ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

A Border Node Based Routing Protocol for Partially Connected VANETS with Communication Security

Karthick Kumar S[1], Venkatakrishnan P[2]

PG Student, Department of ECE, K. L. N College of Information Technology, Pottapalayam-630 611, Sivagangai, India[1]

Professor, Department of ECE, K. L. N College of Information Technology, Pottapalayam-630 611, Sivagangai, India[2]

Abstract-Vehicular ad hoc networks (VANETs) are a growing research area primarily on efficient routing protocol design with foreseen applications including safety, traffic and infotainment services. VANETs are the promising technology to enable the communication between nodes in rural areas rather in urban areas and hence it is a challenging task to establish a routing reliability in partially connected environment with privacy and security which characterize to be a delay tolerant network. In this paper we examine the challenges of VANETs in partially connected networks using Border node Based Routing (BBR) protocol where the protocol achieves high routing reliability at low node density and high node mobility. Path discovery algorithm is proposed between the communication points with secret key generation for secure transmission. Simulation results with ns2 reveal interesting insights and trade-offs related to packet delivery ratio and packet delays for partially connected networks.

Index terms- VANETs, ad hoc routing, sparse networks, Border node Based Routing protocol, delay tolerant network, communication security.

I.INTRODUCTION

Vehicle communication networks are designed to provide drivers with real-time information through vehicle to vehicle or vehicle to infrastructure communications. Vehicle communication methods often rely upon the creation of autonomous, self-organizing wireless communication networks, or vehicle ad hoc networks (VANETs) designed to connect vehicles with fixed infrastructure and with each other. Research projects such as COMCAR [2] and DRIVE [3] have examined how vehicles in a network communicate with each other or with the external networks, such as the Internet, through the use of such communication infrastructure as wireless cellular networks. Other projects, including FleetNet [4] and NoW (Network on Wheels) [5] have explored ad hoc network techniques.

Recent improvements in mobile ad hoc network (MANET) technology and ever-increasing safety requirements as well as consumer interest in Internet access have made VANETs an important research topic. Vehicle to vehicle and vehicle to roadside communications have become important components of vehicle infrastructure integration. Most of the VANET research has focused on urban and suburban roadway conditions, where the numbers of vehicles are large, the inter-vehicle spacing is small, terrain is not a significant factor and fixed communication infrastructure is available. In rural and sparse areas, the conditions and constraints are significantly different. Node densities are low, inter-vehicle spacing can be large, terrain effects may be significant and there is very little or no fixed communication infrastructure available. The coverage provided by wireless carriers is predominantly in urban areas and along major highways, not in rural areas and minor roadways.

In this paper we propose a Border node Based Routing (BBR) protocol for partially connected VANETs. It is defined as a means of reducing flooding and ensuring the use of intermittently available communication bandwidth. Using ns2, we evaluate the performance of the BBR protocol with suitable routing solutions. Privacy and security issues are paid more attention in making the efficient communication

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

protocol. To future evaluate the BBR protocol performance on a VANET under sparse network conditions, we compare and evaluate the BBR protocol with Hop greedy routing scheme.

The remainder of this paper is organized as follows: Section II related research work on routing protocol design for partially connected networks. The proposed BBR protocol is discussed in Section III. We present the results comparing the BBR protocol with Hop greedy protocol in section IV. The conclusion is drawn in the final section.

II. RELATED WORK

The automotive industry is currently undergoing a phase of revolution. Today, a vehicle is not just a thermo mechanical machine with few electronic devices rather; recent advancement in wireless communication technologies has brought a major transition of vehicles from a simple moving engine to an intelligent system carrier. A wide spectrum of novel safety and entertainment services are being driven by a new class of communications that are broadly classified as vehicle-to-vehicle communication and vehicle-to-infrastructure communication. Routing of data in a vehicular ad hoc network is a challenging task due to the high dynamics of such a network. Recently, it was shown for the case of highway traffic that position-based routing approaches can very well deal with the high mobility of network nodes. However, baseline position-based routing has difficulties to handle two dimensional scenarios with obstacles (buildings) and voids as it is the case for city scenarios [6]. An ad hoc network that uses the generalized message relay approach is also called a Delay Tolerant Mobile Network (DTMN) [7]. Data delivery in partially connected ad hoc networks is generally based on the store-and-forward message relay approach [8]-[11]. A message ferrying approach was presented in [10], where a set of special mobile nodes called message ferries move around the deployment area according to known routes while other nodes transmit data to distant nodes out of range by using the ferries as relays. Currently, intelligent transportation system components provide a wide range of services such as freeway management, crash prevention and safety, driver assistance, and infotainment of drivers and/or passengers. Although various hierarchical algorithms exist for computing shortest paths, their heavy pre computation/storage costs and/or query costs hinder their application to large road networks [12]. By detecting a hierarchical community structure in road networks, a community-based hierarchical graph model that supports efficient route computation on large road networks. The current domain of vehicular research includes routing, congestion control, collision avoidance, safety message broadcast, vehicular sensing, security, etc. Since vehicles communicate through wireless channels, a variety of attacks such as injecting false information and replying to the disseminated messages can be easily launched. VANETs based on the security parameters offers conditional privacy preservation: while a receiver can verify that a message issuer is an authorized participant in the system only a trusted authority can reveal the true identity of a message sender. Second, it is spontaneous: safety messages can be authenticated locally, without support from the roadside units or contacting other vehicles. Third, it is efficient: it offers fast message authentication and verification, cost-effective identity tracking in case of a dispute, and has low storage requirements [13]. A security attack on vanets can have severe harmful or fatal consequences to legitimate users. Here we discuss the problems and the corresponding motivations.

CONNECTIVITY AND DISCOVERY PROBLEM

Here the problem is discussed with using the Hop Greedy algorithm. Multihop information dissemination in VANETs is constrained by the high mobility of vehicles and the frequent disconnections. By detecting a hierarchical community structure in road networks, we develop a community-based hierarchical graph model that supports efficient route computation on large road networks To obtain destination position, some protocols use flooding, this can be detrimental in city environments. Further, in the case of sparse and void regions, frequent use of the recovery strategy elevates hop count. However, the shortest path or the path with higher connectivity may include numerous intermediate intersections. As a result, these protocols yield routing paths with higher hop count [1]. It has the major disadvantage that it does not work in sparsely connected networks and once a decision has been made

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

in Greedy routing algorithms it is never reconsidered. The short term solutions made by the greedy routing leads to long term worst outcome. And using this Greedy algorithm is not automatic.

SECURITY PROBLEM

In view of the potential to revolutionize the driving experience and create a new traffic flow control framework, VANETs are receiving increasing attentions from academia and industry. Traffic related messages, such as traffic events, current time, the position, direction and speed of the vehicle, are broadcast to improve the driver environment, and thus plays a key role in VANET applications. Though extensive research efforts have been made by both industry and academia to investigate key issues in VANETs, it cannot be deployed and applied without the guarantee of security and privacy since the attacks may jeopardize the VANET's benefits. In order to resist the modification and replay attack using previously disseminated messages, authentication of the message issuer is mandatory to reduce the risk of such attacks [14]. At the time of authentication, the user-related private information of a vehicle should be hidden; otherwise user's location and moving patterns will be traced by the attacker. Thus, anonymous safety message authentication has become a fundamental design requirement for securing VANETs.

III.BORDER NODE BASED ROUTING (BBR) PROTOCOL

In this section we present a Border node Based routing (BBR) protocol for partially connected environment. The proposed routing is designed for sending messages from any node to any other node (unicast) or from one node to all other nodes (broadcast). The general design goals are to optimize the broadcast behaviour for low node density and high mobility networks and to deliver messages with high reliability while minimizing delivery delay.

The BBR protocol has two basic functionalities: a neighbourhood search discovery process and border node selection process. The neighbourhood search discovery process defines the neighbours that are within their one hop neighbour information. The border node selection process defines the node for packet forwarding based on the one hop neighbour information.

The overall performance of the BBR protocol with the path discovery algorithm is explained in the below described flow chart.

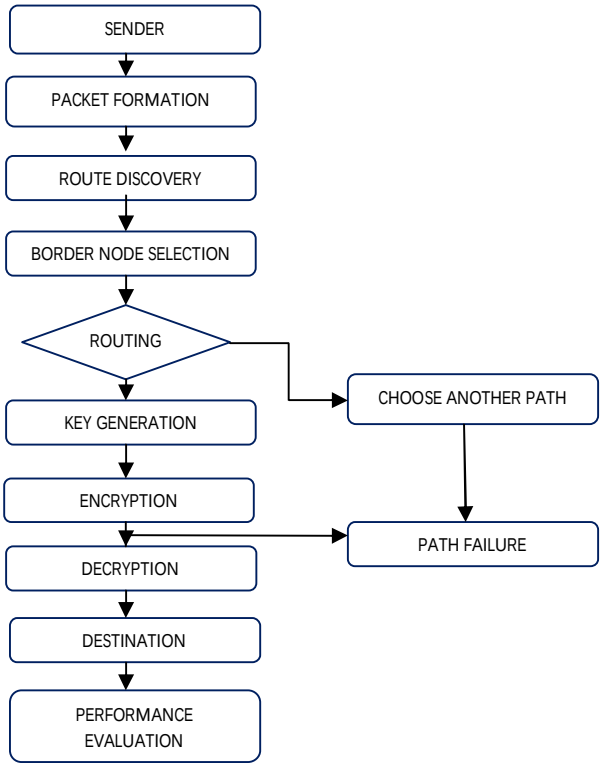

Figure 1 Algorithm description.

A. SYSTEM MODEL

The protocol design is based on the following assumptions. First, no node location information is available. Second, the only communication paths available are via the ad hoc network itself. Third, node power is not a limiting factor for the design. Fourth, communications are message oriented. Real time communication traffic is not supported. The protocol requires no assumptions regarding network topology, and can be applied to scenarios where the nodes are unconstrained as well as where the nodes are constrained to move on roadways, as explained and demonstrated below.

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

B. NEIGHBOURHOOD DISCOVERY PROCESS

Neighbourhood discovery process is defined as the process of selecting the current one hop neighbours within its transmission range, since all the nodes in its transmission range has its own neighbour set. Since all the nodes may be moving it may have different set of neighbours with its dynamic nature and since it should be frequently updated to form an efficient routing mechanism. Normally the neighbourhood discovery process is obtained between the nodes is realized by frequent exchange of HELLO packets. Where this forms the update procedure more efficient for updating its one hop neighbour. A node updates its neighbour node set after receiving HELLO messages from other nodes.

C. BORDER NODE SELECTION PROCESS

In the BBR protocol, border nodes are selected per broadcast event. A border node is defined as a node which has the responsibility of saving received broadcast packet/packets and forwarding the packet/packets when appropriate. For a group of nodes that receive the same broadcast message, only those nodes selected to be border nodes will keep the received data and rebroadcast it later when those nodes meet new neighbours. The selected border node must use broadcast, rather than unicast, as it has no knowledge of the trajectories of the nodes that are within its transmission range, or of their routing tables. The decision whether a node is a border node or not for a particular broadcast event is made independently by an individual node based on its one-hop neighbour information and the received broadcast information.

1. Discovery and problem solving for the selection of Border Nodes.

For discovering the Border nodes certain methods are determined with which each border node should have an ultimate one hop neighbour for its broadcasting behaviour of packets and forwarding when needed. The following terms are considered with similar approach.

Encircled: consider a node g is encircled by a node h. It means that g is within the transmission range of node h and it could receive packets from node h.

Neighbour nodes: The one hop neighbour of each node is called as the neighbour nodes. Now for node i the one hop neighbour set is denoted by N_i and the another node j has one hop neighbour set as N_j and the third node s which lies between i and j is called as the common neighbour node denoted as s € N_i and s € N_j.

2. Border node selection process.

With BBR algorithm, a source node that generates a data packet by default is chosen as the border node. Each packet has its own packet ID, generated by the originating node. The packet ID remains unchanged as the packet moves from source to destination. When a node receives a data packet, it first searches for the packet entry with the same packet ID. If there is, then the data packet is ignored. This approach conserves energy and bandwidth. Otherwise, the node checks the attached neighbour of the received data packet and carries out the following procedures based on the following cases.

Case 1: Single neighbour on the neighbour list of the broadcast packet. The node is the only node on the neighbour list. Then no border node selection will be carried out and it is a border node by default. The node will check its current one hop neighbour. If this node has no additional neighbour nodes within range, then it will store the data packet. It will carry this data packet and rebroadcast for a total of p times at different time points in the future when there are new neighbours within its transmission range. The rebroadcast parameter p is configurable and indicates the willingness of intermediate nodes to forward a data packet.

Case 2: Multiple neighbours on the neighbour list of the received broadcast packet. There are multiple neighbours on the neighbour list. Those nodes receiving the data packet for the first time will initiate two timers, an access delay timer T_{delay} and a maximum delay timer $T_{max\ delay}$. The timer T_{delay} is used to decide when a node needs to rebroadcast if it has to do so. The timer $T_{max\ delay}$ is used to decide when a node should initiate the border node selection process. The value of timer $T_{max\ delay}$ is used to decide when a node should initiate the border node selection process. The value of

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

timer $T_{max\ delay}$ is set to $T_{max\ delay}$=a× (n×Δt), where n is the total number of neighbours of received packet. The parameter Δt is the estimated transmission delay for sending one packet, which can be approximated, by (packet length / data transmission speed). The parameter a (a ≥1) is used to increase the value of the timer to make sure that a node receives all the rebroadcast packets that might be coming from the neighbours of the previous forwarding node.

The value of T_{delay} is set to T_{delay}= (i-1)* Δt, where i is the position of the node on the neighbour of the received packet. During $T_{max\ delay}$ each node in the group decides to rebroadcast or not when its T_{delay} timer expires. The decision is made depending on whether all its current one hop neighbours are covered or not, namely, whether they have received the broadcast packet information or not.

During the whole $T_{max\ delay}$ interval, each node will listen continuously. Rebroadcast packets from its neighbours will also be recorded and saved temporarily for the use of the border node selection procedure.

When $T_{max\ delay}$ expires, a node checks whether it is the node with the least common neighbour number with the previous broadcast source. If it is, it will select itself as a border node. Otherwise it is not a border node.

D. PATH DISCOVERY ALGORITHM

Usually, in Vehicular Ad hoc Network the vehicles act as a communication point which are also called as nodes. In general if the data is exchanged in a packet format, it is necessary to provide id for security purpose and are called packet ID. This algorithm initializes the data packets with packet ID and encodes the packet with secrete key. The routing process is established to find the efficient path. If the path fails it choose an alternate path to reach the destination. The receiver receives the original data and the decoding process occurs. The path discovery algorithm is described with the following steps.

Step 1:
Initialize the vehicular communication point (sender) VC_{ix}

Data is formatted into P_{ckt} and also P_{id}

Generate secrete key (Encode and Decode of the data) S_K

Switch over process (handoff) region H_{ax}

Encode the original information E_{Code} <- P_{id}

Step 2:
Initialize the routing process R_{ix}

R_{ix} <- E_{Code} + VC_{ix}

Path selection process (path discovery) P_D

Path selection process with routing
For (P_D =0; $P_D < N$; P_D ++)
if
P_D =0; //path failure
else
P_D =1; choose another path (H_{ax})
end if
end

Step 3:
Receive the original data (P_{id})

Decoding process D_{Code}

Extract original data using (D_{Code}) decode method
Original information received

Here, Path Discovery Protocol is used with handover process. Moreover, the data is transmitted to multiple regions in the network and if the Access Point (AP) of any one of its region is failure, then switchover/handover to another AP or Base Station (BS). The signal strength is analyzed using Key Algorithms in which the signal strength is compared with 0's and 1's, that means when it becomes '0', the signal has poor strength i.e., path failure. If the path is failure it chooses another path and it uses the encoded packet for secure transmission. Finally, to recover the original information; the encoded packets are decoded and overall network performance is calculated.

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

IV. SIMULATION AND RESULTS

The BBR protocol was implemented in ns 2[15]. The simulation part consists of the study of BBR protocol performance on a VANET in a sparse area. To make comparisons, the performance of the Hop greedy routing protocol is also evaluated under the same network configurations. Hop greedy routing protocol is chosen as the basis for comparison because it yields a routing path with the minimum number of intermediate intersection nodes while taking connectivity into consideration.

TABLE 1. SIMULATION PARAMETERS

Simulation software	ns 2	
Simulation area	1000×1000m^2	
Number of nodes	30	
Data rate	2Mbps	
Data traffic	Packet inter-arrival time	Uniform (1,3)s
	Packet size	Exponential average:1024 bits
BBR configurable parameters	Hello interval	2s
	Time delay slot	3 ms

Metrics measured to evaluate the protocol performance are defined as follows:

Packet delivery ratio: The ratio between the number of non-repeat packets delivered to the destination and the number of packets sent by the source.

Delay: The average end-to-end transmission delay calculated by taking into account only the packets non-repeatedly received.

A detailed comparison of these two protocols is shown in the figure for the delivery with Normal transmission and figure for the End to End delay with packet sending rate.

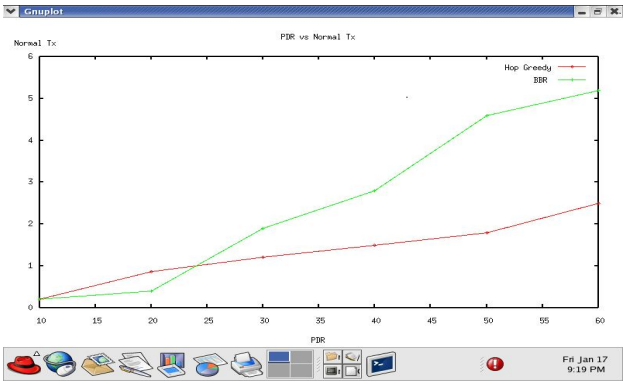

Figure 2. Packet delivery ratio vs Normal Transmission.

The above figure shows that when the radio range is very small and the network is highly partitioned, the packet delivery ratio with Hop greedy is close to 0 percent. The packet delivery ratios with BBR are also low at very small radio ranges but increase much more rapidly than with Hop greedy as the radio range increases. As discussed above, the packet delivery ratio of BBR is sensitive to the HelloInterval selected. For all simulations shown here, the HelloInterval is 2 seconds. Hence, the BBR routing protocol can yield much better performance than Hop greedy when a network is highly partitioned. This result is expected since packet delivery using Hop greedy is based on the discovery of connected route from source node to destination node at a specific time, which has very low probability when the network is highly partitioned.

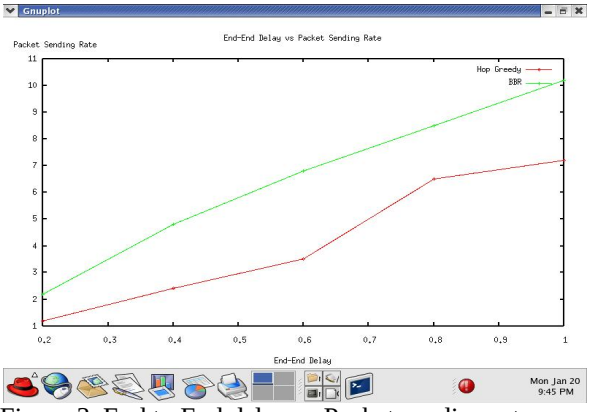

Figure 3. End to End delay vs Packet sending rate

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

The above figure shows the simulation results for average packet delay using BBR and Hop greedy protocol. We note that with Hop greedy, for short radio ranges, the packet delivery probability goes or equals to zero and the delay becomes infinite. For both protocols, the average packet delivery delay drops rapidly as the packet transmission range increases and node mobility also helps to decrease the packet delivery delay. The high delivery delay for BBR at low radio ranges is due to the network being highly partitioned. The delivery of packets is mainly dependent upon node movement. This also explains why the average packet delivery delay is shorter when node mobility is higher. The low delivery delay for the BBR at high radio ranges is the result of the network becoming gradually connected, and packet delivery is dependent upon more on wireless communications among neighbouring nodes instead of node movement. For Hop greedy, the high delivery delay is due to the low probability of finding an end to end path when the network is highly partitioned. Packets must be queued in the send buffer for long time intervals before the route discovery procedure is successfully completed.

For both routing protocols, high node mobility helps to reduce packet delivery delay but decreases the packet delivery ratio. For BBR, the packet delivery ratio is relatively constant over radio ranges considered, but the packet delivery delay is much longer when the radio range is small corresponding to a highly partitioned network. For Hop greedy, the packet delivery ratio remains low until the radio range increases sufficiently to make the network connected.

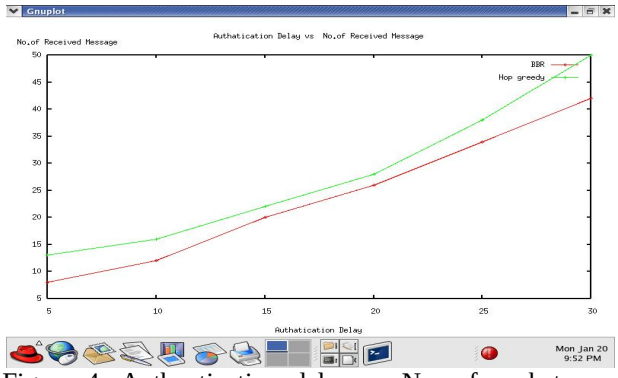

Figure 4. Authentication delay vs No. of packets received

The above figure show the total authentication delay using BBR and Hop greedy. It can be seen that as the number of packets increases the number of packets received, increases with delay in Hop greedy protocol. Also for a constant authentication delay, BBR outperforms with the maximum number of messages that can be authenticated and can be replaced with minimum delay. Consequently, BBR shows the message authentication by 88.78 and 48.04 percent compared to that of BBR and Hop greedy respectively.

V.CONCLUSION

The BBR protocol is proposed for partially connected VANETs. Using ns-2 the performance of the BBR protocol is evaluated. The simulation results indicate that the BBR protocol performs well for networks with frequent portioning and rapid topology changes. This new protocol is well suited for vehicle-to-vehicle communications along sparsely used highways, as would be the case in rural and remote areas. The BBR protocol may also have application in rural public safety networks, where responders must rely on ad hoc networks rather than fixed infrastructure and cannot assume connectivity. Where the communication security demonstrate that the proposed protocol not only provides conditional privacy, a critical requirement in VANETs, but also protects the secrecy of the communication content.

ACKNOWLEDGEMNTS

The author would like to thank Dr. P. Venkatakrishnan for his valuable comments on his work.

REFERENCES

[1]. Pratap Kumar Sahu, Eric Hsiao-Kuang Wu, Member, IEEE, Jagruti Sahoo, and Mario Gerla."BAHG: back-bone-assisted hop greedy routing for vanet's city environments", vol. 14 no. 1. March 2013.

[2]. Ericsson, "Communication and Mobility by Cellular Advanced Radio", ComCar project, www.comcar.de, 2002.

[3]. Online, http://www.ist-drive.org/index2.html

[4] FleetNet Project. Karlshue, Germany: Universitatverlag Karlsuhe, November 2005.

[5]. A. Festag, et al., "NoW-Network on Wheels: Project Objectives, Technology and Achievements", Proceedings of 6th International Workshop on Intelligent Transportations (WIT), Hamburg, Germany, March 2008.

[6]. G. Liu, B. S. Lee, B. C. Seet, C. H. Foh, K. J. Wong, and K. K. Lee," a routing strategy for vehicular ad hoc networks in city environments" in Proc. ICOIN, LNCS, Aug. 2004, pp. 134–143.

[7]. K. Harras, K. Almeroth and E. Belding-Royer, "Delay Tolerant Mobile Networks (DTMNs): Controlled Flooding Schemes in Sparse

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Mobile Networks", IFIP Netwoking 2005
[8]. K. Harras, K. Almeroth and E. Belding-Royer, "Delay Tolerant Mobile Networks (DTMNs): Controlled Flooding Schemes in Sparse Mobile Networks", IFIP Netwoking 2005
[9].Juang, P., Oki, H., Wang, Y., Martonosi, M., Peh, L., Rubenstein, D., "Energy-Efficient Computing for Wildlife Tracking: Design Tradeoffs and Early Experiences With ZebraNet". In ASPLOS (2002).
[10]. Wenrui Zhao, M.H. Ammar, Ellen Zegura, "A Message Ferrying Approach for Data Delivery in Sparse Mobile Ad Hoc Networks," MobiHoc'04, May 24-26, 2004, Roppongi, Japan
[11]. Shah, R., Roy, S., Jain, S., Brunette, W., "Data MULEs: Modeling a Three-Tier Architecture for Sparse Sensor Networks". In IEEE SNPA Workshop (2003)
[12]. Q.Song and X. Wang," efficient routing on large road networks using hierarchical communities" IEEE Trans. Intell. Transp. Syst., vol. 12, no. 1, pp. 132–140, Mar. 2011
[13]. lin x, sun x, ho p-h, shen x. gsis: "secure and privacy-preserving protocol for vehicular communications "eee trans veh technol 2007;56(6):3442–56
[14]. Zhang C, Lin X, Lu R, Ho P-H, Shen X." an efficient message authentication scheme for vehicular communications" IEEE Trans Veh Technol 2008;57(6):3357–68
[15]. The Network simulator- ns 2 http://nsnam.isi.edu/nsnam/index.php/user information,2012.