A New Trusted Routing Protocol for Vehicular Ad Hoc Networks Using Trusted Metrics

Thangakumar Jeyaprakash[1], Rajeswari Mukesh[2]
(Corresponding author: Thangakumar Jeyaprakash)
School of Computing Sciences & Hindustan University[1]
RajivGandhi Salai, Padur, Chennai, India
School of Computing Sciences & Hindustan University[2]
RajivGandhi Salai, Padur, Chennai, India
(Email: tkumar@hindustanuniv.ac.in, rajeswarim@hindustanuniv.ac.in)
(Received Nov. 20, 2015; revised and accepted Mar. 30 & May 31, 2016)

Abstract

Trusted routing in VANET is a challenging task due to highly dynamic network topologies and openness of wireless architecture. To provide secure routing among the Vehicular Ad-hoc Networks (VANET) and to avoid selfish nodes, an Optimized Node Selection Routing Protocol (Trusted-ONSRP) of VANET has been designed based on trusted metrics using a Trusted Computing Algorithm. The results stated that the T-ONSRP routing shows higher performance in security measures than the existing routing protocols.

Keywords: Routing protocol, trust, VANET, vehicular ad-hoc networks

1 Introduction

Vehicle to Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) are two distinguished models for real-time application. The past assertions for a centralized control object are committed to data handling and decision making. Given the self-motivated environment of the complicated communications nodes, the ubiquity along the road becomes a compulsory constraint. This might suggest a high- reasonable work, due to the claimed organization of stretched communication infrastructure road-sided [7]. To provide trust and reputation models [4, 5, 12], the following features such as Low Complexity [8], Scalability, Sparseness, Security [19], Performance and sustainability and Confidentiality have been considered in this proposed paper.

In the upcoming chapter, we will see a brief literature survey about the existing trusted routing protocols protocols for the usability of VANET. Section 3 describes the proposed work and the architecture of Trusted-ONSRP. Section 4 describes the T-ONSRP simulation experiments with various scenarios to find the reputation of vehicles and the last section represents the results of the proposed routing protocol which has been compared with the existing routing protocol.

2 Related Works

Pophali et al. [9] proposed a trusted oppurtunistic routing protocol for VANET to improve the communication security and to safeguard the network from mischievous nodes. The author derives the minimum cost opportunistic routing to calculate the node cost to forward the packet from the source node to the destination. The malicious node has been strictly restricted from joining the network. Here, there is a chance of selfish nodes can be present in the network which restricts the transmission from the source to the destination vehicle.

In Yang [18] framework, the author describes a correspondence mining technique which is used for classifying similar information or same vehicles. The author proposed a reputation evaluation algorithm based on similarity theory. The reputation of each vehicle has been derived from the recommendation of other vehicles based on the weights calculations are made on which the selfish nodes are and other malicious nodes create a confusion instead of a reference given to a particular vehicle waiting for the reputation values.

Goudarzi et al. [1] presents a methodical literature review to provide complete and balanced material about various present trust conceptions in VANETs to upsurge excellence of data in transportation. The authors proposed a Trust model using the fuzzy logic to detect the misbehavior nodes. The authors also stated that there is no lightweight intelligence trust model available for VANETs that satisfies all the desired properties of a trust model.

Tan et al. [13] proposed a Novel trust management system. In this system, they use fuzzy logic and Graph the-

ory to evaluate the node trust value and it is integrated with the Optimized Link State Routing Protocol (OLSR). These algorithms are proposed to prevent malicious and victim nodes from participating in the networks [3] as much as possible. It does not include the selfish behavior nodes.

Rabayah et al. [2] proposed a routing protocol for VANET which associates the features of location based and topology based routing protocol. They integrate the protocol in such a way that if the location information is degraded, it automatically uses the reactive routing protocol to transmit the packet from the source to the destination. The author states the protocol is accessible and scalable and has an overhead over the new scalable Hybrid Routing does not include any Trust model to reduce the selfish nodes.

Wu et al. [11] proposed a new trusted routing protocol in VANET based on GeoDTN+Nav by using a greedy model which is associated with the four steps for initializing the routes, trusted routing establishment and the deletion of routes. As the greedy model [6] has more communication overhead, this model larger number of route discovery to establish the trusted route.

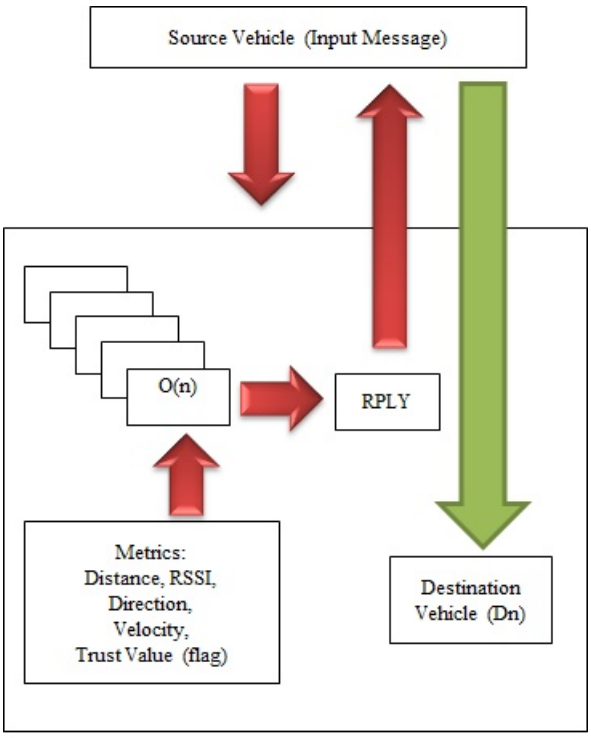

Figure 1: Architecture of ONSRP

3 Proposed Work

3.1 Trusted Routing

There are two different types of trust models: 1) Infrastructure Based; 2) Self-organizing based.

The Infra-structure based trust models are Certificate based and RSS based. The Self Organizing models are entity oriented, data oriented and combined trust models. The reputation of the vehicle can be identified by data oriented Trust Model. The decentralized and self-controlled characteristics of Vehicular Adhoc Network are the widely recognized models, given the wireless-oriented nodes. To provide secured communication, a new trusted routing protocol of VANET has been proposed to avoid the selfish node behavior of the Vehicular Adhoc Networks which includes trust properties such as distance, direction, velocity and Trust value etc.

Figure 1 shows the architecture of ONSRP. Many attacks can be identified to compromise them, if the security requirements have been established for VANETs. Here we described the types of attacks of VANET with the activity of these attacks and their potential consequences. From these attacks, the selfish node behavior, characteristics and issues have been analyzed. The attacks are classified as attacks on identification and Authentication. (Impersonation and Sybil), attacks on Privacy. (Identity revealing and Location Tracking), attacks on non-repudiation (Sharing the same Credentials by two or more), attacks on confidentiality (Eavesdropping), attack on Availability (DoS, Selfish Node Behavior), availability in VANETs is very important in both communication channel and the participating nodes in the network. Network Denial of service leads to non- availability of the network for the participating vehicles which ends in dropping all messages or just a few according to self-interests known as Selfish Behavior.

The communication link failure due to high mobility can be identified by calculating the communication range depends upon the received signal strength. The Received signal strength index (RSSI) at a time period of transmission of packets from one node to another as shown with the following formulae using the distance between the two nodes. The Received signal strength index is directly proportional to the transmitted power and inversely proportional to the power loss. Each node communicates the data to the disseminating side of the next hop in the shortest route destination. The distance between the each node which is optimal is the Received Signal Strength Threshold. When the received signal strength index during the time period of receiving information is lesser than the RSST (RSST), the transmitting vehicle informs the previous node regarding the weaker signal strength which leads to communication link failure and discards the RREQ received from the precedent vehicle. Now the precedent node detects the weaker strength before transmitting the packet and broadcast the RREQ to other nodes.

3.2 Trust Metrics

The optimized node O(n) selection routing protocol works on a hybrid reactive protocol and not on a proactive ba-

sis. The routing information will be shared together on demand using the trusted metrics such as distance, RSSI, direction etc. Otherwise, the route discovery process communication overhead increases, if the proactive routing has been followed. By discarding the broadcasting of RREQs, T-ONSRP is predictable considerably to avoid the communication overhead and reduce the communication delay. In addition to that, the ONSRP does not rely on any HELLO messages or ACK messages to check the status of the links to avoid unnecessary overheads. For the route maintenance or when the route break occurs, ONSRP used the RERR, Route error message to initiate a new route discovery process.

3.3 Distance

In order to determine this direction [14, 15], a node calculates the distance of the neighbor node as follows. At Time T1,

$$Distance(Do) = \Pi Minimum(D1||D2||\cdots||Dn), \quad (1)$$

where $D1$ = Distance between the Last node of path 1 routing table and the Destination node; $D2$ = Distance between the Last node of path 2 routing table and the Destination node; DN = Distance between the Last node of path N routing table and the Destination node.

The communication link failure due to high mobility can be identified by calculating the communication range depends upon the received signal strength. The Received signal strength index (RSSI) at a time period of transmission of packets from one node to another as shown with the following formulae using the distance between the two nodes.

$$RSSIPr[do] = \frac{CtPt}{d^4 Pl} \quad (2)$$

$$RSST = Dn = \sqrt{(X1-X2)^2 + (Y1-Y2)^2} \quad (3)$$

3.4 Direction

In order to determine this direction, a node calculates the direction of the neighbor node as follows.

At time T1, Direction in degrees

$$(Ao) = \Pi D(RWP(i,j))||Min(D1||D2||\cdots||Dn)(i,j), \quad (4)$$

where $D1$ = Distance between the Last node of path 1 routing table and the Destination node; $D2$ = Distance between the Last node of path 2 routing table and the Destination node; DN = Distance between the Last node of path N routing table and the Destination node; D = Destination; RWP = Random way points in the network are; i, j = two successive random way points.

3.5 Velocity

In the following, we utilize the velocity [16, 17] of nodes parameter from viewpoint to develop our Flag Trust model. We consider the velocity distribution over simulation of network to determine the network connectivity status. The velocity of nodes is the main parameter that determines the network topology dynamics. It also plays a significant role in determining the estimated communication time between two vehicles. At Time T1,

$$Velocity(Vo) = \Pi V(Dn)||V(N1||N2||\cdots||Nn), \quad (5)$$

where Dn = Destination node; $N1$ = Velocity of Neighbor Node 1 of Dn; $N2$ = Velocity of Neighbor Node 1 of Dn; Nn = Velocity of Neighbor Node 1 of Dn; Vo = Optimized Velocity.

From Equations (3), (4) and (5):

$$Trustvalue = \Pi Do.Ao.Vo.FlagTrustCount. \quad (6)$$

3.6 The Algorithm

When the source node has the information to send at time T1, the trustworthiness of each node has been calculated using the trusted computing algorithm for each node available between the source and the destination vehicle. At this time T1, the algorithm finds the optimized node to transmit the packet from the source node to the destination node for the most reliable transmission of data. The source node creates a RREQ, Route request message and broadcasts to the neighbor nodes to find the possible route to the destination (See Algorithm 1).

Each node transmits the RREQ to the neighbor nodes to find the destination node for the packet transmission. The intermediate vehicles those received the RREQ are allowed to forward the route REPLY, when its trusted value has been calculated by the trusted routing protocol algorithm. Otherwise, the RREQ will be discarded. When the RREQ arrives at the neighbor node to the destination, and it is assumed to be a trusted vehicle, a route reply will be sent back to the source vehicle to start the transmission of data without link failure due high mobility and selfish node behavior in the Vehicular Adhoc Network.

4 Simulation Experiments

4.1 General Assumptions

Some assumptions have to be made about the ONSRP model [18] to make complexity lesser:

- At most one or two selfish node vehicles are available in the network.
- No hurdles and infrastructures such as buildings etc. in the road topology.
- The type of communication is bidirectional between the two vehicles, if available in the coverage area of the network.

Algorithm 1 Trusted Node Identification

1: Input: A source vehicle(S) and the destination (D) vehicle.
2: Output: Transmission of data with less no of link failure.
3: Get intermediate nodes trusted values using trusted computing algorithm.
4: Calculate the trusted values for all the intermediate nodes present between S and D.
5: Trust Threshold (TTH)= Total no of Nodes (Initialized Value)
6: $O(n) = \alpha\Pi(Do, Ao, Vo)$
7: $T(\beta(O(n))) = initial\_connect\_value + Total\ No\ of\ Nodes$
8: Compare $T(\beta(O(n))$ with Trust Threshold(TTH)
9: **if** $T(\beta(O(n))) >> TrustThreshold(TTH)$ **then**
10: $T(\beta(O(n))$ *to send an RREP to the source vehicle*(S)
11: Discard RREQ Go to Line no 4
12: **end if**
13: Start data transfer
14: End

- Each vehicle is connected to the other in the Vehicular network and follows the car following model. Stand by vehicles are also available in the network.
- Each vehicle is equipped with global positioning system (GPS) to show its own location which helps to provide the absolute information to other vehicles.
- All the vehicles transmits and receive the data using Optimized Node selection routing protocol with the calculated trusted node to avoid the selfish node behavior which leads to communication link failure.
- The energy back up of each vehicle is always sufficient for the requirement of application to transmit the data from one vehicle to another.

4.2 Scenario I: All Vehicles Moving in the Same Direction (Towards East)

When a source vehicle A wants to transmit a packet to the Destination vehicle, it has to obtain the RSSI value of the neighbor node of the destination vehicle to send back the RRPLY for the efficient data transfer. In Figures 2, 3, 4, 5 each vehicle is labelled with a vehicle id presented in the vehicular Adhoc network. Note the A,B,C,D,E,F,G,H,I,J,N are representing the source vehicle, intermediate nodes and the destination vehicle respectively. The nodes K[RSSI(i)], L[RSSI(i+1)],. M [RSSI (n-1)] are the set of intermediate nodes which has been received the RREQ from the source vehicle A. Thus the RREQ is broadcasted for the nodes B,E,G,J,L,N and D,F,H,M,N and C,I,K,L,N respectively. According to the formulae, the RSSI value has been calculated for the standard distance to reduce the complexity of the routing protocol. In Scenario I, as all the vehicles are moving in the same direction, trusted routing algorithm has been implemented to the minimum distance RSSI value node.

The trusted routing algorithm has been implemented to the minimum distance RSSI value node [10].

$$\begin{aligned}
RSSI[(i)] &= 52.45dBmwherei = 1m \\
RSSI[(i+1)] &= 53.47dBmwherei = 2m \\
RSSI[(i+3)] &= 58.23dBmwherei = 4m \\
RSSI[(i+5)] &= 62.34dBmwherei = 6m \\
RSSI[(i+8)] &= 64.45dBmwherei = 9m \\
RSSI[(i+10)] &= 66.32dBmwherei = 11m \\
RSSI[(i+14)] &= 75.43dBmwherei = 15m \\
RSSI[(i+19)] &= 80.71dBmwherei = 20m.
\end{aligned}$$

Trusted Node Calculation: Scenario I

Node M = 52.45 DBm;

If Data Transfer initiated via Node M:

$$\begin{aligned}
&InitialConnectValue = 1; \\
&InitialReputationValue(Rn) = 1; \\
&TotalnumberofNodespresent = 250; \\
&TrustThreshold(TTH) = InitializedValue \\
&\qquad = 250; \\
&O(n) = \alpha\beta(Do, Ao, Vo); \\
&Rn(O(n))) = Rn + initial_connect_value \\
&\qquad + InitializedValue = 252; \\
&Rn(Node(M)) = 252; \\
&Rn(Node(M)) > TrustThreshold(TTH); \\
&setVehicletrustedflag = 1.
\end{aligned}$$

else

$$\begin{aligned}
&InitializeReputationValue(Rn) = 0; \\
&InitialConnectValue = 0; \\
&Rn(O(n))) = Rn + initial_connect_value \\
&\qquad + Initialized\ Value = 250.
\end{aligned}$$

4.3 Scenario II: All Vehicles Moving Bidirectional (Towards East and West)

In the scenario II, the vehicles are moving bidirectionally. In Figure 6, When a source vehicle A wants to transmit a packet to the Destination vehicle, Even though it has to obtain the RSSI value of the neighbor node of the destination vehicle to send back the RRPLY for efficient data transfer, as the vehicles are moving in different lanes with opposite directions. In Scenario II, as all the vehicles are moving in the opposite direction, trusted routing algorithm has been implemented to the nodes moving in the same direction along with the destination node with the minimum distance RSSI value node.

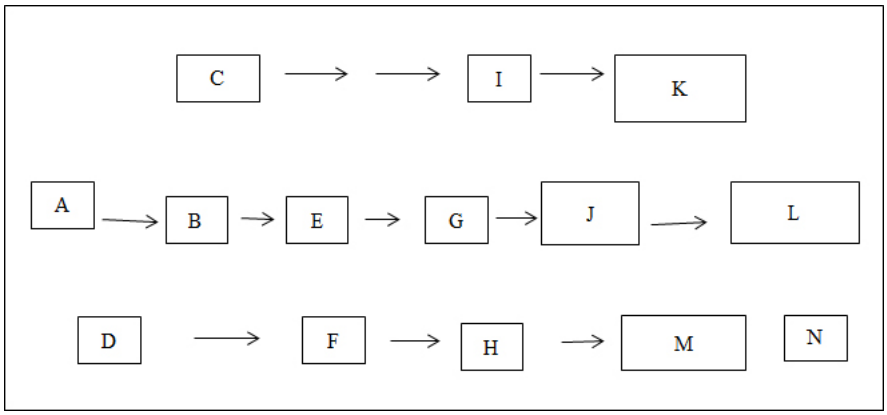

Figure 2: Set of vehicles A, B, C, D, E, F, G, H, I, J, N

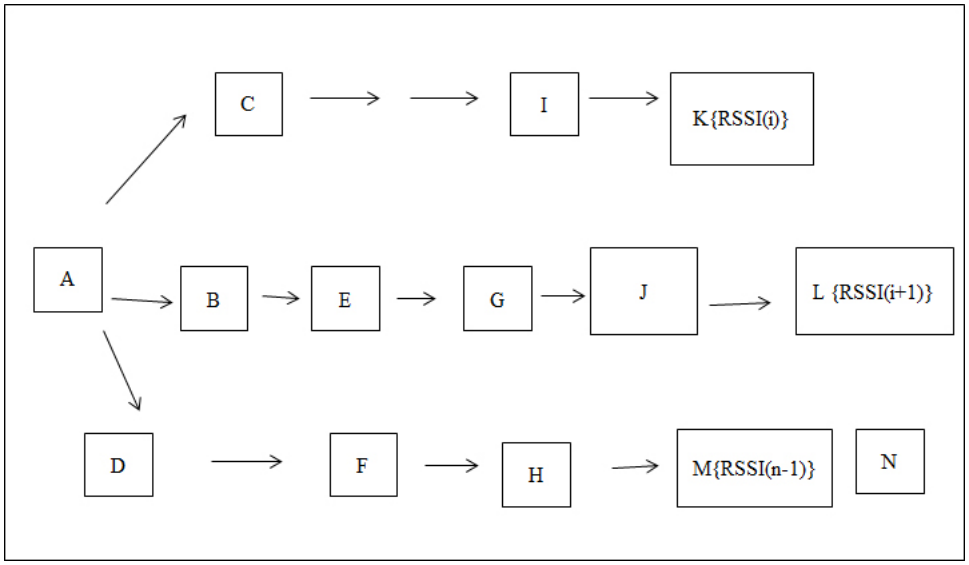

Figure 3: RSSI calculation

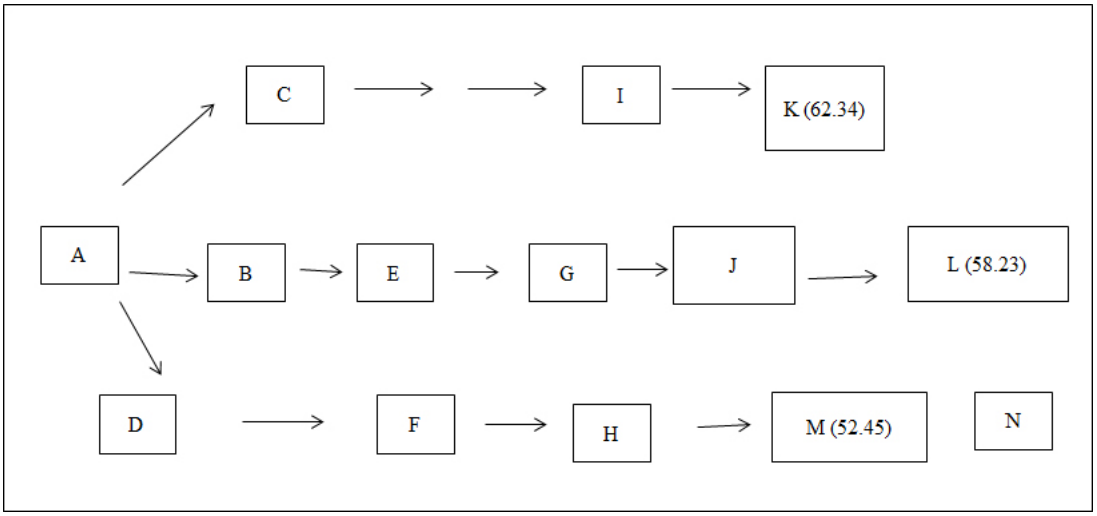

Figure 4: Node with RSSI values (Minimum distance)

Trusted Node Calculation: (Scenario II)

Node M = 58.45 DBm.

If Data Transfer initiated via Node M:

$$InitialConnectValue = 1;$$
$$InitialReputationValue(Rn) = 1;$$
$$TotalnumberofNodespresent = 250;$$
$$TrustThreshold(TTH) = InitializedValue = 250;$$
$$O(n) = \alpha\Pi(Do, Ao, Vo);$$
$$Rn(Node(M)) = 252 fromScenarioI;$$
$$Rn(O(n))) = Rn + initial\_connect\_value + Initialized\ Value = 252 + 1 + 250 = 503;$$
$$Rn(Node(M)) = 503;$$
$$Rn(Node(M)) > Trust\ Threshold\ (TTH);$$
$$set\ Vehicle\ trusted\ flag = 1.$$

else

$$InitializeReputationValue(Rn) = 0;$$
$$InitialConnectValue = 0;$$
$$Rn(O(n))) = Rn + initial\_connect\_value + Initialized\ Value = 250;$$
$$Rn(Node(M)) == Trust\ Threshold\ (TTH);$$
$$set\ Vehicle\ trusted\ flag = 0.$$

4.4 Scenario III: Selfish node Behavior (Node M)

In the selfish node attack situation, there is at most one Selfish node vehicle present in the network. In Figure 7, Assume the vehicle M. Vehicle M could be either a mischievous or a reputed vehicle. According to the formulae, the RSSI value has been calculated for the standard distance to reduce the complexity of the routing protocol. In Scenario III, as all the vehicles are moving in the same and opposite direction with the available of malicious node (selfish node), trusted routing algorithm has been implemented to the find the reputed node or a selfish node for the efficient data transfer to avoid the non-availability of the network.

Trusted Node Calculation: (Scenario III)

Node M = 52.45 DBm;

If Data Transfer initiated via Node M fails due to the Selfish Node Attack:

$$InitialConnectValue = 1;$$
$$InitialReputationValue(Rn) = 1;$$
$$TotalnumberofNodespresent = 250;$$
$$TrustThreshold(TTH) = InitializedValue = 250;$$
$$O(n) = \alpha\Pi(Do, Ao, Vo);$$
$$Rn(O(n))) = Rn + initial\_connect\_value + Initialized\ Value = 252;$$
$$Rn(Node(M)) = 252;$$
$$Rn(Node(M)) > TrustThreshold(TTH);$$
$$setVehicletrustedflag = 1.$$

else

$$InitializeReputationValue(Rn) = 0;$$
$$InitialConnectValue = 0;$$
$$Rn(O(n))) = Rn + initial\_connect\_value + Initialized\ Value = 250;$$
$$Rn(Node(M)) == TrustThreshold(TTH);$$
$$setVehicletrustedflag = 0.$$

5 Results and Comparisons

In Figures 8 and 9, the results shows the performance of ONSRP eventually exceeds the performance of Scalable Hybrid Routing Protocol, Modified Ad-hoc On demand distance vector Routing protocol and Greedy Perimeter coordinator Routing Protocol with the aspects of the packet delivery ratio, End-End Delay and total nunmer of link failures.

In Figure 10, the total number of link failures has been reduced by ignoring the selfish nodes available on the network. The number of link failures has been reduced in a more gradual manner when compared to the existing routing protocol using the Optimized Node selection Routing Protocol. The graph shows the performance of ONSRP against the existing routing protocols in the presence of various mobility models and the Drivers realistic mobility model. From the results of various simulations, we have proved the performance of the proposed ONSRP against the various existing routing protocols.

6 Conclusions and Scope of Work

An Optimized node selection routing protocol of VANET has been implemented using Trusted Computing Algorithms with the features of extended light weight routing and routing messages with trust information which can be updated directly through optimized node selection Routing protocol Algorithm. When performing trusted routing discovery, communication overhead can be reduced

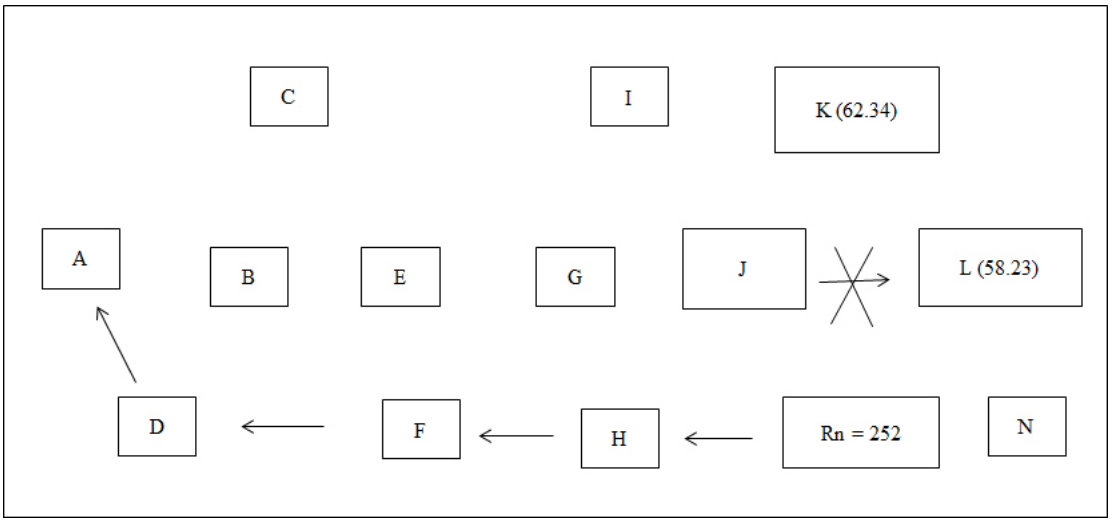

Figure 5: RRPLY sent to source node from node M

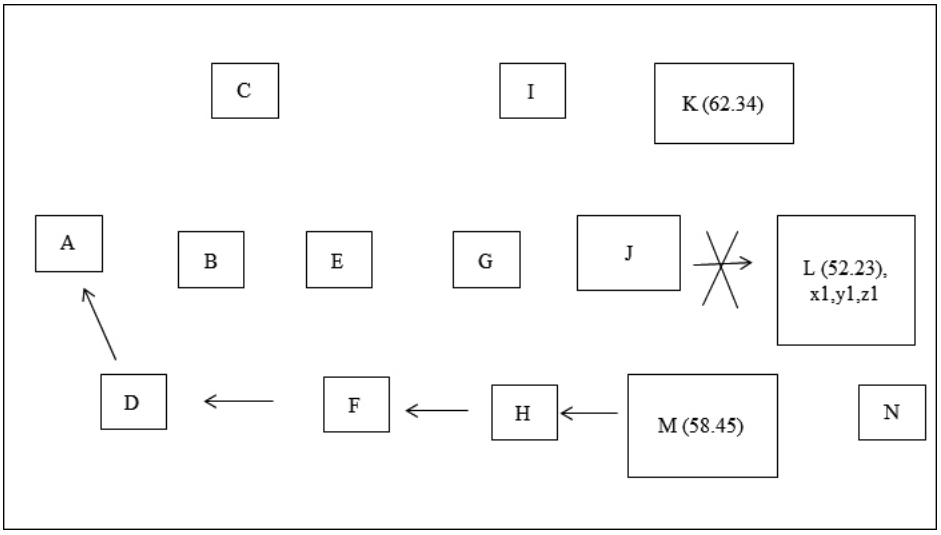

Figure 6: RPLY sent to source node via M (same direction)

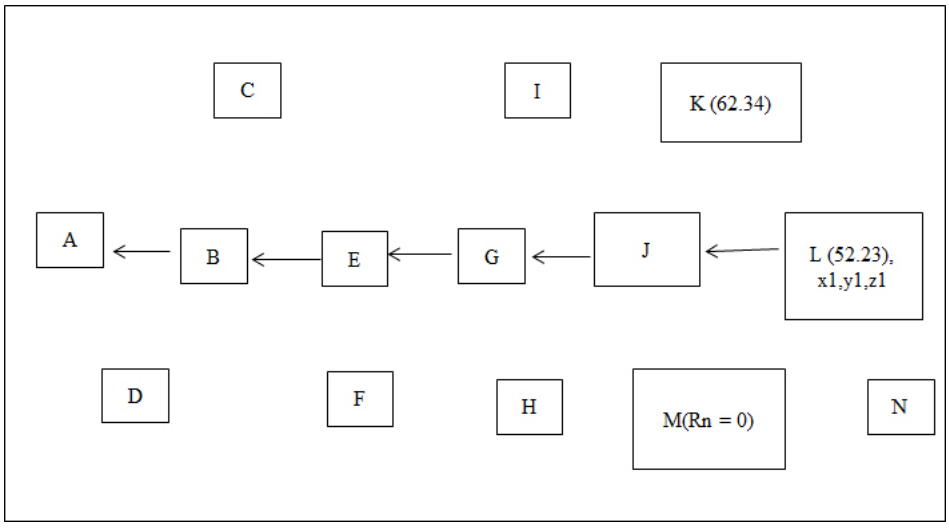

Figure 7: RRPLY sent to source node from node L as M behaves as selfish node (Rn = 0)

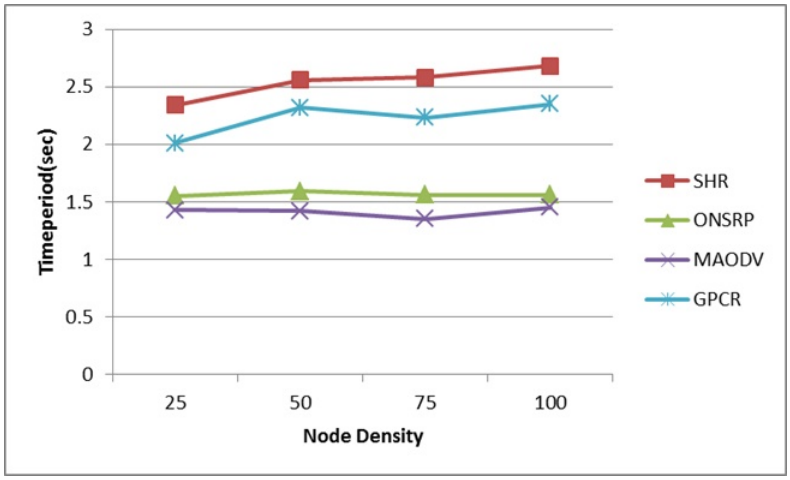

Figure 8: End-End delay analysis

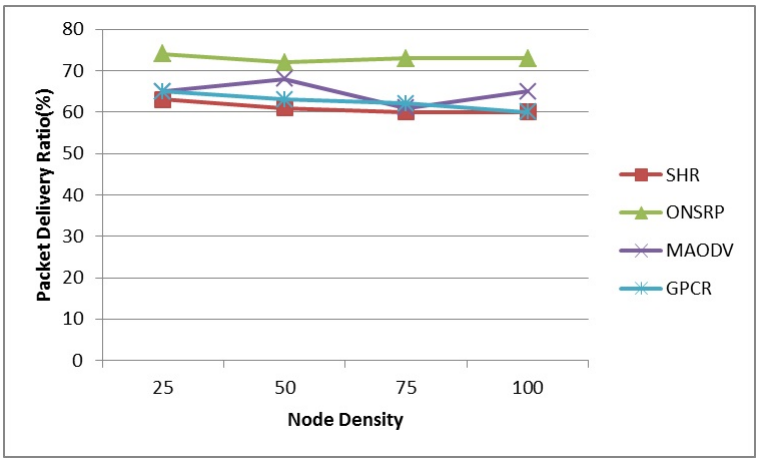

Figure 9: Packet delivery ratio

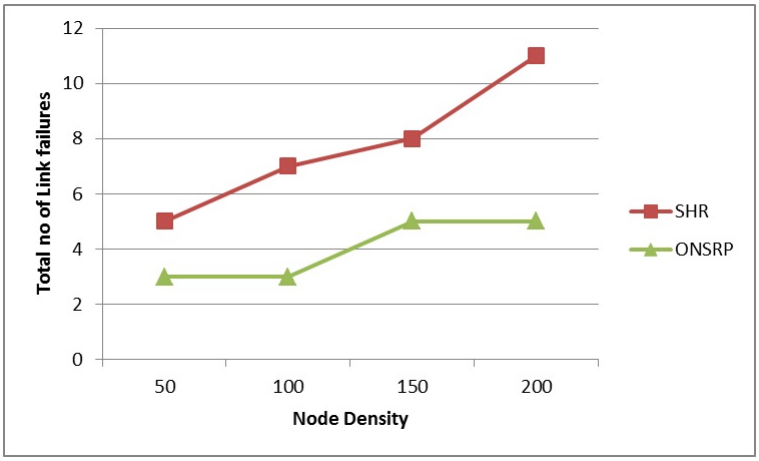

Figure 10: Link failures vs. node density

and packet delivery ratio can be increased by avoiding the frequent route discovery process. This performance has been proved, but can perhaps be shown to be valid for other existing shortest-path protocols. The scope of the work can move towards the comparison of T-ONSRP against other routing protocols in an attempt to further support this performance analysis.

References

[1] S. A. Soleymani, A. H. Abdullah, W. H. Hassan, M. H. Anisi, S. Goudarzi, M. A. R. Baee and S. Mandala, "Trust management in vehicular ad hoc network: A systematic review", *EURASIP Journal on Wireless Communications and Networking*, DOI: 10.1186/s13638-015-0353-y, Dec. 2015.

[2] M. Al-Rabayah and R. Malaney, "A new hybrid location-based ad-hoc routing protocol," *IEEE Global Telecommunications Conference (GLOBECOM'10)*, vol. 1, no. 6, pp. 6–10, Dec. 2010.

[3] C. Bhalodia, A. M. Lathigaraet, "Modified route maintenance in AODV routing protocol," *International Journal of Advance Engineering and Research Development*, vol. 1, no. 5, pp. 1–9, May 2014.

[4] M. Gerlach and F. Friederici, "Implementing trusted vehicular communications," *69th IEEE Vehicular Technology Conference (VTC'09)*, pp. 1–2, Apr. 2009.

[5] F. G. Mármol and G. M. Pérez, "Trip, A trust and reputationinfrastructure-based proposal for vehicular ad hoc networks," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 934–941, May 2012.

[6] B. Karp and H. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in *Proceedings of ACM MobiCom*, pp. 243–254, 2000.

[7] M. Mejia and R. Chaparro-Vargas, "Distributed trust and reputation mechanisms for vehicular adhoc networks," *Vehicular Technologies - Deployment and Applications*, vol. 1, no. 6, pp. 6–10, Dec. 2013.

[8] P. Papadimitratos, L. Buttyan, J. P. Hubaux, F. Kargla, A. Kung, and M. Raya., "Architecture for secure and private vehicular communications," in *7th IEEE International Conference on ITS Telecommunications*, pp. 1–6, 2007.

[9] M. Pophali, S. Mohod, T. S. Yengantiwar, "Trust based opportunistic routing protocol for VANET communication," *International Journal Of Engineering And Computer Science*, vol. 3, no. 8, pp. 7408–7414, Aug. 2014.

[10] R. C. Poonia and V. Singh, "Performance evaluation of radio propagation model for vehicular ad hoc networks using vanetmobisim and NS-2," *International Journal of Distributed and Parallel Systems*, vol. 3, no. 4, July 2012.

[11] W. Qiwu, Q. Liu, L. Zhang, Z. Zhang, "A trusted routing protocol based on GeoDTN+Nav in VANET," *China Communications*, vol. 11, no. 14, pp. 166–174, 2014.

[12] M. Raya, P. Papadimitratos, and J. P. Hubaux, "Securing vehicular communications", *IEEE Wireless Communications*, vol. 13, no. 5, pp. 8–15, Oct. 2006.

[13] S. Tan, X. Li, and Q. Dong, "A trust management system for securing data plane of ad hoc networks," *IEEE Transactions on Vehicular Technology*, DOI: 10.1109/TVT.2015.2495325, 2015.

[14] J. Thangakumar, R. Mukesh, "Simulation of vehicular adhoc network routing protocols with the performance analysis," *Journal of Communication Software and Systems*, vol. 11, no. 2. pp. 86–93, June 2015.

[15] J. Thangakumar, R. Mukesh, "An optimized node selection routing protocol of vehicular adhoc networks - A hybrid model," *Journal of Communication Software and Systems*, vol. 11, no. 2. pp. 80–85, June 2015.

[16] J. Thangakumar, R. Mukesh, "An enhanced routing protocol of VANET using trust computing algorithms," *International Journal of Soft Computing*, vol. 11, no. 2. pp. 45–51, Jan. 2016.

[17] J. Thangakumar, R. Mukesh, "Mathematical analysis of trust routing algorithms," *Elsevier Procedia Computer Science Journal*, vol. 58, pp. 105–112, 2015.

[18] N. Yang, "A similarity based trust and reputation management framework for VANETs," *International Journal of Future Generation Communication and Networking*, vol. 6, no. 2, Apr. 2013.

[19] J. Zhang, "A survey on trust management for vanets," in *IEEE Advanced Information Networkingand Applications (AINA'11)*, pp. 105–112, 2011.

Thangakumar Jeyaprakash has received his B.E Degree in Electrical and Electronics Engineering from Dr.Sivanthi Aditanar College of Engineering, Tamilnadu in 2003. He obtained his M.Tech in Computer Science and Engineering, SRM University, Chennai. He is presently pursuing his Ph.D in Hindustan Institute of Technology and Science, Chennai, Tamilnadu, India. He has Eleven years of industrial, academic and research Experience. He is a member of IEEE, IET. His area of Interests is Mobile Ad hoc Networks, Vehicular Ad hoc Networks, Cryptography and Network Security, Data mining and software Engineering.

Rajeswari Mukesh has received her Ph.D. degree in Computer Science and Engineering from Jawaharlal Nehru University. Hyderabad. At present, she is a Professor and Head of Computer science and Engineering department at Hindustan University. She is guiding 8 PhD candidates. She has published more than 10 international journals and attended more than 15 international and National Conferences. Her area of specialization is Big Data, Biometrics, Adhoc Networks, Cyber Security. She is a Member of IEEE and IET. She has won the Women Engineer award recently from IET.