A Secure Dominating set based routing and key management scheme in Mobile Ad hoc Network

R.PUSHPALAKSHMI, A.VINCENT ANTONY KUMAR
Department of Information Technology
PSNA College of Engineering & Technology
Dindigul, Tamilnadu
INDIA
pushparaman@rediffmail.com

Abstract: - In Mobile Ad hoc Network (MANET) nodes communicate with each other using shared wireless medium. Due to their distributed nature and dynamic topology, MANET is less secured than wired network. To enhance the security of MANET, it is important to establish routing path based on the trustworthiness of each node in the network. Most existing routing protocols in MANET mainly focus at finding efficient routing path. To deal with the effect of malicious node, trustworthiness of node can be taken into consideration in routing decision making. A routing protocol based on distributed dominating set based clustering algorithm is presented in this paper. The dominator set is formed based on the trust ability of the node and probability of future contact of the node in the network. This paper present a adaptive neuro fuzzy logic controller to evaluate the trust level of each node and a composite key management technique used for effective key management within cluster. Simulation results show that proposed routing protocol provides efficient routing path that bypass malicious nodes in the network.

Key-Words: - Mobile Ad hoc network, dominating set, fuzzy controller, trust valuation, key management, secure routing.

1 Introduction

As Mobile ad hoc network (MANET) is self organizing and adaptive network without any pre-existing infrastructure. The topology of ad hoc network is dynamic in nature due to mobile nodes. The mobile nodes that are in transmission range of each other can communicate directly, whereas other nodes communicate through intermediate nodes. No dedicated routers are necessary in ad hoc network. Each node in the network is free to move independently and change its links to other nodes frequently. Without the need of any centralized administration the nodes communicate wirelessly and share the same media. The nodes in a MANET rely on batteries for their energy.

Ad hoc network is network without any fixed infrastructure and the network can be set up at any place and time. It is highly desirable for applications where network must be built quickly or network not possible to deploy e.g. military systems, and disaster relief operations. The dynamic nature of mobile nodes causes frequent route change. Due to lack of centralized administration any malicious node can join the network at any time. It is hard to detect malicious node in the network. Hence MANET is much more vulnerable to attack than wired network. To increase the level of security, the packets must be routed across the nodes that are trustable.

Routing in MANET depends on factors including topology, node characteristics and link characteristics. MANET routing protocols are basically classified into topology based approach, location based approach and power aware approach. Routing in topology based approach is mainly based on node and link connectivity of network. It includes proactive routing protocol, reactive routing protocol and hybrid routing protocol.

In proactive routing protocol, each node maintains route information to all other nodes in the network by periodically distributing routing tables throughout the network. The main disadvantage of these protocols is that the overhead involved in maintaining routing table increases with network size. In reactive or on demand routing protocol, the route is established only on demand. The main drawback in this approach is additional delay incurred in route finding.

Cluster based routing protocol is an on demand routing protocol, where the nodes are divided into clusters. Each cluster includes a cluster head (CH), cluster members and gateway nodes. The CH is elected for each cluster to maintain cluster membership information. The CH maintains its cluster member's information and information about neighboring CHs. Assume node S has data to send node D. Node S send route request to its CH. The CH checks for node D in its member table. If D exists in same cluster, the request is routed directly to node D. Else CH sends the route request to all the nearby CHs. Inter cluster communication is carried out through virtual path established between the CHs. The main advantage of clustering approach is reduced flooding traffic during the dynamic route discovery process. It uses local route repair mechanism to handle broken links.

Dominating sets are widely used in clustering the network. Network is modeled as a graph G= (V, E), where V represent nodes in the network and E represent the connectivity between the nodes. A Dominating Set (DS) of G is subset of nodes such that each node in G is either in DS or has a neighbor in DS. A Connected Dominating Set (CDS) is a dominating set which induces a connected sub graph. Minimum Connected Dominating Set (MCDS) is a connected dominating set with minimum cardinality.

Algorithms that construct a CDS can be divided into two categories: centralized algorithms and decentralized algorithms. In centralized algorithm, all the nodes in the network must know the complete network topology. Cluster based algorithm is one of the decentralized algorithm. It contains two phases. In the first phase, the network is partitioned into clusters and CH is elected for each cluster. In the second phase, a virtual backbone that connects CHs is established.

In this paper we propose a distributed cluster based algorithm to construct a CDS. Several clustering algorithms have been proposed to elect CH that has maximum id, maximum node degree, and maximum residual energy. Ad hoc network is less secured than wired network due to wireless media, and lack of central control. In our proposal to increase the level of security the packets are routed only through more trustable nodes in the network. An adaptive neuro fuzzy logic controller is used to evaluate the trust ability of each node in the network.

A neuro fuzzy system is a fuzzy system that uses a learning algorithm derived from or inspired by neural network theory to determine its parameters by processing data samples. A fuzzy system consists of fuzzifier, inference engine, and defuzzifier. Fuzzifier converts the crisp input to a linguistic variable using the membership function stored in the fuzzy knowledge base. Fuzzy inference engine use IF-THEN type fuzzy rules that convert the fuzzy input to the fuzzy output. Defuzzifier converts the fuzzy output of the inference engine to crisp value using same membership function as used by the fuzzifier.

Fuzzy logic has ability to deal with imprecise or imperfect information. Neural networks are modeless systems that learn from the underlying relationships of data. Neural network has self learning and self tuning capability. Neuro fuzzy refers to the combination of fuzzy set theory and neural network with the advantages of both. Fuzzy logic significantly simplifies design complexity. Most real life physical systems are actually non linear systems. Commonly used approximation methods to handle non linearity includes linear, piecewise linear and lookup table. A linear approximation is simple with limited control performance. A piecewise linear technique is difficult to implement. A lookup table technique requires large memory to handle complex systems.

Fuzzy logic can result in better control performance than linear, piecewise linear and lookup table techniques. In fuzzy logic, non linearity is handled using fuzzy rules, membership functions and the inference process which results in improved performance, simpler implementation and reduced design cost. Due to several advantages of fuzzy logic, an adaptive neuro fuzzy logic controller is designed to evaluate the trust ability of nodes in the network.

The rest of this paper is organized as follows. Section 2 briefly discusses the related work in connected dominating set construction. In section 3, we present our proposed scheme which includes design of fuzzy logic controller to evaluate trust level of the nodes, an algorithm to elect the dominating nodes in the network, composite key management scheme to support secure communication in the network. In section 4, we briefly discuss the results of our experimental analysis, and we summarize our contributions in section 5.

2 Problem Formulation

Algorithm for connected dominating set initially proposed by Wu et al. [1] selects node with maximum node id as a dominator. Marking algorithm proposed by Wu initially marks all nodes as 'F'. Vertex with two not connected neighbors is marked as 'T'. For two vertices u and v of a graph G, vertex v is selected as dominator if u is covered by v and id (u) < id (v). Extended rule proposed by Wu uses node degree or cardinality as a selection factor for dominator. Power aware connected dominating set algorithm proposed by Wu uses energy level of node as dominator selection factor. For two vertices u and v of sub graph G, vertex v is selected as dominator if u is covered by v and el (u) < el (v). If el (u) = el (v), the algorithm choose a vertex with maximum id. Message complexity of the algorithm is $\theta(m)$ where m is number of edges and time complexity of the algorithm is $O(\Delta3)$ where Δ is maximum node degree[1,6].

Connected dominating set algorithm proposed by Alzoubi et al. [2] includes two phases. The algorithm constructs a spanning tree whose root v is selected using leader election algorithm. The first phase assigns rank for each node in the tree. Root node v at level 0 send announcement to its lower level children. Each node except root set their levels as parent level plus one. The process continues until it reaches the leaf node. The leaf node send complete message back to root. Rank of each node is assigned as {ID, level}. Initially all the nodes are unmarked. Node with lowest rank send DOMINATOR message to lower levels. Node that receives DOMINATOR message mark itself as gray and send DOMINATEE message back to dominator node. Node that receives more DOMINATEE message marks it as black. The second phase constructs CDS from Maximal Independent Set (MIS). The black node that joined the CDS broadcast invite message to all other black nodes. When a black node receives an invitation, it joins the CDS. CDS also include gray nodes that relayed the message. The time complexity of the algorithm is O (n) and the message complexity is O (n log (n)) [2].

Stojmenovic et al. [3] proposed CDS algorithm which is similar to the method proposed by Wu and Li [1]. The algorithm replaces node id with key= (degree, x, y) where degree of node is number of 1-hop neighbors, x represents x-coordinate and y represents y-coordinate. A node with maximum degree is added in dominating set. If degree is same for nodes, the dominator is selected based on x-coordinate. If it is same, then nodes are selected based on y-coordinate. The location details of the node can be obtained using Global Positioning System (GPS). The algorithm has time complexity of Ω (n) and message complexity of O (n2) [3].

El-Haji et al. [4] proposed Fast Distributed Dominating Set (FDDS) algorithm which selects dominators based on weightage. Weight of node is computed by using fuzzy logic controller based on nodeinfo {ID, RE, M, T}. Node information includes node id, residual energy of node, mobility of node, node traffic. Node with maximum weight is selected as dominator. Message complexity of the algorithm is O (n) and time complexity is O (Δ2). The algorithm assumes that each node knows its node id, residual energy, mobility and traffic [4].

Samuel et al. [7] proposed a connected dominating set algorithm based on probability of future contacts of node. The probability of future contact is calculated based on duration of previous contact [7]. Node i is added to DS if i $\notin$ DS and N (i) $\not\subset$ DS and node has maximum probability of future contacts. The DS represents the set of nodes that have high probability to meet with all the other nodes in the network.

In this paper, we propose an algorithm that elects the dominator based on trust ability of the node and probability of future contact of the node. We design a fuzzy logic controller to calculate the trust level of the node based on number of packet dropped by the node, number of packet forwarded successfully by the node and number of packets forwarded with alteration by the node.

3 The proposed scheme

3.1 Construction of Dominating Set

The dominating set based clustering elects a node having maximum trust ability and maximum probability of future contact as dominator. The basic algorithm is similar to algorithm proposed by Wu and Li [1]. The algorithm computes trust value of each node based on packet forwarding status of the node. For node I in the network, the algorithm compares I's trust value with trust value of its neighbors and I's node degree with degree of its neighbors. The node with trust ability above a threshold value (TH) and maximum node degree is marked as dominator. If multiple nodes with equal node degree exist, the node with maximum probability of future contact is elected as dominator. A node I is elected as dominator only if it is not in dominating set (DS) and its neighboring nodes N (I) not in DS. The procedure for dominator election is described in following algorithm.

```
1. Initialize DS as empty
2. For each node I in the network
              2. a. Compute trust value T (I)
   End for
3. For each node I in the network
     For each node J in N (I)
       3. a. Find node K with T (K) ≥ TH and
                max (degree)
          If degree (K) = degree (J)
                 Calculate $P_{contact}$ for K and J
```

```
            Find node $D$ with max ($P_{contact}$ )
      Endif
End for
End for
4. Add $D$ to DS if $D$ DS and N($D$) DS
```

The above given algorithm can be understood with the graph shown in Fig.1. We use the same example network cited in [13]. Values associated with each node represent trust value of the node and probability of future contact of the node respectively.

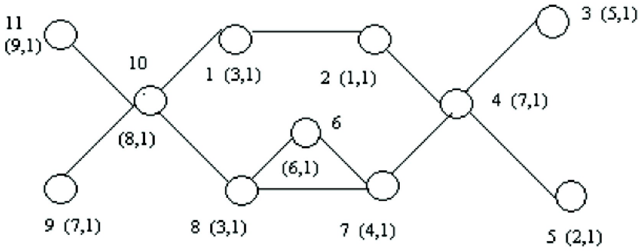
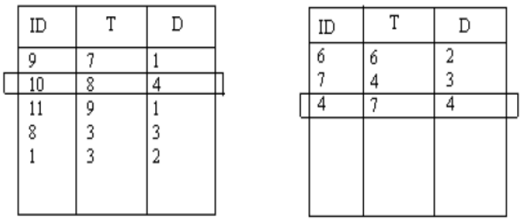


Fig. 1. Graphical representation of network.

Initially DS is empty. The node with trust value above TH and maximum degree is selected as dominator. The value of TH is selected based on security level required by the application. Fig.2 represents node id, trust value of node (T), and node degree (D).



ID	T	D
9	7	1
10	8	4
11	9	1
8	3	3
1	3	2

ID	T	D
6	6	2
7	4	3
4	7	4

Fig. 2. Selection of dominating nodes.

Node 10 with maximum trust ability is elected as dominator in the first step. All the nodes covered by 10 are removed from graph. In second step, node 4 is elected as dominator. The final DS obtained is {10, 4}. The nodes which remain uncovered are maintained in uncovered set (US). The uncovered nodes can be used as connectors to form connected dominating set (CDS).

3.1.1 Trust value Evaluation

In this paper, we propose a fuzzy logic controller to compute trust value of nodes in the network. Trust is the degree of belief about the future behaviour of other entities, its calculation is based on the past experience with and the observation of the others related actions. For MANET, trust is interpreted as a relation among entities that participate in various protocols [11]. Node's trustworthiness is evaluated based on the following: number of packets dropped by the node, number of packets forwarded successfully by the node and number of packet forwarded with alteration by the node.

Fuzzy logic is an approximation process, in which crisp inputs are turned to fuzzy values based on linguistic variables, set of rules and the inference engine provided. The fuzzy controller based on Sugeno inference engine takes three inputs, processes the information and outputs trust value. The block diagram presented in Fig.3 shows the FLC controller in the Matlab simulation.

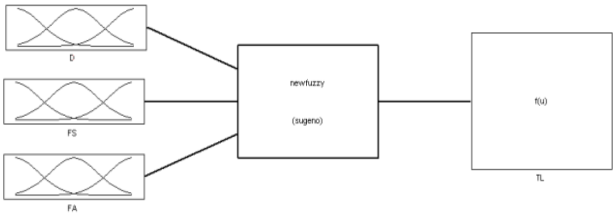
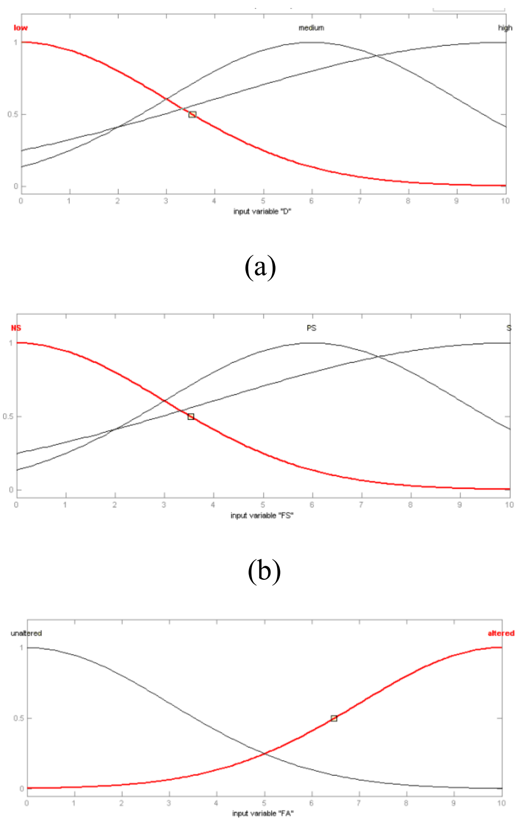


Fig. 3. ANFIS using Matlab.

We considered the following linguistic variables:
Packet drop rate D = {low, medium, high}
Packet forwarded successfully FS = {not successful, partially successful, successful}
Packet forwarded with alteration FA = {altered, unaltered}
Trust level = {not trusted, low, avg, normal, fully trusted}

Packet drop rate has 3 member function low, medium and high, in which low has range from 0pps-5pps, medium has range from 5pps-10pps and high has range from above 10pps. So if the crisp input for packet drop rate is 5, its fuzzy value is low. This model has three input variables with 3 Gaussian membership functions associated with two inputs D, FS and 2 Gaussian membership functions associated with input FA. Fig.4 represents the fuzzy membership functions in input space.



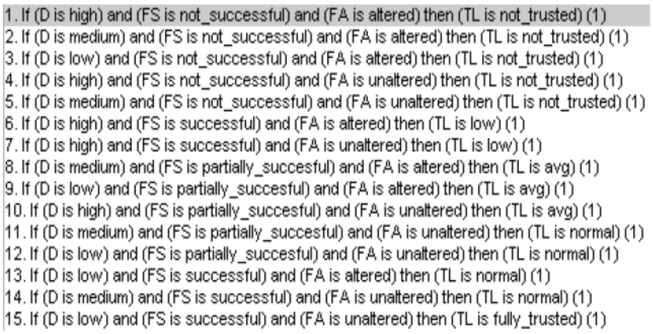
(a)

(b)

(c)

Fig. 4. Fuzzy member functions in input space: (a) Packet drop rate, (b) Packet forwarded successfully, (c) Packet forwarded with alteration.

After we get fuzzy input, we compare it against a rule base. A rule base is a set of rules that is responsible for final output. The rule base for trust value calculation is formed by rules and 3 decision factors. Linguistic rules of fuzzy logic controller are shown in Fig.5. Each node maintains a table to monitor the packet forwarding status of the node, which includes node_id, forwarded, dropped and altered fields. Assume node 'S' transmits a packet to node 'D'. 'S' increments the forwarded field by 1, on receiving an acknowledgement from node 'D'. 'S' increments altered field by 1, on receiving an ACKERR from 'D'. 'S' retransmits the same packet to 'D', when acknowledgement is not received from 'D'. Node 'S' retransmit the packet only for specified number of times to reduce network traffic. 'S' increments dropped field by 1, when it not receive acknowledgement from 'D'. Initially the field value is set as 0. The table is refreshed periodically.



1. If (D is high) and (FS is not_successful) and (FA is altered) then (TL is not_trusted) (1)
2. If (D is medium) and (FS is not_successful) and (FA is altered) then (TL is not_trusted) (1)
3. If (D is low) and (FS is not_successful) and (FA is altered) then (TL is not_trusted) (1)
4. If (D is high) and (FS is not_successful) and (FA is unaltered) then (TL is not_trusted) (1)
5. If (D is medium) and (FS is not_successful) and (FA is unaltered) then (TL is not_trusted) (1)
6. If (D is high) and (FS is successful) and (FA is altered) then (TL is low) (1)
7. If (D is high) and (FS is successful) and (FA is unaltered) then (TL is low) (1)
8. If (D is medium) and (FS is partially_succesful) and (FA is altered) then (TL is avg) (1)
9. If (D is low) and (FS is partially_succesful) and (FA is altered) then (TL is avg) (1)
10. If (D is high) and (FS is partially_succesful) and (FA is unaltered) then (TL is avg) (1)
11. If (D is medium) and (FS is partially_succesful) and (FA is unaltered) then (TL is normal) (1)
12. If (D is low) and (FS is partially_succesful) and (FA is unaltered) then (TL is normal) (1)
13. If (D is low) and (FS is successful) and (FA is altered) then (TL is normal) (1)
14. If (D is medium) and (FS is successful) and (FA is unaltered) then (TL is normal) (1)
15. If (D is low) and (FS is successful) and (FA is unaltered) then (TL is fully_trusted) (1)

Fig. 5. Linguistic rules.

3.1.2 Probability of future contact Evaluation

Probability of future contact of the node depends on node stability and link stability. The stability of the node mainly depends on mobility of the node and energy drain rate of the node. The battery power of the node might drain out for those nodes with more number of previous contacts. So the probability of future contact of such nodes will be low. The node with minimum number of previous contacts has more possibility to be in contact in future. Drain rate of a node is defined as the rate of dissipation of energy of a node. Energy drain rate of a node is calculated using the method cited in [14]. Probability of future contact of node is calculated based on energy drain rate of the node[15]. Higher the drain rate, faster the energy depletion in the node.

3.2 Construction of CDS

The node in uncovered set (US) is used as connector to connect nodes in dominating set provided there exit common neighbours between them.

Case 1: Common neighbour exist between nodes.

1. Node in US selected as connector.

2. Connect the DS nodes and connector using common neighbours.

3. If multiple common neighbours exist, select a neighbour with maximum trust and node degree.

The above given algorithm for constructing CDS can be understood with the following example. DS and US obtained for the graph shown in Fig. 1 is

DS = {10, 4} US = {6}

If a common neighbour exists between DS nodes and US node, the US node can be selected as connector to connect DS nodes. In this example, N (10) ∩ N (6) ≠ Ø and N (4) ∩ N (6) ≠ Ø. So node 6 is selected as connector to connect node 10 and 4 using common neighbouring nodes 8 and 7. The virtual path obtained connecting nodes 8 and 7 includes 10-8-6-7-4.

CDS = {10, 8, 6, 7, 4}

Case 2: No common neighbour exist between DS & US.

1. Let DS be { D1, D2 }
2. Find common neighbour between dominating nodes N (D1) ∩ N (D2).
3. Select a node with maximum trust value and node degree from the resultant set as connector.

The above given algorithm for constructing CDS can be understood with the graph shown in Fig.6.

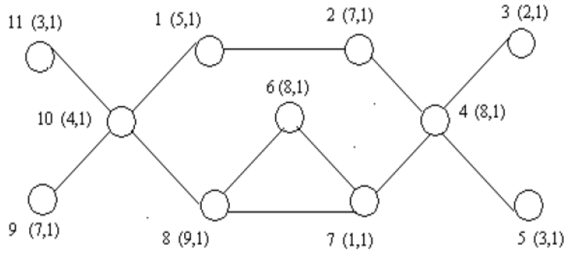
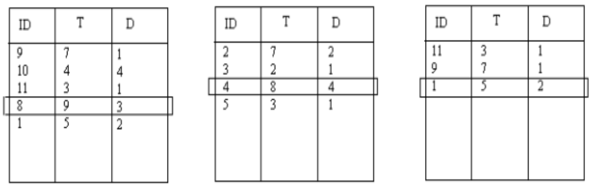


Fig. 6. Network Model.



ID	T	D
9	7	1
10	4	4
11	3	1
8	9	3
1	5	2

ID	T	D
2	7	2
3	2	1
4	8	4
5	3	1

ID	T	D
11	3	1
9	7	1
1	5	2

Fig. 7. Selection of dominating nodes.

DS = {8, 4} US = {11, 9, 1}
No common neighbour exist between {8, 4} and {1}. So we select common neighbours that exist between node 8 and 4.
N (8) = {10, 6, 7} N (4) = {2, 7, 3, 5}
N (8) ∩ N (4) = {7}
Node 7 can be used as connector to connect node 8 and 4. The resultant CDS is {8, 7, 4}. The virtual path obtained connecting node 8 and 4 is 8-7-4.

3.3 Construction of MCDS

The pruning rule used to construct MCDS is similar to rule cited in [13]. If a node k in DS is connected by two adjacent nodes in CDS, then remove k from CDS.

The CDS obtained for the graph shown in Fig.1 is {10, 8, 6, 7, 4}. Here node 6 is connected with two adjacent nodes 8 and 7. Node 6 is removed by applying pruning rule which results in minimum connected dominating set (MCDS) { 10, 8, 7, 4}. The resultant virtual path that connects 10 and 4 includes 10-8-7-4. The CDS obtained for the graph shown in Fig.6 is {8, 7, 4}. In this example, there are no adjacent nodes in CDS. So the resultant MCDS is {8, 7, 4}. The basic of the algorithm is similar to algorithm mentioned in [13]. Our work differs from theirs in that we select the dominators based on trust ability and probability of future contact of node. The virtual path connecting dominators is established using nodes that are trustable and are having long period of life time in the network. The size of the resultant MCDS varies based on the trust level required by the application.

3.4 Local Repair

Case 1: Dominator leaves the virtual path

Dominator that leaves send LEAVE message to its 1-hop neighbours. Let *i* be the neighbour with maximum trust ability and node degree. If node *i* already exist in MCDS, then it can be treated as new dominator in the virtual path. If not, a new virtual path is established to connect the nodes in DS. MCDS obtained for the graph shown in Fig.1 is {10, 8, 7, 4}. Assume node 10 leaves the network. The node 10 send LEAVE message to all its neighbours. The Node 8 neighbour of node 10 with maximum trust ability and degree can be elected as new dominator as it is part of MCDS.

Case 2: Connector leaves the virtual path

Let *i* be the connector that leaves the virtual path. Select a common neighbour that exists between N (*i*). If common neighbour exists, establish a virtual path using common neighbour. If not, construct a new MCDS. When connector node 8 of graph shown in Fig.1 goes down, it sends a LEAVE message to its 1-hop neighbours. As there are no common neighbours between one hop neighbours of node 8, a new MCDS is established connecting the nodes 10-1-2-4.

3.5 Network model for Key Management

Most of attacks on routing protocol are due to absence of encryption for some fields in the routing packets. Unauthorized modification of such fields could case serious security threats. To ensure secure communication, we present a composite key management scheme. Zhou [8] proposed a threshold key management scheme in which certification services are distributed among 'n' serving nodes. Each serving node generates partial certificate. To generate secret key, any node must have 'n' partial certificates. This scheme has following drawbacks: i) serving node must maintain public key of all other nodes in network, which requires more memory space ii) lack of certificate revocation mechanism iii) not suitable for larger network iv) the algorithm doesn't deal with network synchronization when split or join occurs in the network v) serving nodes may not be in contact at all times.

In our proposal, we apply the concept of hierarchical clustering. The cluster head (CH) maintains information only about its cluster member, which needs limited memory. 'K' cluster members with high trust value are selected as serving nodes. The CH act as one of the serving nodes. The public key of members is maintained in CH. We propose an algorithm for key revocation where key revocation decision is made by the CH based on revoke point value. The algorithm is applicable for larger network, as it is based on concept of hierarchical clustering.

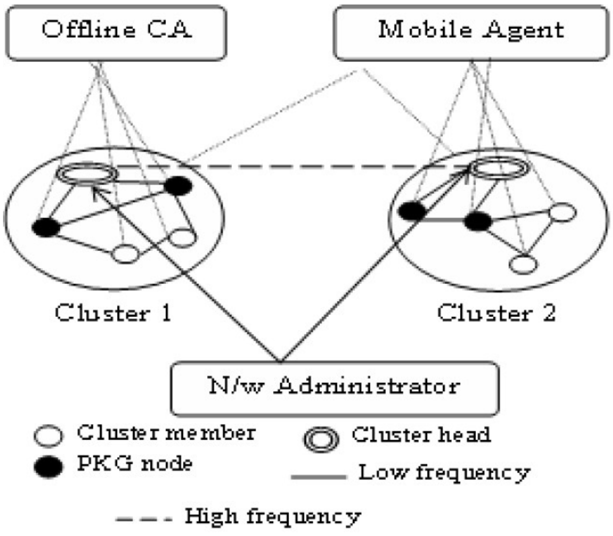


Fig. 8. Network Model.

Fig.8 represents the network model for key management. The network administrator initially selects the CH. 'K' cluster members with high trust value are selected as Primary Key Generation (PKG) serving nodes. Each new node has self assigned public key and register its information in CH. The private key of the node is generated by PKG serving nodes [12]. The CH also acts as one of the PKG serving nodes and plays the role of key combiner. The complete key is generated by the CH by combining private key shares generated by serving nodes. Initial public key of CH is obtained by applying one way hash function on its id. CH public key varies based on its trust level. New public key of CH is computed based on old public key and its new trust value. The private key of CH is initially assigned by network administrator. Later private key shares are computed by PKG nodes. The public key of CH is distributed to all cluster members in the corresponding cluster.

3.5.1 New Node Registration

When a new node wants to join in the network, the registration procedure for a new node is described in following algorithm.

1: CH broadcasts ADVERTISE message at a certain time interval.

2: If CH and new node i lies within transmission range do step3 else do step 4 and 5.

3: Node *i* send REGISTER (node_id, public key) message to CH. The Message is encrypted by session key shared by *i* and CH.

4: Node *i* send HELLO message to one of its closest neighbor.

5: Neighbour forwards new node to CH.

6: CH initially set the trust value and probability of contact of new node as 0.

7: CH adds node *i* detail in its member table.

3.5.2 Intra Cluster Communication

Fig.9 shows a cluster in which CH represents cluster head and *A, B, C* represents cluster member. Node *A* wants to communicate with *C*. The procedure for intra cluster routing is described in following algorithm.

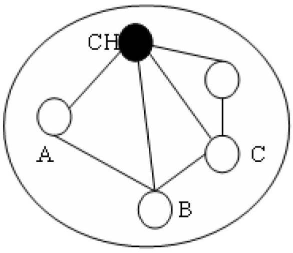


Fig. 9. Intra cluster routing.

```
1. A asks CH for C's public key
2. CH computes trust ability of node A
2. a. TV (A) = compute_trust (A, N (A))
3. If TV (A) >= Threshold
        3. a. CH sends $E_{PKey(A)}$ (PKey(C)) to A
        3. b. A send $E_{PKey(C)}$ (Message) to C
   Else
        3. c. CH drops A's request
   End if
```

3.5.3 Inter Cluster Communication

The communication between the clusters is carried out using the virtual path established between the cluster heads (CH). Fig.10 shows two different clusters *C1* and *C2* under cluster heads CH1 and CH2. *A1* wants to communicate with *B2*. The procedure for inter cluster routing is described in following algorithm.

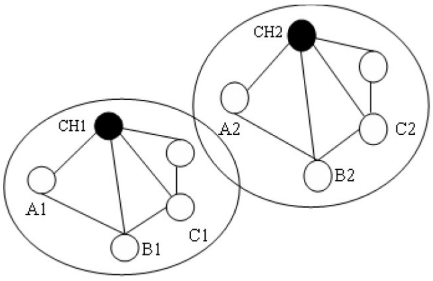


Fig. 10. Inter cluster routing.

```
1: A1 asks for CH1 for B2's public key
2: CH computes trust ability of node A1
     TV (A1) = compute_trust (A1, N (A1))
3: If TV (A1) >= Threshold
   3. a. CH1 search for node B2 in its member list
   3. b. if B2 not in CH1 member list
   3.c. CH1 send SEARCH_REQUEST to its
          neighboring cluster head CH2
   3.d. CH2 search for B2 in its member list. If
          found, do step 3.e. to 3.h. else send
          FAILURE message to CH1.
   3. e. CH2 send $E_{KeyCH}$ (PKey (B2)) to CH1
   3. f. CH1 decrypt the message and send $E_{PKey\,(A1)}$
          (PKey (B2)) to A1
   3. g. A1 sends $E_{Key\,(B2)}$ (Message) to CH1
   3. h. CH1 forwards encrypted message to CH2
          which in turn forward the message to B2.
```

3.5.4 Node Leave

A node may leave a cluster when it has low battery or when it moves outside the cluster. The procedure to handle node leave is described as follows.

```
1: Each cluster member send VISIT message to CH
     at certain time interval.
2: CH refreshes its old member list based on in
     incoming VISIT message.
3: If CH not receive a VISIT message from node i,
     CH send VERIFY (i) message to other cluster
     members.
4: CH waits for certain time interval.
5: If CH receives reply from any of its members it
     update node i detail in member list else, it delete
     node i from member list.
```

3.5.5 CH leave

The CH before it leaves the cluster, send a LEAVE message to PKG nodes. The PKG node with next highest trust ability plays the role of new CH. The old CH sends information about all its cluster members to new CH. The new CH broadcast (oldCH_ID, newCH_ID, new public key) to all other CHs. The CH periodically sends a REFRESH message to all PKG nodes. If any PKG node doesn't receive the REFRESH message within specified time, it contacts other PKG nodes and declares that the CH had left the cluster. New CH is elected based on trust value.

3.5.6 Key revocation

In our work, we use mobile agent to handle key revocation process and to collect information about 'k' trustable nodes. Mobile agent is special type of mobile codes which migrates from one host to another in a heterogeneous network and executes at a remote host until it completes the given task. The main advantages of mobile agent includes: adapting dynamically to changes in network, support heterogeneous environments, save bandwidth, deal with non-continuous network connection, overcome network latency and reduce network load [9].

Mobile agent maintains a data structure which includes cluster member ids and their revoke point. The cluster head initiate the mobile agent periodically. Initially, the revoke point for all the cluster members is set as 0. Mobile agent starts the process from CH and migrates through all its cluster members. The node that suspect a particular nodes, can update the entry for that node in data structure by incrementing its revoke point value. The value of the revoke point is incremented varyingly based on the trust level of the suspecting node. The trust level of the suspecting node can be not trustable, low, average, normal, and fully trustable.

Table 1. Revoke point

	Non Trustabl e	Low	Average	Normal	Fully Trustable
Value	0	V1	V2	V3	V4

V1, V2, V3 and V4 are incremental values for revoke point where V1<V2<V3<V4. The node that suspects a particular node can update the entry for that node in data structure by incrementing its revoke point value by V4, provided the node is fully trustable. Finally, the information provided by mobile agent is processed by CH. The certificate of the node with revoke point greater than or equal to threshold will be revoked by CH. The CH broadcasts REVOKE (ID) message to all other nodes in the cluster.

4 Experimental Results

Performance of the proposed fuzzy controller to evaluate trust value of node is investigated by means of simulation in the MATLAB. The fuzzy controller attributes are
name: 'anfis'
type: 'sugeno'
andMethod: 'prod'
orMethod: 'max'
defuzzMethod: 'wtaver'
impMethod: 'prod'
aggMethod: 'max'
input: [1x3 struct]
output: [1x1 struct]
rule: [1x8 struct]
The membership function used is 'gausmf'. The anfis is trained with dataset of size 55 x 4. The fuzzy system is trained for 10 epochs. Fig.11 shows the root mean square error (RMSE) obtained for 10 epochs.

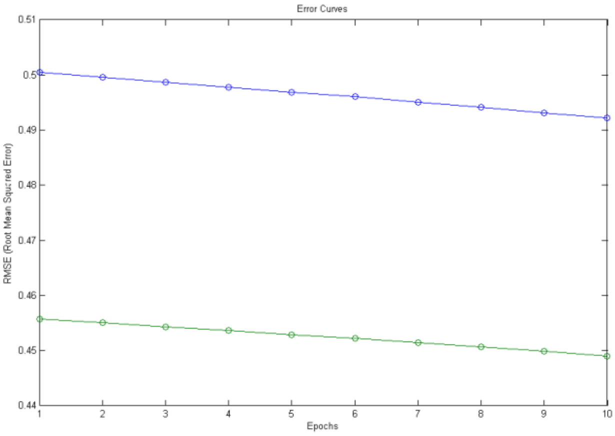


Fig 11. RMSE curve.

The range of the linguistic variables is assumed as follows: D { low (0 to 3), medium (3 to 6), and high (7 to 10)}, FS { not successful (0 to 3), partially successful (3 to 6), and successful (7 to 10)}, FA {unaltered (0 to 5), altered (5 to 10)}, and TL { not trusted (0 to 2), low (2 to 4), average (4 to 6), normal (6 to 8), and fully trusted (8 to 10)}. The trust value of nodes are calculated and displayed in the Table 1 using the proposed neuro fuzzy logic controller and the multiple linear regression approach.

Table 2. Solutions of MLR and fuzzy controller

D	FS	FA	Multiple Linear Regression	Fuzzy Controller
7.6	1.2	5.3	0.87	0.37
7.8	1.6	5.5	0.9	0.511
8	2.1	6	0.8	0.725
5.7	4.49	3.2	3.79	4.26
3	2.2	6.1	1.9	1.6
9.3	2.1	8.3	0.63	0.4
1.2	9.32	2.4	7.29	7.48
3.5	6.14	1.23	5.9	6.13
7.31	0.7	6.4	0.157	0.2
0.01	8.98	0.01	8.62	8.13

Multiple linear regression technique generates the linear function shown in Eq. (1) that properly fits the given set of data points.

$$y = -2.178723979 \cdot 10-1\ x1 + 4.369991843 \cdot 10-1\ x2 - 5.096263044 \cdot 10-1\ x3 + 4.705861706 \qquad (1)$$

where x1 is packet drop rate, x2 is packets forwarded successfully, x3 is packets forwarded with alteration, and y is the trust value. The error between the solution by fuzzy controller and multiple linear regression method is displayed in Fig.12. The numerical values of the required solution, solution by fuzzy controller, and solution by multiple linear regression method is shown in Fig.13. Hence the fuzzy controller solution is accurate and is better than solution by multiple linear regression method.

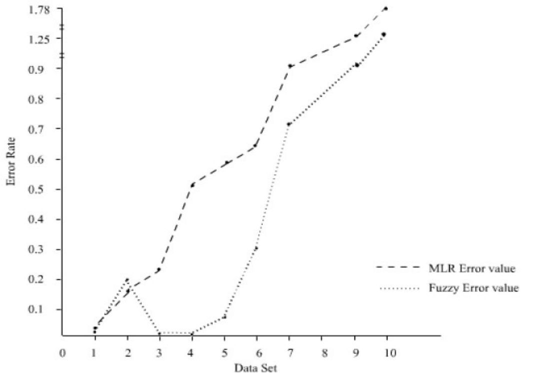


Fig 12. Error curve of MLR and Fuzzy controller.

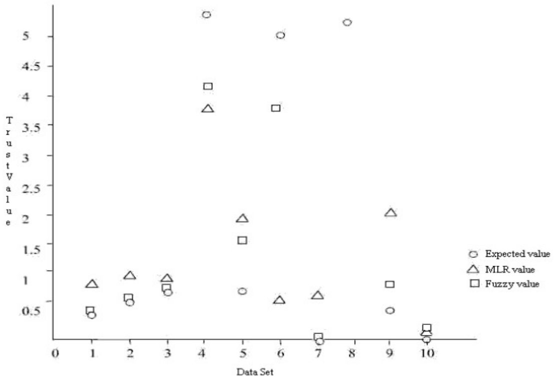
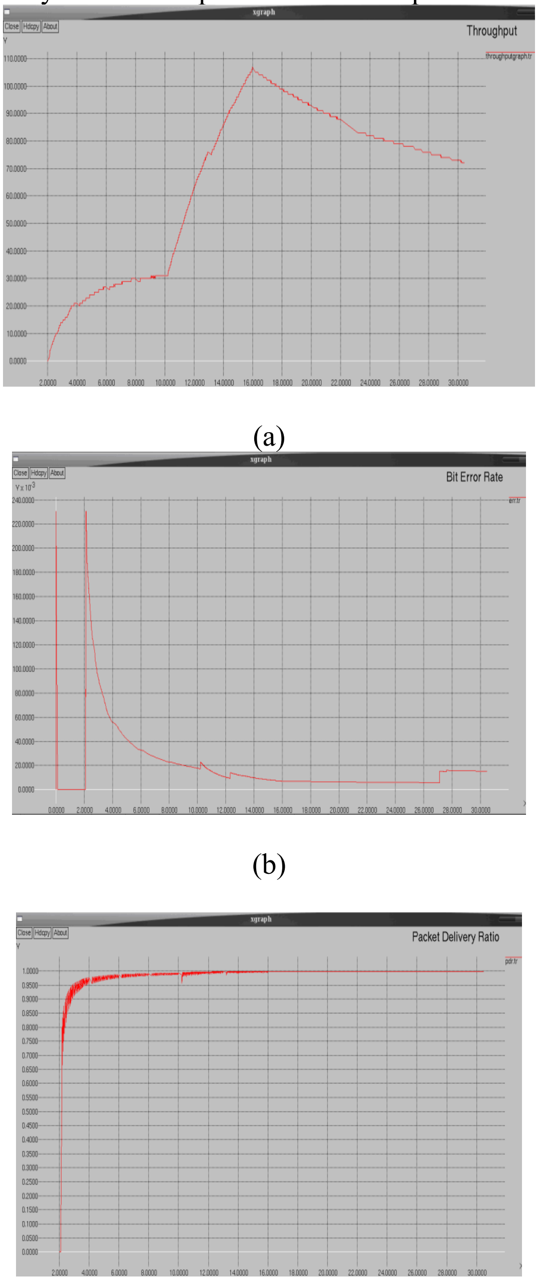


Fig 13. Prediction of trust value of nodes.

In our simulation, we use NS2 simulator. In each of simulation, the nodes are placed uniformly at random within a 750X570m squares. Nodes are assumed to have different transmission range. The maximum transmission range of a node is 40. Fig. 14 show simulation results for secure routing through trustable nodes based on DSR protocol. Bit error rate of transmitted packets reaches its minimum after few initial transmissions. The delivery ratio of the packet remains at peak value.



(a)

(b)

(c)

Figure 14. (a) Throughput, (b) Bit error ratio, (c) Packet delivery ratio.

5 Conclusion

In this paper, we proposed a secure minimized dominating set based routing protocol for MANET. This protocol follows two different phases. In the first phase, the protocol uses mechanisms to detect the trust level of nodes and its probability of future contact with the neighboring nodes. In the second phase, the protocol constructs minimized dominating set of nodes for the virtual network topology based on trust ability of the node and its probability of future contact. We designed a fuzzy logic controller to evaluate trust level of nodes based on packet forwarding status of the node. In this paper, we also presented a composite key management scheme for MANET. The system maintains forward secrecy and backward secrecy. We discussed the results obtained on implementing fuzzy logic trust evaluator using MATLAB and simulated results for secure routing using composite key management scheme.

References:

[1] Jie Wu and Hailian Li , A dominating-set-based routing scheme in ad hoc wireless networks, Telecommunication Systems, 2001, 3, pp. 63-84.

[2] K.Alzoubi, P.J.Wan, O.Frieder, New distributed algorithm for connected dominating set in wireless ad hoc networks, In Proceedings of the Thirty-Fourth Annual Hawaii International Conference on System Science (HICSS-35). IEEE Computer Society Press, 2002.

[3] Ivan Stojmenovic, Mahtab Seddigh, Jovisa Zunic, Dominating sets and neighbor elimination based broadcasting algorithms in wireless networks, IEEE transactions on parallel and distributed systems,2002, 13, (1), pp. 14-25.

[4] Wassim El-Hajj, Zouheir Trabelsi, Dionysios kountanis, Fast distributed dominating set based routing in large scale MANETs, Elesvier B.V. doi:10.1016/j.comcom.2007.03.011, 2007.

[5] R.PushpaLakshmi, Dr.A.Vincent Antony Kumar, Security aware Minimized Dominating Set based Routing in MANET, In Proceedings of the IEEE ICCCN, Tamilnadu, 2010.

[6] J. Wu, H.L. Li, On calculating connected dominating set for efficient routing in ad hoc wireless networks, in: Third ACM International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, 1999.

[7] Hany Samuel, Weihua Zhuang, Bruno presiss, DTN based dominating set routing for

MANET in heterogeneous wireless networking, Mobile Netw Appl, 2009, 14, pp. 154-164.

[8] L. Zhou, Z.J.Haas, Securing Ad hoc Network, IEEE Networks, 1999, 13, (6), pp. 24-30.

[9] S.S.Manvi, P.Venkataram, Mobile agent based approach for Qos routing, IET Communication, 2007, 1, (3), pp. 430-439.

[10] Matlab, http://www.mathworks.com/products/matlab/.

[11] Hongjun Dai, Zhiping Jia and Zhiwei Qin, Trust Evaluation and Dynamic Routing Decision Based on Fuzzy Theory for MANETs, Journal Of Software, 2009, 4, (10), pp. 1091-1101.

[12] Zhang Yi, Zhu Lina and Feng Li., Key Management and Authentication in Ad Hoc Network based on Mobile Agent, Journal Of Networks, 4(6).

[13] Ariyam Das, Chittaranjan Mandal, Chris Reade, Manish Aasawat, An improved greedy construction of minimum connected dominating sets in wireless networks, Proceedings of 2011 IEEE Wireless Communications and Networking Conference 2011 (IEEE WCNC 2011 - Network), Cancun, Mexico, 2011, pp 1601-1606.

[14] Shuchita Upadhayaya, Charu Gandhi, QOS routing using link and node stability in mobile ad hoc networks, Journal of Theoretical and Applied Information Technology.

[15] Anuradha Banerjee, Paramartha Dutta, Link Stability and Node Energy Conscious Local Route-Repair Scheme for Mobile Ad Hoc Networks, American Journal of Applied Sciences ,2010, 7, (8), pp. 1139-1147.

PushpaLakshmi R received her M.E degree in Computer Science from Anna University, India in 2004. She is currently an associate professor in department of information technology, PSNA CET, India. Her research interests include ad hoc network security, Qos routing, and wireless networks.

Vincent Antony Kumar A received his MCA degree from Madurai Kamaraj University, India and the Ph.D degree from Gandhigram rural University, India in Mathematics and Computer Applications. He is currently a professor and head in department of information technology, PSNA CET, India. His area of research includes genetic programming and optimal control, neural networks and genetic algorithm.