Regional Trusted Authority providing Authorization in Vanet

R.Rajadurai[#1], N.Jayalakshmi[*2]

[#]Associate Professor Dept of CSE, [*]M.Tech Networking, Pondicherry University

[#*]Sri Manakula Vinayagar Engineering College, Madagadipet, Pondicherry-605107.

[1]king8125@gmail.com , [2]jaya.nasa40@gmail.com

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. VANET is different from MANET due to high mobility of nodes and the large scale of networks. Vehicular network have been emerged in advance to wireless technologies by this vehicular network is called as novel class of wireless technology and also as contribute on automotive industries. Vehicular network is formed between moving vehicles and wireless interfaces. In our paper we mainly focuses what are the VANET threats and their defects that been addressed in this research, we also have suggested a set of solutions using RTA to provide security and privacy in VANET.**

Keywords— **VANET, threats, attacks, defects.**

I. INTRODUCTION

VANET is a real life application of adhoc network. Vehicular network aims to provide communication between V2V(vehicle to vehicle) by means of inter vehicle communication(IVC) and V2R(vehicle to road side base station) by help of Roadside-to-Vehicle Communication (RVC).vehicular network is used in ITS(intelligent transport system) focuses on traffic management, public transport management, vehicle safety, emergency management .vehicular networks will contribute to safer and efficient roads by providing timely information to drivers, passengers and concerned authorities. Vehicular networks motives to avoid congestion and finds better routes by processing real time data by this one can save b time and also fuel provide economical gain. In road side Departing vehicles will inform other vehicles about their departure on the highway and arriving cars can send warning messages to other cars traversing that intersection. Most of the deaths caused by crashing of cars are avoidable .Routing in Vehicular Networks are more Feasible, and prevails in highly Secure manner. Characteristics in Vehicular Network: Unlimited transmission power: Power is usually not a constraint in vehicular networks as in the case of classical ad hoc or sensor networks. Higher computational capability: Node (vehicle) itself can provide continuous power for computing and communication and sensing. Predictable mobility: vehicle movements are usually in a dynamic environment. Roadway information is known from positioning systems and map based technologies such as GPS (global positioning system). Potentially large scale: vehicular networks will work efficiently on entire road network. High mobility: The environment in which vehicular networks operate is extremely dynamic and covers wide area. Network topology and connectivity: vehicles changing their position constantly, and exist in a dynamic nature. VANET provides road safety application to driver and vehicle, entertainment, commercial applications to passengers, they help to minimize the accidents and improve the traffic by providing timing information about collision warning, road sign alarm, in-place traffic view.

VEHICULAR NETWORKS CHALLENGES:

The vehicular network meets several major challenges required such as:

A. Mobility:

Basic idea from Ad Hoc Networks is that each node in the network is mobile, and can move from one place to another within the coverage area, but still the mobility is limited, but in VANET nodes moving in high mobility, vehicles make connection with another vehicles that may be never faced before, and this connection lasts for only for few seconds as each vehicle goes in its direction, and these two vehicles may never meet again. So securing the vehicle ion high mobility is hardest problem.

B. Volatility:

The connectivity among nodes can be highly transient, and maybe will not happen again, Vehicles traveling throw coverage area and making connection with other vehicles, these connections will be lost as each car has a high mobility, and maybe will travel in opposite direction[2],[8]. Vehicular networks lacks the relatively long life environment, so personal contact of user's device to a hot spot will require long life password and this will be unfeasible for securing VC.

C. Network Scalability:

The scale of this network in the world approximately exceeds 750 million nodes [7], and this number is growing, another problem arise when we must know that there is no a global clout to govern the values for this network (e.g. [2], [8], [9])

D. Self- sustaining:

At this moment only few number of cars will be having the tools required for the DSRC radios, so if we want to make communication we have to assume that there is a limited number of cars that will receive the communication, in the future we must concentrate on getting the number higher, to get a financial benefit that will courage the business secure to invest in this technology.

Our paper presents in section 2 an analysis of VANET model, in section 3 we analyzed the various VANET challenges and threats which should be considered in the hardest security problems of VANET, in section 4 we analyzed various authentication and privacy issues and in section 5 we discussed the RTA model to achieve a secure system, that been addressed by other papers and researchers.

II. VEHICULAR NETWORK MODEL

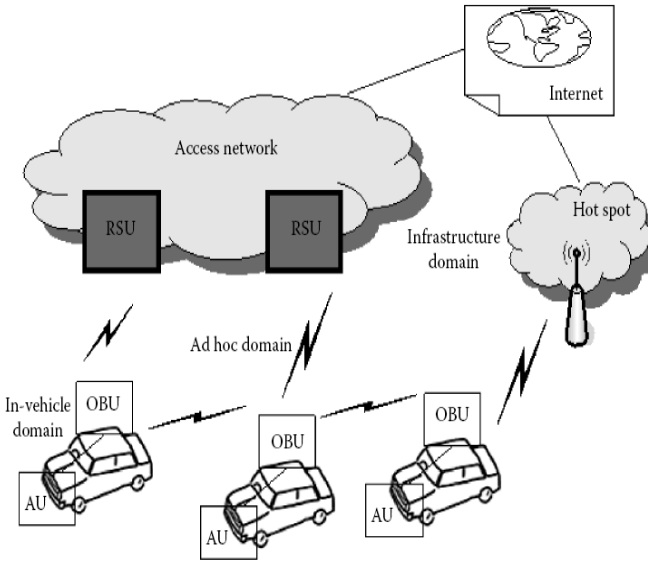

Fig 1: VANET Model

Each vehicle logically composed of two types of units: (i) an on-board unit (OBU) and (ii) one or more application unit(s) (AUs). An OBU is a device in the vehicle having communication capabilities (wireless and/or wired), while an AU is a device executing a single or a set of applications while making use of the OBU's communication capabilities. Indeed, an AU can be an integrated part of a vehicle and be permanently connected to an OBU. It can also be a handy device such as a laptop or PDA that can dynamically attach to an OBU. The AU and OBU are usually connected with a wired connection, while wireless connection is also possible (using, e.g., Bluetooth, WUSB, or UWB). This distinction between AU and OBU is logical, and they can also reside in a single physical unit.

III. ISSUES OF VEHICULAR NETWORKS

VANET faces many attacks and their problem they face; these attacks are discussed in the following subsections:

A. Attacks and Threats

In this paper we are concentrating on attacks perpetrated against the message itself rather than the vehicle, as *Denial of Service, Message Suppression, Fabrication, Alteration, Replay and Sybil, Snoops/Eavesdropper, Industrial Insiders.*

1) Denial of Service Attack: This attack happens when the attacker takes control of a vehicle's resources or jams the communication channel used by the Vehicular Network, so it prevents critical information from arriving. It also increases the danger to the driver, if it has to depend on the application's information. For instance, if a malicious wants to create a massive pile up on the highway, it can make an accident and use the DoS attack to prevent the warning from reaching to the approaching vehicles (e.g. [2], [8], [9], [10]). See fig 2.

2) Message Suppression Attack: An attacker selectively dropping packets from the network, these packets may hold critical information for the receiver, the attacker suppress these packets and can use them again in other time[8]. The goal of such an attacker would be to prevent registration and insurance authorities from learning about collisions involving his vehicle and/or to avoid delivering collision reports to roadside access points [12]. For instance, an attacker may suppress a congestion warning, and use it in another time, so vehicles will not receive the warning and forced to wait in the traffic.

3) Fabrication Attack: 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. This attack includes fabricate messages, warnings, certificates.

4) Alteration Attack: This attack happens when attacker alters an existing data. It includes delaying the transmission of the information, replaying earlier transmission, or altering the actual entry of the data transmitted [8].

5) Replay Attack: This attack happens when an attacker replay the transmission of earlier information can take advantage of the situation of the message at time of sending [8]. It does not contain sequence numbers or timestamps. The goal of such an attack would be to confuse the Authorities.

6) Sybil Attack: This attack happens when an attacker creates a large number of pseudonymous, and claims or acts like it is there is jam ahead, and force them to take alternate route (e.g.[8],[13]) See Fig 3.

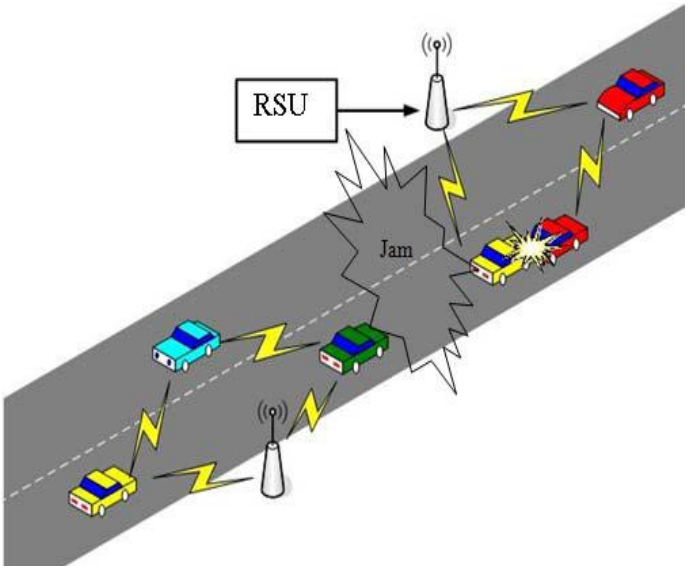

Fig. 2 DoS Attack

7. Snoops/Eavesdropper

In this type of attack people will try to collect information about you. Two types of attacks are done by snoops. First Masquerade 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. Second 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. Thus, vehicles can be tracked and anyone can identify a vehicle's owner. This raises some serious privacy issues as in applications like safety, traffic management.

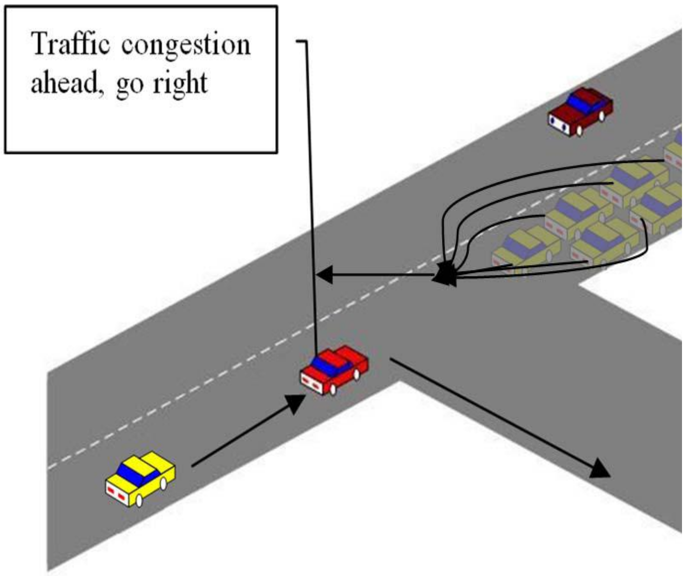

Fig. 3 Sybil Attack

8. Industrial Insiders

Industrial insiders are those who stay inside the car manufacturing company. 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.

B. Adversaries Attacks:

1) Selfish Driver

A Selfish Driver can tell other vehicles that there is congestion in the road, so they must choose alternate route, so the road will be clear for it. See fig 4.

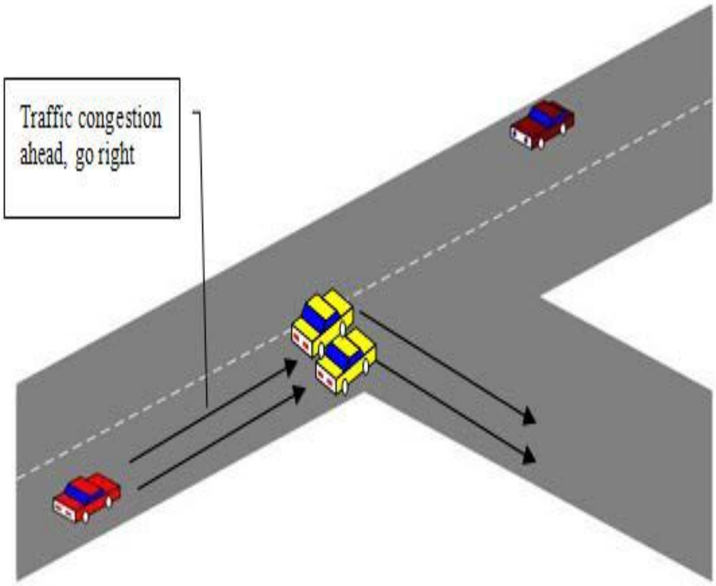

Fig. 4 Selfish Driver

2. 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 [2], [8]

.

3. Pranksters

Include bored people probing for vulnerabilities and hackers seeking to reach fame via their damage [8]. For instance, a prankster can convince one vehicle to slow down, and tell the vehicle behind it to increase the speed.

IV. AUTHENTICATION AND PRIVACY ISSUES IN VANET

In this Section, all possible attacks are investigated on authentication and privacy, and also perform preventive measures.

Attacks on authentication:

The two main attacks related to authentication in VANET are as follows:

1. Impersonation attack: The attacker pretends to be another entity. It can be performed by stealing other entity's credential. As a consequence, some warnings sent to a specific entity would be sent to an undesired one.

2. Sybil attack: The attacker uses different identities at the same time. In this way, e.g., a single attacker could pretend vehicles to report the existence of a false bottleneck in traffic.

Attacks on privacy:

Attacks on privacy over VANET are mainly related to illegally gathering sensitive information about vehicles. As there is a relation between a vehicle and its driver, exposure of vehicle's situation could affect its driver privacy.

1. Identity revealing attack: Getting the owner's identity of a given vehicle could put its privacy at risk. Usually, a vehicle's owner is also its driver, so it would simplify getting personal data about that person.

2. Location tracking attack: The location of a vehicle in a given moment, or the path followed during a period of time is considered as personal data. It allows building that vehicle's profile and, therefore, tracking its driver.

Privacy preservation of vehicular network:

For privacy preservation, pseudonyms of a vehicle are generated instead of the real-world ID in authentication process.

We define the pseudonym of a vehicle as the following form .

PSv^{def}=*RandomNo.*||H(IDv)@HR@RSUC

Where *RandomNo.* is a random number generated by the Pseudo-Random Number Generator (PRNG). H(IDv) is a hash value generated from the vehicle's real-world ID. HR denotes the home region where the entity is registered. RSUC denotes the ID of the current corresponding RSU, where the vehicle generates its new pseudonym for secure authentication and communication.

V. REGIONAL TRUSTED AUTHORITY

RTAs are set in different regions; the region can be a city, a province or a country. Before a vehicle get into the road in a region, the driver first can drive to the RTA for registration. For each vehicle, the RTA publishes the certified domain parameters for authentication on the network.

A. OBJECTIVES OF RTA

The goal is to construct an authentication framework with privacy preservation using ID-based key management for different kinds of communication in VANET. For authentication, the RTA preloads an ID pool of regional RSUs into a vehicle, and the RSU ID pool does not need to update/replenish unless the RSU ID changes or increases. For the vehicle privacy, we utilize a form of self-defined pseudonyms as real-world IDs without exposing privacy. Therefore, a vehicle can change its pseudonym anytime it wants for privacy preservation. The goal of the proposed authentication framework is to guarantee the privacy-preserving authentication in VANET.

The ID-Based Signature (IBS) scheme and the IDBased Online/Offline Signature (IBOOS) scheme are used, for authentication between the Road Side Units (RSUs) and vehicles, as well as authentication among vehicles, respectively. In order to reduce the computational cost in the ID-based Signature (IBS) process for VANETs, the ID-based Online/Offline Signature (IBOOS) scheme is preferable for authentication in VANETs, which is also an attractive solution. An IBOOS scheme [9] increases efficiency of pairing process by separating signing process into an offline phase and an online phase, in which the verification is comparatively more efficient than that of IBS. Therefore, we propose an authentication framework utilizing both the IBS and the IBOOS schemes for better performance. In VANETs, the offline phase can be executed initially at RSUs or vehicles, while the online phase is to be executed in vehicles during V2V communication.

B. RTA STRUCTURE COMPONENTS

A VANET with guaranteed security basically consists of three network components as shown in fig 5 Road Side Units (RSUs), vehicles (users) and a Regional Trusted Authority (RTA). In this VANET consisting of a RTA, finite numbered registered RSUs along roads, and a large number of vehicles on or by the roads, the RSUs are always reliable, while vehicles are vulnerable to being compromised by attackers. The wireless communication in VANET can be classified mainly into three types, V2R communication (R2V) communication, and V2V communication. Other communications are through secure channels, such as inter-RSU communication and RSU-to-RTA communication.

Concerning security issues, there are kinds of attacks which threaten the V2R and V2V communication on the road. All vehicles use symmetric radio channel, and tamper-proof modules (TPMs) are mounted to store sensitive information. The energy of vehicles is adequate and no constrained in a VANET.

The main responsibilities of a RTA are shown as follows

- A RTA generates cryptographic key materials for the RSUs and the vehicles in its region, and delivers these keys to them over secure channels.
- It manages a list of the vehicles of which participations have been revoked, updates the list periodically, and advertises the list to the network to isolate the compromised vehicles.
- If a message sent by a vehicle creates a problem on the road, the RTA is responsible for tracing and identifying the source of the message to resolve the dispute.
- RTAs at different regions have to be cross-certified. Thus vehicles from different regions or different manufacturers can authenticate each other via RTAs.

C. ID-based Signature (IBS)

An IBS scheme consists of four steps including setup, key extraction, signature signing and verification.

• *Setup*: The RTA computes a master key *s* and public Parameters *param* for the Private Key Generator (PKG), and gives *param* to all vehicles.

• *Extraction*: Given an ID string, the algorithm generates a private key sekID associated with the ID using a master key *s*.
• *Signature signing*: Given a message M, time-stamp t and a signing key, the algorithm generates a signature SIG.

• *Verification*: Given the ID, M and SIG, the verification algorithm outputs "accept" if SIG is valid, and outputs "reject" otherwise.

D. ID-based Online/Offline Signature (IBOOS)

An IBOOS scheme consists of five steps including setup, key extraction, offline signing, online signing and verification.

• *Setup*: Same as that in the IBS scheme.

• *Extraction*: Same as that in the IBS scheme.

• *Offline signing*: Given public parameters, the algorithm generates an offline signature SIGoffline.

• *Online signing*: From the input of the private key sekID, the offline signature SIGoffline and a message M, the algorithm generates an online signature SIGonline of M.

• *Verification*: Given ID, M and SIGonline, the verification algorithm outputs "accept" if SIGonline is valid, and outputs "reject" otherwise.

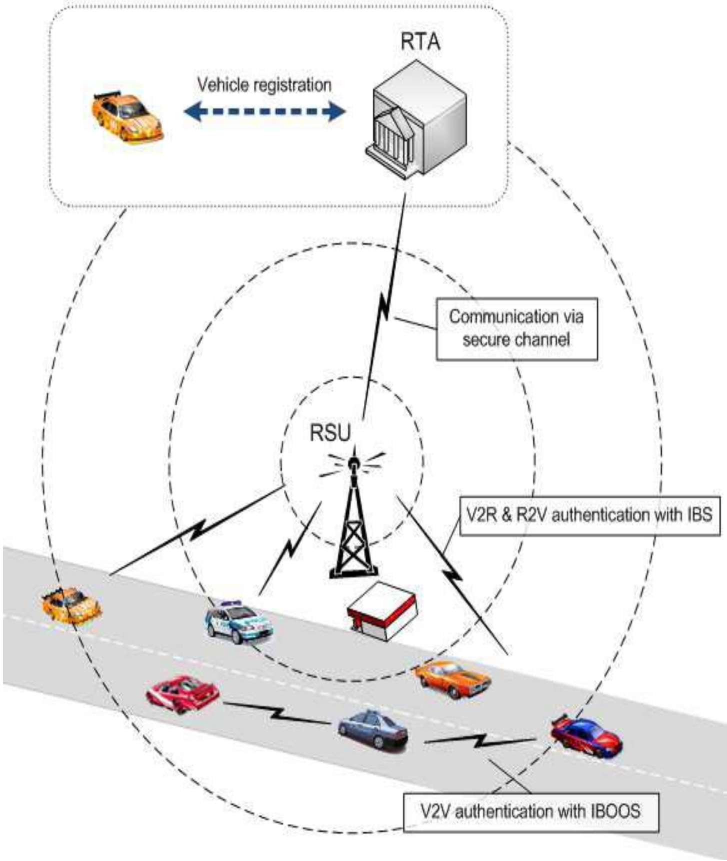
RTA
Vehicle registration
Communication via secure channel
RSU
V2R & R2V authentication with IBS
V2V authentication with IBOOS

Fig 5 Authentication by RTA

VI. CONCLUSION

The principle of VANET's is to ensure the road safety and applications to provide comfort for vehicle drivers. In this way, the vehicles act as communication nodes which exchange data to ensure the collision prevention and accident warning, services providing as traffic information, breakdown and fuel services, office locations. This paper gave a wide analysis for the current threads and solutions, and critic for these solution, we also proposed RTA model to provide authentication for the users using IBS and IBOOS that will help to maintain a secure VANET network.

REFERENCES

[1] http://www.who.int/features/2004/road_safety/en/

[2] M Raya, P Papadimitratos, JP Hubaux, “Securing Vehicular Communications”, IEEE Wireless Communications, Vol13, October 2006 .

[3] R. Lind et al, .The network vehicle.A glimpse into the future of mobile multimedia, IEEE Aerosp. Electron. Syst. Mag., 1999.

[4]GMT Abdalla, SM Senouci “Current Trends in Vehicular Ad Hoc Networks”, Proceedings of UBIROADS workshop, 2007.

[5] Car-to-Car Communications, www.car-2-car.org

[6]H Fussler, S Schnaufer, M Transier , W Effelsberg ,”Vehicular Ad-Hoc Networks: From Vision to Reality and Back”, Proc. Of IEEE Wireless on Demand Network Systems and Services, 2007.

[7] M Raya, D Jungels, P Papadimitratos, I Aad, JP Hubaux,”Certificate Revocation in Vehicular Networks“,Laboratory for computer Communications and Applications (LCA) School of Computer and Communication Sciences ,EPFL, Switzerland, 2006 .

[8] B. Parno and A. Perrig, “Challenges in Securing Vehicular Networks”, Proc. of HotNets-IV, 2005.

[9]I Aad, JP Hubaux, EW Knightly, ”Impact of Denial of Service Attacks on Ad Hoc Networks”, Networking, IEEE/ACM Transactions on Volume 16, August, 2008.

[10]M Raya, J Pierre Hubaux,” The security of VANETs ”Proceedings of the 2nd ACM international workshop on Vehicular adhoc networks, 2005.

[11]M Raya, J Pierre Hubaux, “The Security of Vehicular Ad Hoc Networks “, Proc. of the 3rd ACM workshop on Security of ad hoc and sensor networks, 2005.

[12] Security & Privacy for DSRC-based Automotive Collision Reporting.