A novel approach to enhance the Security in Vehicular Ad-Hoc Network through Node Authentication using Hash Value and Steganography Schema

Ravinder Kaur
Department of CSE, Chandigarh Engg. College, Mohali, Punjab, India.

Dr. Neeraj Sharma
Head, Department of CSE, Chandigarh Engg. College, Mohali, Punjab, India.

Abstract – VANET is a vehicular ad hoc network where a short-lived network is formed among the VANET nodes. VANET nodes communicate and interchange messages with other vehicular nodes either in an infrastructure or infrastructure-less network. Due to lack of fixed infrastructure, VANET is prone to varied attacks. In impersonation attack, identity of the legitimate node is stolen by an attacker. In this paper, an enhanced level of security is implemented on the VANET system to reduce malicious activates into the network. Here the security is done by the authentication of individual node by some enhanced scenario which is based on the HASH value and steganography technique. Each vehicle will be authenticate by centralize authentication and it will helps to reduce the malicious activates.

Index Terms – VANET, HASH, RSU, V2V, V2I.

1. INTRODUCTION

Vehicular ad-hoc network are wireless networks where all the vehicles from the nodes of the network. It is for the driver comfort and road safety, the inter-vehicle communication provide them. Vehicular ad-hoc network is subclass of mobile ad hoc networks which provides a distinguished approach for intelligent transport system. It is very necessary for all the vehicles. Vehicular ad hoc network is special form of MANET which is vehicle to vehicle roadside wireless communication network [22]. It is autonomous and self-organizing wireless communication network, where all the nodes in VANET involve themselves as servers or client for exchanging and sharing information. The network architecture of VANET can be classified into three categories pure cellular, pure ad-hoc and hybrid [1].

The characteristics of this network are: wireless medium, mobile nature, high mobility, absence of infrastructure, high dynamic network topology [2].

One of the main areas of research studies of communication among the vehicles and road-side units more specifically the vehicular ad-hoc network (VANETS). In this network all the vehicles and elements of roadside infrastructure connected with each other without requiring an underlying infrastructure, send and receive information and give warning about current traffic situation. In today era used Wi-Fi IEEE 802.11 based technology [3] it is very commonly used for deploying VANETs. All the vehicles connected with the wireless network interface it can be use either 802.11b or 802.11g are the two standards for access media. These standards are general purpose standards and they do not fit properly the requirements of high dynamic network such as VANETs. [4]. Over the last few decades, many researches and efforts have been done to investigate various issues related to V2I, V2X areas. Several approaches to deal with identification of the node and its authentication in VANET have been proposed in the literature. Norbert Bibmeyer [10] et al proposes a scheme based on data plausibility check that ensures positional reliability in order to assess the trustworthiness of the neighboring node. S. RoselinMary [3] et al proposes an attacked packet detection algorithm to detect the position of the vehicle and checks whether the packet sent by the vehicle has been attacked or not.

The proposed scheme floods the beacons into the network to discover the presence of the neighboring vehicles and accurate position of the messaged vehicle is detected. It verifies theMD5 hashes assigned to the VANET nodes and once a malicious node is detected, warning message will be broadcasted to all the trusted VANET nodes and the malicious node is isolated from the communication environment. Authentication is done through VANET Content Fragile Watermarking. In this paper we focus on security, faulty node detection and authentication schemes. A city scenario is considered with 10 vehicles and 3 RSUs and it is further analyzed on the basis of various performance metrics.

2. LITERATURE SURVEY

Rakesh Kumar and MayankDav (2012) there are so many types of VANET applications and their communication protocol needs a systematic literature survey. In this paper mainly define the VANET applications based on the various broadcasting data dissemination protocols are surveyed separately and their fundamental characteristics are revealed. At the end of this paper comparison of all the protocols [8].

Aswathy M and Tripti represent a paper in (2012) this paper defines the vehicles on road as nodes of network. With the help of VANET give us many applications as an intelligent transportation system. In the dynamic network architectures and node movement characteristics differentiates VANETs from other kind of ad-hoc networks. The dynamic change in topology shortens the effective time of routing. Routing in the VANET is quite complicated task. AODV (ad-hoc on demand distance vector) mostly used in the topology based routing protocol for VANET [23]. This paper main aim to improving the performance of AODV by enhancing the existing protocol by creating stable clusters and performing routing by cluster head and gateway nodes [18, 21].

Patil V.P (2012) in this paper suggest more innovative approach to deal with this traffic congestion problem using the characteristics of vehicular ad-hoc networks (VANET). This system is developed and tested using the AODV protocol ad-hoc mobile network to deal with the problem of vehicle traffic congestion in vehicular network. Traffic congestion can be measured on following patterns like packets broadcast, percentage of packet delivered and percentage of traffic diverted and overhead to manage the problem of data traffic in the network. In the main simulation shows the domain of vehicle traffic congestion in VANET is demonstrated [5].

In year 2012, Miguel Sepulchre performed a work on V2V communication based on cooperative safety applications. The work is about the study of network respective to time and space analysis between the vehicle movement. The work includes the driver based analysis in real world with effect of cooperative system to achieve the network security [13].

In Year 2012, KeyvanGolestan presented a work on Vehicle Localization. The work is the analytical study of different techniques of localization along with data Fusin as well as vehicle-to-vehicle communication and to integrate the available data and improve the accuracy of the localization information of the vehicle [14].

In year 2012, R.K.Chauhan1, ArzooDahiya On demand set up, fault tolerance and unconstrained connectivity are the major advantages of mobile computing, and that's why it continues to enjoy rapid growth. In last three decades, tremendous improvement is made in the area of wireless adhoc network. Now a days, one of the most attractive research topic is inter vehicle communication i.e. realization of mobile adhoc network VANETs have been attracting an increasing attention from both industry as well as research communities. Therefore, this paper proposes a scheme that avoids the delay of communication that occurs due to frequent disconnection in routing. For this, the meta heuristic search i.e. ant colony optimization is combined with AODV and route repair strategy is applied to ACO [17].

In year 2012, Lucas **Wang** has performed a work on rapid traffic information using named data. The author has presented a simple traffic information dissemination application for previous work and to evaluate its performance through the simulation. The simulation results are presented under distance and density parameters [15].

3. PROBLEMS WITH EXISTING SYSTEM

As we know VANETs work on the basis of real time system where the vehicles are moving nodes and travel with authentication, tunnel attacks, intelligent system approach, collision detection, congestion avoidance, communication system approach etc

The present work is presenting an intelligent route identification approach in case of accident occurrence for V2V communication. The intelligent vehicles are been defined respective to distance, direction and speed analysis. If some accident over the network, the neighbor node information flow will be performed the route analysis. In this work a bio inspired V2V communication approach is been suggested to identify the safe path over the network. Ii is based upon clustering, ACO and reliable packets and uses different trust metrics.

Table 1: Different trust metrics

Traffic Rule Obey (TRO)
Data Packet Forwarded (DPF)
Data Packet/Message Procession (DPP)
Control Packet Forwarded (CPF)
Control Packet/Message Procession (CPP)

In this method they make a clustering of vehicles and choose path through ACO and the paths should be based upon the reliable packets if the packets are not look to be reliable then the vehicles will do not do trust on them and drop them. VANETs as any other communication network require a set of security and privacy needs to perform its functions correctly and a successful use.

In previous work it selects some random vehicles which will send hello message to another vehicles and from this process it will calculate the speed and distance between vehicles.

Suppose if the speed difference between two vehicles is more than their distance will be more and it will be increase.

So here we use formula to calculate distance

Sqrt((x2-x1)^2+(y2-y1)^2)

After calculation the network is divided into 3 clusters. The cluster selection is done on the bases of direction, Speed and distance. Figure1 shows the clustering scenario. Here to calculate direction we find out the total distance travel by hello message from each random vehicle.

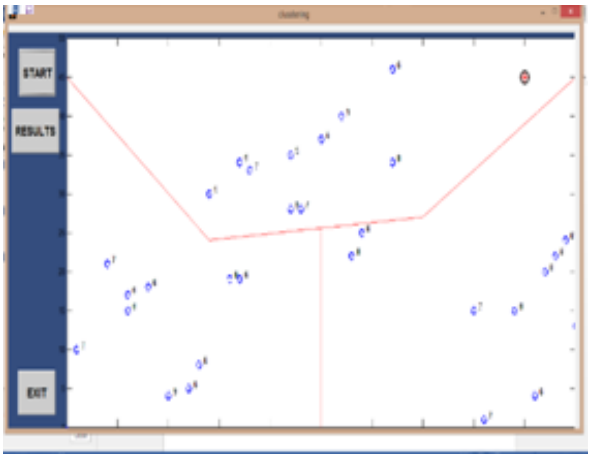

Figure 1: Clustering Scenario

So the minimum distance is from node 4 which is 80m. So here we can say that the node 4 is moving with respect to other nodes in same direction because if the direction will be opposite the distance should be more. The value which is assigned on each node is a trust value which will use for the cluster head selection. On the bases of trust value in each cluster 4 nodes will be selected which are having high trust value.

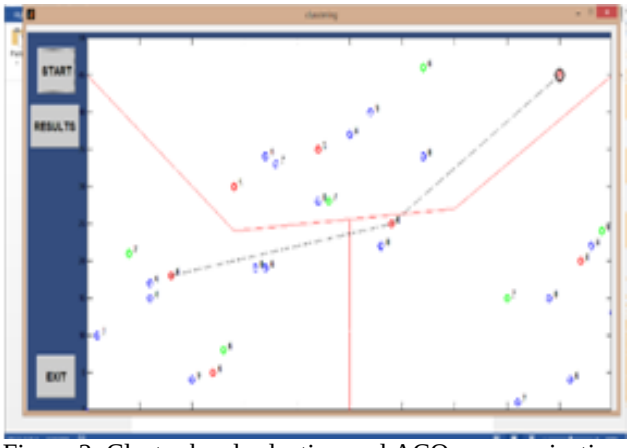

Figure 2: Cluster head selection and ACO communication

ACO is used for communication. It helps to select path. Now the communication will be on the bases of cluster heads only, means only cluster head to cluster head communication. So by using ACO we will select any random node as a cluster head from red nodes and start transmission up to RSU.

4. METHODOLOGY

In proposed work, we are providing security over VANET in terms of vehicle authentication, it means if a new vehicle want to be on VANET road it has to authenticated from centralize authentication, now the centralize authentication (CA) contain a hash value of every vehicle. This hash value is generated from the license number which is an individual govt. identity of a person and a city code. Impersonation can be detected on the basis of location. There are two postulates in which states that two vehicles cannot occupy the same space at the same time and one vehicle can occupy only one space at a given time. As we know that the attacker can also hack this hash value, so to make it more complex we will add image steganography and image compression techniques in it. At user end we will calculate the hash value and then store it into image using image steganography and after that apply image compression on it to reduce its size. Than user will send this compressed image to CA. now CA have its own database and it will extract hash value from image and compare it with its database values. If the value is matched it means it's a valid vehicle otherwise its some malicious vehicle so in that case it will inform to all road side units so that other vehicles can isolate it.

There are two types of methods used to enhance the security in vanet through node authentication.

- Generation of Hash Value
- Steganography Technique

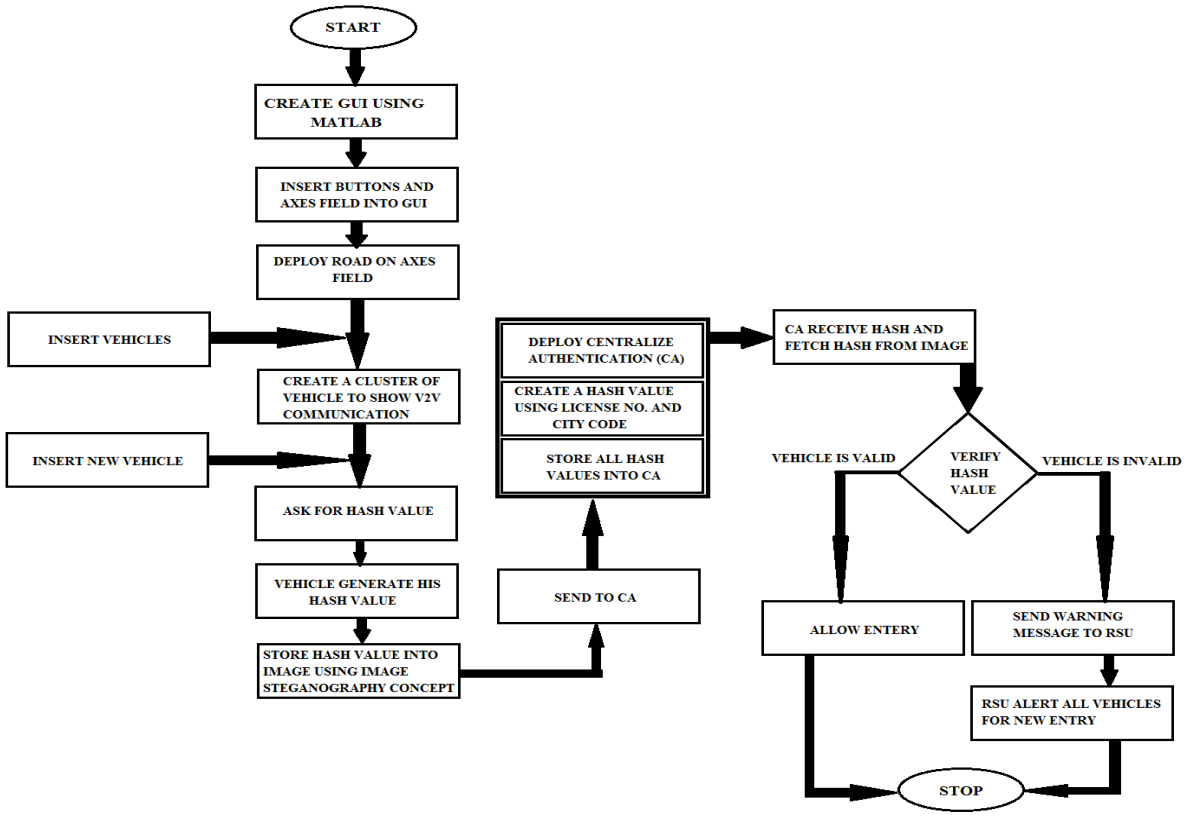

Figure 3: Working Schema

4.1 GENERATION OF HASH VALUE

Hash value is related to cryptography. Here the purpose of hash value is to combine two meaningful values in such a way so that it will appears as meaningless value. The steps to generate the hash value are as follows:-

1. Take first value.
2. Take second value.
3. Apply operation on operands.
4. Generate HASH value.

4.2 STEGANOGRAPHY TECHNIQUE

Subtraction steganography technique is used which will work as the following:-

i. Take a random image.
ii. Use imread() function to show the color values of image.
iii. Convert color values into binary numbers.
iv. Now take a HASH.
v. Generate corresponding binary numbers
vi. Now subtract binary numbers from image same as HASH value.
vii. Now insert HASH's binary number into image.
viii. Use imshow() function to show image again.

4.3 PSEUDO CODE FOR THE PROPOSED SYSTEM

- Create GUI using MATLAB
- Insert buttons and axes field into GUI
- Deploy road on axes field
- Insert vehicles into road
- Create a cluster of vehicle to show V2V communication
- Deploy centralize authentication (CA)
- Create a hash value using license number and city code
- Store all hash values into CA
- Insert new vehicle
- Ask for hash value to new vehicle
- Vehicle generate his hash value
- Store hash value into image using image steganography concept
- Send to CA
- CA receive hash and fetch hash from image
- Verify hash value
- Vehicle is valid

- Vehicle is invalid
- Send warning message to RSU
- RSU alert all vehicles for new entry

5. SIMULATION & RESULTS

The whole simulation has been take place in MATLAB environment. Below figures shows the implementation results of the proposed schema.

5.1. Cluster Creation Time

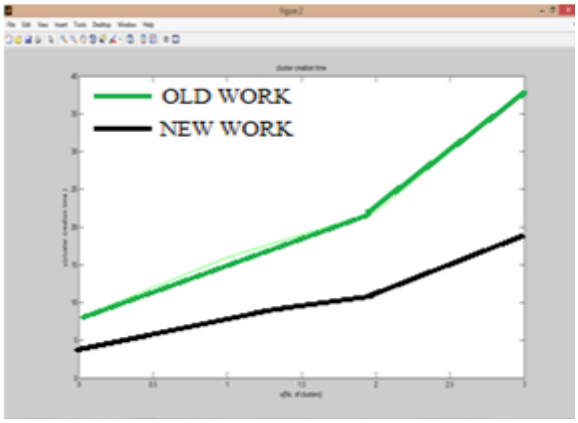

Figure 4: Cluster Creation Time

The figure 4 shows the comparison between both cases for the cluster creation time and here the black curve represents the cluster creation time for new case and green curve shows time for old case and its clearly shown that time taken for cluster creation in proposed work is less than existing work.

5.2. Cluster Head Selection Time

The figure 5 shows the cluster head selection time in proposed system is less because the system is providing the security through authenticate the node. The cluster head selection time depends upon the different cluster size by varying the number of clusters.

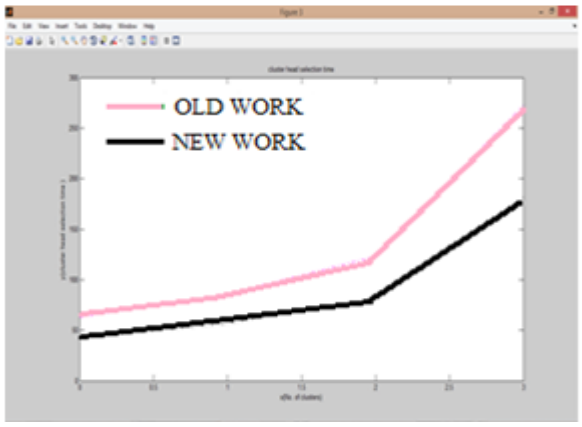

Figure 5: Cluster Head Selection Time

5.3. Throhghput

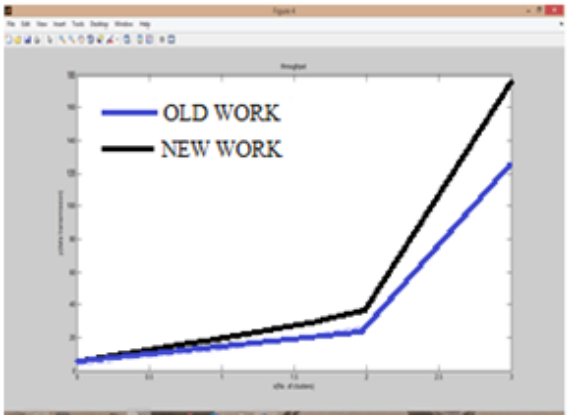

Figure 6: Throughput of systems

The Figure 6 represents the throughput comparison of both cases. Black curve represent throughput for new case and blue curve represent throughput for old case. And here from comparison it's clear that new case is having high throughput then old case.

5.4. Routing Overhead

The figure 7 represent overhead between two systems and the routing protocol is defined as the control messages per number of data packets successfully received at the destinations. Here the simulation shows that AODV routing overhead increases less as compared to TACR routing overhead. The overhead in proposed work is less the previous work.

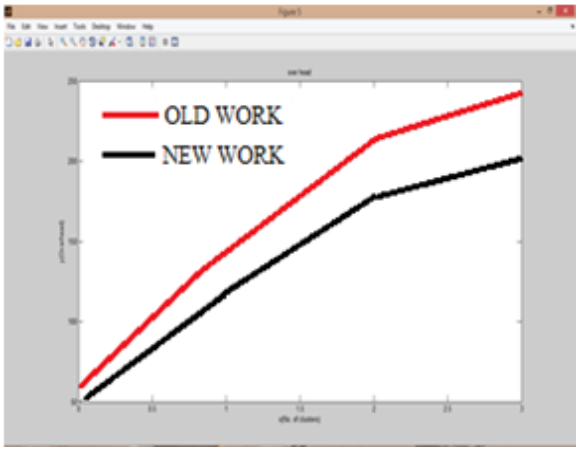

Figure 7: Routing Overhead

6. CONCLUSION & FUTURE SCOPE

Detection of the attackers is an important requirement for the trustworthy communication among VANET network nodes. In this paper, an enhanced level of security is implemented on

the VANET system to reduce malicious activates into the network. Here the security is done by the authentication of individual node by some enhanced scenario which is based on the HASH value and steganography technique. Each vehicle will be authenticate by centralize authentication and it will helps to reduce the malicious activates. In the future work, improvement over the method would be done to conduct more simulation experiments to ensure the effectiveness of the proposed method.

REFERENCES

[1] V. Lakshmi Praba, "Isolating Malicious Vehicles and Avoiding Collision between Vehicles in VANET," International conference on Communication and Signal Processing on IEEE, 3-5 April 2013, pp. 811-815.

[2] Mohammed ERRITALI, Bouabid El Ouahidi, "A Review and Classification of Various VANET Intrusion Detection Systems," IEEE, 26-27 April 2013, pp. 1-6.

[3] S. RoselinMary, M. Maheshwari, M. Thamaraiselvan, "Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA)," IEEE, 21-22 February 2013, pp. 237-240.

[4] Dimitris Glynos, Panayiotis Kotzanikolaou, Christos Douligeris, "Preventing Impersonation Attacks in MANET with Multi-factor Authentication," WIOPT'05 Proceedings of the Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, 2005, pp. 59-64.

[5] PATIL V.P.Smt. Indira Gandhi college of Engineering, New Mumbai, INDIA,"Vanet Based Traffic Management System Development AndTesting Using Aodv Routing Protocol" (2012) 1682-1689.

[6] Rasmi Ranjan Sahoo, Rameswar Panda, Dhiren Kumar Behra, Mrinal Kanti Naskar, (2012) "A trust based clustering with ant colony routing in vanet.

[7] Irshad Ahmed Sumra, Iftikhar Ahmad, Halabi Hasbullah, "Behavior of Attacker and Some New Possible Attacks in Vehicular Ad hoc Network (VANET),"Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011 3rd International Congress on IEEE 5-7 Oct. 2011, pp. 1-8.

[8] Rakesh Kumar and Mayank Dave Department of Information Technology, M. M. University, Mullana, Haryana, India Department of Computer Engineering, N. I. T. Kurukshetra, Haryana, India,"A Review of Various VANET Data Dissemination Protocols"(2012) p1-8.

[9] Md. Mashud Rana, Khandakar Entenam Unayes Ahmed, Nazmur Rowshan Sumel, Md. Shamsul Alam, Liton Sarkar, "Security in Ad Hoc Networks: A Location Based Impersonation Detection Method," IEEE International Conference on Computer Engineering and Technology, vol. 2, January 2009. pp. 380-384.

[10] Norbert Bibmeyer, Sebastian Mauthofer, Kpatcha M. Bayarou, Frank Kargl, "Assessment of Node Trustworthiness in VANETs Using Data Plausibility Checks with Particle Filters," IEEE Vehicular Networking Conference (VNC), 14-16 November 2012. pp. 77-85.

[11] Wei-Fan Hsieh, Pei-Yu Lin, "Analyze the Digital Watermarking Security Demands for the Facebook Website", IEEE Sixth International Conference on Genetic and Evolutionary Computing, 25-28 August 2012. pp. 31-34.

[12] Rodrigo Fonseca, Sylvia Ratnasamy, Jerry Zhao, Cheng Tien Ee, "Beacon Vector Routing: Scalable Point-to-point Routing in Wireless Sensornets," NSDI'05 Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation, vol. 2, 2005, pp. 329-342.

[13] Miguel Sepulcre (2012) ,"Experimental Evaluation of Cooperative Active Safety Applications based on V2V Communications", VANET'12, June 25, 2012, Low Wood Bay, Lake District, UK.

[14] KeyvanGolestan (2012),"Vehicle Localization in VANETs Using Data Fusion and V2V Communication", DIVANet'12, October 21–22, 2012, Paphos, Cyprus, pp 123-130.

[15] Lucas Wang (2012),"Rapid Traffic Information Dissemination Using Named Data", Mobility NoM'12, June 11, 2012, Hilton Head, South Carolina, USA, pp 7-12.

[16] Chao Song (2012),"Towards the Traffic Hole Problem in VANETs", VANET'12, June 25, 2012, Low Wood Bay, Lake District, UK, pp 139-140.

[17] R.K.Chauhan1, ArzooDahiya, Deptt. of Computer Science and Applications, Kurukshetra University, Kurukshetra, Journal of Emerging Trends in Computing.

[18] Aswathy M and Tripti Department of Computer Science & Engineering, Rajagiri School of Engineering & Technology, Rajagiri valley, Cochin, India," A CLUSTER BASED ENHANCEMENT TO AODV FOR INTER-VEHICULAR COMMUNICATION IN VANET"(2012) p41-50.

[19] Chen Lyu, Dawu Gu, Xiaomei Zhang, Shifeng Sun, Yingi Tang, 2013, "Efficient, Fast and Scalable Authentication for VANETs," IEEE Wireless Communications and Networking Conference, 7-10 April 2013, pp. 1768-1773.

[20] Noriaki Tanabe, Eitaro Kohno, and Yoshiaki Kakuda, "An Impersonation Attack Detection Method Using Bloom Filters and Dispersed Data Transmission for Wireless Sensor Networks," IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing, 20-23 November 2012. pp. 767-770.

[21] Ramakrishnan, B., R. S. Rajesh, and R. S. Shaji. "CBVANET: A cluster based vehicular adhoc network model for simple highway communication."International Journal of Advanced Networking and Applications 2.04 (2011): 755-761.

[22] Ramakrishnan, B., R. S. Rajesh, and R. S. Shaji. "An efficient vehicular communication outside the city environments." International Journal of Next-Generation Networks (IJNGN) Vol 2 (2010).

[23] Ramakrishnan, B., R. S. Rajesh, and R. S. Shaji, "Performance Analysis of 802.11 and 802.11p in Cluster Based Simple Highway Model", International Journal of Computer Science and Information Technologies, Vol. 1 (5) , 2010, 420-426.

Authors

Ravinder Kaur presently is a PG scholar in Department of Computer Science, Chandigarh Engineering College,Punjab Technical University, Landran, Mohali. She received the B-Tech Degree in Information Technology from Punjab Technical University, Jalandhar, India in 2013. Her research area of interest is networking.

Dr. **Neeraj Sharma** received his B-Tech degree from MDU, Rohtak in 2001 and M.tech degree from MDU, Rohatk in 2007. He received PHD degree from NIMS University, Jaipur in 2012. Presently, He is a Head of Department (CSE) in Chandigarh Engineering College, Punjab Technical University, Landran, Mohali. His research area of interest is Wireless Ad-Hoc Network, Wireless Sensor Network, Software Define Network, MANETs.