Indian J.Sci.Res. 17(2): 416-421, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

# AN EFFECTUAL TECHNIQUE BASED ON LOCATION BASED PATH ROUTING PROTOCOL FOR AODV PROTOCOL

[1]RadhikaThalla,[2]G.Rajeshwari,[3]Swapna A
[1,3] Department of Computer Science and Engineering,Vignana Jyothi Institute of Arts & Sciences, Secunderabad, Telangana.
[2] Department of Computer Science and Engineering, St. Francis College for Womens, Hyderabad,Telangana.

***Abstract-***A Mobile Ad hoc Network is an autonomous system of mobile stations connected by wireless link to form a network. It does not rely on predefined infrastructure to keep the network connected therefore it is also known as infrastructure less network. Trusted routing in MANET is a challenging task due to highly dynamic network topologies and openness of wire-less architecture. To provide secure routing among the Mobile Ad-hoc Networks (MANET) and to avoid selfish nodes and Selection Routing Protocol (Secure-SRP) of MANET has been designed based on trusted metrics using a Secured Computing Algorithm. The results stated that the E-SRP routing shows higher performance in security measures than the existing routing protocols.

***Keywords:*** Routing protocol, trust, MANET, vehicular ad-hoc networks

## I. Introduction

Mobile networks are utilized in disaster relief, conference and parcel environments, and received important attention in recent years [1,2,3].Many existing routing protocols (DSDV, OLSR, DSR, AODV, TORA) projected among the MANET social unit of IETF, are designed to scale in networks of a couple of hundred nodes. They consider state regarding all links within the network or links on a route between a supply and a destination. This might lead to poor scaling properties in larger mobile circumstantial networks. In additional recently, there has been a growing specialize in a category of routing algorithms that bank for the most part or fully, on location information.[2] This idea is to use the situations management messages, packet delay, to create simplified forwarding selections (GPSR).

The source uses the last far-famed destination location so as to estimate the zone during which the destination is predicted to be found. [7] This is used to determine a request zone, as a set of nodes that should forward route requests. GPSR use solely neighbour location data for forwarding knowledge packet to a neighbour nearer to the physical location of the destination. This native optimum alternative repeats at every intermediate node till the destination is reached.[6] AODV may be a reactive routing protocol, it minimizes the amount of broadcasts by making routes primarily based on demand.[4] Once any supply node desires to send a packet to a destination, it broadcasts a route request (RREQ) packet. The neighbouring nodes in flip broadcast the packet to their neighbour s and the method continues till the packet reaches the destination. It will increase the overhead as a result of the exaggerated quantity of management messages.

We proposed a routing protocol, referred to as dynamic routing, that aims at keeping the measurability edges of location-based routingwhereas addressing the two problems with irregular topology and node quality. We tend to conjointly found that our routing methodology will perform higher than the present AODV protocol we tend to compared it to, whereas addressing the two problems with irregular topology and node quality. We tend to conjointly found that our routing methodology will perform higher than the present AODV protocol we tend to compared it to. Dynamic routing

uses the subsequent ingredients to realize its goal. First, it combines a location-based routing methodology with a link state-based mechanism. Second, it uses a special variety of restricted search mode (Restricted Native Search, RNS). These first two ingredients solve problems due to the inaccuracy of location information, in particular for control packets. Third, it introduces the concept of anchors, which are geographical points imagined by sources for routing to specific destinations. This helps efficiently route around connectivity holes. An overview of dynamic routing is given in Section 2, and a detailed description in Sections 3 and in the form of protocol walkthrough. We tend to evaluate the performance of our protocol by elaborated simulations and its measurability by analysis in Section 4.In all cases, dynamic routing is characterized by low routing overhead, even when we include the overhead of location management

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

[1]Corresponding Author

complicated communications nodes, the ubiquity along the road be-comes 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 for the usability of MANET. 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.

## II. Related Works

Pophali et al. [9] proposed a trusted opportunistic routing protocol for MANET 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 pro-posed 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 in-stead of a reference given to a particular vehicle waiting for the reputation values.

Goudarzi et al. [1] presents a methodical literature re-view to provide complete and balanced material about various present trust conceptions in MANETs to upsurge excellence of data in transportation. The authors pro-posed a Trust model using the fuzzy logic to detect the misbehaviour nodes. The authors also stated that there is no lightweight intelligence trust model available for MANETs 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

Dynamic routing uses a combination of location-based routing (Dynamic Far (Remote) Routing, DFR), used when the destination is far, and link state routing (Dynamic Local Routing, DLR), used when the destination is close. DLR uses location independent addresses only. DFR uses a combination of direct paths, perimeter mode, and anchors, as described in the rest of this section. A direct path is an approximation of the straight line, and is built as follows: Assume that the source S knows an approximate location of the destination D. S sends the packet to a neighbour that brings the packet closer to the assumed location of D, and this is repeated by inter mediate nodes, as long as it works.

Dynamic routing uses a combination of location-based routing (Dynamic Far (Remote) Routing, DFR), used when the destination is far, and link state routing (Dynamic Local Routing, DLR), used when the destination is close. DLR uses location independent addresses only.

DFR uses a combination of direct paths, perimeter mode, and anchors, as described in the rest of this section. A direct path is an approximation of the straight line, and is built as follows: Assume that the source S knows an approximate location of the destination D. S sends the packet to a neighbour that brings the packet closer to the assumed location of D, and this is repeated by inter mediate nodes, as long as it works.

In HASBE [8], the user access rights were provided by the hierarchical access structure framed for each user ofthe system. This scheme ensures the property of scalability through the extension of ASBE (Attribute-Set Based Encryption) technique [6]. It defines a hierarchical structure that delegates the operation of trusted authority and private key generation to the domain authorities of the lower level. Here the user attributes were converted into the stable structure of the recursive type that permits the users to de ne constraints dynamically by representing a different combination of attributes, which satisfies the user access policy. That ensures the property of flexibility and ne-grained access control over HASBE systems. The concept of Hierarchical Based Access Structure is extended to form the Hierarchical Structure used in this paper.

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

### A. DLR

When a packet has arrived up to two hops away from the destination, a link state approach is used, which does not use location. In Fig. 1a, some intermediate node on the direct path finds that D is one or two hops away, using its DLR reach ability information (which is based on

permanent addresses, not location).The combination of DLR and DFR is able to keep the scalability benefits of location-based routing, while avoiding problems due to mobility. However, combining DLR and DRR in one protocol poses a number of design challenges (in particular, avoiding loops), which we Anchored paths, however, come at the price of computing good anchors. We propose two methods. They are always implemented at sources:

Friend Aided Path Discovery (FAPD, Section 3.1) assumes that some nodes (FAPD responders) are able to provide assistance to others, typically because they have a stable view of the network density.[4] FAPD responders help find anchors, but are not used in the data path.

Geographical Map-based Path Discovery (GMPD, Section 3.2) assumes that network density maps are available to a source node. This is for an ad hoc network where all nodes are individually mobile, but the node density can still be predicted a common assumption for car networks.[3] We find that GMPD performs better, but requires the overhead of map distribution; methods for distribution of density maps are left outside the scope of this paper.

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 behaviour nodes.

Rabayah et al. [2] proposed a routing protocol for MANET 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 proto-col in MANET 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.

## III. Proposed Work

### A)Trusted Routing

There are two different types of trust models: 1) Infra-structure 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 MANET has been proposed to avoid the selfish node behaviour of the Vehicular Adhoc Net-works which includes trust properties such as distance, direction, velocity and Trust value etc.

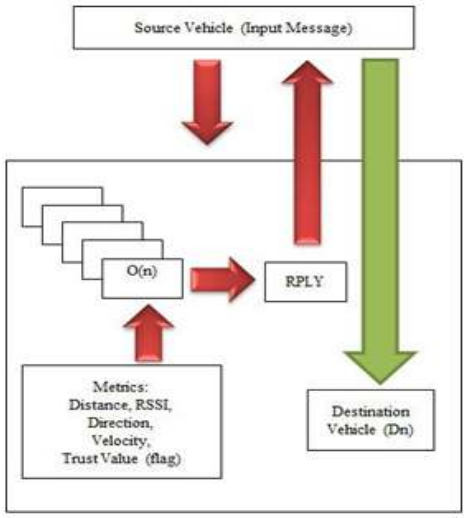


Figure 1: Architecture of ONSRP

Figure 1 shows the architecture of ONSRP. Many at-tacks can be identified to compromise them, if the security requirements have been established for MANETs. Here we described the types of attacks of MANET with the activity of these attacks and their potential consequences. From these attacks, the selfish node behaviour, characteristics and issues have been analysed. 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 Behaviour), availability in MANETs 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 theParticipating vehicles which ends in dropping all messages or just a few according to self-interests known as Selfish Behaviour.

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.

**B)Trust Metrics**

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

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.

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,

$$\text{Velocity}(V_o) = V(Dn)\,jj\,V(N1\,jj\,N2\,jj\,\ldots\,jj\,Nn); \quad (5)$$

whereDn = Destination node; N1 = Velocity of neighbour Node 1 of Dn; N2 = Velocity of neighbour Node 1 of Dn; N n = Velocity of neighbour Node 1 of Dn; V o = Optimized Velocity.

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

**C)Distance**

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

$$\text{Trustvalue} = Do{:}Ao{:}V\,o{:}\text{FlagTrustCount:} \quad (6)$$

**D)The Algorithm**

$$\text{Distance}(Do) = \text{Minimum}(D1\,jj\,D2\,jj\,\ldots\,jj\,Dn); \quad (1)$$

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.

$$RSSIPr[do] = \frac{CtP\,t}{d^4 P\,l} \quad (2)$$

$$RSST = \frac{}{p\,(X1\;X2)^2 + (Y\,1\;Y\,2)^2} \quad (3)$$

$$Dn =$$

**E)Direction**

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

At time T1, Direction in degrees

$$(Ao) = D(RW\,P\,(i;j))\,jj\,M\,in(D1\,jj\,D2\,jj\,\ldots\,jj\,Dn)(i;j); \quad (4)$$

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 neighbour nodes to find the possible route to the destination (See Algorithm 1).

Each node transmits the RREQ to the neighbour 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 proto-col algorithm. Otherwise, the RREQ will be discarded. When the RREQ arrives at the neighbour 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 behaviour in the Vehicular Adhoc Network.

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; RW P = Random way points in the network are; i; j = two successive random way points.

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 networkNo hurdles and infrastructures such as buildings etc. in the road topology.

## IV. 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 number of link failures.

In Figure 10, the total number of link failures has beenreduced by ignoring the selfish nodes available on the net-work. 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.

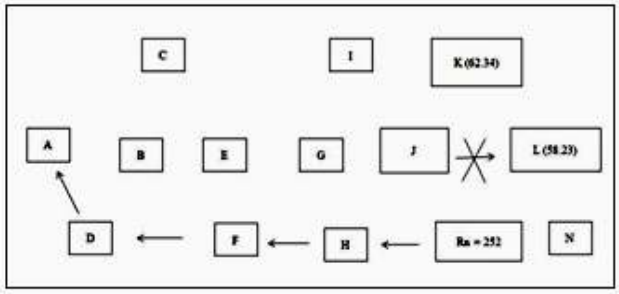


Figure 5: RRPLY sent to source node from node M

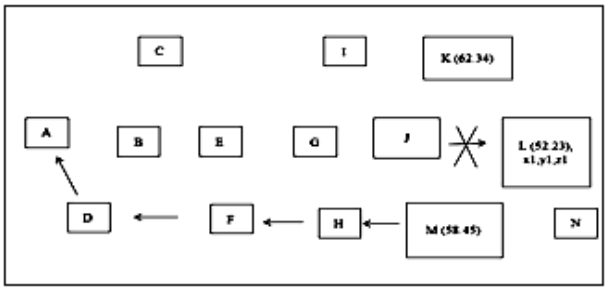


Figure 6: RPLY sent to source node via M

## V. Conclusion

An Optimized node selection routing protocol of MANET 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 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] InduKashyap& R.K. Rathy , ”An Efficient Location Based Multi-path Routing Protocol For MANET”, International Journal Of Computer Applications(0975-8887), Vol 40, No 9-Feb 2012.

[2] Neelesh Gupta and Roopam Gupta, ”Estimated New Routing Scheme in MANETs”, International Journal Of Computer Applications(0975-8887), Vol 17, No 5-Mar 2011.

[3] RaedAlsaqour, MohamadShanudin, Mahamod Ismail, and MahaAbdelhaq (2011) “Analysis Of Mobility Parameters Effect On Position

Information Inaccuracy Of Gpsr Position-Based Manet Routing Protocol", Journal of Theoretical and Applied Information Technology, Vol. 28 No.2, ISSN: 1992-8645.

[4] Nivedita, N. and Radhika, D. (2011) "Variable Range Energy Efficient Location Aided Routing For Manet", Computer Science & Information Technology, Vol 2, Issue 1 pp. 321–33.

[5] J. Li, J. Jannotti, D. De Couto, D. Karger, and R. Morris (2010) "A Scalable Location Service for Geographic Ad Hoc Routing", Proc.Mobicom '10.

[6] MahboobehAbdoos, KarimFaez, and MasoudSabaei, "Position Based Routing protocol with More Reiability in MANET", World Academy of Science, Engineering and Technology 25 2009.

[7] Charu Gandhi and Dr.ShuchitaUpadhyay, "Role Of Location Information To Achieve QOS Route Discovery In Ad hoc Networks-A Review", The Journal of Computer Science and Information Technology,

[8] ISSN 0973-4872, Vol. 6, No. 1, July-Dec. 2007 p.p. 63-68.http://ica1www.epfl.ch/TNRouting,Simulation Source Code of TerminodeRouting (in Glomosim) and Interactive Java applet, 2004.

[9] LjubicaBlazevic, Jean-Yves Le Boudec, and Silvia Giordano, "A location Based routing Method For Mobile Adhoc Networks", IEEE Transactions on Mobile Computing, Vol 3, No 4, Oct-dec2004.

[10] L. Blazevic, J.-Y. Le Boudec, and Silvia Giordano, "A Location Based Routing Method for Irregular Mobile Ad Hoc Networks, "Technical Report IC 200330, EPFL-DI-ICA, May 2003.