Unauthorized Node Detection in VANET

[1] Harshal D. Misalkar

[2] Prof. Mrs. S. S. Sikchi
Assistant Professor, PRMIT & R, Badnera-Amravati (M.S.)

***Abstract*—Detection of Unauthorized node in vehicular ad-hoc network means that, all the nodes of network are continuously monitored with the help of server. Server will determine the nodes as malicious nodes on the basis of database maintained at server. Database contain information of entire network i.e. each and every node which is actually received by the server in the form of acknowledgment. Once the intermediate node is determined as the unauthorized node, the alternate shortest path is employed from current node to the destination. DIJKSTRA'S shortest path algorithm is used for two way handshaking faster communication between vehicle to vehicle and vehicle to server.**

***Index words* — VANET, Routing, Malicious Nodes, Mobility.**

I. Introduction

A wireless ad hoc network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding the data. An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network device in link range.

Vehicular Ad-Hoc Network (VANET) communication has popular in the area of wireless networking as well as the automotive industries. The goal of VANET is to develop a vehicular communication system to enable quick and cost efficient distribution of data for the benefit of passengers' safety and comfort [1]. Vehicular ad-hoc networks (VANETs) are considered to be the special application of infrastructure-less wireless Mobile ad-hoc network (*MANET).* In ad hoc network the VANET maintain and update information on routing between all nodes of a given network at all times. The main characteristic of VANETs is High mobility of node, No problem with power and Predictable topology [2].

Fig.1 shows that Vehicular Ad-Hoc Network is a form of Mobile ad-hoc network, to provide communications among nearby vehicles and between vehicles and nearby fixed equipment, usually described as roadside unit (RSU) equipment. Networks (VANETs) represent a class of MANET. In VANETs the nodes are vehicles which are distributed and highly mobile and with limited degree of freedom [2]. In VANETs the high node mobility causes frequent topology change which greatly affects the network performance. Ad-Hoc Network is a wireless technology where all nodes are one level topology and can communicate directly with each other without the use of centralized nodes [3].

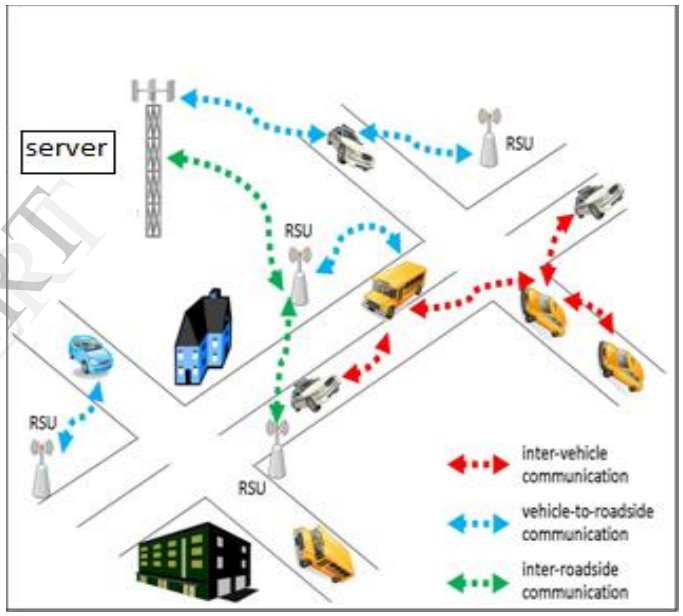

Fig.1 Structure of Vehicular Ad-Hoc Network

Here detection and elimination of unauthorized nodes in VANETs using two way handshaking process between server and each node using vehicle unique number (ID). For the provision of finding shortest path in a network, at the time of sending information from source to destination, DIJKSTRA'S shortest path algorithm is employed for entire network for the faster data transmission from source to the destination. To find the unauthorized nodes among the intermediate nodes, all the nodes are continuously monitored with the help of server. Server will determine the nodes as authorized as well as unauthorized nodes on the basis of database maintained at server. Database contain information of entire network i.e. each and every node which is actually received by the server in the form of acknowledgment.

Once the intermediate node is determined as the unauthorized node, the alternate shortest path is employed from current node 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 [4].

Usage of VANET:

VANET Technology is moving us from wired to wireless networks like Structured Networks (WLAN) and Unstructured Networks (Mobile Ad hoc Network - MANET). This technology is used for Analyzing data dissemination in VANETs. Vehicular Ad hoc Network – VANET used some technologies which are

1) Destination: remote geographic position :

Each node present in network announces its position periodically via broadcast to the server. Server (base station) knows all other nodes and their position in vehicular network.

2) Vehicles equipped with:

Vehicles are equipped with wireless transceivers as well as computerized control modules.

3) Road side unit (RSU)

- Drop unit
- Geographically relevant data
- Gateway to internet

4) Entertainment

- Internet access
- Multimedia entertainment
- Vehicle to vehicle / vehicle to server Communication (V2V / V2S)

With the rapid development of wireless communication technologies, location and sensors, a new decentralized (or semi-centralized) architecture based on vehicle-to-vehicle communications (V2V) [6]. This type of architecture relies on a distributed and autonomous system and is made up of the vehicles themselves without the support of a fixed infrastructure for data routing.

- Processing: With a large processing capacity on board, vehicles now a days are intelligent and are able to interpret the collected information with the purpose of helping the driver to make a decision (particularly in driver assistance systems).
- Storage: A large storage space is required in this context in order to store different classes and types of information. These data structures are updated via broadcast in the communication system.
- Routing and Communication: For information exchange and diffusion in the vehicular network itself or with other networks (IP or cellular for example). This permits to increase the vehicular safety with the help of two way handshaking communication environment and thus give a more accurate prediction of driving problems.

II.VANET Communication Requirements

i) Allowable latency:

It is defined as the maximum amount of time that should elapse between the generations of the message by the transmitter to its reception correctly by the receiver, or more precisely it is the time interval between the packet generation by the on-board device to the time it is received by the road station or vice versa. Allowable latency is especially important in safety applications where it must be very short (milliseconds); since a safety message is useful only for a short period of time and any large delay might not allow the vehicle to respond in time. In order to allow a moving vehicle to establish a connection with other/s vehicles or server, a certain amount of time is needed and that is called connection set up time.

ii) Communication service:

The communication service can be “Connection oriented” where the connection should be set before the information transmission and maintained until its end, or “Connectionless” where each individual message sent from the source contains the destination’s address and reaches the recipient without the need for establishing a channel. However, in connectionless services there is no guarantee of message reception. Therefore, the connectionless communication service can be divided into acknowledged and unacknowledged services. In acknowledged services the transmitter must receive an acknowledgement from the receiver to ensure correct message delivery, where the message is retransmitted in case of a negative acknowledgement or when no acknowledgement is received within a certain time. However, in case of unacknowledged service, since there is no guarantee of message reception and the latency is very low, the message is always repeated to increase the reliability. For safety messages that mostly have a broadcast nature acknowledgement is neither possible nor wanted; but for messages that use point-to-point communication acknowledgement together with re-transmissions can be used to reduce the packet loss rate.

iii) Addressing:

This is an important issue especially for applications that require point-to-point communication. Initially, the roadside units must have an IP address to enable the vehicles to transmit their information to the nearest available unit, this information can then be transferred to traffic centers using mobile communication or Internet. For client/server applications like download of digital maps a vehicle needs its own IP address. The addressing requirement is going to be very important in the future implementation of Internet services in ITS applications allowing for example vehicle communication with back office applications through the internet. However, for applications using broadcast communication, there is no need for addressing mechanisms since it is difficult for the transmitter to know the IP addresses of all the receivers due to the transiency in the relationship established.

III.Mobility Model in VANET

In VANETs the high node mobility causes frequent topology change which greatly affects the network performance. Mobility models play an important role in VANET simulations. Nodes location, density, and direction etc.VANET performance directly. The movement of the nodes and its position in the topology is represented by Mobility Models which is key components of simulation for both MANETs and VANETs routing protocol. Vehicular ad-hoc networks (VANETs) are considered to be the special application of infrastructure-less wireless Mobile ad-hoc network. Mobility Models in VANET are used for carrying reliable vehicle-to-vehicle and vehicle to road station services in an unreliable VANET environment has a range of factors. These variable factors of VANET are due to its multi-hop delivery mechanism with different network involvements[5].

In ad hoc network the VANET not only maintain but also update information on routing between all nodes of a given network at all times. One of the most important parameters in simulating ad-hoc networks is the node mobility. It is important to use a realistic mobility model so that results from the simulation correctly reflect the real-world performance of a VANET. A realistic mobility model should consist of a realistic topological map which reflects different densities of roads and different categories of streets with various speed limits. In this model, each node individually chooses a random destination in the network's geographical limit and also chooses a random movement speed (between a minimum and a maximum). Once the node reaches its destination, it makes a pause during a time period.

Then, the node repeats the process by choosing a different destination and random speed. In this case, mobile nodes move randomly and independently from roads topology. There are other mobility models called "group mobility models" which represent mobile nodes where movements are mutually dependent and which are adapted to applications involving group communications. To the development and definition of a mobility model, considering the characteristics and constraints of the modeled environment.

The main characteristics of VANETs for mobility

- High mobility of nodes
- No prior information about location of nodes
- Predictable topology (to some extent)
- No problem with power
- Crucial effect of security and privacy

IV.Background of Vehicular Communications

The original motives behind vehicular VANET communications were safety on the road, many lives were lost and much more injuries have been incurred due to car crashes. Driver realizing the brake lights of the car in front of him has only a few seconds to respond, and even if he has responded in time cars behind him could crash since they are unaware of what is going at the front. This has motivated one of the first applications for vehicular communications, namely cooperative collision warning which uses vehicle to vehicle communication. Other safety applications soon emerged as well as applications for more efficient use of the transportation network, less congestion and faster and safer routes for drivers. These applications cannot function efficiently using only vehicle to vehicle communications therefore an infrastructure is needed in the form of Road Side Unit (server) [7]. Although safety applications are important for governments to allocate frequencies for vehicular communications, non safety applications are as important for Intelligent Transportation Systems (ITS) for three reasons.

1) ITS systems rely on essential equipment which should be installed in every car and is widely available to the users. However, it is unlikely that individuals can afford such expensive equipment.

2) Safety applications generally require limited bandwidth for short intervals of time. Since bandwidth efficiency is an important factor, non safety applications are important to increase bandwidth efficiency.

3) The availability of RSU provides an infrastructure which can be used to provide a lot of services with only a little increase in cost [8].

Info station sends data to vehicles

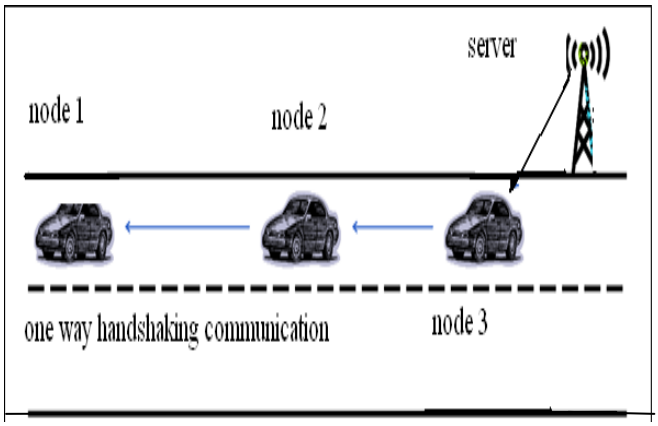

Fig: 2 Info stations (server) send data to vehicles

Fig.2 shows where a single info station is sending data to all vehicles traveling in the same direction along a highway. In such a system, each vehicle will maintain a buffer of all of the packets that it has received. When a vehicle chooses to transmit, it will randomly select one of those packets.

Since coordination among vehicles is undesirable, each vehicle will select a packet to transmit independently of all other vehicles. Whenever a vehicle receives a new packet, it will check whether or not the packet is a linear combination of them packets already stored in the vehicle's buffer. If the packet is a linear combination of packets that the vehicle has already received, then the vehicle can disregard the new packet [9]. On the other hand, if the new packet is linearly independent of the set of prior packets, then the vehicle adds the new packet to the buffer.

V.System Design

This Idea focus on detection and elimination of unauthorized nodes in VANETs using two way handshaking process between server and each node of network using vehicle unique number (ID). For the provision of finding shortest path in a network, at the time of sending information from source to destination, DIJKSTRA'S shortest path algorithm is employed for entire network for the faster data transmission from source to the destination.

To find the unauthorized nodes among the intermediate nodes, all the nodes are continuously monitored with the help of server. Server will determine the nodes as unauthorized nodes on the basis of database maintained at server. Database contain information of entire network i.e. each and every node which is actually received by the server in the form acknowledgment. Once the intermediate node is determined as the unauthorized node, the alternate shortest path is employed from current node 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 malicious nodes[4].

Initially server send data to every node and receive acknowledgment from each and every node, in this way communication is maintained between each node towards the server is carried out this is technique is also known as two way handshaking process. This helps to locate unauthorized node in our network. If we want to transfer data from source to destination user has to provide definition of source and destination. Then source will find out shortest path at its own with help of the DIJKSTRA'S shortest path algorithm and will start transferring data from source towards destination this data is transferred in the form of stream.

To transfer data between two nodes will take some fixed interval of time delay. A node is said to be connected with other node when the other node is within the range of first. In this time delay user will see current situation of system. In the mean time if user creates unauthorized node then server will come to know with the help of handshaking process which is carried out between all nodes and server. In this way server will know tracing location of malicious node in our system. Then server will transfer information about unauthorized node to source, so that source will define new path. Data which is stick at particular node is transferred toward destination using DIJKSTRA'S algorithm which have new path for data transfer. In this way unauthorized node is recognized and eliminated from data transferring path.

This Idea has following phases-

1) Managing network nodes.
2) Range Determination.
3) Establishing connection between nodes and server.
4) Server monitoring.
5) Communication between nodes.
   i) Source & destination node selection for data transfer.
   ii) Sending information of source and destination node to server.
   iii) Server send shortest routing path.
   iv) Initialisation of data transfer.
   v) Managing data routing and simultaneous detection for malicious node.
   vi) Providing new routing if any malicious node is detected by the server.
6) Release all resources after receiving data to destination node.

Dijkstra's Shortest Path Algorithm

Dijkstra's algorithm, conceived by Dutch computer scientist Edsger Dijkstra in 1956 and published in 1959 is a graph search algorithm that solves the single-source shortest path problem for a graph producing a shortest path tree.

One of the main reasons for the popularity of Dijkstra's Algorithm is that it is one of the most important and useful algorithms available for generating (exact) optimal solutions to a large class of shortest path algorithm. The point being that this class of problems is extremely important theoretically, practically, as well as educationally.

Requirements

- Works with directed and undirected graphs
- Works with weighted and un-weighted graphs
- Rare type of algorithm
- A greedy algorithm that produces an optimal solution

VI.Conclusion

This present work proposes Recognition and Elimination of Unauthorized nodes in VANETs using two way handshaking process between server and each node of network with the help of vehicle unique number (ID).

DIJKSTRA'S shortest path algorithm is employed for entire network for the faster data transmission from source to the destination. The proposed methodology and its results shows that by using this, one can easily recognize and eliminate the unauthorized nodes in the Vehicular Ad Hoc Network. In this project, we have concentrated only on finding them is behavior nodes in VANETs.

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.

References

[1] M. Sardari, F. Hendessi, F. Fekri, "DDRC: Data Dissemination in Vehicular Networks Using Rateless Codes", Journal of Information Science and Engineering, vol. 26, May 2010.

[2] M. Johnson, L. De Nardis, and K. Ramchandran, "Collaborative Content Distribution for Vehicular Ad Hoc Networks," Allerton Conf. Communication, Control, and Computing, Monticello, IL, September 2006.

[3] S. Lo and W. Lu, "Design of data forwarding strategies in Vehicular Adhoc Network," in Proc. VTC, pp.1-5, Apr. 2009.

[4] Prashant Sangulagi, Mallikarjun Sarsamba, Mallikarjun Talwar, Vijay Katgi "Detection and Elimination of Malicious Nodes in Vehicular Ad hoc Networks (VANET's)" Indian Journal of Computer Science and Engineering (IJCSE). Vol. 4 No.1 Feb-Mar 2013.

[5] Kun-chan Lan and Chien-Ming Chou "Realistic Mobility Models for Vehicular Ad hoc Network (VANET) Simulations" 978-1-4244-2858-8/08/$25.00 ©2008 IEEE.

[6] Rabah MERAIHI, Sidi-Mohammed SENOUCI, Djamal-Eddine MEDDOUR and Moez JERBI "Vehicle-to-Vehicle Communications: Applications and Perspectives". Published: 27 JAN 2010.

[7] Mainak Ghosh, Anitha Varghese, ArobindaGupta, Arzad A. Kherani, Skanda N. Muthaiah."Detecting misbehaviours in VANET with integrated root-causeanalysis". In Ad-hoc networks journal vol 8issue 7, September 2010, Pages 778-790.

[8] Sushmita Ruj, Marcos Antonio Cavenaghi, Zhen Huang,Amiya Nayak and Ivan Stojmenovic. "Data-centricMisbehaviour detection In VANETs".12 Mar 2011.

[9] Issam Khalil, Mohamed Morsi "Collaborating vehicles for increased traffic safety" Technical report, IDE0617, January 2006, Gothenburg, Sweden.