IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661, ISBN: 2278-8727 Volume 7, Issue 1 (Nov-Dec. 2012), PP 22-32
www.iosrjournals.org

An Adaptive Secure Fuzzy Multicast communication in Large Scale Mobile Ad Hoc Networks

B. G. Obula Reddy[1], Dr. Maligela Ussenaiah[2]
[1]*Associate Professor, Lakireddy Balireddy College of Engineering L.B.Reddy Nagar,Mylavaram, Krishna (Dist):521 230*
[2]*Assistant Professor, Computer Science, Vikrama Simhapuri University Nellore Nellore, Andhra Pradesh, India*

Abstract: *Multicast protocols in MANETs must consider control overhead for maintenance, energy efficiency of nodes and routing trees managements to frequent changes of network topology. Now-a-days Multicast protocols extended with Cluster based approach. Cluster based multicast tree formation is still research issues. The tree reconstruction of cluster-based multicast routing protocol will take place if any link of the trees has malfunction or the nodes move out of the link, therefore, its robust performance is unsatisfactory. The mobility of nodes will always increase the communication delay because of re-clustering and cluster head selections. In our previous proposal, reported on simulation-based experiments evaluating two different approaches clustering to multicast communication in mobile ad hoc networks (MANETs), namely AFMR and CBRP. One of the chief contributions of this work is our objective analysis of these two multicast routing protocol categories in order to characterize their behavior under a wide range of MANET mobility. In this paper, we evaluate mainly security level based in AFMR, named SAFMR and compare it with Cluster-based On Demand Multicast Routing Protocol (CODMRP) and Cluster-based routing protocol (CBRP).*

Keywords: *Fuzzy Clustering, AFMR, SAFMR, CBRP, Kalman Filter, Location Management.*

I. Introduction

The recent advances in wireless and' mobile technology is evident from the fact of widespread usage of mobile and wireless devices such as laptops, palmtops, personal digital assistants etc. The emergence of group oriented real-time applications such as IP telephofiy, video conferencing, and video gaming has generated the demand for group communication support in wireless and mobile
Networks. The parameters such as delay, throughput, jitter, packet loss etc, are very important in these applications [1].

In recent years mobile ad hoc networks (MANETs) have received tremendous attention because of their self-configuration and self-maintenance capabilities. A Mobile Ad hoc network (MANET) is a system of wireless mobile nodes that dynamically self organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension [1]. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network. Security has become a primary concern to provide protected communication between mobile nodes in a hostile environment [1]. Unlike wire line networks, the unique characteristics of mobile ad hoc networks pose a number of non-trivial challenges to the security design [2].

1.1 Characteristics of MANETs

The main characteristics of mobile ad hoc network are:

- Dynamic topology. Since nodes in the network can move arbitrarily, the topology of the network also changes.
- The bandwidth of the link is constrained and the capacity of the network is also variable tremendously. Because of the dynamic topology, the output of each relay node will vary with the time and then the link capacity will change with the link change.
- Power limitation in mobile devices is a serious factor. Because of the mobility characteristic of the network, devices use battery as their power supply. As a result, the advanced power conservation techniques are very necessary in designing a system.
- The security is limited in physical aspect. The mobile network is easier to be attacked than the fixed network. Overcoming the weakness in security and the new security trouble in wireless network is on demand.

1.2 Challenges of MANETs

Mobile ad hoc network has different challenges with respect to wireless security due to some of the following reasons:

1. The wireless network especially liable to attacks because of active eavesdropping to passive interfering.
2. Due to lack of Trusted Third Party adds, it is very difficult to deploy or implement security mechanisms.
3. Mostly Mobile devices have limited computation capability and power consumption functionalities which are more vulnerable to Denial of Service attacks. It is also incapable to run heavy security algorithms which need high computations like public key algorithms.
4. Due to MANET's properties like infrastructure less and self-organizing, there are more chances for trusted node to be compromised and launch attacks on networks. In other words we need to cover up from both insider and outsider attacks in MANET, in which insider attacks are more difficult to deal with.
5. It is difficult to distinguish between stale routing and faked routing information because of node mobility mechanism. In node mobility mechanism it enforces frequent networking reconfiguration which creates more chances for attacks [7].

Routing is essential for a MANET to operate correctly, and a lot of routing protocols have been proposed in the literature, including proactive (table-driven), reactive (demand-driven), and hybrid solutions. Most of the existing protocols have assumed a MANET as a trusted environment. Unfortunately, in the presence of malicious nodes, a MANET is highly vulnerable to attacks due to its open environment, dynamically changing topology, and lack of centralized security infrastructure. To address this concern, several secure routing protocols have been proposed recently [1,5,8–10], such as SAODV [10], SRP [5], SAR [9]. But these secure routing protocols are mostly based on authentication and encryption algorithm. The Security-Level of mobile hosts is not fully considered [9].

1.3 Properties of ad hoc routing protocols

Ad hoc routing protocols should have the following properties:

- Distributed Operation: The protocol should be distributed. It should not be dependent on any centralized authority. This is beneficial because the nodes can enter and leave the network easily.
- Loop Free: For the efficient functioning of the network, the routing protocol should guarantee that the routes are loop free. This avoids the wastage of
  bandwidth and computing power. Also, delays are reduced if the routes are loop free.
- Demand based Operation: To avoid the unnecessary wastage of bandwidth, computing power and battery, the routing protocol should react only when necessary. In other words, the protocol should be reactive.
- Unidirectional Link Support: Unidirectional links are formed in the radio environment. The protocol should use these unidirectional links for the optimal performance of the protocols.
- Security: Security is an important issue in MANETs. MANETs are susceptible to attacks like spoofing. To guarantee the desired behavior in ad hoc routing protocols some security measures are required. Security can be improved by applying encryption and authentication to the routing protocols.
- Quality of Service Support: Quality of Service is an important parameter in the ad hoc routing protocols. The routing protocols should support various QoS. For instance, real time traffic should have low jitter. It should be noted that none of the proposed protocols have all these properties.
- Multiple routes: The protocol should have redundant routes, so when one link fails an alternative route can be used without initiating route discovery. Also, buffering multiple routes makes the protocol resistant to frequent topology changes.
- Power conservation: The nodes that form the ad hoc network have very limited resources. One such important resource which is limited is the battery power. The protocols should conserve the battery power of the mobile devices. They should switch to power saving or standby mode when not in use.

1.4 Security services for MANETs

There are mainly three main security services for MANETs: Authentication, confidentiality, integrity.

- Authentication means correct identity is known to communicating authority.
- Confidentiality means message information is kept secure from unauthorized access.
- Integrity means message is unaltered during the communication between two parties.

1.5 Secure routing protocols for MANETs

Designing efficient routing protocols on MANETS is a primary challenge, but useful for conventional routing protocols. Conventional routing protocols which depend either on distance-vector or link-state usually use periodic broadcast advertisements of all routers to keep routing table up-to-date. In summary, efficient routing on MANETs faces several problems as follows.

- Periodically updating the network topology increase bandwidth overhead;
- Repeatedly awakening mobile nodes to receive and send information quickly exhausts batteries, which are the main power supply of the mobile nodes.
- The propagation of routing information causes overloading, thereby reducing scalability;
- Communication systems often cannot respond to dynamic changes in the network topology quickly enough.

Most secure routing protocols for MANETs use multihop rather than single-hop routing to deliver packets to their destination. The security of mobile nodes is guaranteed by the hop by-hop authentication, and all intermediate nodes need to cryptographically validate the digital signatures appended with a routing message.

Secure routing protocols significantly improve the usefulness of the efficient routing protocol. The idea was to simply incorporate more information in the routing message and routing table, in addition, there are security related operations introduced in the protocols. However, if a secure routing protocol incurs too much overhead, it is possible to render the protocol practically unusable.

1.6 Examples of secure routing protocols for MANETs

A secure on-demand routing protocol for MANETs is developed in (Hu et al, 2002), which is called Ariadne. Ariadne can authenticate routing message using one of three schemes: shared secrets between each pair of nodes, shared secrets between communicating nodes combined with broadcast authentication, or digital signatures.

1.6.1 SEAD: Secure efficient distance vector routing protocol

SEAD (Yih-Chun Hu & Perrig, 2002) is robust against multiple uncoordinated attacks creating incorrect routing state in any other node, even in spite of active attackers or compromised node in the network. The SEAD was designed based on the Destination-Sequenced Distance Vector (DSDV). During the route discovery process, the source node first selects a random seed number and sets the Maximum Hop-count(MHC) value. By using a hash function, h, the source node computes the hash value as h(seed).

1.6.2 Ariadne: A secure on-demand routing protocol

This protocol provides security against one compromised node and arbitrary active attackers, and relies only on efficient symmetric cryptography.

Now-a-days Multicast protocols extended with Cluster based approach. Based on the topology the existed ad hoc multicast routing protocols are classified into two categories i.tree based ii.mesh based. The tree based routing scheme has only one path between the source to receiver. MAODV, AMRIS, AM Route are the best examples for the tree based scheme. But, the mesh-based routing scheme has multiple redundant paths between the sources to receivers. ODMRP, CAMP is the typical examples of mesh-based scheme [2]. Both are giving some salient features to mobile ad hoc network. In earlier days multicast routing protocols are designed with the multiple unicast system [9]. After that it had extended as multicast system, which has only one source in a multicast group[3]. Recently, some prominent researchers have been proposed the cluster based multicast routing scheme for ad hoc networks. By this admissible work we can share different kinds of services or applications simultaneously in the multicast group.

Problems in Cluster-Based routing are the tree reconstruction of cluster-based multicast routing protocol will take place if any link of the trees has malfunction or the nodes move out of the link, therefore, its robust performance is unsatisfactory. So disconnection of one link may not affect the transformation of multicast packets. And another one is Cluster heads have high communication task, So Cluster head will failure due to lack of energy. However, the stability of the cluster heads is very important to the networks and non ideal cluster heads is possible to the "bottle-neck" of the networks [4].

The Kalman filter is the best possible (optimal) estimator for a large class of problems and a very effective and useful estimator for an even larger class. With a few conceptual tools, the Kalman filter is actually very easy to use. By using kalman filter we can predict the location updates within clustered groups, each CH

gets their neighbors locations.CH also exchange their position to members.CH keeps tracks of nodes position it will leads to predicts the new cluster head based on mobility.CH also predict neighbors' future directions.

In our previous proposal, reported on simulation-based experiments evaluating two different approaches clustering to multicast communication in mobile ad hoc networks (MANETs), namely AFMR and CBRP. One of the chief contributions of this work is our objective analysis of these two multicast routing protocol categories in order to characterize their behavior under a wide range of MANET mobility. In this paper, we evaluate mainly the performance according to the security metric in SAFMR and compare it with Cluster-based On Demand Multicast Routing Protocol (CODMRP) and Cluster-based routing protocol (CBRP).

II. Related Works

Shekhar H M P, Arun Kumar M A, and K S Ramanatha have presented an efficient Mobile Agents Aided Multicast Routing (MAMR) protocol which overcomes these limitations. The protocol was a hybrid protocol where intelligent mobile agents can been integrated with existing on-demand multicast routing protocols such as Multicast Ad Hoc On-demand Distance Vector (MAODV) routing protocol, On demand Multicast Routing Protocol (ODMRP) routing protocol and others[1]. Zaiba Ishrat discussed security issues, vulnerable nature of the mobile ad hoc network, security criteria and the main attack types that exist in it. Finally they survey the current security solutions for the mobile ad hoc network and then conclude that paper[2].

R. Pandi Selvam and V.Palanisamy have designed a cluster-based multi source multicast routing protocol with new cluster head election, path construction and maintenance techniques. They compute the maximum performance of proposed routing protocol in various environments, and also it compared with Multicast Ad-hoc On-Demand Distance Vector (MAODV) and On-Demand Multicast Routing Protocol (ODMRP) to prove the performance of delivery ratio, control overhead and forwarding efficiency [3]. XUE-MEI SUN, WEN-JU LIU, ZHI-QIANG ZHANG and YOU ZHAO have developed a Cluster-based On Demand Multicast Routing Protocol（CODMRP）to the lack of extension of flat multicast routing protocols in Ad Hoc networks of large scale. [4].

XUE-MEI SUN, WEN-JU LIU, ZHI-QIANG ZHANG and YOU ZHAO have proposed a Cluster-based On Demand Multicast Routing Protocol（CODMRP）to the lack of extension of flat multicast routing protocols in Ad Hoc networks of large scale. CODMRP refers to the advantages of fitness for high-speed movement of mesh-based ODMRP, and adopts an Enhanced Weighted Clustering Algorithm (EWCA) to manage hierarchically its motion nodes, and forms the forwarding group mainly based on cluster heads [5]. Bey-Ling Su, Ming-Shi Wang and Yueh-Ming Huang proposed the fuzzy modified AODV (FMAR) multicast routing protocol to select two comparably stable routes by computing dynamic route lifetime for multicast routing or layered video streaming [6].

Muhammad Arshad Ali and Yasir Sarwar have discussed different aspects of security in MANET (e.g. multi-layer intrusion detection technique in multi hop network of MANET, security problems relates between multihop network and mobile nodes in MANET etc) and also implement some of the solutions (e.g. comparative study of different routing protocol (AODV, DSR and TORA) security threats within MANET network like intruder behavior, tapping and integrity, MANET link layer and network layer operations with respect to information security etc) with respect to MANET network[7]. Roberto Carlos Hincapi, Blanca Alicia Correa and Laura Ospina investigated a survey on clustering techniques for MANET. Some preliminary concepts that form the basis for the development of clustering algorithms are introduced. These related issues have to do with the network topology, routing schemes, graph partitioning and mobility algorithms [8].

Jing Nie, JiangchuaWen, Ji Luo, Xin He and Zheng Zhou proposed the FLSL Fuzzy Logic Based Security-Level Routing Protocol. The basic idea of FLSL is to utilize the "local multicast" mechanism and the Security-Level to select the highest Security-Level route. The proposed algorithm of Security-Level is an adaptive fuzzy logic based algorithm that can adapt itself with the dynamic conditions of mobile hosts. Their Simulations show that the FLSL routing protocol can improve security of mobile ad hoc networks routing protocol [9]. Rui Huang and Gergely V. Z Aruba proposed a mechanism that allows non-GPS-equipped nodes in the network to derive their approximated locations from a limited number of GPS-equipped nodes. In their method, all nodes periodically broadcast their estimated location, in term of a compressed particle filter distribution. Non-GPS nodes estimate the distance to their neighbors by measuring the received signal strength of incoming messages. A particle filter is then used to estimate the approximated location, along with a measure of confidence, from the sequence of distance estimates [10].

Zhaowen Xing, Le Grunewald and K.K. Phang presented a robust weighted clustering algorithm, called PMW (Power, Mobility and Workload), to form and maintain more stable clusters. In PMW, the weight of each node is calculated by its power, mobility and workload, which can be easily collected and computed locally and cover the major factors that cause re-clustering. Clustering overhead of PMW is analyzed [11]. J. D. Mallapur, S. S. Manvi and D. H. Rao have proposed a scheme for constructing a multicast tree based on a spanning tree by

employing a fuzzy controller. Fuzzy controller uses three fuzzy input parameters namely, link bandwidth, link delay and link reliability for the construction of multicast spanning tree [12].

Byung-Jae Kwak, Nah-Oak Song and Leonard E. Miller proposed measure is consistent because it has a linear relationship to the rate at which links are established or broken for a wide range of mobility scenarios, where a scenario consists of the choice of mobility model, the physical dimensions of the network, the number of nodes. [13]. Dewan Tanvir Ahmed discussed different multicasting protocols, their deployment issues and provides some guidelines for the researchers in this field [14]. Shahram Nourizadeh, Y.Q. Song and J.P. Thomesse proposed a decentralized algorithm to organize an ad hoc sensor network into clusters by using Fuzzy Logic. Each sensor uses a Fuzzy decision making process to find the best Cluster Head. Simulation showed that this protocol is able to dynamically adapt to network mobility and also shows that with fuzzy logic we have stable clusters and so a cluster head have greater lifetime [15].

ZHAO Chun-Xiao and WANG Guang-Xing investigated the use of fuzzy control techniques. For each metric, a fuzzy membership function was defined to predict a more stable link. A fuzzy-inference rule base was implemented to generate the fuzzy cost of each link. A degree clustering algorithm based on a mobility prediction scheme was proposed in a scalable manner [16]. K. Venkata Subbaiah and Dr. M.M. Naidu have proposed a cluster head election scheme using fuzzy logic system (FLS) for mobile ad hoc wireless networks. They used three descriptors: distance of a node to the cluster centroid, its remaining battery capacity, and its degree of mobility. The linguistic knowledge of cluster head election based on these three descriptors is obtained from a group of network experts. [17].

III. Routing Protocols

3.1 Cluster-Based Routing Protocol (CBRP)

In Cluster Based Routing protocol (CBRP) the nodes are divided into clusters. Each node maintains a neighbor table. For each neighbor, the neighbor table of a node contains the status of the link (uni- or bi-directional) and the state of the neighbor (cluster-head or member). In CBRP routing is done using source routing. In forwarding a packet if a node detects a broken link it sends back an error message to the source and then uses local repair mechanism.

CBRP and all those who focus on achieving routing in small partition of network face the same type of problems. One important issue is connectivity among individual clusters. Network formation in such design is another issue i.e. how nodes will be allocated to different clusters or in zones such as in ZRP. It is mentioned in the specification of CBRP that new joining inside a cluster is based on broadcasting a message. But it is not cleared how nodes know in advance which cluster it wants to join. Moreover if the node receives replies from more than one clusters then how it will make its joining decision. Likewise in the case of clusters what scheme CBRP utilizes to aware all the cluster-heads about all other cluster-heads in the network. Specification details some error recovery mechanism but is silent about issues such as link satiability between clusters [2].

3.2 Cluster-based On Demand Multicast Routing Protocol (CODMRP)

In 2006 XUE-MEI SUN, WEN-JU LIU, ZHI-QIANG ZHANG and YOU ZHAO, "CODMRP: Cluster-based On Demand Multicast Routing Protocol", In this paper proposed a Cluster-based On Demand Multicast Routing Protocol（CODMRP）to the lack of extension of flat multicast routing protocols in Ad Hoc networks of large scale. CODMRP refers to the advantages of fitness for high-speed movement of mesh-based ODMRP, and adopts an Enhanced Weighted Clustering Algorithm (EWCA) to manage hierarchically its motion nodes, and forms the forwarding group mainly based on clusterheads.

In CODMRP, to establish a mesh for each multicast group, it also uses the concept of forwarding group. The forwarding group is a set of nodes responsible for forwarding multicast data on shortest paths between any member pairs. A clusterhead becomes a mesh member if it is between multicast sources and receivers. The main distinctness between the CODMRP and the ODMRP is the composing of mesh. The mesh of CODMRP is composed by source, clusterhead and destination nodes, in which the destination nodes are clusterheads and cluster members.

In ODMRP, group members and multicast routes are established and updated by the source "on demand." Similar to on-demand unicast routing protocols, a request phase and a reply phase comprise the protocol.

While a multicast source has packets to send, it floods a member advertising packet with data payload piggybacked to its clusterhead. This packet which is called JOIN QUERY and includes the source node, source clusterhead node and multicast group IDs is periodically broadcasted to the entire network to refresh the membership information and update the routes as follows. When a non multicast source wants to become a multicast member, it broadcasts the JOIN QUERY to its clusterhead, and if its clusterhead is not a multicast group member its clusterhead will continue to broadcast the JOIN QUERY to its neighbor clusterhead.

When a cluster head node receives a nonduplicate JOIN QUERY, it stores the upstream clusterhead node ID into the routing table, and re-broadcasts the packet to its cluster members with small power and its neighbor cluster heads with big power, and examines whether itself and its cluster members are destination nodes. If itself is the destination node, the clusterhead node broadcasts the JOIN REPLY to the source clusterhead, If its cluster members are the destination nodes, then its cluster members broadcast the JOIN REPLY to it.

When a cluster head node receives a no duplicate JOIN REPLY, it checks if the next clustered node ID in the package matches its own ID. If it does not, it discards the package; If it does, the clusterhead node realizes that it is on the path to the source and thus is part of the forwarding group. It then sets the Forwarding Group Flag(FG_FLAG) and broadcast with big power its own JOIN REPLY built upon matched entries. The JOIN REPLY is thus propagated by each forwarding group member composed cluster heads until it reaches the multicast source clusterhead via the shortest path.

When a multicast source clusterhead receives a nonduplicate JOIN REPLY, it finds that itself is the source ID of JOIN REPLY, then it broadcasts with small power the JOIN REPLY to its cluster members. This process constructs (or updates) the routes from sources to destination nodes and builds a mesh (the "forwarding group") which is constructed by source, destination and clusterhead nodes. In the CODMRP, if a multicast source wants to leave the multicast group, it only stops broadcasting the JOIN QUERY; if a receiver wants to leave the multicast group, it only stops broadcasting the JOIN REPLY. A forwarding group member will be lowered to a non forwarding group node if it is not updated before the overtime. Moreover, the CODMRP adopts the passive acknowledgments mechanism in order to assure the reliable transmission.

3.3 Security-level based Adaptive fuzzy System (SAFMR)

3.3.1 Adaptive Fuzzy System (AFS)

Adaptive fuzzy multicast routing (AFMR) is solve reclustering delay in MANETs. Our proposed protocol is three phases; cluster based multicast tree formation, localized clustering and data transfer. The cluster formation is by the calculating the weighted factor of each node has to become the cluster-head by considering two fuzzy memberships like its remaining battery capacity, and its degree of mobility node with respect to the entire cluster.

The nodes send data to the respective cluster -heads, which in turn compresses the aggregated data and transmits it to the group members. For a MANET we make the following assumptions:

- Due to node mobility cluster tree formation and cluster head selection is consider heavy control overhead.
- Location based cluster evaluation is considering for future multicast routing.

In our protocol approach, Considering MANET'S are meant to be deployed over a geographical area with the main purpose of sensing and gathering information, we assume that nodes have minimal mobility, thus sending the location information during the initial setup phase is sufficient.

3.3.2 Adaptive fuzzy logic based security-level

In this section, an adaptive fuzzy logic based Security-Level algorithm is presented. To simplify the model, the following assumptions are made:

(1) The IEEE 802.11 standard and WEP (Wired Equivalent Privacy) [3] are used in MANETs.
(2) The links are bidirectional.

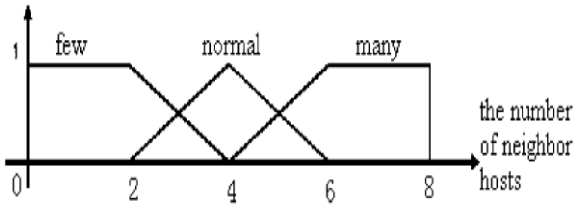

Fig. 1. Membership function of fuzzy variable *n*

The security afforded by the algorithm relies on the difficulty of discovering the secret key through a brute-force attack. We discuss the correlative factor of MH's Security-Level:

(1) The longer the secret key is, the stronger to withstand serious brute force attack. There are two kinds of keys in IEEE 802.11 standard: 128-bits key and 40-bits key. A mobile host using a 128-bits key is more secure than a mobile host using a 40-bits key.

(2) The more quickly the secret key changes, the more secure the mobile host is. It is more difficult to decipher the key in a shorter time. A mobile host changing secret key frequently is more secure than a mobile host using a constant secret key.
(3) The more neighbor hosts the mobile host has, the more potential attacker. That is, the possibility of being attacked is larger.

There are many other factors to affect the security of mobile hosts, e.g., bandwidth. The Security-Level of mobile hosts is a function with multiple variables and affected by more than one condition.

Here a fuzzy logic system is defined [2]. Inputs of the fuzzy logic system are the length of the secret key *(l)*, the frequency of changing keys *(f)* and the number of neighbor hosts *(n)*. Output of the fuzzy logic system is the Security-Level of MH *(S)*. It is assumed that the three factors are independent with each other. The relationship of them is as follows:

$$S \propto l \cdot f \cdot \frac{1}{n}. \qquad \text{----------(1)}$$

It means that the Security-Level ofMH is in direct proportion to the length of the key and the frequency of changing keys, in inverse proportion to the number of neighbor hosts. The *S* value is updated by the fuzzy logic system. When the key length is short, the Security-Level of MH should be low; otherwise the Security-Level of MH should be high.

- The input fuzzy variable "the number of neighbor hosts" has three fuzzy sets—few, normal andmany.The membership function of *n* is illustrated in Fig. 1.
- The input fuzzy variable "the length of the secret key" has two fuzzy sets—short and long. The membership functions of *l* is showed in formulation (2)

$$l = \begin{cases} short & \text{the key is 40 bits,} \\ long & \text{the key is 128 bits.} \end{cases} \qquad \text{----------(2)}$$

- The input fuzzy variable "the frequency of changing keys" has two fuzzy sets—slow and fast. The membership functions of *f* is showed in formulation (3)

$$f = \begin{cases} slow & \text{the secret key is constant,} \\ fast & \text{the secret key is variable.} \end{cases} \qquad \text{----------(3)}$$

- The output fuzzy variable "the Security-Level of MH" has five fuzzy sets -lowest, low, normal, high, highest.

Table 1
Fuzzy logic system rules

Input			Output
l	*f*	*n*	*S*
Short	Slow	Few	Low
Short	Slow	Normal	Lowest
Short	Slow	Many	Lowest
Short	Fast	Few	Normal
Short	Fast	Normal	Low
Short	Fast	Many	Low
Long	Slow	Few	High
Long	Slow	Normal	Normal
Long	Slow	Many	Low
Long	Fast	Few	Highest
Long	Fast	Normal	High
Long	Fast	Many	High

It should be noted that modifying the membership functions will change the sensitivity of the fuzzy logic system's output to its inputs. Also increasing the number of fuzzy sets of the variables will provide better sensitivity control but also increases computational complexity of the system. Table 1 show the rules used in the fuzzy logic system.

IV. FUZZY CLUSTER FORMATION

We evaluate the cluster formation is based on the following two fuzzy membership functions:

- Node Remaining Energy - energy level available in each node, designated by the fuzzy variable energy
- Node Mobility - a value which classifies the nodes based on how central the node is to the cluster, designated by the fuzzy variable mobility.

The linguistic variables used to represent the node energy and node concentration, are divided into three levels: low, medium and high, respectively, and there are three levels to represent the node mobility: close, adequate and far, respectively. The outcome to represent the node cluster-head election chance was divided into six levels: small, very small, rather medium, medium, large, and very large. The fuzzy rule base currently includes rules like the following: if the energy is high and the centrality is close then the node's cluster-head election chance is very large. All the nodes are compared on the basis of chances and the node with the maximum chance is then elected as the cluster-head. Each node in the cluster associates itself to the cluster-head and starts transmitting data.

To do this, we averaged the centroids of all the responses for each rule and used this average in place of the rule consequent centroid. Doing this leads to rules that have the following form:

IF remaining battery capacity (w1) of node F1 1, and its degree of mobility (x3) is Fl 3, THEN the possibility that this node will be elected as a cluster head (ch) is cl avg, where l == 1, 2, 3...9.

$$C^{l} = \frac{\sum_{i=1}^{6} \omega_i^{l}}{\frac{c_i^{l}}{\sum_{i=1}^{6} \omega_i^{l}}} \quad \text{----------(4)}$$

4.1 Kalman Filtering based Location Management

Kalman filter is a well known tool to estimate a linear system's past, present or future state by using a time sequence of measurements of the system state and a statistical model that characterizes the system and measurement errors, along with initial conditions. Extended Kalman filter can also be used to provide higher prediction accuracy, but much calculation overhead may be involved.

There are several advantages of using Kalman filters. First, prediction using the basic Kalman filter is extremely fast and requires little memory. This is essential for the real time requirements. Second, an error estimate is associated with each prediction. Third, these predictions can be computed recursively, bounding the time and memory needed for computation. While the Kalman filter and its extensions are commonly used for prediction and tracking, they have been primarily applied to objects with known or fixed dynamics.

In general, location management may follow two strategies namely location updating and location prediction. Location updating is a passive strategy in which each CH periodically broadcasts its position to the neighboring nodes. Location prediction is a dynamic strategy in which cluster members proactively estimate the location of their neighboring CH. In this case, the tracking efficiency depends on the accuracy of the mobility model and on the efficiency of the prediction algorithm.

We use Voronoi diagrams to limit the scope of CH initiated location updates. The Voronoi diagram of a set of discrete sites partitions the plane into a set of convex polygons such that all points inside a polygon are closest to only one site. For their properties and simplicity of computation, Voronoi diagrams have been widely applied to the WSNs.

The Voronoi cell of CH (V_i) contains all points of the plane that are closer to V_i than to any other CH in the network. A sensor S is said to be dominated by CH *V* if its location lies in the Voronoi cell of *V*. Every CH is responsible for location updates to sensors in its Voronoi cell, and regulates its power so as to limit interference beyond the farthest point in its Voronoi cell. Each sensor will thus expect to receive location updates from the CH it is dominated from. With respect to flooding, the energy consumption for location updates is drastically reduced. With a flooding-like protocol, each CH sends a message to its N neighboring sensors. Each CH can transmit data within its Voronoi cell, therefore no forwarding is needed and hence the energy consumption is in the order of the number of sensors.

The Kalman filter provides a computationally efficient set of recursive equations to estimate the state and can be proven to be the optimal filter in the minimum square sense. The joint use of Kalman filter at the sensor and CH side enables reducing the number of necessary location updates. In fact, the filter is used to

estimate the position at the CH based on measurements, which is a common practice in robotics, and to predict the position of the CH at the sensors, thus reducing the message exchange.

The position observed by the CH at step say m is related to the state by the measurement equation

$$OP_i^k = Hx_i^k + Cn_i^k \quad \text{---------- (5)}$$

Where $OP_i^k = [\, OP_i^{k,x}, OP_i^{k,y} \,]$ represents the observed position of the CH at step k,

$$H = \begin{bmatrix} I & 0 \end{bmatrix}, C = \begin{bmatrix} o \\ I \end{bmatrix}$$

The position of CH can be estimated and predicted at the sensors in its Voronoi cell, based on the measurements OP_i^k taken at the CH and broadcast by the CH.

By using the kalman filter we predict the location updates of all clustered groups and each CH gets their neighbors locations. Also each CH exchanges their position information with all its cluster members. The CH keeps tracks of the nodes position and also predicts the new CH based on mobility. Further to that the CH also predicts the future directions of all its neighbors. Since in our approach the future CH is predicted earlier and it reduces the re-clustering timing.

V. Implementation

5. 1. Simulation Model and Parameters

To evaluate the performance of Secure AFMR, we simulate the fuzzy clustering in a variety of mobile network topologies in NS-2 [18] and compare it with CODMRP [4] and CBRP [5].

As far as multicast communication is concerned, implement the clustering and location management scheme described in Section 3. The MAC layer is based on IEEE 802.11. The monitored area is a 500 m 500 m square, with 50 randomly deployed nodes similar to that used in the previous experiments, but all the nodes move according to the RWP model. The maximum transmission range of nodes is set to 50 m and the bandwidth to 250 Kbit/s. We perform terminating simulations that last 150s, average over different random topologies. The mobility experiment consisted of 5 traffic sources and 20 receivers chosen randomly. Each source transmitted 10 Kbps and thus the overall network load was 50 Kbps. The minimum node speed is 1 m/s and we vary the maximum speed to change the mobility of the network.

5. 2. Performance Metrics

We compare the performance of our proposed SAFMR with the in [13]. We evaluate mainly the performance according to the following metrics.

Average End-to-End Delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Average Packet Delivery Ratio: It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

Bandwidth: It is the measure of received bandwidth for all traffic flows.

Dropping Probability: Its is the measure of dropping in multicast communication to evaluate the security concern.

5. 3. Performance Evaluation

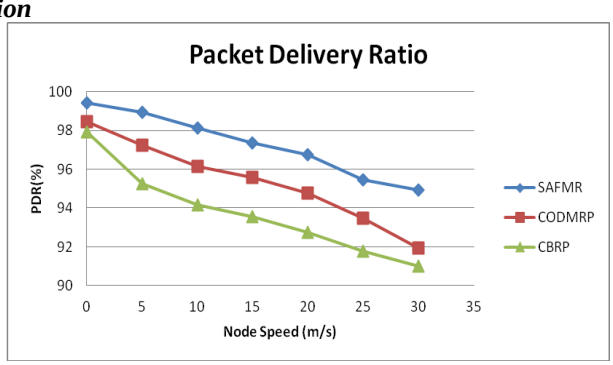

Fig.2 Packet Delivery Ratio

Fig. 2 highlights the effectiveness of the delivery ratio utilized by SAFMR. Even when the maximum node speed increases 0 to 30 m/s, SAFMR still enables nearly 99 percent of the packets to reach the destination while the delivery ratios of CODMRP and CBRP both decrease significantly. We notice that at lower speeds the difference in packet delivery ratio is between5% and 7%.However,at higher speeds the gap in packet delivery ratio starts widening.

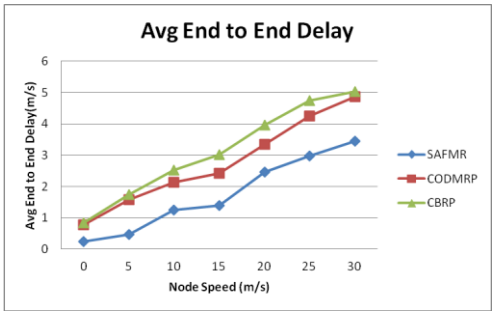

Fig3 Avg End to End Delay

When Fig 3, we can see that SAFMR delivers as many as possible packets at extremely low delay. The near cluster optimum path length contributes to the efficiency. On the other hand, the mitigation of prediction of future cluster head collaboration reduces the end-to-end delay significantly with comparing of CODMRP and CBRP.

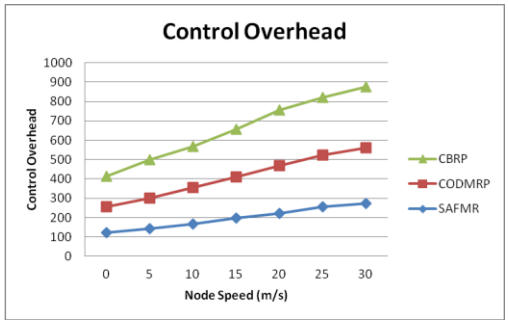

Fig 4 Control Packets Overhead

As for the overhead, Figs.4 and 13f show that SAFMR excellent performance is not at the cost of increased re-clustering. Note that AFMR overhead does not change with mobility as only data header packets contribute to overhead.

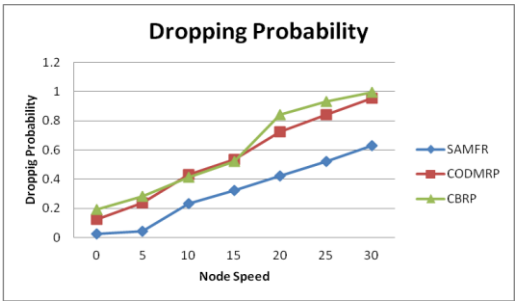

Fig 5 Dropping Probability

From fig5 dropping is for security concern , when comparing this SAMFR is less amount of packet drops with leads to CODMRP and CBRP.

VI. Conclusion

In this paper, we address the problem of reliable and secure multicast data delivery in highly dynamic mobile ad hoc networks. We reported on simulation-based experiments evaluating our proposed approaches fuzzy clustering to secure multicast communication in mobile ad hoc networks (MANETs), namely SAFMR and comparing with existing protocols namely CODMRP and CBRP. We present a cluster head election scheme

using fuzzy logic system for mobile ad hoc wireless networks. Three descriptors are used its remaining battery capacity, and its security level of mobility. In this approach nodes can dynamically switch routing mechanisms based on their perception of the network conditions with security. KalmanR filter used to predict the future clusters and cluster heads, its increasing the performance of clustering phases and reduce the re clustering delay and control packets The efficacy of the involvement of future cluster head prediction against node mobility, as well as the overhead due to fuzzy clustering is analyzed. Through simulation, we further confirm the effectiveness and efficiency of SAFMR: high packet delivery ratio is achieved while the delay and overhead are the lowest with security manner.

References

[1] Shekhar H M P, Arun Kumar M A, and K S Ramanatha,(2005) "Mobile agents aided multicast routing in mobile ad hoc networks" Advanced Communication Technology, 2005, ICACT 2005.

[2] Zaiba Ishrat, (2011) " Security issues, challenges & solution in MANET" in International Journal of Computer Sci ence & Technology Vol. 2, Iss ue 4, Oct . - Dec. 2011

[3] R. Pandi Selvam and V.Palanisamy, (2011) "AN EFFICIENT CLUSTER BASED APPROACH FOR MULTI-SOURCE MULTICAST ROUTING PROTOCOL IN MOBILE AD HOC NETWORKS" International Journal of Computer Networks & Communications (IJCNC) Vol.3, No.1, January 2011

[4] XUE-MEI SUN, WEN-JU LIU, ZHI-QIANG ZHANG and YOU ZHAO,(2006) "CODMRP: Cluster-based On Demand Multicast Routing Protocol "Wireless Communications, Networking and Mobile Computing, 2006. WiCOM 2006

[5] XUE-MEI SUN, WEN-JU LIU, ZHI-QIANG ZHANG and YOU ZHAO,(2006)" CODMRP: Cluster-based On Demand Multicast Routing Protocol" Wireless Communications, Networking and Mobile Computing, 2006. WiCOM 2006.

[6] Bey-Ling Su, Ming-Shi Wang and Yueh-Ming Huang,(2008) "Fuzzy logic weighted multi-criteria of dynamic route lifetime for reliable multicast routing in ad hoc networks" Expert Systems with Applications: An International Journal Volume 35 Issue 1-2, July, 2008

[7] Muhammad Arshad Ali and Yasir Sarwar,(2011) "Security Issues regarding MANET (Mobile Ad Hoc Networks): Challenges and Solutions" in School of Computing, Blekinge Institute of Technology March 2011

[8] Roberto Carlos Hincapi, Blanca Alicia Correa and Laura Ospina,(2006) "Survey on Clustering Techniques for Mobile Ad Hoc Networks" January 20, 2006; revised April 18, 2006.

[9] Jing Nie, JiangchuaWen, Ji Luo, Xin He and Zheng Zhou, (2006) "An adaptive fuzzy logic based secure routing protocol in mobile ad hoc networks" on Fuzzy Sets and Systems Volume 157, Issue 12, 16 June 2006.

[10] Rui Huang and Gergely V. Z aruba,(2006) "Location Tracking in Mobile Ad Hoc Networks using Particle Filter" Journal of Discrete Algorithms Volume 5 Issue 3, September, 2007.

[11] Zhaowen Xing, Le Grunewald and K.K. Phang,(2008) "A Robust Clustering Algorithm for Mobile Ad Hoc Networks" December 2008.

[12] J. D. Mallapur, S. S. Manvi and D. H. Rao,(2009) "A Fuzzy Based Approach for Multicast Tree Computation in Wireless Multimedia Networks" ISSN 1746-7659, England, UK Journal of Information and Computing Science Vol. 4, No. 2, 2009, pp. 083-092

[13] Byung-Jae Kwak, Nah-Oak Song and Leonard E. Miller,(2003)" A Mobility Measure for Mobile Ad-Hoc Networks" Communications Letters, IEEE Issue Date: Aug. 2003

[14] Dewan Tanvir Ahmed, (2005) "Multicasting in Ad Hoc Networks" CSI5140F Wireless Ad Hoc Networking Professor Ivan Stojmenovic Ottawa, Ontario, Canada, Fall 2005

[15] Shahram Nourizadeh, Y.Q. Song and J.P. Thomesse, (2007) "A Location-Unaware Distributed Clustering Algorithm for Mobile Wireless Networks Using Fuzzy Logic"FET2007 Toulouse – France

[16] ZHAO Chun-Xiao and WANG Guang-Xing, (2004) "Fuzzy-Control-Based Clustering Strategy in MANET" Proceedings of the 5th World Congress on Intelligent Control and Automation, June 15-19, 2004,

[17] K. Venkata Subbaiah and Dr. M.M. Naidu, (2010) "Cluster head Election for CGSR Routing Protocol Using Fuzzy Logic Controller for Mobile Ad Hoc Network" Int. J. of Advanced Networking and Applications 246 Volume: 01, Issue: 04, Pages: 246-251 (2010)

[19] B.G.Obula Reddy, Maligela Ussenaiah, (2012) "An Adaptive Fuzzy System in Large Scale Mobile Ad Hoc Networks" IJCSMS International Journal of Computer Science and Management Studies, Vol. 12, Issue 02, April 2012.

[20] Harshavardhan Kayarkar, "A Survey on Security Issues in Ad Hoc Routing Protocols and their Mitigation Techniques" International Journal of Advanced Networking and Application, Vol. 03, Issue 05, pp. 1338-1351, March-April, 2012

[21] Zhongwei Zhang, "A Novel Secure Routing Protocol for MANETs" ISBN 978-953-307-402-3, January 30, 2011 under CC BY-NC-SA.

[22] The Network Simulator ns-2, http://www.isi.edu/nsnam/ns,2011.

Mr. B.G.obula Reddy obtained his Bachelors degree in Computer Science and Engineering from J.N.T.U Anantapoor INDIA in 2005 and his Masters degree in Software Engineering from Avanthi Institute of Engineering, Makavarapalem(Village), Narsipatnam(Mandal), INDIA in 2008. He is pursuing the Doctoral degree in Computer Science and Engineering from Rayalaseema University, Karnool – INDIA.He has 9 years of teaching experience and presently working as an Assoc.Professor in the Department of Information Technology of Lakireddy Balireddy College of Engineering, Mylavaram, Andhra Pradesh, India.

Mr. B.G.obula Reddy is a member of various professional societies like IEEE and ISTE.
Dr.Maligela Ussenaiah, working as Assistant Professor of Department of Computer Science with four years of experience in , Vikrama Simhapuri Unicversity, Nellore, Andhra Pradesh -524001. He is supervising for three Doctoral thesis in the areas of computer networks, mobile wireless networks, Data warehousing & mining and image processing