ISSN XXXX XXXX © 2016 IJESC

Research Article Volume 6 Issue No. 12

# Secure Routing Protocol for MANETs Using Requisite Trust-Based

Mr.Md.Shafiullah[1], Mr. Dadapeer[2], Mr.T.M.Hayath[3], Ms. Shenaz Begum[4]
Department of Computer Science and Engineering
Ballari Institute of Technology and Management, Ballari, Karnataka, India

**Abstract:**
A mobile ad-hoc network (MANET) is an infrastructure less network of mobile devices connected by wireless links. To secure a MANET in colluding nodes environment, the proposed work aims to detect and defend colluding nodes that causes internal attacks. In order to achieve this, the work focuses on the novel algorithm of trust computation and route detection that detects colluding nodes, without message and route redundancy during route discovery by using Requisite Trust based Secure Routing Protocol (RTSR). The trust will be calculated in local forwarding nodes, which are used to discover the route. The trust values from one hop neighbors are used to calculate the single trust value for each node using the constant normalization concept. Route discovery and trust information will be stored in fixed cluster head (CH). Piggybacking bit will reduce the broadcast storm problem.

## I. INTRODUCTION:

Placement of nodes in Wireless Sensor Network (WSNs) is often massive and random. Topology control algorithms focus in lowering the initial network topology, by reducing active nodes and links, thus saving resources and increasing network lifetime. Massive and random placement of sensor nodes on a monitored field renders node communication a difficult task to be achieved. Interference, congestion, and routing problems are possible to arise at any point in such networks. Routing challenges in WSNs stem from the unique characteristics of these networks, such as limited energy supply, limited computing power, and limited bandwidth on the wireless links, which impose severe restrictions on the design of efficient routing protocols. According to theory, a number of routing challenges and design issues like, among others, node placement and energy consumption, can affect routing process in WSNs. Thus, topology control, in conjunction with routing challenges, becomes an important issue that has to be carefully considered in order to achieve proper network operation. Generally, congestion control algorithms in WSNs employ two methods in order to control and avoid congestion. The first method is called traffic control and the second resource control. Algorithms that employ the traffic control method, adjust the rate with which sources inject traffic to the network in order to control congestion. On the other hand, resource control algorithms employ redundant nodes, which are not in the initial path from source to sink, in the process of forwarding data. Thus, algorithms that employ this method do not control the data rate of the sources but the paths though which the data flows. According to studies traffic control algorithms are not affected by different node placements, while according to the same studies resource control algorithms are significantly affected. Different node placements create a variable number of paths which are important for the proper operation of these algorithms. Placement of nodes in Wireless Sensor Network (WSNs) is often massive and random. Permitting all nodes to transmit concurrently without any control will result in high interference, high energy consumption, and reduced network lifetime.

## II. LITRATURE SURVEY:-

In the paper [1] titled *"Cluster based routing protocol"* the authors describe that Massive and random placement of sensor nodes on a monitored field renders node communication a difficult task to be achieved. Interference, congestion, and routing problems are possible to arise at any point in such networks. Routing challenges in WSNs stem from the unique characteristics of these networks, such as limited energy supply, limited computing power, and limited bandwidth on the wireless links, which impose severe restrictions on the design of efficient routing protocols. According to this paper, a number of routing challenges and design issues like, among others, node placement and energy consumption, can affect routing process in WSNs. Thus, topology control, in conjunction with routing challenges, becomes an important issue that has to be carefully considered in order to achieve proper network operation.

In the paper [2] titled *"A trust model based routing protocol for secure ad hoc networks"* the authors describe that congestion control algorithms in WSNs employ two methods in order to control and avoid congestion . The first method is called traffic control and the second resource control. Algorithms that employ the traffic control method, adjust the rate with which sources inject traffic to the network in order to control congestion. On the other hand, resource control algorithms employ redundant nodes, which are not in the initial path from source to sink, in the process of forwarding data. Thus, algorithms that employ this method do not control the data rate of the sources but the paths though which the data flows.

In the paper [3] titled *"Active Trust Transmission Mechanism for Wireless Sensor Networ/C'* the authors describe that According to papers, traffic control algorithms are not affected by different node placements, while according to the same studies resource control algorithms are significantly affected. Different node placements create a variable number of paths which are important for the proper operation of these algorithms.

In the paper [4] titled *"A survey on tnlst managementfor mobile ad-hoc networks"* the authors describe that, generally two methods exists with which algorithm designers attempt to control congestion in WSNs. The first method is called "traffic control". Algorithms that employ the traffic control method, adjust the traffic that is injected to the network by the different sources, in order to cope with the capacity of the currently employed paths. Thus, the rate of the sources is reduced until congestion is alleviated. This method presents similarities with the traditional congestion control algorithms in wired networks and it has also been adopted by the large number of congestion control algorithms in WSNs.

In the paper [9] titled *for.A secure routing protocol against byzantine attacks for MANETs in adversarial environments"* the authors, the second method is called "resource control". This method, the network takes advantage of the redundant deployment of sensor nodes in the field and employs the resources (buffer, power) of nodes that do not participate in the initial routing paths to forward data through them. Thus, sources do not reduce the rate with which they inject packets in the network and excess packets are forwarded through alternative or multiple paths.

In the paper [4] titled *fo'A survey on trust Inanagement.for mobile ad-hoc networks"* the authors, has shown that traffic control algorithms are not significantly affected by different node placements. On the other hand resource control algorithms are affected by different placements. We believe that properly employed topology control algorithms are able to provide additional benefits to resource control algorithms. Source based routing trees provide numerous alternative paths, in comparison with sink-based trees, which, if carefully selected, can increase the performance of such algorithms.

**Proposed System:**

In the current approach all the nodes are divided into the level based structure due to which the propagation time reduces and always a unique node will be picked while discovery the route from source node to destination node. This approach will reduce the number of hops, will reduce round trip time and also reduces the power consumed because of which the no of packets delivered will be more as compared to previous approach.

**1.5 System Architecture**

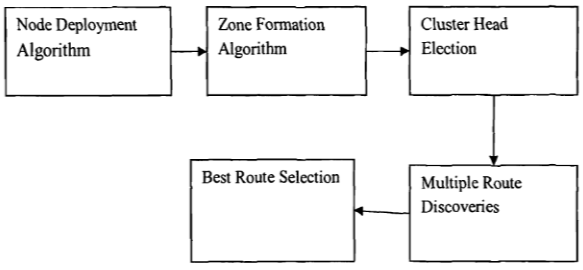

**Fig 1.1 System Architecture**

**Figure .1.1 shows the system architecture diagram for the Requisite Trust Based routing algorithm.**

1. Node Deployment AlgorithM is responsible for deployment of nodes in a particular area.

2. Zone Formation Algorithm divides the entire are into multiple zones. Each Zone having a set of nodes in its zone. This is the algorithm which is responsible for deploying the nodes. The entire area is divided into zones with each zone Reqisite bounded with the limits with some xmin and xmax. The y region is bounded within the limits ymin and ymax. Each zone is allocated a set of nodes.

3. Cluster Head Election algorithm is used to elect the zone leader by computing distance value.The distance value is computed per zone for all nodes and whichever node has minimum value of distance becomes the zone leader.

4. Multiple Route Discovery is used to find multiple routes from source node to destination node

5. Best Route Selection algorithm is responsible for selecting the best route which has the maximum trust.

## III. IMPLEMENTATION:-

Here we are addressing various protocols used by the underlying system. Artificial Hierarchical Partitioned Structure of Network In this algorithm, the network processes are partitioned according to an Artificial hierarchical structure with the sole purpose of reducing the number of entries in the routing tables. The *process and nodes* represent the same. Consider a network where the processes are partitioned into m regions. The processes in each region in turn partitioned into n districts. Each district has r processes. In this network each region i and each district j is connected in the following sense:
a. For each of two processes p and q in region i, there is a sequence of processes p.0,p.l ..... p.r such that p is p.0 and q is p.r and for every k,O :s k < r, p.k & p.k+ 1
are nhbrs in the region.
b. For each of the two processes p and q in district j , there is a sequenc of processes
p.0, ... p.s such that p is p.0 and q is p.s and for each k, 0 :s k < s, p.k and p.k+ I
are nhbrs in district j.
Each process in this network is uniquely identified by three identifiers i, j and k. I indicates the region to which process belongs, j indicates the district in region i, to which
process belongs and k indicates the process in district j in region i

- **Conceptual Methodology of Hierarchical Algorithm**

1. The processes in this artificial hierarchical partitioned network constitute a process array with three indices as follows: process p[i:O .. m-l,j:O .. n-l, k:O .. r-l]

2. In this network, when a data message is to be sent, the three identifier of its destination process are attached to the message before the message is sent.

3. When a data(x, y, z) message arrives at the process, the process uses its routing table and the triple (x, y, z), which detennines the message destination to detennine the best neighbor to which message is forwarded.

4. The routing table of each process p[i, j, k] consists of three arrays named rgn, dstr and prs.

5. Array rgn detennines the best for reaching a destination process whose region is other than i.

6. Array dstr detennines the best nhbr for reaching a destination process whose region is i, but whose district is other than j.

7. Array prs determines the best nhbr for reaching a destination process whose region is i, & whose district is j but the process is other than p[i, j, k] itself.

- **RTMSG (Route the Message Algorithm)**

The RTMSG algorithm is the part of Hierarchical algorithm

1. When the destination node is *not in the same region* (i.e x not equal to i) and the link is *up* then the packet is sent directly to some node in the corresponding region.

2. When the destination node is *not in the same region(* i.e x not equal to i) and the link is *down* then the packet cannot be send.

3. When the destination node is *in the same region* (i.e x = i ) and node is *not in the same district* (i.e y is not equal to j) and the link is *up* then the packet is sent directly to the some node in the corresponding district.

4. When the destination node is *in the same region* (i.e x = i) and node is *not in the same district* ( i.e. y is not equal to j ) the link is *down* then the packet cannot be send.

5. When the destination node is in the *same region* (i.e x=i) and *same district* (i.e y=j) and the *destination node is different* ( i.e z is not equal to k) and the *link is Up* then the packet is send to the destination node .

6. When the destination node is in the *same region* (i.e x=i) and *same district* (i.e y=j) and the *destination node is different* ( i.e z is not equal to k) and the *link isDown* then the packet cannot be send.

7. When the destination node is in the *same region* (i.e x=i) and *same district* (i.e y=j) and the *destination node is reached* ( i.e z = k) and then the packet has reached the destination.

- **Trust Computation Algorithms**

Trust computation algorithm is used to compute the trust level of the individual nodes.The following are the 3 algorithms
a. Bayesian Method
b. Eigen Method
c. Dumpsters Rule of Combination

### a. Bayesian Method

Identifying the neighbor nodes and gathers reputation locally then that reputation is used to evaluate the local nodes. This method supports to calculate the local trust value, rather than global trust value. Hence it requires minimum storage and is easier for data retrieval.

### b.Eigen Method

Eigen method is used to calculate the normalized local trust and aggregate the local trust value as global trust values. These are used to reduce the inauthentic nodes in the network. If the trust is the negative, it will be isolated from the network. This aggregating reputation trust system is called *Eigen Trust.*

**C.Dumpster Rule of Combination** The combination rule is used to ignore the conflicting evidence by nonnalizing the multiple sources. The normalization factor is needed to handle the multiple resources. The novelty is applying the rule in colluding node scenario in different perspectives. Each node's trust value will broadcast to the network while packet transmission to the appropriate nodes. A cover set is nothing but a forward node's one hop neighbor set. The forward node forwards the local trust of each node to cluster head and the fixed cluster head computes the global trust of every node.

## IV.CONCLUSION

Security is the major challenge in MANET. One of the promising mechanisms to secure the network is by adopting the idea of trust model that avoids centralized units (trusted third parties) to issue digital signature. This method avoids large overheads and influences the self-organizing nature of MANET. This study deals with the problem of designing trust based mechanism in an efficient cluster architecture RTSR protocol, has proposed the colluding nodes detection and defense mechanism by using both cluster-based approach and trust-based route discovery through every node in a MANET. The route redundancy and message redundancy will be reduced by broadcasting the packets. Using piggybacking bit for trusts the lesser bandwidth consumption will be maintained and the broadcast storm problem will be reduced .The future work is, the regional cluster will be extended as hexagonal and more than one cluster form. So the trust values get changed as global trusts and global trust will causes trust decay over time and trust delay. These will be maintained through cluster heads and the route discovery can also be magnified from those extensions.

## V. REFERENCES

[1]. J. Broth, D.A. Maltz, D . B. Johnson, Y.C. H u, and J. Jetcheva. "A perfonnance comparison of multi - hop wireless ad-hoc network routing protocols" *in Proc., MOBICOM'* 98,1998, pp. 85-97.

[2]. Haidar Safa , Hassan Artail & Diana Tabet ,"A cluster-based trustaware routing protocol for mobile ad hoc networks", *Springer Link*, vol. 16, pp. 969-984, May. 2010.

[3]. M. Jiang, J. Li & Y.C. Tay ,"Cluster based routing protocol"{ cbrp).Intemet Draft, MANET working group, August 1999.

[4]. Jin-Hee Cho, A. Swalni and lng-Ray Chen ;" A survey on trust management for mobile ad-hoc networks", in Proc., IEEE conference, 2010, vol. 13, pp. 562-583.

[5]. Kari Sentz,"Combination of Evidence in Dempster-Shafer Theory", *Computer and Information Science journal* ,vol. 853, pp.37- 72, 2002.

[6]. X. Li, M.R. Lyu & J. Liu, "A trust model based routing protocol for secure ad hoc networks" in Proc., *IEEE aerospace conference* , vol. 2, pp. 1286--1295, March
2004.

[7]. H. Lim and C. Kim, "Flooding in wireless ad hoc networks", *Computer Communications Joumal*, vo1.24, no.3-4, pp. 353- 363, 2001.

[8]. Ni. S, Y. Tseng, Y. Chen, and J. Sheu, "The broadcast stonn problem in a mobile ad hoc network '" in Proc., *ACMIIEEE MOBICOM'99* 1999 paper 11, pp. 151-· 162.

[9]. Ming yu, Mengchu zhou and Wei su, "A secure routing protocol against byzantine attacks for MANETs in adversarial environments", *in Proc., IEEE transactions*, vol. 58, no. 1, pp. 449-459 , 2009 .

[10]. S.Neelavathy Pari and D.Sridharan , "Mitigating routing misbehavior in selforganizing mobile ad hoc network using K neighborhood local reputation system", in Proc., *IEEE ICRTIT'11,* 2011 pp. 313-317.

[11]. A. Pirzada & C. McDonald, "Establishing trust in pure ad-hoc networks", in Proc.,ofthe 27th Australian *conference on computer science(ACSC'04)* 2004, vol. 26,pp.41-46.