Recognition and Elimination of Malicious Nodes in Vehicular Ad hoc Networks (VANET's)

Prashant Sangulagi
Department of Electronics and Communication, BKIT Bhalki
Bhalki: 585328. KARNATAKA, INDIA
psangulgi@gmail.com

Mallikarjun Sarsamba
Department of Electronics and Communication, BKIT Bhalki
Bhalki: 585328. KARNATAKA, INDIA
ck.mallu@rediffmail.com

Mallikarjun Talwar
[2]Department of Instrumentation and Technology, BKIT Bhalki
Bhalki: 585328. KARNATAKA, INDIA
talwar.mallu@gmail.com

Vijay Katgi
Department of Electronics and Communication, BKIT Bhalki
Bhalki: 585328. KARNATAKA, INDIA
katgivijay@gmail.com

Abstract:
A Vehicular Ad-Hoc Network, or VANET, is a form of Mobile ad-hoc network, to provide communications among nearby vehicles and between vehicles and nearby fixed equipment (Base Stations) via radio waves. These have similar characteristics as mobile ad hoc networks, often in the form of multi-hop networks. Due to the high mobility of nodes network topology changes occur frequently. All nodes share the same channel leading to congestion in very dense networks. One important property that characterizes VANETs is that they are self-organizing, self-creating, and self administering and decentralized systems. This paper proposes detection and elimination of misbehaving nodes in VANETs using mobile agents. Mobile agents are employed for each node, for the collection of information of neighbours and to find the route from source to the destination. To find the malicious nodes among the intermediate nodes, mobility and power ratio of the intermediate nodes are continuously monitored with the help of software agents. Some threshold value of mobility and power ratio for intermediate nodes are maintained at the source node. Based on comparing the monitored and threshold values of these factors, with probabilistic approach we are determining the nodes as malicious nodes. Once the intermediate node is determined as the malicious node, the alternate path is employed from source to the destination. To test the operative effectiveness and performance of the system some of the performance parameters evaluated are, Number of paths available, Number of routes involving misbehaving nodes, Number of misbehaving nodes, Time taken to detect misbehaving nodes.

Keywords: VANET, Mobile Agents, Routing, Malicious Nodes, Mobility.

1. Introduction

Wireless networks are the networks in which nodes are interconnected via wireless links such as radio frequency, microwave links etc. network components in wireless networks communicate with others using wireless channels. These networks provide mobile users with a ubiquitous computing capability and information access regardless of the location [1]. The existing wireless networks can be classified into two main types, Infrastructure mobile networks and Infrastructure-less mobile networks. Infrastructure-less mobile networks can also be called as mobile ad hoc network (MANET). A MANET is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure.

A Vehicular Ad-Hoc Network, or VANET, "is a form of Mobile ad-hoc network, to provide communications among nearby vehicles and between vehicles and nearby fixed equipment (base stations) via radio waves" [2]. These have similar characteristics as mobile ad hoc networks, often in the form of multi-hop

networks. Due to the high mobility of nodes network topology changes occur frequently. All nodes share the same channel leading to congestion in very dense networks. One important property that characterizes VANETs is that they are self-organizing, self-creating, and self administering and decentralized systems. The main difference between VANETs and MANETs is that the nodes move with higher average speed and the number of nodes is assumed to be very large. Also the difference between is that MANET nodes cannot recharge their battery power where as VANET nodes are able to recharge them frequently [3]. Apart from that, VANETs will be operated or at least rolled-out by multiple companies and the nodes belong to people within different organizational structures. Advantages of VANETs like, VANET support high mobility, minimum infrastructure support is needed, disrupting conventional infrastructure based communication model, Effective traffic control. VANET provide two services are, inter vehicular services and vehicle-to-infrastructure communication services. Vehicular Ad hoc Networks can be used in commercial sectors, Military Battlefield, local danger warning, weather information, mobile e-commerce, internet access and in many applications VANTEs are used [4]. Some important issues of VANETs are, Unpredictability of environment, Unreliability of wireless medium, Resource-constrained nodes, Dynamic topology, Security and Reliability, Power Consumption and The limited bandwidth.

Finding the malicious nodes in the Vehicular Ad hoc network is a challenging task. Depending on the factors like mobility, power, delay, channel reliability etc one can easily recognize the malicious node in the VANET. Many researchers have developed efficient schemes to find malicious nodes in the VANETs. The work given in [5], proposes cluster-based schemes. The clusters are formed to divide the network into manageable entities for efficient monitoring. The clustering results in a special type of a node, called “cluster head" to monitor traffic within a cluster. It not only manages its own cluster but also communicate with other clusters. It maintains information of every member of node, which is useful for communication within network. The cluster management responsibility is rotated among the capable members of the cluster for load balancing and fault tolerance and must be fair and secure. This can be achieved by conducting regular elections. The proposed election process is simple. It does not require the clique computation, or the neighbour information. The probabilistic model for detecting of malicious nodes using markov chains for each cluster is described in [6]. The challenges and security aspects were described in [7], [8] and some of the routing protocols like AODV, DSRDV, DYMO etc. are explained in [9], [10], [11] [12]. The need of new routing protocols and features desired for a routing protocol in ad Hoc networks are explained in [13]. The malicious data can in VANETs using sensor drive techniques as explained in [14]. As explained in [15], the malicious node can be detected by knowing node’s position that is done by analysing the signal strength distribution and then verifying its position with the estimated position.

This paper proposes Recognition and Elimination of Malicious nodes in VANETs using mobile agents. Mobile agents are employed to each node, to collect information of neighbours and to find the route from source to the destination. To find the malicious nodes among the intermediate nodes, mobility and power ratio of the intermediate nodes are continuously monitored with the help of software agents. Some threshold value of mobility and power ratio for intermediate nodes are maintained at the source node. Based on comparing the monitored and threshold values of these factors, with probabilistic approach we are determining the nodes as malicious nodes. Once the intermediate node is determined as the malicious node, the alternate path is employed from source to the destination.

The organization of the paper is as follows, section II describes software agents, section III gives proposed work, section IV explains Simulation and results of the proposed methodology and lastly section V concludes the paper.

2. Agent Technology

An agent is a piece of software that can achieve a specific task in an autonomous way in other words an agent is a program that assists people and act on their behalf. Agents function by allowing people to delegate work to them. Mobile agents are agents, which have the additional property of mobility. The agents have possibility of co-coordinating, communication and co-operating with system or to other agents. Some of the special characteristics of agents include autonomy, temporal continuity, local interaction, social ability, reactivity and pro-activeness [16]. Using mobile agents we can carry intelligence (code) required to perform task on the data available on the remote system. The goal of software agents is to automate tasks that require interacting with one or more software accessible systems. Past research has yielded several types of agents and agent frameworks capable of automating a wide range of tasks, including: processing sequences of operating system commands [17]. The advantages of software agents like, simplifying the complexities of distributed computing and overcoming the limitations of current interface approaches. The concept of software agents, its operation and some of the advantages, agent platforms and its properties are described in [18], [19].

The agents are classified into two types namely, mobile agents and static (Stationary) agents. A stationary agent executes only on the system where it begins execution. If it needs information that is not on that system,

or needs to interact with an agent on a different system, it typically uses a communication mechanism such as remote procedure calling (RPC). On the other hand A mobile agent is not bound to the system where it begins execution. It has the unique ability to transport itself from one system in a network to another. The ability to travel, allows a mobile agent to move to a system that contains an object with which the agent wants to interact, and then to take advantage of being in the same host or network as the object. The advantages of mobile agents are, it reduces network load, overcomes network latency, asynchronous and autonomous execution, adaption to dynamic nature, heterogeneous and robust and fault tolerance [20].

In this paper mobile agents are employed to collect the information of neighbour and also to find the path from source to the destination. In this Mobile agent migrate from one node to another and collect information about neighbours and updates nodes database. Now the node conforms that whether the neighbour is friendly node or malicious node.

3. Proposed Work

This paper proposes Recognition and Elimination of Malicious nodes in VANETs using mobile agents. Mobile agents are employed for each node, for the collection of information of neighbours and to find the route from source to the destination. To find the malicious nodes among the intermediate nodes, mobility and power ratio of the intermediate nodes are continuously monitored with the help of software agents. Some threshold value of mobility and power ratio for intermediate nodes are maintained at the source node. Based on comparing the monitored and threshold values of these factors, with probabilistic approach we are determining the nodes as malicious nodes. Once the intermediate node is determined as the malicious node, the alternate path is employed from source to the destination.

3.1 *Network Architecture*

The following VANET architecture has been considered here, which is as shown in figure 1. Here the communicating devices (Nodes) i.e vehicles are spread through the network randomly. Each node is limited by its transmission range, which limits its capacity to communicate with all the remaining nodes directly. Hence a source node should use one or more intermediate nodes to communicate with the intended node. The nodes which lie within the transmission range of a node are said to be neighbouring nodes for that particular node.

The node, which is in need to communicate with some other node, is termed as source node, with which the source node wants to communicate is termed as destination node.

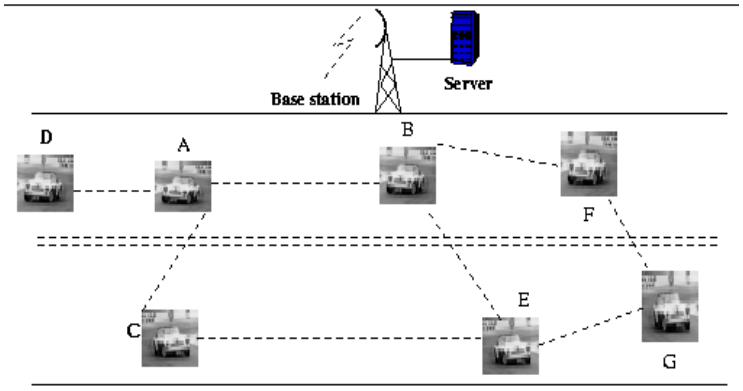

Fig 1: Network Architecture

3.1.1 *Formation of the clusters:*

A node is said to be connected with other node when the other node is within the range of first. Let the coordinates of node1 be (x1, y1) and that of node2 be (x2, y2) the distance between them is calculated by using the formula,

$$D = \sqrt{(x1 - x2)^2 + (y1 - y2)^2}$$

If D <= Range, the node is said to be connected otherwise it is disconnected. Based on the communication range and coverage area of the base station the clusters are formed.

3.1.2 *Detection of misbehaving nodes*:

(1) To find the malicious nodes among the intermediate nodes, mobility and power ratio of the intermediate nodes are continuously monitored with the help of software agents.

(2) Some threshold value of mobility and power ratio for intermediate nodes are maintained at the source node.

(3) Based on comparing the monitored and threshold values of these factors, with probabilistic approach nodes are treated as malicious nodes.

3.1.3 *Alternate route formation by eliminating of misbehaving nodes:*

(1) By comparing the threshold value with the measured value, source node decides the malicious node.

(2) Then source node searches the other routes, where the detected malicious intermediate node will not present.

(3) Route without malicious intermediate node will be considered as the alternate route from source to destination.

3.2 ***Agency at Node***

Agency in the nodes consists of Node Black Board (NBB), Node Management Agent (NMA) and Routing Agent (RA). Agency of node is as shown in figure 2.

(1) *Node Black Board (NBB):* It maintains a list of information like neighbours, and their Id's, mobility, power ratio and position etc.

(2) *Node management agent (NMA):* It is a static agent that controls the actions to be performed at that particular node. It maintains the database of the node, like storing the list of neighbouring nodes and its respective mobility and power ratio.

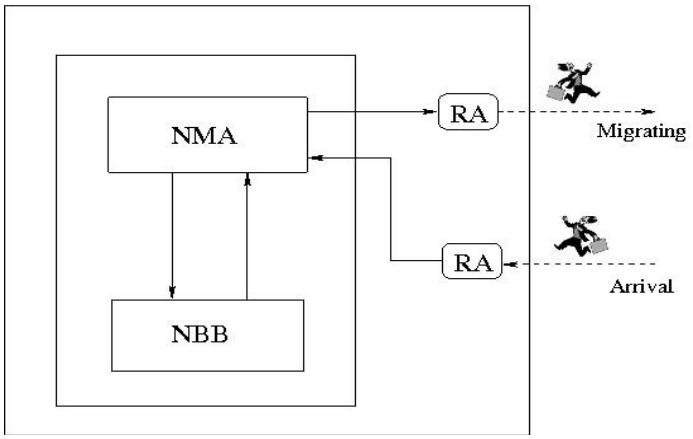

Fig 2: Agents at each node

It addresses the mobile agents arriving at the node by providing them the required information and also initiates the route discovery process whenever the node requires communicating by creating multiple Routing Agents (RA). At the source node it also compares the collected values of mobility and power ratio from Routing Agents (RA) with the threshold values and decides the misbehaving nodes [21].

(3) *Routing Agent (RA):* It is a mobile agent, which arises when a route discovery process is initiated; this agent migrates through the network in search of the destination and collects the information like mobility and power ratio from the NMA of each node. Once it reaches to the destination it traces the path and submits the collected information to the NMA of source node [22].

4. Simulation and Results

The simulation of the proposed model is done using turbo C. In the simulation model we consider "N" number of nodes in the area of length "L" and breadth "B" otherwise the nodes can be allowed free movement if possible. Various mobility models exist for VANETs. One of the very popular models is a modified version of random waypoint model, also known as bouncing ball model. In this model node start of at random position within the field. Each node then chooses a random direction and keeps moving in that direction till it hits the terrain boundary. Once the node reaches the boundary it chooses another random direction and keeps moving in that direction till it hits the boundary again. An important aspect of modified mobility model is that M_{min} (minimum node velocity) is always set to be non-zero. In fact, M_{min} is set equal to M_{max} (maximum node velocity) for most of the simulation. Hence bouncing ball model does not suffer from drawbacks of random mobility model.

Mobility for each of these "N" nodes is initialized. The mobility can be changed or remain fixed throughout the simulation. The number of nodes may vary too during the simulation. The area L*B may be defined. The nodes can be allowed free movement or the area is fixed. The initial position of the nodes are chosen for nodes within the area L*B. These positions are generally randomly chosen. The direction of the node movement is initialized which may vary during the simulation. For more realistic approach the directions are not changed frequently. Certain probability may be set above which the nodes change their direction. The range of each node is fixed. Range can be same for all nodes. The range could be varied during simulation. The mobility

factor is given randomly for each node. Nodes may enter or leave a node's range during the simulation. Each node has their respective values of channel reliability and power ratio.

4.1 *Simulation Procedure*

Begin

i) Generate a network topology with given number of nodes.
ii) Trigger the agents from the source.
iii) Find the mobility and power ratio of the nodes using mobile agents.
iv) Compute the performance of the system.

End

In this M_{min}=1Km/Hr, M_{max}=50km/Hr, L*B=1000*1000 m2, Transmission Range = 30m are considered. Initially we have considered 10 nodes then increased the number of nodes and the following performance parameters are considered here.

4.2 *Performance Parameters*

i) *Number of paths available:* It is the total number of routes available between source and destination for communication.
ii) *Number of routes involving misbehaving nodes:* It is the total number routes involving with malicious nodes from source to destination.
iii) *Number of misbehaving nodes***:** It is the total number of misbehaving nodes present in the route between source and destination.
iv) *Time taken to detect misbehaving nodes:* It is the total time taken to detect the misbehaving nodes in the route from source and destination.

As the node density increases, the number of links between the source & destination increases, thus due to variable mobility of each node the probability of link failure increases. Hence as the vehicle speed increases, the number of routes decreases, as depicted in figure 3. Here we have also shown the variation of these parameters with respect to different value of number of nodes.

The number of routes involving misbehaving nodes increases with number of vehicles as shown in figure 4. Here we have also shown the variation of these parameters with respect to different vehicle speeds.

The number of misbehaving nodes increases with respect to the number of vehicles as depicted in figure 5. Here we have also shown the variation of these parameters with respect to different vehicle speeds.

As the vehicle density increases, the number of links between the source & destination increases, Hence as the vehicle density increases the number of routes increases, thus due to variable mobility of each vehicle the probability of link failure increases. Hence the number of misbehaving nodes in selected path increases as depicted in figure 6. Here we have also shown the variation of these parameters with respect to different vehicle speeds.

From figure 7, as the vehicle density increases, the number of links between the source & destination increases, Hence as the vehicle density increases the number of routes increases, thus due to variable mobility of each vehicle the probability of link failure increases. Hence it will take more time to detect misbehaving nodes. Hence as vehicle density increases time taken to detect misbehaving nodes increases.

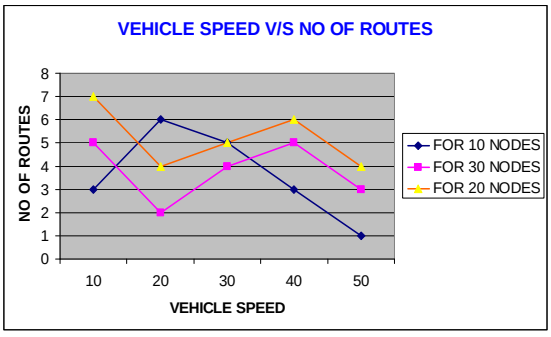

Fig 3. Vehicle Speed (Kmps) v/s. No. of Routes

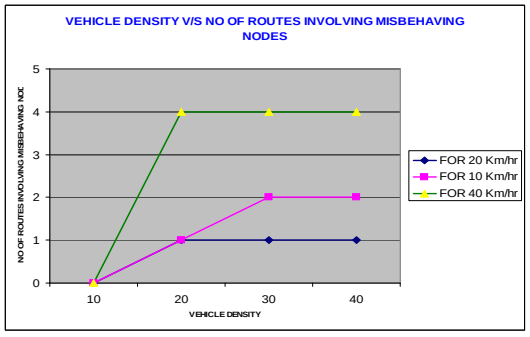

Fig 4. Vehicle density v/s. No. of routes involving misbehaving nodes

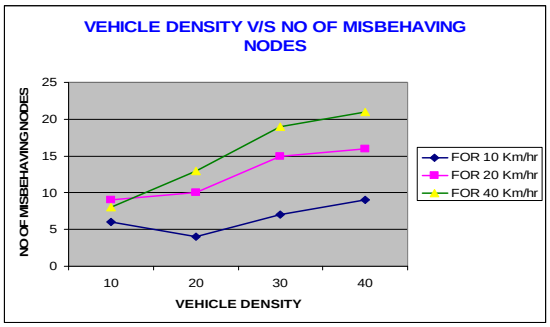

Fig 5. Vehicle density v/s. No. of misbehaving nodes

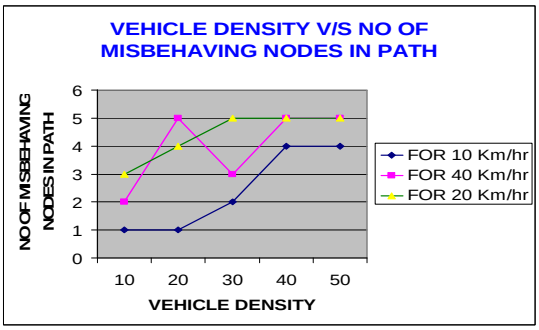

Fig 6. Vehicle density v/s. No. of misbehaving nodes in path

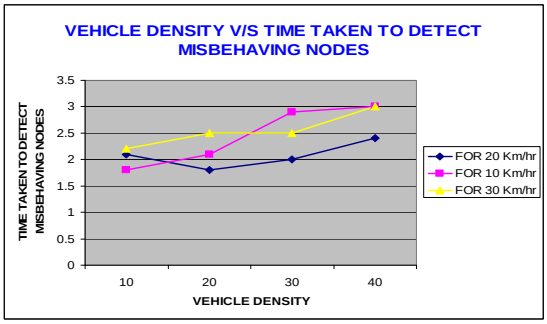

Fig 7. Vehicle density v/s. time taken to detect misbehaving nodes

5. Conclusion

VANET is a form of Mobile ad-hoc network, to provide communications among nearby vehicles and between vehicles and nearby fixed equipment (base stations) via radio waves. This paper proposes Recognition and Elimination of malicious nodes in VANETs using mobile agents. Mobile agents are employed for each node, for the collection of information of neighbours, to find the route from source to the destination, and for the detection of malicious nodes. Performance parameters evaluated are, Number of paths available, Number of routes involving misbehaving nodes, Number of misbehaving nodes, Time taken to detect misbehaving nodes. The proposed methodology and its results shows that by using this, one can easily recognize and eliminate the malicious nodes in the Vehicular Ad Hoc Network. In this paper, we have concentrated only on finding the misbehaviour nodes in VANETs. In future, we may consider more parameters like bandwidth, delay, etc. for routing in VANETs.

References

[1]. S. Tanenbaum (1996), *Computer Networks*, Prentice Hall, Third Edition, Chapter 5, Englewood Clis, pp:357-358.
[2]. Maxim Raya, Jean-Pierre hubaux (2005), *Security Aspects of Inter-Vehicle Communications*, 5th Swiss Transport Research Conference (STRC), pp:1-14.
[3]. Fay Hui (2005), *A survey on the characterization of Vehicular Ad Hoc Networks routing solutions*, ECS 257 Winter 2005, pp:1-15.
[4]. T. Taleb, E. Sakhaee, A. Jamalipour, K. Hashimoto, N. Kato, and Y. Nemoto (2007), *A stable routing protocol to support its services in VANET networks*, IEEE Transactions on Vehicular Technology, Vol. 56, no. 6, pp:3337–3347.
[5]. Ejaz Ahmed, Kashan samad, Waqar Mahmood (2006), *Cluster based intrusion detection architecture for mobile ad hoc networks*, 5th Conference, AusCERT-2006, Gold Coast, Australia. pp:48.
[6]. K. Komathy, P. Narayanasamy (2007), *A Probabilistic Behavioral Model for Selfish Neighbors in a Wireless Ad Hoc Network*, International Journal of Computer Science and Network Security (IJCSNS), Vol.7 No.7, pp:77-83.
[7]. Stephan Eichler, Christoph and Jorg Eberspacher (2006), *Car-to-Car Communication*, Proceeding of the VDE-Kongress – Innovations for Europe, pp:1-6.
[8]. Bryan Parno and Adrian Perrig (2005), *Challenges in Securing vehicular Networks*, Proceedings of the Workshop on Hot Topics in Networks (HOTNETS-Iv), Carnegie Mellon University.
[9]. I. Chakeres and C. Perkins (2008), *Dynamic MANET On-demand Routing Protocol (DYMO)*, Internet Draft, available at http://tools.ietf.org/html/draft-ietf-manet-dymo.
[10]. E. Royer and C-K. Toh (1999), *A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks*, IEEE Magazine on Personal Communications, vol.6, issues: 2, pp:46-55.
[11]. S. Singh, M, Woo, and C. S. Raghavendra (1998), *Power-Aware routing in mobile ad hoc networks*. IEEE international conference on Mobile computing and networking, New York, pp:181-190.
[12]. Ding Y, Wang C, Xiao L (2007), *A static-node assisted adaptive routing protocol in vehicular networks*, In Proceedings of the Fourth ACM international Workshop on Vehicular Ad Hoc Networks VANET, New York, USA. pp 59–68.
[13]. Papadimitratos and Z.J. Haas (2002), *Secure Routing for Mobile Ad hoc Networks*, Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS-2002), San Antonio, USA.
[14]. Phillipe Golle, Dan Green, Jessica Staddon (2004), *Detecting and Correcting Malicious Data in VANETs*, Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, New York, USA, pp:29-37.

[15]. Bin Xiao, Bo Yu, Chuanshan Gao (2006), *Detection and Localization of Sybil Nodes in VANETs*, Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks, pp:1-6.
[16]. Michael Wooldridge and Nicholas R. Jenning (1995), *Agent theories, architectures and languages: a survey*, Springer-Verlag, Woolridge and Jenning, pp:1-22.
[17]. Danny B. Lange (1998), *Mobile Objects and Mobile Agents: The Future of Distributed Computing?*, In Proceeding of the European Conference on Object- Oriented Programming '98, pp:1-12.
[18]. N. Minar ,K. H. Kramer and P. Maes (1999), *Co-operating Mobile Agents for dynamic network routing, in software agents for communication system*, chapter 12, Springer verlog.
[19]. Robert Sugar and Sandor imre (2001), "Adaptive clustering using mobile agents in wireless routing in MANETs", 8th International Workshop on Interactive Distributed Multimedia Systems Springer-Verlag, London, UK pp:199-204.
[20]. Oscar Urra, Sergio Ilarri, Thierry Delot and Eduardo Mena (2010), *Mobile Agents in Vehicular Networks: Taking a First Ride*, Advances in Intelligent and Soft Computing, Springer Verlog Vol. 70, pp:119-124.
[21]. A. V. Sutagundar, S. S. Manvi (2008), *Agent Based Approach to Information Fusion in Wireless Sensor Networks*, IEEE Conference TENCON 2008, Hyderabad, pp:1-6.
[22]. Prashant Sangulagi, A. V. Sutagundar, S. S. Manvi (2011), *Agent based information aggregation and routing in WSN*, CNC 2011, Springer Verlog, Bangalore, pp: 449-451.