**Military Technical College**
**Kobry El-Kobbah,**
**Cairo, Egypt**

**7th International Conference**
**on Electrical Engineering**
**ICEENG 2010**

# Secured and Enhanced Reliable Ad HocMulticasting Protocol (SERAMP)

*By*

Eng. A. Ibrahim* Prof. Dr. M. Hashem** Prof. Dr. A. Fahmy*** Prof. Dr. F. Amer***

***Abstract:***

The Mobile Ad Hoc Network (MANET) is characterized by a lack of infrastructure, and by a random and quickly changing network topology; thus the need for a robust dynamic routing protocol that can accommodate such an environment is an important issue. In this paper we presented an enhanced reliable Ad Hoc multicasting protocol that satisfies efficiency and robustness which is an essential in relative applications. 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 one is to use the most stable route, which remains connected for the longest duration of time while preserving the network robustness.
Due to the nature of ad hoc networks, secure routing is an important area of research in developing secured routing protocols. The paper presents a secured routing protocol for Ad Hoc network to be suitable for relative applications. The proposed protocol based on two key concepts, the first key concept is to authenticate the route of the control packets among nodes according to the Message Authentication Code (MAC); the second one is to encrypt the packet by random selection of algorithm from a set of algorithms which changes each hop.
After words, this paper applies the proposed secured protocol for the previous work and a comparative study has been made between the proposed protocol and the previous protocol.

***Keywords:***

Ad Hoc networks, Ad Hoc multicasting, routing security.

---

* **Egyptian Armed Forces**
** **Department of Computer Science, Ain shams University, Cairo, Egypt**
*** **Department of Computer Science, Cairo University, Cairo, Egypt**

## *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 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 [1], promises to provide connectivity among hosts in a highly volatile environment, while minimizing routing overhead.

Wireless networks do not share the robust and high-speed links enjoyed by their wired counterparts. Wireless connections have a small data carrying capacity, a relatively high error rate, and are unreliable when compared to traditional wired connections. MANET may be an adequate solution to the wireless networking problem. MANETs operate independently of a fixed backbone network, conserve bandwidth, and react quickly to changes in network topology.

Ad hoc wireless networks are self-organizing, dynamic topology networks formed by a collection of mobile nodes through radio links. Minimal configuration, absence of infrastructure, and quick deployment, make them convenient for emergency situations other than military applications. Multicasting plays a very crucial role in the application of Ad hoc networks. As the number of participants increases, scalability of the multicast protocol becomes an important issue [2].

Multicasting is the transmission of datagrams 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 [2].

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. Like wired networks, the following major security goals should be satisfy confidentiality, integrity, availability, authentication, non-repudiation.

The rest of the paper is organized as follows: Section 2 describes briefly the related work of Ad Hoc multicasting protocols, Section 3 discusses briefly the related work of Ad Hoc security, section 4 presents overview of the previous work of the enhancement of Multicasting protocol, and section 5 presents our proposed protocol. The simulation results and performance evaluation are presented in section 6, and finally the conclusion is presented in section 7.

## *2. Multicast Routing Protocols*

One straightforward way to provide multicast in a MANET is through flooding. This approach has a considerable overhead since a number of duplicated packets are sent and packet collisions do occur in a multiple-access-based MANET. We can classify the multicast routing protocols into three categories according to topology, initialization of the multicast session, and the topology maintenance mechanism. Figure (1) shows the classification of Ad Hoc multicast routing protocols.

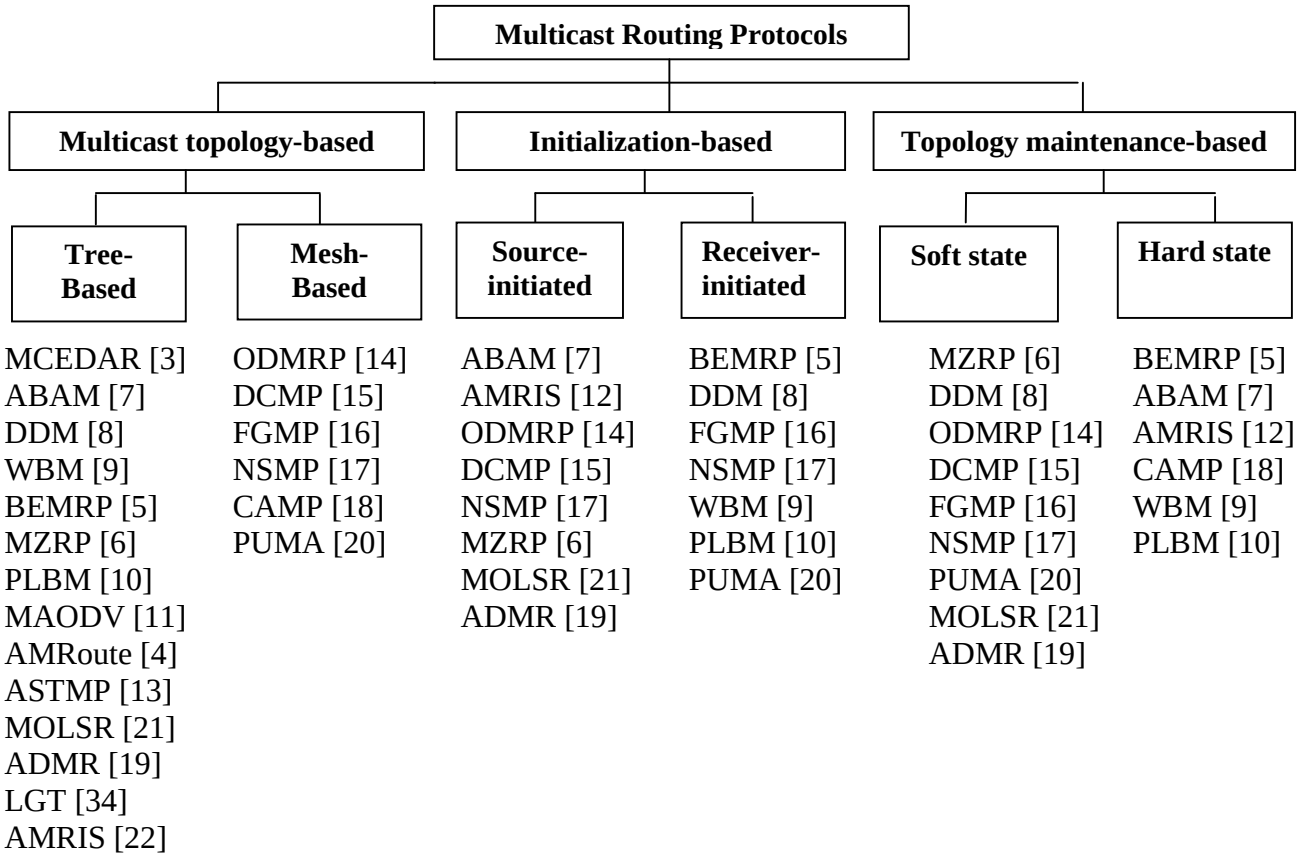


***Figure (1):*** *Classification of Ad Hoc multicast routing protocols.*

## *3. Security:*

Like wired Networks, we can classify the attacks into two brief categories, namely passive and active attacks. A passive attack attempts to learn or make use of information from the system but does not affect system resources. A powerful solution to keep the adversary away from getting useful information is encrypting the data packet. An active attack attempts to alter system resources or affect their operation. Cryptography is not the only method to provide information security, but the most important one. Some cryptography mechanisms will be addressed in the following section. Cryptography can be used to achieve the *Confidentiality, Integrity, Non-repudiation, Availability, and Authentication.*

### *A. Security attacks in ad hoc networks*

***Wormhole attack:*** In this attack, an adversary receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. This tunnel between two adversaries are called wormhole.

***Black hole attack*:** In this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the destination node of the packet that was intercepted.

***Routing attacks:*** In this attack, an adversary attempts to disrupt the operation of the network. The attacks can be further classified into several types, namely routing table overflow attack, routing table poisoning attack, packet replication attack, routing cache poisoning, and rushing attack.

***Denial of service (DoS) attack:*** In this type of attack, the attacker attempts to prevent the authorized users from accessing the services to other nodes, either by consuming the bandwidth or by overloading the system. A simple scenario in which a DoS attack interrupts the operation of ad hoc wireless networks is by keeping a target node busy by making it process unnecessary packets.

### *B. Security Protocols*

In this section a brief overview of possible security solutions in a MANET with their characteristics is presented:

***ARAN (Authenticated Routing for Ad hoc Networks):*** ARAN [23] is an on-demand security routing protocol that makes use of cryptographic certificates to make the routing secure. 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.

***Ariadne:*** Ariadne [26] is a secure on-demand routing protocol for Ad Hoc Network. Ariadne relies on symmetric cryptography and performs MAC through intermediate nodes. The routing message 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.

***LHAP (Lightweight Hop-by-hop Authentication Protocol [30]:*** It's 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. LHAP is based on two techniques. First a hop-by-hop authentication to verify the authenticity of every packet sent in the network. Every node receiving a packet authenticates it before forwarding it. If the authentication fails, the packet is discarded. Secondly, one-way key chain is used for packet authentication.

***SAR (Security-aware Ad hoc Routing:*** SAR [24] 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.

***SEAD (Secure Efficient Ad hoc Distance vector routing protocol:*** SEAD [25] is in 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.

***SLSP (Secure Link State Protocol):*** SLSP [31] 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.

***SMT (Secure Message Transmission):*** The **SMT** [32] purpose as its name says to secure the data transmission. The issue of discovering routes in a secure manner is not treated by SMT and should be done by another protocol, like SRP or Ariadne. The goal in SMT is to secure data forwarding on already discovered routes whether or not the routes contain malicious nodes.

***SPAAR (Secure Position Aided Ad hoc Routing*)**: SPAAR [28] is 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 [24]. 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.

***SRP (Secure Routing Protocol):*** SRP [29] 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.

***TESLA (Time Efficient Stream Loss-tolerant Authentication):*** TESLA [27] enables source authentication. The receiver of any broadcasted data can verify that the packets really originate from the claimed source and that the information hasn't been altered on the way. 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.

## *4. The Enhanced Reliable Ad Hoc Multicasting Protocol (E-PUMA) [33]*

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 focus on: Route load and Route stability/Quality. In what follows the basic modules of the proposed protocol will be discussed.

### *A. 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.
We implement the spanning tree algorithm introduced by Perlman for internetworks of transparent bridges [28] to elect one receiver of a group to be the core of this 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.
We use a single control message for all its functions, the multicast announcement. Each multicast announcement consists of: *Sequence_Number*, *group_ID*, *core_ID*, *Distance_to_core*, *Mesh_member* flag, *Parent* (states the preferred neighbour to reach the core), *X-Y* Coordinates of the node, *Node _Speed*, and *Node_Load*.
During the scenario each node measures its traffic load in the last period (Here, the load period is 3 seconds). Each node gets the control packet calculates the available time between this node and the neighbours. With the information contained in such announcements, nodes elect cores, determine the routes for senders to unicast multicast data packets towards the group and maintain the mesh of the group.

### *B. Data Transfer Phase*

A node that believes itself 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*, *Group_ID*, *Next_Hop*, *Parent*, *Distance_to_Core*, *Sequence Number*, *Time_Received*, *Mesh_Member*, *Route_Load* (the traffic load of the neighbour node), and *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).

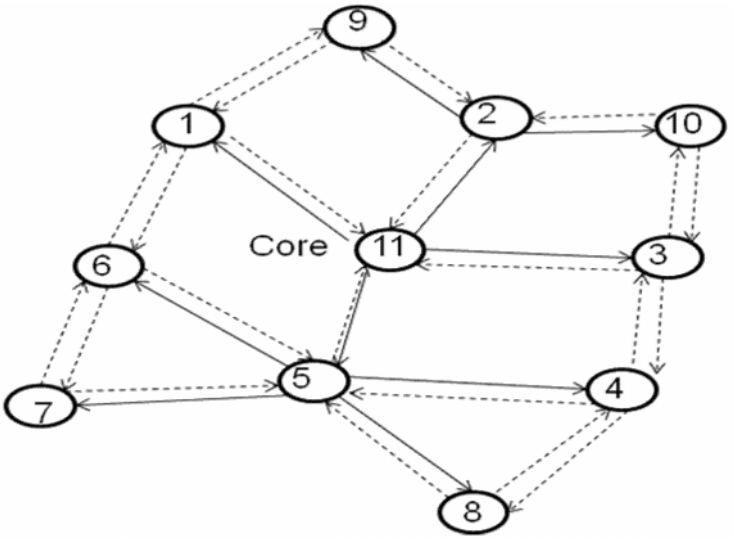


***Figure (2):*** *Mesh Creation*

***Table (1):*** *Connectivity List of E-PUMA at node 6*

| Neighbour | Multicast Announcement | | | | Time (ms) |
|---|---|---|---|---|---|
| | Distance To Core | Parent | Load % | Stability (sec) | |
| 1 | 1 | 11 | 30 | 40 | 12180 |
| 5 | 1 | 11 | 40 | 40 | 12152 |
| 7 | 2 | 5 | 60 | 30 | 12260 |

***Table (2):*** *Connectivity List of SERAMP at node 6*

| Neighbour | Multicast Announcement | | | | Time (ms) |
|---|---|---|---|---|---|
| | Distance To Core | Parent | Load % | Stability (sec) | |
| 5 | 1 | 11 | 40 | 40 | 12152 |
| 7 | 2 | 5 | 60 | 30 | 12260 |

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.
Figure (2) shows the mesh creation, and Table (1) and Table (2) show the connectivity list of the E-PUMA protocol and the SERAMP protocol respectively at certain group/core/sequence number for node 6 where node 1 is incredible node.

## *5. The Proposed Secured and Enhanced Ad Hoc Multicasting Protocol (SERAMP)*

A secure routing protocol for ad hoc networks 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

Our 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 be applicable to a wide range of routing protocols.

### *A. Algorithm*

Our 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).

- **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 MAC. Then the node sends the message.

- **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 MAC otherwise reject it. Then decrypt the message using the Code-Value associated with the Key- table.

- **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 node selects the Hash-Function for authentication. The Authentication is applied on the message and the MAC is calculated. Then the node forwards the message.

***B. Implementation***

In mesh establishment phase two fields are added to the control packet of the multicast announcement: The first field is the *Key-Value* and the second field is the *Authentication-Code*. So that 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:*** x-Coordinate of the node.
- ***Y:*** y-Coordinate 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:*** MAC 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 MAC using the algorithm corresponding to the same Key-Value. After that, the node forwards the message. Each node gets the message do the following steps:

- 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.
- Modifies 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.

In 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 that receives 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 MAC 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 is applied by different authentication and encryption algorithm at each hop through the path.

## *6. Performance Evaluation*

In this section a case study is performed. Table 3 illustrates a simulation environment that 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.
The metrics used for our evaluation are Packet Delivery Ratio (PDR) and the Average Delay (AD). The PDR 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. These metrics represent the multicast routing efficiency.

***Table (3):** Simulation Environment.*

| | |
|---|---|
| Simulator | NS-2.32 |
| Total Nodes | 50 |
| Simulation Time | 900 sec |
| Simulator Area | 1500 x 300 |
| Node Placement | Random |
| Pause Time | 0 |
| Mobility Modem | Random Waypoint |
| Radio Range | 250 meter |
| Data Packet Size | 256 bytes |

For simplicity, we used an authentication algorithm with low communication and computation overhead; we implemented the secured protocol for one case which is:

- From the received key we select the associated 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 MAC.

To compare the proposed secured protocol with the previous protocol, four experiments are performed to explore the performance with respect to some parameters such as: Traffic load, number of senders, number of receivers, and node mobility. The details of each experiment are performed as follows:

- **Experiment 1:** Traffic Load varies from 1 to 50 pkts/sec. Mobility = 0, (Senders , Receivers)= (1,1), (5,5), and (10,10).
- **Experiment 2:** Senders varies from 1 to 10, Mobility= 5 m/s, Members= 10, and Traffic Load= 10 pkts/sec.
- **Experiment** 3: Receivers varies from 1 to 30, Mobility= 5 m/s, Senders= 5, and Traffic Load = 10 pkts/sec.
- **Experiment 4:** Mobility speed varies from 0 to 20 m/s, Senders= 5, Receivers= 5, and Traffic Load = 10 pkts/sec.

### *A. The impact of traffic load*

In traffic load experiment, node mobility speed is moderate with maximum speed 5 m/s, because we want to focus on packet drops caused by congestion and the delays caused by the security algorithm calculations. Both the senders and receivers were chosen randomly from among the 50 nodes. Traffic load was equally distributed among all senders.

The PDR as a function of the traffic load which Changes from 1 pkt/sec to 50 pkt/sec is presented in different cases (as shown in Figure (3), Figure (5), and Figure (7)). After implementation of the secured protocol, we notice that the PDR is the same for the two protocols.

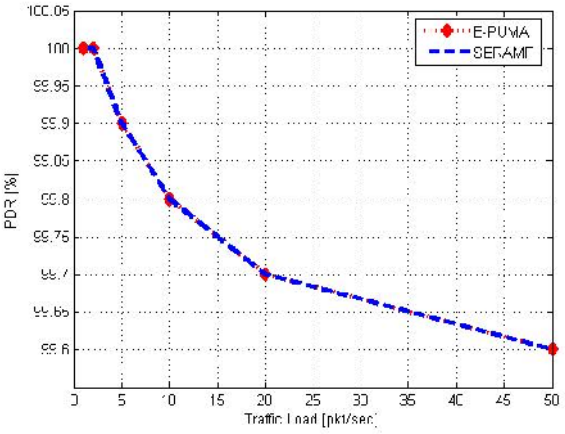


***Figure (3):*** *senders= 1 & receivers= 1.*

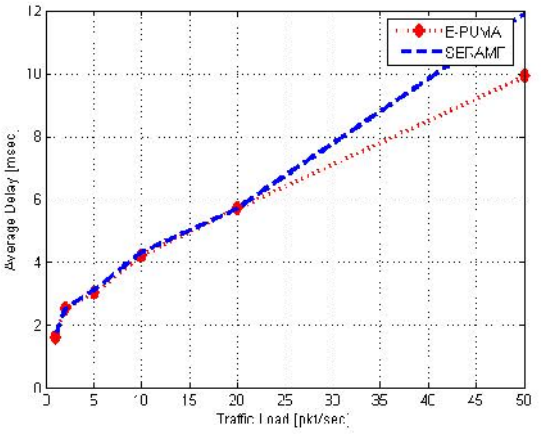


***Figure (4):*** *senders= 1 & receivers= 1.*

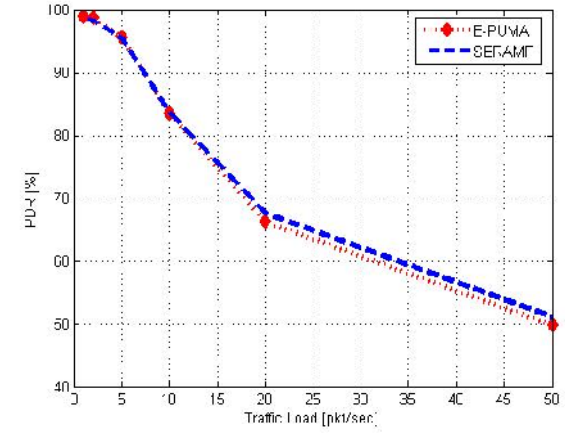


***Figure (5):*** *senders= 5 & receivers= 5.*

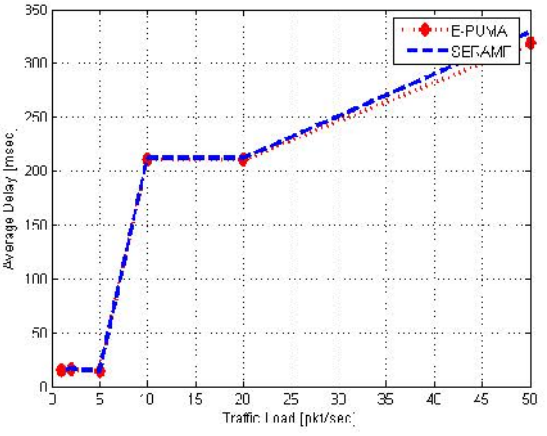


***Figure (6):*** *senders= 5 & receivers= 5.*

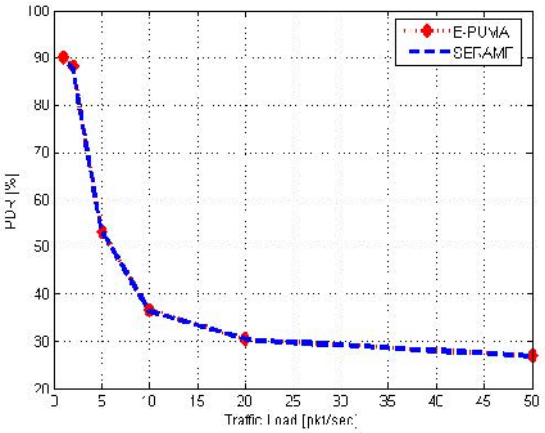


***Figure (7):*** *senders=10 & receivers=10.*

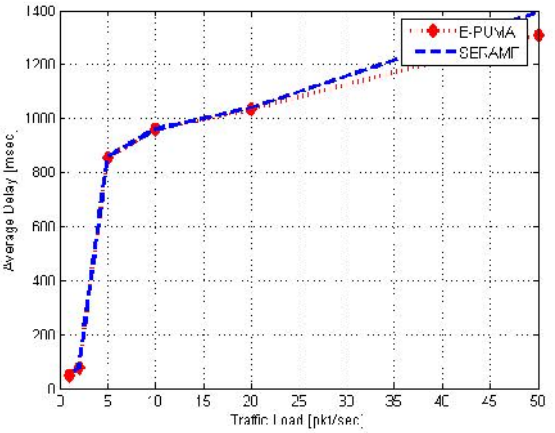


***Figure (8):*** *senders=10 & receivers=10.*

The AD as a function of the traffic load delayed from 0.0% to 0.3% as a result of the authentication, decryption, and encryption calculations which is negligible value compared with the importance of securing the data (as shown in Figure (4), Figure (6), and Figure (8)).

### *B. The impact of number of senders*

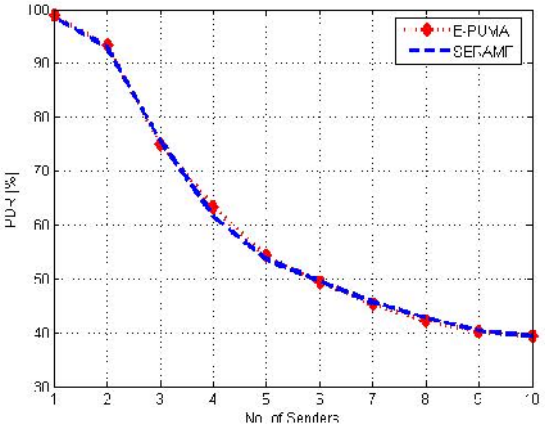


***Figure (9):*** *PDR Vs. number of senders.*

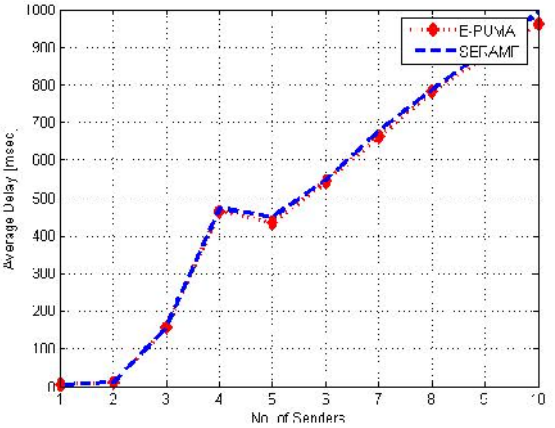


***Figure (10):*** *AD Vs number of senders.*

In case the number of multicast senders increased from 1 to 10, traffic load at 10 pkt/sec, number of receivers is 10, and node mobility speed is moderate with maximum speed 5 m/s. We will show the PDR and the AD as a function of the number of senders for the two protocols. We found that the PDR is not impacted and the AD is still negligible value as shown in Figure (9) and Figure (10).

### *C. The impact of number of receivers*

In this experiment, node mobility speed is moderate with maximum speed 5 m/s. The number of multicast receiver increases from 1 to 30. Figure (11) shows that the PDR doesn't impacted with the security algorithm and Figure (12) shows that the AD is acceptable value.

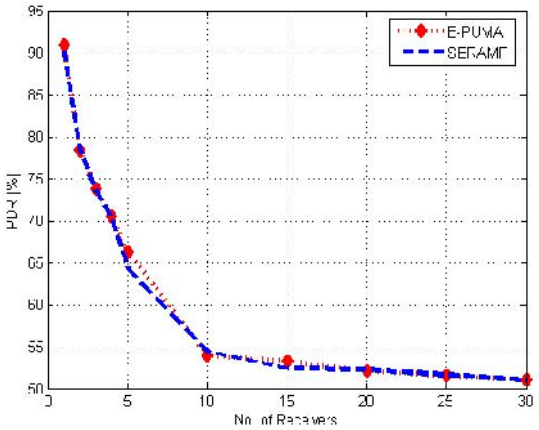


***Figure (11):*** *PDR Vs. No. of receivers.*

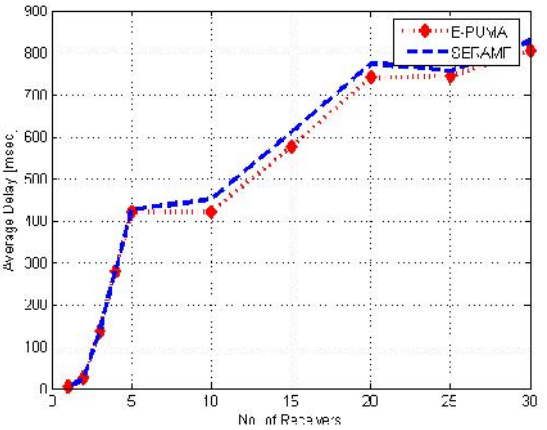


***Figure (12):*** *AD Vs. No. of receivers.*

### *D. The impact of node mobility*

In this aspect, the maximum movement speed of nodes range in the set {0, 1, 5, 10, 15, and 20} m/s, the number of senders is fixed to 5, the number of receivers is fixed to 5 and the traffic load is 10 pkt/sec. We illustrate the PDR and the AD (as shown in Figure (13) and Figure (14)) as a function of the speed for the two protocols.

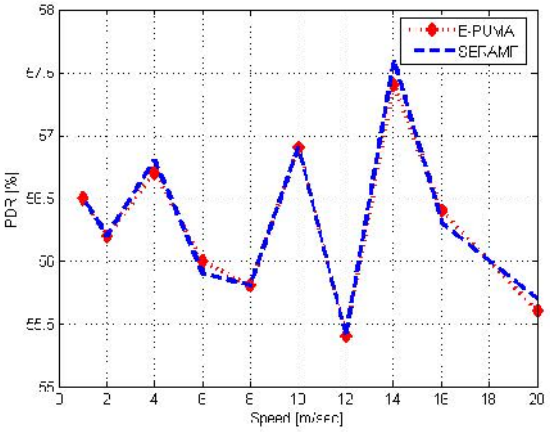


***Figure (13):*** *PDR versus speed*

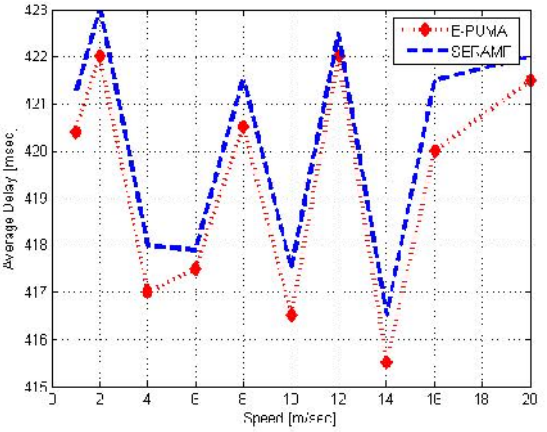


***Figure (14):*** *AD versus speed*

## *7. Conclusion:*

This paper presented a secured multicast routing protocol for Ad Hoc networks which is useful for real-time/disaster environment applications. The first key concept is to authenticate the route of the control packets among nodes according to the MAC; the second one is to encrypt the packet by random selection of algorithm from a set of algorithms which changes at each hop. A comparative case study was established between E-PUMA and SERAMP. The PDR is approximately the same for the two protocols, while the AD of SERAMP is increased from 0.0% to 0.3% higher than E-PUMA as a result of the authentication and decryption and encryption calculations which is considered a very small value. We have to put in consideration that the PDR is calculated for the trusted packets only. The following issues should be taken into concern as a future work:

- Implementation of the proposed protocol model using different Security algorithms.
- Quality of service control – Not all nodes and packets are equal.
- Trusted models – How to deal with the level of trust and compromised nodes rather than reject the message.
- Mobility Models – Not all Mobility Models are equal.
- Radio power usage restrictions – Battery, reveal location, time and importance of the node.
- Hardware implementation of the proposed security algorithm using FPGA.
- Support for 3D Terrain – although not supported in NS2 mobility traces, support of 3D terrain models would allow for more realistic wireless node connectivity calculations.

## ***REFERENCES:***

[1] Charles E. Perkins," Ad Hoc Networking," Addison-Wesley, 2001.

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

[3] P. Sinha, R. Sivakumar, and V. Bharghavan, "MCEDAR: Multicast Core Extraction Distributed Ad Hoc Routing," Proceedings of IEEE WCNC 1999. pp. 1313-1317, September 1999.

[4] Jason Xie, Rajesh R. Talpade, Anthony Mcauley, and Mingyan Liu, "AMRoute: Ad Hoc Multicast Routing Protocol," Mobile Networks and Applications 7, 429–439, 2002.

[5] T. Ozaki, J. B. Kim, and T. Suda, "Bandwidth Efficient Multicast Routing Protocol for Ad Hoc Networks," Proceedings of IEEE ICCCN 1999, pp. 10-17, October 1999.

[6] Xiaofeng Zhang and Lillykutty Jacob, "MZRP: An Extension of the Zone Routing Protocol for Multicasting in MANETs," JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 20, 535-551 (2004).

[7] C. K. Toh, G. Guichala, and S. Bunchua, "ABAM: On-Demand Associativity-Based Multicast Routing for Ad Hoc Mobile Networks," Proceedings of IEEE VTC SOOO, pp. 987-993, September 2000.

[8] L. Ji and M. S. Corson, "Differential Destination Multicast–A MANET Multicast Routing Protocol for Small Groups," IEEE INFOCOM 2001, pp. 1192-1201.

[9] S. K. Das, B. S. Manoj, and C. Siva Ram Murthy, "Weight-Based Multicast Routing Protocol for Ad Hoc Wireless Networks," Proceedings of IEEE GLOBE-COM2002, vol. 1, pp. 17-21, November 2002.

[10] R. S. Sisodia, I. Karthigeyan, B. S. Manoj, and C. Siva Ram Murthy, "A Preferred Link-Based Multicast Protocol for Wireless Mobile Ad Hoc Networks," Proceedings of IEEE ICC 2003, vol. 3, pp. 2213-2217, May 2003.

[11] E. M. Royer and C. E. Perkins, "Multicast Operation of the Ad Hoc On-Demand Distance Vector Routing Protocol," Proceedings of ACM MOBICOM 1999, pp. 207-218, August 1999.

[12] C. W. Wu, Y. C. Tay, and C. K. Toh, "Ad Hoc Multicast Routing Protocol Utilizing Increasing id-numberS (AMRIS) Functional Specification," Internet draft ( work inprogress ), draft-ietf-manet-amris-spec-OO.txt, November 1998.

[13] C. C. Chiang, M. Geria, and L. Zhang, "Adaptive Shared Tree Multicast in Mobile Wireless Networks," Proceedings of GLOBECOM 1998, pp. 1817-1822, November 1998.

[14] S. J. Lee, M. Geria, and C. C. Chiang, "On-Demand Multicast Routing Protocol," Proceedings of IEEE WCNC 1999, pp. 1298-1302, September 1999.

[15] S. K. Das, B. S. Manoj, and C. Siva Ram Murthy, "A Dynamic Core-Based Multicast Routing Protocol for Ad Hoc Wireless Networks," Proceedings of ACM MOBIHOC S008, pp. 24-35, June 2002.

[16] C. C. Chiang, M. Geria, and L. Zhang, "Forwarding Group Multicasting Protocol for Multi-Hop, Mobile Wireless Networks," ACM/Baltzer Journal of Cluster Computing: Special Issue on Mobile Computing, vol. 1, no. 2, pp. 187-196, 1998.

[17] S. Lee and C. Kim, "Neighbour Supporting Ad Hoc Multicast Routing Protocol," Proceedings of ACM MOBIHOC 2000, pp. 37-50, August 2000.

[18] J. J. Garcia-Luna-Aceves and E. L. Madruga, "The Core-Assisted Mesh Protocol," IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1380-1994, August 1999.

[19] J.G. Jetcheva and David B. Johnson, “Adaptive demand-driven multicast routing in multi-hop wireless ad hoc networks,” in Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), October 2001.

[20] Ravindra Vaishampayan, J.J. Garcia-Luna-Aceves], “Efficient and Robust Multicast Routing in Mobile Ad Hoc Networks,” Proceedings of IEEE 2004, pp. 304-313, 2004.

[21] Laouiti, A., Jacquet, P., Minet, P., Viennot, L., Clausen, T., and Adjih, C., “Multicast Optimized Link State Routing,” INRIA research report RR-4721 (2003)

[22] C. W. Wu and Y. C. Tay, "AMRIS: A Multicast Protocol for Ad hoc Wireless Networks," Internet draft, draft-ietf-manet-amris-spec-OO.txt, November 1998.

[23] 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.

[24] 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.

[25] Yih-Chun Hu, David B. Johnson, and Adrian Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks", Ad Hoc Networks 1 (2003) 175–192.

[26] 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.

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

[28] 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.

[29] 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.

[30] 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.

[31] 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 2003 International Symposium on Applications and the Internet, Orlando, FL, January 28, 2003.

[32] 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.

[33] M. Hashem, Ahmed Ibrahim, A. Fahmy, and F. Amer, "An Enhanced Reliable Ad Hoc Multicasting Protocol", International Journal of Intelligent Computing and Information Science, Vol. 10, N. 1, pp. 255-267, January 2010, Ain Shams University.

[34] K. Chen and K. Nahrstedt, "Effective Location-Guided Tree Construction Algorithms for Small Group Multicast in MANET," Proc. INFOCOM, 2002, pp.1180-1189.