Secure and Stable VANET Architecture Model

[1]Ankit Temurnikar , [2]Dr.Sanjeev Sharma

[1] School Of Information Technology , RGPV
Bhopal, M.P, India

[2] School Of Information Technology , RGPV
Bhopal, M.P, India

Abstract

Vehicular ad hoc network (VANET) is known as an essential factor of smart Transportation systems. The key benefit of VANET communication is noticed in dynamic protection systems, which objective to enhance security of travelers by exchanging caution messages between automobiles. Other applications and personal services are also allowed in order to lower the cost and to promote VANET exploitation. To effectively set up VANET, security is one of the main challenges that must be tackled. Another important concern is scalability is a serious issue for a network designer how to maintain stable communication and services in VANET. Extremely dynamic environment of VANETs seems it difficult. This paper proposed a more secure and stable cluster scheme for VANETs that uses drop ratio to categorize nodes as malicious. Here also proposed an entropy-based WCA (EWCA) cluster maintained scheme which can handle the stability of the vehicular network.

Keywords: *Vehicular ad hoc network, Monitoring, Attackers, Stable clustering, Link expiration time.*

1. Introduction

Vehicular Ad-Hoc Networks (VANET) is becoming an important technology for concerning latest computer world. It can be help to get better the driving skill both in terms of security and effectiveness. Figure 1 describes VANET, when multi-hop communication is apply VANET allow a automobile to communicate through other automobiles which are away of radio transmission range. It as well enables vehicles to correspond with roadside unit [1]. VANET will to be expected be a crucial part of upcoming Intelligent Transportation Systems (ITS).

ITS relies on communications deployment. Electromagnetic sensors are set into road outside; traffic cameras are set up at major junction; and Radio Frequency Identification (RFID) readers are organize at main road doorways. A usual method for gathering and give out traffic information is as follows [2]. First, traffic sample are collected by road side sensors and send to local transportation center. After statistics handing, traffic information can then be distributes to a user's communication unit via cellular networks. This is a costly and ineffective mode of distribute location-based information, mainly when the information of concern is just a hardly hundred meters from the user's location. Because of its limited communication ability, VANET might modify this paradigm, generating and disseminating information very simple.

The develop and execution of Vehicular Ad Hoc Networks (VANETs) stay representing an key research challenge, which, if resolved, could show the way to the development of the after that key breakthrough after the Internet and cellular network technologies. Vehicles could participate the role of an allowing structure for a number of vastly used apps (e.g., disaster warning systems, traffic information control and prevention systems, climate and weather conditions observing, etc.), as well as enjoying ones (such as online entertainments, advertisements and promotion, etc.). Apart this, every vehicle, associates in a peer-to-peer approach, can enhance the bandwidth resources that are currently available, as well offering connectivity to novel geographical regions. It shows importance of research on VANETs has proliferated for the duration of these two decades, dealing with all most important different phases that engage their devise: communication protocol layers, applications, and mobility channel models.

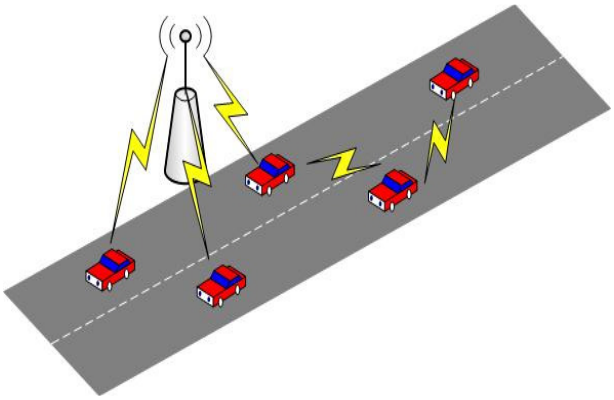

Fig 1: Vehicular ad-hoc networks.

Now, although research efforts on VANETs continuously work on increasing the stage of detail and accuracy of all underlying simulation models, it not being capable to check protocols and systems on practical size vehicular networks represents a significant handicap. Not like node or cellular networks, VANET technologies that occupy a large number of vehicles not at all find a approach of being organized and tested. In literature it is possible to find a number of works that try to fill this gap, by analyzing the exchange of data for only a few hops between two or three vehicles. This is obvious consciousness appear; from learn, of the insufficiency of the projected experimental state, due to the use of restricted amount of vehicles and devices.

2. Related Work

In paper [1], author proposed a lightweight anonymous method based on bilinear pairing to resolve the privacy preserving problem of vehicular ad hoc network (VANET). This scheme can protect drivers' privacy not only between vehicles, but also among vehicles and road side units (RSUs). Meanwhile, this scheme does not ask for vehicles to conduct any bilinear pairing procedures, thus significantly ease the computational complexity of vehicles. Authors demonstrate this scheme through protection analysis and evaluate its computational performance by simulations. The results show that this work scheme performs well in providing secure communications and anonymous authentication among RSUs and vehicles.

Looking for a parking space in a overcrowded area or a large parking lot and preventing auto theft are major anxiety to this work everyday lives.

In paper [2], authors propose a new smart parking scheme for large parking lots through vehicular communication. The proposed scheme can provide the drivers with real-time parking navigation service, intelligent anti-theft protection, and friendly parking information dissemination. Performance analysis via extensive simulations demonstrates its efficiency and practicality.

Vehicular ad-hoc network (VANET) is getting more awareness lately because of its lots of essential applications in transportation, to get better road protection, reduce traffic jamming, to enable competent traffic management etc. However, there are several technical problems to be addressed for its effective exploitation. Steadiness in communication in VANET is hard to accomplish due to quick network changes. Restoration is ineffective while using conventional protocols based on broadcast storm.

In paper [3], authors propose a new adaptive protocol to improve performance for on road safety alert application in VANET. It can alleviate the broadcast storm problem using adaptive wait-windows and adaptive probability to transmit. Simulation shows that this work proposed approach has better performances in terms of number of collision, success rate, and delay, when compared with other existing protocols.

In paper [4], a trustworthy and effective alarm message broadcast routing is proposed for VANET. Distinct other comparable routing algorithms, REAR are based on the actual wireless channel in VANET. REAR utilizes a lesser amount of broadcast packets to spread alarm message. According to the theory model of wireless medium, it estimates the reception possibility of alarm messages for nodes. The contention scheme based on the reception probability is used to choose the optimized relay. Two approaches for utilizing the receipt probability and three functions for calculating contention delay are discussed and analyzed. The simulation and theory analysis are confirmed that REAR has a higher reliability and uses less broadcast packets than the location-based algorithm.

Misbehavior detection schemes (MDSs) form an integral part of misbehaving node eviction in vehicular ad hoc networks (VANETs). A misbehaving node can send messages corresponding to an event that either has not occurred (possibly out of malicious intent), or incorrect information corresponding to an actual event (for example, faulty sensor reading), or both, causing applications to malfunction. While identifying the presence of misbehavior, it is also imperative to extract the root-cause [5] of the observed misbehavior in order to properly assess the misbehavior's impact, which in turn determines the action to be taken.

In paper[10] author proposed three algorithm in first algorithm author proposed a novel clustering algorithm vehicle clustering algorithm VWCA that take into consideration the number of neighbor base on dynamic transmission range the direction of vehicles, entropy, and the distrust value parameters. These parameter increase stability and connectivity and can reduce overhead in network .on the other hand, transmission range of vehicles is important to forward and receiving the massage .when fixed transmission range mechanism is used in VANET .it's likely that vehicles are not located in range of neighbor .this is because of the high rate change in topology and high variability in vehicle density .thus author proposed the allocation and transmission rage (AATR). This technique is used as second algorithm .and finally author proposed the monitoring of malicious vehicle (MMV) algorithm as third algorithm to determine distrust value for each vehicle used in VWCA.

3. Proposed Work

We present the proposed Secure and stable vehicular clustering based on weighted clustering algorithm (SVWCA). First section gives detail about stable clustering method as SVWCA algorithm and second part of proposed work describe security mechanism for malicious node detection in VANET to secure transmission.

3.1 The new stable vehicular clustering based on weighted clustering algorithm (SVWCA)

SVWCA consists of the clustering formation and clustering maintenance phases.

3.1.1 Phase-I: Clustering Formation

For effective cluster formation and remain cluster stable during frequently change topology in highway, this paper proposed new SVWCA more reliable algorithm. In clustering techniques, clusters should be formed in such manner that it not be very large or very small. In a very large cluster, traffic of transmitted information from members to their cluster-head is increased so cluster-head have lost of overheads, and then the cluster-head could not deliver messages on efficient time limit. If cluster formation is very small clusters may not be stable and changed frequently in network because the re-affiliation of network rose [10]. In new SVWCA, this work use two other techniques to cluster creation and cluster maintain.

This paper proposes disbelieve value for check bevies value for any node, among number of neighbors based on dynamic transmission range and direction of vehicles in weighted clustering. In addition, we use the entropy model proposed in [9]. In order to select a trustier node as a cluster-head, we consider the disbelieve value (Td) in SVWCA. The disbelieve value (Td) for vehicle V represents authentication value of behavior for vehicle V when it forwards messages. Every node manages good node list and bad node list. The good node list of vehicle V, represented by GLV, includes the list of connected of vehicle V that their Td values are lower than the threshold values. Value of Td is same for all vehicles within the convinced certificate authentication (CA) in VANET. The bad node list of vehicle V, represented by BLV, consists of neighbors of vehicle V that their Td values are higher than the threshold values. The black list BLV is the copy of the main black list created by the relevant CA. Each CA put out its bad node list once in a while to all cluster-heads which are placed within its area and then every cluster-head forward the bad node list to the vehicles situated within current cluster.

Firstly, each vehicle announces itself as a cluster-head by putting its own address and ID in a beacon to be broadcast. After receiving beacons from its neighbors, each vehicle has complete information from its current neighbors, and it can make decision whether to change its current cluster status or not. For this purpose, vehicles execute SVWCA in order to select their cluster-heads. The SVWCA algorithm has following steps to choose its required parameters as:

Step 1: Determining the neighborhood list for vehicles
Step2: Determining the vehicles priority based on their disbelieve values
Step 3: Determining the direction of vehicles

3.1.2 Phase-II: Stable Clustering Using Mobility prediction

Mobility of vehicles attached with the transient environment of wireless medium regularly results extremely dynamic network topology. Due to mobility some nodes will detach from the current cluster and attach itself to some other cluster. The process of joining a new cluster is known as re-affiliation. If the re-affiliation fails, the whole network will recall the cluster head selection routine. One disadvantage of WCA is high re-affiliation frequency. High frequency of re-affiliation will increase the communication overhead. Thus, reducing the amount of re-affiliation is necessary in ad hoc networks. To prevent this we go for mobility prediction schemes. The impact of mobility prediction schemes on the temporal stability of the clusters obtained using a mobility-aware clustering framework. A cluster for mobile node is given as fig. 2. We propose a simple framework for a mobility prediction-based clustering to enhance the cluster stability.

One way to predict the mobility of nodes is using the Link Expiration Time [6]. The impact of mobility prediction schemes on the stability of the clusters obtained using a mobility-aware clustering framework. Compute the Link Expiration Time (LET) to predict the duration of a wireless link between two nodes in the network. The approach assumes that the direction and speed of motion of the mobile nodes does not change during the prediction interval.

3.2 Link Expiration Time (LET)

The Link Expiration Time (LET) is a simple prediction scheme that determines the duration of a wireless link between two mobile nodes [12]. Dynamic clustering in ad hoc networks has also been extensively studied in the literature. Several distributed clustering algorithms for MANETs have been proposed. Whereas other few methods proposed power utilization balance for vehicle

nodes and few seek to decrease the clustering-related maintenance overall expenses. The Weighted Clustering Algorithm (WCA) [8] is one such scheme, where four parameters are considered for the cluster head selection procedure, which are representative of the degree, the sum of the distances to other nodes in its radio distance, mobility, and battery power of the mobile nodes. Here we propose an enhanced WCA which can enhance the stability of the network. Such a scheme can be tuned flexibly the parameters to suit to different scenarios. To calculate the duration of link between two mobile nodes, we assume that their location, speed and direction of movement remain constant.
Here let:

- Location of node i and node j at time t be given by (xi , yi) and (xj ,yj).
- Vi and Vj be the speeds,
- θi and θj be the directions of the nodes i and j respectively.
- If the transmission range of the nodes is r, then the link expiration time Dt is given by the formula given below

Where

$$a = v_i cos\theta_i - v_j cos\theta_j$$
$$b = x_i - x_j$$
$$a = v_i sin\theta_i - v_j sin\theta_j$$
$$b = y_i - y_j$$

The LET gives an upper bound on the estimate of the residence time of a node in a cluster. In the proposed clustering framework, when LET-based prediction is used, a node is allowed to join a cluster only if the predicted LET of the link between the node and the cluster head is greater than the cluster's admission criteria Tj [6, 7].

For every node N that detach from current cluster we check whether the node is a Cluster Head (or) Cluster member.

1. If it is a Cluster Head then call for cluster head selection within the particular cluster and form a new cluster.
2. If it is a Cluster member then calculate Link Expiration Time with Cluster Head of each cluster and the node that re-affiliates must be within transmission range of cluster head where transmission range is fixed.

Check whether LET is greater than threshold value (Tj), Here Tj is average of all LET, and if it is greater than the Node is eligible to join the particular cluster which shares greater LET.

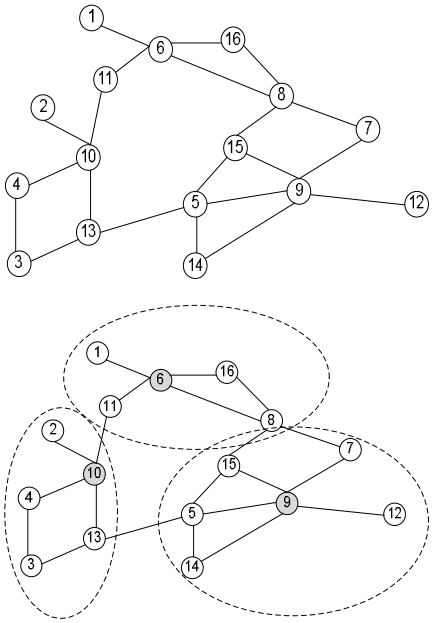

Fig 2: Clustering Example

3.3 Malicious vehicles node detection (MVND) algorithm

Considering the lack of coordinating ND unit in VANET, vehicles should cooperate with each other in order to increase security in the network [11]. In order to verify behavior of vehicles and detect abnormal behavior in the network, the following algorithm (see Fig. 3) is proposed:

Step 1: Distributing cluster keys
Step 2: Allocating initial disbelieve value
Step 3: Determining threshold value □.
Step 4: Behavioral data collection.
Step 5: Determining abnormality of vehicles
Step 6: Modifying disbelieve value
Step 7: Updating black and white lists based on Td
Step 8: Repeating MVND after increasing Td

3.3.1 Behavioral Data Collection

The behavioral data collection module is responsible for the collection of node behaviors and formation of behavioral dataset. In this paper, a node's behavior is described in terms of the percentage of the amount of behavior for total amount of packets that the vehicle has received, such as PDR (packet drop rate), PMOR (packet modification rate) and PMIR (packet misroute rate). An example training dataset is shown in Table I. Here, we create a m-dimensional feature vector for each node. In the example shown in Table I, m = 3. For collection of behavior of nodes following secure algorithm used. For instance, if all the nodes choose to observe the behaviors of packet drop,

modification and misroute, then PDR, PMOR and PMIR may be calculate as by following equations, in that order.

PDR = *Number of Packet Dropped/Total Number of Incoming Packets*

PMOR = *Number of Packet Modified/Total Number of Incoming Packets*

PMIR = *Number of Packet Misrouted/Total Number of Incoming Packets*

During the testing stage, the Behavioral Data Collection module on each node first observes and records the behaviors of their neighbors. It also receives and integrates node behaviors reported by other nodes.

Table 1. An example of the training dataset used to classify VANET nodes as malicious or non- malicious.

Node ID	***PDR***	***PMR***
1	90%	10%
2	2%	0
3	30%	60%
4	5%	0
5	10%	0
. . .	. . .	. . .
. . .	. . .	. . .

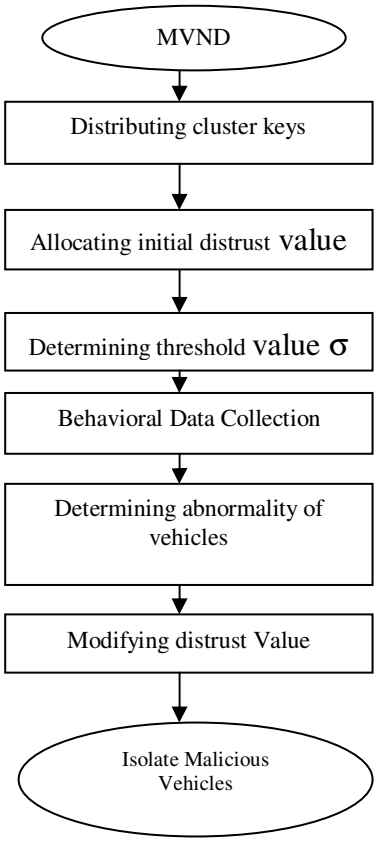

Fig 3: Flowchart of the MMV algorithm

4. Performance evaluation and analysis

In this section, we examine the performance of the SAT scheme, and its performance is compared to that of the baseline mechanism. Overall, the experiments can be divided into two phases: first phase is used SUMO for simulating vehicles as real world street condition and in second phase using NS-3 pcap utility used for capture packets form this vehicle network to identify malicious node in network according to its behavior as explained in proposed work.

4.1 Simulation Setup

This work is implemented in linux environment using ubutu 12.04 GUI versions. For VANET SUMO version 0.14.0 is used and also need to configure NS-3 as the simulation platform. SUMO is open source freely available software yet very powerful for traffic and highway simulation. It is extremely manageable, tiny and nonstop highway traffic simulation pack designed to able for hold vast road networks.. Table II list the parameters used in the simulation scenarios.

Table 2. Parameter list

Parameter	***Value***
Mobility Model	Waypoint model
Nodes (Wi-fi Node's)	50 nodes
Simulation Time	100s
Packet Size	1000 bytes
Sink Nodes	17
Update Interval	15s
Node Speed	10 m/s
Settling Time	6
Routing Protocols	AODV

Each simulation scenario has 30 runs with distinct random seeds, which ensures a unique initial node placement for each run. Each experimental result is the average over the 30 runs for this simulation scenario.

4.2 Behavioral Data collection Method

4.2.1 NS-3 Simulation

1. Design Wi-Fi topology
2. Install MAC, IP and Application protocol on each node.
3. Select VANET routing protocol (AODV) start simulation
4. For each node i
   a. do
   b. RREQ start (in case of AODV)
   c. Flooding of RREQ

d. Build routing table (AODV. route file)
i) Collect behaviors statistics such as No. of packet transmitted, received, lost, delay time, modified etc.
ii) Calculate PDR, PMOR, PMIR
iii) Serialize into .xml or .csv file format

4.2.2 Behavior Classification

1. Input .xml/.csv data file Generated by NS-3
2. Extract PDR, PMOR and PMIR using DOM
   a. For each node i repeat
   b. Input .xml onto DOM (Data Object Module)
   c. Extract behavior from DOM result file.

5. Results

Table III shows statics capture by pap utility of NS-3 for 25 nodes ID starting from 0 to 24 total no. of packets transmitted, total no. of packets received and packet drop ration(PDR) for each node during simulation.

Table 3. Simulation classification data

Node ID	*PDR*	*PMIR*	*PMOR*
0	0	0	0
1	0	0	0
2	0	0	0.028169
3	0	0	0
4	0	0	0
5	0	0	0
6	0.621984	0.276145711	0.135135
7	0	0	0
8	0	0	0
9	0	0	0
10	0	0	0
11	0	0	0
12	0.433566	0.297327813	0.079037
13	0.117188	0.03968254	0
14	0.194175	0.1	0.066667
15	0.23569	0.069444444	0
16	0.036765	0	0
17	0.147059	0.120845921	0.030211
18	0.183486	0	0
19	0.184049	0.031347962	0
20	0.222222	0.0456621	0
21	0.209059	0.071684588	0.071685
22	0.13289	0	0
23	0.516416	0.240029542	0.070162
24	0	0	0

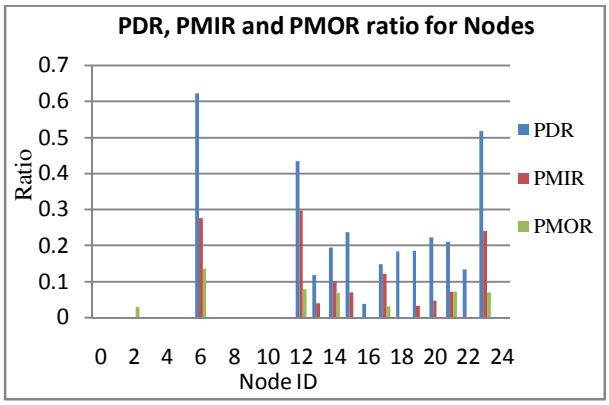

Fig 4: PDR, PMIR and PMOR ratio for every node during simulation

We have perform VANET simulation many time for detecting malicious node in network for which first three detection data is shown in following graph for different no. of node. This graph shows for example 10 node network size in first simulation result 1 malicious node found such next time no node is malicious and for third simulation it gives 2 nodes are abnormal because of PDR greater than 0.5 value, PMIR greater than 0.1 and PMOR greater than 0.1.

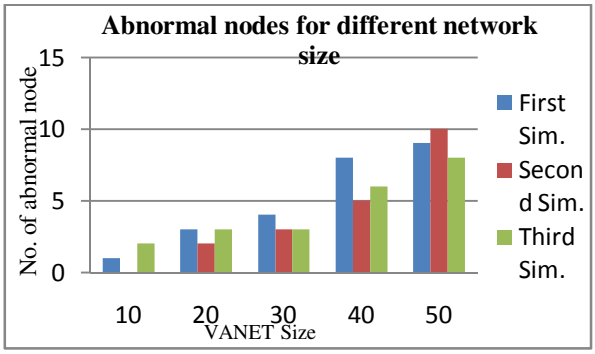

Fig 5: Abnormality of nodes for different network size during simulation

6. Conclusion

VANET is a capable wireless communication technology for improving highway protection and information services. This paper has estimated two different algorithms appropriate for VANET in highway road. First, algorithm have proposed SVWCA as a new vehicular clustering algorithm based on the WCA technique in two part first one for formation of cluster and second for maintain of cluster properly for less overheads. The SVWCA technique primarily focuses on improving the CH duration, membership duration and security and second for maintaining cluster stability as possible. Using SVWCA, communication cost for joining to a new cluster in network decreases because the membership duration for every

vehicle has improved. SVWCA be able to enhance network connectivity while selecting cluster-heads.

SVWCA make use of disbelieve value in the weighted sum operation. The disbelieve value has been obtained from this work next proposed malicious vehicle node detection (MVND) algorithm. Using disbelieve value, vehicles that have lower disbelieve value than their neighbors are selected as cluster-heads. Therefore, cluster-heads are more reliable vehicles than other vehicles in the network using their PDR value.

In future works developing algorithms for a city scenario based on the techniques proposed here for highways and introducing a new security algorithm based on key distribution and the proposed clustering algorithm.

References

[1] Lightweight Anonymous Authentication Scheme for VANET Based on Bilinear Pairing", INCoS, Page(s): 222 – 228, 4th International Conference, 2012,

[2] Rongxing Lu, Xiaodong Lin ; Haojin Zhu ; Xuemin Shen, "SPARK: A New VANET-Based Smart Parking Scheme for Large Parking Lots", Page(s): 1413 – 1421, INFOCOM 2009, IEEE

[3] Suriyapaiboonwattana, K., Pornavalai, C. ; Chakraborty, G., "An adaptive alert message dissemination protocol for VANET to improve road safety", Page(s): 1639 - 1644 FUZZ-IEEE 2009.

[4] Hao Jiang, Hao Guo, Lijia Chen, "Reliable and Efficient Alarm Message Routing in VANET", Distributed Computing Systems Workshops, 2008, Page(s): 186 - 191

[5] Mainak Ghosh, Anitha Varghese, Arobinda Gupta, "Detecting misbehaviors in VANET with integrated root-cause analysis", India 2010

[6] H. Deng, Q.-A. Zeng, and D. Agrawal, "Svm-based intrusion detection system for wireless ad hoc networks," in Proceedings of 2003 IEEE 58th Vehicular Technology Conference, 2003. VTC 2003-Fall.,vol.3, Oct. 2003, pp. 2147–2151.

[7] C.-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe,and K. Levitt, "A specification-based intrusion detection system for aodv," inSASN '03: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks. New York, NY, USA: ACM, 2003, pp. 125–134.

[8] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confidant protocol," in MobiHoc '02: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing. New York, NY, USA: ACM, 2002, pp. 226–236.

[9] Liu X, Fan Zh, Shi L., "Securing vehicular ad hoc networks". In: Proceedings of the second conference on international pervasive computing and applications. July 2007, p. 424–9.

[10] Ameneh Daeinabi, Akbar Ghaffar Pour Rahbar, Ahmad Khademzadeh "VWCA: An efficient clustering algorithm in vehicular ad hoc networks", Journal of Network and Computer Applications 207–222, 2011.

[11] Wenjia Li, Anupam Joshi, Tim Finin, "SAT: an SVM-based Automated Trust Management System for Mobile Ad-hoc Networks", Proceedings of the Military Communications Conference, 2011.

[12] S. Muthuramalingam, R. Viveka, B. Steffi Diana and R. Rajaram, "A Modified Weighted Clustering Algorithm for Stable Clustering using Mobility Prediction Scheme", Internetworking Indonesia Journal, 9-16, 2010.

Dr.Sanjeev Sharma has graduated in Electrical & Electronics from Samrat Ashok Technical Institute, India and post graduated in Microwave and Millimeter from Maulana Azad College of Technology, India. He completed his Doctorate in Information Technology from Rajiv Gandhi Proudyogiki Vishwavidyalaya. Currently he is working as Head in School of IT, RGPV (Bhopal), India. He possesses teaching and research experience of more than 17 years. His areas of interest are Mobile Computing, Data Mining and Information Security. He has edited proceedings of several national and international conferences and published more than 70 research papers in reputed journals.

Ankit Temurnikar was born in Bhopal (M.P) India on 06Th Frb 1987. He receives the B.E. degree in Computer Science from Rajiv Gandhi Proudyogiki Vishwavidalaya Bhopal in 2009. He is presently pursuing M.Tech from Rajiv Gandhi Proudyogiki Vishwavidalaya Bhopal. His area of research is Vehicle adhoc Network (VANET) and Adhoc Network .