The effect of Mobility Models on a Secured Enhanced and Reliable Ad Hoc Multicasting Protocol

Sherif M. Badr, Ph.D
College of Computer science, Modern Academy
Cairo, Egypt

ABSTRACT

Mobile Ad-hoc networks are characterized as networks without any physical connections. In these networks there is no fixed topology due to the mobility of nodes, interference, multi-path propagation and path loss. One particularly challenging environment for multicast is a mobile ad-hoc network (MANET), where the network topology can change randomly and rapidly, at unpredictable times. As a result, several specific multicast routing protocols for MANET have been proposed. [1].

The objective of this paper is to study the effects of mobility models on the new proposed secured and enhanced reliable Ad Hoc Multicasting Protocol (SERAMP). SERAMP is a new technique to be used for Multicasting in Ad-Hoc Networks and to solve the security problems associated with multicasting in Ah-Hoc Networks. The proposed protocol added two parameters to secure the network, the first parameter is the encryption of the message using random key for the selection of the encryption algorithm, and the second parameter is to use the same random key to calculate the authentication code of the message [2].

This paper applies the proposed secured protocol for the previous work and a comparative study has been made between the proposed secured enhanced and reliable Ad Hoc Multicasting Protocol under the two mobility models, Random Way Point Mobility Model and Reference Point Group Mobility Model.

Keywords

Ad Hoc networks, Ad Hoc multicasting, routing security, Mobility Models.

1. INTRODUCTION

Traditional network routing techniques fall short when asked to provide mobile hosts with a reliable connection in a wireless environment. Wireless links allow for a high degree of mobility, but have two obstacles; first, they support low data rates second, they have a limited range that can lead to frequent link failures. These two obstacles necessitate a new approach to routing protocols. An emerging class of networks, known as Mobile Ad Hoc Networks [3], promises to provide connectivity among hosts in a highly volatile environment, while minimizing routing overhead.

A mobile ad hoc network (MANET) is an autonomous system of mobile hosts (also serving as routers) connected by wireless links, the union of which forms a communication network modelled in the form of an arbitrary communication graph [4]. In cellular networks, communications between two mobile nodes completely rely on the wired backbone and fixed base stations. In a MANET no such infrastructure exists, and the network topology may dynamically change in an unpredictable manner since nodes are free to move.

Multicasting is the transmission of datagram's to a group of hosts identified by a single destination address and hence is intended for group-oriented computing. In MANETs, multicasting can efficiently support a variety of applications that are characterized by close collaborative efforts. It has a self-organizing capability and can be effectively used where other technologies either fail or cannot be deployed effectively. Advanced features of wireless mobile systems, including data rates compatible with multimedia applications, global roaming capability, and coordination with other network structures, are enabling new applications. Therefore, if we can efficiently combine the features of a MANET with the usefulness of multicasting, it will be possible to realize a number of envisioned group-oriented applications [5].

Due to the issues such as shared physical medium, lack of central management, limited resources, no fixed and highly dynamic topology, ad hoc networks are much more vulnerable to security attacks. Hence it is very necessary to find security solutions, which are much more difficult to develop than in wired networks. As well as in wired networks, the following major security goals should be satisfy confidentiality, integrity, availability, authentication, non-repudiation.

The objective of this Thesis is to achieve a secured and enhanced real time transmission of multicasting data transmission and study the effects of the mobility models on the proposed protocol.

2. MULTICAST ROUTING IN MOBILE AD HOC NETWORKS

We can classify the multicast routing protocols into three categories: Based on topology, based on initialization of the multicast session, and based on the topology maintenance mechanism. Figure 1 shows the classification of Ad Hoc multicast routing protocols [6]. In this section we discuss multicast routing protocols proposed for MANETs. For simplicity, we can classify these into two categories based on how routes are created to the members of the group: Tree-based approaches and Meshed-based approaches [7][8].

2.1 Tree-Based Multicast Routing Protocols:

Tree-based multicasting is a well-established concept used in several wired multicast protocols to achieve high multicast efficiency. In tree-based multicast protocols, there is only one path between a source-receiver pair. The main drawback of these protocols is that they are not robust enough to operate in highly mobile environments. Tree-based multicast protocols can be classified into two types: source-tree-based multicast routing protocols and shared-tree-based multicast routing protocols. In a source-tree-based protocol, a single multicast tree is maintained per source, whereas in a shared-tree-based protocol, a single tree is shared by all the sources in the multicast group. Shared-tree-based multicast protocols are more scalable compared to source-tree-based multicast protocols.

2.2 Mesh-Based Multicast Routing Protocols:

In ad hoc wireless networks, wireless links break due to the mobility of the nodes. In the case of multicast routing protocols, the path between a source and receiver, which consists of multiple wireless hops, suffers very much due to link breaks. Multicast routing protocols which provide multiple paths between a source-receiver pair are classified as mesh-based multicast routing protocols. The presence of multiple paths adds to the robustness of the mesh-based protocols at the cost of multicast efficiency. There are several advantages to Ad Hoc wireless mesh networks. Because each device only needs to transmit to the next closest device, this decentralized network can decrease costs by reducing the number of access points and wired connections that are necessary. These mesh networks can also be reliable: if one device leaves the network or has a hardware failure, the path can switch to a different route [9].

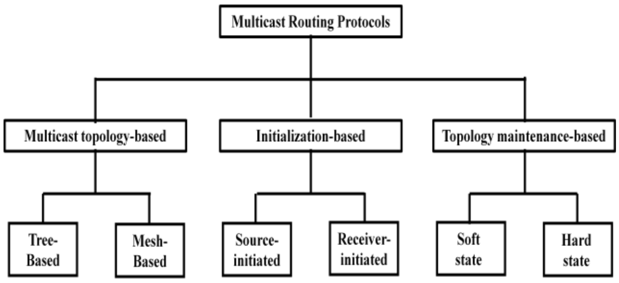

Figure 1 Classification of Ad Hoc multicast routing protocols.

2.3 Efficient and Robust Multicast Routing in Mobile Ad Hoc Networks (PUMA):

Uses a receiver initiated approach in which receivers join a multicast group using the address of a special node without the need for network-wide flooding of control or data packets from all the sources of a group. PUMA eliminates the need for a uni-cast routing protocol and the pre-assignment of cores to multicast groups.

PUMA implements a distributed algorithm to elect one of the receivers of a group as the core of the group, and to inform each router in the network of at least one next-hop to the elected core of each group. The election algorithm used in PUMA is essentially the same as the spanning tree algorithm introduced by Perlman for internetworks of transparent bridges [10].

Every receiver connects to the elected core along all shortest paths between the receiver and the core. All nodes on shortest paths between any receiver and the core collectively form the mesh. A sender sends a data packet to the group along any of the shortest paths between the sender and the core. When the data packet reaches a mesh member, it is flooded within the mesh, and nodes maintain a packet ID cache to drop duplicate data packets.

PUMA uses a single control message for all its functions, the multicast announcement. Each multicast announcement specifies a sequence number, group ID; core ID, the distance to the core, a mesh member flag that is set when the sending node belongs to the mesh, and a parent that states the preferred neighbour to reach the core. Successive multicast announcements have a higher sequence number than previous multicast announcements sent by the same core.

With the information contained in such announcements, nodes elect cores, determine the routes for sources outside a multicast group to uni cast multicast data packets towards the group, notify others about joining or leaving the mesh of a group, and maintain the mesh of the group. For the same core ID, only multicast announcements with the highest sequence number are considered valid. For the same core ID and sequence number, multicast announcements with smaller distances to the core are considered better. When all those fields are the same, the multicast announcement that arrived earlier is considered better. After selecting the best multicast announcement, the node generates the fields of its own multicast announcement. The connectivity list stores information about one or more routes that exist to the core.

3. SECURITY PROTOCOLS FOR AD HOC WIRELESS NETWORKS

As the approach of ad hoc networking varies from traditional networking approaches, the security aspects that are valid in the conventional wired networks are not fully applicable in the context of ad hoc networks. In ad-hoc networks, adverse nodes can freely join the network, listen to and/or interfere with network traffic, and compromise network nodes leads to various network failures [11].

While the basic security requirements such as confidentiality and authenticity remain, the ad hoc networking approach restricts the set of applicable security mechanisms to be used since the level of security and the performance are related to each other and must be carefully balanced.

3.1 Passive Attack:

A passive attack does not disrupt the operation of the network; the adversary snoops the data exchanged in the network without altering it. Here, the requirement of confidentiality can be violated if an adversary is also able to interpret the data gathered through snooping. Detection of passive attacks is very difficult since the operation of the network itself does not get affected. One way of overcoming such problems is to use powerful encryption mechanisms to encrypt the data being transmitted, thereby making it impossible for eavesdroppers to obtain any useful information from the data overheard.

3.2. Active Attacks:

Unlike the passive attacks, an active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network. Active attacks may allow a malicious node to delete or inject to the network traffic erroneous messages, modify messages and impersonate as another node, hence violating availability, integrity, authentication and non-repudiation. As opposed to passive attacks, active attacks can be detected and limited with the utilization of various schemes.

4. SECURE AD HOC ROUTING PROTOCOLS

The objectives of secure multicast are preserving authentication and confidentiality for all group communication. This requires a group key management solution to distribute and to maintain cryptographic with registered group members. Most research on secure group communication has focused on the architecture of secure groups and on how to distribute and manage group key [12]. The following sections make a brief overview of possible security solutions in a MANET with their characteristics:

4.1. ARAN (Authenticated Routing for Ad hoc Networks)

Is an on-demand security routing protocol that makes use of cryptographic certificates to make the routing secure. It protects an ad hoc environment against malicious actions from third parties and peers. ARAN consists of a preliminary certification process, a mandatory route instantiation process that guarantees end-to-end authentication and an optional stage for providing secure shortest path. ARAN introduces authentication, message integrity and non-repudiation as the main thing for a minimal security policy in an ad hoc environment. ARAN makes use of a trusted certificate server. All nodes that want to participate have to have a fresh certificate from the trusted server and also know the public key of the trusted server. The key distribution must be done in advance. [13]

4.2. Ariadne:

Is a secure on-demand routing protocol based on Dynamic Source Routine (DSR) and TELSA authentication protocol. Ariadne relies on symmetric cryptography and performs by message authentication code (MAC) through intermediate nodes. Ariadne doesn’t need a trusted hardware or powerful processes. It only uses symmetric cryptography, which is quite efficient compared to asymmetric. The routing message in Ariadne can be authenticated by the following three types: shared secrets between each pair of nodes, shared secrets between communicating nodes combined with broadcast authentication, and digital signatures, respectively. Besides, there are two advantages in Ariadne: one is that it can defend adversaries or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and the other is that it also can prevent ample types of DoS attacks. The threats that are treated in Ariadne are malicious nodes that fabricate and modify routing information. There is also an advanced version of Ariadne that can deal with the threat of the wormhole attack, but then the network system has to be precisely time synchronized. [14]:

4.3. LHAP (Lightweight Hop-by-hop Authentication Protocol)

Is designed as a general network access protocol, which provides authentication for every packet. It prevents unauthorized nodes from being able to inject packets into the network. LHAP is transparent to and independent of the routing protocol. It can be implemented under any routing protocol and handle the authentication without the routing protocols knowledge. It resides between the data link layer and the network layer and make up for the lack of the security in the routing protocol. [15]

4.4. SAR (Security-aware Ad hoc Routing)

Is an extension to existing on demand ad hoc routing protocols? To ensure security in a wireless network it uses a generalized framework. The framework gives nodes different level of security by assigning them trust values. This means that when a packet is sent, it is assigned a trust value and certain security attributes, which is done by the user. Depending on the trust value the packet can only be routed through nodes with equal or greater trust value. If a node has lower security level it simply discards the packet. In case there isn’t a node in the network with the right level of security, then the packet can’t be send, unless the packets level of security is altered. [16].

4.5. SEAD (Secure Efficient Ad hoc Distance vector routing protocol)

Is a part based on the design of the Destination-Sequenced Distance-Vector routing protocol. It uses a one-way-hash function and asymmetric cryptography operations. This gives SEAD the ability to be used by nodes with limited CPU processing capability and to defend against Denial-of-Service attacks like forcing nodes to consume much bandwidth or processing time. To avoid long-lived routing loops and to defend against the replay attack SEAD uses destination numbers. Authentication is used in SEAD both to authenticate the routing information and to ensure that the information originates from the correct node. [17]

4.6. SLSP (Secure Link State Protocol)

Is a secure routing protocol that can be stand-alone or fit in a hybrid network framework together with a reactive protocol? Its goals are to, with a proactive approach, give correct up-to-date and authentic link state information in terms of discovery and distribution. It is robust against threats like Byzantine behaviour and failure of individual nodes. [18]

4.7. SMT (Secure Message Transmission)

The goal in SMT is to secure data forwarding on already discovered routes whether or not the routes contain malicious nodes. SMT requires a Security Association between the source and destination. The relationship can be achieved by letting one of the communicating nodes know the public key of the other communicating node. As a result there is no need for cryptographic operations in the nodes between the communicating partners. [19]:

4.8. SPAAR (Secure Position Aided Ad hoc Routing):

SPAAR targets a specific environment. It’s designed to be used in a high-risk tactical MANET and provides *authentication*, *non-repudiation*, *confidentiality* and *integrity*, which are the necessary elements for this environment. The goal is to satisfy a number of security requirements and in so doing the protocol safe for its environment [20]. For threats like eavesdropping, impersonation, message replay and message distortion SPAAR uses encryption. Every node has a public/private key pair, a signed certificate that binds the public key to the node and the trusted certificate server public key.

4.9. SRP (Secure Routing Protocol):

Is implemented as an extension to a reactive protocol. It can be applied to several existing routing protocols and it guarantees correct route discovery because of security association. The attacks that are treated in SRP are attacks that try to disrupt the route discovery process. It provides correct routing information in other words, factual, up-to-date and authentic connectivity information. The requirement is that when a pair of nodes wishes to communicate in a secure manner, the end nodes must have a security association, because only the end nodes need to perform cryptographic operations. [21]

4.10. TESLA (Time Efficient Stream Loss-tolerant Authentication):

The main idea of the basic TESLA protocol is that a MAC is attached to every packet. This MAC is computed using a key *k* that only the sender knows. When the receiver gets the packet it buffers it and waits for the sender to disclose the key *k* so it can authenticate the packet. If the receiver doesn't get the packet in time, it is discarded. Thus attaching a single MAC to every packet makes it possible to provide source authentication. The only thing that has to be done in advance is for the receiver and sender to synchronize their clocks. The synchronization doesn't need to be precise. It's sufficient that they are loosely time synchronized. The basic version of TESLA has a low computation and communication overhead. It also has perfect loss robustness, which means that every packet that arrives in time will eventually be authenticated as long as some later packet arrives. [22]

4.11. SAODV (Secure Ad Hoc on Demand Distance Vector):

SAODV is an extension of AODV routing protocol and similar to ARAN. The requirement for this protocol is the assumption that each node of the Ad Hoc network possesses a public and private key for asymmetric cryptography, and knows the public keys of the other nodes. The basic idea is that the originator of a control message appends a RSA signature and the hash algorithm, which are used to represent the message in the packet header. Although authentication and non-repudiation are provided, an adversary still can add the hop count to fake a routing packet. Furthermore, SAODV also needs high computation power. [23]

5. Mobility Models in Ad Hoc Networks

A mobility model is a representation of a certain real or abstract world that contains moving entities. A mobility model is usually used to describe the mobility of an individual subscriber. Sometimes it is used to describe the aggregate pattern of all subscribers. A mobility model should attempt to mimic the movements of real MNs. Changes in speed and direction must occur and they must occur in reasonable time slots. For example, we would not want MNs to travel in straight lines at constant speeds throughout the course of the entire simulation because real MNs would not travel in such a restricted manner [24].

The mobility of nodes is one of the most important factors in the performance evaluation of MANETs. The protocol performance is highly influenced by them. The understanding of each observed mobility pattern can help to improve the network behaviour. The following discussion attempts a brief overview of the commonly used mobility model, for entity mobility models and for group mobility models, to analyse design systems in wireless ad hoc networks:

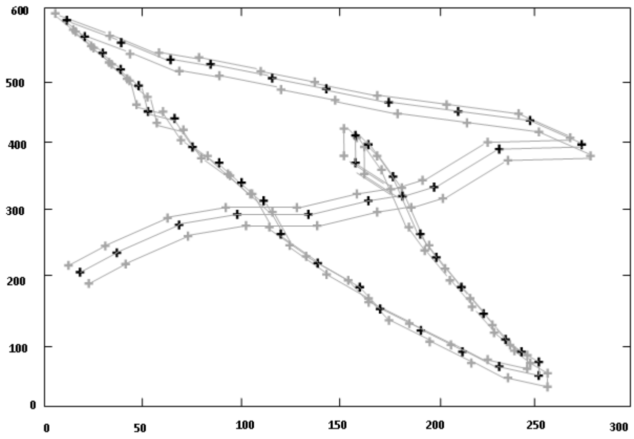

Fig. 2 Traveling pattern of RWMP

5.1. Entity Mobility Models

There several mobility models that represent mobile nodes whose movements are independent of each other (i.e., entity mobility models), as Random Direction Mobility Model, Random Walk Mobility Model, Gauss-Markov Model, Freeway Mobility (FW) Model, Manhattan Mobility (MH) Model, and Random Waypoint (RW) Mobility Model. In this Section, we present a brief discussion of the more detail.

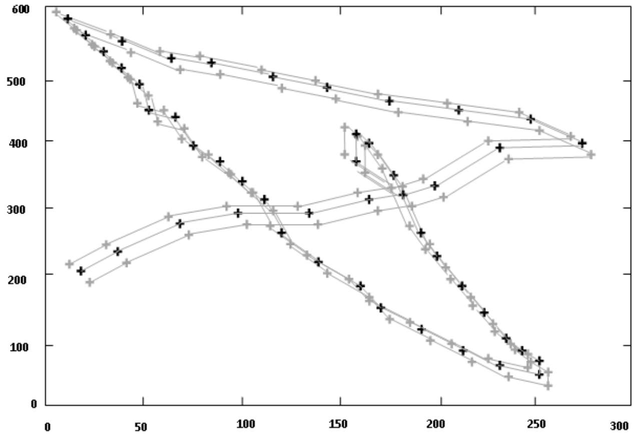

Fig. 3: Traveling pattern of RPGM

5.2. Random Waypoint (RW) Mobility Model

Is the most widely used and studied mobility model in the many simulation studies of ad hoc routing protocols. In this model each node is assigned an initial position uniformly distributed within a region (rectangular region). At every instant, a node randomly chooses a destination called waypoint uniformly inside the region and moves towards it with a constant velocity chosen randomly from [0,Vmax], where Vmax is the maximum allowable velocity for every mobile node. After reaching the destination, the node stops for a duration by the 'pause time' parameter. Then, it again chooses a random destination and repeats the whole process again until the simulation ends. All nodes move independently of each other at all times.

To avoid the transient period from the beginning, one solution is to choose the nodes' initial locations and speeds according to the stationary distribution; another one is to discard the initial time period of simulation to reduce the effect of such transient period on simulation results. Figure 2 shows the travelling pattern of an MN using the Random Waypoint Mobility Model.

We note that the movement pattern of an MN using the Random Waypoint Mobility Model is similar to the Random Walk Mobility Model if pause time is zero and [0, MAXSPEED] = [speedmin, speedmax].This is a simple mobility model and is hence adopted by many authors in their simulation studies.

5.3. Group Mobility Models

Entity mobility models do not provide realistic mobility scenarios for tactical networks, where mobile troops in military battlefield communication are moving in formations. There several mobility models that represent mobile nodes whose movements are dependent on the other mobile nodes in the group (i.e., group mobility models), as Column Mobility Model, Nomadic Community Mobility Model, Pursue Mobility Model, and Reference Point Group Mobility (RPGM) Model. In this Section, we present the most general group mobility model, RPGM.

5.4. Reference Point Group Mobility (RPGM) Model

Represents the random motion of a group of MNs as well as the random motion of each individual MN within the group [25]. Each group has a logical centre (group leader) that determines the group's motion behaviour. Initially, each member of the group is uniformly distributed in the neighbourhood of the group leader. Subsequently, at each instant, every node has a speed and direction that is derived by randomly deviating from that of the group leader.

Each node deviates its velocity (both speed and direction) randomly from that of the group leader. The group motion behavior is important in some applications like ubiquitous computing, military deployment etc. The movement can be characterized as follows:

Vmember(t) = Vleader(t) + random() * SDR * max_speed
theta_member(t)=theta_leader(t)+random()*ADR*max_angle, where 0 <= SDR, ADR <= 1. SDR is the Speed Deviation Ratio and ADR is the Angle Deviation Ratio. SDR and ADR are used to control the deviation of the velocity (magnitude and direction) of group members from that of the leader. Since the group leader mainly decides the mobility of group members, group mobility pattern is expected to have high spatial dependence for small values of SDR and ADR.

6. THE PROPOSED SECURED ENHANCED AND RELIABLE AD HOC MULTICASTING PROTOCOL

It should be clear that the conservation of bandwidth is imperative to the success of any wireless network. While previous MANET multicast protocols focused only on the reductions of control overhead, the multicast protocol investigated in this study attempts to reduce the amount of bandwidth used by the network both in terms of control overhead and data rebroadcasts. It can usually be assumed that data transmission consumes more bandwidth than control overhead. Even a small decrease in data retransmissions should substantially improve network performance.

Unlike previously proposed MANET multicast algorithms, this new protocol will focuses on: Route load and Route stability/Quality [26].

The military aspects in a mobile ad hoc network are especially interesting and complicated. In a military scenario with a hostile environment there are more things to consider and harder constraints than in a MANET for educational or business purposes. Military networks are probably the most difficult ad hoc network to handle when it comes to mobility management and mobile communication. There are a number of things to take into concern.

The routing itself has to be reliable and accurate, with issues concerning bandwidth and radio range putting in consideration that the shortest path may not the best path. But also the question of information security is of equal importance. The information sent through the network shouldn’t be tampered with, altered or read by unauthorized persons. These aspects are hard to combine in a MANET and there isn’t a lot of work in progress that tries to solve both routing and security problems. But the Proposed protocol applies a security protocol on an enhanced and reliable Ad Hoc multicasting protocol which should be able to:

- Detect the spiteful nodes in the network and to prevent them from participating in routing process.
- Assure that a correct route could be found, if it exists.
- Guarantee the confidentiality of network topology.
- Be stable against attacks.

The best way to solve the security problems would be, if possible, to combine several protocols in order to take advantage of the solutions for the different problems. The proposed protocol goal is to design simple and efficient mechanisms with low computation and communication overhead achieving high attack robustness. These mechanisms should be sufficiently general to allow application to a wide range of routing protocols. In what follows the basic modules of the proposed protocol will be discussed.

6.1. Algorithm:

The proposed protocol depends on the values of two tables which built-in at the trusted nodes. The first table contains the keys list available and the associated Code-Values for the encryption, the second table contains the list of the keys and the associated hash functions of the Message Authentication Code (HMAC).

6.1.1 Packet Initiation:

During the scenario the core node generates a random number (Key-Value). From the table of the Key-Values the node selects the Code-Value and encrypts the message. From the second table the node selects the Hash-Function for authentication. Apply the Authentication function on the message and calculate the Message Authentication Code. Then the node sends the message.

6.1.2 Packet Reception:

When the node receives the message it reads the Key-Value and applies the authentication function to ensure that the resultant value equals to the message authentication code otherwise reject it. Then decrypt the message using the Code-Value associated with the Key- table.

6.1.3 Packet Forwarding:

To forward the message, the node generates a random number (Key-Value). From the table of the Key-Values the node selects the code value and encrypts the message. From the second table the selects the Hash-Function for authentication. Apply the Authentication function on the message and calculate the Message Authentication Code. Then the node forwards the message.

6.2. Implementation:

Mesh establishment phase: In mesh establishment phase we use a receiver initiated approach in which receivers join a multicast group using the address of a special node (core ID), without the need of network-wide flooding of control or data packets from all the senders of a group.

Every receiver connects to the elected core along all shortest paths between the receiver and the core. All nodes on shortest paths between any receiver and the core collectively form the mesh. A sender sends a data packet to the group along any of the shortest paths between the sender and the core. When the data packet reaches a mesh member, it is flooded within the mesh, and nodes maintain a packet ID cache to drop duplicate data packets.

A single control message was used for all its functions, the multicast announcement. Each multicast announcement consists of:

- ***Sequence number:*** The sequence number in the best multicast announcement
- ***Group_ ID:*** The group ID in the best multicast announcement
- ***Core_ID:*** The core ID in the best multicast announcement
- ***Distance_ to_Core:*** One plus the distance to core in the best multicast announcement
- ***Mesh_Member:*** Receivers consider themselves mesh-members and set the mesh member flag to TRUE.
- ***Parent:*** The neighbor from which it received the best multicast announcement.
- ***X, Y:*** x-y Coordinates of the node.
- ***Node_Speed:*** The Speed of the current node.
- ***Node_Load:*** The total load of the current node.
- ***Key-Value***: Random value generated by the current node.
- ***Authentication-Code:*** Message authentication code calculated according to the algorithm of the Key-Value.

During the scenario the core node generates a random number (Key-Value). From this Key-Value the node encrypts the message using the algorithm corresponding to this value which is built-in in the trusted nodes. The node calculates the Message-Authentication-Code using the algorithm corresponding to the same Key-Value. After that, the node forwards the message.

Each node gets the message do these steps:

- Measure its traffic load in the last period (Here, the load period is 3 seconds).
- Calculate the available time between this node and the neighbours.
- Apply the authentication algorithm using the Algorithm corresponding to the attached Key-Value and verifies that the resultant value is equal to the value contained in the Authentication-Code. Else it will reject it.
- Decrypt the message using the Key-Value algorithm.
- Modify the message content according to the current node calculation.
- Set the Key-Value with a new generated random number.
- Apply the Encryption algorithm to the message using the Key-Value algorithm.
- Calculate the Authentication-Code using the Algorithm corresponding to the attached Key-Value.
- Put the calculated Authentication-Code into its field.
- Forward the message.

From the above algorithm we notice that every node that forwards a packet will generate a new random Key-Value to the packet and authenticate and encrypt it. The next node receiving the packet can then authenticate it by applying a different algorithm according to the new Key-Value which is generated by the previous node.

Keyed Message Authentication Code are employed to authenticate routing messages and the validity of the path selected and also intermediate nodes authenticate all the packets received before forwarding it, which makes our approach computationally efficient compared with prior approaches based on digital signatures of the source.

In this secured protocol multiple messages (which are actually the same message) received from different neighbours are different in content with respect to the anomaly node, but with respect to the trusted nodes is the same message. This makes it very difficult for an attacker to launch replay attacks, since the packet applied by different authentication and encryption algorithm every hop through the path.

6.3. Data Transfer Phase:

A node that believes it to be the core of a group transmits multicast announcements periodically for that group. As the multicast announcement travels through the network, it establishes a connectivity list at every node in the network. Using connectivity lists, nodes are able to establish a mesh, and route data packets from senders to receivers.

A node stores the data from all the multicast announcements it receives from its neighbours in the connectivity list. Fresher multicast announcements from a neighbour (i.e., one with a higher sequence number) overwrite entries with lower sequence numbers for the same group.

For the same core ID and sequence number, multicast announcements with smaller distances to the core are considered better. When all those fields are the same, the multicast announcement that the neighbours has minimum load is considered better. The last check is to detect the route that will remain connected for the longest duration of time. After selecting the best multicast announcement, the node generates the fields of its own connectivity list which consists of:

- Core_ID: The core ID in the best multicast announcement.
- Group_ID: The group ID in the multicast announcement.
- Next_Hop: The neighbour node.
- Parent: The neighbour from which it received the best multicast announcement.
- Distance_to_Core: One plus the distance to core in the best multicast announcement.
- Sequence number: The sequence number in the best multicast announcement.
- Time_Received: The time of the multicast announcement.
- Mesh_Member: Receivers consider themselves mesh-members and set mesh member flag to TRUE.
- Route_Load: The traffic load of the neighbour node.
- Route_Stability: Using [(X, Y), Speed] of the current node and the neighbour to calculate the duration that the link between the two nodes stays connected.

Within a finite time the forwarding mesh is constructed and every node in the network will have the routing information of the new multicast session in the Connectivity List. The sender can receive multiple Receiver Control packets from multiple nodes in the forwarding group. The sender chooses one of the routes, as an active route, according to the path quality and sends the data packets through it.

7. PERFORMANCE EVALUATION

In this section a case study, which consists of 50 simulated wireless mobile nodes roaming in a 1500 meters x 300 meters flat space for 900 seconds of simulated time? The radio transmission range is 250 meters. Group scenario files determine which nodes are receivers or senders and when they join or leave a group. It is assumed that a multicast member node joins the multicast group at the beginning of the simulation (first 30 seconds) and remains as a member throughout the whole simulation [27].

The metric used for our evaluation is packet delivery ratio which is defined as the data packets delivered divided by the data packets expected to be delivered. The data packets expected to be delivered is the data packets sent times number of receivers. This metric represents the multicast routing efficiency.

The Random Waypoint Mobility Model is used in many prominent simulation studies of ad hoc network protocols. It is flexible, and it appears to create realistic mobility patterns for the way people might move in, for example, a conference setting or museum (see Figure 3). One concern with this model is the straight movement pattern created by the MN to the next chosen destination.

The Reference Point Group Mobility Model (RPGM) is a generic method for handling group mobility. An entity mobility model (or models) needs to be specified to handle both the movement of a group of MNs and the movement of the individual MNs within the group [28].

To compare the proposed secured protocol under the two mobility models (RWM and RPGM), three experiments are performed to explore the performance with respect to some parameters such as: Traffic load, number of senders, and number of receivers. The details of each experiment are performed as follows:

- Experiment 1: Traffic Load varies from 1 to 50 pkts/sec. Speed = 0-20 m/sec, (Senders, Receivers) = (1,1), (2,2), (5, 5), (2, 10), (5, 10), and (10, 10).
- Experiment 2: Senders varies from 1 to 10, Speed= 0-20 m/sec, Members= 10, and Traffic Load= 10 pkts/sec.
- Experiment 3: Receivers varies from 1 to 25, Speed= 0-20 m/s, Senders= 5, and Traffic Load = 10 pkts/sec.
- For simplicity and we need an authentication algorithm with low computation and communication overhead we implemented the secured protocol for one case which is:
- Each node generates a random code from the code list which is built-in at each trusted node.
- Using this code to make an exclusive or (XOR) with the message contents to encrypt it.
- And also from the received key we select the corresponding algorithm (Hash-Function) and apply it to calculate the message authentication code [29][30].

8. THE IMPACT OF MOBILITY MODELS TO THE PROPOSED PROTOCOL

In this section, we illustrate how the performance results of an ad hoc network protocol significantly change when the mobility model in the simulation is changed. Figures 4 to figures 9 illustrate the performance of the proposed SERAMP, the PDR versus Traffic-Load (experiment 1), with different mobility models, RWPM and RPGM. As shown, the PDR increases by using RPGM than using RWPM by values varies between: 0.0% to 25.0%.

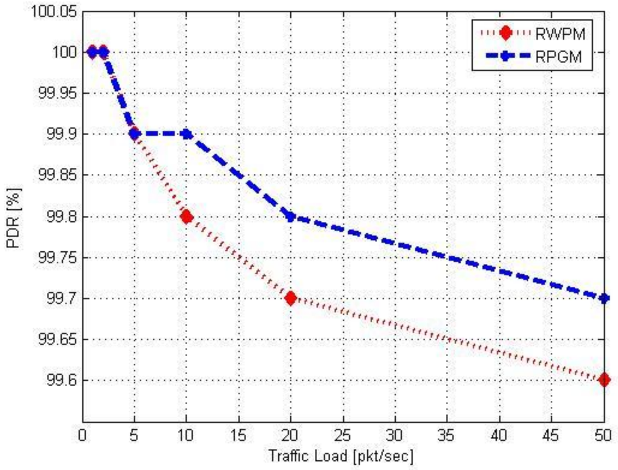

Fig. 4 Case 1: senders= 1 and receivers= 1

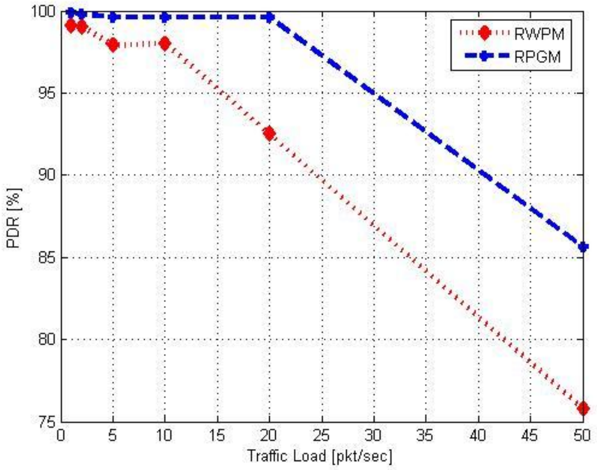

Fig. 5 case 2: senders= 2 and receivers= 2

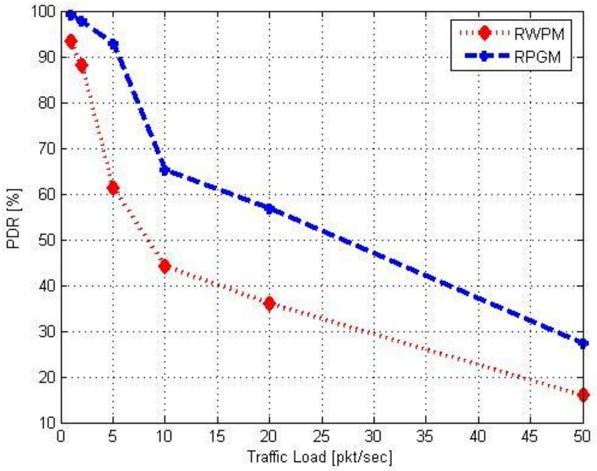

Fig. 6 Case 3: senders= 5 and receivers= 5

Figure 10 show the PDR versus the number of sender's increases (experiment 2), as shown the PDR increases by using

RPGM than using RWPM by values varies between: 0.0% to 10.0%. Figure 11 show the PDR versus the number of receiver's increases (experiment 3), as shown the PDR increases by using RPGM than using RWPM by values varies between: 2.0% to 10.0%.

The results presented prove the importance of choosing an appropriate mobility model for the performance evaluation of a given ad hoc network protocol. In summary, if a group mobility model is desired, we recommend using the Reference Point Group Mobility Model with appropriate parameters.

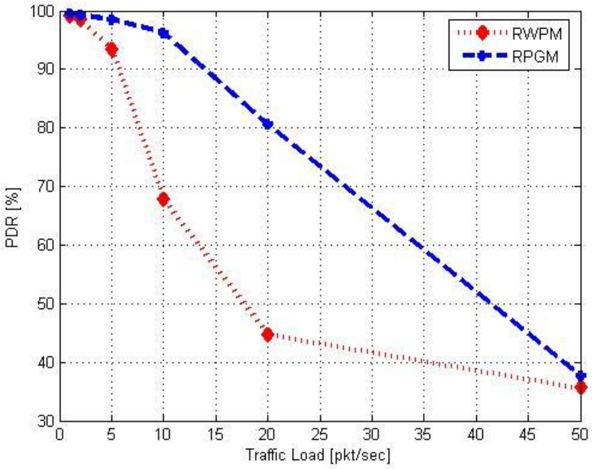

Fig. 7 case 4: senders= 2 and receivers= 10

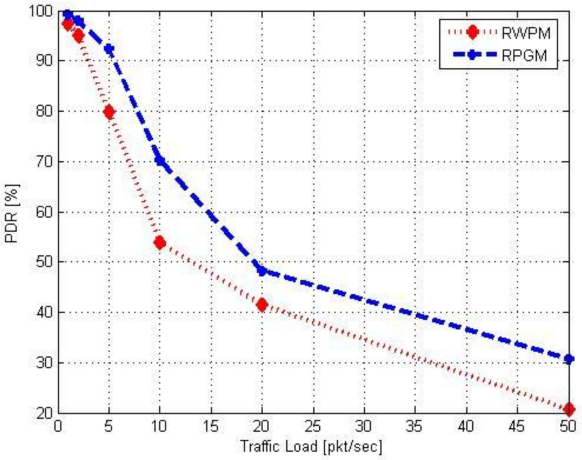

Fig. 8 Case 5: senders= 5 and receivers= 10

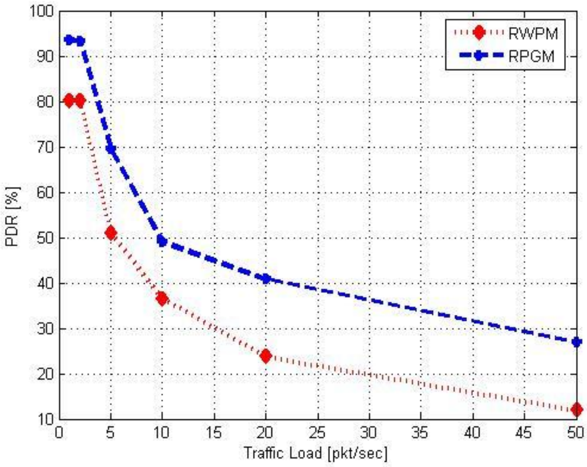

Fig. 9 case 6: senders= 10 and receivers= 10

The performance of an ad hoc network protocol can vary significantly with different mobility models. figures 4 to figures 11 illustrate the performance of one ad hoc network routing protocol with different mobility models. As shown, the performance of the protocol is greatly affected by the mobility model.

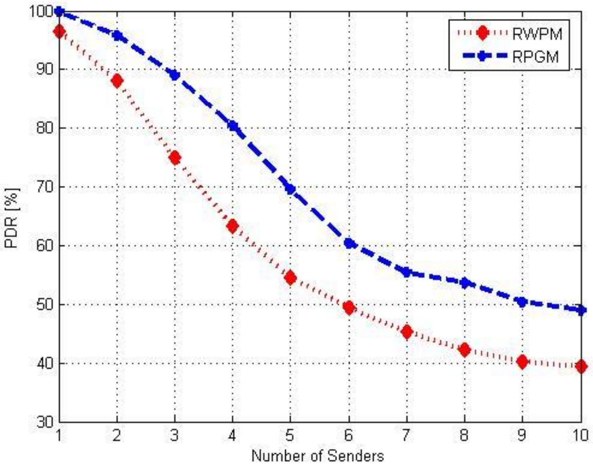

Fig. 10 PDR Vs number of senders

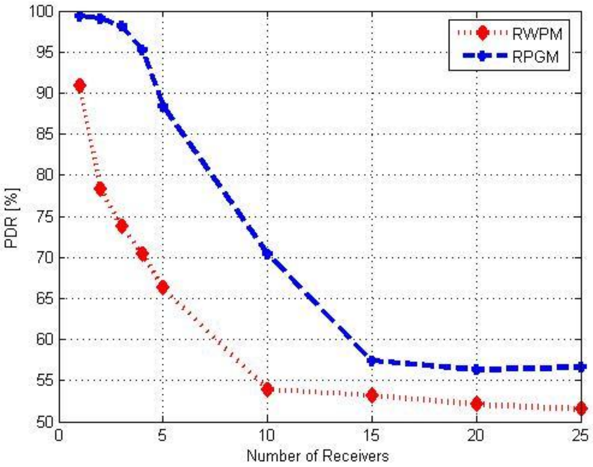

Fig. 11 PDR Vs number of Receivers

9. CONCLUSION:

The main objective of this paper is to present a secured and enhanced multicast routing protocol for Ad Hoc networks which is useful for real-time/disaster environment applications. The new routing protocol secures and enhances the performance of reliable multicast and reduces the bandwidth utilization overhead in maintaining the network topology.[31]

To enhance the multicasting routing there are two key concepts, the first key concept is to fair the distribution of the data packets among nodes according to the states of nodes load, and the second key is to use the most stable route while preserving the network robustness.

To secure the enhanced multicast routing protocol for Ad Hoc networks there are two key concepts, the first key concept is to authenticate the route of the control packets among nodes according to the Message Authentication Code; the second key is to encrypt the packet by random selection of algorithm from a set of algorithms which changes each hop. To study the effectiveness of the mobility models on the proposed protocol, we apply two mobility models, Random Way Point and

Reference Point Mobility Models, and get the results which indicates that the selection of the mobility model have a significant effect on the performance investigation of an ad hoc network protocol. The future work is:

- Implementation of the proposed protocol model using different Security algorithms.
- Adding different encryption techniques to the proposed algorithm.
- Quality of service control: Not all nodes and packets are equal.
- Radio power usage restrictions – Battery, reveal location, time and importance of the node.
- Trusted models – How to deal with the level of trust and compromised nodes rather than reject the message.
- Hardware implementation of the proposed security algorithm using FPGA.

REFERENCES:

[1] Anuj K. Gupta, Harsh Sadawarti, Anil K. Verma ,"Performance Analysis of MANET Routing Protocols in Different Mobility Models", International Journal of information technology and computer science, 2013.

[2] Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi, "A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET)", International Journal of Information and Education Technology, 2013.

[3] Charles E. Perkins, AD HOC Networking", Addison-Wesley, 2001.

[4] D. P. Agrawal and Q-A. Zeng, Introduction to Wireless and Mobile Systems, Brooks/Cole, 2003.

[5] C. Siva Ram Murthy, B. S. Manoj "Ad Hoc Wireless Networks Architectures and Protocols", PRENTICE HALL, 2005.

[6] Ahmed Ibrahim, M. Hashem, A. Fahmy, F. Amer "Secured and Enhanced Reliable Ad Hoc Multicasting Protocol (SERAMP)", International MultiConference of Engineers and Computer Scientists 2010.

[7] K.Kavitha1, K.Selvakumar2, "Analyzing Multicasting Routing Protocols with Different Mobility Model", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com , 2013.

[8] Xiaojing Xiang, Xin Wang, and Yuanyuan Yang "Stateless Multicasting in Mobile Ad Hoc Networks", IEEE Transactions, 2010.

[9] I. Karthigeyan, B. S. Manoj, and C. Siva Ram Murthy, "A Distributed Laxity-Based Priority Scheduling Scheme for Time-Sensitive Traffic in Mobile Ad Hoc Networks," to appear in Ad Hoc Networks Journal.

[10] Elizabeth M. Royer and Charles E. Perkins. Multicast ad hoc on demand distance vector (maodv) routing. IETF Internet Draft. draft-ietf-manetmaodv-00.txt, July, 2000.

[11] Carlos De Morais Cordeira, Hrishikesh Gossain and Dharma P. Agarwal, "Multicast Over Wireless Mobile Ad-Hoc Networks: Present and Future Directions" IEEE Network, 2003, pp 2-9.

[12] A. Perrig, R. Canetti, D. Song, and J. D. Tygar, "Efficient and secure source authentication for multicast," in Proc. of NDSS'01, 2001.

[13] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Elizabeth Royer, and Clay Shields. A secure routing protocol for ad hoc networks. In Proceedings of the 10 Conference on Network Protocols (ICNP), 2002.

[14] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure ondemand routing protocol for ad hoc networks," in Proc. of MOBICOM, September 2002.

[15] S. Zhu, S. Xu, S. Setia and S. Jajodia, "LHAP: A Lightweight Hop-by-Hop Authentication Protocol For Ad-Hoc Networks", *ICDCS 2003 International* Workshop on Mobile and Wireless Network (MWN 2003), May 2003.

[16] Seung Yi, Prasad Naldurg, and Robin Kravets. A security-aware ad hoc routing protocol for wireless networks. In *The 6th World Multi-Conference on* Systemics, Cybernetics and Informatics (SCI), 2002.

[17] Yih-Chun Hu, David B. Johnson, and Adrian Perrig. Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks. In Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02), pages 3– 13, June 2002.

[18] P. Papadimitratos and Z. J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks", IEEE Workshop on Security and Assurance in Ad hoc Networks, in conjunction with the International Symposium on Applications and the Internet, Orlando, FL, January 28, 2003.

[19] P. Papadimitratos and Z. J. Haas, "Secure Data Transmission in Mobile Ad Hoc Networks", Proceedings of the 2003 ACM workshop on Wireless security San Diego, *CA*, USA, Pages: 41 – 50, 2003.

[20] S. Carter and A. Yasinsac, "Secure Position Aided Ad hoc Routing Protocol", Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN02), Nov 4-7, 2002.

[21] J. Marshall, "An Analysis of SRP for Mobile Ad Hoc Networks", *Proceedings of* the 2002 International Multi-Conference in Computer Science, Las Vegas, USA, 2002.

[22] A. Perrig, R. Canetti, J. Tygar, and D. Song, "The TESLA Broadcast Authentication Protocol," RSA CryptoBytes, 5, 2002

[23] M. Zapata, N. Asokan, Securing ad hoc routing protocols, in: Proceedings of ACM WiSe 2002, Atlanta, GA, September 2002.

[24] Tracy Camp, Jeff Boleng, Vanessa Davies "A Survey of Mobility Models for Ad Hoc Network Research", Wireless Communication & Mobile Computing (WCMC): vol. 2, no. 5, pp. 483-502, 2002

[25] X. Hong, M. Gerla, G. Pei, and C. Chiang, "A group mobility model for ad hoc wireless networks. In Proceedings of the ACM International Workshop on Modeling and Simulation of Wireless and Mobile Systems", (MSWiM), August 1999.

[26] Ahmed Ibrahim, M. Hashem, A. Fahmy, F. Amer "A New Model for Solving Multicasting Problems in Military Applications", Ph. D thesis, 2011.

[27] Jagdeep Kaur, Er.Parminder Singh, "Performance Comparison Between UNICAST AND MULTICAST Protocols VANETS", International Journal of Advanced Technology & Engineering Research (IJATER) 2013.

[28] Ranjeet Singh, Harwant Singh Arri, "Comparison of AAMRP and IODMRP Using SBPGP", International Journal of Computer Science and Management Research , 2013.

[29] Nagendra Sah, "Impact of Mobility and Node Speed on Multicast Routing In Wireless MANETs", International Journal of Engineering and Advanced Technology (IJEAT) , 2012.

[30] V.p.patil, B.p.saoji, "Impact of routing protocol on performance of wireless ad hoc vehicular network", International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) , 2012.

[31] Sherif M. Badr, PhD. "A Framework for Integrated Routing Protocols for Mobile Ad Hoc Network", *IJCA (0975 – 8887) Volume 60– No.9, December 2012*