Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

International Conference on Mobility in Computing- ICMiC13, Organized by Mar Baselios College of Engineering and Technology during December 17-18, 2013 at Trivandrum, Kerala, India, pg.108 – 113

SURVEY ARTICLE

Security Enabled Junction-Based Multipath Source Routing Algorithm for VANETs

Ann Mary Jacob[1], Saritha S[2]

Dept. of Information Technology
Rajagiri School of Engineering & Technology, Kochi, India
[1]annmaryjac@yahoo.co.in; [2] saritha_s@rajagiritech.ac.in

Abstract— ***Junction Based Multipath Source Routing Algorithm(JMSR) is a geographic routing protocol, in the sense that it exploits the location of the nodes and also of the street junctions, known via digital street maps. JMSR is characterized as junction-based because it is a geographic or position-based routing protocol, where the junctions' positions are of much higher importance than the positions of the nodes themselves. The disadvantage of JMSR is that it does not specify how routing happens in presence of a malicious node. An improvement of JMSR is proposed through this paper. In this paper a method is discussed to deal with malicious nodes in VANETs.***

Keywords*— *VANETs; Junction-based Routing; Malicious nodes; Security attack; Packet duplication; Ranking.

I. INTRODUCTION

Vehicular Ad hoc Networks (VANETs) are a subclass of Mobile Ad hoc Network (MANET).VANET assists vehicle drivers to communicate and to coordinate among themselves in order to avoid any critical situation. It aims to provide:

(1)Connectivity while on the road to mobile users.

(2)Efficient vehicle-to-vehicle communications that enable the Intelligent Transportation Systems (ITS).

Some of the unique features of VANET include the following. The major feature is the geographically constrained topology. This means that unlike in MANETs the nodes in VANETs are not free to move around an area or surface. Rather they could only move within the roads formed by obstacles around them. An interesting feature of VANET is the large scale of the network, i.e, a network may consist of a large number of nodes that may either be too close or too far away. Finally power consumption is not a critical factor for VANETs [1]. Most widely used routing protocols in VANETs are Greedy Perimeter Coordinator Routing [3], Geographic Source Routing [4] or Connectivity-Aware Routing [5], use only one single route from the source to destination [6] handles each packet separately. The major conclusion of these routing protocols were that a single route is beneficial only when the number of intermediate nodes are less than 6.For large number of intermediate nodes it is better to include two routes. JMSR was designed to overcome mainly two drawbacks.

These drawbacks are:

(i)For large number of intermediate nodes it is better to have a multiple routes so as to distribute the traffic flow.

(ii)A location based routing is much more efficient than position-based routing.

In JMSR a location-based routing is used. Nodes being mobile change its position and hence it is not reliable to depend on the location of the nodes. Location based routing protocol is characterized by the fact that the location of junction is given importance than the location of the nodes. Thus whenever a route is identified from source to destination the intermediate nodes will be junctions, which are fixed points in the network. Once the route is identified the packets are forwarded to the nodes available in the junction at that particular time. Furthermore in order to provide an efficient traffic flow, two routes are identified at a time and the entire packet is distributed among them.

However this protocol does not specify how to deal with malicious nodes in the network. This paper proposes a mechanism by which the malicious node can be dealt with. The reminder of this paper is organized as follows: Section II gives a brief description about malicious nodes. Section III describes the designing of the proposed system and finally section IV concludes the paper.

II. BACKGROUND

In VANET nodes refer to the vehicles moving on the road. These vehicles are equipped with GPS facilities as well as the digital map of the city obtained using the GPS. Most of the modern vehicles are equipped with these basic requirements. In VANETs most of the nodes will be intermediate nodes and thus its major functionality will be to forward the packet. These intermediate nodes could act as a malicious node. Attacks in VANET [7] are classified depending on the Availability, Authentication /identification, Confidentiality, Privacy, Non-repudiation, and Data-trust. Fig.1 [9] gives an idea about classification of VANET attacks. The major categories of attacks are based on availability, authentication, confidentiality, privacy,non-repudiation and data trust. Calculation and sending affected message, this can be done by manipulating sensors in vehicle, or by changing the sent information [11].

A. Attack on Availability

Availability means the information in VANETs at any particular time. This type of attack includes Black-hole attack, malware, message tampering, spamming and denial of service attack. These attacks aim to make the information unavailable.

B. Attacks on Authentication/Identification

These attacks deal with the authentication or source information. Thus the source of information is questioned through this attack. These attacks include Masquerading, Replay Attack, Global Positioning System (GPS) Spoofing,, Tunneling, Sybil Attack, ID Disclosure.

C. Attacks on Confidentiality

Confidentiality is one of the important security requirement in vehicular communication, it assure that the message will only be read by authorized parties [11].An evesdropper can gather information thereby challenging the confidentiality of the message transmitted between two systems.

D. Attacks on Privacy

This type of attack is related with unauthorized accessing important information about vehicles. There is direct relation between driver and vehicle. If the attackers illegally access some data this directly affect the driver's privacy [11].

E. Attacks on Non-repudiation

When two or more user shares the same key then non-repudiation [11] is occurred. Due to this, two users are not distinguished from each other and hence their actions can be repudiated. An identical key in different vehicle should be avoided using a reliable storage.

F. Attacks on Data Trust

Data trust can be compromised by simply inaccurate data calculation and sending affected message, this can be done by manipulating sensors in vehicle, or by changing the sent information [11].

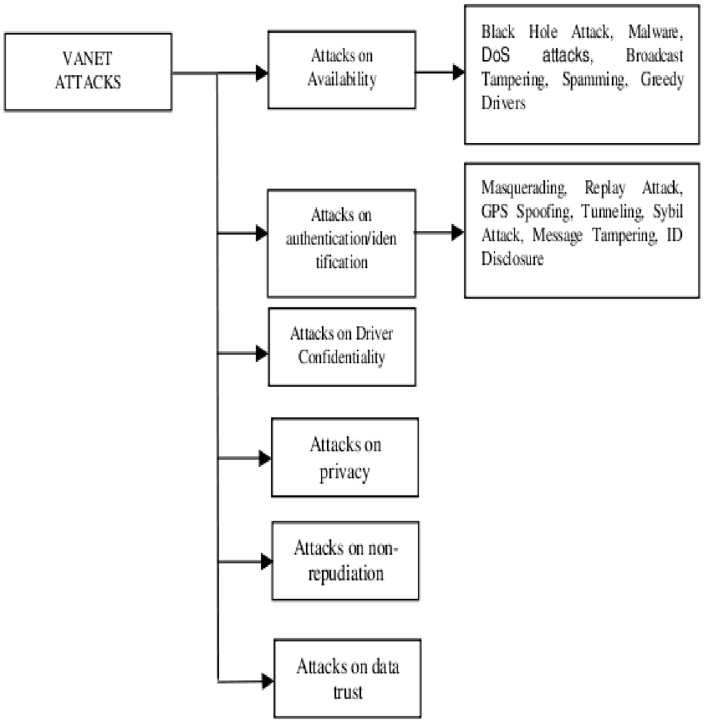
VANET ATTACKS
Attacks on Availability
Black Hole Attack, Malware, DoS attacks, Broadcast Tampering, Spamming, Greedy Drivers
Attacks on authentication/identification
Masquerading, Replay Attack, GPS Spoofing, Tunneling, Sybil Attack, Message Tampering, ID Disclosure
Attacks on Driver Confidentiality
Attacks on privacy
Attacks on non-repudiation
Attacks on data trust

Fig. 1 Types Of Attack

III. Design Of The Proposed System

In this paper focus is on the availability attack, mainly tampering of message. Tampering of message attacks include deliberately dropping packets instead of forwarding them and also the attacker jams the main communication medium and network is no more available to legitimate users. Packet header consists of a lot of information some of them include source address, destination address, TTL value etc. Modifying any of these fields will cause serious effect on routing. A malicious node could attempt to flood the network with its own unicast data packets, potentially using many different destination addresses.

Replaying packets in an ad hoc network is an attack that differs from replay attacks in conventional wired networks, in terms of both time and space. Malicious nodes can move to different areas of the network to replay data packets. A malicious node [10] could move as far away as possible from the destination node before replaying packets in order to involve more intermediate nodes, and to deplete their resources while forwarding the packets.

Here through this paper we propose a technique through which dropping of packets by intermediate packets can be avoided. This technique uses duplicating of packets and assigning a rank to each of the duplicates.

A. Construction of Graph From Digital Map

A digital map is a collection of data that is compiled and formatted into a virtual image. Digital maps are obtained using the GPS system. The primary goal of this technology is to provide an exact overview of the city. This also allows the calculation of distances from one place to other. As mentioned earlier the protocol being location based, there will be predefined junctions which will be marked in the digital map. These junctions will act as nodes for the graph. Now edges are established between two nodes if there is a communication range existing between those two junctions. Once the network is constructed the next part of the protocol is to identify route between source and destination. In order to provide an efficient traffic flow two routes are considered and packets are distributed among those two routes.

B. Identification of route and Forwarding of packets

The routes are identified using Dijkstra's algorithm and in-order for the routes to be farther apart the technique as specified in [2] is used. Once the routes are identified the next aim will be to forward the packet. Since for each intermediate node to be aware of the route through which to deliver the packet, the source node injects the entire route information inside the packet. Thus each intermediate node will checks the header for the next hop information and thereby forwards the packet. This process goes on until the packet reaches the destination.

C. Dealing with Malicious Nodes

Once the source node has generated the packet with the header consisting of route information, the packet needs to be forwarded. Being junction based protocol, the packet is forwarded depending on the junctions. It checks to see if a node is available in the junction. Hello beacons are used to ensure the presence of nodes. When a node is identified the packet is forwarded to that particular node.

Now, suppose that the node is a malicious node. When the packet arrives the node, it can simply discard the packet. The source node without knowing that the node was a malicious one, it assumes that the packet was delivered at the destination. One way to deal with this is to forward the packet to more than one nodes in the particular junction [2].This works well for a position-based routing protocol. However implementing this in location-based protocol will lead to flooding .The same idea can be used but in a modified form to handle malicious nodes.

The source node sends the packet to three nodes in the junction. It is obvious that all nodes in the network is not malicious and that among the three nodes atleast one is not a malicious. Now using the JMSR protocol, each of these three nodes will forward the packet to three other nodes in the next junction. If the nodes have forwarded the packet to three different nodes, then it will result in nine packets at intermediate junction two. Now these nine will be forwarded and these goes on each time the number of packets get increasing. This will finally result in flooding.

The source node when injecting the route information it also injects a rank to the packet. The same copy of the packet is duplicated thrice and each of them is given a rank, say for the first packet rank1, second rank2, and finally third rank3.

Now the nodes which receive the packet will broadcast a packet saying it receives a packet and also its rank. The node with highest rank (rank1) will only forward the packet to the next junction. Here also, the same duplication and ranking is done by the node. The other nodes have to monitor whether the node with highest rank is forwarding the packet. If the other nodes which also received a copy finds that the packet was forwarded it drops the packet it have.

Now if the packet with highest rank was received by a malicious node two things can happen

A. The node will not broadcast that it receives the packet.
B. The node will broadcast the information but will not forward the packet.

If the node hasn't broad-casted the information then the node with the next highest rank (rank 2) will take up the duplication and forwarding of packets. Now if the second option was that happened then the other nodes will identify that the packet was not forwarded and so assume the one with rank 1 is malicious. So the node with next rank will take up the duplication and forwarding.

IV. CONCLUSION

Junction-based routing technique provides a novel reliable routing protocol for VANETs. In VANETs there can occur malicious nodes also.. Malicious nodes can cause different types of attack. This paper deals with a sort of denial of service attack. The proposed method is based on duplication of packets and assigning a rank to each of these packets. The future enhancement of the protocol includes dealing with other types of attack, mainly replay attack, where a modified copy is forwarded by the malicious node.

REFERENCES

1. I. Broustis and M. Faloutsos, "Routing in vehicular networks: Feasibility,modelling and security," International Journal of Vehicular Technology,vol. 8, Mar. 2008.

2. P Sermpezis, G Koltsidas, and F Pavlidou," Investigating a Junction-based Multipath Source Routing algorithm for VANETs",Communications Letters, IEEE ,mar. 2013.

3. C. Lochert, M. Mauve, H. F □ ßler, and H. Hartenstein, "Geographic routing in city scenarios," ACM SIGMOBILE Mobile Computing and Communications Review, vol. 9, pp. 69–72, Jan. 2005.

4. C. Lochert, H. Hartenstein, J. Tian, H. Fuessler, D. Hermann, and M. Mauve, "A routing strategy for vehicular ad hoc networks in city environments," in Proc. IEEE Intelligent Vehicles Symposium ,Jun.2003.

5. V. Naumov and T. Gross, "Connectivity-aware routing (CAR) in vehicular ad-hoc networks," in Proc. 26th IEEE International Conference on Computer Communications (INFOCOM), Anchorage, AK, USA, May 2007, pp. 1919–1927.

6. B. Karp and H. Kung, “GPSR: greedy perimeter stateless routing for wireless networks,” in Proc. ACM/IEEE International Conference on Mobile Computing and Networking, Boston, MA, USA, Aug. 2000.
7. S Shrivastava ,S Jain ,”A Brief Introduction of Different type of Security Attacks found in Mobile Ad-hoc Network”,Satyam Srivastava International Journal of Computer Science & Engineering Technology
8. F. Wang, D. Zeng, and L. Yang, "Smart Cars on Smart Roads: an IEEE Intelligent Transportation Systems Society Update," IEEE Pervasive Computing, Vol. 5, No. 4, pp. 68 - 69, 2006.
9. A Dhamgaye, N Chavhan,”Survey on security challenges in VANET”,IJCSN International Journal of Computer Science and Network, Vol 2, Issue 1, 2013.
10. P Golle,D Greene,J Staddon,” Detecting and Correcting Malicious Data in VANETs”,VANET’04, October 1, 2004, Philadelphia, Pennsylvania, USA.Copyright 2004 ACM 1-58113-922-5/04/0010 .
11. Fuentes, José María de, Ana Isabel González-Tablas,and Arturo Ribagorda. "Overview of security issues in Vehicular Ad-hoc Networks." (2010).