claims having an optimum route to the node whose packets it wants to intercept. On receiving the request the malicious node sends a fake reply with extremely short route. Once the node has been able to place itself between the communicating nodes, it is able to do anything with the packets passing between them. For instance, malicious node “4” advertises itself in such a way that it has a shortest route to the destination node “D”, it initiates the route discovery process. The malicious node “4” when receives the route requests, it immediately sends a response to source. If reply from node “4” reaches first to the source than the source node “s” ignores all other reply messages and begin to send packet via route”2”. As a result, al data packets are consumed or lost at malicious node.

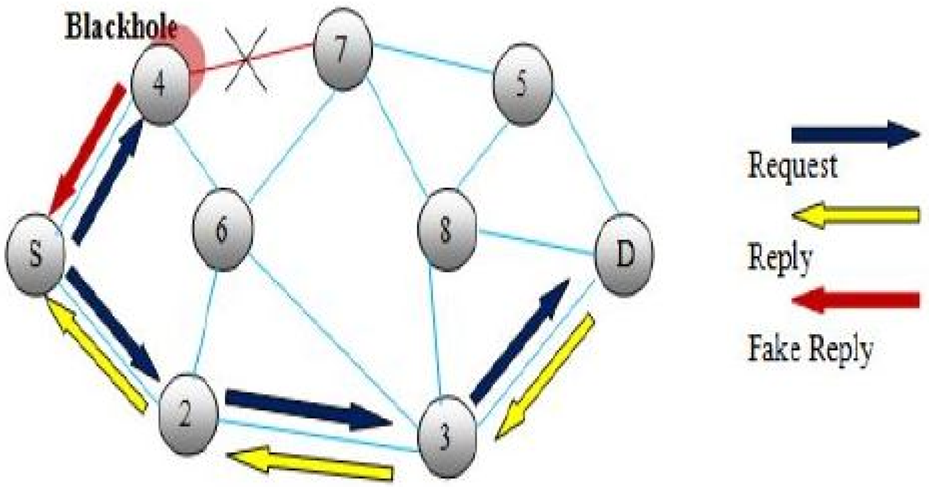

Fig 3: Black hole attack.[18]

10.15662/ijareeie.2014.0311067

5. Denial of Service attacks

This attack takes place when the attacker takes control of the vehicles resources or jams the communication channel used by the vehicular network, due to which it prevents important information from arriving to the vehicles. It also increases the danger to the driver, if that application information is required to driver for driving. For example, if suppose an attacker wants to jam a highway, it can make use of the DOS attacks and can prevent the information of accident to get spread to other vehicles approaching to highway. For this a possible solution is to switch between different communication channels or communication technologies (example Bluetooth for very short ranges).

6. SYN flooding attack

These are the types of attacks which are a kind of a denial of service attack. In this attacker tries to create large number of half opened TCP connection with node which is victim. These half opened connections direct the victim node never to complete the handshake to fully open the connection.

7. Alteration attacks

This attack happens when attacker alters an existing data. It includes making delay in the transmission of the information, replaying earlier transmission, or altering the actual entry of the data transmitted. For example, an attacker can alter a message telling other vehicles that the current road is clear while the road is the congested one.

8. Link withholding and Link spoofing attacks

Link withholding attack is the attack in which malicious node does not broadcast any information about the links to specified nodes. As a result of which the links between the nodes are lost.

In link spoofing attack, the node which is a malicious one, broadcasts or advertises the fake route information to disrupt the routing operation. This results in making malicious node to manipulate the data or routing traffic.

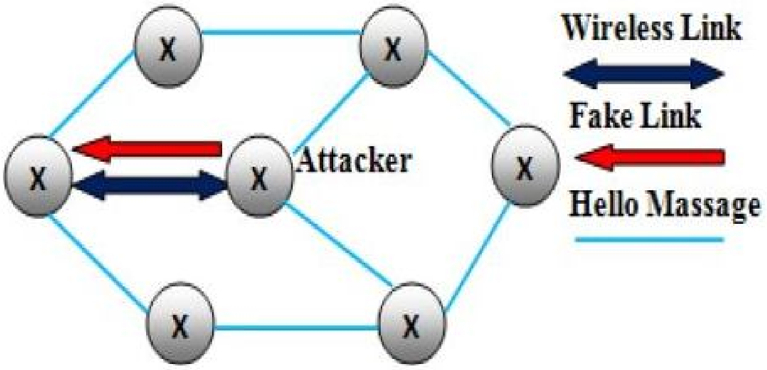

Fig 2: Link Spoofing Attack. [18]

9. Repudiation attacks

This attack refers to a denial of participation in all or part of communications. Packet security used at different layer by many of encryption mechanism and firewalls at different layer are not sufficient. In order to provide security of packets against many attacks, application layer firewalls may be taken into account. For instance, In order to monitor mission critical services spyware detection has been developed.

10. Fabrication Attack

These attacks can be made by the attacker by transmitting the false information into the network, this information could be false or transmitter could possibly act as other identity than original. This attacks include fabricate messages, warnings, certificates and identities.

10.15662/ijareeie.2014.0311067

III. PROPOSED WORK

There are various other ways in which security can be made prominent just by using simple basic techniques like multiple channels, directional antennas, digital signatures, certificates etc. Some of the techniques are discussed below:

1. Mean of multiple channels

This method can typically be used when only security is the main concern not the cost and resources. In this method multiple channels can be used to send the data over the air (no of channels are proportional to security and accuracy). Along with the multiple channels we use the concept of frequency reuse that states that the whole bandwidth can be divided into no. channels. So that a pool of channels are made, these channels are grouped together to form one blocks of multiple channel along with guard band between the channels so that interferences i.e. co-channel and inter channel interferences can be avoided. So the platform of the communication is multiple channels along with frequency reuse. The data for communication is sent on these multiple channels (the data is same on all the channels, but obviously the data would have been encrypted already to make the communication security more prominent). On the receiving end the data is received on the multiple channels and is decrypted, mean of the data is taken out and then the output is displayed for example if on any expressway there are ten cars moving ahead of the communicating vehicle which is communicating with road side unit (RSU) deployed for VANET, now the attacker hacks any one or two of the multiple channels used for communication and manipulates the data i.e. twenty cars instead of ten. Now on the receiving end the vehicle will receive ten and twenty both the data, had only one channel been used then there would have been problem but while using multiple channels partial incorrect data is received which is improved partially by taking mean of the received data. Here in the example mean of ten and twenty will be around fifteen according to the number of channels used by the network, therefore the motive of the attacker is failed by using multiple channels up to an extent.

The complexity and security are related stuff, more complex is the system more secure it becomes, the concept of metadata (data about the data) can also be implemented and then mean of the data received by the concept of metadata can be implemented but the complexity increases drastically along with the bandwidth and data-rate requirements.

One of the major problems that arise is of data-rate; it should obviously be as large as possible. To make this thing point feasible the range of the road side units and on board units should be reduced up to a considerable level so as to maintain the required data rate because the closer is the communicating device with the access point date rate improves accordingly.

As the ranges of the RSUs and OBUs have been reduced issue of handoff comes into light. Handoffs can be dealt on priority basis as there are no. of vehicles moving at different speeds. By using different heights of the antennas (RSUs) and different power levels it is possible to provide large and small cells which are co-located at a single location. This is called umbrella cell approach and is used to provide large area coverage to high speed users.
So by the use of multiple channels concept the security is enhanced and accuracy is also maintained up to an extent.

2. Pool of registered vehicles

In VANETs all the vehicles that are communicating with the RSUs and other OBUs must be registered and should be given a unique vehicle identification number just like IMEI numbers in the mobile communication. This will help in protecting the network from mischievous attackers which are out of the network, as only those OBUs will be able to communicate which are authentic. If at all the vehicles is stolen or something like that happens those OBUs may be deactivated or may be blacklisted so that the attacker do not get the access of network ever after being in the network. So in brief a pool of the registered OBUs and RSUs must have to be predefined so as to protect the network from adversaries

3. Directional antennas

Directional antennas can also be used to partially prevent the attackers it's not exactly one of the security techniques but the probability of the attacks by the attackers may be reduces considerably. While on the go information (like accidents ahead, traffic congestion etc.) required is of the things which are ahead of the vehicles in which we are travelling. This can be done by the use of directional antennas. Information received from the antennas in the direction of propagation may only be taken in consideration for processing not from all the directions. Four directional antennas

10.15662/ijareeie.2014.0311067

can be used and by the mechanism of switching only that information may be processed in which the driver is headed towards. This technique will show its importance when the attackers in the network try to spread wrong information from behind so as to profit themselves in the traffic situations.

4. Authentication

Authentication is an important part of a network's security when it comes to ensuring the identity of the users. There are a number of ways that the authentication can be accomplished; some of them are as follows.

Network access authentication provides with the verification of the user's identity to the specified network. The user has to provide their credentials whenever he or she wants to access the network.

Certificate services consist of data that is used for authentication and securing of communications especially on unsecured networks.

Digital signatures can be used to acknowledge the authenticity of the users such that the messages are not from the unauthorized users and data integrity is maintained.

Layered Authentication- It is an access management process in which the identity of an individual node is verified by more than one authentication process.

While using multiple channels different authentication methods can be implemented on different channels. To make the security more prominent multi-layered authentication may be used but it has got a very huge disadvantage as it has to be implemented on the vehicles which are moving so there is very less time for establishment of connection so multi-layered authentication is somewhat not possible. Now again this may be done if at all the speedy and slow moving vehicles can be differentiated. Multi layered authentication can be done on the slowly moving vehicles and for speedy nodes simple authentication method may be followed.

IV.CONCLUSION

We can see that as the number of vehicles is increasing exponentially security threats are increasing proportionately. By using the multiple channels and putting in different encryption techniques into it can be prominent solution but again there are a number of issues as bandwidth requirement, data rate cost, handoffs etc. which needs to be dealt with. Directional antennas are very useful too when it comes to congestion free network that reduces unnecessary data transfer quite considerably. However these methods can be implemented for a secure and reliable communication network for the vehicles.

REFERENCES

1. M Raya, P Papadimitratos, JP Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, Vol 13, October 2006.
2. GeorgiosKaragiannis, OnurAltintas, EylemEkici, Geert Heijenk, BoangoatJarupan, Kenneth Lin, and Timothy Weil., "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions", IEEE Wireless Communications, October 2011.
3. M Raya, J Pierre Hubaux," The security of VANETs", Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks, 2005.
4. Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures, "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)", IEEE Wireless Communications, October 2010.
5. GMT Abdalla, SM Senouci "Current Trends in Vehicular Ad Hoc Networks", Proceedings of UBIROADS workshop, 2007.
6. Car-to-Car Communications, www.car-2-car.org
7. [7]. J. Douceur," the Sybil Attack", First International Workshop on Peer-to-Peer Systems, 1st ed, USA, Springer, 2003.
8. Prof. Vaishali D. Khairnar and Dr. S. N. Pradhan. "Comparative Study of Simulation for Vehicular Ad-hoc Network". International Journal of Computer Applications (0975 – 8887) Volume 4– No.10, August 2010.
9. Yi Qian, Kejie Lu and Nader Moayeri, "A Secure VANET MAC Protocol for DSRC Application".
10. X Lin, R Lu, C Zhang, H Zhu, P Ho,and X Shen. "Security in Vehicular Ad Hoc Networks ", IEEE Communications Magazine, vol. 4, April 2008.
11. Security & Privacy for DSRC-based Automotive collision Reporting.
12. P Papadimitratos, L Buttyan, JP Hubaux, F. Kargl, A. Kung, M. Raya, "Architecture for Secure and Private Vehicular Communications", 7th International Conference on ITS, 2007.
13. Robert Simon, Leijun Huang, Emerson Farrugia and SanjeevSetia, "Using multiple communication channels for efficient data dissemination in wireless sensor networks", 2005 IEEE.
14. F. Karnadi, Z. Mo, "Rapid Generation of Realistic Mobility Models for VANET ", proc. IEEE WirelessCommunications and Networking Conference, 2007.
15. Security & Privacy for DSRC-based Automotive Collision Reporting.
16. Wireless Communication, Rappaport.
17. F. Borgonovo, A. Capone, M. Cesana RR-ALOHA, "a Reliable R-ALOHA broadcast channelfor ad-hoc inter-vehicle communication networks".
18. Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review, Gagandeep, Aashima, Pawan Kumar.