A NEW GENERATION OF DRIVER ASSISTANCE AND SECURITY

Shivam Srivastava[1], Urvashi Hasani[2], Vivek Kumar[3], Lucknesh Kumar[4]

[1,2,3]Student, Department of CSE, Galgotias College of Engineering Technology, Greater Noida, India
[4]Assistant Professor, Department of CSE, Galgotias College of Engineering Technology, Gr. Noida, India

ABSTRACT

Vehicular ad hoc networks are tremendously and very effectively used for safety related applications. Especially for driver assistance and when it comes to safety of either from an accident or stealing of data VANET is the future of the all such problems."A New Generation of Driver Assistance and Security" gives a idea about VANET and also provide solutions to various problems comes in this. Authentication will be provided by Group signature and Identity based (ID- based) Signature scheme. The scheme Provides cost effective, highly privacy preserving of user, efficient message authentication and verification than existing system for VANETs. This required CA (Central Authority) and LA (Local Authority) where LA is group leader and which has to concern with CA. This safety technique is efficient, robust, and scalable for VANET's authentication and provide real-life solution match with the standard.

KEYWORDS

VANET, CA, LA, RSU, OBU, AU, GPS

1. INTRODUCTION

Now days, the sheer volume of road traffic affects the safety and efficiency of traffic environment. Approx 1.2 million people are killed each year on the road accidents. Road traffic safety has been the challenging issue in traffic management. One possible way is to provide the traffic information to the vehicles so that they can use them to analyse the traffic environment. It can be achieved by exchanging the information of traffic environment among vehicles. As all the vehicles are mobile in nature and they change their position every single second hence to provide a static solution can't solve the problem. And a survey explains that if driver can get information about 30 seconds ago then the accident can be avoided.

In VANET there are two types of communication are present one is pure wireless ad hoc network where vehicle to vehicle without any support of infrastructure. Second is communication between the road side units (RSU), a fixed infrastructure, and vehicle.

Vehicle to Vehicle communication (V2V):

First mechanism is (V2V), in which a autonomous mobile vehicle stabilized communication to other autonomous mobile
Vehicles in the wireless network, exchange, transmit, receive valuable information related to traffic

DOI: 10.5121/ijci.2017.6208

Vehicle to Infrastructure communication(V2I):

second is a vehicle connect to fixed Road Site Unit infrastructure (RSU) for traffic information, connect to Central Authority (CA),and connecting to different mobile vehicle node of different wireless networks or beyond its wireless communication range . Each node in VANET is equipped with two types of unit i.e. On Board Unit and Application Unit (AU). OBU has the communicational capability whereas AU executes the program making OBU‘s communicational capabilities. GPS unit and sensors for communication to other vehicles.Figure-1 Describes the C2C-CC architecture of VANET.

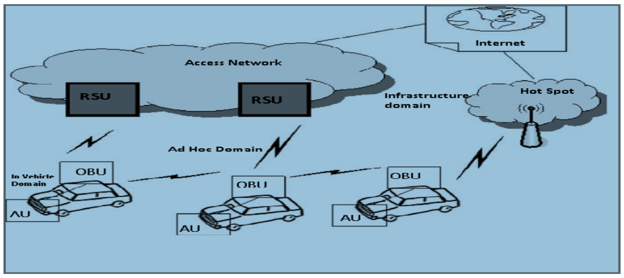

Figure-1 C2C-CC Architecture

To establish a VANET, IEEE has defined the standard 802.11p or 802.16 (WiMax). A Dedicated Short Range Communication (DSRC) is proposed which is operating on 5.9GHz band and uses 802.11 access methods. It is standardised as 802.11p which provides short range communication with low latency. USA has allocated 75MHz of spectrum in the 5.9GHz band for DSRC to be used by Intelligent Transportation Systems (ITS).

2.USER AUTHENTICATION PROTOCOLS AND ALGORITHMS

User Authentication can be confirmed by a number of protocols and algorithms. Practically, we use a combination of these protocols as they have higher efficiency as compared to individual protocols. We discuss here a few of them that are considered most efficient and thus, used widely. For this authentication system uses CA and LA where both are required for the successful completion of message sending and receiving. CA will decide which system are free for sending message and which system is free for receiving messages.

3. SECURITY ISSUES IN VANET

Among all the challenges of the VANET, security got less attention so far. VANET packets contains life critical information hence it is necessary to make sure that these packets are not inserted or modified by the attacker; likewise the liability of drivers should also be established that they inform the traffic environment correctly and within time. These security problems do not similar to general communication network. But they can be make more secured if we consider those network attacks also.

3.1 Security Challenges in VANET

The challenges of security must be considered during the design of VANET architecture, security protocols, cryptographic algorithm etc. The following list presents some security challenges:

- **Real time Constraint**: VANET is time critical where safety related message should be delivered with 100ms transmission delay. So to achieve real time constraint, fast cryptographic algorithm should be used. Message and entity authentication must be done in time.

- **Data Consistency Liability**: In VANET even authenticate node can perform malicious activities that can cause accidents or disturb the network. Hence a mechanism should be designed to avoid this inconsistency. Correlation among the received data from different node on particular information may avoid this type of inconsistency.

- **Low tolerance for error**: Some protocols are designed on the basis of probability. VANET uses life critical information on which action is performed in very short time. A small error in probabilistic algorithm may cause harm.

- **Key Distribution:** All the security mechanisms implemented in VANET dependent on keys. Each message is encrypted and need to decrypt at receiver end either with same key or different key. Also different manufacturer can install keys in different ways and in public key infrastructure trust on CA become major issue. Therefore distribution of keys among vehicles is a major challenge in designing a security protocols.

- **High Mobility:** The computational capability and energy supply in VANET is same as the wired network node but the high mobility of VANET nodes requires the less execution time of security protocols for same throughput that wired network produces. Two approaches can be implementing to meet this requirement.

- **Low complexity security algorithms***:* Current security protocols such as SSL/TLS, DTLS, WTLS, generally uses RSA based public key cryptography. RSA algorithm uses the integer factorisation on large prime no. which is NP-Hard. Hence decryption of the message that used RSA algorithm becomes very complex and time consuming. Hence there is need to implement alternate cryptographic algorithm like Elliptic curve cryptosystems and lattice based cryptosystems. For bulk data encryption AES can be used.

4. Security Requirements In Vanet

VANET must satisfy some security requirements before they are deployed. A security system in VANET should satisfy the following requirements:

- **Authentication**: Authentication ensures that the message is generated by the legitimate user. In VANET a vehicle reacts upon the information came from the other vehicle hence
- authentication must be satisfied.

- **Availability**: Availability requires that the information must be available to the legitimate users. DoS Attacks can bring down the network and hence information cannot be shared.
- **Non-Repudiation**: Non-repudiation means a node cannot deny that he/she does not transmit the message. It may be crucial to determine the correct sequence in crash reconstruction.

- **Privacy**: The privacy of a node against the unauthorised node should be guaranteed. This is required to eliminate the massage delay attacks.

- **Data Verification**: A regular verification of data is required to eliminate the false messaging.

4.1 Attackers on Vehicular Network

To secure the VANET, first we have to discover who are the attacker, their nature, and capacity to damage the system. On the basis of capacity these attackers may be three types [5].

- **Insider and Outsider**: Insiders are the authenticated members of network whereas Outsiders are the intruders and hence limited capacity to attack.

- **Malicious and Rational**: Malicious attackers have not any personal benefit to attack; they just harm the functionality of the network. Rational attackers have the personal
- profit hence they are predictable

- **Active and Passive**: Active attackers generate signals or packet whereas passive attackers only sense the network.

4.2 Attacks in the VANET

To get better protection from attackers we must have the knowledge about the attacks in VANET against security requirements. Attacks on different security requirement are given below:

- **Impersonate:** An impersonation attack is an attack in which an adversary successfully assumes the identity of one of the legitimate parties in a system. The goal of a strong identification or entity authentication protocol is to make negligible the probability that for a given party *A*, any party *C* distinct from *A*, carrying out the protocol and playing the role of *A*, can cause another party *B* to complete and accept *A*'s identityThis attack can be performed in two ways:

a) *False attribute possession:* In this scheme an attacker steals some property of legitimate user and later with the use of attribute claims that it is who (legitimate user) that sent this message. By using this type attack a normal vehicle can claim that he/she is a police or fire protector to free the traffic.

b) *Sybil***:** In this type of attack, an attacker use different identities at the same time.

- **Session hijacking:** sometimes also known as cookie hijacking is the exploitation of a valid computer session sometimes also called a session key—to gain unauthorized access to information or services in a computer system.

- **Location Tracking**: The location of a given moment or the path followed along a period of time can be used to trace the vehicle and get information of driver.

- **Repudiation:** Repudiation is the ability of users (legitimate or otherwise) to deny that they performed specific actions or transactions. Without adequate auditing, repudiation attacks are difficult to prove Information disclosure. Information disclosure is the unwanted exposure of private data.

- **Eavesdropping:** Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message, and videoconference or fax transmission. The term eavesdrop derives from the practice of actually standing under the eaves of a house, listening to conversations inside.

- **Denial of Service:** DoS attacks are most prominent attack in this category. In this attack attacker prevents the legitimate user to use the service from the victim node. DoS attacks can be carried out in many ways.

a) *Jamming:* In this technique the attacker senses the physical channel and gets the information about the frequency at which the receiver receives the signal. Then he transmits the signal on the channel so that channel is jam.

b) *SYN Flooding:* In this mechanism large no of SYN request is sent to the victim node, spoofing the sender address. The victim node send back the SYN-ACK to the spoofed address but victim node does not get any ACK packet in return. This result too half opens connection to handle by a victim node's buffer. As a consequence the legitimate request is discarded.

c) *Distributed DoS attack:* This is another form Dos attack. In this attack, multiple attackers attack the victim node and prevents legitimate user from accessing the service.

- **Routing attack**: Mobile ad hoc networks (MANETs) are a set of mobile nodes which are self-configuring and connected by wireless links automatically as per the defined routing protocol. These nodes communicate with each other by exchange of packets, which for those nodes not in wireless range goes hop by hop. Following are the most common routing attacks in the VANET:

a) **Black Hole attack:** A packet drop attack or blackhole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes.

b) **Worm Hole attack:** The attacking node captures the packets from one location and transmits them to other distant located node which distributes them locally. A wormhole attack can easily be launched by the attacker without having knowledge of the network or compromising any legitimate nodes or cryptographic mechanisms.

5. PROPOSED WORK

By analyzing the various type of attacks this paper deals with impersonate, session hijacking, location tracing, identity revealing attacks by developing such kind of secure environment which will be preventing our vehicles by hiding their reality so that an attacker can be confused.We will be creating a session, in such a way that acknowledgement signal will be shared between legitimate node and victim node through Central Authority. Central Authority will have information of each and every vehicle in encrypted form. Tracking id of vehicle will be changed within fixed time duration by random generation. Will be covering the confidentiality of data access, by maintaining a primary key between Central Authority and legitimate user so that in case of urgency, details of legitimate vehicle can be get from CA directly.

The New Generation of Driver Assistance and Safety aims at following criteria:

- Reduces the chances of accidents between car to car or car to RSU.
- Enhances the security of one vehicle and its messages.

- It secures the session between two units and use the method of acknowledgement to ensure this security.
- Hides the personnel information of one unit so that one cannot harm other intentionally.
- Enhances the use of CA so that data centralization become and easy and secure.

The tool used to achieve the specified objectives of the The New Driver Assistance and Security is OMNET++ and SUMO simulator.

6. CONCLUSION

In the last few years, there is an enormous potential worldwide for increase in vehicle use. Thus, developing an intelligent transportation system that support both safe driving and comfort application has received much attention for the automotive industry and government agencies. To reach this goal and to overcome the VANET challenges, many met heuristics approaches have been used.

This section concludes the dissertation of our research work. This research report developed a secure Authentication scheme which is random Vehicle Id generation and encrypting password and user details will be stored by using steganography technique and if one has to

REFERENCES

[1] R.Hajlaoui, H.Guyennet, and T.Moulahi, "A Survey on Heuristic-Based Routing Methods in Vehicular Ad-Hoc Network Technical Challenges and Future Trends", IEEE SENSORS JOURNAL, VOL. 16, NO. 17, SEPTEMBER 1, 2016.

[2] D.Tiwari, M.Bhushan, A.Yadav, S.Jain, "A Novel Secure Authentication Scheme for VANETs", Second International Conference on Computational Intelligence & Communication Technology,2016.

[3] Pham Thi Ngoc Diep, Chai Kiat Yeo," A Trust-Privacy Framework in Vehicular Ad Hoc Networks (VANET)", IEEE SENSORS JOURNAL, VOL. 16, NO. 17, JUNE 1, 2016 .

[4] A.Dahiya, V.Sharma, "A survey on securing user authentication in vehicular ad hoc networks". [Last Accesssed on 20-Nov-2016]

[5]ResearchGate

https://www.researchgate.net/publication/274173982_Security_Challenges_Issues_and_Their_Solutions_For_Vanet [Last Accessed on 17-oct-2016]

[6] Mohan Li mohan.li (at) wustl.edu (A paper written under the guidance of Prof. Raj Jain).

[7] Y.Bevish Jinila, K. Komathy, "An Efficient Authentication Scheme for Vanet Using Cha Cheon's ID Based Signatures", Volume : 4 | Issue : 6 | June 2014 | ISSN - 2249-555XResea Rch PaPeR, "INDIAN JOURNAL OF APPLIED RESEARCH".

[8] Y. Bevish Jinila, K. Komathy, "A Study of Privacy Preserving Authentication for Safety Message Communication in VANET"," International Conference on Mathematical Computer Engineering - ICMCE - 2013".

[9] Ram Shringar Raw1, Manish Kumar1, Nanhay Singh, "SECURITY CHALLENGES, ISSUES AND THEIR SOLUTIONS FOR VANET", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013.

[10] A. Dahiya, V. Sharma, "A survey on securing user authentication in vehicular adhoc networks", International Journal of Information Security, Vol. 1 (2001) pp. 36-63.

I am currently pursuing engineering in Computer Science from Galgotias College of Technology. I am critical thinker and always try to solve old problem with new efficient techniques. Me and my team worked on this vehicle ad-hoc network to make city an idea city with approximately zero accident rate.