Trust-Based Routing for Vehicular Ad Hoc Network

Suparna DasGupta and Rituparna Chaki

Abstract Vehicular ad hoc networks are likely to become the most relevant form of mobile ad hoc networks with special requirements in terms of node mobility and comprise of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. The deployment of vehicular communication systems is strongly dependent upon their underlying security and privacy features. The effective trust management schemes for VANETs have been given the dire consequences of acting on false information management. The urgent nature of communication necessitates that messages should be signed and verified before they are trusted and it should be done to keep secrecy of vehicles real identity. Prerequisite to communicate within VANETs is an efficient route between network nodes which must be adaptive to the rapidly changing topology of VANET. In this paper, we have proposed a new trust-based efficient routing protocol for VANETs and provide the solution for avoiding the channel congestion and performance bottleneck problem. Conducted simulation experiments on different scenarios show the performance analysis and effectiveness of the new proposed routing protocol for vehicular ad hoc networks.

Keywords Vehicular ad hoc networks · Security · Privacy · Trust · Congestion

S. DasGupta (✉)
Department of Information Technology, JIS College of Engineering, Kalyani, West Bengal, India
e-mail: suparnadasguptait@gmail.com

R. Chaki
A.K. Choudhury School of Information Technology, University of Calcutta, Kolkata
West Bengal, India
e-mail: rituchaki@gmail.com

R. Chaki et al. (eds.), *Applied Computation and Security Systems*, Advances in Intelligent Systems and Computing 304, DOI 10.1007/978-81-322-1985-9_13

1 Introduction

Vehicular ad hoc networks is a wireless network that is formed between vehicles on demand basis and have become a popular area for both the academic research community and automobile industry, with specific attention to improving driving experience and road safety. As the vehicles change their location constantly, there is a continuous demand for information on the current location and specifically for data on the surrounding traffic, routes, and much more.

In vehicle-to-vehicle (V2V) communication, three broad categories of architecture are related, such as infrastructure-based, ad hoc networks, and hybrid. The infrastructure-based architecture takes advantage of the existing cellular networks. This network has few drawbacks as: high operation cost, limited bandwidth, and symmetry channel allocation for uplink and downlink. As infrastructure do not required in ad hoc networks, the cost of building such network will be very low and it can even operate in the events of disasters. The hybrid architecture combines these two architectures by considering vehicles as data relays between roadside base stations. This architecture also requires the function of multi-hop communication between vehicles, which is the essential part of ad hoc network architecture.

VANET consists of vehicles and road-side units as network nodes and enables inter-vehicle communication or IVC along with the road side-to-vehicle communication, i.e., RVC. Road conditions such as congestion, collisions, or constructions are shared by vehicles through VANETs. IVC and RVC can be divided into two categories, such as: safety-related applications and infotainment applications. Besides the fundamental security requirements, sensitive information, i.e., identity and location privacy should be preserved; on the contrary, traceability is required where the identity information needs to be revealed. In addition, privilege revocation is required by network authorities. V2V and vehicle-to-infrastructure (V2I) communication can enable a range of applications to enhance transportation safety and efficiency as well as infotainment.

VANETs face many interesting research challenges in multiple areas, from privacy and anonymity to the detection and eviction of misbehaving nodes. Securing vehicular communication is a tough problem due to tight coupling between application and the network fabric, as well as additional social, legal, and economical consideration, which raise a unique combination of operational and security requirements. Privacy and security are important issues in vehicular networks. Users wish to maintain location privacy and anonymity, location and direction of movement of the vehicle are known only to those legally authorized to have access to them and remain unknown to anybody unauthorized. Security-related key challenges for VANETs are control access, user authentication, message authentication, message integrity, message identification, message privacy, accountability anonymous certification, group signatures, PKI: managing certificate revocation, pseudonyms, etc. In case of designing any routing algorithm for VANET, the above-discussed issues should be taken into account.

In this paper, we have introduced a new reliable communication mechanism depending on a proposed system module for VANET. This proposed scheme consists of two different steps. (1) Registration procedure has been introduced for new vehicles, and trust value has been assigned to each of the registered vehicles. (2) Communication mechanism has been presented for existing vehicles.

The rest of the paper is organized as follows. Comprehensive surveys of related works of different secure routing protocols for VANETs are discussed in Sect. 2. In Sect. 3, we have presented new trust-based routing for VANET. Intensive performance analysis of our proposed scheme is presented in Sect. 4. We conclude our paper with final remarks in Sect. 5.

2 Related Works

For full deployment of VANETs, two paramount issues should be resolved, namely security and privacy. The information communicated by vehicles should be secured. Many researchers have been already published number of research papers, addressing the security issue of vehicular ad hoc networks. In this section, we have discussed some of the security-related research challenges of VANET.

In VANETs, the connection between two vehicles is often intermittent due to dynamic vehicular movement. Routing in VANETs has been studied, and many different protocols were proposed. Granelli et al. proposed a motion-based routing algorithm [1] for VANET. The routing metric enables to exploit not only positioning information but also the direction the vehicles movement. Extensive evaluation outlines the advantages of MORA [1], especially in case of high mobility of vehicles and frequent topology changes. But considering these parameters are not enough for a best next hop selection in VANETs. A vehicle that is almost out the communication range should not be selected as a next hop, which cannot be guaranteed without taking into account the speed. Menouar et al. [2] proposed MOPR, taking into account neighboring vehicles movement speed additional to MORA [1]. Vehicle that is estimated to go out the communication range in a short-duration time will not be selected as a next hop. This approach helps in minimizing the risk of broken links and in reducing data loss. The performance of the scheme largely depends on the prediction accuracy and the estimate of the transmission time that depends, in turn, on several factors such as network congestion status, driver's behavior, and the used transmission protocols. In Kumar and Rao [3] proposed a position-based greedy routing protocol, which uses the location, speed, and direction of motion of their neighbors to select the most appropriate next forwarding node. Like GPSR [4], it uses the two forwarding strategies greedy and perimeter. It predicts the position of nodes within the beacon interval whenever it needs to forward a data packet. DGRP [3] selects better next hop node than MOPR [2] as MOPR selects only those nodes for forwarding which are going to be communication range for next one second. In [3], if link stability between the forwarding node and its neighbor node is weak, possibility of packet loss is high in DGRP [3] and also prediction of position information is not reliable at all instances. Gong et al. [5] proposed a predictive directional greedy routing protocol, in which the weighted score is calculated from two strategies namely, position first forwarding and direction first forwarding. Using these strategies, the current neighbors and possible future neighbors of packet carrier are found. In PDGRP [5], next hop selection is done based on prediction and it is not reliable at all situations. In Jayasudha and Chandrasekhar [6] proposed a hierarchical cluster based greedy routing protocol. The main objective of the algorithm is to optimize the packet behavior in ad hoc networks with high mobility and to deliver messages with high reliability. We have also proposed a routing solution in [7]. In [8], J. Serna et al. proposed a geo-location-based trust for VANET's privacy and used as an authorization paradigm based on a mandatory access model and a novel scheme which propagates trust information based on a vehicle's geo-location. A trust-based privacy preserving model for VANETs has been presented by Ayman Tajeddine et al. [9], which is unique in its ability to protect privacy while maintaining accurate reputation-based trust. In [10], a reputation based trust model has been presented by Qing Ding et al. This is an event based reputation model to filter bogus warning messages. A dynamic role dependent reputation evaluation mechanism has been presented to determine whether an incoming traffic message is significant and trustworthy to the driver. BROADCOMM [11] is a popular broadcast algorithm for emergency situation in VANET. By exchanging Hello message to neighbor nodes, all nodes determine their own cell boundary. A cell reflector node is selected for each cell. These nodes actually relay the broadcasted message from one cell to other cell. Its' simple to implement nature is ideal in emergency alert system.

The above discussions lead to the conclusion that is mainly cryptographic, and certificate-based techniques [12] are being preferred by the researchers for securing communication within VANETs. This leads to another problem namely, certificate revocation problem [13].Some researchers have chosen trust value-based authentication, but the parameters influential in trust value assignment of a vehicle are not properly identified. A trust based solution in this issue is also proposed by us [14]. Maintaining pseudonym [15] is another approach for achieve security. But it also leads to an extra maintenance cost. This paper aims to provide a reliable communication mechanism for vehicular ad hoc network, and the proposed solution is used to overcome performance bottleneck and channel congestion problem.

3 Trust-Based Routing Protocol for Vehicular Ad Hoc Networks

In this section, we are going to propose a solution of above-discussed problem. In our proposed solution, we have distributed VANET in a layered architecture. In the lowest layer, all nodes (i.e., vehicles) present in the system. Local registration authority (LRA_i) implies a road-side unit that acts as a middle layer element within

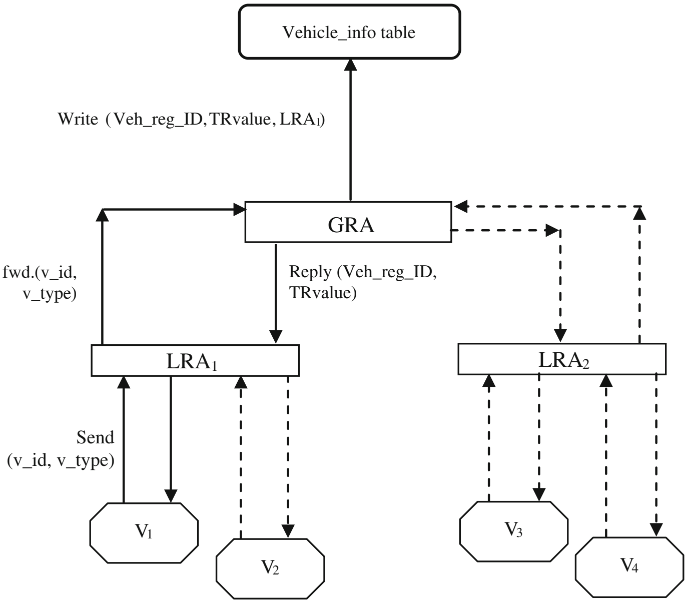

Fig. 1 Modular diagram of the system

the framework. LRA$_i$ is responsible for maintaining vehicles registered under it. The highest layer component, called global registration authority (GRA), is nothing but a repository having all lower layer information (Fig. 1).

3.1 Registration Procedure

Here, we have assumed that all nodes in a VANET are distributed according the proposed layered architecture. On entry of a new vehicle in the system, it sends a request for a registration certificate to its LRA$_i$, i.e., LRA$_i$ in its range and this request is termed as registered to communicate (RTC). LRA$_i$ estimates trust value of that vehicle forwards it and vehicle number to GRA. GRA generates a unique sequence number, i.e., USN for that particular vehicle. This USN acts as Veh_reg_id for the corresponding vehicle. At the registration time, LRA$_i$ do not know the behavior of the vehicle. For this reason at this time, an initial trust value is given to the vehicle.

- **Trust Value Initialization**

In this subsection, we have been presented an algorithm for new vehicle entering in the system. Every new vehicle has to register under its local LRA$_i$. For this reason, it sends a registration request to LRA$_i$. In this request, each vehicle has to send their types and the unique features of it. After receiving the request, LRA$_i$ assigns a unique number and a trust value to the requesting vehicle. After initialization of trust

Table 1 Vehicle_info table

Veh_reg_ID	LRA_i	TR_{value}

value, it will forward to GRA and GRA keeps all this information in Vehicle_info table and the corresponding vehicle is registered under the communicating LRA_i (Table 1).

Algorithm 1: Registration Procedure	
Step 1:	New vehicle sends (vehicle_id, v_type) to LRA_i
Step 2:	LRA_i call Trust_init_func(vehicle_id, v_type)
Step 3:	LRA_i forward that vehicle_id and TR_{value} to GRA
Step 4:	GRA generates a Veh_reg_ID
Step 5:	GRA write Veh_reg_ID, TR_{value} and LRA_i in Vehicle_info table.
Step 6:	New vehicle is registered under LRA_i
Step 7:	END.

Vehicles are all highly mobile in nature, and within a very short-time interval, it can move from one LRA_i region to another LRA_i region. Once registered, all information about the corresponding vehicle is maintained by parent LRA_i. Information of every registered vehicle's is also stored in GRA, and GRA actually acts as a global repository of all registered vehicles. LRA_i monitors all vehicles registered under it. When a vehicle moves out of its region, it broadcast a message consisting information about that vehicle. In this way, the new LRA_i in which region the vehicle enters can know information about it. The information sends by the following message format (Fig. 2).

In the above-message format, FM_i denotes an identifier that uniquely identifies the message. Veh_reg_id, TR_{value}, and Parent_LRA_i denote registration identifier, trust value, and initial LRA_i, respectively, for the corresponding vehicle. In this way, when LRA_i found any new vehicle in its region, it also had some essential information about that vehicle. If LRA_i needs more detail information, then it can query to GRA and gets required information from it.

At the execution of all the above-mentioned steps, two kinds of problem can be occurred as; performance bottleneck problem for LRA_i and channel congestion problem.

- **Performance Bottleneck Problem**

LRA_i is busy for registering new vehicles, estimating there trust value in a certain time interval, sending frequent message to other LRA_i, etc. All these jobs have done for a large number of vehicles depending locality. As a result large

FM_i	**Veh_reg_ID**	**TR_{value}**	**Parent_LRA**

Fig. 2 Message format

number of jobs may be waiting in a queue. For this reason, priority should be assigned to each job for job scheduling. In this way, high-priority job performed first and low-priority job have to wait. In this way, a starvation problem has been occurred for low-priority job. To solve this problem, aging technique can be introduced.

- **Channel Congestion Problem**

For performing assign jobs, LRA_i has to communicate with each other and with vehicles. Vehicles also communicate with each other for data transmission. All these communication take place using message passing through network channels. Due to this large number of data transmission, channel congestion can occur which cause to data loss. For avoiding this problem, channel availability should check at link layer. When a node wants to communicate, it sends a request to send (RTS) and waits until it received an ACK message. We can assume for this time this node become busy. On the other hand, when a node receives RTS, it also become busy until it sends ACK message. For other nodes, when RTS or clear-to-send (CTS) is received (but it is not send by themselves), they can assume that for that time period channel will be used. And, we assume this time period is a specified time period, as network transmission time (NTT). For calculation of this NTT, we can take one of the two following techniques.

- **No Persistent Technique**

In this technique, messages send after a certain time interval. This interval value can be estimated depending on some network property. By a thorough survey, we have assessed that this time interval depends on maximum transfer unit (MTU) of a network. A relation between channel capacity and NTT is also found. From our observation, we can write

$$\begin{aligned} & \mathrm{MTU} * \mathrm{CC} \propto 1/\mathrm{NTT} \\ & \mathrm{MTU} * \mathrm{CC} = \mathrm{K}\ /\mathrm{NTT}, \quad \text{where K is a constant} \\ & \mathrm{NTT} = \mathrm{K}/\mathrm{MTU} * \mathrm{CC} \end{aligned} \tag{1}$$

That means other nodes have to wait for this specified time period before starting the requesting process to access channel.

- **N-persistent Technique**

In this technique, messages send depending on a probability of n % success. The probability of failure is $(1 - n)$ %.

3.2 Communication Procedure

- Assumptions
- All LRA_i' maintain information about their child nodes and store in a list, defined child_list $\{$Veh_reg_ID, address, $TR_{value}\}$.

- LRA_i maintains information about vehicles in its one-hop distance.
- All vehicles registered under LRA_i, are in a one-hop distance of each other.

Communication taken place in this type of network can be categorized into two types.

- **Query Driven**

This type of communication is reactive in nature. A node broadcasts the query to procure necessary information. Then, it waits for T_{qb} time period, where

$$T_{qb} = \mathrm{pkt}_{size} * \ \mathrm{NTT} \ * 2 * T_{range} \tag{2}$$

The communication completes successfully if reply from any node is received within the time. If no such information is received, the LRA_i of sender vehicle multicast its query to all LRA_i and starts the timer for T_{qm} time period, where,

$$T_{qm} = \ \mathrm{pkt}_{size} * \ \mathrm{NTT} \ * 2 * \ \mathrm{LRA}_{dist} \tag{3}$$

After this specific time period, sender LRA_i checks for reply. If any reply found, then it forwards to the sender vehicle node. Otherwise communication declared as a failure.

Algorithm 2: Query-driven Communication	
Let V1 requires some information. So, it starts a communication session.	
Step 1:	V1 broadcasts a query and waits for time T_{qb} periods, where $T_{qb} = \ pkt_{size} * \ NTT \ * 2 * \ T_{range}$
Step 2:	If reply comes, then go to step 6
	Else go to next step.
Step 3:	V1 requests it's LRA_{v1} to forward it's query.
Step 4:	LRA_{v1} multicasts this query to other LRAs and waits for time T_{qm} periods, where $T_{qm} = \ pkt_{size} * \ NTT \ * 2 * \ LRA_{dist}$
Step 5:	If reply comes, then forward to V1
	else sends a failure message to V1
Step 6:	Communication successful.

- **Specific Vehicle-to-Vehicle Communication**

This type of communication takes place when any vehicle wants to communicate with any other specific vehicle. A prerequisite of this type of communication is a logical route establishment between sender and receiver vehicle. In the beginning of the communication, sender vehicle initiates a query about address of receiver vehicle. Sender vehicle search for receiver vehicle, in LRA_i child_list{Veh_reg_ID, TR_{value}}. If found then directly communicate with that specific vehicle. Otherwise, sender vehicle's parent LRA_i send message to all LRA_i. The receiver vehicle should be enlisted in the child list of any of the LRA_i.

Table 2 Data Dictionary

Parameter	Details
LRA	Local registration authority
GRA	Global registration authority
RTC	Registered to communicate
USN	Unique security number
Veh_reg_ID	Vehicle registration identifier
$\mathrm{TR}_{\mathrm{value}}$	Trust value
Vehicle_id	Vehicle identifier
V_type	Vehicle type
FM_{i}	Frequent message identifier
T_{o}	Time of a vehicle entering in system
T_{mr}	Total number of request send within time period
T_{mn}	Total number of reply received within time period
MTU	Maximum transfer unit

Unavailability of reply is suggestive of either the specific node has roamed to a different node or it is temporarily down. After receiving the reply, sender node can start communicating with receiver node (Table 2).

Algorithm 3: Routing Procedure	
Let S is the sender vehicle and D is the receiver one.	
Step 1:	Sender vehicle S searches in it's $\mathrm{LRA}_{\mathrm{i}}$ child list for destination vehicle.
Step 2:	If destination vehicle found then, go to step 5
	Otherwise send communication request to it's $\mathrm{LRA}_{\mathrm{i}}$
Step 3:	$\mathrm{LRA}_{\mathrm{i}}$ sends a request message to other $\mathrm{LRA}_{\mathrm{i}}$ for searching destination address.
Step 4:	If found, then send it back to source node, Otherwise send a failure message to sender vehicle.
Step 5:	Send a success message to sender vehicle.

4 Performance Analysis

In order to implement the above-discussed proposal, the system performance needs to be tested in real life, despite the many obstacles that make this difficult such as the expense, high mobility, network complexity, and distributed environments. Simulation tools are considered the best means with which to evaluate the performance of any network type particularly wireless and ad hoc networks. For example, this method enables the user to emulate the network in terms of routing protocols, security constraints, and other factors that are similar to real-life situations, thus avoiding the difficulties resulting from the existence of obstacles.

Table 3 Simulation environment parameters

Parameter	Value
Channel type	Wireless channel
Radio-propagation model	Two-ray ground
Antenna model	Omni antenna
Network interface type	Wireless Phy
Mac type	802.11
Number of nodes	25

We choose the NS2 simulator for this analysis because it realistically models arbitrary node mobility as well as physical radio-propagation effects such as signal strength, interference, capture effect, and wireless propagation delay. Our propagation model is based on the two-ray ground reflection model. The simulator also includes an accurate model of the IEEE 802.11 Distributed Coordination Function Wireless MAC protocol. Using NS2, we evaluate the performance of the proposed protocol and present the following metrics for comparing the performance with the different well-known traditional routing. The simulation model consists of a network model that has a number of wireless nodes, which represents the entire network to be simulated (Table 3).

We have to examine whether the proposed routing algorithm works robustly or not. For this reason, we have compared our routing algorithm with LAR, DSR, AODV, and GPSR according to the following metrics.

(i) Packet delivery ratio: Measures the ratio of data packets delivered to the destinations and the data packets generated by the CBR source.

Say, N is the number of packet generated by the CBR source. Among those D packets are received by destination node

$$\text{Packet delivery ratio, PDR} = \mathrm{D/N} \tag{4}$$

This number indicates the effectiveness of a protocol.

(ii) End-to-end delay: Measured in milliseconds, includes processing (pd), route discover latency (rl), queuing delays (qd), retransmission delay (rd) at the MAC, and propagation (pr) and transmission times (tr). This number measures the total delay time from a sender to a destination. So, we can compute

$$\text{End-to-end delay} = \mathrm{pd} + \mathrm{rl} + \mathrm{qd} + \mathrm{rd} + \mathrm{pr} + \mathrm{tr} \tag{5}$$

(iii) Normalized routing load (NRL): Measures the number of routing packets transmitted per distinct data packet delivered to a destination. Let DP is the number of data packet and for delivering these; we have required CP number of routing packet.

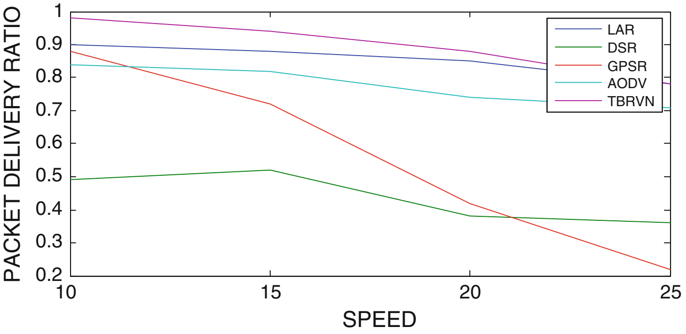

Fig. 3 Packet delivery ratio versus speed

$$\mathrm{NRL} = \mathrm{CP}/\mathrm{DP} \tag{6}$$

The routing overhead is an important metric for comparing these protocols as it measures the scalability of a protocol, and its efficiency in terms of throughput and power consumption. In our simulation study, we have performed sensitivity analysis to investigate the effect of various network parameters.

- **Effect of Speed**

This study is based on 100 nodes with 10 communication sessions. We have set our simulation with zero pause time to stress the mobility in the network. To understand the effect of speed on performance, we varied the speed of the vehicles between 10 m/s (or 22 miles/h) and 25 m/s (or 56 miles/h). The simulation results are presented in Figs. 3, 4 and 5. They show performance trade-off in some techniques.

Though AODV, LAR, and our proposed algorithm deliver almost similar number of packets irrespective of mobility, AODV and LAR have high end-to-end delay and control packet overhead. In a highly mobile scenario, links tend to break frequently. In such situation, these two algorithms need to send more route discovery message. LAR also suffers from inaccurate prediction of the request zone, which leads to network-flooding problem. DSR performs similar to our proposed protocol in terms of end-to-end delay and number of control packet transmitted per data packets. However, it gives poor result with respect to packet delivery ratio. This is because DSR has to rediscover routes more frequently as vehicle speed increases. In case of GPSR, high-control overhead is caused by maintaining neighbor location, and high end-to-end is caused by the outdated neighbor information. This causes GPSR to forward to non-existing neighboring nodes. From these results, we can conclude that connection-oriented approaches either drop a large amount of data packets (for example, DSR) or require a large number of control packet to keep routes up-to-date (for example, AODV and LAR) and

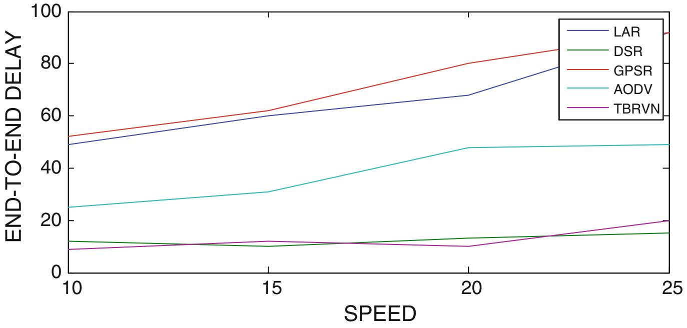

Fig. 4 End-to-end delay versus speed

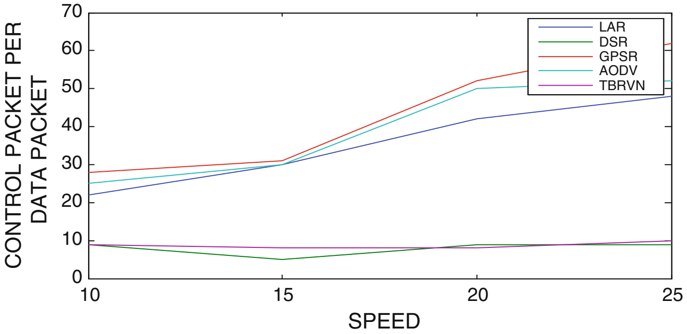

Fig. 5 Control packet per data packet versus speed

neighboring nodes information (for example, GPSR). In our proposed one, all vehicles' information is stored in vehicle_info table. This is maintained by a centralized authority, GRA. From this any vehicle's location is accessible. In addition, when a vehicle leave a region of an LRA_i (because of its' speed) and enters another LRA's region, then through frequent messaging 2nd LRA_i becomes aware about this particular vehicle. For this reason, despite of speed increase proposed protocol gives a consistence result.

- **Effect of Network Density**

In this case, we assumed node mobility is 25 m/s. For testing the effects of network density, we simulated with 50, 100, 150, 200, and 400 nodes. The results of analysis are plotted in Figs. 6, 7 and 8. In terms of packet delivery, AODV and LAR perform initially better than our proposed protocol. From our simulation result, it is clearly visible that with the increase of network density our protocol starts to perform better than AODV and LAR. If we compare on the basis of end-to-end delay obviously our proposed protocol perform best than others. Due to increment of number of nodes, number of control packets also increases for AODV

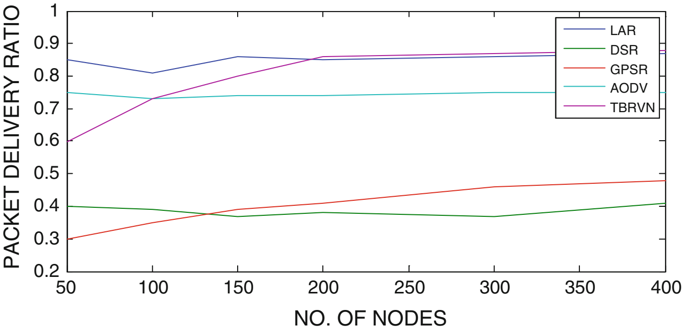

Fig. 6 Packet delivery ratio versus number of nodes

and LAR. DSR is not performed well. For GPSR, increasing number of nodes means more number nodes to maintain. So, route selection procedure becomes more time-consuming. This situation is reflected in the following figure. Though there is a centralized repository maintained by a centralized authority, the total responsibility of routing is actually distributed among LRA's. The LRA's are distributed locationwise. Thus, increases in the number of nodes are not going to reflect very much in case of proposed protocol.

From the above different comparisons we can see that the proposed routing protocol provides the better result than traditional well-known routing.

We have also examined our protocol's functionality with respect to BROADCOMM [11], a routing protocol specially aimed at vehicular communication. BROADCOMM [11] is chosen due to its' easy-to-implement features which have made it a popular choice for routing in VANET. The metrics for comparison between our proposed technique and BROADCOMM are as follows: packet delivery ratio, end-to-end delay, and routing load (Fig. 9).

It has been observed that performance of BROADCOMM [11] is better than the proposed technique. The reason is BROADCOMM does not involve any checks on the trust worthiness of the vehicles involved in communication. Our algorithm has

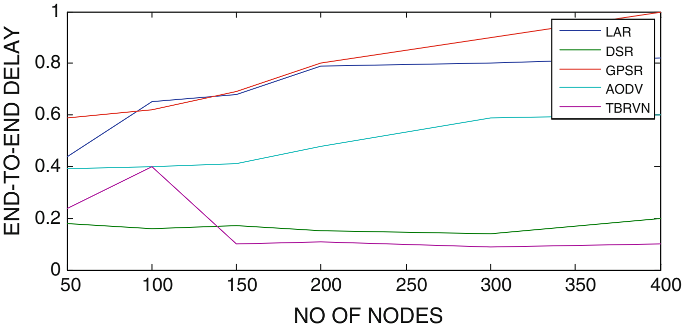

Fig. 7 End-to-End delay versus number of nodes

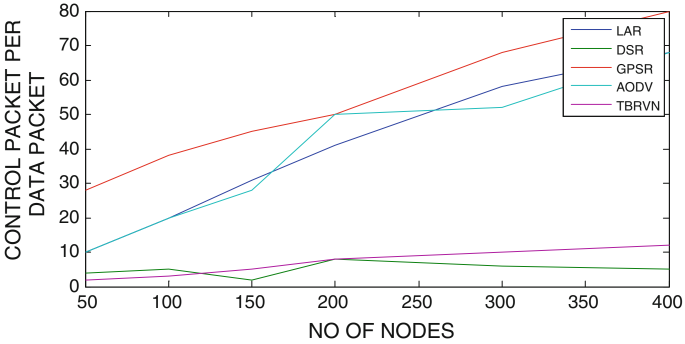

Fig. 8 Control packet per data packet versus number of nodes

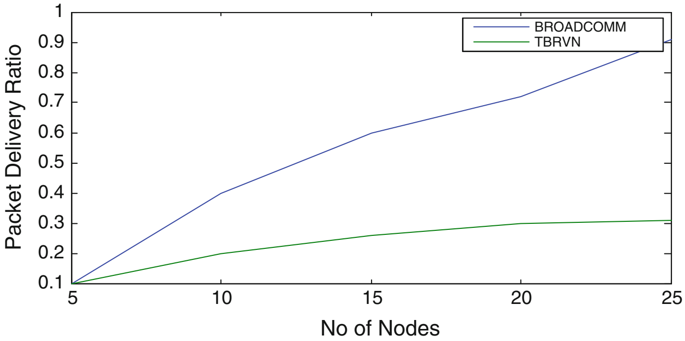

Fig. 9 Packet delivery ratio versus number of nodes

to perform certain mandatory checks and that adds to the delay in packet delivery ratio. Thus, in an ideal situation, BROADCOMM [11] proves to be a better performer (Fig. 10).

The performance of our proposed logic is much better than that of BROADCOMM [11] as far end-to-end delay is concerned. In BROADCOMM [11], communication takes place using pure flooding mechanism. This is the cause of additional delay in routing packets from source to destination. In TBRVN algorithm, use of selective forwarding technique helps to reduce the end-to-end delay (Fig. 11).

In case of BROADCOMM [11], flooding causes an exponential incrimination of control packets. In our proposed logic, selective forwarding mechanism is used for routing which limits the number of control packets to a linear order. This result is to reduce control packet for delivery of data packet.

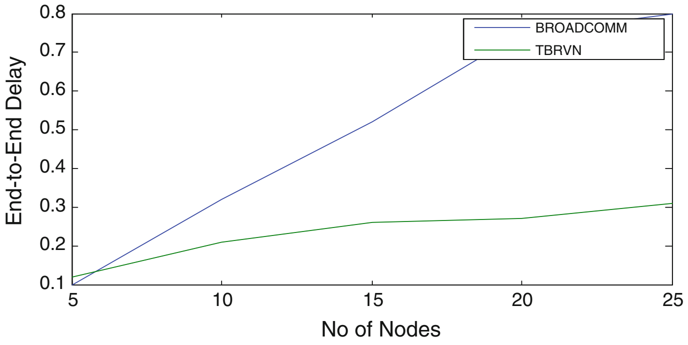

Fig. 10 End-to-end delay versus number of nodes

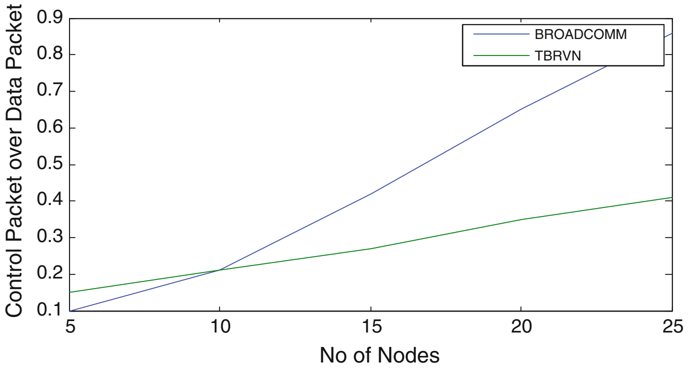

Fig. 11 Control packet per data packet versus number of nodes

5 Conclusions

In this paper, we have presented a reliable routing protocol for vehicular ad hoc network. Here, we have proposed a trust-based registration mechanism to provide the reliability. A layered structure has been presented for the authenticate vehicles communication. Performance bottleneck and channel congestion problem also have taken care consideration in this proposal. The results show that proposed routing protocol provides better result compared with the existing well-known routing protocol. We have also compared our proposed routing algorithm with BROADCOMM, a routing algorithm specially aimed at VANET environment. Results proved that TBRVN has less delay and routing overhead as compared with existing routing protocols.

References

1. Granelli, F., Boato, G., Kliazovich, D.: MORA: A movement-based routing algorithm for vehicle ad hoc networks. In: Proceedings of IEEE Workshop on Automotive Networking and Applications (AutoNet 2006), San Francisco, Dec 2006
2. Menouar, H., Lenardi, M., Filali, F.: Movement prediction based routing concept for position based routing in vehicular networks. In: Proceedings of the 66th IEEE Vehicular Technology Conference, 30 Sept–3 Oct 2007
3. Kumar, R., Rao, S.V.: Directional greedy routing protocol (DGRP) in mobile ad hoc network. In: Proceedings of International Conference on Information Technology, ICIT (2008)
4. Karp, B., Kung, H.T.: GPSR: greedy perimeter stateless routing for wireless networks. In: Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom) (2000)
5. Gong, J., Xu, C., Holle, J.: Predictive directional greedy routing in vehicular ad hoc networks. In: Proceedings of 27th International Conference on Distributed Computing Systems Workshops (ICDCSW '07) (2007)
6. Jayasudha, K., Chandrasekhar, C.: Hierarchical clustering based greedy routing in vehicular ad hoc networks. Eur. J. Sci. Res. **67**(4), 580–594. ISSN 1450-216X, Euro Journals Publishing, Inc. (2012)
7. DasGupta, S., Chaki, R.: SRPV: a speedy routing protocol for VANET. Published in the Proceedings of the International Conference on Advances in Computing, Communication and Control (ICAC3-2011), Communications in Computer and Information Science, vol. 125, Part 2, pp. 275–284, 28–29 Jan 2011
8. Saha, S.B., DasGupta, S., Chaki, R.: A Survey of prediction based routing protocols for vehicular ad hoc networks. In: Proceedings of the IEEE International Conference on Information Technology (ICIT-2009), Dec 2009
9. Gerlach, M., Festag, A., Leinmüller, T., Goldacker, G., Harsch, C.: Security architecture for vehicular communication. In: Proceedings of 4th International Workshop on Intelligent Transportation (WIT2007) (2007)
10. Lin, X., Sun, X., Ho, P.H., Shen, X.: A secure and privacy preserving protocol for vehicular communications. IEEE Trans. Veh. Technol. **56**(6), 3442–3456 (2007)
11. Durresi, M., Durresi, A., Barolli, L.: Emergency broadcast protocol for inter-vehicle communications. In: Proceedings of 11th IEEE International Conference on Parallel and Distributed Systems (ICPADS'05)
12. Papadimitratos, P., Buttyan, L., Hubaux, J.P., Karg, F., Kung, A., Raya, M.: Architecture for secure and private vehicular communications. In: Proceedings of 7th International Conference on ITS Telecommunications (ITST'07), pp. 1–6, June 2007
13. Raya, M., Jungels, D., Papadimitratos, P., Aad, I., Hubaux, J.P.: Certificate revocation invehicularNetworks. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.92.2291S. 2006
14. DasGupta, S., Chaki, R., Choudhury, S.: TruVAL: trusted vehicle authentication logic for VANET. Published in the Proceedings of the International Conference on 3rd International Conference on Advances in Computing, Communication and Control (ICAC3-2013) in Mumbai, 18th–19th Jan 2013
15. Wiedersheim, B., Ma, Z., Kargl, F., Papadimitratos, P.: Privacy in inter-vehicular networks: why simple pseudonym change is not enough. In: Proceedings of 7th International Conference on Wireless On-demand Network Systems and Services (WONS), pp. 176–83 (2010)