RESEARCH ARTICLE OPEN ACCESS

Enhancing Stability and Privacy In Inter Vehicle Communication (IVC) Using Virtual-Id in Vehicular Ad-Hoc Network

Er. Varinderjit Singh [1], Mr. Karan Mahajan [2]
Student, M-Tech [1], Assistant Professor [2]
Department of Computer Science and Engineering
Global Institute of Management & Emerging Technologies
Amritsar (PUNJAB) - India

ABSTRACT
Vehicular Ad hoc Networks (VANETs) have come out as one of the attractive topic for researchers and automotive industries due to its remarkable prospective to recover traffic safety, efficiency and other added services. Computing real-time road situation is actually hard and it is not achieved with GPS. However, a malicious node can produce multiple virtual identities for transmitting forge messages using different forged positions. Though VANETs are themselves defenseless against attacks that can directly lead to the fraud of networks and then possibly aggravate big losses of time, money, and even lives. A malicious vehicle can spread false traffic information in order to force further vehicles and vehicular establishment to take incorrect decisions. There are a variety of techniques that can sense the attack but Security expert or forensic investigator examines the network traffic by the empirical knowledge. There is no rule to perfectly distinguish attack from network traffic. Thus, there is need of more efficient attack detection system which will analyze the network traffic and provide a security to the VANET network by detecting various attacks. It is observed that VANET is very useful and it is the demand of future as well. VANET can provide enormous benefits, if privacy is maintained. A technique is proposed through which when a node want to send a message to a destination and if it doesn't want to explore its identity as well as destination's identity then it must communicate first to the stable node (trusted node) and get a virtual id for that particular time period. Also a session key is provided for encryption of message to the source and decryption key to the destination for maintaining the confidentiality of the message. This approach provides privacy to the user and reduces the packet loss by a selfish node.

Keywords :- MANET, VANET, Key management, GPS, Opportunistic network.

I. INTRODUCTION

Vehicular ad hoc networks (VANETs) have a high degree of openness. Therefore, if a new vehicle node wants to access the network, we need to validate the vehicle node carefully to ensure the security of the entire networking. There are a large number of vehicle nodes, and the strange degree among the nodes is very high in VANETs. In addition, VANETs are human-oriented networks. All vehicle nodes in the VANET have the right to decide whether to accept a new node. [1]

VANET is an application of mobile ad hoc network. More precisely a VANET is self-organized network that can be formed by connecting vehicle aiming to improve driving safety and traffic management with internet access by drivers and programmers. Two types of communication are provided in the VANET. [5]

A vehicular ad hoc network (VANET) uses cars as mobile nodes in a MANET to create a mobile network. A VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. Automotive companies like General Motors, Toyota, Nissan, Daimler Chrysler, BMW and Ford promote this term.

II. INTELLIGENT TRANSPORTATION SYSTEM

In intelligent transportation systems, each vehicle takes on the role of sender, receiver, and router to broadcast information to the vehicular network or transportation agency, which then uses the information to ensure safe, free-flow of traffic. Vehicles must also be fitted with hardware that permits detailed position information such as Global Positioning System (GPS) or a Differential Global Positioning System (DGPS) receiver. Though it is safe to assume that infrastructure exists to some extent and vehicles

have access to it intermittently, it is unrealistic to require that vehicles always have wireless access to roadside units. Inter-vehicle, vehicle-to-roadside, and routing-based communications rely on very accurate and up-to-date information about the surrounding environment, which, in turn, requires the use of accurate positioning systems and smart communication protocols for exchanging information. In a network environment in which the communication medium is shared, highly unreliable, and with limited bandwidth, smart communication protocols must guarantee fast and reliable delivery of information to all vehicles in the vicinity. It is worth mentioning that Intra-vehicle communication uses technologies such as IEEE 802.15.1 (Bluetooth), IEEE 802.15.3 (Ultra-wide Band) and IEEE 802.15.4 (Zigbee) that can be used to support wireless communication inside a vehicle.

III. OPPORTUNISTIC NETWORK

A new network is invented or a class of delay tolerance network in which some device which is carried by the users in their daily life and can pass message when they get opportunity, hence network is called opportunistic network. It is formed by the nodes having capability to support this network, the nodes are connected wirelessly. The nodes are mobile or stable so no fixed infrastructure is present in this network and this network can work even in disconnected environment. Every node has a finite range in which they can communicate or can forward the message. A node can forward a message only when any other node comes in his range. The nodes have to store the message until another node is not come in his range. All nodes have to work in the store-carry-forward manner in this network. In this network, group of intermediate nodes help to send a message from source to destination. Nodes have no predefine topology of the network, two node might be or never connected, no fix route between two node is use to send message. Network topology may change due to activation and deactivation of the node. If destination node is not in the range of source node then it passes the message to the nearest node in its range and so on node by node closer to the destination. This network is very easy to implement in any situation or any environment like war and disaster prone areas where communication is for short time and needs very quickly. In such environment we have less time to implement the network topology or to make an infrastructure. At such a location or time this network is very useful to facilitate the user to communicate.

The various key terms used in an opportunistic network are as follows:-

- Nodes
- Information sprinkler
- Find Opportunity
- Message Exchange

IV. PROBLEM FORMULATION

VANETs have a high degree of openness. Therefore, VANET needs face a diverse of security threats. Firstly, through accessing the VANETs, the attacker can conduct privacy spy and obtain the moving track of the vehicles. Secondly, some attackers release some false news (such as traffic accidents, road congestion, etc.), and the false news can lead to disordered traffic and accidents. What is more, the openness and highly dynamic of VANETs make the malicious attacks easy to implement and difficult to detect. Due to the application characteristics and application scenarios of VANETs, these attacks can threat the information security and the property safety of users. Therefore, how to accurately authenticate the new accessing vehicle node is becoming an urgently required research problem. Current trust management researches are focused on message evaluation and user privacy protecting. The message evaluation can stop delivering of false message and enhance the security of VANETs. In VANET scenario, privacy is the main concern and in this network there is no fixed infrastructure is present and the message is forward through many intermediate nodes, there may be a selfish node which is not interested to forward the message to a particular destination, or the user doesn't want to show his identity when want to communicate or send message to a particular destination, then it is risk to the privacy of user or the packet dropped by the selfish node.

Also the content of message is also access by the intermediate nodes, so there is a problem that how to encrypt the message and share a key between source and destination without showing it to intermediate nodes. As no fixed infrastructure is available in VANET and nodes keep on moving, the message has to be travel through number of intermediate nodes which are responsible for transmission of message from source to destination. So, precautions must be taken which guarantees that the message will be transferred through a secure path without any harm. So to achieve this, there must be some mechanism which ensures that the path is reliable and secure to transfer data. The method to achieve this surety is to examine the node(s) within the path. This can be attained through a concept of token/ virtual ID which a node will exchange with other node(s). This ID will help to authenticate the node and helps the transmitter node to decide whether to transfer data to that particular node or not. The aim of the implementing privacy in the VANET is to attract more users to use this network. As privacy is the main

concern and in this network there is no fixed infrastructure is present and the message is forward through many intermediate nodes, there may be a selfish node which is not interesting to forward the message to a particular destination, or the user doesn't want to show his identity when want to communicate or send message to a particular destination, then it is risk to the privacy of user or the packet dropped by the selfish node. Also the content of message is also access by the intermediate nodes, so there is a problem that how to encrypt the message and share a key between source and destination without showing it to intermediate nodes.

Steps of Problem Formulation:

- **i.** No Fixed Infrastructure is present.
- **ii.** Message is passes through many intermediate nodes.
- **iii.** Intermediate nodes may or may not forward the message i.e. risk of loss of packet.
- **iv.** Message should be kept secure from intermediate nodes.
- **v.** Use of key between Source and Destination to secure data.

V. METHODOLOGY FOLLOWED

For the whole implementation Network Simulator Version 2(NS-2) will be used. For this NS -2 has to be installed .So, I have to install LINUX because NS-2 works on LINUX. There are different versions of NS-2 available. I have used Network Simulator Version 2.34.

VI. PROPOSED WORK

As, it is cleared from my objectives that a new technique is to be proposed that can improve the security level in VANET through virtual ID concept. This concept helps to authenticate node(s) within the network for reliable/ secure transmission of data.

VII. IMPLEMENTATION STEPS

1. The network is initialized with the limited number of nodes. 13 nodes will be used in this execution. Every node has a range in which it can communicate with other nodes. All nodes are mobile and can change their location except stable node. In this implementation, only three nodes can move and all the other nodes are fixed in the scenario.

2. The whole network is divided into clusters. As clustering provides better network which can perform accordingly. Cluster based networks are easy to handle and troubleshoot. Network of 13 nodes are divided into 2 clusters. Every cluster has a stable node which is directly connected with the stable node of other cluster.

3. In each cluster fixed node is defined. In every cluster there is a fixed node called stable node or sprinkler node. Features of this node are same as the other node. It also transfers a message only when other nodes come in its communication range.

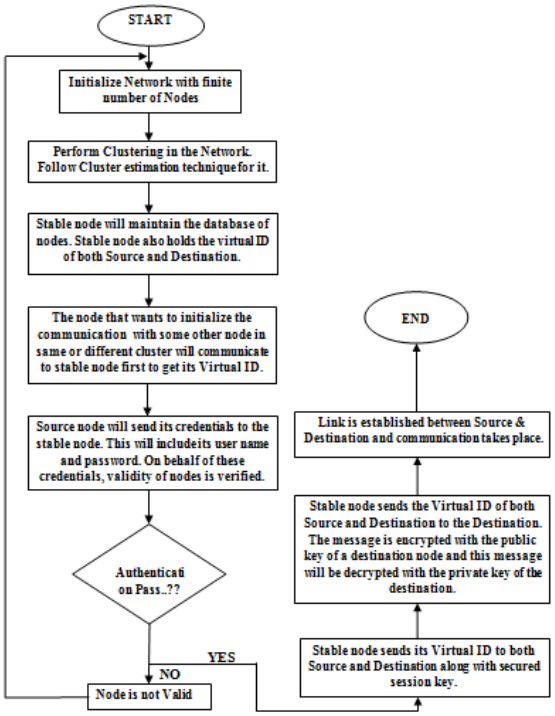
4. Every fixed node is responsible for maintaining the database. In this database ID and password of each node is stored. Whenever node initializes its operation, authentication of node is performed on behalf of stored database.

5. The node which wants to communicate to the other node will first communicate to get the virtual ID. When a node wants to send message, it first sends a request message to the node to get a virtual ID.

6. The source node sends its credentials (USER_NAME & PASSWORD) which authenticate the validity of a node. The source node also sends the destination node ID to which it want to send the message. This message is encrypted by the public key of stable node which is visible to all nodes.

7. When credentials are verified, node communicate with the cluster in which destination is present and will send the virtual ID's of the source and destination, to the source node along with the secure session key. Once the source node authenticates the user then information exchange takes place. Now node of source cluster will sends a new virtual ID to the source , new ID of destination and a session key with which the source node encrypt the message. This message is now encrypt by the public key of the destination node. Node also sends a new virtual ID to the destination, virtual_ id of source node and session decryption key. This message is decrypted by the private key of destination node.

8. Source node now send message with new ID and encrypt the message with session key.



Flowchart 1- Proposed Methodology

VIII . SIMULATION & RESULTS

The simulation setup is done in NS2. Fig 1 shows the basic setup of scenario. Here, in this setup thirteen nodes are deployed. These nodes are place in two clusters. As discussed in the methodology that the actual transmission takes place through stable nodes. So, in both clusters one stable node will be deployed. Only one stable node of a cluster can communicate to the other stable node of another cluster. So, every node of a cluster which wants to communicate anywhere have to go through this stable node. In short, only stable node is authorized to perform the actual transmission by validating nodes through its credentials User name and password).

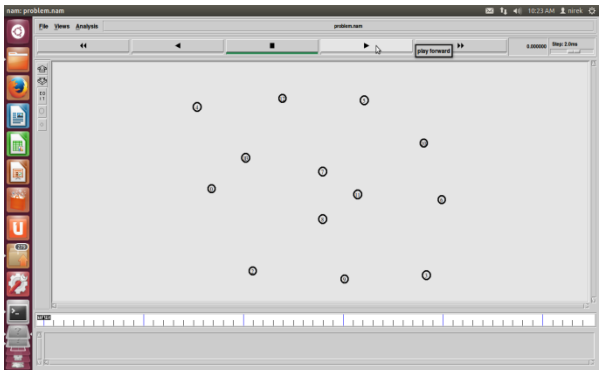


Fig. 1- Basic setup

Fig. 2 shows the placements of nodes. In this fig. node 0 is acting as a source node where as node 11 is acting as a destination node. There are two stable nodes i.e. node 2 and node 9. This means that there are two clusters. Node 2 is acting as stable node for cluster 1 and node 9 is acting as a stable node of another cluster.

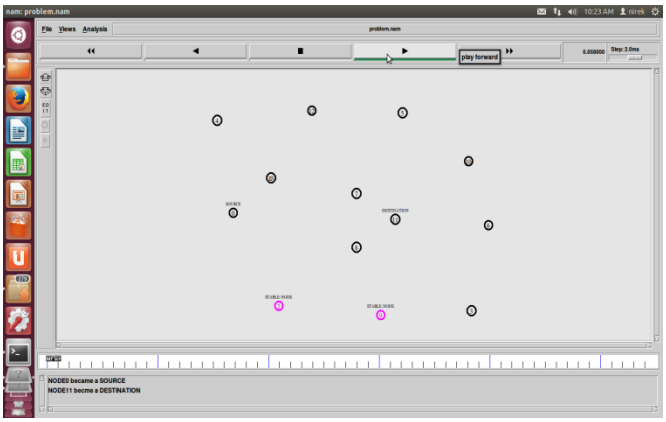


Fig. 2- Source, destination and stable nodes

This is a basic scenario under which concept of a virtual ID is not used. The data is exchanged without virtual ID. So, this is insecure and there are certain chances that the data will be lost. In fig. 3 data is storing by the node 113. This node will keep on collecting data. After it collected the whole data it will change its position to transfer to another node. If this node is malicious or selfish then it will drop all the packets. As no credentials were checked before transmission. So, there are chances that the data will never reach to the destination.

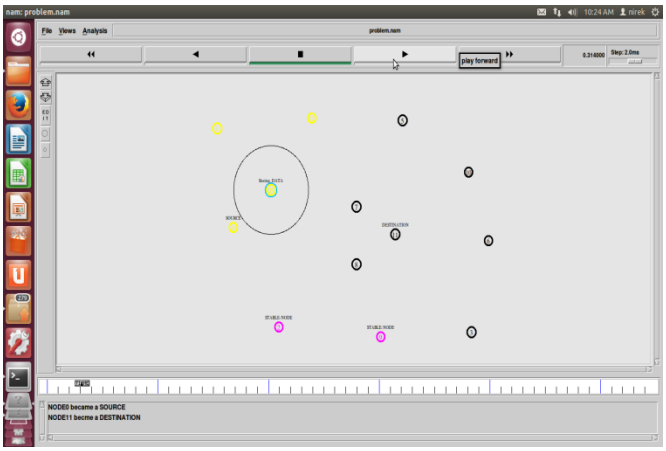


Fig. 3- Storing data

Fig. 4 depicts that the stored data by node 13 is lost. It drops all the packets at an extreme rate. This is a major issue that must be discussed that if data is forwarded to some node in the network without verifying its credentials then the loss of data must be there because there are certain chances that the node to which data is forwarded is a selfish node.

In fig. 5, node 4 which is a source node is requesting for a ticket from its stable node and after verifying its credentials stable node will generate one virtual ID and assign it to node 4. The virtual ID will be generated only after verifying the authentication of the source node. In fig 6, it is represented that after authentication and assigning of virtual ID source is transferring its data to node 1. Node 1 keeps on storing the information. In the next fig. 5.7 node 1 after storing data forwarded it to the destination i.e. node 10.

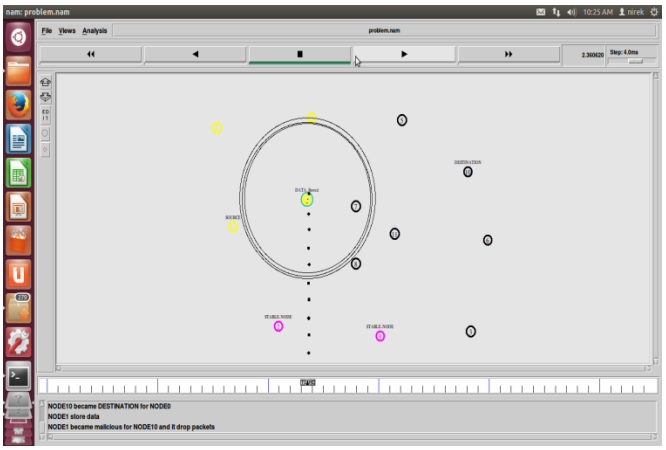


Fig. 4- Packet Drop

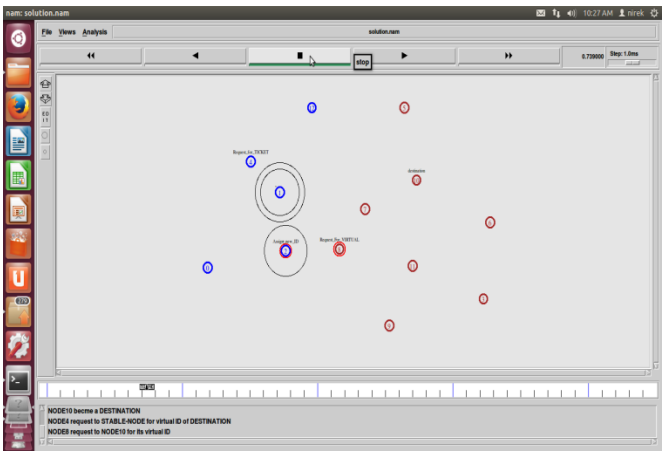


Fig. 5- Assigning of ticket/ virtual ID

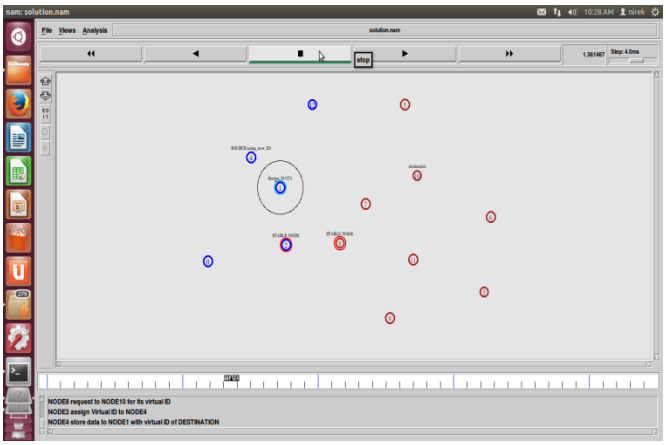


Fig. 6- Transferring data

Fig. 8 shows the graph of delay in which a delay of packet transmission is shown. This fig. depicts the both cases of the scenario and evaluates the delay of packet during transmission without introducing virtual ID concept and after introducing virtual ID concept.

Fig. 7- Data reached to destination

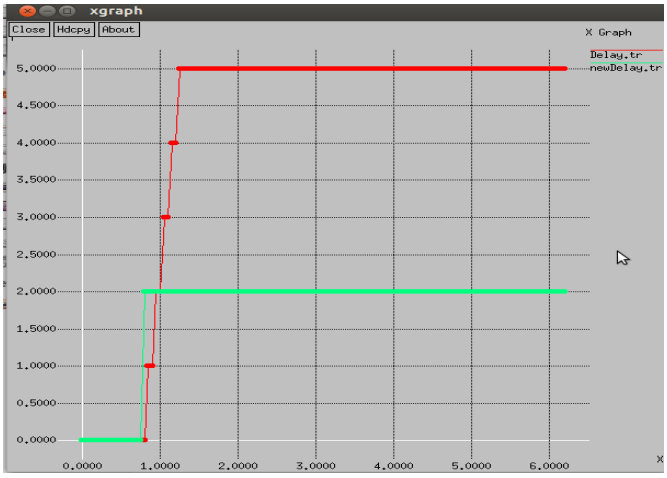


Fig. 8- Delay graph

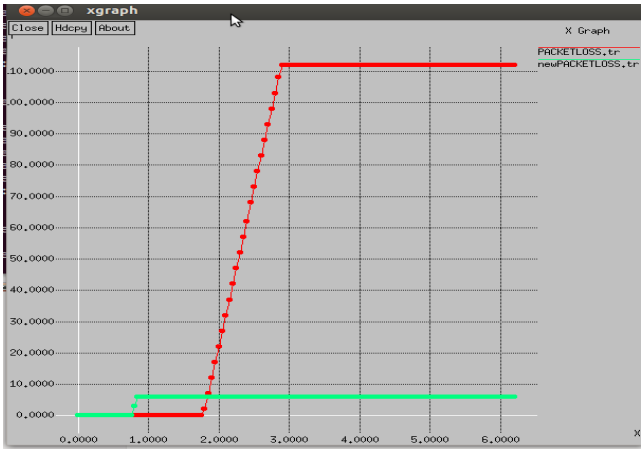


Fig. 9- Packet loss graph

When virtual ID is not used and data transferred without authenticating node, then the packet loss occur and data is delaye. After authentication and following proper channel the delay is reduced and performance is increased. Fig. 5.10 reflects the packet loss graph in which the effect of packet loss is shown. When the packet loss is more, that it is confirmed that the throughput of the network will be highly affected. In second case which is shown in green color reflects the loss of packet is reduced. This loss will takes place due to some failure in network not by selfish node of any false activity.

In Fig. 10 throughput of network is shown. This throughput graph shows throughput of the network when transmission is done without exchanging tickets and when it is done after generating virtual ID. If delay and packet loss is reduced, the throughput of network will be improved.

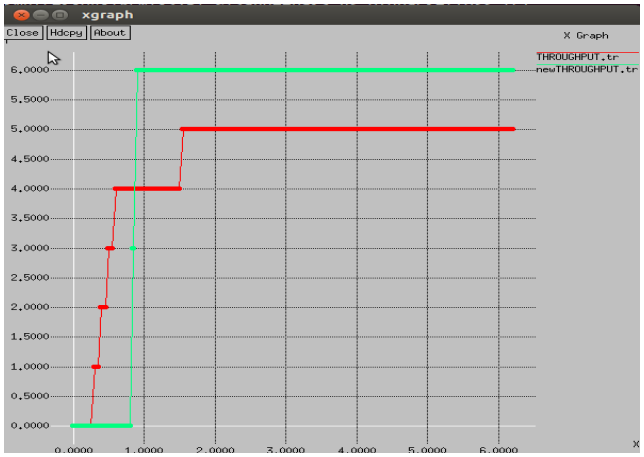


Fig. 10- Throughput graph

IX. CONCLUSION

There are a variety of techniques that can sense the attack but Security expert or forensic investigator examines the network traffic by the empirical knowledge. There is no rule to perfectly distinguish attack from network traffic. Thus, there is need of more efficient attack detection system which will analyze the network traffic and provide a security to the VANET network by detecting various attacks. From the research, it is observed that VANET is very useful and it is the demand of future as well. VANET can provide enormous benefits, if privacy is maintained. A technique is proposed through which when a node want to send a message to a destination and if it doesn't want to explore its identity as well as destination's identity then it must communicate first to the stable node (trusted node) and get a virtual id for that particular time period. Stable node act as special node, which contains information of every node of the cluster and authenticate the nodes which needs to communicate and provide virtual ID to that node. And also a session key is provided for encryption of message to the source and decryption key to the destination for maintaining the confidentiality of the message. This approach provides privacy to the user and reduces the packet loss by a selfish node. And the graphs represent the change in packet loss, delay and throughput of VANET.

X. FUTURE SCOPE

In the research, a technique is proposed which provide privacy to a user in VANET on the basis of virtual ID provided by a stable node, which is present in every cluster. But this technique increases the work load of a sender who

wishes to communicate. For future work, a new mechanism can be proposed which can hide the ID of user to maintain network security.

REFERENCES

[1] Ao Zhou et al., "A security authentication method based on trust evaluation in VANETs', EURASIP Journal on Wireless Communications and Networking, Springer, **DOI 10.1186/s13638-015-0257-x, 2015**, **pp 1-8.**

[2] Divya Chadha, Reena, "Vehicular Ad hoc Network (VANETs): A Review", International Journal of Innovative Research in Computer and Communication Engineering, **2015**.

[3] Hamid Reza Arkian, Reza Ebrahimi Atani, Atefe Pourkhalili, Saman Kamali, "Cluster-based traffic information generalization in Vehicular Ad-hoc Networks", Elsevier **2014, pp. 197-207.**

[4] Ming-Chin Chuang and Jeng-Farn Lee, "TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks", IEEE, Volume: 8, Issue: 3, **2013, pp.749- 758.**

[5] Kamal Deep Singh, Priyanka Rawat and Jean-Marie Bonnin, "Cognitive radio for vehicular ad hoc networks (CR-VANETs): approaches and challenges", Springer, 2014:49 , **2015, pp. 1-25**

[6] Rasmeet S Balia, Neeraj Kumara, Joel J.P.C.Rodriguesb, "Clustering in vehicular ad hoc networks: Taxonomy, challenges and solutions", Elsevier, Volume 1, Issue 3, **2014, pp. 134-152.**

[7] Omar Chakroun, Soumaya Cherkaoui, "Overhead-free congestion control and data dissemination for 802.11p VANETs", Elsevier 2014, **pp. 123-133**.

[8] Diyar Khairi M S, Amine Berqia, "Survey on QoS and Security in Vehicular Ad hoc Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 5, **2015, pp- 42- 52.**

[9] Praveen G Salagar, Shrikant S Tangade," A Survey on Security in VANET', International Journal For Technological Research In Engineering, Volume 2, Issue 7, **2015, pp. 1397- 1402.**

[10] Jaydeep P. Kateshiya, Anup Prakash Singh, "Review To Detect and Isolate Malicious Vehicle in VANET", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 2, **2015, pp. 127-132.**

[11] Arif Sari, Onder Onursal, Murat Akkaya, "Review of the Security Issues in Vehicular Ad Hoc Networks (VANET)", Int. J. Communications, Network and System Sciences, 2015, pp **552- 566**.

[12] K. Maraiya, K. Kant, N. Gupta, "Application based Study on Wireless Sensor Network" International Journal of Computer Applications (0975 – 8887), Volume 21– No.8, **2006, pp. 9-15, 2006.**

[13] K. Maraiya, K. Kant, N. Gupta, "Efficient Cluster Head Selection Scheme for Data Aggregation in Wireless Sensor Network" International Journal of Computer Applications, Volume 23-No. 9, **2011.**

[14] K. Latif, A.Ahmad, N.Javaid, Z.A. Khan, N. Alrajeh, "Divide-and-Rule Scheme for Energy Efficient Routing in Wireless Sensor Networks" 4th International Conference on Ambient Systems, Networks and Technologies (ANT), **2013, pp. 340-347.**

[15] L. Tao, "Avoiding Energy Holes to Maximize Network Lifetime in Gradient Sinking Sensor Networks", Wireless personal communications, 70 (2), **2013, pp. 581–600**.

[16] Vinay Kumar, Sanjeev Jain and SudarshanTiwari, "Energy Efficient Clustering Algorithms in Wireless Sensor Networks: A Survey ",IJCSI International Journal of Computer Science , Issues, volume 8,Issue5, No 2, **2011, pp. 1694-0814.**

[17] Ebin Deni Raj, "An Efficient Cluster Head Selection Algorithm for Wireless Sensor Networks–Edrleach" IOSR Journal of Computer Engineering (IOSRJCE), volume 2, Issue 2, **2012**, **pp. 39-44.**

[18] Ewa Hansen, Jonas Neander, Mikael Nolin and Mats Bjorkman, "Efficient Cluster Formation for Sensor Networks", Malardalen Real-Time Research Centre, 2011 **pp. 1-8.**

[19] B. Amutha , M. Ponna vaikko ,N.Karthick and M. Saravanan, "Localization algorithm using varying speed mobile sink for wire", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.1, No.3, **2010.**

[20] Peyman Neamatollahi, Hoda Taheri, Mahmoud Naghibzadeh"A Hybrid Clustering Approach for Prolonging Lifetime in Wireless Sensor Networks"International Symposium on computer networks and distributed systems (CNDS), 2011, **pp. 170 – 174**.

[21] Abdullatif shikfa, Melek Onen and Refik Molva,

"Local key management in Opportunistic network". International Journal Networks and distributed Systems, Vol.9, Nos.1, **2012, pp. 97-116.**

AUTHORS PROFILE

Er. Varinderjit Singh is doing his M-Tech in Computer Science and Engineering from Global Institute Of Management And Emerging Technologies, Amritsar, PUNJAB. This paper is published as a Review paper of his M-Tech Dissertation. He is doing his thesis in VANET to enhancing the scalability and privacy of IVC.

Er. Karan Mahajan has done his M-Tech in Computer Science and Engineering from Lovely Professional University, Jalandhar, PUNJAB. He is working as Assistant Professor in Global Institute Of Management And Emerging Technologies, Amritsar, PUNJAB and he has four year teaching experience. His area of interst Cloud Computing, Mobile Computing and VANET