International Journal of Security and Its Applications
Vol. 9, No. 6 (2015), pp. 89-100
http://dx.doi.org/10.14257/ijsia.2015.9.6.10

Reliable and Secure Routing ADHOC Algorithm Based on Collaborative Monitor Nodes in VANETS

Sun Yuezhongyi

Harbin University of Science and Technology, Harbin, China
hrb_zl@sina.cn

Abstract

There are always VANETs malicious nodes attempt to disrupt the message during normal delivery in the routing protocol of VANETs (Vehicular Ad hoc Networks). At the same time due to the dynamic changes of the vehicle, so that the topology of VANETs changes rapidly, it is very easy to make the communication link of vehicles attacked, or there is no reliable disconnection phenomenon. Based on this, it presents a secure and stable cooperative with node VANETs routing protocols (RSVR). First regular intervals to detect signal strength, residual energy and interface queue length, and then check the data transmission, while the message load and transfer process certificate for authentication, and then set the collaborative monitoring message passing node in the routing protocol, for messages can not be delivered to the destination node, which will serve as the task of passing messages, and adjust the final routing allows data transmission can selectively defense, or selective forwarding data. Experimental results show that RSVR packet delivery rate increase 15%, to consider combining overhead and latency, etc., it come in a wide range of node RSVR intensive environment, that has better reliability and security.

Keywords: *Collaborative Monitor node; Reliable and Secure Vanets Routing; Wireless Net; Data Communication Link; VANETs*

1. Introduction

Frequent accidents, worsening traffic congestion and strong user demand for Internet access jointly promote the development of Intelligent Transportation Systems (ITS) [1]. ITS can provide a wide range of applications, including improving road safety, traffic efficiency and entertainment. In order to realize these applications, vehicles will be equipped with sensors and communications equipment and form the communications network that is Vehicular ad-hoc network (VANET). In VANET, the vehicle collects information through the advanced sensing and interact information with other vehicles. These vehicles are equipped with an on-board unit (OBU) [2]. Vehicles can realize the function of receive / achieve information through the OBU. Vehicles can also communicate with static equipment side of the road, such as road side facilities (RSU). Therefore, VANETs support the Vehicle-to-Vehicle communication (V2V) and Vehicle-to-Infrastructure communication (V2I) [3-4].

Because of the High-speed mobile nodes and dynamic topology, the traditional wireless network routing protocols are difficult to directly apply to VANETs. For this reason, many scholars pay much attention to the routing scheme applicable to VANETs, such as GSR [4] (Geographic Source Routing) and GPCR [5] (Greedy Perimeter Coordinator Routing). GSR belongs to location-based routing protocol, which utilizes the geographic information as the amount of weight, and calculates the shortest path through the Dijkstra algorithm. Meanwhile, the greedy forward is used to choose the best route. However, GSR does not apply to the node sparse environment. When the node is scarce, there may be not enough nodes to forward packets. STAR also belongs to the location-based routing. Literature [6] proposes the STAR (Spatial and Traffic Aware Routing) program. Nodes are required to establish a neighbor table and a traffic table. According to the information in the table, the shortest path is chosen and the packet is greedy forwarded along the shortest path. With performance, STAR is better than GPSR (greedy perimeter stateless routing) [7]; however, STAR consumes more resources than GPSR. GyTAR program [8] (Improved Greedy Traffic Aware Routing) combines the vehicle density information and dynamic obtains the data information of the next anchor. Between the anchors the improved greedy algorithm is used to forward packets. When a packet is forwarded with local optimum, the caching forwarding mechanism is taken. Compared with other wireless networks, in addition to the unreliable and shadow fading outside in wireless transmission network, the implementation of VANETs still faces many challenges. Some strict real-time requirements like fast-moving vehicles, dynamic topology changes and security information add difficulties for the implementation of VANETs. When designing the communication protocol of VANETs these issues must be considered [9-10]. In order to solve the above problems, the IEEE 802.11p is proposed to be used in the MAC (Medium Access Control) of VANETs. However, the random access channel of IEEE 802.11p causes the without estimated delay and broadcast storms [11]. In addition, there are strict real-time constraints of secure message, and when it is necessary there are reliable broadcasting services. Therefore, the TDMA (Time Division Multiple Access) based on MAC protocol is called ADHOC MAC [12, 13], which is used to achieve the reliable broadcast and P2P (Point-to-Point) VANET communication. However, since the dynamic topology of VANET, TDMA MAC protocol may cause the waste of Time slot. When there are not enough neighbor nodes to use intra all time slots, waste of time slots is generated [14]. Moreover, once the data transmission fails, the source node will wait for the next frame to retransmit even if the channel is idle, because there is no available time slot in the frame. Accordingly, even if the IEEE 802.11p is used and MAC-based TDMA is under poor channel conditions, it is difficult to overcome the increase of packet loss and the decease of throughput.

Many techniques, such as diversity and channel coding can effectively alleviate the deterioration of the radio channel and improve the network throughput [15, 16]. However, these techniques will cause additional overhead or need multiple antennas. The common solution is cooperative communication, which through the nearby neighbor nodes improves the communication performance between the source nodes to the destination nodes. Broadcast nature of wireless transmission makes the neighbor node can receive data packets transmitted from the source nodes to the destination nodes. When the direct transmission between source nodes and the destination nodes is suffered by harsh channel conditions, a neighbor node will forward the packet to destination node with the help of the neighbor nodes. The neighbor nodes help the nodes retransferring data packets to destination nodes are called Helper Node. So for the MAC layer, the cooperative program is proposed, called as RSVR (Cooperative AD HOC MAC). Compared with TDMA and IEEE 802.11p, RSVR uses the distributed TDMA based on MAC protocol. In RSVR, nodes occupy their time slots and neighbor nodes form the clusters and share time frame. Through the collaboration on the link layer, the help node can use the idle time slots to retransmit the packets that failed to reach the destination node. By utilizing the idle slots to forward packets, the proposed RSVR protocol improves the throughput of VANET.

2. Proposed Method

In this section, the proposed system model of RSVR protocol is analyzed, including network topology, movement and node distribution.

A. Network topology and channel model and Neighbor Nodes

It is assumed that in VANET the vehicle moves along the multi-lane; vehicles are randomly distributed; there are L lanes, and the width of each lane is ω_l ; $l \in \{1,2,3,\cdots,L\}$; in the observation period the relative movement of the vehicles is ignored, therefore, it is relative stationary between vehicles. The communication range of vehicle is r . Within the communication range of the source nodes, the probability of successful transmission of the received packet is assumed as p . Probability p depends on the channel conditions. The smaller the p value is, the worse the channel condition is. Due to the simultaneous transmission of multiple nodes the collision is caused; in this case, p is not reflected.

Each vehicle maintains a list with one hop or two hops neighbor. One hop or two hops node is the refer node with the transmission distance as one hop or two hops. Accordingly, these neighbor nodes with one hop or two hops are totally called as One-Hop Set, Two-Hop Set. Shown in Figure 1, node A belongs to the two One-hop sets, which respectively are OHS1 and OHS2. In addition, node A also belongs to Two-hop set THS1. A node can directly communicate directly with other nodes within OHS1and OHS2. Similarly, among the nodes within the same THS it is communicated with two-hop.

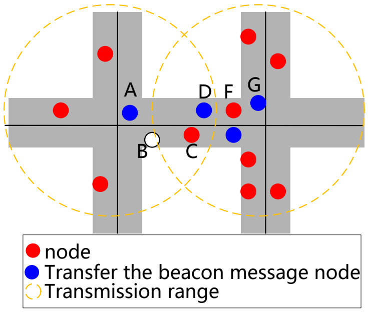


Figure 1. Sample of One-hop and Two-hop

B. Channel Access

Based on ADHOC MAC [17] and VeMAC [18], the proposed channel access mechanism is based on a distributed TDMA scheme. By TDMA, channel time is divided into different frames; each frame is further subdivided into time slots. The length of each slot is a fixed period of time; each frame contains a fixed number of time slots denoted as F . Each vehicle is able to identify the start of a frame and the start of a time slot. So it is synchronic with the required accurate time between nodes. Global Positioning System (GPS) can be installed in the car to achieve sync. In addition, with the RSVR, the node communication model is consideration as point-to-point. Helper node assists other nodes to retransmit the packet.

Multiple nodes can form two-hop neighbor cluster and the cluster is composed of a group of nodes with the maximum two-hop. There is no cluster head in the cluster, and the node can belong to multiple clusters. The nodes belongs to the same THS will compete for occupying one slot. To get the slot, nodes first spy the channel with F consecutive slots, and then try to occupy a slot. If multiple nodes simultaneously occupy the same slot, the access collision is generated. After it is successful access to the slots, node will transfer packet between the slot of each frame until meet the merging collision caused by relative movement [19]. Merging collision is the collision caused by the nodes belong to different clusters while use the time slot [5]. Literature [7] shows that due to the movement of the nodes, throughput is decreased. In order to overcome the decline of throughput, literature [9] proposes the VeMAC program. With the VeMAC, the slots are grouped into three disjoint groups, and three groups are respectively corresponding to the positive and negative direction of the vehicle and the RSU of the vehicle movement. In this way, the problem of decrease of throughput caused by vehicle movement is effectively solved.

The purpose of this study is to improve the transmission reliability, so it is considered that if all the nodes can strictly maintain synchronous and occupy the corresponding time slot, there is no access collisions happened. Also, it ignores the relative movement between the nodes and avoids Merging collision.

B. RSVR scheme

This section analyzes the specific programs of RSVR, including the collaborative decision-making choices and assisted selection. Nodes transmit packets in the occupied time slots. This data contains the frame information, cooperation head, header, load data and CRC (Cyclic Redundancy check), as shown in Figure 2.

RoadID	Location(x,y)	At junction (Yor N)	TTLJ or Channel load

Figure 2. Format of Packet

Wherein, RSVR program includes the data header and load data; CRC is the same with ADHOCMAC and VeMAC but different with the frame information. In addition, in the RSVR, the new content is introduced - Cooperation header.

As shown in Figure 2, FI is the set of ID area (IDF). The slot corresponding to each frame IDF, its address is less than 1-2bytes compared with MAC. The short ID makes nodes can be freely selected. Short ID reduces the size of data packet FI and thereby reduces the burden of MAC.

If the destination node D successfully receives the data packet in the time slot s^{th} from the source node, the time slot s^{th} belongs to node S. At this time, the node D stores the ID of the node S stored at the s^{th} IDF region of FI. Node S successfully receives data packet, and node D can obtain the following information: (a) node S is its one-hop neighbors; (b) node S occupies the time slot s^{th}; (c) node S belongs to the entire neighbors with one-hop and their corresponding slots. Thus, by successfully received FI information from the one-hop neighbor nodes, the node is to maintain its neighbor node table, including all hop neighbor nodes of (i); (ii) all two-hop neighbor nodes; (iii) time slots occupied by all these nodes. If there is no signal in a slot, there is no occupied slot of this node; in this case, the corresponding area of IDF is empty ϕ, as shown in IDF-2 2.

Cooperation is realized by the one-hop neighbor nodes between source nodes and destination nodes. Since the unoccupied time slots are the same with channel conditions of the time slots of the source node, there is no benefit for the source node to retransmit packets in unoccupied time slots, and there is a waste of transmission resources. In other words, in the unoccupied slot, through the independent channels, cooperative forwarding transmission of data packets is achieved to realize the data transmission diversity; thus the source node and the destination node can effectively transmit the data under the harsh channel conditions to improve the reliability of data transmission. Next, nodes' decisions and cooperation are analyzed.

It is supposed that time slot within a frame $\Gamma = \{1, 2, 3, \cdots, F\}$. O_x and T_x represent the OHS and THS of node x. $\Re_x$ represents all slots of THS belonging to T_x. The occupied time slots of the source node S and the destination node D are respectively s^{th}

and d^{th}. Node H is the help node. Only when all the following conditions are met, the forward transmission is set up.

(1) Failure of direct transmission

When direct transmission between the source node and the destination node fails, the cooperation is started. Once the transmission fails, the node D is beyond the communication range of the node S, *i.e.*, $S \notin \mathrm{O}_D$. After receiving FI information from the node D, the potential help node can get the failed transmission.

(2) Based on the purpose of retransmission, the help node successfully receives the data packet

Only when node successfully receives the data packets from source node S at time slot s^{th}, the node may make it cooperate and auxiliary transmit data, thereby performing retransmission.

(3)Destination node is within the communication range

When the destination node D can not receive data from the source node S, help node H can forward packets to the destination nodes D, which indicates that the node D is within the communication range of node H. Therefore, node D and S must be the one-hop neighbors of node H, namely $S, D \in \mathrm{O}_H$.

(4) There is an available time slot

When the condition (1), (2) and (3) are met, if there is at least one available slot $h \in \Gamma$, the help node H can offer cooperation. There is no collision of slot h and transmission H from its neighbor nodes, namely $\forall h \notin \Re_H$.

If these conditions are met, the help node H can offer cooperation for source node and destination node, and it can finish the cooperative transmission at slot h. If there are many potential help nodes, the first node answering will forward the packets, and becomes the help node. While there is no need for other potential help nodes dealing with the packet, that is, they will abandon cooperation.

Figure 3 shows that in the process of cooperation with RSVR, there is a exchange of necessary information. When the destination node D can not receive data packets from the source node S, as shown in 3 (a), the node D report this message through its neighbor nodes FI shown in Figure 3 (b). After receiving FI information, if cooperation is decided, this node (Assumed as node H) expresses its willing of cooperation through COH (Cooperation header), as shown in Figure 3 (c). Within the slot h^{th}, C-ACK (Cooperation acknowledgement) is received from destination node D, and the help node H transmits the packet, shown in Figure 3.

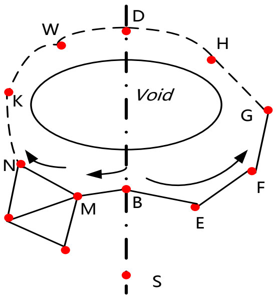


Figure 3. Information Exchanges Process of RSVR Program on the Cooperation Stage

C. Cooperation Confirmation

Once the nodes decide to cooperate, they will pass the cooperation willing through COH within the packet. COH contains the following information:

(a) Decisions of cooperation;
(b) Number of slots of the source nodes when the transmission failure occurs;
(c) Number of slots when the help node retransmits data for the destination node

The information above is loaded in COH and transmitted in the slot of the help nodes. Once the other potential receives cooperation decision from the help node, the cooperation willing is stoped. Thus, the node H becomes the first cooperative node offering service for routing from the source node to the destination node D. However, when both the potential help node are beyond the scope of OHS, they may collide at the destination node, so the destination node C-ACK (Cooperation acknowledgement) at the available time slot, as shown in Figure 4. With the C-ACK, the destination node loads the help node ID. Through C-ACK transmission, other potential nodes stop their transmission to avoid collisions.

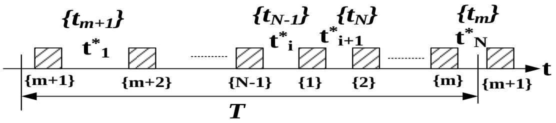


Figure 4. Transmitting Cooperative Acknowledge at Available Time Slot

D. Cooperation

When the transfer failed, cooperation will be started. Based on the previous analysis, once the following conditions meet, cooperation will be started.

(1) Event 1 (): There is at least a potential help node.
(2) Event 2 (): There is at least a slot UTS

Event E_1 depends on the channel conditions of the node from source node to the destination node. The event E_2 depends on the number of THS of the help node members, and E_1 and E_2 are independent. For a route the direct transmission is failed, the cooperation probability p_{coop} can be expressed as following:

$$p_{coop} = \Pr\{E_1\}\{E_2\} \tag{1}$$

Next, the probability of E_1 and E_2 are analyzed.

For two communicating entities of source node and destination node, OHS's number of neighbors obeys the binomial distribution. These nodes are potential help node. It is assume that the random variable Y represents these potential help nodes. The number of nodes within OHS from the source node to the destination node is Set as N_0, and $N_0 = k$. If $k \le 2$, there is no potential secondary node. If $3 \le k \le F$, $k-2$ node is supposed to be the help node. Thus, when $N_0 = k$, the probability mass function of Y is shown in formula (2):

$$\Pr\{Y=a\,|\,N_o=k\}= \begin{cases} 1, & \text{for}\, a=0 \text{if}\, k\le 2 \\ \binom{k-2}{a} p_s^a(1-p_s)^{k-a-2}, & \text{for}\, 0\le a\le k-2 \text{if}\, 3\le k\le F \\ \binom{F-2}{a} p_s^a(1-p_s)^{F-a-2}, & \text{for}\, 0\le a\le F-2 \text{if}\, k>F \end{cases} \tag{2}$$

When $Y>0$, event E_1 occurred. When $N_0=k$, the probability of occurrence of an event E_1 is as following:

$$\Pr\{E_1\,|\,N_o=k\}=1-\Pr\{Y=0\,|\,N_o=k\} \tag{3}$$

Combined with formula (1) (2) and (3), the probability of occurrence of the event E_1 is as follows:

$$\begin{aligned}\Pr\{E_1\}&=\sum_{k=3}^{F}\left(1-(1-p_s)^{k-2}\right)\frac{(1.5\rho r)^k e^{-1.5\rho r}}{k!}\\ &+\left(1-(1-p_s)^{F-2}\right)\left(1-\sum_{k=0}^{F}\frac{(1.5\rho r)^k e^{-1.5\rho r}}{k!}\right)\end{aligned} \tag{4}$$

For event E_2, if UTS exists within frame, event E_2 occurs, and the probability of occurrence is as follows:

$$\Pr\{E_2\}=\sum_{j=1}^{F-1}\frac{(2\rho r)^k e^{-2\rho r}}{j!} \tag{5}$$

According to formula (1), (4) and (5), the cooperation probability is calculated as p_{coop}.

It can be found that the start of cooperation does not necessarily guarantee the success retransmissions. Only when the help node forwards the data to the destination node, the cooperation takes effect, and earns benefit. Therefore, cooperative benefit represents the help node successfully forwarded the data, and the probability is p_s^{coop} :

$$p_s^{coop}=p_s+p_s(1-p_s)\,p_s^{coop} \tag{6}$$

E. Throughput

Throughput is defined as the ratio of the number of success slots STS in each frame F and the overall slots. σ and σ_{coop} are respectively the throughput of RSVR and ADHOC MAC shown in formula (7).

$$\begin{cases} \sigma=\dfrac{E[X]}{F} \\ \sigma_{coop}=\dfrac{E[X]}{F} \end{cases} \tag{7}$$

Normalized throughput gain is shown in formula (8) as follows:

$$\sigma_{gain}=\frac{\sigma_{coop}-\sigma}{\sigma} \tag{8}$$

3. RSVR Experiments and Analysis

In order to analyze the performance of RSVR, this section presents the mathematical model to evaluate the performance of RSVR throughput.

3.1. Simulation Parameters

It selects a relatively simple scenario in this simulation. There are 11 vehicles in total on the road of a four-lane and each lane width 2.5m of a 500m long highway. That N=11, in which the number of jammer respectively is 1, 3, 5. The initialization distribution of the vehicle is shown in Figure 5. According to IEEE 802.11p vehicle, transmit the beacon interval, the specific parameter values are as shown in Table 1.

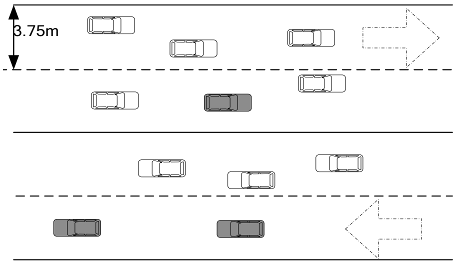


Figure 5. The Initial Distribution of the Vehicle

Table 1. Simulation Parameters

Variables	value
N	25
T	0.1s
AIFS	$100\mu s$
W	16
L	400 bytes
R	3 Mbit/s
σ	$13\mu s$
T_h	$52\mu s$

Under the three cases of $PER = 0, 0.01, 0.05$, it makes simulation. The ping times simulation is done 1000 times and analysis, detection rate, leak alarm rate and false alarm rate. Leakage alarm rate FNR (False negative rate) and the false alarm rate FPR (False positive rate), which leak alarm rate refers interference by those who are identified as non-interference ratio, the lower the leakage alarm rate is, the detection rates of interference were more higher. False alarm rate value represents the non-interference by those who are identified as interference ratio. It made simulation for two types of interference Random jamming case, ON-OFF, simulation results shown in Figure 6.

Figure 6 shows the initial stage of the time consumed. Three curves represent the three cumulative distribution function CDF while PER=0, 0.01, 0.05. It shows from the figure, the consumed time increases with the increasing of the PER. The elapsed time is less than 150ms while PER=0.01.

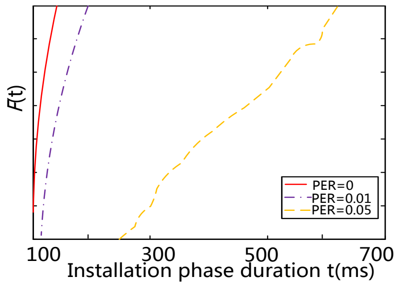
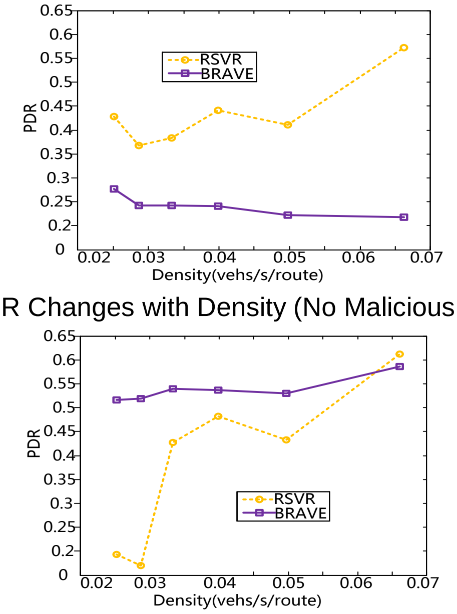


Figure 6. Cumulative Distribution Function CDF in the Initial Stage (Cumulative Distribution Function)

When analyzing the performance of two types of routing protocols, P% is assumed presence of malicious nodes in the network simulation, P% respectively was 0, 5%, 10%, 15% in the simulation. Also it assumed that the nodes of the network have enough buffer space. In this case, the node can store the certificate in a node encounters.

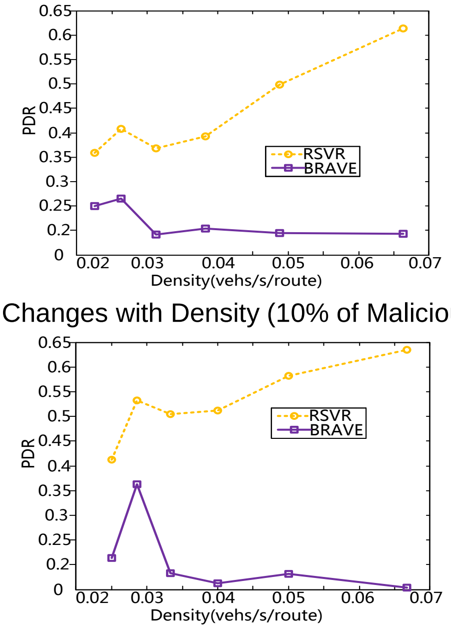
Figure 7 shows the changes with the two types of protocol packet delivery rate PDR in vehicle density. It shows from Figure 7(a) that, in the absence of malicious nodes, two types of routing protocols are up more than 80% packet delivery ratio. In the areas of sparse vehicle density, the PDR performance of RSVR bellows than BRAVE. As the vehicle density enhancement, RSVR performance gradually improved. When the vehicle density reaches 1/15, its performance is higher than the BRAVE.

It was seen from Figure 7(b) that, the PDR performance of two types of routing protocols decline rapidly. The PDR of RSVR varied within the region from 40 to 70% while the PDR of BRAVE only within the region from 10 to 30%, Compared to Figure 7 (a), the packet transfer rate has dropped by half.



(a) PDR Changes with Density (No Malicious Nodes)

(b) PDR Changes with Density (5% of Malicious Nodes)



(c) PDR Changes with Density (10% of Malicious Nodes)

(d) PDR Changes with Density (15% of Malicious Nodes)

Figure 7. Changes of PDR with the Density

Figure 7 (c) and Figure (d) show the PDR cases of malicious nodes of 10% and 15%. It knows from the figure, the PDR performance of RSVR is better than that of BRAVE. It can be seen from Figure 7 (c), in the case of 10% of the malicious nodes, BRAVE reached only 13% of the PDR; In the case of 15% of malicious nodes (Figure 7 (d)), the BRAVE reached only 10% of the PDR. Under similar conditions, the PDR of RSVR respectively reached 40% and 45%. This is mainly because when the vehicle density decreased, the RSVR can handle some of the attacks, but there are still selective forwarding attacks. When increasing vehicle density, so that there is more to monitor nodes to detect the attacker.

4. Conclusion

This paper analyzes the VANETs routing security issues. Firstly it analyzes the BRAVE routing protocol. Faced with high speed mobile of nodes, BRAVE requires the use of storage - forwarding policy.。For this reason, the introduction of interactive mechanisms to ensure the authenticity of the certificate and the integrity of the forwarding node forwards the message to the destination node. Meanwhile, for the safety of routing protocols, it will play neighbor nodes to monitor nodes and defense selective forwarding attacks. Monitoring node supervision forwarded the message, if found the forwarding node fails to deliver the message, it will monitor message forwarding node undertake tasks and achieve collaboration. To compare the two types of agreement RSVR and BRAVE, it uses the NS2 network simulation software. The simulation data shows that, the PDR performance of RSVR in terms of packet delivery rate is better than that of BRAVE. However, there are still some distance between RAVR and security routing protocols. In the vehicle sparse environment, due to the lack of neighbor nodes, the routing performance of RSVR is not gifted than that of BRAVE. But in the environment of dense vehicle, the PDR of RAVR is 15% higher than the BRAVE agreement. In addition, the RSVR has not been effectively improved in end transmission delay and controlling overhead, which is the focus of post-study work.

References

[1] H. Huang, H. Chen, R. Wang, Q. Mao and R. Cheng, "(t, n) Secret Sharing Scheme Based on Cylinder Model in Wireless Sensor Networks", Journal of Networks, vol. 7, no. 7, **(2012)**, pp. 1009-1016.

[2] United States Department of Transportation.Intelligent transportation systems, [Online]. Available: http://www.its.dot.gov/index.htm.

[3] H. Hartenstein and K. P. Laberteaux, "A Tutorial Survey on Vehicular Ad Hoc Networks", IEEE Communications Magazine, vol. 46, no. 6, **(2008)**, pp. 164-171.

[4] J. Isaac, S. Zeadally and J. Camara, "Security attacks and solutions for vehicular ad hoc networks", Communications, IET, vol. 4, no. 7, **(2010)**, pp. 894-903.

[5] M. Burmester, E. Magkos and V. Chrissikopoulos, "Strengthening Privacy Protection in VANETs", IEEE Int. Conf. Networking and Communications, 2008 (WIMOB '08), **(2008)**, pp. 508-513.

[6] Telecommunications and Information Exchange between Systems–Local and Metropolitan Area Networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments," IEEE Standard for Information Technology, **(2010)**.

[7] F. Borgonovo, A. Capone, M. Cesana and L. Fratta, "ADHOC MAC:New MAC architecture for ad hoc networks providing efficient and reliable point-to-point and broadcast services", Wireless Netw., vol. 10, **(2004)**, pp. 359-366.

[8] M. Hassan, H. Vu and T. Sakurai, "Performance analysis of the IEEE 802.11 MAC protocol for DSRC safety applications", IEEE Trans. Veh., Technol., vol. 60, no. 8, **(2011)** October, pp. 3882-3896.

[9] H. Omar, W. Zhuang and L. Li, "VeMAC: A TDMA-based MAC protocol for reliable broadcast in VANETs", to be published.

[10] Z. Lv and T. Su, "3D seabed modeling and visualization on ubiquitous context", SIGGRAPH Asia 2014 Posters, ACM, **(2014)**, pp. 33.

[11] Z. Lv, L. Feng, S. Feng and H. Li, "Extending Touch-less Interaction on Vision Based Wearable Device", Virtual Reality (VR), 2015 iEEE. IEEE, **(2015)**.

[12] D. Jiang, Z. Xu, P. Zhang and T. Zhu, "A transform domain-based anomaly detection approach to network-wide traffic", Journal of Network and Computer Applications, vol. 40, **(2014)**, pp. 292-306.

[13] Y. Geng, Y. Wan, J. He and K. Pahlavan, "An Empirical Channel Model for the Effect of Human Body on Ray Tracing", 2013 IEEE 24nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), London, Britain, **(2013)** September, pp. 47-52.

[14] Y. Geng, J. He and K. Pahlavan, "Modeling the Effect of Human Body on TOA Based Indoor Human Tracking", International Journal of Wireless Information Networks (IJWIN), vol. 20, no. 4, **(2013)** December, pp. 306-317.

[15] K. Pelechrinis, M. Iliofotou and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: the case of jammers", IEEE Commun.Surveys and Tutorials, vol. 13, no. 2, **(2011)**, pp. 245-257.

[16] W. Xu, W. Trappe, Y. Zhang and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks", 2005 ACM International Symposium on Mobile Ad Hoc Networking and Computing, vol. 6, no. 8, **(2005)**, pp. 34-42.

[17] W. Xu, W. Trappe, Y. Zhang and T. Wood. "The feasibility of launching and detecting jamming attacks in wireless networks", MobiHoc 05, Urbana-Champaign, Illinois, USA, vol. 34, no. 2, **(2005)** May 25-27, pp. 46-57.

[18] A. L. Toledo and X. Wang, "Robust detection of MAC layer denialof-service attacks in CSMA/CA wireless networks", IEEE Trans. Inf. Forensics and Security, vol. 3, no. 3, **(2008)**, pp. 347-358.

[19] A. Hamieh, J. Ben-othman and L. Mokdad, "Detection of radio interference attacks in VANET", 2009 IEEE Global Telecommunications Conference, vol. 6, no. 9, **(2009)**, pp. 45-56.

Author

Sun Yuezhongyi, male, was born in Harbin. His research Areas: Internet of Vehicles and Mobile Computing.