ijecs open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 8 August, 2014 Page No. 7959-7962

Efficient Routing in VANETs using Traffic Awareness

B. V. Visweswar Reddy[1], Dr. P. Bhargavi[2]

[1]M. Tech, Dept. of CSE
Sree Vidyanikethan Engineering College
Tirupati-517 102, Andhra Pradesh, India
visweswar.bijjam000@gmail.com

[2]Assistant Professor (SL), Dept. of CSE
Sree Vidyanikethan Engineering College
Tirupati-517 102, Andhra Pradesh, India
pbhargavi18@yahoo.co.in

Abstract*: The basic idea in VANETs is to have an adhoc connection between close by vehicles. The routing in vehicular networks is exposed to danger by the harmful nodes which aim to endanger the delivery of messages. Compromised nodes can extremely impact the performance of the network by capitalizing a number of attacks. To minimize these problems, a way of securing beacon-less routing algorithm for vehicular environments (S-BRAVE) against selective forwarding attacks using neighbouring nodes as guard nodes is developed. They watch for the message to be sent by the next forwarder, in case this vehicle does not forward the message, they take the responsibility of sending the message to the next hop. To increase the packet delivery ratio S-BRAVE routing algorithm is extended by including the traffic awareness of the roads, thereby routing the packets in a denser environment gives higher probability of delivering the packets to their respective destinations.*

Key words: Routing, traffic awareness, vehicular adhoc networks.

1. Introduction

Vehicular Adhoc Networks (VANETs) have come into view as a high prospective technology to empower new networking environments. They consist of a set of vehicles that are possessed with wireless interfaces that enable direct communication among the vehicles. By using the multi-hop communication vehicles, the data can be sent to other vehicles located outside their radio range. The Process of sending data to one or multiple destinations located several hops away from the sender is called VANET routing. The role of VANET routing protocol is to find the list of vehicles connecting the source and destination. In the context of VANET the nodes follow a confined movement pattern because vehicles advance the path across the streets.

Last few years, a large number of VANET routing solutions [1] came up. These routing protocols are based on the concepts of the traffic densities, geographic locations using maps of the area, and so on. There are some protocols which are simple like Greedy Parameter Coordinated Routing (GPCR) [2] and Connectivity Aware Routing (CAR) [3]. These protocols depend only on the control messages received by the vehicles. In both above protocols the main idea is to forward the messages along the roads and make the decision of routing when the packet reaches the junction.

Other protocols like Greedy Source Routing (GSR) [4] and Spatially Aware Routing (SAR) [5] suppose that the vehicles are equipped with maps of cities and use that information for the working of the protocol. The greedy routing is used to move the packet along the streets after finding the path by using the map. There are other protocols such as MOVE and GeOpps [6] in which routing decisions are drawn based on the directions of neighbouring vehicles. Each node takes data messages and each message is only advanced to a neighbour if its evaluated direction is better based on some routing metric. For example, GeOpps functions based on diminishing the evaluated time of delivery.

There are some other protocols that are based on the traffic on the roads such as A-STAR [7], improved Greedy traffic aware routing [8], MDDV [9], Vehicle assisted data delivery [10] and SADV [11] that assume not only the utilize of digital maps, but also knowledge about the traffic along the various streets. The objective is choosing routes with sufficient vehicles for the routing to advance. In GyTAR, the information of traffic density is used to decide the best path after reaching cross roads. A-STAR inflicts priority to streets passed over by bus lanes. In the same way, MDDV uses the figure of lanes in a street to value the significance of that street. VADD and SADV include holding period into their decisions. VADD evaluates the delay to pass over streets either through multi-hop forwarding or by any of the cars carrying the message.

SADV introduces static nodes in each cross road to reserve the messages until a vehicle passing down the desired street moves along.

Most of the above protocols include beacon packets for the routing process. Beacon packets are the 1-hop hello messages which are used by nodes to denote their positions. These packets consume the bandwidth of the network and interfere with the transmission of the data. To avoid the overhead, contention, etc. caused by beacons, beaconless geographic routing protocols like BOSS, BLR, GeRaF use a reactive neighbourhood discovery. That is, the current node routing the data packet broadcasts a message and neighbours answer with their positions.

The above said protocols have shown a great performance in terms of delivery ratio but are not able to deal with the certain situation like selective forwarding and sinkhole attacks, where malicious nodes try to impair the routing protocol by not forwarding the information to other nodes. Whereas, the S-BRAVE [12] can encounter above attacks but the performance is less when compared with others in case of packet delivery ratio. So, we use the statistical vehicular traffic information to determine the path of the packet at reactively at each node. Since the packet is passed through the high vehicular traffic path the connectivity between the vehicles is more and packet drops of nodes are less excluding the malicious nodes and increasing the packet delivery ratio.

2. Efficient and Secure Routing in VANETs

Most geographic routing protocols use the method of transmitting periodic beacons. The beacon packets are the control packets that have the information of the neighbour's position. To avoid too much overhead, responses are usually ordered according to a delay function and the first response cancels other responses. So, if a neighbour is better according to some routing metric than others it waits less time before answering and other neighbours cancels their responses. For instance, if the routing metric is distance to destination, the neighbour which provides more progress towards the destination answers first. This type of routing process is used in S-BRAVE mechanism. The above routing mechanism can also avoid the malicious nodes which endanger the delivery of packets. In the process of routing, the traffic awareness of the roads into account to stabilize a path between source and destination. This allows the protocol to avoid the trajectories which have less connectivity as the data travels to the destination.

2.1 Assumptions

We assume that each vehicle in the network is equipped with a Global Positioning System (GPS) and with this device the node can know its own geographic location. A sending node requires knowing the location of the destination in order to make the routing decision. This information is assumed to be provided by the location service like Grid Location Service (GLS) [13], [14]. Moreover, we consider that each vehicle can determine the position of its neighbouring junctions through the preloaded digital maps, which provides a street level map. The presence of such maps is a valid assumption when the vehicles are equipped with onboard navigation systems.

2.2 Traffic Awareness

Traffic awareness is the use of traffic information on a street. Traffic here refers to the vehicular traffic including cars, buses and other road way vehicles. It is known that in a metropolitan region, the streets are wider and can fit in with more vehicular traffic than the others. On such type of streets the vehicular nodes density is high. So, the connectivity between the nodes can be higher. With this consideration, value can be assigned to the streets based on the amount of traffic that fit within the street, i. e, the streets that can accommodate more traffic is given the lower value, the less traffic more value. The street map in use is assumed to be loaded with the above predefined value of streets based on the traffic. Such a map with pre-computed information is called a statistically evaluated map. The traffic conditions in the areas of a city are not always the same. It could be possible that forthcoming inter vehicular communication systems would be able to monitor the metropolitan traffic conditions and share such information to every vehicle connected to the vehicular network. This information could be used to recalculate the values of the roads on a map.

2.3 S-BRAVE Mechanism

In S-BRAVE there are four types of messages: DATA, RESPONSE, SELECT and ACK. If a node wants to send data to a destination, it broadcasts the DATA packet. After receiving the DATA packet the neighbouring nodes send a RESPONSE message after waiting for a period of time. The sender selects the neighbour whose RESPONSE message arrives first. Then a SELECT message is broadcasted so that other nodes will become aware of the next forwarder and go back to initial state. The selected node now starts the whole process again. If the forwarding node has no neighbouring nodes then it stores the message in the buffer and ACK message is sent. S-BRAVE employs the notion of watchdog nodes. Every neighbouring vehicle to the forwarding vehicle will act as a watchdog node. The vehicles that are not selected as the next forwarder will act as next forwarder and will try to ensure that the whole DATA forwarding process is completed. They keep on listening to the next forwarder of the packet, checking whether it retransmits the DATA message. If a watchdog node does not receive this message, it will take the role of the next forwarder by taking the responsibility of sending the DATA message to the next vehicle. They also schedule a timer that waits for the exchange to be succeeded within a period of time, or else the watchdog nodes concludes that a malicious node is attacking by preventing the packet from being delivered.

3. Use of Algorithm

The below shown algorithm finds the node in the effective path by calculating the pre-assigned values of the streets and forwards the message to the destination from the source.

Let us assume EP is the Effective Path from source to destination i. e, least value among all the path values from source to destination. The value of a path is the sum of all streets in a given path from source to destination. Here 'n' is the current node.

```
if n==sender
    find EP=least value path using Dijkstra algorithm
    send DATA
    await response
    if (neighbour's EP<=current node EP)
```

```
            send SELECT
        end if
    end if

    if n==dest
        EP=0
        send RESPONSE
        await to be selected
    end if

    if n== receiver
        find EP=least value path using Dijkstra algorithm
        send RESPONSE
        await to be selected
    end if
```

If a vehicle tends to send the message to a destination then the sender first calculates the value of the EP from the statistically evaluated map present in its navigation system. Once it is computed the EP value is broadcasted along with the DATA message to all the nodes. The sender waits for the response. The neighbour includes its EP value in the RESPONSE message. On receiving the response message the sender compares both the EP values and if the neighbours EP value is better than it selects that neighbour node as the next packet forwarder. If the receiver is destination then it sets its EP value to zero and responds to the DATA message and waits to be selected as next node. Once the exchange is complete it sends the ACK message to the forwarder.

When a vehicle receives a DATA message and if the node is the final destination it will immediately answer with a RESPONSE message, scheduling a timer to receive the SELECT message. If the previous sender receives the DATA message it will take that as a implicit acknowledgement for the data transmission. If the node is a guard node that receives the DATA packet it will cancel its timer of watching the packet. When a vehicle receives a RESPONSE message, it will send back to the most promising forwarder a SELECT message, also scheduling a new timer. On the other hand, if the vehicle is not the best forwarder, it will schedule a new timer to watch the messages exchange to act as a guard node.

When a vehicle receives a SELECT message and if it has already sent a RESPONSE message, it will be selected as the next forwarder. In case the vehicle is the final destination, it will send an ACK message back to the previous hop. Otherwise, it will broadcast the DATA message unless it will not have any neighbours around it. In the latter case, it will store the message in a buffer, answering with an ACK which specifies guard nodes will cancel their timers and will schedule new ones because the messages exchange is being performed correctly. If the vehicle that receives the ACK is the sender, it will cancel its timer assuming the whole messages exchange is completed. On the other hand, guard nodes will analyze the reason of sending this ACK. In case the message indicates a forwarding not heard by them, they will take the role of forwarders by broadcasting the DATA packet.

4. Performance Evaluation

4.1 Simulation Setup

We have compared the proposed mechanism and S-BRAVE within the Network Simulator NS-2 of version 2.34. To produce the simulation screenplay (street map) and the vehicular node movement patterns, we have utilized the popular Simulation of Urban Mobility (SUMO) road traffic simulator.

Vehicles move through 18 routes established in advance at a speed of 50 km/h at most in the city that crosses the scenario during 1000 seconds. In our simulations, the wireless signals propagate depending on the two-ray-ground model. Vehicles process their communications through an 802.11p interface card, applying the enhanced ns-2 802.11 physical and medium access control (MAC) models [15]. The transmission power is adjusted to allow a maximum transmission range of 250 m. Within this scenario we have simulated 5 runs for each configuration of density of vehicles, each of them with different traffic sources randomly selected.

4.2 Analysis of Results

We considered the packet delivery ratio (PDR) and end-to-end delay to evaluate the performance. We compared both the algorithms for a percentage of 10% malicious nodes that apply selective forwarding attack.

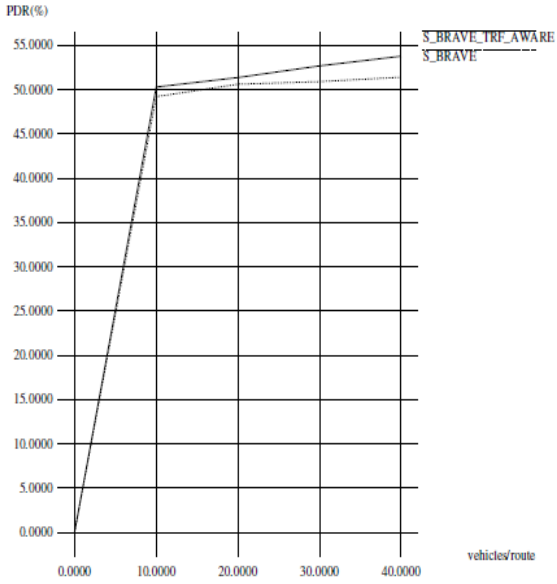
TABLE 1

Density of Vehicles	*S-BRAVE WITH TRAFFIC AWARENESS*		*S-BRAVE*	
	PDR%	Delay (ms)	PDR%	Delay (ms)
10	50.29	506.3	49.2	456.3
20	51.36	428.2	50.6	398.2
30	52.68	314.8	50.9	294.8
40	53.77	221.3	51.4	211.3

Performance of S-BRAVE with Traffic Awareness vs S-BRAVE

Figure 1. PDR% of S-BRAVE_TRF_AWARE vs S-BRAVE

Fig. 1 shows the performance of both approaches in terms of PDR%. The x-axis represents the number of vehicles per route and y-axis represents the % of packet delivery ratio. Analyzing the figure in more detail, we can see that the performance of S-BRAVE with traffic awareness is slightly greater than S-BRAVE. This is caused by the awareness of vehicular traffic



by which the data packets are passed through high traffic routes. Due to more traffic the false positives of the guard nodes are reduced.

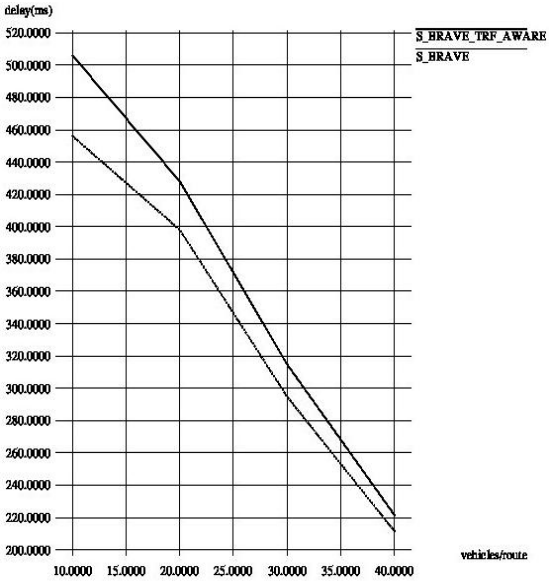


Figure 2. Delay of S-BRAVE_TRF_AWARE vs S-BRAVE

Fig. 2 represents the performance of both the approaches in terms of delay. The x-axis represents the number of vehicles per route and y-axis represents the delay in milliseconds. Analyzing the figure in more detail, we can see that the proposed approach suffers slightly more delay than S-BRAVE. This is due to the checking of the effective path value at every intermediate node involved in the routing process. The delay increases as the number of attackers in the network increases because if the nodes cannot find the legal forwarder in the presence of attackers it stores the data packet and forwards later.

5. Conclusion

In this paper we analyze the problems of efficient and secure routing in the vehicular networks. These are challenging due to the built-in effects of VANETs such as recurring disconnections, variable topology, constrained mobility, etc.
We proposed a method of routing by considering the traffic awareness of the streets for efficient routing and secure beaconless routing for securing the packets. The attacks like sinkhole and selective dropping can be mitigated. The delivery ratio of the packets can be increased but there will be slight increase in end to end delay. The mechanism can be extended by using dynamical information of the traffic on the roads.

References

[1] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: A survey," *IEEE Veh. Technol. Mag.*, vol. 2, no. 2, pp. 12–22, 2007.

[2] B. C. Seet, G. Liu, B. S. Lee, C. H. Foh, K. J. Wong, and K. K. Lee, "*Geographic Routing in City Scenarions*," December, 2004, pp. 989-999., in Proceedings of 3rd International Networking Conference IFIP-TC6.

[3] V. Naumov and T. Gross, "Connectivity-aware routing (car) in vehicular ad-hoc networks," in *Proc. 26th IEEE International Conference on Computer Communications (INFOCOM '07)*, Anchorage, Alaska, USA, May 2007, pp. 1919-1927.

[4] C. Lochert, H. Hartenstein, J. Tian, H. Fussler, D. Hermann, and M. Mauve, "A routing strategy for vehicular adhoc networks in city envi-ronments," in *Proc. IEEE IVS*, 2003, pp. 156–161.

[5] J. Tian, L. Han, K. Rothermel, and C. Cseh, "Spatially aware packet routing for mobile ad hoc inter-vehicle radio networks," in *Proc. IEEE ITSC*, 2003, pp. 1546–1551.

[6] I. Leontiadis and C. Mascolo, "GeOpps: Geographical opportunistic rout-ing for vehicular networks," in *Proc. WoWMoM*, 2007, pp. 1–6.

[7] B. Seet, G. Liu, B. Lee, C. Foh, K. Wong, and K. Lee, "A-STAR: A mobile ad hoc routing strategy for metropolis vehicular communications," in *Proc. IFIP-TC6 Netw.*, 2004, pp. 989–999.

[8] M. Jerbi, R. Maraihi, S. M. Senouci, and Y. Ghamri-Doudane, "Gytar: improved greedy traffic aware routing protocol for vehicular adhoc networks in city environments", in *VANET '06: Proceedings of the 3rd international workshop on Vehicular adhocnetworks*, New York, NY, USA: ACM, 2006, pp. 88-89.

[9] H. Wu, R. Fujimoto, R. Guensler, and M. Hunter, "Mddv: a mobility centric data dissemination algorothm for vehicular networks", in *VANET '04: Proc. of the 1st ACM international workshop on vehicular adhoc networks*, 2004, pp. 47-56.

[10] J. Zhao and G. Cao,"Vadd: Vehicle-asssted data delivery in vehicular adhoc networks", in *IEEE INFOCOM '06*, 2006.

[11] Y. Ding, C. Wang, and L. Xiao,"A static-node assistant adaptive routing protocol in vehicular networks", in *VANET '07: Proc. of the fourth ACM international workshop on vehicular adhoc networks*, 2007, pp. 59-68.

[12] J. A. Martinez, D. Vigueras, F. J. Ros, and P. M. Ruiz, "Evaluation of the Use of Guard Nodes for Securing the Routing in VANETs", in *IEEE Journal of Communications and Networks, Vol. 15, No. 2, April 2013.*

[13] J. Li, J. Jannoti, D. S. J. De Couto, D. R. Karger, and R. Morris, "A scalable locationservice for geographic adhoc routing," in *Proc. MOBICOM '00*, Boston, USA, Aug. 2000, pp. 120-130.

[14] I. Stojmenovic and B. Vukojevic, "A routing strategy and quorum based location update scheme for ad hoc wireless networks," SITE, University of Ottawa, Ottawa, Canada, Tech. Rep. TR-99-09, Sept. 1999.

[15] Q. Chen, F. Schmidt-Eisenlohr, D. Jiang, M. Torrent-Moreno, L. Delgrossi, and H. Hartenstein, "Overhaul of IEEE 802.11 modeling and simulation in NS-2", [Online]Available:http://dsn.tm.kit.edu/english/Overhaul_NS-2.php