VANET- based Vehicle Tacking on Message Authentication and Secure Navigation Route

T.S Vamsi Krishna
Student,
Dept. of Information Technology,
Vel Tech
Dr. RR and Dr. SR Technical University

R. Hariharan
M.Tech
Assistant Professor,
Dept. of Information Technology,
Vel Tech
Dr. RR and Dr. SR Technical University

ABSTRACT
Computing real-time road condition is really tough and it is not achieved using GPS. However, a malicious node can create multiple virtual identities for transmitting fake messages using different forged positions. A malicious vehicle can disseminate false traffic information in order to force other vehicles and vehicular authorities to take incorrect decisions.To overcome these difficulties we propose that vehicle should be authenticated by Trusted Authority (TA) via RSU, only then the navigation query sent to RSU through tamper proof device (in the Vehicle) for identifying best destination route. After authentication, TA generates a re-encryption key to requested vehicle for encrypting the query. Based on vehicle request, contacted RSU identifies the shortest path to reach the destination RSU by passing the vehicle request to neighbouring RSU's. After identification of shortest path, it sends the encrypted message to requested vehicle using re-encryption key. Finally it decrypts the message using its own private key. Moreover, the network checks each vehicle speed for avoid accident based on predecessor and successor vehicle's speed using chord algorithm. It also implementing priority based vehicle movement so, Network gives high priority in emergency vehicle, it gives medium priority for registered vehicle and it gives low priority for unregistered vehicle.

Keywords
DSRC protocol, V2V communications, V2I communications, Traffic security, MChord, Message Authentication, VANET, Beaconing, P2P network transmissions.

1. INTRODUCTION
Every user has a common experience to find a correct route of certain destination. In past days, a user usually refers to a hard copy of map. After the introduction of Global Positioning System (GPS), GPS-based navigation systems becoming popular for example in such systems a tiny proof of device is installed into an vehicle. The receiving of GPS signals will capable to find its current location and it shows the geographically shortest route for certain destination based on a local map. However, the route finding event of these system is based on a local map and real-time road conditions will not taken into account. To learn about real-time road conditions, a user will transform the message to know about another system named Traffic Message Channel (TMC) as shown in fig: 1, which has been adopted in a number of developed countries. TMC is a specific application makes use of the FM Radio Data System (RDS) used for Broadcasting real-time traffic and weather information to drivers.

Data messages are received silently though Special equipment is required to decode or to filter the information received. However, only special road conditions (e.g., severe traffic accident) are broadcasted and a driver cannot obtain information like the general fluency of a road from TMC. Recently, vehicular ad hoc network (VANET) becomes increasingly popular in many countries.

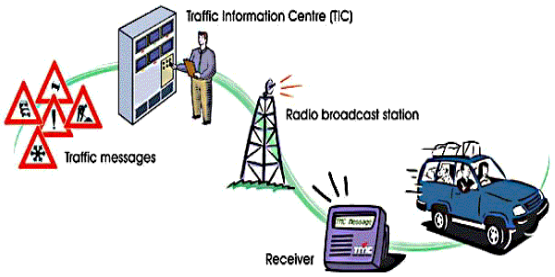

Fig: 1 Traffic Message Channel (TMC)

In VANETs each vehicle will connected through an ad hoc formation in a wireless network. The vehicle can follow a subgroup of mobile ad hoc networks (MANETs). It includes vehicle to vehicle communications (V2VC), vehicle to infrastructure communications (V2IC), and important system element named as Intelligent Transportation Systems (ITSs). In a typical system, each vehicle will attach a onboard units (OBU) through along its road-side units (RSU) was installed in the roads. A Trusted Authority (TA) and some other application servers also installed at the same time. The communication between onboard unit and road-side unit has prescribe to follow a Dedicated Short Range Communications (DSRC) protocol, over the wireless channel and through communication is fixed in each secure network to transform along RSU, TA and other application server (e.g., the internet). The North American DSRC standard produces a IEEE 802.11p, since each node will produce intent communication in wireless networks.

The basic application of VANET is to allow arbitrary vehicles to broadcast safety messages (e.g., vehicle's speed, vehicle's direction and vehicle's accident information) will transmitted to other neighbour vehicles (represented as vehicle-to-vehicle or V2V communications) and also to RSU (represented as vehicle-to-infrastructure or V2I communications). The other vehicles will regularly divert their travelling routes at the time neighbour RSUs transmit their information to traffic control centre to adjust the traffic signals in order to avoid the vehicles collision. During, a VANET also reputed to its sensor network because of base station service centre will capable to transmit all the useful information to traffic control centre or some other central servers to know about its present road condition. But before introducing of VANET some problems

has occurs based on increase traveller safety by 10.8 million vehicle crashes from 1990 to 2009. Over 36000 fatalities have marked negative repetition; due to vehicle's crash to other objects also cost exceeds more than $100 billion per year. But now-a-days it is natural to investigate how to utilize the collected real-time road conditions to provide useful applications using of VANET.

2. RELATED WORK

In order to identify related issues regarding for security and privacy faced by different challenges in VANETs, but to claim in public key infrastructure (PKI) should be deploy to protect the transited messages and mutually authenticate among each network entities. The spreading process of classical PKI certificate will transmit only secure network communications to VANET. In this approach, vehicle must be pre-load a reasonable memory space to each anonymous package certificates. Although, long period of time allocate to package certificate will load the information to complete transmission to each vehicle's security purposes, e.g., a year. Each vehicle can update its certificate package through trusted authority only because TA act as a central servers to intercept transmit in tiny device by vehicle's annual inspection. The certificate package will increase vehicle incurs inefficiency for every certificate management as revoking one vehicle implies revoking the huge numbers of certificates are loaded. The trusted authority will reduce the time limit by working contribution for CRL size is decreased to check the revocation status takes a long period. Since overheads in message authentication and communication network will suffer whole period of delay contention. The batch verification and certificate packages has reached successfully, by RSU to increase sufficient time limit and stores maximum memory space to reduce the delay and whole system transmit through secured manner.

The present development of vehicular communication technology, which combines a standard of IEEE 802.11p will exist the adaptive technology that progressed to upstream direction. The vehicular communication i.e. without road-side access points will remove minimum market penetration to achieve each vehicle's communication. The pair in commercial loop will reach at its best initial roll-outs region. In order to installed road side infrastructure to accelerate revenue investment to every RSU, but it must fixed through neighbour's vehicle transmission. This kind of communication must have a major reason to invest for installation; cost and maintenance to act as a successful transmit of each obstacle. In road-side towers, neighbour RSU will contact to exchange the secure information between each vehicle and reduce the collision among them using wireless sensors. The WSNs is a cost effective device to solve and creating an addition element will subject to produce energy and processing its constraints. In WSN would fed to contribute of each road side, road surface and boundaries (curves, tunnels and bridges), even extent up to much wider scale. The physical mixture to vehicle sensor node proceeds in periodic level of temperature, humidity, light and other track movements. The representation of hybrid architecture that combine both of vehicle-to-vehicle Communication and vehicle-to-roadside sensor communication. The fixed position of each road side sensor node will generate high premises of signal, to transmit high speed of data in each surface transfer to aggregate its corresponding value.

The Regional Authority (RA) is a part of traditional Elliptic Curve Digital Signature Algorithm (ECDSA) related to PKI certificate contribution, where RAs certificate will identify original RSU to transmit its desire location or online transmission of signal from one region to other. Though, VANET provide better security that will give high performance to PKI certification. In this work, RA act as regional certify to transform each authority nodes to link with OBU and signed certificates, which will identify its current location and return back to RAs position. Finally road authorities signed by PKIs certificate to find a proper position of RSU or to identify the public key of each RA will generate its own key through online extent. The hard mode of maps is similar (current location of GPS navigation systems) to contact its OBUs each boundaries has to include Meta data of about each signal distribution to an appropriate region for RA (via VANET communication for RSU or URL for online RAs). OBU can periodically (e.g., weekly) download for signed Certificate Revocation Lists (CRLs) using these region which as no longer for valid RAs. The OBU is relatively slow processor to assume its proper contribution that helps to reduce the cost of vehicle. In comparison, RAs have more computational resources. The positive intensive operation (such as OBU revocation in each sets of TACKs) should be offloaded to RAs. The control messages are different varieties using in digital signature. The message is signed only by a valuable depended digital signature, each message will additionally transform in secret public key has to signed with authorization. The complete message has defined hash function to generate either a smaller, fixed size or message digest region. In public key cryptosystems, the sender signs the message digest using its private key and receivers can verify the authorship of the message with signer's public key. The one-way property of hash functions also assures the message has not been modified. The sender must attach a digital signature at the end of every control message. Note that some routing protocols use variable fields in their control messages, such as hop- count and time-to-live field. The authentication will be the first line of defence against attackers. The given pair of public/private key connection is a secure way to transmit from device to neighbour RSUs, but before communication e.g., keys must be entered manual process or transmission of secure protocols. Assuming the private key is only known to the designated node and stored in a perfectly secure way, proving a node has the corresponding key is equivalent to proving a node's identity. By using this it will provide a better security and no access to unauthorized persons.

In this scheme, system will generally contribute to produce privacy for VANET to scan into different divisions not entirely separable, categories: preventing identity information to leakage for credentials (e.g., information in certificate that bound together in cryptographic manner) and tacking vehicles to prevent from unrelated third-parties for users. Also these categories are not entire separable due to unrelate third-parties can track its target vehicle or user easily, by either single or multiple associations Author D¨otzer provided a variety of privacy topics for VANETs. The important topic among vehicle manufactures can choose the customer to select different types of vehicle based on its technology which attract to in-line customer's view based on privacy matters. The correlate message will extent up to long period due to leaking identity information to observe perfect time reputed its interested over-heaving parity. It requires multiple layers to propose the integrity identifier only by privacy compromising adversaries. The pseudonyms act as implicit proposal for both vehicle and multiple identifiers. However, such identifier changes may not be sufficient if an adversary is able to identify a vehicle based on its RF fingerprint, to produce

realistic vehicle movement traces for the network simulations. The result shows that the model is quite accurate and the proposed algorithm enhances the DSRC performance compared with other algorithms in the literature.

3. PROBLEM STATEMENT

3.1 Assumption of Overviews

The user faces many difficult tasks to find an important traffic route from source to destination. In previous trend, user usually refers a hard copy of map every time. This drawback is quite obvious. But this situation they introduce a Global Positioning Systems (GPS) to show the correct route of navigation systems become more popular, for example. In this system, a tiny hardware device is installed in a vehicle which capable to receive the GPS signals, by using this device it will identify its current location and transforms to local map database to show the geographical shortest route. The route finding procedure of both local map database and real-time road condition systems are not taken into an account. When the user need to know about real time road situation at the same time user has to analyze another system know as Traffic Message Channel (TMC), which adopt into number of developed countries. The TMC can detect frequency modulation radio system to broadcast real-time traffic and weather information to users. The information can be received by using a special equipment hardware device is used to decode or to filter valid substances. The user can obtain information even from severe traffic zone condition (e.g., any case of traffic accident) can broadcast to others, but user cannot obtain information like the general fluency of a road from TMC.

3.2 Requirement of VANETs Reception Management

Due to assumption of following properties are necessary to require the characteristics of VANETs reception management scheme, also VANET data flow assignment as shown in fig: 2.

VANETs short-term likability to users, In VANET context the vehicles and the users are closely related to each other. The relationship between vehicles and users are categories to three roles. A given user may be an owner, a user will give request to vehicle's question or either passenger will acknowledge back to user queries. Usually there is a many-to many association between the vehicle and the user role, but at a given instant of time, only one user is a driver.

It is worth mentioning that the user role is more important than the others because he is the one controlling the vehicle in the VANET. The trusted authority will resist each vehicle to fix a tiny hardware named as tamper proof device. This component can be installed during the manufacturing process (for recent model vehicles) and if the component is not installed by the manufacturer, users can buy and install it later.

OBU key management to Road Side Unit (RSU), it allows several connections towards internet and serves the gateway to RSU, to act as static component in VANET. The vehicle-to-road side infrastructure communication (V2I) scheme is involved its own traffic attribution. The authorized authorities send some administrative task to main region of RSU, which capable to solving disputes.

Message integrity to Trusted Authority, TA or CA (Certificate Authority) is an essential entity in VANETs which provides identity for vehicles and Monitors the network. In the network, TA is responsible to solve any dispute happens in a system. The VANET will deploy at start operation, at this case TA will capable to detect errors from its surrounding regions. There are many possible candidates for TA: current road and transport authorities, automobile manufacturers, trusted third parties or both combinations of them.

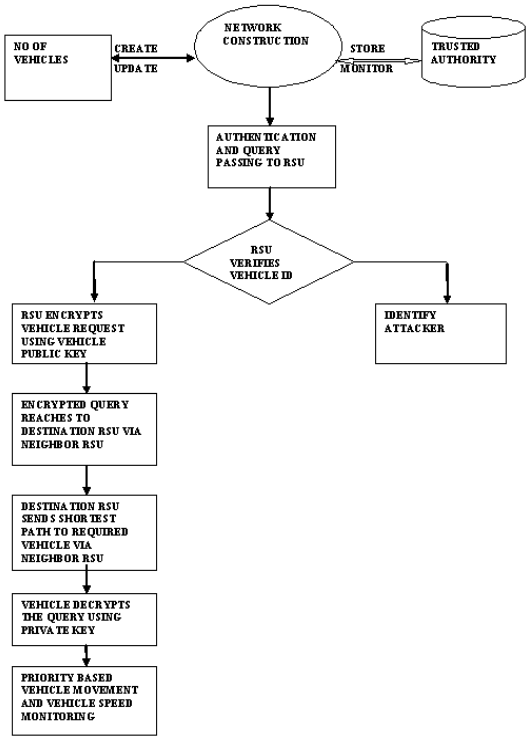

Fig: 2 VANETs Data Flow Assignment

Information Dissemination, in each vehicle having high range of velocity localized in VANETs challenging task, but any one in network has a capability to change its topology. Due to network partitioning in each vehicle's communication is the reason, that vehicles are unable to receive previous message. The main aim of communication patterns to send a request query to each vehicle must received successfully. Though, communication pattern uses different types of transmission as, single-hop broadcast, multiple forwarding of packets, store the message in different RSU areas.

V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure), there are two main types of communication in VANETs: Vehicle-to-Vehicle (V2V) communication and Vehicle-to-Roadside Infrastructure (V2I) communication. In V2V communication, the information contains important messages will exchange from one vehicle to others. Using this communication, vehicle can transform the message through via mobile networks. V2I communication usually covers neighbour Road Side Units (RSUs) until it reach the destination RSU. The internet is a main communication to get contact easily with other networks. For V2I technologies, they follow WLAN, DSRC, wi-max and mobile network through satellite communication can also be used.

3.3 Trust Establishment in VANETs

The traffic signal controller will disseminate both spatially and temporally by fine-grained, but also calculate speed and location information of vehicles can trace by VANET. The additional capabilities such as vehicle's speed and vehicle's location are unable to predict at this time instance, but vehicle

can reach the intersection line. The comparison arise between road side sensors and loop detectors to identify vehicles, could be presence or may be absence, hence vehicle will send continuous request to detect the size of queues.

Furthermore, it is cheaper to equip vehicles with wireless devices than to install roadside equipment. Traffic adaptive signal control has been widely studied. Examples include the well-known Split, Cycle, and Offset Optimization Techniques (SCOOT) and Sydney Coordinated Adaptive Traffic System (SCATS). SCOOT uses a loop detector as a sensor that is placed at the entry point of every link to an intersection. SCAT also relies on loop detectors, which are immediately placed before the stop line of an intersection. RHODES and its successor MILOS are probably the most sophisticated traffic adaptive control systems that have been recently developed. They are also based on loop detectors, and they optimize lost times on a global scale.

3.4 Assumptions

In MILOS, the traffic signal scheduling is done for a network of traffic controllers, including freeway ramp controllers. Loop detectors provide vehicle's position information to a central controller, which then generates schedules for the entire traffic network. In a detailed survey of vehicle-actuated traffic signal control methods is given, both for one-way and two way streets.

The VANET-based vehicle-actuated traffic method is based on the study presented with additional enhancements that take advantage of the finer grain information enabled by a VANET. These enhancements take advantage of the ability of the VANET infrastructure to estimate when a vehicle is going to approach the stop line. The controller uses this information to extend the GREEN time by an appropriate amount so that the vehicle can pass through the intersection. Another example of VANET-based traffic signal control is Traffic View. This work modified the Webster's method to leverage VANETs to communicate with the traffic signal controller. VANETs have also been used to enhance other traffic control and management applications.

The study to presents a VANET-based method for variable speed limits to improve the flow of vehicles in freeways. In VANETs are used to detect highway incidents and broadcast this information to drivers. In an extension to this work, examines the "memory" that platoons of vehicles can keep to more efficiently broadcast freeway incident messages. VANETs have also been used in many driver experience improvement applications. For example, VANETs have been used to monitor road conditions. In addition to VANET, cellular communications have been used to design a system that estimates traffic delays.

4. SYSTEM MODEL AND PERFORMANCE PARAMETERS

In the process of safety applications in VANETs, vehicles broadcast two types of messages: event driven messages and status messages. While event driven messages usually contain safety-related broadcast information, statuses messages will periodically sent to all vehicles within their range and contain vehicle's state information such as speed, acceleration, direction, and status of vehicle's position. Therefore, emergency vehicle's messages will give the highest priority, whereas status messages will precede the other priority substances. These concepts are clearly explained in VANETs architecture as shown below in fig: 3.

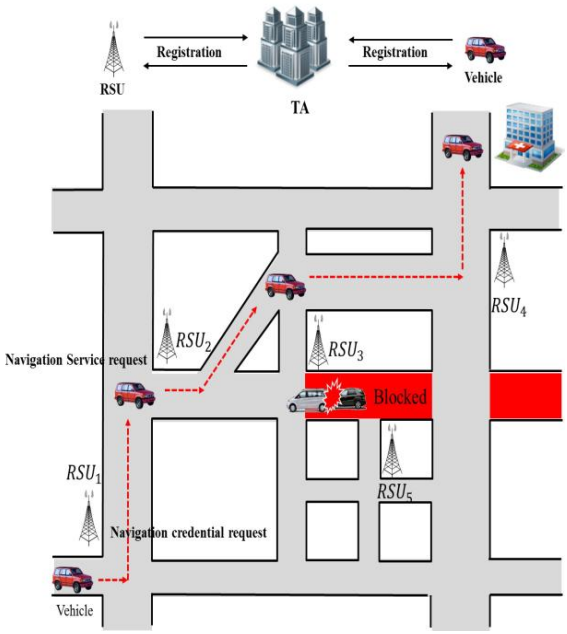

Fig: 3 VANET's System Architecture

In our model, Initially A vehicle should be authenticated by Trusted Authority (TA) via RSU, now the message can transmit from TA to RSU then the navigation query sent to RSU through tamper proof device (in the Vehicle) for identifying best destination route. After authentication, TA generates a re-encryption key to requested vehicle for encrypting the query; it will send the query up to identification of best destination route travel through along RSU. Based on vehicle request, contacted RSU identifies the shortest path to reach the destination RSU by passing the vehicle request to neighbouring RSU's. After identification of shortest path, it sends the encrypted message to requested vehicle using re-encryption key for security purpose. Finally it decrypts the message using its own private key. Then only user can view the traffic information messages and further travel through this route. Also the, network checks each vehicle speed for avoid accident based on predecessor and successor vehicle's speed using chord algorithm. We also implementing priority based vehicle movement. Network gives high priority in emergency vehicle, it gives medium priority for registered vehicle and it gives low priority for unregistered vehicle.

4.1 Chord and DHT Computations

In real time computing, chord algorithm is a protocol normally treated as peer-to-peer communication. This type of algorithm stores a key value for distributed hash table that will assign keys to every node but same time, all the values in a node assigning same keys that will stores in a particular substance. Chord assigns the keys to every node, it will locate through its territory and, how a node will discover the keys to each node. In this case chord algorithm specify an e.g., for DHT applications based on point-to-point protocol substance. In VANET chord proceed the overlay networks for every exception to find the shortest route. In DHT abstraction, chord will observe many attractive features such as fault-tolerant, scalable, self-organized and complete distribution. The global digest function has predefined hashed value for every node and every object such as SHA-1, MD4 and MD3. Either node or object, the digest function is based on hash value treated by global unique key in each message digest system.

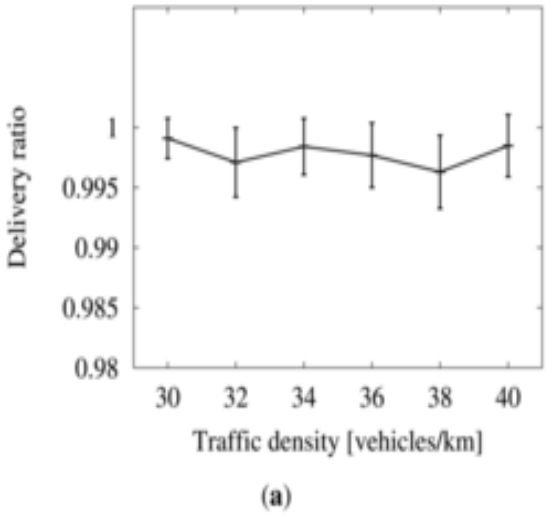

Fig: 4(a) Vehicle's traffic density ratio

The high probability medium in both key space and digest function, not in linear identification but also be selected carefully. The possible keys of maximum and minimum space have identity of each node using ring wrapped method. Every node A maintains successor process, which node having small number of keys among larger than A's, but the predecessor process is the node having large number of keys among smaller than A's, also the list of node will maintain each set of operation in the formation of O(log N). In the ring segment each node is responsible for others (Key of A, Key of A's i.e. successor). The random distributions of key space have positive number of observation, for each work load it will occupy average number of nodes. The ping message in VANET is to realize the consistent stage, in order to instant a point-to-point overlay by sending a direct message to exchange information among each nodes using predecessor and successor. The operation will be guaranteed for specific number of keys to follow a direct correctness of every node, to change the key frequently. The key space k have a equal number of bits in each node maintain by a hash table. The m^{th} entry of hashing table follow larger number of records, but the first node has key+2m-1, where m=(1,2,3,.....n). The hash entity mechanism will have logarithmic complexity to be accomplished. Notice that, physical position will not capable to enclose the neighbour nodes, but it necessary to need a data transmission in each node.

4.2 MChord Techniques in VANET

Due to the node mobility and frequent topological changes cause the design mechanism to reduce protocol overhead and some alternative problems.

1. The available information of each modelling will update frequently from Chord to MChord.

2. The aggressive table update: also try to use any informative process (for Chord) and over-lay table formation (for MChord).

3. The broadcast over-lay application will transform the message in point-to-point network, though neighbour node always transmit in unicast mode instead of using ping to keep a live mechanism.

4. The representation of chord's table creation will select a near node in over-lay aggressive table, by using a latest

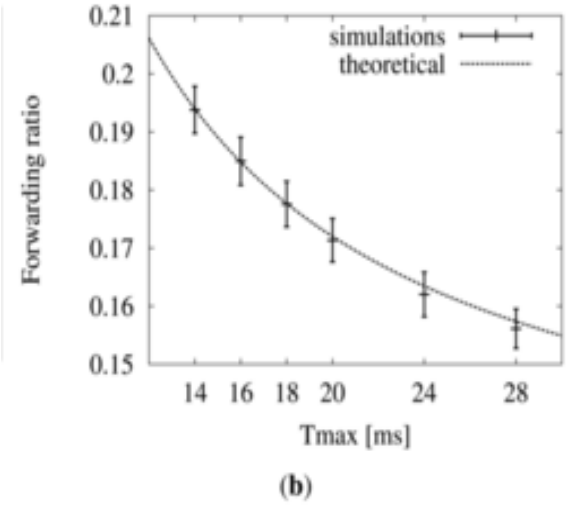

Fig: 4(b) Vehicle's packet Forwarding ratio

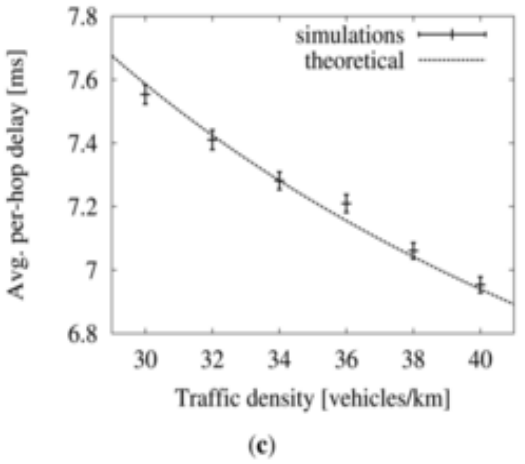

Fig: 4(c) vehicle's Avg. Hop delay

selective technique towards a greedy forwarding method.

The vehicle's traffic Density at the delivery ratio and reduce the Maximum average hops delay as shown in Figure 4(a) and (c).

5. The broadcast in over-lay table will combine to point-to-point network instead, joins a new node of combination to learn the process in whole set of network information, by using its passive boot strapping.

4.3 VANETs Message Authentication and Transmission

The VANET will produce connectivity to perform a cross layer extension and traffic reduction. Initially, a vehicles should authenticate its identity using devices know as Trusted Authority (TA). It can travel through along RSU until the signal sets a navigation path to proper destination RSU. Then the navigation query will send from tamper proof device (fixed in a vehicle) to RSU for identifying best destination route. The authentication is accepted, then it generates a TA will send a re-encryption key to request the vehicle by transform the node to chord's over-lay table process, since the message is transmitted only in unicast format. The message is encrypt by vehicle's query, also the vehicle based request will contacted to RSU to pass the message through neighbour RSU until it has to reach the destination RSU, to identify the

shortest path in a navigation route. The message transmission process will have capability to store more information, which containing in over-lay table to store more number of packets will also be saved. The shortest path will identified to send a encrypted message to request vehicle by using a re-encryption key. In such network, causes the problem having high traffic region leads to drop packets, but chord specify a non-congestive process to reduce both the traffic and message loss segment. The user needs the information about shortest path route, the receiver message containing decryption procedure of its vehicle's own private key. The over-lay broadcast table stores both the public and private keys until the cross layer enhancement will depend on vehicle's request, always be active position to send a secret key for particular users. Moreover, the network checks the vehicle speed to avoid accident, based on chord's predecessor and successor method. If a route breaks, the intended receiver will not receive an acknowledge, so DSRC will communicate to transmit the packet, by 802.11p for retransmit the packet once again until it reach the limitation. The implement process gives the

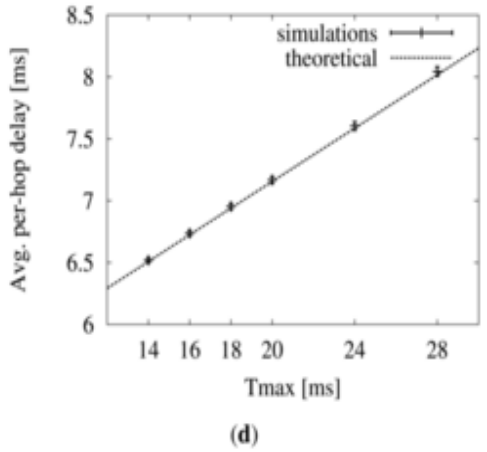

Fig: 4(d) Max. Time limit between peak hop delay

result to priority based vehicle movement; also vehicular mobility has a link which is vulnerable to break. Network gives higher priority to emergency vehicles (e.g., ambulance, fire engines, etc), it gives medium priority for register vehicle (user gets identity from Trusted Authority (TA)), also it gives lower priority for unregister vehicles. This scheme establish a maximum packet forward ratio in each vehicle's node, so it reduce the hop delay and will increase the maximum time limitation due to this vehicle's can send and receive messages easily as shown in figure 4(b) and (d).The most packets get lost in transmission due continuous presents of mobility failure. The chord algorithm and cross layer have a constant transmission of unicast packet to allocate different routes to different destinations. Therefore, it results no loss in transmission, packets having high probability by receiving a status message in each vehicle, to provide high security for vehicles and also less communication overhead, timing consume is less, so user can find the shortest navigation route to reach the destination quickly.

4.4 Vehicular Network in Over-lay Broadcasting

The interval period and broadcast over-lay table will have more dependency matched system, due to increase the node density at fixed period. The VANETs network information should increase its transmission compare with other networks, also the performance will enhance to store information in over-lay dense network. The broadcast over-lay method has simultaneous presents to change the utilization of more cross layer enhancement. The performance degrades to short interval period thus; the information will have less chance to update the system frequently. The over-lay broadcast network has some important observation due to increase the performance of cross layer segment. The piggyback effect will have more number of knowledge stores in over-lay table section; at the same time broadcast operation is infrequent to cross layer harvest systems. In order to maintain good over-lay protocol consistency, it precedes both the cross layer enhancement and over-lay table network have to reduce their limitations. As a result, could apply the over-lay protocol to combine with topmost layers to provide high efficiency duties in VANET towards this operation.

5. VANETs MODULE VALIDATION

In this section, VANET scheme has present to reduce the traffic congestion in all possible routes, to gives the shortest path, since vehicle can reach the destination, these consumptions are undertake by network simulation. This simulation will proceed to save the travelling time for significant period and also this function operates minimum amount of cryptographic prophecy. Note that internetworking credentials are the generation of VANETs modulation to be compared separately.

5.1 Module Enhancement Flow

A modular design will reduce the complexity, changes of facilities (critical problems solved by software presentation), and different parts are encouraged by parallel development system. In simple computation software can easily developed because of effective modularity and interface are simplified. The module software can form a simple architecture will give the name and addressable for each component know as modules, these integrities will satisfy the require problems.

Modularity leads to single attribute of software that allows the program to perform intellectually managed. The five important aspects which enable for design amplification method with respect to multiple sources, for develop an effective modular design are: Modular ability to understand, Modular ability to decomposed, Modular ability to comps, Modular ability to continuous and Modular ability to protection. These following modules will give respect to complete its project system; also existing techniques will give high support for future enhancement.

Vehicle Construction and key Assignment, In this module, every vehicles store their information details in Trusted Authority (TA) to identify number of possible routes. The TA maintains the vehicle's connection information from one node to other. There are many available routes has localized so, the vehicle can connect through other vehicles in all the directions. Only the registered vehicle can get the information from central server i.e. TA. When the movement takes place, TA will generate a revocation list for each vehicle, from this case both the vehicle details and the vehicle status are noted separately. When the user is ready to transmit the query, TA maintains re-encryption key and secret key for each vehicle to send the information securely.

Verification of Vehicle and Encryption based on RSU, In this module, vehicle search the shortest path to identify a best destination route, in order to transmit the query through Road Side Unit (RSU) and get the acknowledge back to RSU. The TA will send a request to RSU to verify the vehicle's id, based on secret key which already installed in vehicles to identify

authenticate user or not. After verification of vehicle id, RSU receive the vehicles re-encryption key for encrypt the vehicle's query based on TA. Finally, RSU encrypt the user query passed through destination RSU travelling via neighbour RSU.

Path Identification and Decryption, In this module, based on user query destination RSU finds the best and shortest path in a travelling sequence. Then it transmitted the required path to user's vehicle towards a neighbour RSUs. The user's vehicle request receives the encrypted query, and then it decrypts the message on its own private key, only then user can able to view the shortest path. After decryption process, vehicle moves freely from one network to other networks.

Priority based Vehicle Movement, In this module, network allows each vehicle based on priority manner. The vehicle movement based on priority will leads to avoid collision. Network gives higher priority for emergency vehicles like ambulance, fire engines etc. It gives medium priority for registered vehicles, because those users installed the device in vehicles and frequently update the information to TA. Finally, the lower priority gives to unregistered vehicles; this case user fixed the device no further information has been proceeds to vehicles.

Verification of Vehicle Speed based on Chord Algorithm, In this module, TA will maintain the vehicle's speed limitations, which already installed in tamper proof device, transmit through one network to others. Chord algorithm monitor's the vehicle speed in every moment node transmission from one network area to another. Based on the chord algorithm, network detects the current vehicle speed and monitor towards each node by predecessor and successor method. When the user receives shortest path destination, in case vehicle moves high speed means, network has a control access to block that vehicle based on predecessor and successor method, also vehicle's high speed must be noted in TA separately.

5.2 VANETs Tacking Movements

The vehicles registered with TA based on tacking connection between tamper proof device and RSU. The TA monitors the tacking signal and assign id for each vehicle, also the user's request query transmitted from TA to RSU. The vehicle's tacking device receives both the re-encryption key and user's private key via through TA. When a user installed the device in vehicle, registration system should support for tacking signal i.e. transmission of vehicle's query to-RSU-to other vehicles. The tacking signal in TA maintains the secure id information for each vehicle and encrypts the query by using re-encryption key following the protocol of DSRC communication and pass the query through neighbour's RSU. The user installed the device in vehicle which always present in active position. Therefore, malicious node cannot detect multiple virtual identities to send a fake message in different forged position. The user tacking device will capable to block the false traffic information in this situation, user vehicle cannot deviate its direction route. Using the tacking system in vehicles, it proceed more advantages to users for e.g., less time consuming, less communication overhead, provides high security and direct communication between vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). The VANET tacking moments in vehicle security system has consulate more in overcoming existing system but, provide high importance to future enhancements.

5.3 Network Simulation Results

The Network Simulation (NS) in VANET has showed most expected outcomes in all possible effects. The network component and network setup has both undertaken in simulation event, because NS is object oriented TCL (OTCL) script interpretation. The other way to use NS, by programming the script follows the user in OTCL script language. The network topology in plumbing function will intimate to traffic source in each network objects, to setup the initiate event scheduler of both start and stop transmitting packets in library region, user should setup and run the simulation using its OTCL script language. Compare with input TCL script, the OTCL language has more specific contribution. The NS produce more text based output files, it contain detail simulation results about user's data until the TCL script is finished.

The Network Simulator NS-2 will produce the coding towards shortest path for secure navigation route. The simulation process consist of three following steps,- i) vehicle construction and key assignment for each path, ii) verification of vehicle and encrypt the keys using TCL script i.e. code for RSU (creation of dynamic nodes), iii) path identification and decryption for both message delivery and responses. The first step shows that, TA connected to each vehicle using the DSRC communication protocol. When, the vehicle registered with TA it sends a secure keys to each vehicle also network coverage will extend up to users radius range. The vehicle received the secure keys and transmitted towards the RSU, but each vehicle will initiate and distribute the key separately. The TA transmits the secure keys to each vehicle, at same time information will interchange from vehicle-to-vehicle (V2V) and details are updated for registered vehicles. Therefore, every time TA will update the vehicle's detail and transform to RSU coverage areas. Always frequent transmission of information occurs between vehicles to RSU. The TA transferring secure keys to each vehicle shown in fig: 5.

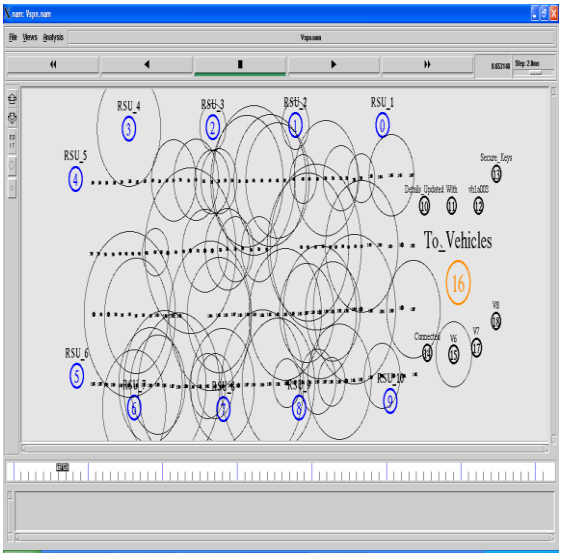

Fig: 5 Vehicle's TA transferring secure keys

The second step shows that, every vehicle has included the secure keys to connect with each other. When TA passes the tacking signal to each vehicle, same time RSU also receive those signal by users private key initiate distributive system. These keys send through RSU will reach up to destination RSU travel via, neighbour's RSU. Every time vehicle receives the secure keys and also details are updated frequently, so the

vehicles easily connect between the tacking signal and central servers. The vehicle receives the request query it transmits towards RSU by using re-encryption key and travel through neighbours RSU, to set a shortest path secure navigation route. The user received private key in order to send an acknowledgement back to TA. Now, the TA is connected to near RSU will forward and maintains the packet until it reach the destination. The revocation list is generated from TA, signals are forward towards several direction at each time. The tacking signals release the secure id for each vehicle will interconnect between RSU and TA. The list maintains by TA, but RSU sends a message to central server for confirmation its identity process. The TA maintains separate revocation list that will stores all the vehicle information details. After the detail updating, due to vehicle request the encryption and secret key will transmit to vehicle based on priority. Now every user has its own secret key, that will assign to RSU and vehicles but details are stored in TA revocation list. The user ready to send a query from vehicle to RSU, same time number of vehicles start to send query in different places. In this system, TA separates the id for different vehicles and sets the path to identify a best destination route. The user sends its id to RSU for verification using its secret key, in order to find shortest distance for secure navigation route. When, RSU receives the re-encryption key also it search for neighbour RSU to transmit the key for identify the secure route and further details are stored in vehicles TA. Similarly, these procedures are followed to other coverage vehicles to find the best secure route.

The third step shows that, TA transmit the secret key to connect each vehicles, but similarly vehicle's message and status are stored in TA device. The above procedure is repeated for this simulating

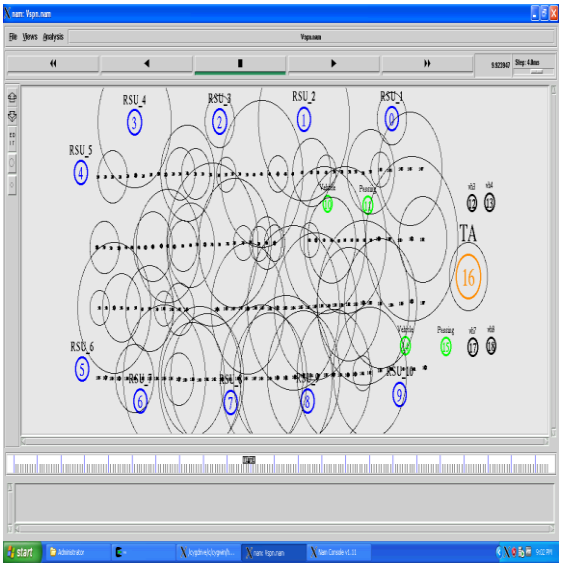

Fig: 6 Vehicle's based on priority

purpose as vehicle initiate and distributes the secure key transmission from one to other; further details are updated to TA. Also, it repeats until how many vehicles is connected to TA during the coverage of radius range, but allows the vehicle based on priority connection method as shown in fig: 6. The user can transmit the online information of vehicle's status from one vehicle to neighbour vehicle based on vehicle-to-vehicle communication (V2V). The priority sets for each vehicle, which has the access for connection and registration with TA. The same method follows that, RSU has a connection of vehicle's query request using its own private key to forward and maintain the revocation list. This system forwards the request to neighbour's RSU to find the best destination route in particular time limit so, this situation user not to waste time in traffic areas. The user encrypt the query and forward to near RSU to find the updating details, request passed through next RSU and their information is stored in TA list. When the vehicle id is received from TA the neighbour RSU inform to user about alternative path to move the vehicles. The verification will undertake for each vehicle due to its secret key, and then only vehicle receives the information about shortest navigation route. The re-encryption key is transmitted towards destination RSU to verify the user's private key and sends the acknowledgement back to source unit. The user receives the request from destination RSU, by decrypt the message using its own private key. Now the vehicle moves freely in shortest path from source to destination, at same time query passed to neighbour vehicles they also receives information about shortest route, based on priority manner vehicle movement will occurs. The RSU transmits the online information to each vehicle in case any obstacles are blocking the route means, immediate alert information generate to vehicles and finds another shortest route, this alert information exchange to neighbour vehicles also to save their time limit. This procedure repeated until all the vehicles are connected through TA device based on user's request it allocate their navigation route. When the vehicle moves from one network to another network, the device which control the vehicles speed based on chord algorithm. If vehicle moves high speed network block the vehicle based on predecessor and successor method, using this approach TA gives high security to vehicles.

Finally, VANET networks are location based experiments in order to show the secure navigation route for each vehicle. For instance, most of the countries are developing different kinds of VANET network to be organized regionally. The vehicle has to move freely across each domains based on TA generate a certificate, which governed to built a true relationship among manufacturers and users. In initial stage, VANET are not followed by realistic experiment in certificate authority. At this case, time is incurred for each user due to older days TA device is too costly to fix in vehicles. Now-a-days VANETs are characterized for strict time requirement to work for long chain region. In addition, previous revocation list are formed in difficult sets, which distribute to all the areas and travel through each vehicles in different region will issue its own revocation. The VANET helps in all the domains, also this project is planned to produce high security support for future life.

6. CONCLUSION

In this paper, most of the security primitives are adopted based on nontrivial method to represent some following techniques. The pseudo identity of tacking signal are authenticate to each vehicles due to its proper navigation route. The navigation queries and results are properly protected from unauthorized persons. Besides, vehicle's navigation query can link up its own identity based on TA. The message authentication is send towards the tacking signal and information is generating to RSU, showing the secure navigation route. Although, both privacy route and security requirements will produce more efficient to this solution, in order to make sense vehicle transmit the information to neighbour vehicles also but, the navigation query and received notification both produce in limited period. In practically, this scheme adopts to lower rate systematic development

approach, also vehicle moves freely from one network to other. Note that VANETs concept applied through many development areas, in which TA generates route searching procedure collects all the information about vehicle's speed, vehicle status, area specification, movements and travelling direction are updating frequently from TA to RSU. The message authentication is simple between each vehicle because, users need verification from TA which present the result inform of digital signatures. However, in large cities VANET operates in centralized approach, to implement this scheme the network must be scalable and to increase its performance furthermore. In future enhancement VANET extent his methods to investigate how best the address efficient to user's revocation issues, dynamic addition of attributes and secure vehicle-to-vehicle communication (V2V). Also, in future VANET improves his scalability by periodic manner.

7. REFERENCES

[1] T.W. Chim, S.M. Yiu, Lucas C.K. Hui, Senior Member, IEEE, and Victor O.K. Li, Fellow, IEEE "VSPN: VANET-Based Secure and Privacy-Preserving Navigation" on Vol. 63, No. 2, February 2014.

[2] C. Zhang, R. Lu, P.H. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," Proc. IEEE INFOCOM '08, pp. 816-824, Apr. 2008.

[3] Khalid Abdel Hafeez, Student Member, IEEE, Lian Zhao, Senior Member, IEEE,Bobby Ma, Senior Member, IEEE, and Jon W. Mark, Life Fellow, IEEE " Performance Analysis and Enhancement of the DSRC for VANET's Safety Applications" on Vol;. 62, No. 7, September 2013.

[4] I. Leontiadis, P. Costa, and C. Mascolo, "Extending Access Point Connectivity through Opportunistic Routing in Vehicular Networks," Proc. IEEE INFOCOM '10, Mar. 2010.

[5] Vaishali D. Khairnar and Dr. Ketan Kotecha "Performance of Vehicle-to-Vehicle Communication using IEEE 802.11p in Vehicular Ad-hoc Network Environment" on Vol.5, No.2, March 2013.

[6] H. Oh, C. Yae, D. Ahn, and H. Cho, "5.8 GHz DSRC Packet Communication System for ITS Services," Proc. IEEE VTS 50th Vehicular Technology Conf. (VTC '99), pp. 2223-2227, Sept. 1999.

[7] Lei Shi and Ki Won Sung "Spectrum Requirement for Vehicle-to-Vehicle Communication for Traffic Safety" on 2012.

[8] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANET Based Smart Parking Scheme for Large Parking Lots," Proc. IEEE INFOCOM '09, pp. 1413-1421, Apr. 2009.

[9] Yuchen Wu, Yanmin Zhu, and Bo Li "Infrastructure-Assisted Routing in Vehicular Networks" on 2012.

[10] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs," 2009.

[11] A.Euodial, P.Joyce Beryl Princess. "BVFG: Batch Verification Scheme for Filtering of Gang Injected False Data in Wireless Sensor Networks" on Volume 3, Issue 3, March 2013.

[12] A. Festag, W. Zhang, L. Le, and R. Baldessari, Vehicular Networks: Techniques, Standards and Applications, chapter Geocast in Vehicular Networks, Taylor&Francis, H. Moustafa and Y. Zhang (edts.), December 2008.

[13] Patil V.P. "Design, Development and Testing of Parking Availability System Based on Vehicular Ad hoc Network" on Volume 2, Issue 10, October 2012.

[14] M. Raya and J.-P. Hubaux. The security of vehicular ad hoc networks. In Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), Nov. 2005.

[15] Mostofa Kamal Nasir, A.S.M. Delowar Hossain, Md. Sazzad Hossain, Md. Mosaddik Hasan, Md. Belayet Ali. "Security Challenges And Implementation Mechanism For Vehicular Ad Hoc Network" on Volume 2, Issue 4, April 2013.

[16] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki. CARAVAN: Providing location privacy for VANET. In Proceedings of Embedded Security in Cars (ESCAR), Nov. 2005.

[17] L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE Networks Special Issue on Network Security, 1999.

[18] Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang, Fellow, IEEE. "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks" on Vol. 21, No. 9, September 2010.

[19] X. Lin, X. Sun, P.-H. Ho, and X. chung, "Gsis: A secure and privacy preserving protocol for vehicular communications," IEEE Transactions on Vehicular Technology, vol. 56, no. 6, pp. 3442–3456, November 2007.

[20] Dr.Sumegha Sakhreliya, Prof.Neha Pandya. "A Review on Security Issues and Its Solution's overhead in VANETs" on Volume 3, Issue 11, November 2013.

[21] G. Badawy, J. Misic, T. Todd, and D. Zhao, "Performance modelling of safety message delivery in vehicular ad hoc networks," in Proc. IEEE 6th Int. Conf. Wi*Mob*, Oct. 2010.

[22] Su-Hyun Kim and Im-Yeong Lee. "A Secure and Efficient Vehicle-to-Vehicle Communication based on Sensor Network" on Vol.7, No.6 (2013).

[23] X. Ma and X. Chen, "Performance analysis of IEEE 802.11 broadcast scheme in ad hoc wireless LANs," IEEE Trans. Veh. Technol., vol. 57,Nov. 2008.

[24] M. Al-Qutayri, C. Yeun and F. Al-Hawi. "Security and Privacy of Intelligent VANETs, Computational Intelligence and Modern Heuristics" INTECH, 2010.