Middle-East Journal of Scientific Research 24 (8): 2616-2623, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.24.08.23875

An Efficient MChord based Authentication for Vehicular Ad-Hoc Networks

[1]R. Sugumar and [2]B. Murugeshwari

[1]Department of Computer Science & Engineering,
Velammal Institute of Technology, Panchetti, Chennai-601204, India
[2]Department of Information Technology,
Velammal Institute of Technology, Panchetti, Chennai-601204, India

Abstract: The Vehicular Ad-Hoc Network (VANET) is a network to provide communication between nearby V2V (Vehicular to vehicular) and V2I(Vehicular to Infrastructure). In order to increase the network efficiency, it is required to have stability of transmission and security of reliability**.** Efficient authentication is one of the key challenges in vehicular networks. In order to provide the security between any two vehicles in VANETs, an MChord based Authentication is proposed. 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 reencryption 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.

Key words: V2I communications · Traffic security · Mchord · Message Authentication · VANET · Beaconing

INTRODUCTION

VANET is basically combination of an on-board unit (OBU) and more application units (AUs) [1]. A device with communication capabilities placed inside the vehicle is known as OBU. An AU is a device executing applications by using OBU's communication capabilities. The both units of VANET are usually attached with a wired connection or wireless. The Ad-hoc domain includes vehicles equipped with on board units and stationary units placed along the road. 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.

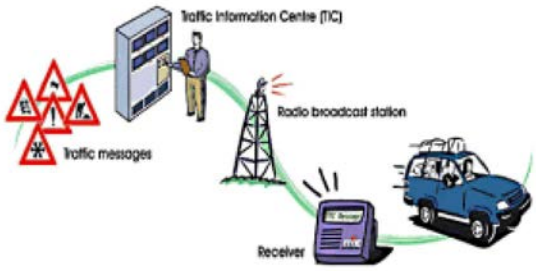

Fig. 1: Traffic Message Channel (TMC)

Corresponding Author: R.Sugumar, Department of CSE, Velammal Institute of Technology, Panchetti, Chennai, India.

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.

Related Work: To provide secure VANET, many researchers present a set of solutions to solve different security problems which are discussed in this section.

Isaac, J.T.; Zeadally, S.; Camara, J.S. in [1] surveys the major security techniques and presents the corresponding countermeasures and cryptographic solutions.

Researchers in [2-5] dealt with routing protocols and gave effective solutions so that the communication between the nodes is computational effective and leading to less congestion of network traffic. Yong Hao, Yu Cheng and Kui Ren in [6] proposed a solution of group formation combined with RSU is illustrated, which resulted in easy revocation of malicious vehicle, location privacy protection is improved and the system maintenance becomes flexible. Wang, J., Yan, W in [7] suggested a new protocol for message checking, this protocol involves checking the Certificate Validity (CV) of the sender, the receiver of the message checks the CV of the message sender, the result of checking has three cases: in the first case, the receiver will consider the message if the sender has a valid certificate, second case occurs when the sender has invalid certificate, in this case the receiver will not regard the message, in the third case, the sender has not CV at all, the receiver will inform the RSU with the sender and check the received message, if it is correct the RSU will issue CV for the sender, otherwise it will issue invalid certificate and record vehicle's identity into the Certificate Revocation List (CRL).

To protect vehicular network against Sybil attacks, researchers B. Liu, B. Khorashadi, H. Du, D. Ghosal, C-N. Chuah and M. Zhang in [8] proposed a solution involves using on road radar, where each vehicle can see surrounding vehicles and receive reports of their GPS coordinates. By comparing what is seen to what has been heard, a vehicle can corroborate the real position of neighbors and isolate malicious vehicles. Jinyuan Sun; Chi Zhang; Yanchao Zhang; Yuguang Fang in [9] proposes an identity based security system for VANET to solve the conflicts between privacy and tractability very effectively. The system uses a pseudonym based scheme to preserve user privacy. It uses a threshold signature based scheme to enable tractability for law enforcements. This is particularly attractive to service providers since they can achieve better efficiency of their services. Chowdhury, P.; Tornatore, M.; Sarkar, S.; Mukherjee, B., Wagan, A.A.; Mughal, B.M.; Hasbullah, H. in [10] proposed a hybrid technique that takes advantage of both asymmetric and symmetric cryptographic schemes. The technique employs hardware that integrates both asymmetric and symmetric cryptography modules for safety messaging.

Azogu, I.K.; Ferreira, M.T.; Hong Liu in [11] proposes an Asymmetric Profit Loss Markov (APLM) model to measures integrity level of the security schemes for VANET content delivery. The model uses Markov chains to record the system's ability to adjust itself given profit and loss. Given the measurement by the model as heuristics, integrity schemes for VANET can be optimized to provide better content delivery. Researchers G. Samara and W. Al-Salihy in [12] proposed using of Vehicular Public Key Infrastructure (VPKI), every node sends a safety message, it signs that message with its private key and attaches it with Certificate Authority (CA). The receiver party of the message, will get the public key of the sending party by using the certificate and check the signature of that sender, using its certified public key, but this solution requires that the CA public key be known by the receiver party. Azogu, I.K.; Ferreira, M.T.; Larcom, J.A.; Hong Liu in [13] explores security metrics for VANET that can in turn guide the design of defense mechanisms against jamming style Deny of Service attacks. The researchers propose a new class of anti jamming Defensive mechanisms: hideaway strategy, the effectiveness of this new class is investigated through the simulations. The researchers implement a simulation package integrating VANET modules (OBU and RSU) and attack/defense modules along with traffic simulation. Result shows that the hideaway strategy achieves steady efficiency advantage over traditional anti jamming schemes. Prabhakar, M.; Singh, J.N.; Mahadevan, G. in [14] proposed an essential complements to the passive mechanisms of encryption. For inputs as given security measures of the VANET, the defensive mechanism adopts game theoretic approaches and is comprised of three stages(i) uses heuristics based on ant colony optimization to identify known and unknown opponents (ii) Nash Equilibrium is employed for selecting the model for a given security problem and (iii) enables the defensive mechanism to evolve over traffic traces through the game theoretic model from the first stage.

Problem Statement

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.

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-toroad 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.

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.

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.

In the proposed 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

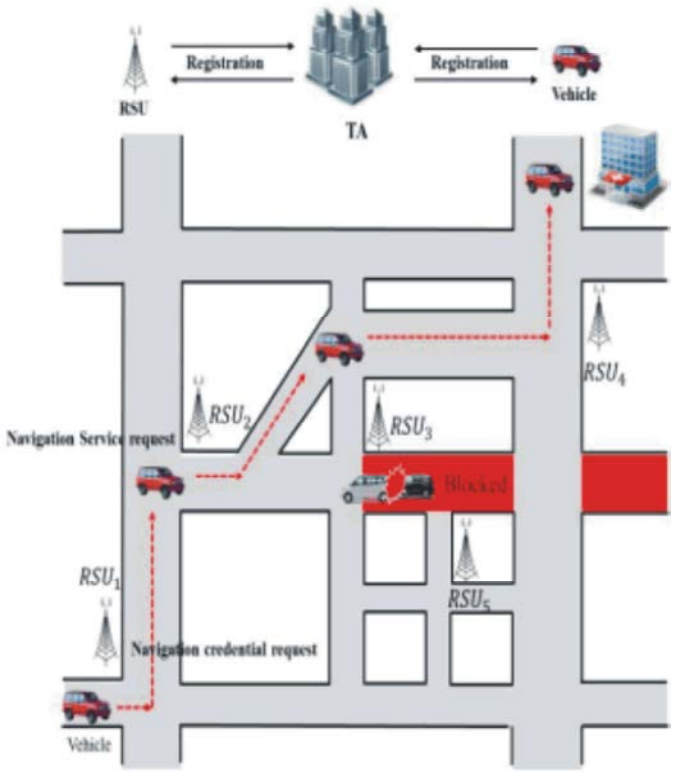

Fig. 3: VANET's System Architecture

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 reencryption 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.

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.

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.

- The available information of each modelling will update frequently from Chord to MChord.
- The aggressive table update: also try to use any informative process (for Chord) and over-lay table formation (for MChord).
- 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.
- The representation of chord's table creation will select a near node in over-lay aggressive table, by using a latest 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).

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

Implementation of Mchord Based Authentication: 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.

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.

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

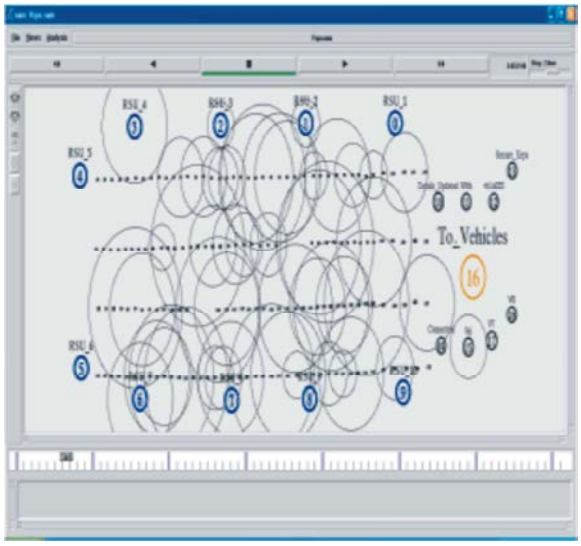

Fig. 5: Vehicle's TA transferring secure keys

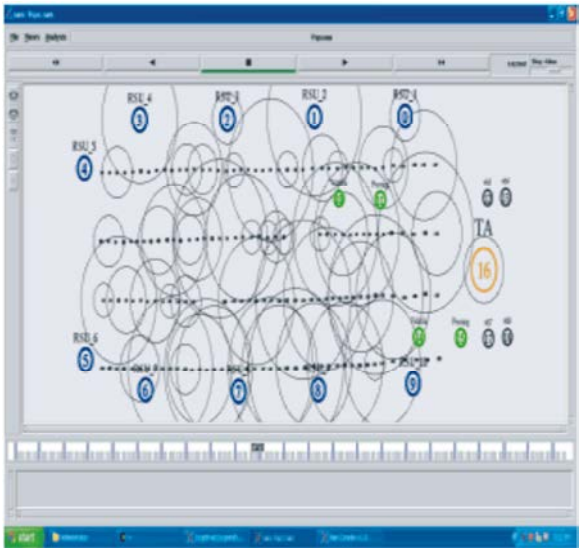

Fig. 6: Vehicle's based on priority

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.

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 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 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-tovehicle

communication (V2V). The priority sets for each vehicle, which has the access for connection and registration with 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-tovehicle 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.

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.

REFERENCES

1. Isaac, J.T., S. Zeadally and J.S. Camara, 2010. Security attacks and solutions for vehicular ad hoc networks, Communications, IET, vol. 4, no. 7, (2010) April 30: 894, 903
2. Hui, F., 2005. A survey on the characterization of Vehicular Ad Hoc Networks routing solutions ECS 257, Winter, pp: 1-15.
3. Yin, J., T. El. Batt, G. Yeung and B. Ryu, 2004. Performance Evaluation of Safety Applications over DSRC Vehicular Ad Hoc Networks, Proceeding of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, pp: 1-9.
4. Wang, S.Y., 2004. Predicting the Lifetime of Repairable Unicast Routing Paths in Vehicle-Formed Mobile Ad Hoc Networks on Highways, 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, (PIMRC), 4: 2815-2829.
5. Briesemeister, L., A.G. Daimler Chrysler, Berlin, Germany and G. Hommel, 2000. Role-Based Multicast in Highly Mobile but Sparsely Connected Ad Hoc Networks, First Annual Workshop on Mobile and Ad Hoc Networking and Computing, (MobiHOC), pp: 45-50.
6. Hao, Y., Y. Cheng and K. Ren, 2008. Distributed Key Management with Protection Against RSU Compromise in Group Signature Based VANETs, IEEE GLOBECOM, pp: 4951-4955.
7. Wang, J. and W. Yan, 2009. RBM: A role based mobility model for VANET, Proc. Int. Conf. Communications and Mobile Computing, 2: 437-443.
8. Liu, B., B. Khorashadi, H. Du, D. Ghosal, C.N. Chuah and M. Zhang, 2009. VGSim: An Integrated Networking and Microscopic Vehicular Mobility Simulation Platform, IEEE Communication Magazine Automotive Networking Series, 47(5): 134-141.
9. Sun, J., C. Zhang, Y. Zhang and Y. Fang, 2010. An IdentityBased Security System for User Privacy in Vehicular Ad Hoc Networks, IEEE Transactions on, Parallel and Distributed Systems, 21(9): 1227-1239.

10. Chowdhury, P., M. Tornatore, S. Sarkar, B. Mukherjee, A.A. Wagan, B.M. Mughal and H. Hasbullah, 2010. VANET Security Framework for Trusted Grouping Using TPM Hardware, Second International Conference on Communication Software and Networks, (ICCSN '10), (2010) February, pp: 309-312.
11. Azogu, I.K., M.T. Ferreira and H. Liu, 2012. A security metric for VANET content delivery, Global Communications Conference (GLOBECOM), 37: 991-996.
12. Samara, G. and W. Al-Salihy, 2012. A new security mechanism for vehicular communication networks, Proceeding of the International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), pp: 18-22.
13. Azogu, I.K., M.T. Ferreira, J.A. Larcom and H. Liu, 2013. A new antijamming strategy for VANET metrics directed security defense, IEEE Globecom Workshops (GC =Wkshps), pp: 1344-1349.
14. Prabhakar, M., J.N. Singh and G. Mahadevan, 2013. Defensive mechanism for VANET security in game theoretic approach using heuristic based ant colony optimization, IEEE International Conference on Computer Communication and Informatics (ICCCI), pp: 1-7.