A Secure Routing Protocol for VANET

Chandrabhaga Patil , Dr. K . R. Nataraj2
1 M.Tech-IV Sem, Digital Communication and Networking (Dept. of EC&E), S.J.B.I.T, Bangalore-560060, India
2 HOD, Dept. of Electronics &Communication Engineering, S.J.B.I.T, Bangalore-560060, India

Abstract- Vehicular Ad hoc Networks (VANETs) is the new wireless networking concept of the wireless ad hoc networks in the research community. Vehicle-to-Vehicle (V2V) communication plays a significant role in providing a high level of safety and convenience to drivers and passengers. Routing in VANET is a major challenge and research area. Position based routing protocol has been identified to be suitable for VANETs because of frequently changed network topology and highly dynamic nature of vehicular nodes. Many position based routing protocols have been developed for routing messages in greedy forwarding way in VANETs. However, few of them are efficient when the network is highly dynamic. Security is a main issue nowadays in VANET because malicious drivers in the network disrupt the system performance In this paper we present a secure position based routing protocol known as Secure B-MFR protocol ,designed to find and efficient routing path with minimum hops and relay the data by encrypting with secrete key. Simulation results shows Secure B-MFR protocol shows better results than MFR in terms of end to end delay, packet reception ratio and number of hops.

***Keywords*: Vehicular ad hoc network (VANET), most forward within radius (MFR), Border node based most forward within radius (B-MFR), Security.**

I INTRODUCTION

VANETs (Vehicular Ad Hoc Networks), a combination of ad hoc networks, cellular technology and wireless LAN, is an emerging technology. It is frequently employed to boost traffic security and ease the traffic flow on busy or congested roads. This is the technique through which wireless technology is implemented in vehicles, and each vehicle acts as a node that can potentially forward traffic towards the destination, thereby forming an ad-hoc network which nodes can join and depart in a very dynamic manner. Therefore, it is also known as Inter-Vehicle communication (IVC) or vehicle-to-vehicle (V2V) communication [1].The nature of nodes in VANETs is extremely dynamic; hence a well-organized routing protocol for VANETs is a necessity.

As shown in Figure 1, the architecture of VANETs falls in three main categories:

- **Inter-vehicle communication:** This is also known as vehicle-to-vehicle (V2V) communication. In this category, the vehicles communicate among each other with no infrastructure support. Any valuable information collected from sensors on a vehicle can be sent to neighbouring vehicles.
- **Vehicle-to-roadside communication:** This is also known as vehicle-to-infrastructure (V2I) communication. In this category, the vehicles can use cellular gate ways and wireless local area network access points to connect to the Internet and facilitate vehicular applications.
- **Inter-road side communication:** Vehicles can use infrastructure to communicate with each other and share the information received from infrastructure with other vehicles in a peer-to-peer mode through ad hoc communication. This architecture includes V2V communication and provides greater flexibility in content sharing.

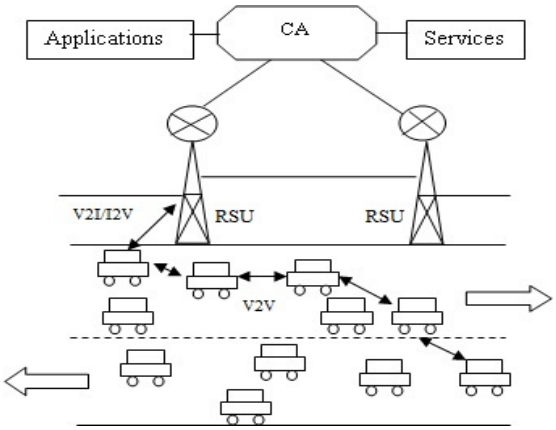

Fig.1 VANET Architecture

VANET have some characteristics. First, no stable infrastructures are available, so vehicles must setup an ad hoc network to communication and may not use any base stations. Second, due to the high speed of vehicles, network topology and states may change rapidly. Nodes may perhaps have no long communication session time, while power and memory are not problems in VANET. Third, VANET may have many building obstacles between nodes in city urban

environments, which make potential network data exchange availability impossible.

Routing is the process of finding optimal path between source and destination node and then sending message in a timely manner. Routes between source and destination node may contain multiple hops. Since the network topology in the VANETs is frequently changing, finding and maintaining routes is very challenging task in VANET. Position-based routing protocols such as GPSR, GPCR, GSR, A-STAR, CAR, MFR, Greedy Routing [6] etc are more suitable than other routing protocols.

Security is the main issue in VANET routing because nowadays active and passive attacks [3], [16], are the most dangerous threats to the network performance. These attacks lead to alteration of the messages and degrade the road safety issue and many malicious drivers are entering into the network to create disruptions and reduce the network performance. In this paper, Secure position based routing protocol is designed to find an efficient routing path and relay the data by encrypting it with the Session Key (SK).We are using Border-node based Most Forward within Radius routing (B-MFR) [10] which uses the concept of border-node within the sender's communication range to minimize the number of hops between source and destination. After finding the border node the main thing is to check whether the node is genuine or not, for that station to station key management protocol is used which does not uses a third party for checking the nodes genuineness but it uses the CAs certificates for the vehicles to check whether the node is a genuine node or imposter node. Simulation results shows Secure B-MFR shows better results than MFR in terms of end to end delay and packet reception ratio and number of hops.

The rest of this paper is organized as follows. We discuss the related work in section 2. In section 3, the design of Secure B-MFR routing protocol is introduced. Section 4 presents the simulation phase in which the Secure B-MFR protocol is compared with MFR. Finally, we conclude this paper in section 5.

II.RELATED WORK

MFR is a well-known method for finding a route in a network by utilizing position information of nodes [7]. The neighbor with the greatest progress on the straight line is chosen as next hop for sending packets further. Therefore MFR forwards the packet to the node that is closest to the destination node in an attempt to minimize the number of hops. In Figure 2, S and D denote the source and destination nodes and the circle with radius R indicates maximum communication range of source node S. The source node S has five neighbors within its communication range. It selects node an as next hop for forwarding packet to the destination since the projection A' of A on the line SD is closest to destination D.

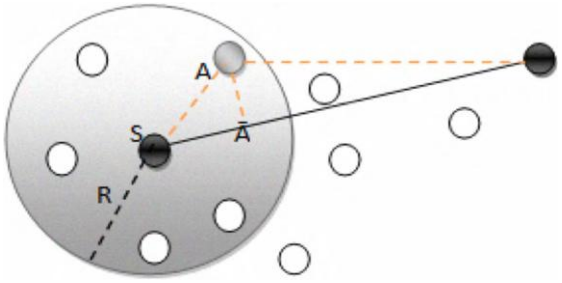

Fig.2 Most forward within radius forwarding method.

In MFR, next-hop neighbor node is decided through unicast forwarding by using the position information of the sender node, its next neighbor nodes, and the packet destination node. To obtain the position information of the next neighbor node, each node (vehicle) within the communication range send a beacon or a Hello packet containing their identity (ID), the current position and other important information (see figure 3) in the network. On the reception of a Hello packet from the neighbor node, the receiving node obtains the position information of its neighbor node. In the greedy position-based routing scheme, a source node finds the position information of its direct neighbor nodes and selects that direct neighbor node which is nearest to the destination node as the next-hop node.

Vehicle's Hello Packet				
ID	Location	Speed	Current time	Direction

Fig.3 Format of Hello Packet

III.PRAPOSED WORK

A. Assumptions

The Secure B-MFR protocol design is based on the following assumptions.

- Border nodes are used for forwarding packets.
- Hello control messages are exchanged between next-hop neighbors.
- Nodes (vehicles) are equipped with GPS receiver.
- No other communication infrastructure is available.
- Forwarding direction is always towards destination.
- Message is decrypted only at the destination using secrete key.

B. Border-node based Most Forward within Radius Protocol (B-MFR)

A border node [8, 9] is defined as a peripheral node, whose distance from the central node is exactly Ro, which is equal to the maximum transmission range R of the central node.

Next-hop forwarding method like greedy forwarding scheme for linear network does not support well in highly mobile ad hoc network such as vehicular ad hoc network. Therefore, other position based protocols such as MFR, GEDIR, Compass routing, etc. have been used for

VANET to improve its performance for non-linear network in a high vehicular density environment. These protocols can be further improvement by utilizing farthest one-hop node in a dense and highly mobile network. In this paper, we propose a routing protocol that uses Border-Nodes with maximum projection. We call this protocol Border-node based Most Forward within Radius (B-MFR). This method selects the border-node as a next-hop node for forwarding packet from source to destination. In this method, a packet is sent to the border node with the greatest progress as the distance between source and destination projected onto the line drawn from source to destination.

In figure 3, node A is a border-node of source node S, since node A is positioned at maximum transmission range and has maximum progress distance SA' where A' is projection of A on SD. Therefore, A is selected as the next hop forwarding node. Node A is the next-hop forwarding node when it receives the message from S. It uses the same method, to find the next forwarding node with greatest projected distance towards destination. In this case, node B is selected as a border node of A for forwarding packets to destination. Finally node B directly delivers the message to destination node D.

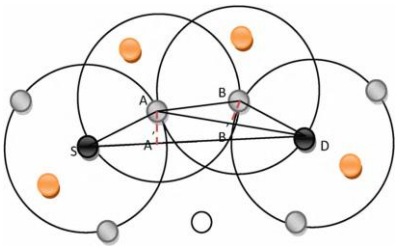

Fig.4. B-MFR forwarding method

B-MFR Algorithm steps:

1. Each Node (Vehicle) broadcast the Hello packet to its Neighboring node (Neighboring vehicle)
2. The source node check whether the destination node is in communication range
   If(Destination stored id==destination id received)
   Data is sent by encrypting with Secrete key (SK)
   Else
3. Calculate the Euclidian distance between source node and the neighbouring node
   i.e. $d(p,q)=Sqrt((p_1-q_1)^2+(p_2-q_2)^2)$,where (p_1,p_2)=source node position ,(q_1,q_2)=Neighbouring node position
4. If (maximum Euclidian distance $d_i(p,q)$of NN_i==r)
   Set of border node
   Else
   Set of internal node
5. Source node forwards the data to border node which is closest to the destination.

C. Secure data delivery phase

Notations:

R1: value calculated by source node
R2: value calculated by border node
X: large random number (0≤x≤p-1) chosen by source node
Y: large random number (0≤y≤p-1) chosen by border
P: large prime number
G: generator of order p-1
(P, g): public
e: public key of source node /border node to verify the signature

1. Source node sends a message to border node to establish a SK
2. Source node and border node chooses two numbers p and g
3. source node calculates R1
   $R1=g^x \bmod p$
4. First message R1 is send to border node
5. R2 is calculated by border node
   $R2=g^y \bmod p$
6. SK is calculated by border node
   $SK= (R1)^y \bmod p$
7. Second message is to source node which includes R2.
8. SK is calculated by source node
   SK= (R2)xmod p
9. SK is shared
   $SK= (R1)^y \bmod p=(g^x \bmod p)^y \bmod p$
   $SK= (R1)^x \bmod p=(g^y \bmod p)^x \bmod p$
   $SK=g^{xy} \bmod p$
   // $SK_{source\ node}==SK_{border\ node}$
10. Message is send from source node to border node by encrypting it with secrete key (SK).

IV. SIMULATION RESULT

The performance of secured B-MFR protocol is compared with the MFR by considering the 8 circular region with 5 vehicles in each region and the GPS range of each vehicle to find the inner vehicle is considered as 30 m and threshold value considered as 10 to find the border node which is in the range of GPS range plus threshold value. Starting Token ID took as 23 and the number of iterations considered as 20 and the number of packet sent per second is 200.The performance is evaluated by considering the time taken to transmit the packet (end to end delay) and packet reception ratio as a performance parameter. As security mechanism is used in secure B-MFR routing protocol to check packet dropping attack, the end to end delay is quite less than MFR. The packet delivery ratio for secure B-MFR is much higher than MFR and number of Hops also less than MFR. Figure 5 shows a route discovered from source to destination. Figure 6 shows the end to end delay. Figure 7 shows the packet reception ratio of Secure B-MFR and MFR .

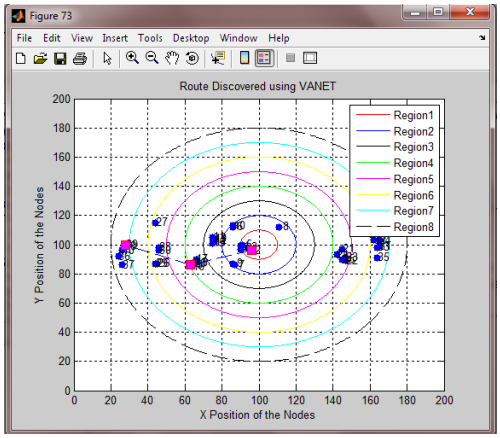

Fig. 5 Route discovered between source to destination

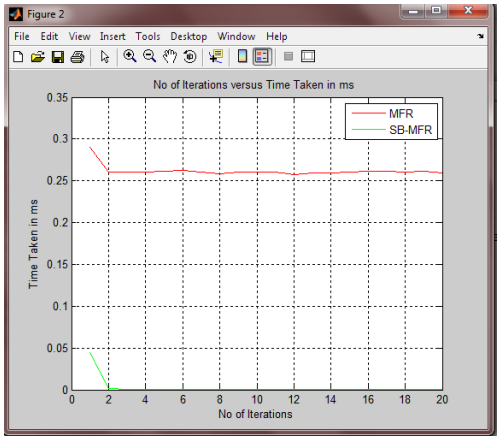

Fig.6. End to end delay

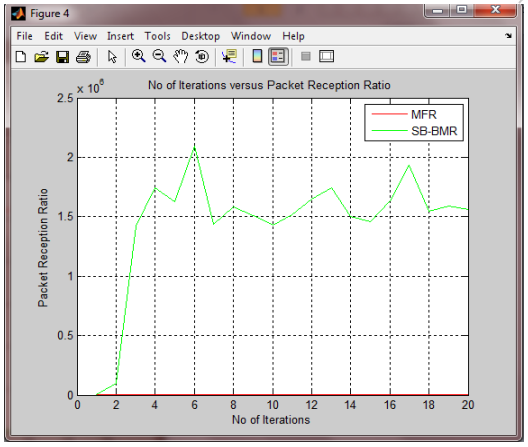

Fig.7. Packet reception ratio

V. CONCLUSION

The routing of data packets in VANETs is challenging and subject of intensive research. In this paper we have taken position-based routing protocols proposed for V2V communication among vehicular ad hoc networks (VANETs).The secure B-MFR routing protocol provide better performance in terms of packet reception ratio and end to end delay. When packet dropping attack occurs to the system it is difficult to resist for MFR ,as Secure B-MFR uses the secrete key to encrypt the message using secrete key by doing this the attacker not able to decrypt the message.

In future this algorithm is expanded by adding the concepts V2I communication and we can add concept of traffic lights to control road traffic and congestion. The delay in sending the data can be reduced by finding new solutions for communication void problem and optimal path problem. Image processing techniques can also be used to track persons on roads (catching terrorists).

REFERENCES

1. F. Li, and Y. Wang, "Routing in vehicular ad hoc networks: A survey," *IEEE Vehicular Technology Magazine*, vol.2, no.2, pp.12-22, June 2007
2. T. Leinmuller, E. Schoch, and F. Kargl, "Position Verification Approaches for Vehicular Ad Hoc Networks," *IEEE Wireless Communications*, vol.13, no.5, pp.16-21, October 2006
3. Y. Gongjun, S. Olariu, and M. Weigle, "Providing location security in vehicular Ad Hoc networks," *IEEE Wireless Communications*, vol.16, no.6, pp.48-55, December 2009
4. S. Zeadally, R. Hunt, Y. S. Chen , A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenge," *Telecommunication System*, Volume 50, Issue 4, pp. 217-241, August 2010
5. R.S. Raw, and D.K. Lobiyal, "B-MFR routing protocol for vehicular ad hoc networks," *Networking and Information Technology (ICNIT), 2010 International Conference on*, pp.420-423, 11-12 June 2010
6. U. Nagaraj, M. U. Kharat, and P. Dhamal, "Study of Various Routing Protocols in VANET," *International Journal of Computer Science & Technology*, vol. 2, Issue 4, pp 45- 52 Oct. Dec. 2011
7. K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET", *IEEE Journal on Selected Areas in Communications*, Vol. 25, No. 8, Oct. 2007.
8. X. Liu, Z. Fang, and L. Shi, "Securing Vehicular Ad Hoc Networks," *IEEE 2nd International Conference on Pervasive Computing and Applications*, pp.424-429, 26-27 July 2007
9. T. Leinmuller, E. Schoch, and C. Maihofer, "Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks," *IEEE 4th Annual Conference on Wireless on Demand Network Systems and Services*, pp. 84-91, 2007
10. H. Hartenstein, and K. P. Laberteaux, "A Tutorial Survey on Vehicular Ad Hoc Networks," *IEEE Communications Magazine*, pp. 164-171, Jun 2008
11. C. Langley, R. Lucas, and H. Fu, "Key Management in Vehicular Ad-Hoc Networks," *IEEE International Conference on Electro/Information Technology*, pp.223-226, 18-20 May 2008
12. M. Burmester, E. Magkos, and V. Chrissikopoulos, "Strengthening Privacy Protection in VANETs," *IEEE International Conference on Wireless & Mobile Computing, Networking & Communication*, pp. 508- 513, 2008
13. T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "Security and Privacy Issues for Inter-vehicle Communications in VANETs," *IEEE Sensor, Mesh and Ad Hoc Communications and Networks Workshops*, pp. 1-3, 2009
14. F. Schaub, Z. Ma, and F. Kargl, "Privacy Requirements in Vehicular Communication Systems," *IEEE International Conference on Computational Science and Engineering*, pp. 139-145, 2009
15. F. Sabahi, "The Security of Vehicular Ad hoc Networks," *IEEE Third International Conference on Computational Intelligence, Communication Systems and Networks*, pp. 338-342, 2011
16. J. M. de Fuentes, A. I. Gonzalez-Tablas, and A. Ribagorda, "Overview of security issues in Vehicular Ad-hoc Networks", *IGI Global*, 2011.