A Node Authentication Mechanism to Enhance the Security in VANETs

Ravinder Kaur
Department of CSE, Chandigarh Engineering College Landran, Mohali, India

Dr. Neeraj Sharma
Head, Department of CSE, Chandigarh Engineering College Landran, Mohali, India

Abstract – As per today's scenario, wireless networks are becoming more popular day by day as it is difficult for people to constrain their needs to wired networking. VANET works on the basis of real time system where the vehicles move as nodes and travel with a very high speed on roads. There are many security issues like authentication, tunnel attacks, intelligent system approach, collision detection, congestion avoidance etc. A number of methods have been proposed to deal with various issues in VANET. In this paper, an enhance level of security is implemented on the VANET system to reduce malicious activities 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 and eye retina sample. Each vehicle will be authenticate by centralize authentication and it helps to reduce the malicious activities.

Index Terms – VANET, RSU, V2V, V2I, CA

1. INTRODUCTION

Vehicular Ad Hoc Network (VANETs) is a mobile network where a short lived and self-organizing network is formed among the vehicles. Network operates either in an infrastructure network (V2X) or in an infrastructure less network (V2V). In an infrastructure network, Road Side Units (RSUs) interacts with vehicles' wireless equipment in a sporadically mode when a vehicle passes by it. In an infrastructure less network, Vehicles communicate with other vehicles' on-Board Units (OBUs) to exchange security messages [21,22, 23]. Each vehicle is equipped with a set of sensors such as GPS, Radar, and Directional antenna [1]. Due to lack of fixed infrastructure, nodes are prone to varied attacks. Securing the communication among vehicles is the main challenge that lies in the vehicular network. Deployment of network intrusion detection system helps in identifying the attack taken place in vehicular network [3]. Nodes in VANET are subjected to various types of impersonation attacks, few of which are hard to deal with, even if any security mechanisms are enforced. Some of which are Sybil attack, stolen identity attack, Man-in-the-Middle attack. Identification of the node and its authentication are of fundamental importance within a secure network [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 [9] 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.

1.1. VANET Characteristics

As Vehicular ad hoc network share common properties with conventional ad-hoc sensor network such as self-organized and lack of central control. VANETs have unique challenges that impact the design of communication system and its protocol security. These Challenges include:-

1.1.1. High Mobility

Nodes potentially move with high speed so all the nodes are not able to interact properly with each other. Also, when vehicle pass each other, the duration of time remains for exchange of data packets is rather small.

1.1.2. High application requirement on data delivery

Most important applications of VANETs are for traffic safety to avoid road accidents, such as safety of life. The high requirements are with respect to real time and reliability.

1.1.3. Potentially high number of nodes

VANETs are based on intelligent Transportation System (ITS) that large area of vehicles will be equipped with communication capabilities for vehicular communication. In addition to road-side units into account, VANET needs to be scalable with a very high number of nodes.

1.1.4. Privacy and Authentication

A proper authentication system must be set up to ensure privacy in the networks. A system to ensure the authentication in VANET should be established which will also increase the throughput of the network.

1.2. Security and Privacy Needs of VANETs

VANETs as any other communication network require a set of security and privacy needs to perform its functions correctly and a successful use. Related to information security, there are some requirements:-

1.2.1. Confidentially

It ensures that messages will only be accessed by intended parties. It specifies that only the authorized users should be able to read the contents of information. It is required in some private services like location-based ones.

1.2.2. Data integrity

It ensures that they have not been altered since their creation means assets can be modified by authorized users only. A related need is data trust i.e. data are fresh, updated and reliable.

1.2.3. Authentication

One key aspect is the existing trade-off between liability and privacy. So, it is necessary not only to uniquely identify each communicating node, but also authenticate it. In this way, it is possible to determine the liability for a malicious action. A related security need is non-repudiation, which ensures that an entity performing an action will not be able to deny having done it.

1.2.4. Availability

It specifies that resources must be available to other nodes at all times that every node must be able to timely process and send the required information.

2. LITERATURE SURVEY

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]. 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].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]. 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. 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 [18,23]. 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 and 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].

3. PROBLEM FORMULATION

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. In the existing Research Algorithm, A clustering has been created by considering direction, position and relative speed of the vehicle for managing scalability issue and algorithm for selecting the most appropriate cluster head by considering real time updated position and trust value of vehicles**.** It is based upon clustering, ACO and reliable packets and uses different trust metrics. The intelligent vehicles are been defined respective to distance, direction and speed analysis. In this work a bio inspired V2V communication approach is been suggested to identify the safe path over the network. VANETs as any other communication network require a set of security and privacy needs to perform its functions correctly and a successful use. The existing work takes into account only trust metrics for cluster head selection and other parameters in order to ensure that whether selected node is a normal or malicious vehicle but it does not consider the security issues.

Traffic Rule Obey (**TRO**)
Data Packets Forwarded (**DPF**)
Data Packet/message Precession(**DPP**)
Control Packet Forwarded (**CPF**)
Control Packet/message Precession(**CPP**)

Table 1: Different trust metrics

The trust value of moving vehicle is being calculated in order to ensure whether the selected vehicle is normal or malicious vehicle. Trust defines the level of confidence of a vehicle depending on the performance evaluation of the assigned task. Trust value of a vehicle is time dependent i.e. trust value of vehicle will vary based on transaction performed.

4. PROPOSED METHODOLOGY

The proposed work considers an enhanced level of security of the VANET system to reduce malicious activities 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 and eye retina sample. Each vehicle will be authenticate by centralize authentication and it helps to reduce the malicious activities.

In proposed work, it provides 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 and eye retina sample. This hash value is generated from the license number which is an individual govt. identity of a person and a city code.

When a person will apply for license then the person must take his eye retina samples which will store in database of CA. 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 add image steganography and image compression techniques in it. At user end it 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. Then user send this compressed image and eye retina sample to CA. now CA have its own database and it will extract hash value from image and eye retina sample 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 inform to all road side units so that other vehicles can isolate it. If someone misplace his license number and other is going to use this then his eye sample will not match with this license number and he will be detected as malicious.

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

A) Generation of Hash Value

B) Steganography Technique

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 appear 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.

Hash value is used for accessing data or for security. A hash value is also called message digest. In proposed schema hash value is generated using license number and city code.

4.2. Steganography Technique

Steganography is a process of hide a secret message into an image. 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.

For eye retina sample, it converts the eye retina sample into numeric values and then store it into the variable and CA. When authentication take place it converts the eye retina samples into numeric values and compare it with CA values.

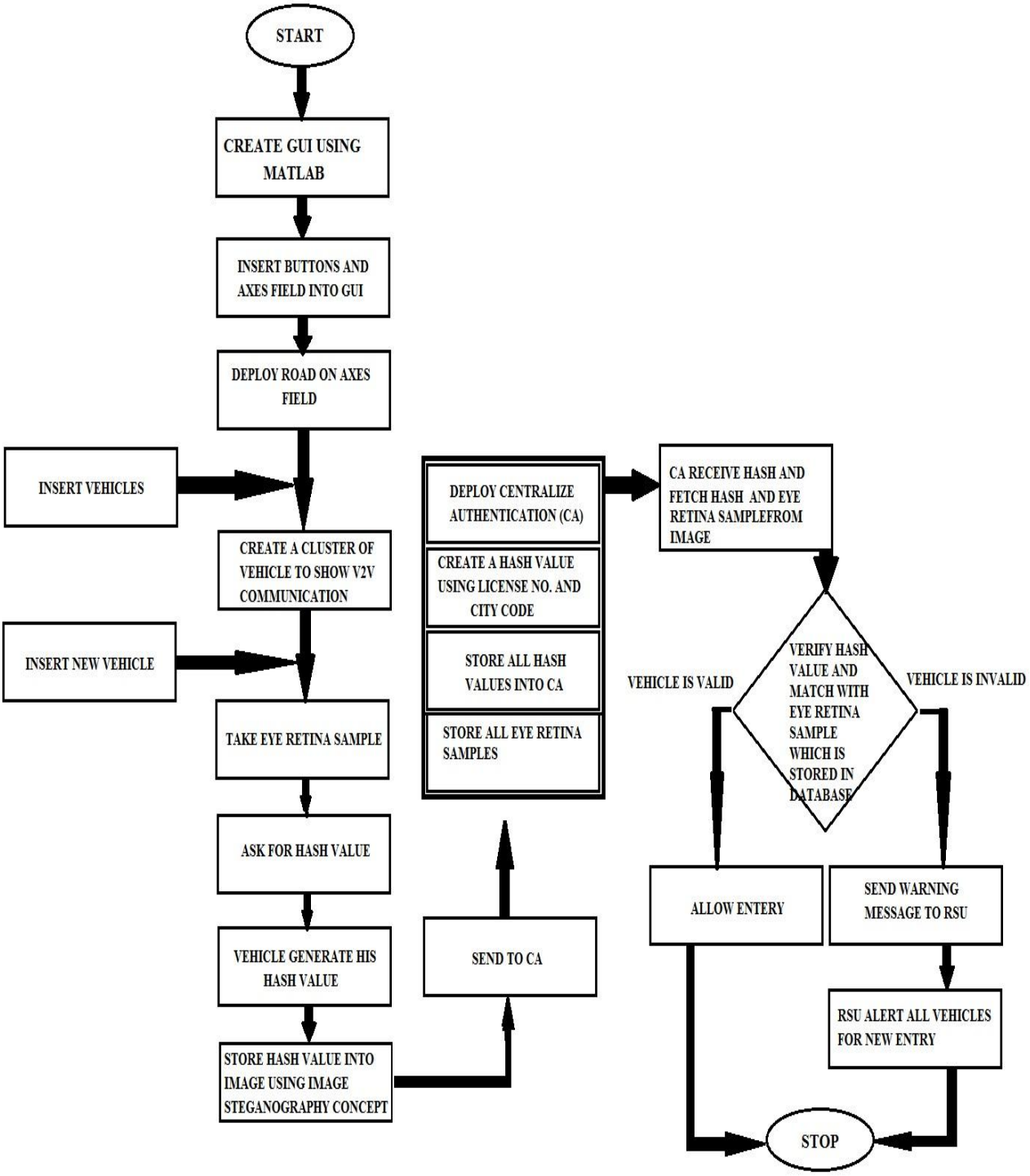

Figure 1: Working Schema

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
- Take eye retina sample
- Ask for hash value to new vehicle
- Vehicle generate his hash value
- Store hash value into image using image steganography concept
- Store eye retina sample
- Send to CA
- CA receive hash and fetch hash from image and eye retina sample
- Verify hash value and eye retina sample
- Vehicle is valid
- Vehicle is invalid
- Send warning message to RSU
- RSU alert all vehicles for new entry

5. SIMULATION AND RESULTS

The whole simulation has been take place in MATLAB environment.

5.1. Evaluation of Research Work

Research work of this dissertation in such a manner that outcome provides the security mechanism in terms of authentication of Vehicular Ad-hoc Network using hash value and steganography schema.

5.2. Result Evaluation Parameters

The following input parameters are used in this research to describe the result.

5.2.1. Cluster Creation Time

Cluster Creation Time is directly proportional to the number of clusters. The input parameters are number of clusters formed and time taken for cluster information.

5.2.2. Cluster Head Selection Time

The Cluster Head Selection Time is estimated for different cluster size by varying the number of clusters. The input parameters are number of clusters formed and time taken to select cluster head.

5.2.3. Throughput

Throughput is the ratio of number of packets which are forwarded and received. So that input parameters are packets and number of nodes.

5.2.4. Overhead

The routing overhead is defined as being the number of routing packets per number of data packets successfully received at the destinations. Overhead Graph is plotted in between network overhead and number of clusters so the input parameters are number of nodes that form clusters and data packets which are used to calculate overhead.

6. PERFORMANCE GRAPHS

The performance and result of a proposed schema to enhance the security through node authentication of vanet using hash value and steganography schema are shown below in Graphical Form:-

6.1. Cluster Creation Time

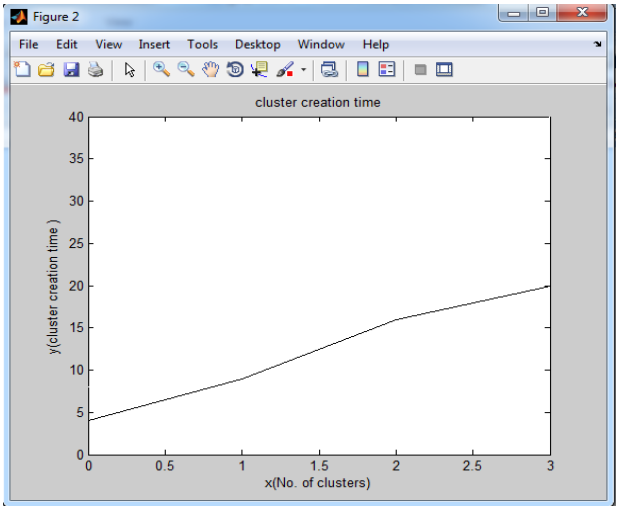

Figure 2: Cluster Creation Time

The figure 2 shows the cluster creation time. Cluster creation time is directly proportional to the number of clusters. It is clearly shown that time taken for cluster creation is less.

6.2. Cluster Head Selection Time

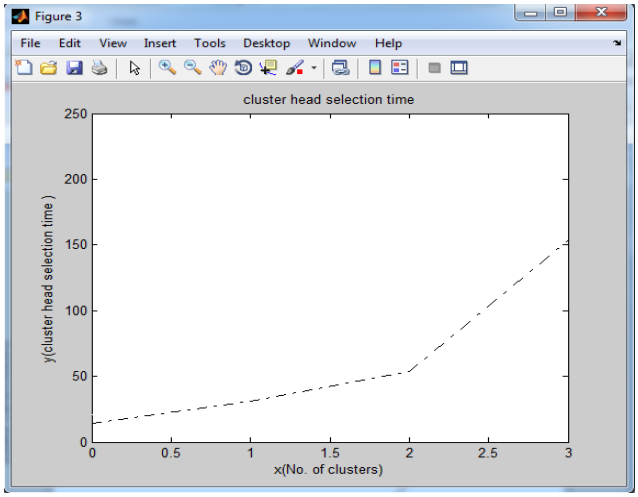

Figure 3: Cluster Head Selection Time

The figure 3 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.

6.3. Throughput

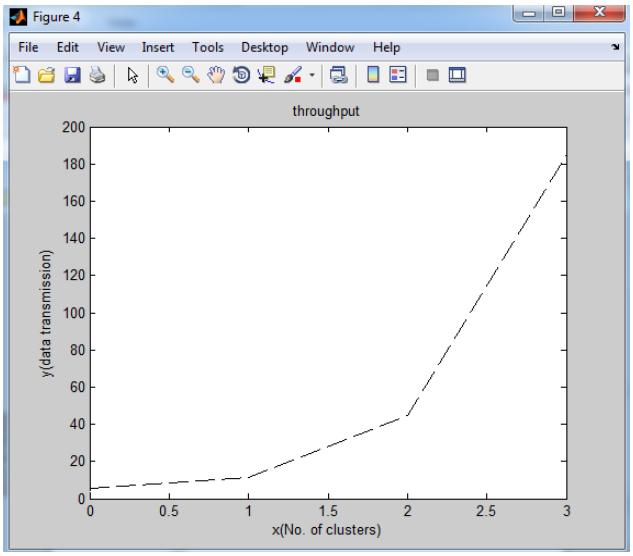

Figure 3: Throughput of System

The figure 3 shows that the system has high throughput. Throughput is a measure of how many units of information a system can process in a given amount of time.

6.4. Routing Overhead

The figure 4 represents routing overhead 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.

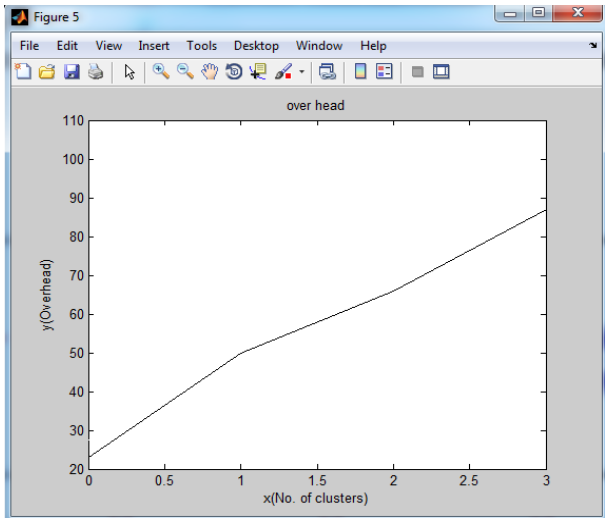

Figure 4: Routing Overhead

7. CONCLUSION & FUTURE WORK

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 activities 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 and eye retina sample. Each vehicle will be authenticate by centralize authentication and it helps to reduce the malicious activities. 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] M. Milton Joe, B. Ramakrishnan, "WVANET: Modelling a Novel Web Based Communication Architecture for Vehicular Network", Wireless Personal Communications - DOI 10.1007/s11277-015-2886-0.
[22] Ramakrishnan, B., Milton Joe, M., & Bhagavath Nishanth, R. (2014). Modeling and simulation of efficient cluster based manhattan model for vehicular communication. Journal of Emerging Technologies in Web Intelligence, 6(2), 253–261.
[23] Ramakrishnan, B., Rajesh, R. S., & Shaji, R. S. (2011). CBVANET: A cluster based vehicular ad hoc network model for simple highway communication. International Journal of Advanced Networking andApplications, 2(4), 755–761.

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.