# Vehicular Network: Properties, Structure, Challenges, Attacks, Solutions for Improving Scalability and Security

N.Jayalakshmi, R.Rajadurai, K.Indumathi

**Abstract**—VANET is a form of Mobile Ad-Hoc Network or MANET and its different from MANET due to high mobility of nodes and the large scale of networks. The escalating amount of budding applications related to intelligent transportation systems (ITSs) has attracted more number of researchers to the area of vehicular networks (VNs). Some main curriculums of applications have lately gained popularity, i.e., security, scalable, safety, and traffic information and service location applications. In our paper we discussed what the challenges, attacks faced by vehicular networks and we provided solutions for some of the challenges which comprises more important factor. For improving scalability in vehicular network we introduced two sets of protocol (LocVSDPs and GeoVCom) and also suggested a set of resolution to progress the security in VANET.

**Index Terms**— VANET, RTA, LocVSDPs, GeoVCom, scalability, security

## 1 INTRODUCTION

### 1.1. VANET

Vehicular networks are considered as a novel class of wireless networks, it is also considered as one of the ad hoc networks real-life applications. VANET (Vehicular Ad hoc network) provides communications among nearby vehicles as well as between vehicles and nearby fixed road equipment's. Vehicles can be private or belong to an individual or public and provides promising communication to drivers and passengers. 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. VANET provides timely information to drivers and concerned authorities by which it will contribute to safer and more efficient roads. Cooperation among vehicular networks must be introduced into transportation networks to improve overall safety and network efficiency.

### 1.2. VEHICULAR NETWORK ADVANTAGES

Vehicular networks motives to avoid congestion and finds better routes by processing real time data by this it can save time and also fuel by which it results in 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.

- Increase comfort
- Reduce (or avoid) traffic jams
- Relieve driver efforts
- Decrease travel times
- Smooth traffic flow
- Decrease Emissions of CO2, NOX, Noise etc.

### 1.3. FEATURES

Some of the unique features in VANET are

1. **Safety**

Providing safety is the key objective of vehicular communication networks. Vehicles can discover a looming danger and report to others. Electronic sensors in each car can detect rushed changes in path or speed and send an apposite message to neighbors. In more advanced systems, at intersections the system can decide which vehicle has the right to pass first and alert all the drivers. For providing safety in vehicular networks it does a list of following measurements

- Warnings on entering intersections
- Warnings on departing the highways
- Obstacle discovery
- Sudden halts warnings
- Reporting accidents

**2. Traffic management**

Traffic management is consumed by authorities to ease traffic flow and provide a factual time response to congestions. Authorities may change traffic rules according to a specific situation such as hot pursuits and bad weather. Other Applications include

- Variable speed limits
- Adaptable traffic lights
- Automated traffic intersection control

**3. Driver assistance systems**

Roadside units can provide drivers with information which help them in controlling the vehicle. Even in the absence of RSUs, small transmitters may be able to issue warnings such as bridge or tunnel height or gate width. Some of the other applications to driver include

- Parking a vehicle
- Cruise control

**4. Pricing and payments**

Electronic payment results in convenient payments and avoiding congestions caused by toll collection and makes pricing more manageable. For instance tolls can be variable for weekdays and weekends and during rush hours [4]

**5. Direction and route optimization:**

For reaching a destination there are usually many different routes. By collecting relevant information system can find the best paths in terms of travel time, expenses (such as toll and fuel).

Our paper presents in section 2 properties of vehicular network and gave an overview of VANET model, in section 3 we analyzed the various VANET challenges and attacks which should be considered in designing the hardest security problems of VANET and description on LBS, in section 4 we described two protocols (LocVSDPs and GeoVCom) as a solutions for improving the scalability in vehicular networks and in section 5 we discussed the methods to improve the security in vehicular network .Finally suggested RTA model to achieve a secure system in VANET.

## 2. VEHICULAR NETWORK PROPERTIES AND VANET MODEL

**2.1. PROPERTIES:** Vehicular networks have several unambiguous characteristics. Some of their characteristics proscribe the use of current routing protocols.

- 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.
- Partitioned network: Vehicular networks will be frequently partitioned. The dynamic nature of traffic may result in large inter vehicle gaps in sparsely populated scenarios, and hence in several isolated clusters of nodes [4].
- Geographically Constrained Topology*:* Roads will limit the network topology to actually one dimension- the road direction. Even in urban areas, when they are located close to each other, there exist obstacles, such as buildings and advertisement walls, which prevent wireless signals from traveling between roads [5].

### 2.2. VANET STRUCTURE

It is used to represent that vehicular networks provides safety by providing promising communication between vehicles to communicate with each other via Inter-Vehicle Communication (IVC) as well as between roadside base stations via Roadside-to-Vehicle Communication (RVC). Vehicular Ad-hoc Networks are expected to communicate with each other via wireless technologies such as Dedicated Short Range Communications (DSRC) which is a type of Wi-Fi. Other candidate wireless technologies are Cellular, Satellite, and Wi-MAX.RSU (road side base stations are randomly

distributed throughout the vehicular networks and the base stations will communicate with each other by means of communication cable.

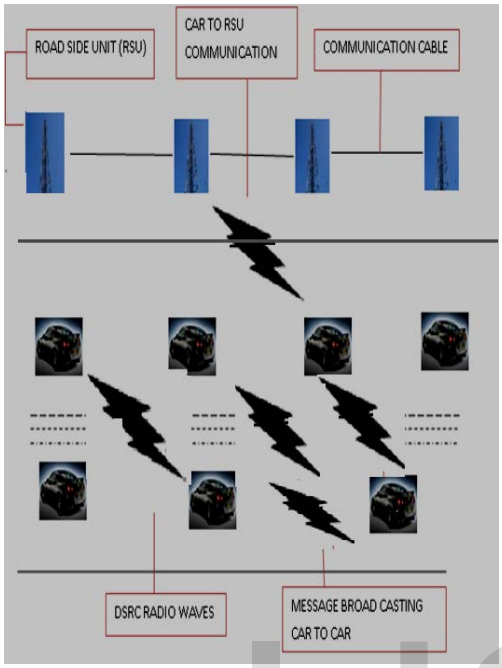


Fig 1: VANET Structure

### 2.3. INTELLIGENT TRANSPORTATION SYSTEMS (ITS)

Vehicular Networks are a cornerstone of the envisioned Intelligent Transportation Systems (ITS). Vehicular Ad-hoc Networks can be viewed as one of the component of the (ITS). Some of the ITS vehicle services are:

- Traffic management
- Public transport management
- Traveler information
- Vehicle safety
- Commercial vehicle operation
- Emergency management

## 3. CHALLENGES,ATTACKS,LOCATION BASED SERVICES

### 3.1. FEW CHALLENGES FACED BY VANET

- Scalable: if number of vehicles on the road side increases

- Interoperatability: it's by the result of different wireless technologies

- Reliable communication: vehicular network provide communication with the help of multi hop transformation of information by which it tremendously extend the network operators from fixed infrastructure to virtual infrastructure as a result of this reliable communication is a major challenge[6].

- Security and privacy: are major concerns in the development and acceptance of services.

### 3.2. THREATS AND ATTACKS

**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. 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.

**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.

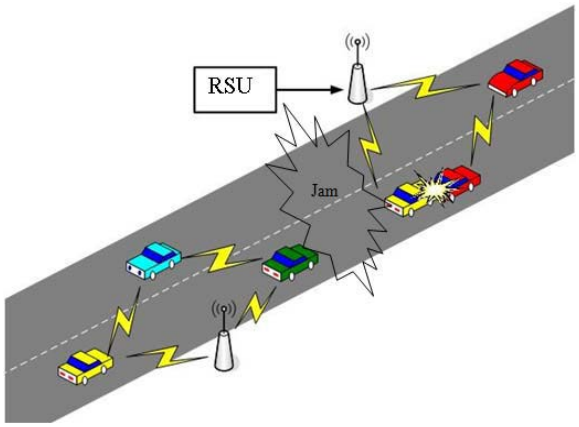


Fig. 2 DoS Attack

**7) Snoops/Eavesdropper:** In this type of attack people will try to collect information about user. 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[10].

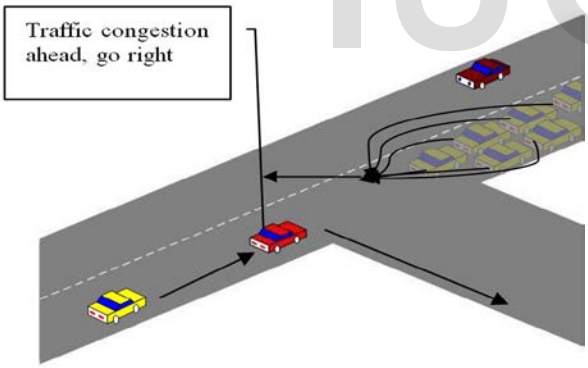


Fig. 3 Sybil Attack

**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 [9].

**9) 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.

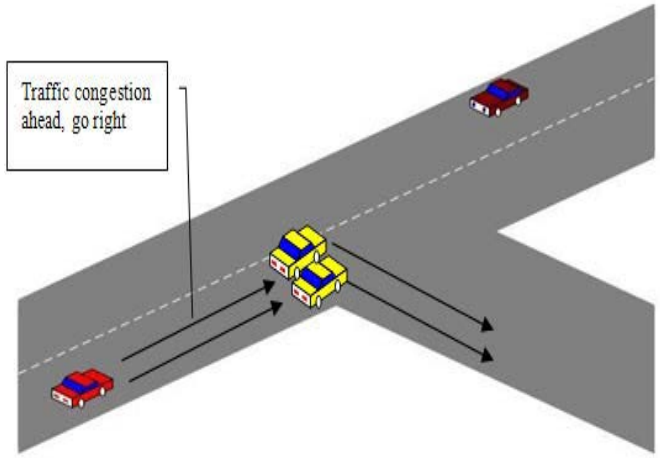


Fig. 4 Selfish Driver

**10) 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]

**11) 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.

### 3.3. LOCATION-BASED SERVICES

Location-Based Services (LBS) is a general class of computer program-level services which include specific reins for location and time data as control features in computer programs and it provides a number of uses in social Networking today as an entertainment service, which is accessible with mobile devices through the mobile network and also used for geographical position of the mobile device. LBS include services to identify a location of a person or object, such as discovering the nearest banking cash machine or about a friend or employee and include other services such as parcel tracking and vehicle tracking. LBS include mobile commerce when taking the form of coupons or advertising directed at customers based on their

current location. They include personalized weather services and even location-based games [1].

LBS are used in location management and it acts as a gateway and mediator between positioning equipment and LBS infrastructure. LBS are responsible for generating client location records and sending them to the Location component. A point of interest (POI) is a location that the user is interested. The point of interest can either be a geographic region or a physical store [11].

## 4. PROTOCOLS FOR IMPROVING SCALABILITY IN VANET

### 4.1. GEOVCOM

GeoVCom balance very well with vehicular solidity. It uses an efficient message suppression technique in impenetrable networks to avoid redundant transmissions from close by nodes. It provides reliability even in sparse networks by choosing appropriate nodes to forward packets and works well in high mobility. GeoVCom is stateless and does not maintain states like neighbor table, routing information. GeoVCom does not require conventional network coverage. It can work even in rural areas with deficiency in WAN cellular coverage [12]. A primary benefit of GeoVCom is that it can operate without relying on the WAN altogether, thereby avoiding overstrain of the WAN resources. GeoVCom entail no connections to preset infrastructure nodes, servers in the Internet.

GeoVCom uses a scalable ad hoc geocast protocol (SAGP) defined by Hall [7]. SAGP is a topology-free scalable geographic routing protocol, running over an ad hoc 802.11 network between mobile devices. When a geocast packet is instigated by a SAGP enabled device, it is assigned an unique identifier which works globally. The originator then uses a trouble-free broadcast to convey the geocast packet, with the packet header which includes originator location, destination region as well as other fields to be described. Each SAGP device hearing a broadcast geocast packet enqueues the packet for retransmission after a pseudo random undulating back off time. The rationale of this delay is to desynchronize retransmissions among peer devices. When the back off delay expires, the device applies a set of heuristics to decide whether to cancel retransmission or to go ahead and forward the packet[14].

### 4.2. LOCATION BASED VEHICULAR SERVICE DISCOVERY PROTOCOL DESCRIPTION

The LocVSDPs (location based vehicular service discovery protocol) infrastructure relies on clusters of wireless roadside routers (RRs) which are randomly distributed in the vehicular network. The allocation of clusters mainly depends on the application requirements in the VANET. Clusters of RRs are primarily formed around and near the service providers to manage service queries when there is increase in the number of service request. LocVSDPs provides a scalable scaffold for the breakthrough of time-sensitive and location-based services in VANET[14]. This LocVSDPs protocol will help drivers and passengers to find the services, such as restaurant menus or gas station, by specifying their location of desired region called as region of interest (RI). The LocVSDPs find services located in the RI specified in the driver's or passenger's request using efficient location based propagation of the request and efficient computation of the reply.

LocVSDPs protocols rely on a cluster-based infrastructure where clusters may possibly form near service providers, or in congested areas (more number of service request). The cluster-based infrastructure will efficiently provides management of service queries and also guarantees network connectivity. LocVSDPs simultaneously find the service provider and its routing in sequence, which fallout on the whole of savings in usage of bandwidth. The protocol tenacity make use of different channels (for exchanging discovery information and routing information) which resulting in an efficient tradition of the radio spectrum and also provides lessening in the impediment of service queries. The random distribution of RRs around the known service providers will prevent traffic jam when many service requests are directed to the same RI. This protocol can be processed even if new and unknown service providers are introduced into the VANET. RRs are randomly distributed around intermittent areas in the VANET to enable consistent connection among VANET. RRs which are communication range to each other will form a cluster. The total numbers of RRs used in VANET are nRR.

**SERVICES PROVIDED BY LOCVSDPS**

Some of the services provided by location based vehicular service discovery protocol are:

1) Fixed services have a predetermined location, and their position does not change over time. Examples of services could be restaurants menus, gas station prices, and available parking spots.

2) Moving services are the services provided by the vehicles on roads. The location of these services depends on the

location of the moving vehicle. Examples of services in this category could be music sharing, game sharing, or file sharing.

3) Migratory services have a fixed location, but they are provided by moving vehicles. When vehicles are moving around the fixed location, they provide the service; when they are far from the fixed location, the service migrates to provider vehicles close to the fixed location. Examples of services in this category could be sightseeing, traffic condition monitoring, or accident or disaster monitoring.

## 5. PROPOSED SOLUTIONS TO IMPROVE SECURITY IN VANET

In VANET many security solutions have been proposed, and large number of papers is introduced to solve the security related problems. In our paper we suggested few solutions for improving security.

### 5.1. VPKI (Vehicular Public Key Infrastructure)

In VPKI each node will have a public/private key. When a vehicle sends a safety message, it signs it with its own private key and adds the **Certificate authority (CA's**) certificate. The receivers of the message will obtain the public key of V using the certificate and then verify V's signature using its certified public key. In order to do this, the receiver should have the public key of the CA [11]; this solution is cited in [4], [8], [15], and [16]. That CA should handle all the operations of certificate: generating, renewing and revoking, and CA must be responsible in initiating keys, storing, managing and broadcasting the CRL.

Using VPKI in VANET accompanied with some challenges, like certificate of an attacker that must be revoked, authors in[2] discussed the Certificate Revocation solution, this solution is used to revoke the expired certificate to make other vehicles aware of their invalidity[17],[18]. The most common way to revoke certificates is the distribution of CRLs (Certificate Revocation Lists) that contains all revoked certificates, but this technique has some negative aspect: First, CRLs can be very long due to the huge number of vehicles and their high mobility. Second, the short lifetime of certificates still creates a openness window, and there is no infrastructure for the CRL. Authors in [2] mentioned a solution that will help to maintain the privacy by using a set of anonymous keys that change usually (every couple of minutes) according to the driving speed. Each key can be used only once and expires after its usage; only one key can be used at a time. These keys are preloaded in the vehicle's TPD for a long duration; each key is certified by the issuing CA and has a short lifetime, drawback of this solution is that the keys need storage[19].

### 5.2. GROUP SIGNATURE

Authors in [17] suggested an idea of using the group signature, but this idea has a major drawback because it is causing a great transparency, every time that any vehicle enters the group area, the group public key and the vehicle session key for each vehicle that belongs to the group must be changed and transmitted, another issue must be considered that the mobility of the VANET prevents the network from making a static group, so the group is changing all the time, and the signatures and keys are frequently changed and transmitted. After 9 ms for group signature verification delay, the average message loss ratio was 45%, another result was the loss ratio reaches as high as 68% when the traffic load is 150 vehicles.

### 5.3. REGIONAL TRUSTED AUTHORITY (RTA)

VANET consisting of a RTA, finite numbered registered RSUs along roads, and a large number of vehicles on or by the roads. RSUs are always reliable, while vehicles are vulnerable to being compromised by attackers [13].

Vehicles when entering the vehicular network have to register with Regional trusted authority. For each vehicle, the RTA publishes the certified domain parameters for authentication. The wireless communication in VANETs can be classified mainly into three types, Vehicle-to-Roadside (V2R) communication, Roadside-to-Vehicle (R2V) communication, and Vehicle-to- Vehicle (V2V) communication. Other communications are through secure channels, such as inter-RSU communication and RSU-to-RTA communication. The transmission range of an RSU is assumed to be much longer than that of vehicles. 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.

**WORKING OF RTA:**

- 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.

manufacturers can authenticate each other via RTAs.

VANET architecture with guaranteed security will basically consists of three components as shown in Fig 5: Road Side Units (RSUs), vehicles (users) and a Regional Trusted Authority (RTA).

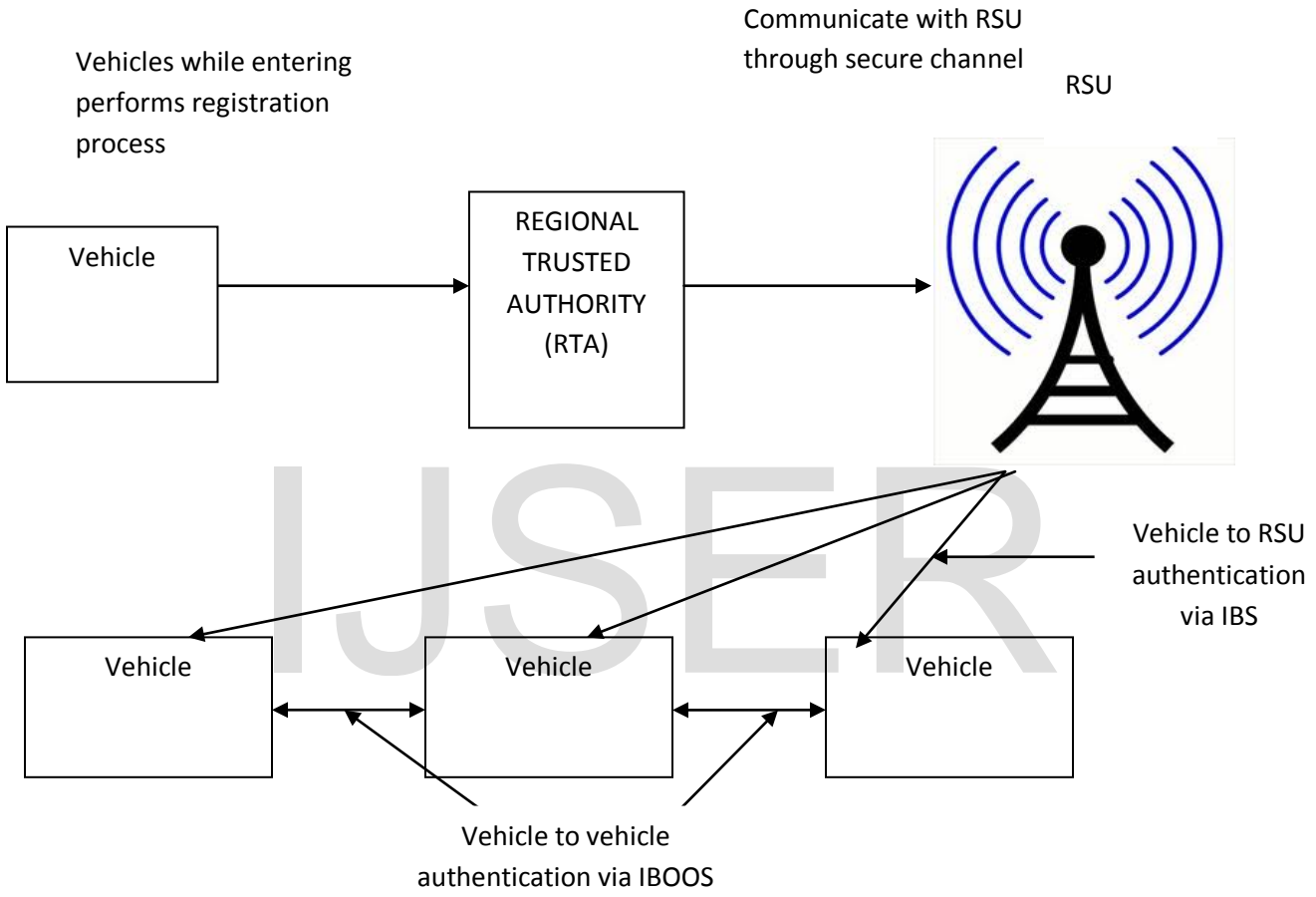


Fig 5: BLOCK DIAGRAM OF VANET WITH RTA

- RTAs at different regions have to be cross-certified. Thus vehicles from different regions or different

## 6. CONCLUSION:

The principle of VANET's is to ensure the road safety and applications are used to provide comfort for vehicle drivers. In this way, the vehicle act as communication nodes which exchange data to ensure the collision prevention and accident warning, and provides services such as traffic information, breakdown, fuel services, office locations. Through this paper we made a wide analysis on the VANET characteristics, structure, and described various attacks which VANET faces. We also discussed some of the protocols which is used for improving the scalability in VANET and suggested set of solutions useful for providing security by making use of VPKI, Group Signature, Regional trusted authority.

## 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.

[13] Huang Lu and Jie Li, Mohsen Guizani, "A Novel ID-based Authentication Framework with Adaptive Privacy Preservation for VANETs",IEEE transactions 2012.

[14] F. Karnadi, Z. Mo, "Rapid Generation of Realistic Mobility Models for VANET ", proc. IEEE Wireless Communications and Networking Conference, 2007.

[15] 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.

[16] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and JP Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks ",IEEE Magazine, vol. 10, October 2007.

[17] W Ren, K Ren, W Lou, Y Zhang,"Efficient user revocation for privacy-aware PKI", - Proceedings of the 5th International ICST Conference, 2008.

[18] 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.

[19] R Lu, X Lin, H Zhu, PH Ho, X Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular", In proceeding The 27th Conference on Computer Communications, INFOCOM 2008