International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Navigation Query Security through Privacy Preservation and Cryptography in VANETs

Anuradha T[1], Saba Tahseen[2]

[1]Department of Computer Science and Engineering, PDA College of Engineering, Kalaburagi, Karnataka, India

[2]M.Tech in Computer Science and Engineering, PDA College of Engineering, Kalaburagi, Karnataka, India

Abstract: ***Vehicular Ad hoc Network (VANET) is an autonomous network with dynamic topology where moving vehicles exchange information regarding their position with other vehicles. Depending on the position information of other nodes, nodes can determine their actions like change in route or change in speed and so on. Many navigation methods are provided in order to guide drivers to reach destination. Providing safety to the drivers is a crucial aspect of this paper. In this paper, VANET security is provided by making sure that the nodes are authenticated through a key exchange with server using intermediate road side units (RSU). Instead of sending the complete query at a time, navigation queries are protected by breaking them down into fragments. The identity of the sender is hidden by encrypting it with the symmetric key. The overhead into the communication framework is not added in the system, this can be shown through the simulation results and nodes can manage a good packet delivery ratio with low latency. The system also helps the nodes to maintain their speed by correctly adjusting speed relative to navigation queries.***

Keywords: VANET**,** Public key Cryptography**,** AODV, Authentication, Security.

1. Introduction

MANET has given rise to a new area called Vehicular Ad hoc Network (VANET), which aims to provide road safety, efficient driving, information and entertainment. VANET can be considered as a subclass of MANET. VANET is an autonomous network with dynamic topology. VANET has become the recent advancement in wireless network. Infrastructure provided by the VANET for developing new systems enhances driver's security and comfort. VANETs are distributed into Ad hoc network that are formed between moving vehicles and are equipped with wireless communication devices.

In order to create a network, VANET considers moving cars as nodes. Every car that is participating in VANET will be turned into a router or a node. Every car will be connected to other car in the range of 100 to 300 meters [1]. When the car is out of the range, it will be dropped off the network, other cars can join in and hence connecting vehicles to one another and a Mobile Internet is created. Delivering timely information in a cost effective manner to the drivers is the main characteristic of VANET. Vehicles in VANET consists of on-board sensors and the road side units have been deployed along highways which can be used for providing communication between vehicles(V2V) and between vehicles and infrastructure(V2I).

Fig1 shows the architecture for VANET. The interaction between Node 1 and Node 2 refers to V2V communication. Node 2 can also interact with Node 3 and Node 4 directly. But the Node 1 cannot directly communicate with Node 3 or Node 4, as it is out of range. The vehicles communicate with each other and interaction can also exists between vehicles and road side unit (RSU). Node1 can communicate with Road Side Unit. Node 4 cannot directly interact with RSU. The interaction between vehicles and that between vehicle and RSU takes place by using Dedicated Short Range Communication (DSRC) protocol. The interaction between base station and RSU is by fixed network.

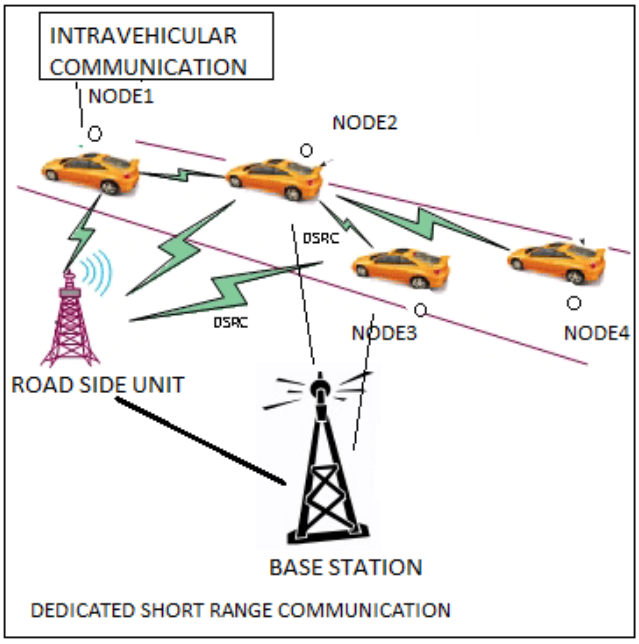

Figure 1: Communication in VANET

Characteristics of VANET

- The movement of each vehicle is restricted to roads pattern making it somewhat predictable, but it has highly dynamic topology. Vehicles in VANET move at a very high speed and therefore the topology of network changes frequently.
- The chances of network disconnection are quite high as the density of vehicles is low.
- As the vehicles can enter and leave the network easily, hence the network size is unbounded.

- Each vehicle has on-board sensors and GPS provide information so that it can be further used to form links for communication and dissemination of data.
- Applications in VANET do not require higher data rates but they have hard delay constraints.

Security issues in VANET

Security in VANET has got less attention, in comparison to other challenges. Some security requirements must be satisfied before the VANET is deployed. The following must be satisfied by the security system in VANET:

- Authentication: Authentication refers to the generation of message by a legitimate user.
- Availability: Availability refers to the information be available to the legitimate users wherever needed. The information cannot be shared in case of Denial of Service (DOS) attack and this can brings down the network.
- Non-Repudiation: The node cannot deny the transmission of message.
- Privacy: The privacy of the node should be guaranteed against the unauthorized node.

In order to prevent against the attackers, one should have full knowledge about the attacks in VANET. In this paper, Distributed Denial of Service Attack (DDOS) is considered. DDOS is a type of DOS attack, in which multiple systems are compromised. It is an attack in which network resources are made unavailable to its intended users. This is made by suspending or interrupting temporarily the services of host connected to the network.

Public key cryptography is used over open networked environment for securing communication. A variety of communication security problems are susceptible over open network environment such as internet. Public key cryptography is also known as asymmetric cryptography. The public key cryptography uses two separate keys. One is public key that is used for encryption and the other is private which is used at receiver for decryption. In a dynamic network like VANET where there is a frequent change in configuration of node, secure routing is difficult to assure.

2. Organization

The paper is organized as: section 1 discusses Introduction, section 3 discusses Related Work, section 4 discusses Proposed Work, section 5 discusses Simulation & Results and section 6 discusses Conclusion.

3. Related Work

Many works have been conducted for the privacy and security in VANETs. In [2] Authors have studied the security requirements and challenges to implement the security measure in the VANET. Different types of attacks and their solutions were also discussed. They concluded that among all requirements, authentication and privacy are the major issues in VANET. Confidentiality is not required in the VANET because generally packets on the network do not contain any confidential data. A system is proposed in [3] such that the system should be able to help establish the liability of drivers; but at the same time, it should protect as far as possible the privacy of the drivers and passengers. In [4] a mutual authentication technique for RSU and vehicle is proposed. The RSU is used as a mediator for authentication of both the RSU and the requesting vehicle. In this technique CTA is responsible for verifying the credentials, and hence the load of RSU is reduced drastically. In [5] Authors have proposed a novel proxy re-encryption scheme and concluded that it provides better result on the basis of the privacy, security and authentication and it reduces overheads while roaming networks. In [6] a novel method based on cryptography is studied to detect Sybil attack and the operations are done by Certificate Authority (CA). The delay of detecting Sybil attack depends on the number of messages and not on the number of vehicles is discussed. In [7] the authors have discussed the different types of attacks that may be applicable to VANET. They have proposed a model to provide solution to DOS and DDOS attacks, and to ensure network availability for secure communication between the nodes. Finally they concluded that it is important to maintain network availability and to develop trust in the VANET network. A method is proposed in [8] in which the VANET is made into small clusters with long Cluster Head solution. This method reduces effectively the total number of control packets generated during route discovery process and also reduces the total number of unused routes generated during that process. It is studied in [9] that for the strong security of VANETs communication, not only the secured communication frameworks is needed but also powerful routing algorithms is required that can facilitate the detection of malicious vehicles in networks and mitigate them. In [10] topology based routing protocol is focused and they have examined how different topology routing protocol suffers from the highly mobile nature of VANET. They have concluded that the AODV is preferable because of higher packet delivery ratio. In [11] Authors have concluded that position based and geographical protocols are best suited protocols over table driven and reactive routing algorithm. They have showed that STAR routing is preferred in case of uneven concentration of vehicles on road. Geographical routing is preferred as it provides transmission independent of network topology and is also capable of handling dead end simulation. A key revocation mechanism is proposed in [12] that protects valid user in VANETs from cruel attacks. The concept of trust and mistrust vehicles is used that strengthens the authentication process. It is studied in [13] that malicious users always try to challenge the network with selfish behavior. They have concluded that Ad hoc protocols play the main role in VANET but they have size limit. A verification method is proposed in [14] that updates a group key in the vehicle using a Bloom filter so that it reduces the overhead of group rekeying by road side unit (RSU). In [15] a novel RSU-aided message authentication scheme named RAISE has been proposed. In this method, RSUs are responsible for verifying the authenticity of the messages sent by the vehicles and notifying authentication results back to all associated vehicles. They have also proposed a cooperative message authentication scheme called COMET that works in the absence of RSU. In [16] a public key cryptography using time stamp key management system is

proposed. This method reduces collision in MAC layer and also minimizes delay.

4. Proposed Work

The proposed method for navigation query security through privacy preservation and cryptography in VANET uses AODV routing protocol. RSA algorithm is used to encrypt the Ids for the source node by using the symmetric key. When the source node generates the query, the query is divided into fragments in order to hide the complete information from the intruders. Even if the message is exposed to the intruder, the intruder will not have access to the source address due to source address encryption.

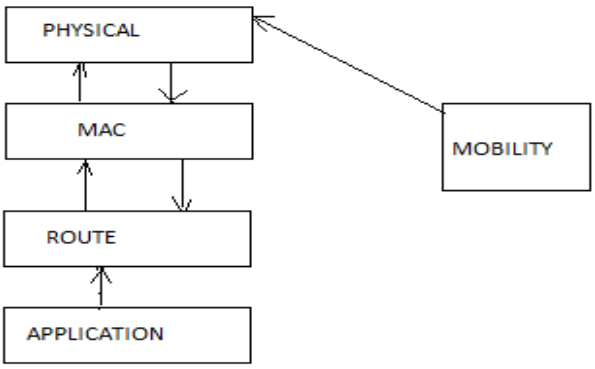

Figure 2: Internal Structure of a Vehicle

4.1 RSA

The method for securing the navigation query by using privacy preservation and cryptography is proposed using RSA algorithm. RSA stands for initials of the designer. They are Ron Rivest, Adi Shamir and Leonard Adleman. RSA is the cryptographic system that uses public key encryption. It is used for preserving the sensitive data when it is being sent on unreliable network.

4.2 Algorithm for RSA

RSA Algorithm requires generation of key, encryption and decryption. The algorithm requires the generation of private and public key. Public key is used for encryption and that key can be known to everyone in the network, where as the private key is used for the decryption at the receiving end and this key is to be kept secret. The encrypted message has to be decrypted within reasonable amount of time.

The steps involved in the generation of keys are:

- Select two distinct prime numbers of similar bit length. Make sure that the numbers are chosen randomly for security purpose and name them p and q.
- Compute n = pq,
  n will be the modulus of both private and public keys.
  This gives the key length.
- Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n - (p+q-1)$, where φ is Euler's totient function.
- Choose an integer e such that $1 < e < \varphi(n)$ and gcd $(e, \varphi(n)) = 1$, such that e and $\varphi(n)$ are co-prime, e will be the public key exponent.
- Determine d such that $d \equiv e^{-1} \pmod{\varphi(n)}$, which is equivalent to $ed + \varphi k = 1$, for some integer k
  Since gcd(e ,φ(n)) = 1.
  Therefore, the above expression will be
  $ed + \varphi k = \gcd(e, \varphi)$.
- The encryption function is
  $E = M^e \bmod n$.
- The decryption function is
  $D = M^d \bmod n$.

4.3 Algorithm for navigation query security through privacy preservation and cryptography in VANETs

- Application module generates the packet if the node is specified as source.
- The query is divided into fragments in order to hide the complete information from the intruders. The query fragmentation is implemented in application layer.
- This message comes to routing layer, which checks if there is a path till destination. If there exists a path, then transmission starts or else RREQ packet is generated.
- In RREQ packet generation, the identity of the source node is hidden by using a value that is known only to server and RSUs. In this method, it is assumed that the process of encryption is multiplication and decryption is division.
- The message is exposed to the RSUs as well as attackers . The intruder cannot get the source address due to source address encryption.
- RREQ packets are forwarded by the RSUs or cluster heads. The route is established from one vehicle through remaining RSUs till it reaches destination.
- On generation of Route Error, update the routing table and reschedule all the remaining packets and regenerate RREQ.
- Once the query is received by the server, the query is decrypted with the private key.

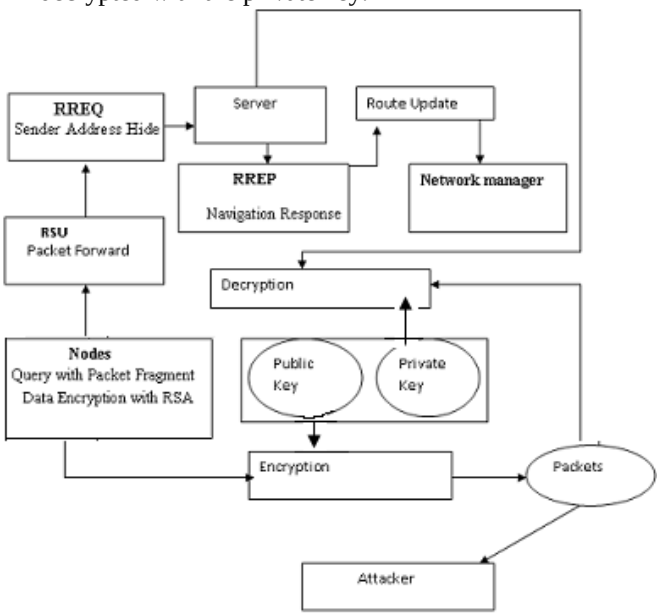

Figure 3: Flow diagram showing routing of packet

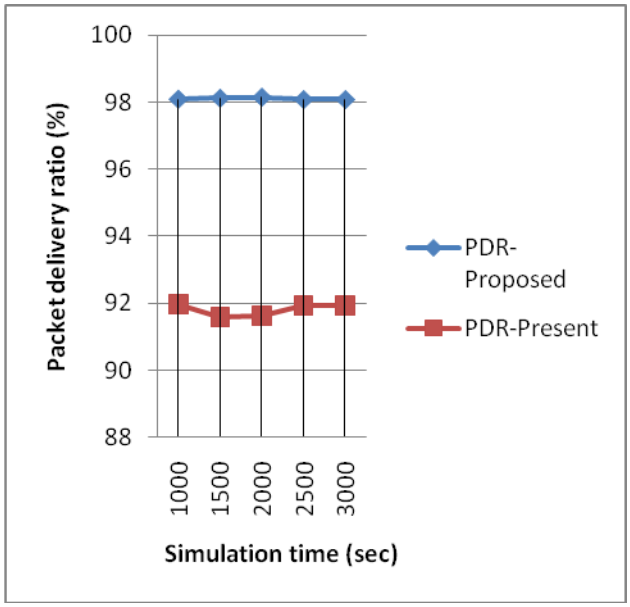

Figure 4: Packet delivery ratio Vs Simulation time

5. Simulation and Results

The simulation experiments are conducted using Omnetpp-3.3 simulator by using the proposed algorithm. The simulation runs for 3000 seconds.

The performance is analyzed in terms of packet delivery ratio (PDR), throughput, latency and energy remaining of the node. The comparison is made between present system where the query is not divided into fragments and the proposed work.

Table 1: Simulation parameters and their values

Parameters	Values
Packet Size	512 bytes
Initial Energy of the node	10Joules
Simulator	Omnetpp-3.3
Transmission Range	150 meters
Nodes placement	Random
Simulation Run Time	3000 seconds
Number of Nodes	50 nodes
Topology	Line Topology
Routing Protocol	AODV
Traffic	Constant Bit Rate(CBR)

Packet Delivery Ratio: It is the ratio of total number of packets received successfully at the destination to the total number of packets sent by the source. Fig 3 determines that packet delivery ratio by varying the simulation time for 1000s, 1500s, 2000s, 2500s and 3000s. Packet delivery ratio proves that the proposed system produces consistent PDR over time which is nearly 100%. Short packet burst ensures no jamming which results in good PDR performance. The graph shows better performance of packet delivery ratio for proposed algorithm, when compared to the present system.

Throughput: It is the average number of packets that are successfully delivered per second. Fig4 analyzes the throughput by varying the simulation time by 1000s, 1500s, 2000s, 2500s, 3000 s. Throughput of the proposed system improves over time and almost double of that of the present system. This is due to the fact that proposed system is capable of eclipsing the attacker successfully. However conventional VANET suffers from over packet flooding by the intruders and thus the effective throughput is lower. The graph below shows better performance of throughput for proposed algorithm, when compared to the present method.

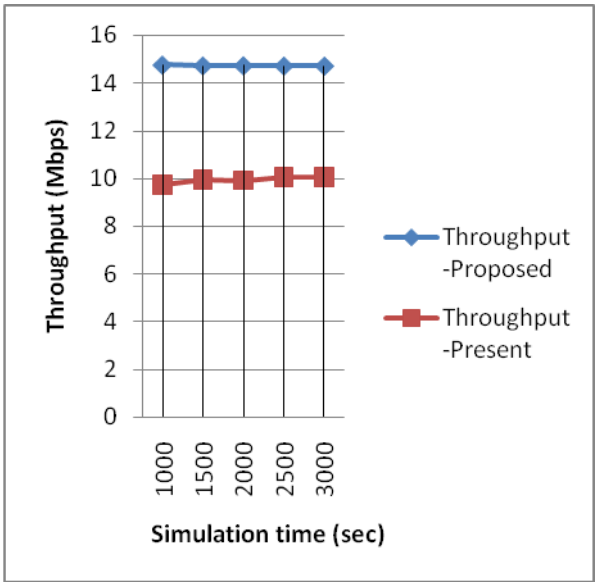

Figure 5: Throughput Vs Simulation Time

Energy remaining of the node: It is the energy that is left by the node after the simulation ends. It is measured in mili joules. Fig 5 clearly shows that in the conventional system, since the query is fragmented into smaller parts so the energy of the nodes will be more as compared to the energy that is retained by the node in the proposed method.

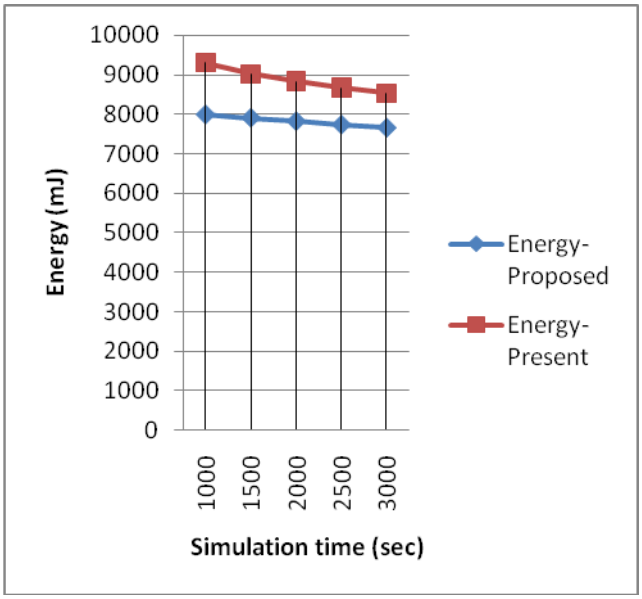

Figure 6: Energy left by the node Vs Simulation Time

Latency: Latency is defined as the amount of time for the packet to traverse from source to destination. Latency in secured VANET increases with time due to more number of queries and route processing. But as paths are updated with constant rate, in proposed system latency is consistent over time. Increase in latency is again attributed due to

encryption-decryption of RREQ packets and route updates. In fig 6, the graph shows that the latency for the proposed algorithm is lower as compared to the present system. The present system does not fragment the query into smaller parts.

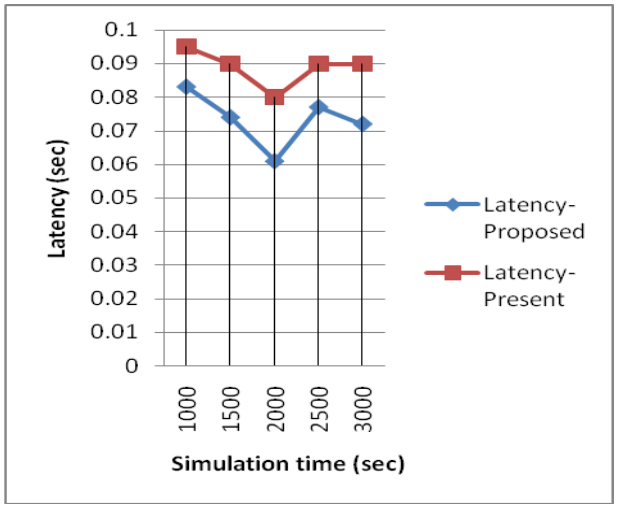

Figure 7: Latency Vs Simulation Time

6. Conclusion

VANET now has become a popular architecture in urban traffic management and information mitigation. Vehicles loaded with GPS sensors now utilize navigation queries more than ever to find out the best route for a destination, route alert as well as to obtain traffic information. Due to increasing number of vehicles and low security capability of such dynamic nature network, such communication system presents great security threat. In this paper, a unique navigation system for VANET with strong authentication and encryption options are presented. The proposed model extends the conventional VANET with multi layer key based solution with the use of both symmetric keys and public key cryptography. The techniques like source node hiding and header encryption beside data encryption have been adopted. The routes are updated frequently in order to keep intruders at bay. Therefore the proposed system not only provides better security than the conventional VANET, it also improves the communication performance. The result also shows that the proposed system helps the vehicle traverse longer distance over time due to ideal navigational alert.

In future, the system can be extended by implementing multicast groups and extending peer based security techniques to group authentication schemes which will further reduce the communication overhead. The system can be extended suitably to deal with other types of attacks in the network.

References

[1] Rekha Patil., Pooja Aspalli, "Adaptive Probablistic Broadcasting in VANET", International Journal of Emerging Science and Engineering (IJESE), Volume-1, Issue-11, September 2013, ISSN: 2319–6378, pp 1- 5.

[2] Ram Shringar, Raw Manish Kumar, Nanhay Singh, "Security Challenges, Issues and Their Solutions for VANET", International Journal of Network Security & Its Applications (IJNSA), Vol.5, Issue.5, September 2013, pp 95- 105.

[3] 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", International Journal Of Scientific & Technology Research Volume 2, Issue 4, April 2013, ISSN: 2277-8616, pp 156-161.

[4] Brijesh Kumar Chaurasia, Shekhar Verma, "Infrastructure Based Authentication In VANETs", International Journal of Multimedia and Ubiquitous Engineering, Vol. 6, No. 2, April, 2011, pp 41-53.

[5] Surabhi Mahajan Prof. Alka Jindal, "Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks**",** International Journal of Computer Applications (0975 – 8887) Volume 1– No.20, February 2010, pp 17-21.

[6] Mina Rahbari and Mohammad Ali Jabreil Jamali, "Efficient Detection of Sybil Attack Based On Cryptography in VANET", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011, pp 185-195.

[7] Halabi Hasbullah, Irshad Ahmed Soomro, Jamalul-lail Ab Manan, "Denial of Service (DOS) Attack and Its Possible Solutions in VANET", International Scholarly and Scientific Research & Innovation 4(5) 2010, pp 348-352.

[8] Aswathy M C and Tripti C, "A Cluster Based Enhancement to AODV for Inter-Vehicular Communication in VANET", International Journal of Grid Computing & Applications (IJGCA) Vol.3, No.3, September 2012, pp 41-50.

[9] Vinh Hoa LA, Ana Cavalli, " Security Attacks And Solutions In vehicular Ad hoc Networks: A Survey ", International Journal on Ad Hoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014, pp 1-20.

[10] Namita Chandel, Mr. Vishal Gupta,"Comparative Analysis of AODV, DSR and DSDV Routing Protocols for VANET City Scenario", International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 2, Issue: 6, June 2014, ISSN: 2321-8169, pp 1380–1384.

[11] Vishal Sharma, Harsukhpeet Singh, Shashi Kant, "Challenging Issues in VANET Network and its Routing Algorithms- An Analysis", Proc. of Int. Conf. on Advances in Communication, Network, and Computing 2013, pp 48-51.

[12] D.Sujeetha, R. Saranya, "Key Revocation for Secure Vehicular Ad Hoc Network", International Journal of Engineering Science and Innovative Technology (IJESIT)", Volume 3, Issue 1, January 2014, ISSN: 2319-5967, pp 360-367.

[13] Ayonija Pathre, Chetan Agrawal, Anurag Jain, "Identification of Malicious Vehicle in VANET Environment from DDOS Attack", Journal of Global Research in Computer Science", Volume 4, Issue 6, June 2013, ISSN: 2229- 371X, pp 30-34.

[14] Su-Hyun Kim, Im-Yeong Lee, " A Secure and Efficient Vehicle-to-Vehicle Communication scheme using Bloom Filter in VANETs", International Journal of Security and its Applications, Volume 8, Issue 2, 2014, ISSN: 1738-9976, pp 9-24.

[15] Chenxi Zhang, Xiaodong Lin, Rongxing Lu, Pin-Han Ho, Xuemin (Sherman) Shen, "An Efficient Message Authentication Scheme for Vehicular Communications", IEEE Transactions on VEHICULAR Technology, Vol. 57, No. 6, November 2008, pp 3357-3368.

[16] Shruti Bandak, Rekha Patil, " Public Key Cryptography based Secured Dynamic Routing in VANET Time Stamp Based Key Management System", International Journal of Science and Research(IJSR), Volume 3, Issue 6, June 2014, ISSN: 2319-7064, pp 2213-2217.