International Journal of Engineering Research & Management Technology

May- 2015 Volume 2, Issue-3

Email: editor@ijermt.org www.ijermt.org

"Sharpening Skills..... Serving Nation"

User Privacy ISP Using VANET

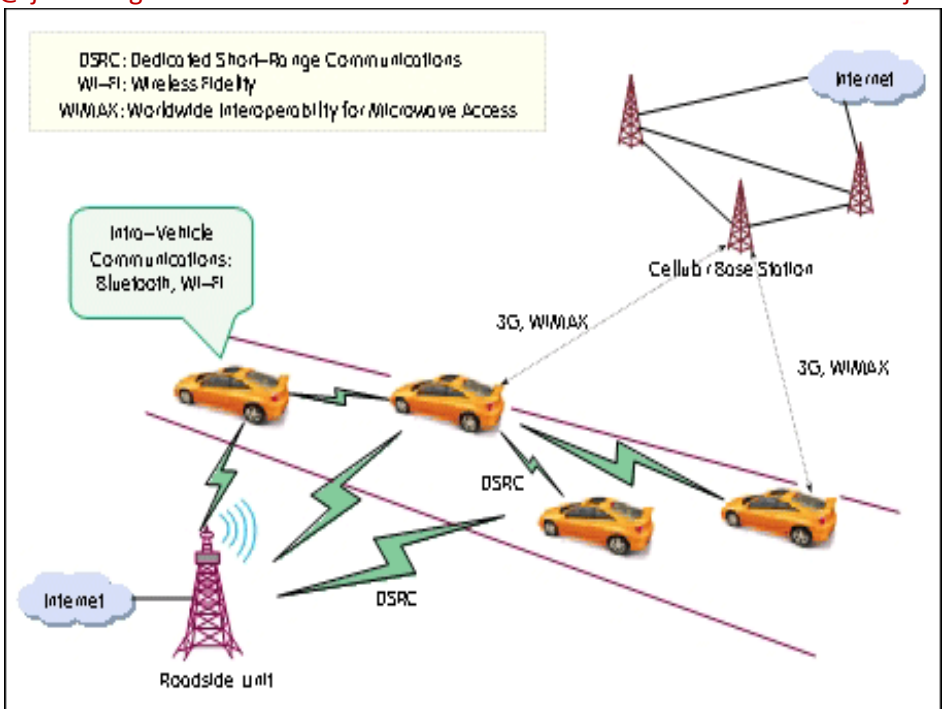
Shipra Saini[1], Rashmi[1], Ritu Chaudhary[1], Saurabh Kumar Gaur[2]
B.Tech Student [1], Assistant Professor[2]
Department of CSE
Lord Krishna College of Engineering, Ghaziabad

ABSTRACT:
The present perspective of time needs to be more modernized using advanced technologies in transportation system because of increasing mishaps and for better management of traffic jams as well.
We can incorporate the use of internet, which is widespread now-a-day, in the vehicles as Vehicular ad hoc Network(VANET).VANET can offer better services for the people as it is specially made for the road transport system. But the most important thing which is to be taken into mind is maintaining user's privacy like misuse and attacks on user's data. So, it is a vital necessity for applying strict security measures. In our paper, we are trying to maintain user's privacy using ISP (Independent Security Pattern) using VANETs. This will lead to achieve user's privacy as well as traceability required by law enforcement authorities. We propose a system under which vehicles may have obstacle detecting sensors and network amplifying devices so that risk of accidents could be reduced. We present user privacy ISP preserving defence network authorities to handle misbehaviour in VANET access. Our system aims to employ an identity based crypto-system where certificates are not compulsorily needed for authentication.

INTRODUCTION:
A **vehicular ad hoc network** (**VANET**) uses cars as mobile nodes in a MANET to create a mobile network. The intent of VANET is to make a system such that every participating car into a wireless router or node, that allows cars approximately 100 to 300 metres of each other to connect and, in turn, a network with a wide range is created. As a car falls out of the signal range and drop out of the network, other cars can join in, that connects vehicles to one another that create a mobile internet.
Safety and security service providers like police, fire brigades and ambulances etc are needed to be first added to this technology. Various reputed automotive companies are interested to implement VANET.
The movement of nodes (ie cars) in vanet system is confined by traffic laws.Machines cannot break laws while those of humans do most commonly.Therefore there will be lesser chances of accidents due to human faults because machines will work as per human instructions. As per as instructions and protocols are followed correctly the system will work perfectly.

ARCHITECTURE:
VANETs are the subclass of MANETs (Mobile ad hoc networks) since the vehicles implementing this trade will be in dynamic mode. The system is supposed to have 3 kinds of connection facilities:
1. V2Vi.e interconnection in between the vehicles running on road.
Vehicle-to-vehicle (V2V) communication can provide a data exchange
Structure for the drivers to share information and warning messages in order to increase driver's ease
The connection V2V involves a large number of privacy issues as we can not make the entire information of some vehicle public.

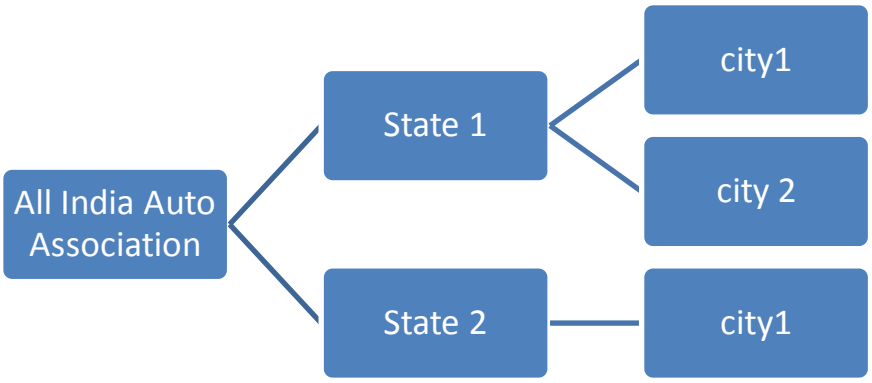
2. V2I I.E CONNECTION BETWEEN THE VEHICLES AND THE ROAD INFRASTRUCTURE:
Vehicle-to-road infrastructure (V2I) communication is one of the interestingfield in VANETs. V2I communication enables real-time traffic/weather updates for drivers and provides environmental sensing and monitoring.



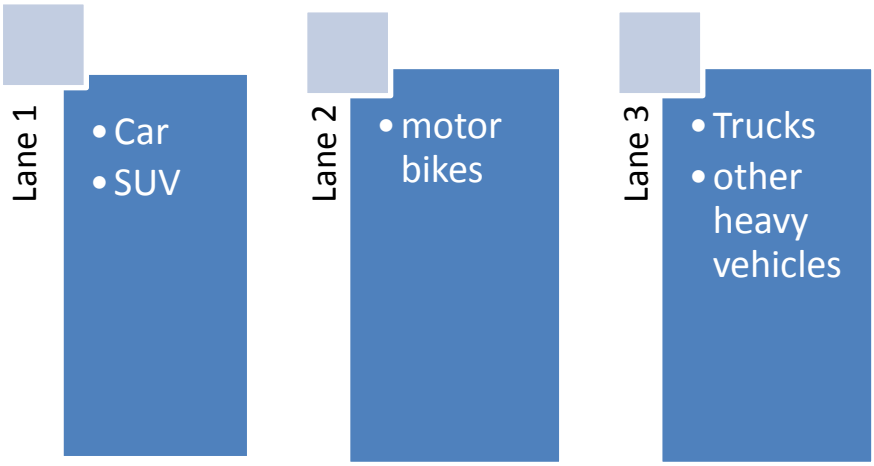
3. V2B I.E CONNECTION BETWEEN THE VEHICLES AND THE MOBILE BROADBAND CONNECTION:

Vehicle-to-broadband cloud (V2B) communication means that vehicles may communicate via wireless broadband mechanisms such as 3G/4G. As the broadband network can have more traffic information and monitoring data as well as assistance manuals and guide, this type of communication will be useful for active driver assistance and vehicle tracking.

A solution for un-authorisation could be a hierarchical grouping of vehicles. Such systems could be possibly the various transport associations. Like-



1. This system will be helpful to enquire the guilty/victim vehicle in case of any mishap.
2. The hierarchical grouping will maintain privacy in order such that if some crime is committed and we have to find the guilty/suspect/victim then, firstly the enquiry will be done at the city level, then at state level followed by national level. In this way, authentication at different levels could be maintained.
3. The automotive companies by themselves can allot some specific number for revealing the vehicle's id and only authorised people like the owner and the police should know this while investigating. Another way to increase the safety of pedestrians, heavy vehicles and light vehicles is to adopt a LANE system, in which each kind of vehicle will have its own separate lane.



Emergency vehicles such as ambulances, police vans and fire brigades etc would have another separate lane and they should be allowed to move always smoothly keeping other vehicles paused for small interval if necessary.
There should be frequent transmission of messages and warnings while intersection traversing and lane merging.

MECHANISM:
Since the MANET provides network for smooth and continuous devices, it is not applicable for vehicular activities which involve frequent pauses and resumes. Vanets should use specific routing so that proper connectivity could be provided among the vehicles, road infrastructure, and the network operators.
VANET offers its special features such as:

1. High mobility:
The nodes implementing vanet are highly mobile and they can have frequent pause and resume and can have very high speeds too.
2. Dynamic Network topology:
The network topology of vanet changes in very short period of times.
3. Wide Network Range
A large number of vehicles at very distant places can be needed to connect.
It can involve a city, a state and a nation also.
4. Fast message service
The messages transmission in vanetamong the vehicles,road and the service providers is supposed to be smooth and fast enough to take the action at time.
5. Help and support by infrastructure
Vanets can take support from road infrastructure , while Manets cannot do this. This will enhance safety of vehicles on road as it is very helpful to make better policies and protocols.
6. Easy and ample resources
Vanet nodes are characterised by high energy and analytical resources.
7. Physical security
Vanets are less compromise-able therefore security threats are treated well.

GPS SYSTEM:
Implementing GPS (Global Positioning System) will help to locate the vehicles while they are moving. The GPS navigation devices can be used detect the nodes at real time.They are used to analyse geographical locations and weather informationas well by receiving information from GPS satellites. GPS fed directions directly to an independent vehicle. When DSRC (Dedicated Short Range Communication) is adopted in combination with GPS technology, it results into a low cost but highly beneficial scheme.GPS technology can analyse the speed and acceleration of the vehicle. It can also track the vehicle control system as well like its

transmission state, break states, steering wheel angle, path history and path prediction as well.GPS can be integrated with traffic reports to provide an optimal route to travel.

ROUTING IN THE EXISTING SYSTEM:

There can be three kinds of routing systems for implementing VANET:

Broadcasting/Geo-casting

Since the vehicles always move in unspecified directions and we need to distribute the unknown/unspecified destinations, there should be protocols based on geo-casting/broadcasting so that message service could be frequent.

There can be single-hop wireless systems (vehicles to base-stations) and multi-hop wireless systems (i.e inter-vehicle communication). Broadcasting provides better solution because of their low cost and tendency to spread data at high rate and large amount.

MULTICASTING:

Multi-casting is necessary for group communications in emergency and critical situations like accidents, road blockage, high traffic density etc.There are two types of approaches in which multicasting can be implemented:

One is location based approach and the second approach is toplogy based.

UNICASTING:

There are three kinds of unicast protocols:

1.Greedy-The first one is greedy approach-the data packets are sent to the most distant neighbour nodes such as improved greedy traffic-aware routing(Gytar).

2.opportunistic-The data is forward when it is needed by some node. We can also use some kind of device in the vehicle that can amplify the network waves when it moves away from the broadcast server(ie network becomes slow). This will help to decrease the congestion ,traffic jams as well as help to run the entire transportation system smoothly.

3.Flight /trajectory based-Optimal route is selected to transfer data within nodes so that faster service could be made. It uses various shortest path algorithms.

PROPOSED SYSTEM:

There can be several kinds of models that can be used to apply VANETs practically:

DRIVER AND VEHICLE MODEL:

This model is applicable to evaluate single vehicle characteristics only. There can be different kinds of drivers driving in different types of cars. Such as a F1 car racer will move its car very swiftly whereas an ordinary car driver will drive his car very safely.

TRAFFIC FLOW MODEL:

There can be three kinds of traffic flow model: microscopic, mesoscopicand macroscopic. The main objective of this model is to study the interaction between vehicles, drivers and infrastructures and create efficient and best road network.

COMMUNICATION MODEL:

This model plays an important part in research in VANET technology since it should entertain the privacy issues in a healthy manner. It should help to create communication such that only handful knowledge is available to the neighbouring node. The aim of this model is to maintain interaction between nodes such that un-authentication is avoided.

APPLICATION MODEL:

The behaviour and quality of cooperating VANETs is analysed under this head. It is useful for market introduction.

There are two causes for implementing this model:

8. Difference in visualisations and activities of the vehicles manufactured by different automobile companies.
9. Priority of transmitting information and warning messages.

SIMULATION METHODS:

Simulation is very necessary for implementing the VANET technique because it will help to understand and apply the system efficiently. There are two kinds of simulators which must be used:

TRAFFIC SIMULATORS

Traffic simulators are used to evaluate position and movement information of some vehicle in Vanet. Examples of some existing simulators are SUMO (simulation of urban mobility) and VISSIM (simulation of the position and movement for vehicles as well as city and highway traffic).

NETWORK SIMULATORS:

Network simulators are helpful to model and analyse the working of VANETs. These are responsible for creating the best routes, and deliver messages as fast as possible. Some of the desirable characteristics of network simulators are comprehensive mode, efficient routing protocols like AODV (ad hoc on demand distancevector), and communication standards like IEEE 802.11[p] and IEEE 1609 specifications.

Challenges and their proposed solutions

Authentication based privacy issues are resolved under this head. The v2v connection can have a large number of privacy concerns. Since it is the layer of the network on which the researchers have to work the most.

PSEUDONYM GENERATION AND AUTHENTICATION FOR PRIVACY:

RTA and border RSUs are making progress in this phase to assign pseudonym/private key pairs to both vehicles traveling in their home region and vehicles from other RTAs' domains in order to authenticate with RSUs and other vehicles to achieve services and useful messages.

THRESHOLD SIGNATURE FOR NONFRAMEABILITY:

This process is used to share the secret or private information for revealing a guilty vehicle's identity. Apart from it, it also prevents corrupted authorities from accessing full power to accuse some vehicle. The working part of this procedure is the threshold.

THRESHOLD-AUTHENTICATION-BASED DEFENSE:

It is specially designed for the network authorities. This procedure is used to obtain a misbehaving vehicle's document and restricting the vehicle from interfering the system more. The threshold authentication technique provides a mechanism to allow some particular types of misbehavior that should not occur in repetition. For example, the misbehavior may be caused by malfunctioning hardware which can create mishaps. The occurrence or frequency of these misbehaviors is low, typically, lower than a predetermined threshold.

MEMBERSHIP REGISTRATION:

RSUs and vehicle users need to register with the RTA to use VANETs. A member public/private key pair (mpk; msk) is issued to each RSU and vehicles. The members' documents with the issued public key and includes the pair of information into a credential list IDlist.

ACCESS GROUP SETUP:

RSUs and vehicles can maintain their own access groups, the member of which is granted privilege to communicate with the access group owner. The group owner adds members to the group and updates related public information. Every member will have its own acces key provided by the group head.

ACCESS GROUP REVOKING:

The access group own can take back the privileges of some vehicle if some kind of misconduct and misbehavior is found. The access group owner can delete the member from the access group and updates related public information.

THRESHOLD AUTHENTICATION:

This process is held between an RSU and a vehicle, or between neighboring vehicles. The authentication process is successful if and only if the following conditions are met :

Some user A authenticating with another user which is a registered member of the VANET system, the user A is a legitimate member of the same access group (if the peer is not an access group owner) whose member privilege has not been taken back, and the authentication threshold has not been exceeded.

TRACING:

Any group member can analyse the activities of the same access group member. Thereafter he can inform the group head to take the decision for the misconducting vehicle.

REVOCATION/RECOVERY:

The decision made by the authorities is passed to the member and it is deprived of the credentials for driving on road or given some kind of warning and asking for heavy penalties.

CONCLUSION:

The proposed User Security ISP(Internet Security Pattern) using VANET focuses towards safe transportation system as its main concern is towards how to disable some user to crack the information of other vehicle so that no one can make misuse of it. The functionalities are understood by the pseudonym-based techniques, the threshold signature, and the threshold authentication based defense scheme. security and efficiency analysis of our system facilitate to contentthesecurity concerns and desired automotive properties. We will be focusing toward the more reliable settings for user in vanets in future.

REFERENCES:

1. Z. Li, Z. Wang, and C. Chigan, “Security of Vehicular Ad Hoc Networks in Intelligent Transportation Systems,” in Wireless Technologies for Intelligent Transportation Systems, Nova Science Publishers, 2009 (in press)
2. Vehicular ad-hoc Network: Wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/VANET
3. International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013 279 VANET System for Vehicular Security Applications Saurabh Kumar Gaur, S.K.Tyagi, Pushpender Singh
4. A. Stampoulis and Z. Chai, “A survey of security in vehicular networks.
5. Secure VEhicular COMmunications,”http://www.sevecom.org/.
6. Enhancing location privacy in wireless lan through disposable interface identifiers- a quantitative analysis,” pp. 315–325, 2005.
7. K. Lee, S.-H. Lee, R. Cheung, U. Lee, and M. Gerla, “First experience with cartorrent in a real vehicular ad hoc network testbed,” in 2007 Mobile Networking for Vehicular Environments, 2007, pp. 109–114.
8. Noncoperative Content Distribution In Mobile Infostations Networks- wing Ho, Yuen Roy D.Yates Siun-chuon Mau
9. Comparative Study of Data Dissemination Models of VANETs” Praveen Shankar, LIftode, Mobiquitous 2006.
10. M. Raya, P. Papadimitratos, and J.-P. Hubaux, “Securing vehicular communications.” [11] http://en.wikipedia.org/wiki/Intelligent_vehicular_ad-hoc_network [12] Rosslin Robles and Maricel O. Balitanas,” A Review on Strategies to Optimize and Enhance the performance of WLAN and Wireless Networks” , IJMUE/vol2_no2_2007.
11. en.wikipedia.org/wiki/Intelligent_vehicular_ad-hoc_network