International Journal of Advanced Science and Technology
Vol.109 (2017), pp.1-12
http://dx.doi.org/10.14257/ijast.2017.109.01

Secure Node Communication With Cryptographic Algorithm in Vehicular Ad Hoc Networks

Pallavi Agarwal

Gwalior, India
pallaviagarwal015@gmail.com

Abstract

Vehicular Ad hoc Network (VANET) is the furthermost remarkable and an advantageous technique for the research field for improving the security and protection of drivers and passengers. It is an interesting subclass of Mobile Ad-hoc Network, which authorizes smart communication between vehicles furthermore in the middle of the vehicle and roadside frameworks. It is an application of a wireless network for switching the data – to the domain of vehicles. For the creation of trustful surroundings, trust can be practiced to increase the safety in vehicular networks, which is a major section of security. Trust can be considered by directly observing the human actions or indirectly by getting the neighbor's opinion which produces a trusted communicating environment. They turn into a principal component of intelligent transportation systems. There is a transitivity model in the existing work in which the Authentication Server (AS) provides the authority to Law Executor (LE) for authenticating the other vehicles as a trustful vehicle. So in proposed work a new technique in which there is no vehicle in the network to provide the authority. Trust is estimated by the nodes, then this value sends to the AS where this value is calculated and updated regularly. This method enhances the security of the network. NS2 simulator is used for the overall operation of the proposed work and throughput, PDR and routing overhead show the efficiency of the network.

Keywords: *VANET, OBU, RSU, LE, AS, Security, and Hashing Algorithm*

1. Introduction

VANET is likewise perceived as a vehicular sensor network by which safety of driving is improved through between vehicle interchanges or correspondences with roadside framework [1]. In VANETs, vehicles are furnished with remote onboard units (OBUs), which interchange message with each other or with roadside units (RSUs) with a Dedicated Short Range Correspondence (DSRC) protocol [2]. As indicated by the DSRC protocol, which applies the IEEE 802.11p standard for wireless communication, every vehicle in a VANET communicates by broadcasting traffic safety message each 100-300 ms, which keeps the vehicle's driving-related data, for example, area, speed, turning goal, and driving status (*e.g.*, normal driving, sitting waiting for traffic light, congested driving conditions, and so on.), to different vehicles. With the incoming data, different drivers can make an early reaction on account of remarkable circumstances, for example, accidents, emergency braking, and congested roads. Despite the various points of interest of launching a VANET, security concerns must be very much tended to before we set these application situations in preparation. Premier of all, message respectability must be guaranteed. Besides, message senders ought to be validated so as to protect attacks of impersonation [3]. We see a twist phase of VANETs where Road Side Units (RSUs) are broadly installed, and every vehicle is fitted with an OBU. Specifically, trust authority

Received (August 30, 2017), Review Result (November 13, 2017), Accepted (November 14, 2017)

ISSN: 2005-4238 IJAST
Copyright ⓒ 2017 SERSC Australia

(TA), a server, few static RSUs and vehicles traveling on the roads installed with OBUs, as indicated in Figure 1.

A. TA:

Trust authority plays a significant role in the whole system, which takes charge of registration of the server, all RSUs, and vehicles.

B. Server:

In general, the server delivers a high storing and computational capability which stores the feedback data table, trust table and reputation table for the whole organization. Employing the information in those tables, the server also calculates the trust scores for other vehicles and reputation scores for vehicles. Specifically, every time when a potential user's vehicle requests to link up a platoon, the server will respond this request by recommending the most trusted vehicle.

C. RSUs:

RSUs are associated with wired lines and protected channels to the server and TA, in the meantime, they deliver wireless connections to the vehicles. Both the feedbacks of used vehicles and trip details updates of vehicles will be forwarded through RSUs to TA or host. From this point of view, RSUs can be regarded as relays of data between vehicles and TA or between vehicles and server. In our system model, we assume that RSUs are widely deployed on the roads to compensate the whole area which assures that the vehicles are able to update the information timely when driving along the roads. In few regions where RSUs are thinly organized, the update of the feedbacks and traveling data of vehicles are postponed. Only, in the long run, the system is still proficient [4].

D. Vehicles:

The vehicles can be considered as a group of extremely mobile nodes equipped with OBUs which permit them to communicate with other vehicles or RSUs. Through V-2-I communication, a vehicle updates its own traveling information or uploads feedback scores to the server when passing RSUs. The drivers of the vehicles can demand either to drive individually or to bring together a platoon.

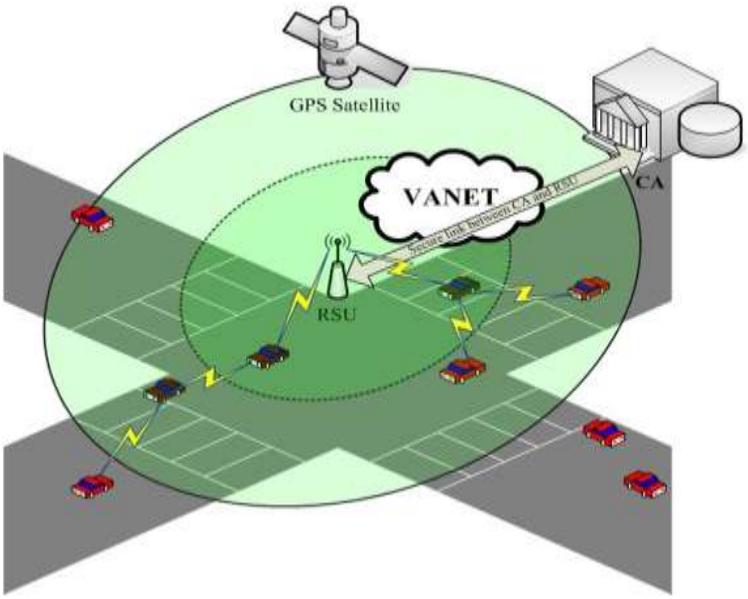

Figure 1. VANET Framework

 Copyright ⓒ 2017 SERSC Australia

2. Related Work

Hu *et al.*, [2016] in this paper, they proposed a consistent trust-based platoon service recommendation scheme, named REPLACE, to support the user vehicles to avoid selecting badly-behaved platoon head vehicles. In particular, at the center of REPLACE, a reputation system is intended for the platoon head vehicles by gathering and displaying their user vehicle's feedbacks. And so an iterative filtering algorithm is designed to share with the untruthful feedbacks from other vehicles. A detailed security analysis is given to demonstrate that our proposed REPLACE scheme is safe and robust against badmouthing, ballot-stuffing, newcomer and on-off attacks existing in VANETs. In summation, we conduct extensive experiments to illustrate the correctness, accuracy, and validity of our proposed method [4].

Wenjia Li *et al.*, [2016] proposed ART which is an attack-resistant trust administration method called ART is proposed to survey the dependability of the two information activity and vehicle hubs for VANETs. In this framework, the creator had assessed the reliability of the information and hubs into two separate grids Data Trust and Node Trust individually. The trustworthiness of nodes further consists of functional trust and recommendation trust. The data trust is used to appraise whether or not and to what extent the reported traffic data are trustworthy. On the other hand, node trust indicates how trustworthy the nodes in VANETs are. The proposed scheme uses the Cosine-based similarity metric which is utilized to evaluate how similar the two vectors are. It has been proven that this ART scheme does not incur extra communication overhead & can still hold out the zigzag attack and achieve high precision and recall even when there are 40% of malicious nodes [5].

Hind Al Falasi *et al.*, [2015] uses the similarity to assign trust ratings to the vehicles in the network & then use these trust ratings to recognize the abnormal vehicles. Throughout the journey, the vehicle listens for beacons sent from its one-hop neighbor. The received data is processed and stored in the receiving vehicle for handling later. According to this system, at a given time, a vehicle in the VANET listens to only those vehicles that preserve the similar speed by itself. The resulting similarity rating is forwarded to the Decision Maker Module for calculating the Trust rating of the neighborhood vehicles. The higher the trust rate of the vehicle, more reliable is the data from that vehicle. The author has designed the system to use data mining techniques to find the highly valuable information in a highly dynamic network. Merely, this scheme does not regard any other attribute than Speed in the neighborhood to estimate the similarity rating in the VANET [6].

Alexandra Rivero-Garcia *et. al.*, [2016] presented a real of event alerts. This scheme is based on several components like the confirmation votes of the users, their profiles &their Trust levels. The proposed scheme is founded on the assumption that system will melt on the mobile device of the drivers. And the smartphones are the connections between the user and the community through clouds, using audio notification. The basic focus of this proposal to install VANET to smartphones. The user can accomplish three actions: Generate, Verify or Deny an event. The author had introduced a collaborative warning system of road events based on user trust. The main complication in this arrangement is that they don't have feedback from and between users, as user tests to measure satisfaction, user rates between them or even comments or relationship ties. The only thing system considers is the user behavior in other events [7].

Wu *et al.*, [2011] proposed that an RSU Aided Scheme for Trust Establishment is offered which lays emphasis on data rather than on the reputation of the providing entities. This scheme has the power to integrate observed data with feedback information, when judging the trustworthiness of data, and eventually improves the accuracy of the evaluation result [8].

Copyright ⓒ 2017 SERSC Australia

Kothari *et al.*, [2016] the proposed solution based on Information oriented trust [7]. As according to our method we should concentrate more on evaluating the trustworthiness in data, because if a node receives a serious information regarding an accident on the road, and so it is more important to calculate trust on that data rather than centering on which guest has sent this info. The primary advantage of our approach is that it prevents attacks which are managed by the trusty nodes, which act maliciously for their own personal motives. Agreeing to methodology every node also takes into attention similarity parameter in terms of speed which plays a significant part in evaluating trust value [9].

Sharma *et al.*, [2015] in this work, the utilization of Dempster-Shafer Theory (DST) for processing trust in the VANET condition for area assurance is exhibited. Trust-based location finding in VANET is essential to deter the spread of selfish or malicious messages and also enable other vehicles to filter out such messages. The outcome indicates that the proposed scheme is operable in the VANET environment [10].

3. Trust

Security and trust are very important factors in the vehicular network and basic user requirements [11]. The user, vehicle, and RSU are some of the components of the vehicular network. Trust is the key component of the security framework. At the point when users get any message from another vehicle or from the framework, it ought to be trusted because user responds as indicated by the message. To build the trust, it is required to provide trust between the users in the communication vehicle to vehicle (V2V) and vehicle to infrastructure (V2I). The attackers change the contents of the message and break the trust between the vehicles. Figure 3 shows the trust components of the vehicular network. Trusted Users (TUs) are those who perform their task properly in the network. The behavior of a trusted user may change upon receiving messages from other vehicles or from the RSU. When a trusted user receives an accident warning or traffic jam message, the user is required to modify his/her conduct, that is, slow down his/her vehicle or route change. Figure 4 describes the state of affairs in which vehicle C sends a warning message to other vehicles (D, E). As a solution, the users of vehicles D and E slow down their speeds and may call for an alternative route due to the accident warning message [12]. VANET is a decentralized, open system, *i.e.*, there is no centralized infrastructure and peers may get together and give the net any time respectively. If a peer is interacting with a vehicle right away, it is not guaranteed to interact with the same vehicle in the hereafter. And in such an environment, there is much uncertainty in determining whom to believe. Trust refers to the confidence of an entity of VANET on another entity. It is established on the desire that the other substance will play out a specific activity accepted/expected/accepted by the originator. Trust depends on the way that the trusted substance won't act maliciously in a specific circumstance [13]. As nobody can be certain beyond a doubt of this reality, trust is totally reliant on the conviction of the trustor. An element is a physical gadget that participates in the correspondence procedure, *e.g.*, OBUs and RSUs utilized as a part of VANET. Trust denotes to how much a hub ought to be dependable, secure or reliable for any connection with different hubs. A hub can take part in the procedure of communication in VANET just if this hub is treatable for different hubs and fulfills the trustful necessity. A hub can have distinctive trust esteems when assessed by various hubs since the fact that the necessity of trust calculation might be diverse for singular hubs. Trust is dependent on time as it can develop and decline over some undefined time frame

Assume T(A, B) is a relationship of trust between hub A and B. On the off chance that one hub trusts another hub to play out the normal operation, the trust connection between these hubs can be set up dependably from initiator's perspective. On the off chance that hub A needs some activity performed by hub B and if B is effectively playing out this activity, B is a trusted for hub A. Hub A will build the value of trust of B for its great

 Copyright ⓒ 2017 SERSC Australia

nature. So, the trust esteem continues expanding for every action performed by a hub that was normal by the initiator. Trust foundation and administration are basic parts of a security system of VANET. Building trust in ad hoc networks is an interesting task. It depends on setting up trust relationships involved with neighboring hubs. These trust connections start, create and terminate much of the time. The procedure of trust foundation is basically difficult because of the non-existence of static framework, brief span of connections, shared remote medium and physical weakness. For beating these issues, trust is built up in especially ad hoc networks using few expectations like pre-configuration of nodes with secret keys and existence of centralized authority.

The number of hub's movement is denoted as hub's trust confirmation and it builds/diminishes once it collaborates effectively with the correspondence initiator or not. Trust relations depend on the proof made by the past cooperations of the substances inside the application. At first, the reliability of the considerable number of hubs in the system is set to some default esteem. This esteem is changed at whatever point a hub gets some data with respect to its dependability as far as both immediate and secondary perceptions. At whatever point a hub watches any kind of bad conduct from neighboring hub, it decreases its trust an incentive as indicated by the discipline factor. This discipline factor is diverse for various mischievous activities. Misbehavior incorporates dropping, alteration and misrouting of data at the system layer and sending false RTS/CTS in the MAC layer, and so on. The vast majority of the security plans rely upon predefined edge or preparing information to develop the malicious performance of the attackers. In any case, it is extremely hard to set edges and gather preparing informational indexes of attacks in ad hoc networks [14].

4. Proposed Work

In our proposed work, firstly we did not provide any authority to LE for authenticating other MTVs. So if LE behaves maliciously then the security cannot be affected. When vehicles come in a range of RSU then it directly communicates with RSU and RSU communicate to AS. For sending some data from source to destination, every vehicle has to send HELLO packet to all its neighbors. By this, vehicles can interact with its neighboring vehicles, then calculate the trust. When the neighboring vehicles forward or aren't dropping the HELLO packet, then it is considered as a trustful vehicle otherwise MTV. We calculate the trust of each vehicle on the basis of their behavior. If the vehicle is trustful then its trust value increases or vice-versa. Each vehicle calculates trust of its neighbor and sends this value to RSU. Then RSU updates these values with the help of AS and then broadcast this value. Now all the vehicles have a trust value of vehicles so that send data by using hashing technique. All vehicles forward data by using the trusted path to send the data source to a destination so that security enhances.

Here we used SHA-1 (Secure Hash Algorithm) because it has very fast computation process and also very secure to transmit the data. When sender X sends the data, then they used its private key and receiver Y verifies it by using the sender's public key. It produces a hash value of 160 bits and 80 rounds, which is enough for securing the data in VANET. It converts the message into the block of 512 bits. Where || is a concatenation of two strings M and N. K is a key which is used to convert the messages and nonce value.

Copyright ⓒ 2017 SERSC Australia

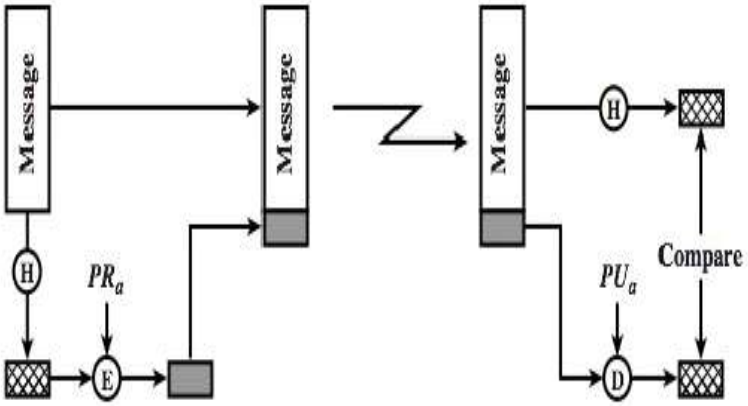

Figure 1. Hash Value by using Public Key Encryption

An example is SHA 1: $\{0,1\}^{128} \times \{0,1\}<2^{64} \rightarrow \{0,1\}^{160}$

This hash function takes a 128-bit key and an input M of at most 2^{64} bits and returns a 160-bit output. SHA1 was proposed by Ron Rivest in 1990 which is derived from a function called MD4 that and the key ideas behind SHA1 are already in MD4. Besides SHA1, MD5 is another well-known form of MD4, which was similarly proposed by Rivest. The MD4, MD5, and SHA1 algorithms are all quite similar in structure. The first two produce a 128-bit output that goes from 512+128 bits to 128 bits, while SHA1 produces a 160-bit output that goes from 512 + 160 bits to 160 bits.

Proposed Algorithm:

Step 1: Start
Step 2: Broadcast request packet
Step 3: Forward packet towards the destination
Step 4: Get the response from the destination
Step 5: Now calculate trust value of each node
Step 6: If(drop>threshold)
Increase trust value
Else
Decrease trust value
Step 7: Evaluate the trust value and send to RSU
Step 8: Now RSU sends this to AS
Step 9: Update trust value
Step 10: Nodes perform login process every time when coming in a range of RSU
Step 11: Apply hashing algorithm to secure the data
Step 12: Send data with hashed data towards the destination
Step 13: Exit

 Copyright ⓒ 2017 SERSC Australia

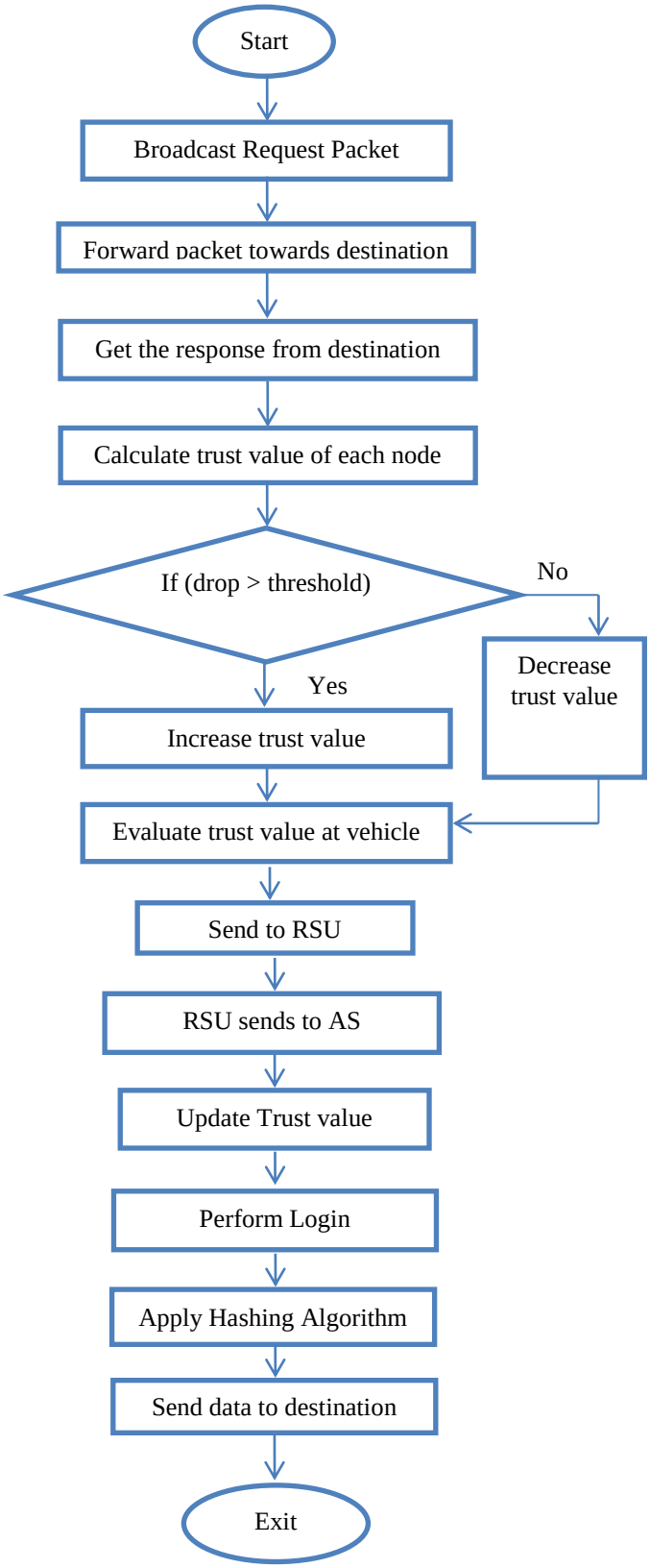

Figure 2. Flow Chart of Proposed Algorithm

Copyright ⓒ 2017 SERSC Australia

5. Result Analysis

The simulation is done in NS2 [22] which show the topology of 800m x 1000m. Various parameters are described in Table 1. The performance of network analyses of PDR, throughput and routing overhead over the network.

Table 1. Simulation Parameters and their Values

Parameters	Values
Network Size	800m x 1000m
Number of Vehicles	50
Packet Size	512 Bytes
Simulation Time	100s
MAC Protocols Used	Medium Access Control/802_11
Routing Protocol Used	AODV
Traffic Type	Constant Bit Rate (CBR)

A. Packet Delivery Ratio (PDR)

The total number of packets received by the destination node as compared to the total number of packets transmitted by the source node which is defined as the packet delivery ratio. The Figure 3 represents a PDR graph between base approach and the proposed approach. The packet delivery ratio of the proposed approach generates the better result than the existing approach.

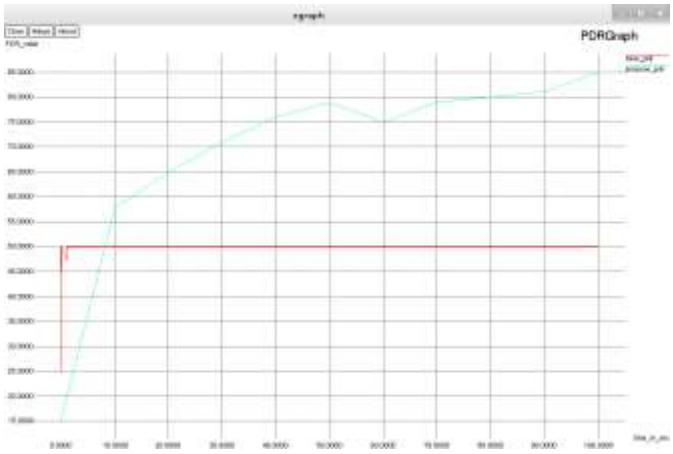

Figure 3. PDR Graph

Table 2. Packet Delivery Ratio

Time (in ms)	Base paper	Propose paper
10	49.9931	57.727
20	49.9967	64.8016
30	49.9979	70.9358
40	49.9984	75.9495
50	49.9987	78.9522
60	49.9989	74.969
70	49.9991	78.989
80	49.9992	79.9893
90	49.9993	80.9896
100	49.9994	85

 Copyright ⓒ 2017 SERSC Australia

B. Throughput graph

The total number of the data packet received during the particular time period which is known as throughput. The Figure 4 signifies a throughput graph between the base approach and the proposed approach. The throughput of the proposed approach generates the better result than the existing approach.

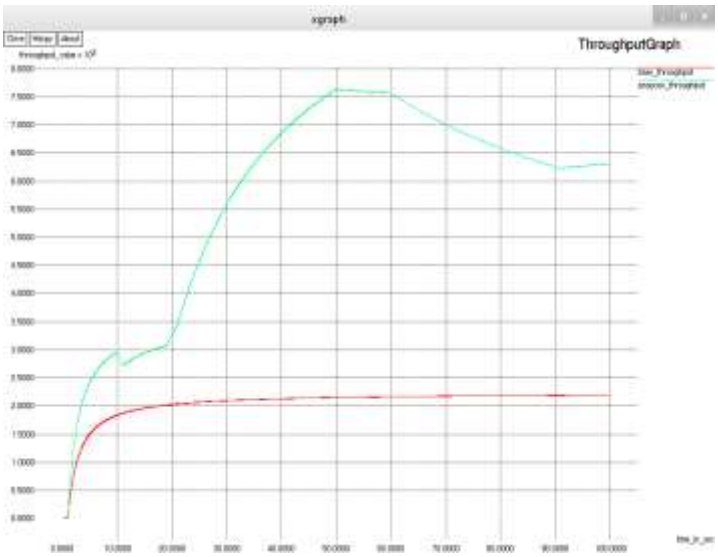

Figure 4. Throughput Graph

Table 3. Throughput

Time (in ms)	Base paper	Propose paper
10	1835.36	2969.34
20	2027.68	3276.05
30	2096.08	5588.66
40	2131.15	6858.48
50	2152.48	7630.72
60	2166.82	7560.16
70	2177.12	7002.7
80	2184.88	6582.82
90	2190.93	6255.18
100	2197.4	6284.31

C. Routing overhead

The routing overhead is defined as flooding of data in the network transmitted by an application, which utilizes a bit of accessible transfer rate of communication protocols. The Figure 5 signifies a routing overhead graph between base approach and the proposed approach. The overhead of the proposed approach is less than the base approach. Since the overhead should be minimized and the routing decreases in the proposed work the overhead also decreases.

Copyright ⓒ 2017 SERSC Australia

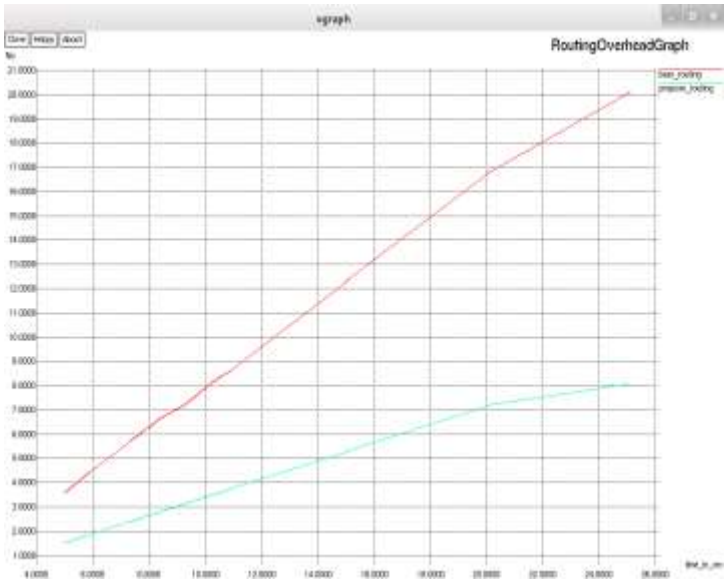

Figure 5. Routing Overhead Graph

Table 4. Routing Overhead

Time (in ms)	Base paper	Propose paper
5	3.579	1.513
10	7.92	3.403
15	12.252	5.263
20	16.715	7.153
25	20.014	8.072

6. Conclusion

The safety application in vehicular ad hoc network provides active road safety to avoid road accidents by disseminating life serious details among drivers securely. Such information must be protected from the access of an intruder or attacker. In trusting vehicular networks, trust and security are 2 main user's necessities. The broadcasting nature of the wireless channels, the nonappearance of a static infrastructure, the active network topology, and the self-organizing characteristic of the network rise the susceptibilities of a VANET. Trust formation is a serious problem in VANET. In centralized trust formation method, the key disadvantage is impersonation attacks, where one node can steal and use the individuality of additional nodes. In totally distributed trust formation approach, the chief difficulty is that a node might obtain numerous identities from different issuers.

References

[1] S. Zeadally, R. Hunt, Y. Chen, A. Irwin and A. Hassan, "Vehicular Ad Hoc Networks (VANET): Status, Results, and Challenges", Telecommunication Systems, vol. 50, no. 4, **(2012)**, pp. 217-241.
[2] H. Oh, C. Yae, D. Ahn and H. Cho, "5.8 GHz DSRC packet communication system for ITS services", Proceedings of the 50th IEEE Vehicular Technology Conference (VTC,'99), **(1999)**, pp. 2223-2227.
[3] J. Cui, J. Zhang, H. Zhong and Y. Xu, "SPACF: A Secure Privacy-preserving Authentication Scheme for VANET with Cuckoo Filter", Journal of Latex Class Files, vol. 14, no. 8, **(2015)** August.
[4] H. Hu, R. Lu, Z. Zhang and J. Shao, "REPLACE: A Reliable Trust-based Platoon Service Recommendation Scheme in VANET", DOI 10.1109/TVT.2016.2565001, IEEE Transactions on Vehicular Technology.

 Copyright ⓒ 2017 SERSC Australia

[5] W. Li and H. Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks", IEEE Trans. Intell. Transport. Syst., doi: 10. 1109/tits.2015.2494017, vol. 17, no. 4, **(2016)**, pp. 960-969.
[6] M. M. Masud Hind Al Falasi and N. Mohamed, "Trusting the Same- Using Similarity to Establish Trust Among Vehicles", In: International Conference on Collaboration Technologies and Systems, **(2015)**, pp. 64-69.
[7] A. Rivero-Garcia, "VANET Event Verification Based on User Trust", In: 2016 24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP), **(2016)**.
[8] A. Wu, J. Ma and S. Zhang, "Rate: A RSU-aided scheme for data-centric trust establishment in VANETs", Wireless Communications, Networking and Mobile Computing (WiCOM), IEEE, pp. 1-6, **(2011)**.
[9] A. Kothari, Dr. P. Shukla and Dr. R. Pandey, "Trust Centric Approach Based on Similarity in VANET", International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016.
[10] K. Sharma and B. Kumar Chaurasia, "Trust-Based Location Finding Mechanism in VANET using DST", 2015 Fifth International Conference on Communication Systems and Network Technologies.
[11] I. A. Sumra, H. Hasbullah and Jamalul-lail, "Trust and trusted computing in VANET", Comput. Sci., 1 **(2011)**.
[12] R. Gilles Engoulou, M. Bella¨iche, S. Pierre and A. Quintero, "VANET security surveys", Computer Communications, vol. 44, **(2014)** May 15, pp. 1-13.
[13] Y. Ren and A. Boukerche, "Modeling and managing the trust for wireless and mobile ad hoc networks", In IEEE International Conference on Communications, ICC '08, **(2008)** May, pp. 2129-2133.
[14] L. Eschenauer, V. D. Gligor and J. Baras, "On trust establishment in mobile ad-hoc networks", In Security Protocols, Darlinghurst, Australia, Australia, Springer Berlin / Heidelberg, **(2004)**, pp. 47-66.

Copyright ⓒ 2017 SERSC Australia

Copyright ⓒ 2017 SERSC Australia