International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue (6) NCRTCST-2013, ISSN 2249–071X

National Conference on Recent Trends in Computer Science and Technology (NCRTCST)-2013

Security Threats on Vehicular Ad Hoc Networks (VANET): A Review Paper

Senthil Ganesh N.
I Year M.Tech., Deptt. of Telecommunication Engineering,
SRM University, Chennai, India.
Email: senthilganesh90@gmail.com

Ranjani S.
Asst. Professor, Deptt. of Telecommunication Networks,
SRM University Chennai, India.
Email: ranjani.s@ktr.srmuniv.ac.in

***Abstract* – The constant growth of automotive market and the increasing demand for the car safety, also driven by regulatory (governmental) domain, the potential of car-to-car connectivity is immense. Emerging Vehicular Ad-Hoc Networks (VANET) has the potential to improve the safety and efficiency of future highways. While during with wireless communication security plays a major role for vehicular network application. A vehicle in VANET is considered to be an intelligent mobile node capable of communicating with its neighbors and other vehicles in the network.**

In this paper, we take the position that VANETs would indeed turn out to be the networking platform that would support the future vehicular applications. We analyze the various security threats and the existing solutions to overcome the threat factors and show that there are active research efforts towards making VANETs a reality in the near future.

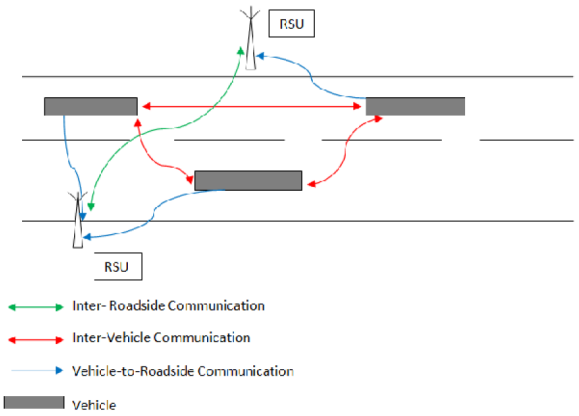
***Keywords* – Security, Vehicular Ad Hoc Networks, Threats, Network Attacks, Road Side Unit (RSU).**

I. INTRODUCTION

A Vehicular Adhoc network (VANET), a form of Mobile Adhoc Networks (MANETs), provides communication among nearby vehicles, between vehicles, and nearby fixed equipments called Road Side Units (RSUs). The Figure shows the VANET architecture. Every node i.e., a vehicle or RSU communicates with other nodes in single hop or multi hop. VANETs are designed with the goals of enhancing driving safety and providing passenger comfort. The various types of communication in VANET are the following:

- Vehicle-to-Vehicular (V-V) or Inter-Vehicular Communication
- Vehicle-to-Infrastructure (V-I) or Vehicle-to-Roadside Communication
- Inter Roadside Communication.

IEEE 802.11p is an improvement of the IEEE 802.11 standard to add Wireless Access in Vehicular Environments (WAVE). It defines enhancements to 802.11 and supports Intelligent Transportation Systems (ITS) applications. This includes data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure in the licensed ITS band of 5.9 GHz (5.85-5.925 GHz). IEEE 1609 is a higher layer standard based on the IEEE 802.11p.



The Car2Car Communication Consortium is initiated by six European car manufacturers. Its goal is to create a European industrial standard for car-to-car communications extend across all brands. European Commission is pushing for a new research effort in this area in order to reach the goal of reducing the car accidents of 50% by 2010, aiming to reach a satisfactory level of secure VANET. In the U.S., FCC has delegated 75 MHz for DSRC (VANET radios) use in the 5.9 GHz band and the EU has dedicated 30 MHz to vehicle-to-vehicle communication. The car manufacturers are also inclined towards favoring VANETs. In the recent years, the main feature additions to the car had been on the software end and, to keep up with the competition and raise the profit margins, the car companies are sponsoring research activity in making VANETs a reality.

II. ARCHITECTURE

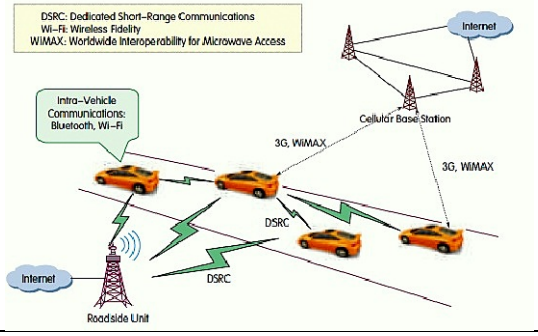
VANETs are a form of mobile ad-hoc networks to provide communications among nearby vehicles and between vehicles and nearby fixed equipment. To this end, special radios and sensors would be embedded within the car. The V2V communication infrastructure assumes the presence of high bandwidth with low latency.

The radios typically operate on unlicensed band making the spectrum free. The most compelling application for V2V would be the safety related application since the latency requirements for these applications are very stringent. The V2V infrastructure in VANETs can provide low latency data dissemination from the point of impact to the nearby vehicles using short range radios. The radio used for the communication is Dedicated Short-Range Communications (DSRC). DSRC/WAVE is part of the Federal Highway Authority's Vehicle Infrastructure Integration (VII) initiative and supports vehicle-to-vehicle (V-V) and vehicle-to-infrastructure (V-I) communications for emerging Intelligent Transportation Systems (ITS). DSRC/WAVE systems remove the drawbacks in the wireless infrastructure by aiding low latency, geographically local, high data rate, and high mobility communications.

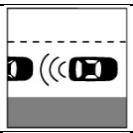
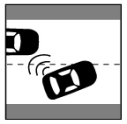
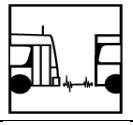
Inter-vehicle communication: The inter-vehicle communication configuration uses multi-hop multicast/broadcast to transmit traffic related information over multiple hops to a group of receivers. Vehicles send broadcast messages periodically and at regular intervals. If the message comes from a vehicle in front, the receiving vehicle sends its own broadcast message to vehicles behind it. This ensures that all enabled vehicles moving in the forward direction get all broadcast messages.

Vehicle-to-roadside communication: The vehicle-to-roadside communication configuration represents a single hop broadcast where the roadside unit sends a broadcast message to all equipped vehicles in the vicinity. Vehicle-to-roadside communication configuration provides a high bandwidth link between vehicles and roadside units. The roadside units may be placed every kilometer or less, enabling high data rates to be maintained in heavy traffic. For instance, when broadcasting dynamic speed limits, the roadside unit will determine the appropriate speed limit according to its internal timetable and traffic conditions.

Routing-based communication: The routing-based communication configuration is a multi-hop unicast where a message is propagated in a multi-hop fashion until the vehicle carrying the desired data is reached. When the query is received by a vehicle owning the desired piece of information, the application at that vehicle immediately sends a unicast message containing the information to the vehicle it received the request from, which is then charged with the task of forwarding it towards the query source.



III. VANET APPLICATIONS

Co-operative Collision Warning	
Lane Change Warning	
Intersection Collision Warning	
Approaching Emergency vehicle	
Rollover Warning	
Work Zone Warning	
Inter-Vehicle Communications	
Coupling/Decoupling	
Electronic Toll Collection	

IV. SECURITY

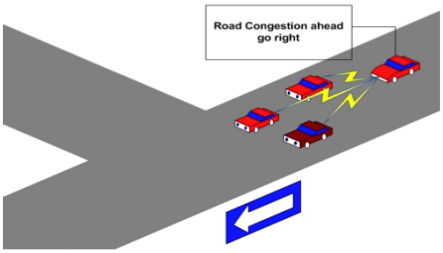
Security is an issue that needs to be carefully assessed and addressed in the design of the vehicular communication system. Several threats potentially exist, including fake messages causing disruption of traffic or even danger, compromising driver's private information, etc. Safety and traffic management require real time information and this conveyed information can affect life or death decisions.

Because VANET mobility is higher than MANET, routing with capability of ensuring security in VANET is more problematic than Adhoc. Illegal collection of messages by eavesdropping and gathering of location information available through the transmission of broadcast messages. Location privacy and anonymity are important issues for vehicle users.

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.

Security Threats:

- *Black Hole Attack* - Nodes refuse to participate in the network or when an established node drops out. All network traffics are redirected to a specific node, which does not exist at all that causes those data to be lost.
- *Malware* - Malware attacks, such as viruses in VANETs, have the potential to cause serious disruption to its normal operation. Malware attacks are more likely to be carried out by a malicious insider rather than an outsider. Malware attacks may be introduced into the network when the cars' VANET units and roadside station receive software updates.
- *Spamming* - The presence of spam messages on VANETs elevates the risk of increased transmission latency. The lack of centralized administration causes serious problems in VANET
- *Selfish Driver* - Some drivers try to maximize their profit from the network by taking advantage of the network resources illegally. A Selfish Driver can tell other vehicles that there is congestion on the road ahead. They must choose an alternate route. Thus the road will be clear for him/her.



- *Malicious Attacker* - This kind of attacker tries to cause damage via the applications available on the vehicular network. In many cases, these attackers will have specific targets, and they will have access to the resources of the network. For instance, a terrorist can issue a deceleration warning, to make the road congested before detonating a bomb.
- *Denial of Services (DoS)* – In DoS attack the main objective is to prevent the legitimate user from accessing the services and from the resources. The attack occurs by jamming the network or channeling the system so that no vehicle can access it and aggressive injection of dummy messages. This avoids communication completely in the network which is devastating in real time applications. Three different ways in which the attacker can achieve this are:
  - In basic level, the attacker overwhelms the node resource so that the node becomes continuously busy and will not be able to process further.
  - In extended level, the attacker jams the channel by generating high frequency in the channel. Thus the vehicle will not be able to communicate in the network.
  - Drops the packets. The goal of is to overwhelm the node resources such that the nodes cannot perform other important and necessary tasks. It leads to Jamming the Channel and Distributed Denial of Services (DDoS):
- *Masquerading* - The attacker actively pretends to be another vehicle by using false identities and can be motivated by malicious or rational objectives. Message fabrication, alteration, and replay can also be used towards masquerading. For example, assume an attacker tries to act as an emergency vehicle to defraud other vehicles to slow down and yield.
- *Global Positioning System (GPS) Spoofing* - The GPS satellite maintains a location table with the geographic location and identity of all vehicles on the network. An attacker can fool vehicles into thinking that they are in a different location by producing false readings in the GPS positioning system devices. This is possible through the use of a GPS satellite simulator to generate signals that are stronger than those generated by the genuine satellite. This also affects routing in VANETs, especially geographical-based routing.
- *Pranksters* - People probing for vulnerabilities and hackers seeking to reach fame via their damage. For instance, a prankster can convince one vehicle to slow down, and tell the vehicle behind it to increase the speed
- *Sybil Attack* - Attacker creates large number of pseudonymous, and claims or acts like it is more than a hundred vehicle Threats to Confidentiality les to tell other vehicles that there is jam ahead, and force them to take alternate route.
- *Timing Attack* - Time is a crucial aspect in any application so users need accurate information on right time without any delay. Time is also an important issue in ITS safety applications. In this attack attacker with-out manipulating the actual content add some time slot to create a delay in the message due to this user will receive the message after the required time. ITS safety applications are time critical application which requires data transmission on time otherwise major accidents can happen.
- *Message Tampering* - Any node acting as a relay can disrupt communications of other nodes. It can drop or corrupt messages, or meaningfully modify messages. In this way, the reception of valuable or even critical traffic notifications or safety messages can be manipulated. An attacker can make this attack by transmitting false information into the network, the

information could be false or the transmitter could claim that it is somebody else.

- *ID Disclosure* - This attack discloses the identity of other nodes in the network and tracks the current location of the target node. A global observer monitors the target node and sends a 'virus' to the neighbors of the target node. When the neighbors are attacked by the virus, they take the ID of the target node as well as the target's current location. Rental car companies are using this technique to track their cars.

V. REVIEW WORK

In this Section we will analyze the main existing proposals to provide the security services in VANETs. In this way, we will discover the most relevant trends and the Existing solution for each thread.

S.No	Threats in VANET	Existing Solutions
1.	Black Hole Attack	Exploit the packet sequence number included in any packet header. Find alternative route to the destination. This solution may impose overload to network. Finding additional node increases unwanted parameters such as delay or cost of service.
2.	Spamming	Privacy can be introduced by using Pseudonyms in the form of additional set of public/private keys which are given to the user which 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 its sender by other vehicles.
3.	Selfish Driver	All vehicles must be trusted to follow the protocols specified by the application. One proposed solution to mitigate this attack is to verify the received data in correlation with the data received from other sources.
4.	Malicious Attacker	The vehicles transmitting should be an authenticated user registered to a Certificate Authority in order to uniquely identify the vehicle.
5.	Denial of Services (DoS)	If the private key shared between the Access Point and car only, the attacker can never be able to exhaust the resource of the Access Point. Hence the delay in the request could also be prevented which usually occur in case of proxy-re encryption method of authentication.
6.	Global Positioning System(GPS) Spoofing	1.) Global Navigation Satellite System (GLONASS): This is a radio-based satellite navigation system. This is in operation with global coverage and of the same precision as GPS, but the disadvantages of GPS still hold good for GLONASS. 2.) Map Matching (using Geographic information systems): Where a vehicle's position is being identified using some fixed point in map like "university library". One can then calculate the distance after a vehicle has passed the point. The main disadvantage is loss of accuracy. 3.) Distributed Relative Ad-hoc positioning: Here if any one of the vehicles has GPS, the others can relative calculate the distance using the GPS enable vehicle and simulate its position in global map. This requires no Infrastructure support. But it is highly accurate.
7.	Pranksters	To overcome this, the services provided by the RSU should be available to the vehicles whenever it is required.
8.	Sybil Attack	A novel solution that uses on-board radar as the virtual 'eye' of a vehicle. Although the 'eyesight' is limited because a modest radar transmission range, a vehicle can see surrounding vehicles and receive reports of their GPS coordinates. By comparing what is seen to what has been heard, a vehicle can corroborate the real position of neighbors and isolate malicious vehicle
9.	Timing Attack	Using a globally synchronized time for all nodes and other is using nonce (Timestamp).
10.	Message Tampering	Unauthorized manipulation must be detected, so that the content of the messages sent between the vehicles should not be changed.
11.	ID Disclosure	The data being transmitted by the vehicles should be received by the registered vehicles only. Protocol should ensure that the vehicle ID is never revealed in the open. TPD ensures that the keys are not revealed to user.

VI. CONCLUSION

With the wireless technology becoming pervasive and cheap, VANET is going to turn out to be the networking platform that would support the future vehicular applications. In this paper we present some possible attacks and their solutions. In future we intend to develop the system for detecting the critical attacks and verifying it through simulation by applying our novel idea on the procedure to protect the safe messages.

We are working on increasing the precision of our system to detect all compromised vehicles and on simulating the Sybil attack and some combination of Sybil attacks and position attacks.

REFERENCES

[1] VANETs: The Networking Platform for Future Vehicular Applications - Gayathri Chandrasekaran
[2] Security on Vehicular Ad Hoc Networks (VANET): A Review Paper Ankita Agrawal1, Aditi Garg2, Niharika Chaudhiri3, Shivanshu Gupta4, Devesh Pandey5, Tumpa Roy6
[3] Vehicular ad hoc networks (VANETS): status, results, and challenges - Sherali Zeadally · Ray Hunt · Yuh-Shyan Chen · Angela Irwin · Aamir Hassan
[4] Threat Analysis and Defence Mechanisms in VANET Maria Elsa Mathew and Arun Raj Kumar P.
[5] Vehicular Ad-Hoc Networks: An Information-Centric Perspective - Bo Yu Chengzhong Xu
[6] Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET) Ghassan Samara#1, Wafaa A.H. Al-Salihy*2, R. Sures#3
[7] Overview of security issues in Vehicular Ad-hoc Networks José María de Fuentes, Ana Isabel González-Tablas, Arturo Ribagorda
[8] Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks - Surabhi Mahajan, Prof. Alka Jindal
[9] Security issues in VANET Rizwanul Karim Sakib
[10] VANET: Security attacks and its possible solutions - ajay rawat1, santosh sharma2, rama sushil3