# SECURITY BASED SERVICE INFRASTRUCTURE FOR WIRELESS ADHOC NETWORKS USING FUZZY LOGIC

Dr.J.Preetha
*Department of Computer Science and Engineering*
*Muthayammal Engineering College, Rasipuram, Tamil Nadu, India*
psgpreeetha@gmail.com

Dr.S.Lavanya
*Department of Computer Science and Engineering*
*Muthayammal Engineering College, Rasipuram, Tamil Nadu, India*
lavanyasharvesh@gmail.com

**Abstract- MANET is a gathering of versatile nodes that are shaped progressively by an independent framework and corresponds with one another with no supporting base. These systems are helpless against various security dangers because of their open nature, absence of framework, node portability and physical security of the nodes. Henceforth planning a protected direction has turned into a well-known examination point. For example, BeeAdHoc have been offered for creating directing calculations for MANETs. In this paper, the security vulnerabilities of BeeAdHoc are examined and after that a security structure, FBeeAd-Hoc is framed, which uses a set hypothesis and computerized mark is proposed. The structure has the capacity to minimize the dangers and accomplishes better execution with higher security features and higher availability .To achieve better performance we route the data based on MPLS(multi-protocol label switching) technology which ensures constant rate of data flow even when there exists security threats. so a high level of Qos is attained.**

**Keywords: MANET, BeeAdhoc, FBeeadhoc, Multi Protocol Label switching**.

## 1. INTRODUCTION

MANETs that are connected by means of remote connections without utilizing a settled infrastructure and built up as a part of any environment which is required . These net-works are a type of remote systems which nodes communicate to others specifically or in a round robin way . Every node has a restricted Trans-mission range. All nodes convey specifically in the transmission range of one another. Something else, the correspondence between them has to depend on alternate nodes for connectivity. The dependability in this network are conveyed between the nodes and every node additionally plays the part of a switch for packets bound for the other nodes. The system topology of MANETs can change much of the time, subsequent to each node has the capacity move freely in any bearing. MANETs have increased real consideration as of late and they are valuable in numerous application situations, for example, territories where earthquakes or other normal catastrophes have decimated communication foundations, front line, calamity administration thus on. One of the primary difficulties in MANETs is the means by which to route data packets over the system. Directing conventions relying upon how the source discovers a route to the destination are grouped into three categories: proactive, receptive and cross breed. In proactive protocols, nodes keep up accessible routes in the steering table. At whatever point a node needs a route to a particular destination, it can focus a proper route by dynamic routing protocols.

## I. RELATED WORK

AODV [2] is a routing protocol with the resource constraints and dynamic specification of MANET. It works on need basis, which means a route is discovered when needed and routes are retained as long as they are needed to transfer data. The construction of routes uses network wide redundant message flooding of route request and route reply which may cause considerable energy drain. We have addressed the issue of attacks from intruders by authentication technologies that rely on mutual trust between nodes.[3] We have observed the performance of the network with and without our secured routing scheme. Our scheme ensures better performance on analysis.[7] Bee

Ad Hoc, for MANETs. A honey bee colony has many features that are desirable in MANETs: efficient allocation of foraging force to multiple food sources, different type of foragers for each commodity, foragers evaluate the standard of visited food sources and then recruit optimum number of foragers for their food source inside the hive, no centralized control and foragers try to optimize the energetic efficiency of nectar collection and foragers take resolutions without any global knowledge of the environment.DSR (Dynamic Source Routing) is a reactive source routing algorithm while AODV (Ad-Hoc On- demand Distance Vector Routing) is a reactive next hop routing algorithm. The algorithms DSR or AODV as an underlying route discovery and maintenance mechanism, and then use energy as a cost metric for routing. The success of Bee Hive motivated us to take the foraging principles of bees as an inspiration for designing our new security framework Bee Ad-hoc protocol.

## II. BEEADHOC AND ITS VULNERABILITIES

Bee Ad-Hoc is a responsive source steering calculation with compelling vitality for directing in MANETs, which has been roused from honey bee practices. It utilizes two sorts of operators; scouts to find new routes and foragers to transport information from source to destination. At the point when a node is required to send information to a specific destination, the forward scout is telecast on the system. The moderate nodes that get the scout, add their locations in the source route of the scout until it touches base at the destination. At the point when a forward scout came to on the destination, a regressive scout is sent back to the source node utilizing connection inversion. When a scout comes back to its source node, it promotes the route to different foragers and after that foragers transport information to the destination node. On their excursion, they gather the data about the system state and assess the nature of the crossed way.

### *A. Security Risk Analysis*

The security risk investigation of Bee Ad-Hoc has demonstrated that a vindictive node could dispatch various assaults which upset the typical steering conduct. We portray an assaults couple here Scout related assaults: Scouts find new routes from source to destination node. A noxious node can alter the source route in a scout; additionally it can produce a scout by ridiculing the source address or embedding fake scout ID, or both. Forager route related assaults: Foragers execute the primary working Bee Ad-Hoc calculation. They convey information packets in their pay-stack and are transmitted as uni-cast data. A noxious node can alter the forager's source route or dispatch a manufactured forager with mock source address and source route toward the destination.- Forager route data related assaults: A vindictive node can adjust the directing data, conveyed by foragers, to expand the nature of a way spuriously. Therefore, the likelihood of sending more information would increment on a low quality route.- Consequently altered or produced honey bee operators, scout and forager, result in building up fake routes, which upsetting the normal routing conduct and diminish the system's execution.

## III. DETERMINING TRUST FROM FUZZY RULE

In this area, at first fuzzy rationale is clarified and afterwards the fuzzy rationale weighted multi-criteria are portrayed for allocating trust quality to every node. Trust is a relationship between two neighbor nodes. Our proposed structure assesses node trust and route trust. The node trust implies the node quality and gave administrations to transmit data, while route trust is nature of route.

### A. Fuzzy Logic

Fuzzy Logic, is a multi-esteemed rationale that permits halfway values to be characterized between conventional assessments like genuine/false, yes/no, and so on. Ideas like rather tall or quick can be planned scientifically and processed by PCs, keeping in mind the end goal to apply a more human-like way of deduction in PC programming Fuzzy rationale (FL) is practically synonymous with the hypothesis of fuzzy sets, a hypothesis which identifies with classes of items with unsharp boundaries in which participation is a matter of degree .Some of the fundamental ideas in the hypothesis of fluffy sets are: fuzzy set, enrolment capacity and if-then principles. Fluffy rationale begins with the idea of a fluffy set. A fluffy set is a set without a crisp, clear characterized limit. It can contain components with just a standard trial level of participation. An enrolment capacity (MF) is a curve that characterizes how every point in the information space is mapped to a membership worth (or level of participation) somewhere around 0 and 1. On the off chance that then rule proclamations are utilized to figure the contingent statements that include fluffy rationale. The fluffy methodology requires an adequate master information for the plan of the tenet base, the sets mix and the defuzzification. In General, the applying of fluffy rationale may be helpful, for exceptionally complex procedures, when there is no straightforward mathematical model, for exceedingly nonlinear procedures or if the procedure of expert learning is to be performed

### B. Trust Computation

In this model, in time t, TV (t) alludes to the node's trust, which is a genuine number in the interim The trust esteem "0" is to distrust and "1"represents total trust in a specific node. Let vi and vj show the assessing and assessed nodes.

#### *1)* Node Trust Computation

This methodology for processing node's trust utilized three criteria under the fluffy environment. Considered criteria are: parcel for-warding proportion, data transfer capacity and vitality utilization, which packet sending proportion utilized for evaluation of sending practices of neighbors by a sender and vitality utilization and data transfer capacity are node's ability level to give the parcel transmission services. We characterize the enrolment capacities relating to every paradigm in the semantic set. The criteria rating can be evaluated by phonetic terms, for example, low (VL), low (L), medium (M), high (H)and high (VH) . In fact, the data variables is the first stride of the fluffy surmising procedure. This stride decides the extent to which include variables have a place with each of the proper fluffy sets by means of enrolment capacities. Information variables that are fresh numerical worth, guide to a fluffy level of enrolment in the qualifying semantic set, where in the proposed approach we utilize etymological terms, for example, Very Low (VL), Low (L), Medium (M), High(H) and Very High (VH), there is a cover in the scale quality doled out to VL and L, L and M, M and H and H and VH. Truth be told, when we show a fluffy depiction of criteria, for example, vitality, we characterize the fluffy set. Vitality level may be having a place with one or more fluffy set; yet the level of participation of a sure vitality level in this interim, in every set is diverse.

Sending proportion is the number's extent of forwarded accurately to the aggregate number of packets sent. Right sending means a sending node transmits to its next bounce node earnestly. Along these lines, if a pernicious node adjusts or produces the packet, it is not considered as right sending. At time t, FR(t)is figured as takes after:

$$FR(t) = Ncor(t) / Nall(t) \quad (1)$$

Where Ncor(t) and Nall(t) speak to the quantity of correct forwarding the aggregate number of packets sent from time 0 to t, individually. Since the packets in MANETs arranged into control packets and data, FR isolated in control packet sending proportion, appeared as CFR, and data sending proportion, appeared as DFR. Consequently sending of node vj assessed by node vi by means of taking after mathematical statement:

$$\mathbf{t}v\mathbf{frij(t) = w1 * CFRij(t) + w2 * DFRij(t)}$$

where w1and w2 are assigned weights to CFRij(t) and DFRij(t),respectively at time t. At the point when a node transmits control data, it places itself in promiscuous mode to check the retransmission by the sending node. Utilizing this strategy, the sender screens the packet is sent effectively or not. For a telecast parcel, a sender builds Nall for control packets of every one of its neighbors before sending data by 1 except the node where the parcel originates from. In any case, for a unicast packet, the sender just builds Nall for control packets or Nall for information parcels of next jump by 1. On the off chance that the parcel is sent effectively by sending node, the sender adds 1. If the pernicious neighbor node changes the packet wrongfully, its sending proportion will diminish. At the point when the rating of trust quality communicated will be low .The trust level of every node can be computed by the following equation: $Tv(i) = wf*tvfr(i) + wb* BW(i) + we * E(i)$ $wf + wb + we = 1$

#### 2. Route Trust Computation

As respects the trust estimation of the route ought not be more prominent than the trust estimations of middle nodes, at time t, the route trust is figured by the accompanying mathematical statement:

$$\mathbf{RouteT}v\mathbf{sd(t)} = \pi(\{\mathbf{TVij(t)}|v\mathbf{i}, v\mathbf{j} \in \mathbf{P\ and\ }v\mathbf{i} \rightarrow v\mathbf{j}\})$$

where vs and vd are the source node and the destination node of route P, respectively, vi and vj are two adjacent nodes and vi→ vj means that vj is the next-hop node of vi. Indeed the route trust is the account trust values of all intermediate nodes .

## IV. A SECURITY FRAMEWORK FOR BEEADHOC PROTOCOL

In this area, security structure for Bee Ad-Hoc which is outlined in light of fuzzy set hypothesis and advanced mark is represented.

A. Scout and Forager authentication

When a source node has information to send to the destination, it first checks its move floor to determine a forager for an information parcel. In the event that it find some, then it utilizes the complete source route as a part of forager for information packet transmissions. Else, it telecasts a forward scout to all its neighbors for finding new routes to the destination node. This forward scout contains source ID, destination ID, source route and TVs added by the middle of the road nodes along the route. After the transmission of any forward scout, the sender places itself in promiscuous mode and figures the trust estimation of assessed nodes by using the methodology portrayed above. When a node gets a forward scout, it can affirm that the forward scout not been adjusted by a pernicious node with the help of the rundown of node TVs. It affixes its location in the source route and TV acquired from the upstream node on the route to the for-ward scout and retransmits it. At the point when a forward scout came to the destination, it contains the rundown of nodes and TVs of each hop along the route. The destination node figures Route TvP for the route P by utilizing equation . This worth used to choose the best route when more than one route is found and they have the equal hop check.

At that point the destination node unicast the retrogressive scout back to the source node and subsequent to transmitting figures the trust value of assessed node. Once the regressive scout is gotten by the source node, it can verify that the retrogressive scout have not altered by a malicious node by utilizing the rundown of node TVs. At that point, it enroll the foragers for transport information to the destination node. Essentially, after the transmission of forager, every node, figures the trust estimation of evaluated node. In this methodology, to secure the directing data discovered by forager along the highway, a sending node uses a computerized signature that processes an authentication

$$\textbf{AuthRIi = sign(H(routing information), keyPi)}$$

A accepting node analyses the verification process to ensure the reliability of routing data, Verify

$$(\textbf{AuthRIi , H(routing information), keyUi)}$$

In which, H(M) represents hash of message M and key Pi and key Ui represent private key and public key of node i. Algorithm shows security for foragers

***Algorithm (1): Security for forward scouts***

```
        for all (FS launched from S to D)
            do
               if (FS broadcast from nodei) then compute TV
                 for all neighbors by nodeistore TV in neighbor table of nodei
                      else if (FS received at nodei) then verify TV value
               if (TVFSfails) then
                       drop FS and exit
               end if
                 if(nodei/= D for FS) then
                   append address of nodei in the source route append TV obtained
                       from the upstream node on the route to the LTV
                       pas FS to entrance for re-broadcasting
                         else
                           pass FS to entrance to convert to BS
   end if
     end if
         end
```

Algorithm (2): Security for backward scouts for all

```
   (BS returning from D to S) do

        if(BS unicast from nodeito nodei+1) then

                     if (nodei= = D for BS) then compute RouteTvP

                        for the route PstoreRouteTvP in the BS
```

```
            end if
              if (nodei/= S for BS) then compute TV of nodei+1append TV to the LTV
             end if
                        else if (BS received at node) then verify TV value
                              if(TVBSfails) then drop BS and exit
             end if
     if (nodei= = S for BS) then

   verify TV value      if(TVBSfails)

    then drop BS and exit elsepass

     BS  for entry in dance floor

   end if
  end if
 end if
```

**Algorithm (3): Security for foragers**

```
for all (F going from S to D) do
       if (F unicast from nodeito nodei+1) then compute TV
               for nodei+1 by nodei store route information compute and store AuthRIisend F to next hop
       else if (F received at nodei) then verify TV value
           if (TVFfails) then drop F and exit
               end if verify AuthRIiif (AuthRIifails) thendrop F and exit
       end ifpass F and send F to next hop
  end
```

VI Graphical analysis:

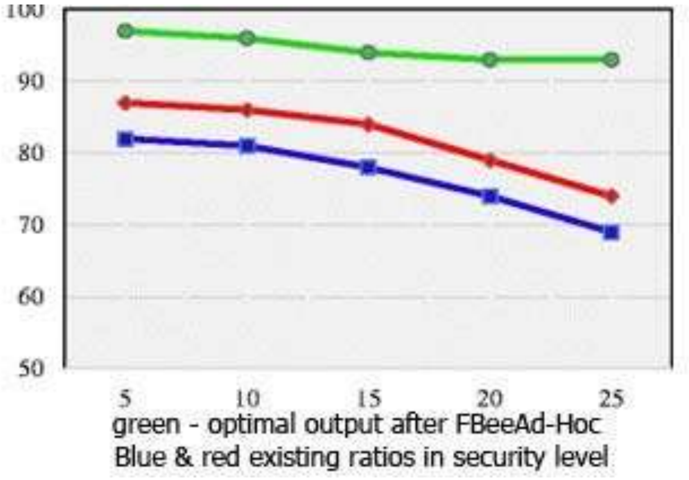

***Fig 5.1 Green – optimal output after FBeedAdhoc Blue  and Red existing ratios in security level***

IV.CONCLUSION

In this paper, at first security vulnerabilities of BeeAdHoc is examined. In this convention a hub has the capacity to dispatch various assaults and upset typical conduct of the convention. At that point, a safe structure for BeeAdHoc is proposed which is planned taking into account fluffy set hypothesis and computerized signatures. Moreover, the system execution of expert postured secure system, FBee Ad-Hoc, is around the same as compared to non-secure Bee Ad-Hoc and superior to anything AODV. FBee Ad-Hoc can be further be upgraded by streamlining of fuzzy membership capacity by advancement calculations, for example, particle swarm improvement (PSO), furthermore discovery of childish hubs in the system by utilizing Swarm Intelligence

REFERENCES

[1] B. Corona, M. Nakano, H. Pérez, “Adaptive Watermarking Algorithm for Binary Image Watermarks”, *Lecture Notes in Computer Science, Springer, pp. 207-215, 2004*.

[2] A. A. Reddy and B. N. Chatterji, "A new wavelet based logo-watermarking scheme," Pattern Recognition Letters, vol. 26, pp. 1019-1027, 2005.

[3] P. S. Huang, C. S. Chiang, C. P. Chang, and T. M. Tu, "Robust spatial watermarking technique for colour images via direct saturation adjustment," Vision, Image and Signal Processing, IEE Proceedings -, vol. 152, pp. 561-574, 2005.

[4] F. Gonzalez and J. Hernandez, " A tutorial on Digital Watermarking ", In IEEE annual Carnahan conference on security technology, Spain, 1999.

[5] D. Kunder, "Multi-resolution Digital Watermarking Algorithms and Implications for Multimedia Signals", Ph.D. thesis, university of Toronto, Canada, 2001.

[6] J. Eggers, J. Su and B. Girod," Robustness of a Blind Image Watermarking Scheme", Proc. IEEE Int. Conf. on Image Proc., Vancouver, 2000.

[7] Barni M., Bartolini F., Piva A., Multichannel watermarking of color images, IEEE Transaction on Circuits and Systems of Video Technology 12(3) (2002) 142-156.

[8] Kundur D., Hatzinakos D., Towards robust logo watermarking using multiresolution image fusion, IEEE Transcations on Multimedia 6 (2004) 185-197.

[9] C.S. Lu, H.Y.M Liao, “Multipurpose watermarking for image authentication and protection,” *IEEE Transaction on Image Processing*, vol. 10, pp. 1579-1592, Oct. 2001.

[10] L. Ghouti, A. Bouridane, M.K. Ibrahim, and S. Boussakta, “Digital image watermarking using balanced multiwavelets”, *IEEE Trans. Signal Process*., 2006, Vol. 54, No. 4, pp. 1519-1536.

[11] P. Tay and J. Havlicek, "Image Watermarking Using Wavelets", in *Proceedings of the 2002 IEEE*, pp. II.258 – II.261, 2002.

[12] P. Kumswat, Ki. Attakitmongcol and A. Striaew, "A New Approach for Optimization in Image Watermarking by Using Genetic Algorithms", *IEEE Transactions on Signal Processing*, Vol. 53, No. 12, pp. 4707-4719, December, 2005.

[13] H. Daren, L. Jifuen,H. Jiwu, and L. Hongmei, "A DWT-Based Image Watermarking Algorithm", in *Proceedings of the IEEE International Conference on Multimedia and Expo*, pp. 429-432, 2001.

[14] C. Hsu and J. Wu, "Multi-resolution Watermarking for Digital Images", *IEEE Transactions on Circuits and Systems- II*, Vol. 45, No. 8, pp. 1097-1101, August 1998.

[15] R. Mehul, "Discrete Wavelet Transform Based Multiple Watermarking Scheme", in *Proceedings of the 2003 IEEE TENCON*, pp. 935-938, 2003.