Wireless Pers Commun (2016) 88:357–370
DOI 10.1007/s11277-015-3124-5

Towards Modelling a Trusted and Secured Centralised Reputation System for VANET's

T. Thenmozhi[1] · **R. M. Somasundaram**[2]

Published online: 9 November 2015

Abstract Vehicular Networks facilitate communication among vehicles to notify and exchange road-related information and thereby ensure road safety. In VANETs', the network infrastructure provides a facility to generate the messages. But all these messages need not be reliable. Therefore, in order to build reliability on the message, the vehicle in which the message was generated can be evaluated based on a reputation score that it has earned during its prior transmissions. This paper aims to design and analyse a Reputation System for VANET's which aids the receiving vehicle to decide the reliability on the message based on the score that has been earned by the transmitting vehicle.

Keywords VANET's · Security · Message reliability · Centralised architecture · Reputation systems

1 Introduction

The development of technological innovations has led to the communication enabled between vehicles with the aid of V2V communication and V2I communication. The VANET is characterised by the mobile and self-organising nodes. VANET's provide timely updates on safety related information, Entertainment updates etc., which are broadcasted across the network. The neighbouring vehicles are dependent on the message transmitted by the nodes. Therefore a valid secured infrastructure is required to authenticate the messages sent in the network [1].

Without security the network is open for attacks like suppression of messages, faulty message propagation etc. Messages related to the safety of vehicles are safety-related

✉ T. Thenmozhi
thenmozhi74@yahoo.co.in

[1] Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India

[2] SNS College of Engineering and Technology, Coimbatore, India

messages and an announcement scheme is followed by the vehicle for generating and broadcasting these messages. Therefore, proper authentication of messages is required in the infrastructure to build belief about the sending node. Various cryptographic techniques are used for proving the authentication of the messages. Even then, only if the vehicles are reliable, the messages benefit the receiving nodes. If the sending vehicle is reliable, then so is the message too. The consequences of an unreliable message is very high. These unreliable messages may be generated by a faulty sensor in the vehicle or may even be generated intentionally too. Therefore, any message generated by the vehicle should be evaluated for its reliability [2].

In general, all the participating vehicles do not have a major trust on the vehicles from which it receives the message. Therefore, when a message is received, the level to which the message can be depended upon is a serious issue and it becomes mandatory for a Reputation System so that the communication becomes very much trustworthy.

A Reputation system aids in building a trust value for every vehicle in the network. These values help the other vehicle to determine which vehicles can be relied on Resnicke Zeckhauser [3] defines the operational objective of a Reputation systems as (a) To provide information that helps in distinguishing a reliable and unreliable vehicle (b) To encourage vehicles' to behave in a trustworthy way (c) To discourage suspected vehicles from not participating in this system.

Initially, the reputation of any vehicle is void. When the vehicle starts transmitting warnings and when other vehicles finds it valid, the reputation value increases if other vehicles finds it valid. Reputation of a vehicle is the measure of belief which other vehicles have about the sender based on the reliability of earlier sent messages [4]. Usually, the belief is represented as a numerical value. With time, the participating vehicles rate the vehicle with a score. As the vehicle becomes reliable among the neighbours, it scores a positive feedback and a positive value, else and the score earned decreases.

2 Related Work

The reliability of the transmitted messages is based on the validity of the messages that have been transmitted by the vehicle. Various schemes have been proposed to implement security, reliability, authentication of messages in VANETs. Digital signatures [5] provide integrity and authentication of the transmitted messages. The Threshold method [6] verifies if same message is received from a "n" no of vehicles, but consumes a long time to check for the message validity. Network modelling [7] allows detection and correction of malicious nodes in the vehicle. But possessing the knowledge of all participating vehicles is highly infeasible and unpractical and imposes storage constraints. Decentralised infrastructure reputation based models have been proposed, but does not guarantee Robustness. In [8], Opinion piggybacking, the Vehicle appends its opinion to the already received opinions, but does not explore on the Computational burden on the vehicles like Initialisation and updating of scores. In [9], Vehicle behaviour analysis is proposed, but has a limitation that the neighboring vehicles arein a position to react immediately. A simple, practical model of a Reputation system based announcement scheme has been proposed in [10] which analyses a secure and efficient announcement scheme. A method to improve the reception rates of the messages has been proposed in [11], which uses an adaptive broadcast protocol. In order to increase the level of reliability for safety applicatons in Vanet's, a sublayer has been suggested in [12].

3 Proposed System

In order to scale the Reputation System to a very large area, thereby benefitting many vehicles, we propose to design and analyse a Reputation system for Vanet's. The proposed system analyses the drawbacks of the earlier approaches as below:

1. The existing Centralised infrastructure can be utilised to a greater extent in designing and establishing a reputation system.
2. The Reputation system evaluates and disseminates the reliability score of the vehicle which assists the other vehicles in the network.
3. Broadcasted messages are transmitted to the vehicles are received by the vehicles in a small area. A large number of vehicles can benefit if the technique can be extended to a greater area. A Centralised Reputation Server which collectively groups the scores from certain number of Regional Reputation Servers, extends the service to a larger area.
4. Reputation scores help the vehicle to decide on either accepting the message or not. The score earned by the vehicle indicates the level to which the vehicle had involved in reliable transmission.

4 Network Modelling and Simulation

4.1 System Components

In order to develop a Centralised Reputation System, a three Tier architecture is proposed as shown in the Fig. 1, comprising of the following components:

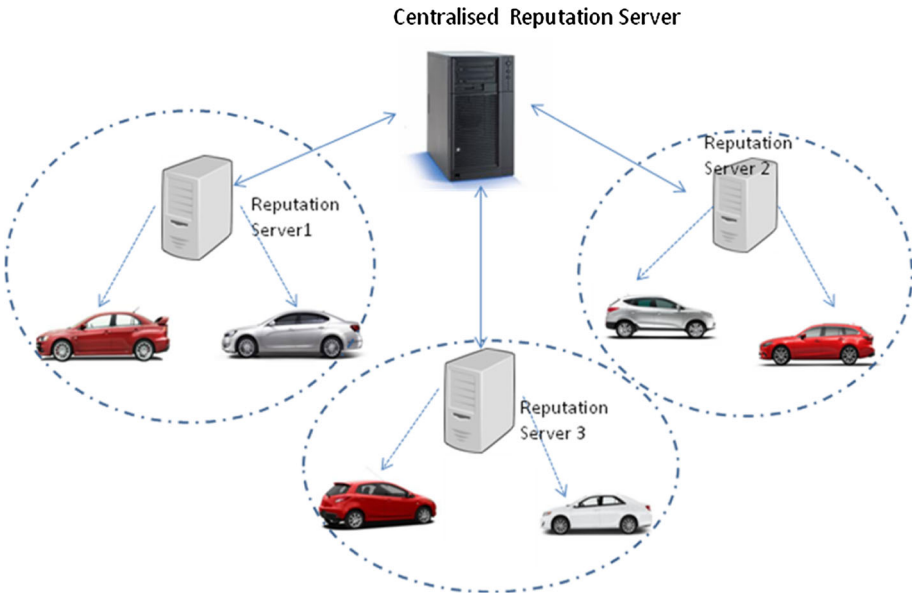

Fig. 1 3-Tier architure

a. *Centralised Reputation Server (CRS)*: The Centralised Reputation Server is the topmost entity in the hierarchy. The CRS covers a large area and controls a certain number of RSU's. In this model, CRS is the trusted authority. The CRS aggregates the scores received from various Regional Reputation Servers and calculates the score for a period of time. These scores can further be sent to the reputation servers on a query.
b. *Regional Reputation Server (RRS)*: Admission and revocation of the vehicles are monitored by the Regional Reputation Server. The RRS plays the role of receiving the scores from other neighbours, aggregating them and sends them to the CRS.
c. *Access Points (AP)*: Wireless communication devices facilitate connection between the Reputation Server and the vehicles. These access points can be installed in frequently visited points. The number of access points is decided on the area to be covered.
d. *Vehicle (V)*: Vehicles broadcast and receive messages from their neighbours. On experiencing the road related messages, the vehicles compose a feedback and sends to its Regional Reputation Server.

4.2 System Settings and Simulation

The basic assumptions for the design, the components of the Network, the algorithmic components and the operation of the system are discussed in detail. The Network model is simulated in Ns-2 with the following assumptions.

(i) Assumptions:

a. Vehicles move at random speeds on the roads.
b. Traffic jam and other road conditions are simulated to occur randomly, lasting for few seconds.
c. Vehicles are comparatively closer to the occurring event.
d. Any message received is evaluated for reliability based on a reputation threshold parameter and a time discount function.
e. When the receiving vehicle is experiencing the event that was informed earlier, the vehicle reports to the reputation server and it is assumed that all such experiences are reported immediately.
f. Assuming that all the vehicles are within the communication range, the latest reputation certificates are received and reports are sent without delay.
g. When a feedback is received for a vehicle, the existing reputation score is further updated and stored. Based on the new score, the certificate is generated accordingly.
h. It is assumed that the vehicles in the network do not have any earlier trust built among them.
i. It is assumed that all the vehicles, Servers, RSU's have a synchronised clock settings.

(ii) Algorithmic components
The algorithm uses the following components:

a. Aggr—an aggregation algorithm, that calculates the feedback obtained by the vehicle. The Reputation score is computed based on the feedback obtained.
b. Time Discount (TD)- Time discount function—When a score is received, it need not be accepted as such, because with time, the score might have either

increased or decreased after this received value. Therfore, a time discount fuction can be used. Based on the time when the score is received, the reputation value is offset by multiplying score with some value in the range of [0,1] to discount the reputation value.

c. Digital Signature Schemes: Message integrity can be verified using Digital Signatures. Here, two schemes namely DS_1, DS_2 such that $DS_1 = (KG_1, Sign_1, Verify_1)$, $DS_2 = (KG_2, Sign_2, Verify_2)$ can be used.
d. Hash Function H, Message authentication Code algorithm, MAC
e. Three configurable parameters Th_{rs}, Th_t, Th_{cert} and T such that

i. Th_{rs}—a threshold value to determine whether another vehicle is reputable, usually a value between 0 and 1.
ii. Th_{time}—a threshold used to determine whether a message tuple is sufficiently fresh for feedback reporting.
iii. T— a large time interval during which the vehicles report feedback.
iv. Th_{cert}—time period for which the certificate is valid.

5 Initialisation of the System Components

5.1 Initialisation of the Centralised Reputation Server

The Centralised Reputation Server (CRS) is initialised with a set of public and private key pairs that are to be assigned for the Regional Reputation Servers. The CRS is geographically placed such that it covers a set of RRS covering a larger area. This enables the reputation scores of a smaller area to be aggregated by the CRS and then transmitted to a larger number of vehicles. Any RRS that registers with the CRS receives a pair of keys for further communication. The three tier architecture is as shown in Fig. 1.

i. The CRS receives the aggregated reputation scores that are collected by the RRS at specific intervals.
ii. The scores are then segregated and stored as per the identity of the vehicles.
iii. The feedback ratings are the calculated for the individual vehicles and using continuous feedback rating algorithm, the ratings are prepared and stored locally.
iv. Any RRS can further enquire the CRS for obtaining the scores of the vehicles that are not within the range.

5.2 Initialisation of the Regional Reputation Server (RRS)

The Regional Reputation Server is initialized as follows:

i. The Regional Reputation Server registers itself with the Centralised Reputation server using a public, private key pair (PU_{RRS1}, PR_{RRS1}).
ii. The RRS receives the scores from all the vehicles within its range and creates a local database for storing the details of the vehicles, such as the vehicle's identity, Public Key, MAC Key, current reputation score of the vehicle and a feedback value.
iii. The reputation score of a vehicle is aggregated using the algorithm $Aggr$.

5.3 Installation of the Access Points

The access point are installed in the system to facilitate a communication between the Vehicles and the RRS for which a communication channel needs to be established.

6 Operation of the Reputation System

The CRS, RRS, access Points and the vehicles are initialised and installed with certain algorithms for their operation some of the basic terminologies used in here are as below:

Notation	Purpose
Aggr	Reputation aggregation algorithm
MAC	Message authentication code algorithm
KG_1, KG_2	Key generation algorithm
DS_1, DS_2	Digital signature schemes
TD	Time discount function
$Verify_1$, $Verify_2$	Verification algorithms
Th_{rs}	Reputation threshold (range 0–1)
Th_{time}	Threshold to determine the freshness of a message
Th_{cert}	Certificate validity time
id_{V_1}, id_{V_2}	Identity of the vehicles
$(pu_{V_1}, pk_{V_1}), (pu_{V_2} pk_{V_2})$	Public private key pair of vehicles
(PU_{RRS1}, PR_{RRS1})	Public private key pair of regional reputation server
t_1	Certificate generation time
t_2	Message broadcast time
t_3	Message reception time
rs_{V_1},	Reputation score of vehicle V_1
$H(m)$.	Hash of the message "m"
F_r	Feedback Rating in the range {0, 1}
mk_{V_1}, mk_{V_2}	MAC Key of the vehicles V_1 and V_2
t_{RRS}	Time when the consolidated score is sent by RRS to CRS

Once the System components have been installed, the stage wise process by which the CRS, RRS and the vehicles work collaboratively to establish and maintain a Reputation System is as below.

6.1 Vehicle Registration and Requisition for Reputation Certificate

The registered vehicle requests for its Reputation Certificate from the Regional Reputation Server as below:

i. The vehicle sends its identity id_{V_1} to the RRS.
ii. On receiving a request the RRS creates a new record in the database for the requesting vehicle with the identity id_{V_1}.

iii. If the requesting vehicle had earlier registered with the RRS, then the Certificate can be retrieved locally. Otherwise, the request for the Certificate is sent to CRS. The query for the vehicle id_{VI} is then sent as $Q = ((id_{V_1})_{pr_{RRS_1}})_{pu_{CRS}}$ and receives a reply as $R = ((id_{V_1}, rs_{V_1})_{pu_{RRS_1}})_{pr_{CRS}}$ from which the Certificate can be generated. The Certificate, C for the requesting vehicle is then generated as $C = (id_{V_1}, pu_{V_1}, t_1, rs_{V_1}, \alpha)$, which holds the identity of the vehicle id_{V_1}, the public key of the vehicle pu_{V_1} the time t_1, when the certificate was generated and the reputation score of the vehicle as rs_{V_1}, which it has earned at time t_1. Here, α *is* Digital Signature using the algorithm $Sign_1$ such that

$$\alpha = Sign_1(id_{V_1}, pk_{V_1}, t_1, rs_{V_1})_{pr_{RRS1}}.$$

iv. The Certificate is then sent to the requesting vehicle, which is further stored by the vehicle locally. The Certificate remains valid for the defined time interval, Th_{cert}.

6.2 Road-Related Warnings Generated and Broadcasted by the Vehicle

On obtaining the certificate C from the RRS, the vehicle now generates the message and broadcasts to its neighbours.

i. A message *"m"* could be any information composed by the driver or generated from the sensors of the vehicle. The Hash of this message is calculated as $H(m)$.
ii. At the receiving time t_2, a time stamped Signature is generated by the Vehicle as Θ, which is $\Theta = Sign_2(t_2, H(m))_{prv_1}$.

The vehicle composes the message $M = (m, t_2, \Theta, C)$ and broadcasts to all the nodes in the network.

6.3 Reliability of the Message is Evaluated

When a vehicle V_2 receives the message $M = (m, t_2, \Theta, C)$ from the sender at time t_3, the message is retrieved as below:

i. V_2 checks if the reputation score is acceptable i.e., $rs_{V_1}.TD\,(t_2 - t_1) \geq Th_{rs}$.
ii. Checks if the message received is also fresh, $t_3 - t_2 \leq Th_t$.
iii. The verification algorithm $Verify_1$ is used to check if $\alpha \in C$ by using the public key of the reputation Server PU_{RRS}.
iv. A check on the validity of the message received by V_2 is performed using the verification algorithm $Verify_2$ and the public key of the Vehicle, pu_{V_1}, that is extracted from the certificate C.
v. Once the validity of the message is verified, the vehicle from which the message was received is considered reliable. The message "m" is therefore considered and a feedback is computed for the vehicle. This feedback is further stored for future reporting. If the vehicle is not a reputable one, then further messages from the vehicle is not considered.

6.4 Generation and Reporting of Feedback

On receiving the message m at the time t_3, the vehicle stores the message and waits to experience the warning received. Once the vehicle V_2 experiences the event that was described by m, the reliability of the message received can be justified. If the vehicle V_2 wishes to participate in reporting the feedback about the vehicle to the RRS, then the feedback is generated, which may be either 1 (if true) or 0 (if false) and is calculated as below:

i. V_2 generates a feedback $F_r \in \{0, 1\}$, where 1 indicates a reliable message and 0 indicates an unreliable message.
ii. V_2 submits $(id_{V_2}, id_{V_1}, F_r, t_2, t_3, H(m), \Theta)$ to the trusted hardware.
iii. The trusted hardware computes the Message Authentication Code "D" from t_2, Θ and its MAC key mk_{V_2} as $D = MAC(id_{V_1}, id_{V_2}, F_r, t_3, t_2, H(m), \Theta)_{mk_{V_2}}$.
iv. V_2 generates the feedback tuple F as $F = (id_{V_1}, id_{V_2}, F_r, t_3, t_2, H(m), \Theta, D)$. If the value of F_r is 1, it is a positive feedback else if its value is 0, it is a negative feedback.

6.5 Aggregation of Reputation Score at the RRS

The RRS checks the following:

i. RRS receives the feedback score from the set of registered vehicles.
ii. RRS performs the set of following tasks
    a. whether $t_3 - t_2 \leq Th_{time}$.
    b. calculates D by calculating MAC from the tuple (id_{V1}, id_{V2}, f_r, t_2, t_3, $H(m)$, Θ) using mk_{V_2}.
    c. checks if Θ is valid, using the algorithm $Verify_2$ and pr_{V_2}.
iii. For a vehicle with id_V, the scores received by the vehicle for a time period say "t_{start}" to "t_{end}" are aggregated. If any of the above check fails, then the message F is discarded.
iv. For a vehicle with id_V, the scores received by the vehicle for a time period say "t_{start}" to "t_{end}" are aggregated. If any of the above check fails, then the message F is discarded.
v. The RRS applies the Aggregation algorithm "$Aggr$" for a specific Vehicle V_x on all the received feedback messages and replaces the new score with the already available score rs_{V_1}.
vi. This aggregated Reputation score "S" is further composed into messages and sent to the CRS, at time t_{RRS}.

$$S = (id_{V_1}, rs_{V_1}, t_{RRS1}, Th_{cert})pr_{RRS1}$$

6.6 Reputation Aggregation Algorithm

i. For a specific vehicle V, the algorithm selects all the feedback that have been reported from the start time t_{start} until the present time t_{end}, from the available database in the RRS, as:

$$S = \{F : (id_{V_1} = id_V)\ \&(\ t_{start} < t_3 < t_{end})\}$$

ii. Multiple Feedbacks reported for a vehicle is then aggregated into a single value, by averaging and denoted as ''r_{V_i}''.

6.7 Vehicle Revocation

A belief parameter r_{belief} is configured for a node, (say) 70 %. The vehicle should have earned at least 70 % scoring. For a set of (say), 10 transmissions, the vehicle should have earned a reputation score of value "1", at least for 7 transmissions. If a vehicle does not satisfy this constraint, it cannot be issued a Reputation Certificate for further communication.

7 Network Simulation

The Simulation is performed using Ns-2 with the parameters as shown in Table 1. The configurable parameters Th_{rs}, Th_t, Th_{cert} and T are set as 0.7, 30 min, 30 min and 10 min respectively. These minimal values helps to visualise the effect of these parameters within the simulation time.

Three Regions with quite a geographical distance between them is considered for this simulation. Vehicles with ID's 1, 2, 3, 4, 5, 11 are configured under region 1, Vehicles with

Table 1 Simulation parameters

1	No. of nodes	60
2	Total simulation time	30 min
3	Channel	Wireless channel
4	Propagation	Two ray ground
5	Net info	Phy/Wireless Phy
6	MAC	MAC/802_11
7	Ifq	Queue/DropTail/PriQueue
8	Antenna	Antenna/Omni Antenna
9	Ifqlen	150
10	Routing protocol	AODV

Table 2 Reputation scores of the vehicles in region 1 stored at RRS1

Veh. ID	Time t1	Time t2	Time t3	Time t4	Time t5	Time t6	Time t7	Time t8	Time t9	Aggr score t5 < t < t9
1	7	1	6	0	4	8	8	1	7	28
2	2	9	5	5	3	1	3	0	8	15
3	4	6	4	6	1	9	7	9	7	33
4	6	9	9	3	4	8	4	9	7	32
5	8	7	0	3	3	8	5	7	3	26
11	7	2	4	2	1	1	6	1	6	15

Table 3 Reputation scores at RRS2

Veh. ID	Time t1	Time t2	Time t3	Time t4	Time t5	Time t6	Time t7	Time t8	Time t9	Aggr score t5 < t < t9
6	5	0	2	2	6	7	0	4	5	22
7	8	8	6	3	2	2	4	1	0	9
8	6	2	2	0	2	2	5	2	2	13
9	4	3	3	4	9	5	6	3	9	32
10	9	6	3	7	1	9	4	4	7	25
12	9	2	1	6	1	9	9	2	7	28

Table 4 Reputation scores at RRS3

Veh. ID	Time t1	Time t2	Time t3	Time t4	Time t5	Time t6	Time t7	Time t8	Time t9	Aggr score t5 < t < t9
13	7	2	1	2	4	1	2	4	0	11
14	6	2	0	7	0	6	3	2	2	13
15	4	8	9	0	2	5	2	1	8	18
16	0	1	5	3	0	8	2	4	4	18
17	3	8	0	8	1	4	2	3	5	15
18	6	0	2	9	3	1	6	7	0	17
19	2	4	1	0	5	8	4	2	5	24
20	5	5	0	0	6	9	1	2	8	26

IDs' 6, 7, 8, 9, 10, 12 under Region 2 and ID's 13, 14, 15, 16, 17, 18, 19, 20 in Region 3. The three locally configured RRS's collect the scores from the vehicles within their geographical domain, aggregate them and further send the scores to the Centralised Reputation Server. The Centralised Reputation Server accumulates all the scores and stores these values for further queries. Any RRS can query the CRS to obtain the scores for a far away Vehicle. For instance, when RRS1 queries the CRS for the score of Vehicle with ID 11, that does not belong to its geographical domain, the value so far aggregated for the vehicle is sent by the CRS. Thus the reputation of the vehicle earned so far can be distributed to vehicles in Larger area. The reputation scores that are aggregated at the Regional level, RR1, RR2, RR3 and RR4 are as shown in Tables 2–5 respectively.

The CRS identifies the minimum and maximum scores obtained by the Vehicles. When the vehicles decides the next forwarding vehicle based on the reputation score it had earned, there is a considerable better performance and the throughput is found to increase as in Fig. 2. The Centralised scores earned by the vehicle aids in efficient forwarding of the packets thus aiming a better performing network.

Compared to the previous schemes, the time taken by the vehicles in the current scheme to update the scores has been comparatively reduced as shown in Fig. 3.

Table 5 Aggregated scores at CRS at time t9

Vehicle ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Score	28	15	33	32	26	22	9 (Min)	13	32	25	15	28	11	13	18	18	15	17	24	36 (Max)

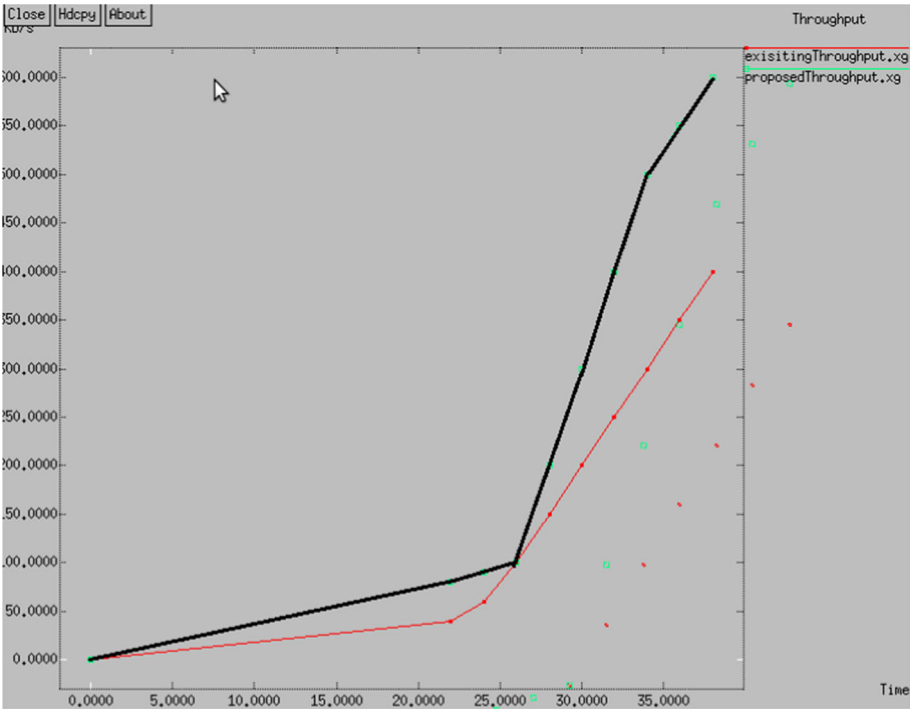

Fig. 2 Better throughput obtained when vehicles use Reputation Scores

Therefore, as in Fig. 2, the throughput is found to increase and Fig. 3 shows reduction in time to send the packets in the 3-Tier architecture. Therefore, it can be seen that the proposed 3-Tier Centralised architecture for Reputation Systems, exhibit a better performance.

8 Conclusion and Future Work

The message reliability can thus be achieved by establishing a secured Centralised Reputation system. The system can be established to serve a large number of vehicles spanning to a large geographical area. Compared to the earlier schemes, this 3-Tier architecture, the messages shared and the scores earned can be utilized by the vehciles in a much gretaer area. In this paper, we have analysed the possibilty of implementing a Centralised Reputation System for VANETs' and it has also been analysed that the message drop rate is minimised and the reputation scores are at a higher value than the earlier scheme. In future, the discrete ratings can be converted to Contiuous ratings and privacy protection schemes may be incorporated into the architecture for security.

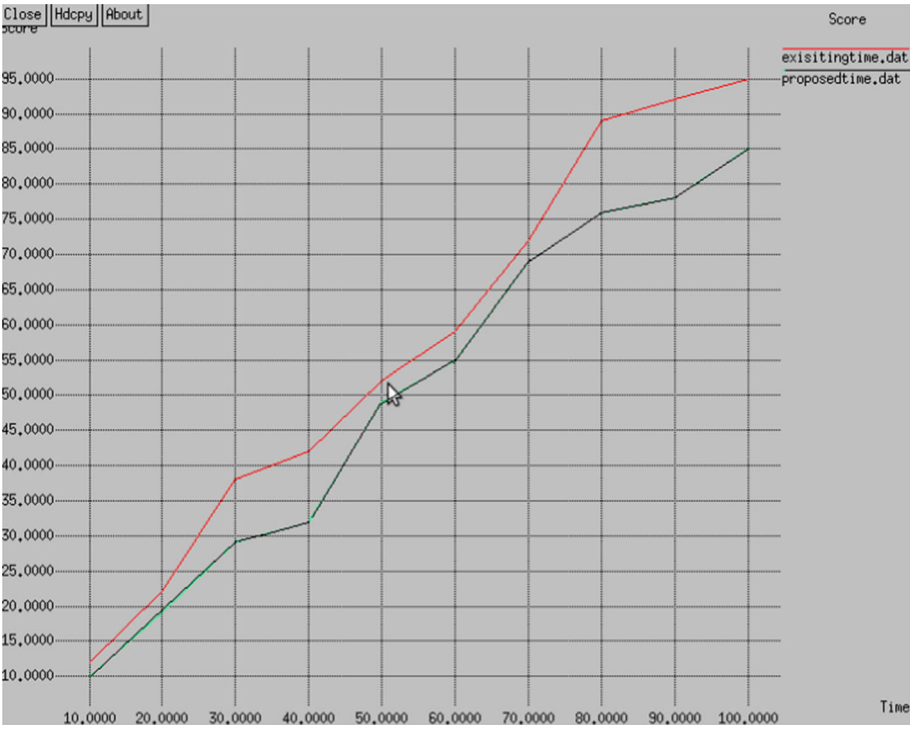

Fig. 3 Less time consumption to update the scores

References

1. Luo, J., & Hubaux, J. P. (2004). A survey of inter-vehicle communication, Tech. Rep. IC/2004/24, EPFL, Lausanne, Switzerland.
2. Leinmüller, T., Buttyan, L., Hubaux, J. P., Kargl, F., Kroh, R., & Papadimitratos, P., et al. (2006). Sevecom—secure vehicle communication.
3. Resnick, P., Zeckhauser, R. (2002) Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system. In Michael R. Baye (eds.) The economics of the internet and E-Commerce, volume 11 of Advances in Applied Microeconomics (pp. 127–157). Elsevier Science.
4. Swamynathan, G., et al. (2007). Globally decoupled reputations for large distributed networks. *Advances in Multimedia, 1*, 12.
5. Raya, M., & Hubaux, J. (2007). The security of vehicular ad hoc networks. *Journal of Computer Security, 15*(1), 39–68.
6. Kounga, G., Walter, T., & Lachmund, S. (2006). Proving reliability of Anonymous information in VANET's. *IEEE Transactions, Vehicular Technology, 56*(6), 3442–3456.
7. Golle, P., Greene, D. H., & Staddon, J. (2004). Detecting and correcting malicious data in VANETs. In Proceedings of 1st ACM international workshop vehicular Adhoc networks, pp. 29–37.
8. Dötzer, F., Fischer, L., & Magiera, P. (2005) VARS: a vehicle ad hoc network reputation system. In Proceedings of 6th IEEE international symposium world wireless mobile multimedia networks (Vol. 1, pp. 454–456).
9. Minhas, U., Zhang, J., Tran, T., & Cohen, R. (2010). Towards expanded trust management for agents in vehicular ad hoc networks. *International Journal of Computer Intelligence Theory Practice, 5*(1), 3–15.
10. Li, Qin, Malip, Amizah, Martin, Keith M., Ng, Siaw-Lynn, & Zhang, Jie. (2012). A reputation-based announcement scheme for VANETs. *IEEE Transactions on Vehicular Technology, 61*(9), 4095–4108.

11. Balon, N., & Guo, J. (2006). Increasing broadcast reliability in vehicular ad hoc networks. In VANET '06 Proceedings of the 3rd international workshop on vehicular ad hoc networks, pp. 104–105.
12. Hassanabadi, B., & Valaee, S. (2014). Reliable periodic safety message broadcasting in VANETs using network coding. *IEEE Transactions on Wireless Communications, 13*(3), 1284–1297.

T. Thenmozhi is currently an Assistant Professor (Senior Scale) and HoD In-charge of Information Technology with the Faculty of Engineering, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India. She has graduated in B.E. Computer Science and Engineering, M.B.A. in Marketing and Finance, Masters in Computer Engineering and currently working towards her Ph.D. Degree in Anna University of Technology, Chennai. Her research interests include Applied Cryptography, Wireless Network security and Vehicular Adhoc Networks.

R. M. Somasundaram received his Ph.D. in Computer Science in 2000, from the University of Periyar, Tamilnadu, India. He is currently working as a Professor at SNS College of Engineering, Coimbatore, Tamilnadu, India. He has teaching experience of over three decades, and has authored many books that add on to his credit. His current areas of interest include Automata Theory, Computing, Wavelet Transforms, and Applied Algebra. He has his publications in the area of Computer Vision applied to automation, Motion Analysis, Image Matching, Image Classification and View-based object recognition and Network Security in leading journals and magazines.