International Journal of Electrical and Computer Engineering (IJECE)
Vol. 6, No. 4, August 2016, pp. 1857~1865
ISSN: 2088-8708, DOI: 10.11591/ijece.v6i4.9941

Secure Multicast Routing Protocol in MANETs Using Efficient ECGDH Algorithm

Gopi Arepalli[1], Suresh Babu Erukula[2], Arepalli Peda Gopi[3], C. NagaRaju[4]
[1] Research Scholar, KL University, Guntur, Andhra Pradesh
[2] Department of CSE, KL University, Guntur, Andhra Pradesh
[3] Department of CSE Vijanan University, Guntur,Andhrapradesh
[4] Department of CSE, YSR College of YV University, Proddutur, Andhra Pradesh

Article Info

Article history:

Received Jan 17, 2016
Revised May 16, 2016
Accepted May 27, 2016

Keyword:

Diffie-hellman
Elliptic curve group
Man in the middle attack
MANETs
PUMA

ABSTRACT

An Ad-hoc Network covers a set of autonomous mobile nodes that communicates through wireless communication in an infrastructure-less environment. Mostly MANETs are used in group communication mechanisms like military applications, emergency search, rescue operations, vehicular ad-hoc communications and mining operations etc. In such type of networks, group communication is takes place by multicasting technique. Communication and collaboration is necessary among the nodes in the groups in multicast protocols. PUMA has the best multicast routing protocol compared to tree and mesh based multicast protocols although it suffers from security issues. PUMA mainly suffers from Man In The middle attack. MITM attack generates traffic flow, drop the packets and miscommunicate the neighbor nodes with false hop count. So defending from MITM attack we designed a new mechanism called Elliptic Curve Group Diffie-Hellman (ECGDH). This paper compares results of PUMA [1] routing protocol with legitimate, under attack and after providing security against attack. Finally we observed ECGDH [2] gives efficient results even attack has happened.

Corresponding Author:

1. INTRODUCTION

A Mobile ad hoc network is an autonomous collection of nodes do not rely on any pre-established infrastructure that forms dynamic communicative network. Nodes in these network make use of mobility and wireless communication to maintain connectivity. However, the limited propagation range of these wireless environmentmake a challenging issue to establish the routes. Subsequently, MANETS are multi-hop infrastructures less network that establishes the routes themselves "on the fly". These networks are suitable for applications like battlefield, emergency search, rescue operations, vehicular ad-hoc communications and mining operations etc. In such applications, communication and collaboration of nodes among the group is necessary. Therefore, multicast communication is very much intended to the group communication which saves network resources and bandwidth. Moreover, Multicasting is a service for disseminating information to a group of hosts that sends the data from a source to multiple destinations in the network. The unique properties of multicast communication is first, the node can join anytime and can leave anytime from multicast group dynamically. Second, the nodes have no constraints on the group regarding its location and members in the group. Third, a node may be a member of several groups. However, the nodes have send the packets to the members in the group, even it is not a member of a group.

Over the last decade, researchers proposed several multicast routing protocols for MANETs for effective multimedia communication. More importantly these routing protocols can be categorized intotree-based and mesh-based routing protocols. However, other multicast routing protocols are also available, which is out of scope of this paper. First, the tree based multicast routing protocols maintains a single path and establishes a shared multicast routing tree to transmits the packets from source to receivers in a multicast group. The main idea behind these protocols is to maintain memory for their children instead of all the nodes. Additionally, these protocols do not provide sufficient robustness due to the limited bandwidth efficiency. One of the tree based multicast routing protocol is MAODV [3]. While, Mesh based multicast routing protocols establishes a mesh network and maintains multiple paths between sources to receivers. Due to the multiple paths, mesh based multicasting is more suitable for frequently changing topological environments and provide more robustness. PUMA and ODMRP [4] are the routing protocols that falls under mesh based routing protocols.Moreover, in spite of the routing issue many mobile adhoc network applications requires various multicast routing protocols that need to operate correctly even in hostile environment. Because the MANETS are more vulnerable to different routing attacks wormhole, black hole, rushing attack, man in the middle attack, etc., due to its inherited characteristicsof MANETs. This paper proposes a novel method to secure the multicast routing protocol against man in the middle attack in MANETs. Further, we also analyzed with various performance metrics such as throughput, PDF, control overhead and total overhead. This paper is categorized into several sections. Section II describes the related work regarding this paper. Section III explains the multicast routing protocols, section IV explains the man in the middle attack, section V mainly focused on security through ECGDH [5] and finally section VI explains the simulation results of PUMA routing protocol with legitimate, under attack and after ECGDH security.

2. RELATED WORK

The existing works mainly focusing on normal routing procedure. But the natures of group communication pose many challenges to the real world. In this section we describe different methods of multicast routing protocols. RavindraVaishampayan et al proposed a PUMA directing convention it increases high information conveyance proportion with restricted control overhead furthermore increase higher bundle conveyance proportion contrasted with other multicast steering conventions. MenakaPushpa and K.Kathiravan proposed answers for two interior assaults in particular guard dog based information bundle drop assault recognizable proof and MA parcel manufacture assault. Elizabeth M. Royer et al., proposes Multicast Ad hoc On-interest Distance Vector steering convention (MAODV) [6] is an on-interest multicast directing convention that develops a common conveyance tree to bolster numerous senders and collectors in a multicast session. To give ideal correspondence capacity, a directing convention for such a dynamic self-beginning system must be equipped for unicast, telecast, and multicast.

Broadened Ad-hoc On-Demand Distance Vector Routing (AODV) [7], a calculation for the operation of such specially appointed systems, to offer novel multicast capacities which take after normally from the way AODVbuilds up unicast courses. AODV manufactures multicast trees as required (i.e., on-interest) to associate multicast bunch individuals. Control of the multicast tree is circulated so that there is no single purpose of disappointment. AODV gives circle free courses to both unicast and multicast, even while repairing broken connections. We incorporate an assessment philosophy and reproduction results to accept the right and productive operation of the AODV calculation. Yunjung Yi et al., proposed ODMRP. It is a cross section based, as opposed to a traditional tree-based, multicast plot and utilizes a sending bunch idea (just a subset of hubs advances the multicast parcels by means of checked flooding). It applies on-interest methodology to powerfully assemble courses and keep up multicast bunch enrollment. ODMRP is appropriate for specially appointed remote systems with versatile hosts where data transfer capacity is restricted, topology changes much of the time and quickly, and force is obliged.

Felipe Tellez et al gave answers for an elliptic bend cryptosystem (ECC) [8] is suitable to Ad-Hoc systems and it adequate to guard, distinguish, keep away from the Wormhole assaults. VadhadiyaJanki et al give security to join the incorporating module, in that to utilize distinctive sorts of calculations such as RSA, MD 5, SHA-1, and other encryption decoding calculation and additionally steering calculation. VaidehiPanwala et al proposed on interest and beneficiary started approach multicast steering convention called Adaptive Multicast to increase better Quality of Service in Wireless Networks. Yogesh Joshi et al proposed and executed a novel way to deal with settle man in the center assault over SSL which utilizes the authentic site URL. To handle such assaults we propose hashing the client secret word with the general population key of the server's advanced authentication. Zhen Cheng et al proposed the calculation for elliptic bend Diffie-Hellman key trade taking into account DNA tile self-get together. To start with we give the DNA [9] tile self-get together model to figure the scalar duplication, and then we can effectively execute the Diffie-Hellman key exchange over elliptic curve [9] by dig out the result constituent of the scalar exponentiation.

3. MULTICAST ROUTING PROTOCOLS

In general the multicast routing protocols used in mobile ad hoc networks are broadly classified into two broad categories one is Tree based multicast routing protocol and other is Mesh based multicast routing protocol.

3.1. Tree based multicast routing protocol

Tree based multicast protocol maintains shared medium with a single link to establish communication between source to destination. The examples of Tree based multicast protocols are AMRIS [10] and MAODV. Here, in this paper we chosen MAODV to compare with mesh based protocols. So we will discuss the MAODV. MAODV is a receiver initiated tree based protocol and it is the extension of AODV routing protocol. MAODV [10] inherited the control messages like Route REQest (RREQ), Route REPly (RREP), Multicast AcTivations (MACT) and GrouP Hello (GRPH) from AODV [11] protocol. Connection process: MAODV creates routes [12] on demand. Source node injected to broadcast the RREQ packet into network to establishing the connection with receiver. Receiver node is unicasted the RREP packet to the sender by same forwarded path. Sender sends MACT packet to the receiver to intimate multicast path is established between them. Initial node in the group acts as a controller of the group and also responsible for maintaining and broadcasting the group sequence numbers to multicast group. Nodes identifies the group leader by using GRPH. The main goal of MAODV is to build the tree after completion of multicast network. In MAODV, controller node maintains up to date information of multicast tree because if any link is destroyed in a group then the path will be lost. MAODV is vulnerable from man in the middle attack. It broadcast route request packet into the network, noxious nodes are present in the communication path and observes the data flow. Due to this attack, the performance of MAODV is degraded slightly.

3.2. Mesh based multicast routing protocol

Mesh based multicast routing protocol maintains multiple paths and forms a mesh network. Examples of mesh based multicast routing protocols are ODMRP and PUMA. The On-Demand Multicast Routing Protocol (ODMRP) is a source started on-interest lattice based steering convention. ODMRP [13] is works for both unicast and multicast exchanges. The association strategy of ODMRP comprises two stages like piggybacking those are solicitation stage and answer stage. In the solicitation stage sender surges join question parcel into the system. The bundle achieves the neighboring hubs furthermore surges from those hubs lastly achieves the recipient hub. After destination hub gets the join inquiry parcel then it produces the join table. Join table comprises multicast bunch address, succession of source address and neighboring hub address, jump check. On the off chance that any hub gets join table then it checks the following hub location of one of the passage is its location then it distinguishes it is in a sending way to a source hub. After that it advances join table to next jump hubs. Each time network hubs keep up the breakthrough data. Be that as it may, this directing convention is defenseless against man in the center assault. As a result of the openness and absence of trusted power MITM assault is propelled and adjust the system execution measurements.

The other mesh based multicast routing protocol is Protocol for Unified Multicasting through Announcements (PUMA) [14] in which Panther is cross section based element collector started approach and backings to send multicast information alloted to a given multicast gather and don't require separate unicast directing system since it goes about as both multicast and unicast. Jaguar utilizes a control message to control for every one of its operations, i.e. multicast declaration bundle (MAP). Every MAP determines arrangement number, bunch ID (location of the gathering), center ID (location of the center), separation to the center to hubs (bounce tally), work part hail (either True or False), and a guardian hub that expresses the sought neighbor to achieve the center. Fresher MA parcel have a higher succession number than going before MAP sent by the same center. Taking into account the data contained in such control bundles, hubs progressively choose the centers, decide the courses for non-part aggregate hubs to multicast bunch, tell about the joining or leaving in the cross section amass and keep up the lattice system of the gathering.PUMA have 5 functions to maintain mesh and connectivity procedure those areConnectivity List record and transmission of Multicast Announcements, Mesh Establishment and Maintenance, Core Election process, Forwarding Multicast Data Packets and Recycling Sequence Numbers.

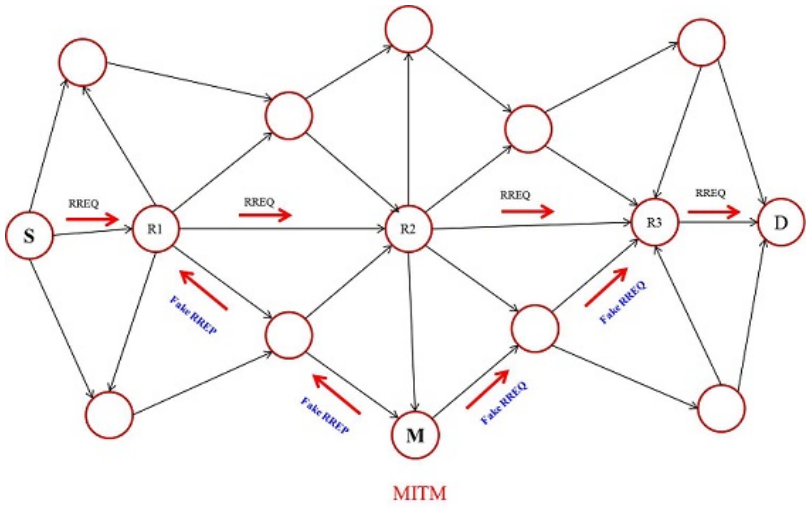

Figure 1. Man in the Middle attack Scenario

4. MODELING A MAN IN THE MIDDLE ATTACK

In the man in the middle attack**,** the attacker can put himself in the middle of the communication by impersonating both the source node and destination node. Let us illustrate with an example how MITM [15] can be launched in PUMA routing protocol. Here, an MITM node can send MA with its address to another node in the group to impersonate the receiving node, Attacker node can modify the hop count data as it has the shortest path to the destination by sending a MA to the source node, The attacker repeatedly sends MA packet to the source node with its radio range moreover, this malicious node do not forward the MA packets to the source node which was received from its intermediate node. Which may leads to the connection failure. Hence, the functionalities of PUMA makes more vulnerable to launch MITM attack, which may degrade the performance of the PUMA routing protocol.

5. SECURING MULTICAST GROUP COMMUNICATION THROUGH ECGDH

5.1. Review of Elliptic Curve Cryptography

Elliptic curve is a two dimensional curve. The standard curve equation is $y^2=x^3+ax+b$ with special constraint $4a^3+27b^3\neq 0$. One of the public key cryptography mechanism is Elliptic curve cryptography [15] and its use has been increased tremendously in recent years because the use of larger key size in remaining public key mechanisms like RSA, digital signatures, Diffie-hellman, etc. Elliptic curve cryptosystems [8] provide more efficiency in computations and offer strong equivalent security with smaller key sizes. The resources like bandwidth, storage capacity, processing speed are used more in Elliptic curve cryptography.

ECC have two fields, those are prime Galois Field (p) and binary extension Galois Field GF (2^m). Prime field uses all real numbers, rational numbers and complex numbers. Binary field is used to calculate keys in binary format. ECC have some efficient algorithms for finite field operations such as addition, multiplication and inversion. These specialized algorithms are evaluated with the help of the discrete logarithms (by mod operations). Elliptic Curve domain parameters are used to represent the elliptic curve cryptography. The parameters are **T= { $E(F_p)$, n, a, b, G, p, m_i, $P_u(S_a)$, $P_r(S_i)$}**

$E(F_p)$	:	Elliptic curve equation
N	:	Order of group
a, b	:	Curve coefficients
G	:	Group generator point (Gx,Gy)
P	:	Prime base point p ϵ $E(F_p)$
m_i	:	i-th group member i ϵ [1,n]
$P_r(S_i)$	:	Private Secret key of m_i (a random integer)
$P_u(S_i)$	:	Public key of m_i, calculated through scalar multiplication operation

5.2. Diffie Hellman Algorithm Using Elliptic Curve Cryptography

Multicasting is a group communication mechanism. To secure these multicast communications, group key management key exchange methods are used. One of the well-known multicasting routing protocols is PUMA, it is a receiver initiated approach likewise elliptic curve group diffie-hellman is also receiver initiated approach it means new node acts as a group controller. So we implemented Elliptic curve group diffie-hellman mechanism to provide security for PUMA routing protocol.

Algorithm: Elliptic Curve Diffie-Hellman

Step 1 : $N_a \leftarrow P_r(S_a)$ and $N_b \leftarrow P_r(S_b)$

Step 2 : Calculate

$N_a \rightarrow P_u(S_a)$

$N_b \rightarrow P_u(S_b)$

$P_u(S_a) \leftarrow P_r(S_a) * G$

$P_u(S_b) \leftarrow P_r(S_b) * G$

Step 3 : $N_a \xrightarrow{\text{sends } P_u(S_a)} N_b$

Step 4 : $N_b \rightarrow S_k(N_b)$

$S_k(N_b) \leftarrow P_r(S_b) * P_u(S_a)$

Step 5 : $N_b \xrightarrow{\text{sends } P_u(S_b)} N_a$

Step 6 : $N_a \rightarrow S_k(N_a)$

$S_k(N_a) \leftarrow P_r(S_a) * P_u(S_b)$

Step 7 : $S_k(N_{a,b}) \rightarrow S_k(N_a) = S_k(N_b)$ else got problem in computation

The above algorithm generates secret key for two party communications. Let us Assume Node 'a' N_a and node 'b' N_b wants to communicate securely through a secret key. Firstly, N_a and N_b randomly selects private keys $P_r(S_a)$, $P_r(S_b)$ respectively. Next, both nodes generate public keys $P_u(S_a), P_u(S_b)$by using group generator point and exchanging their public keys into each other after that both nodes calculate secret keys $(S_k(N_a), S_k(N_b))$individually and finally, both must generate equal results.

Algorithm: Joining of new node in to the multicast group

Step 1 : $N_c \leftarrow P_r(S_c)$

Step 2 : Calculate

$N_c \rightarrow P_u(S_c)$

$P_u(S_c) \leftarrow P_r(S_c) * G$

Step 3 : $N_{gm} \xrightarrow{\text{sends } P_u(S_a), P_u(S_b), S_k(N_{a,b})} N_c$

Step 4 : Calculate

$N_c \rightarrow P_u(S_{c,a}) P_u(S_{c,a}) \leftarrow P_r(S_c) * P_u(S_a)$

$N_c \rightarrow P_u(S_{c,b}) P_u(S_{c,b}) \leftarrow P_r(S_c) * P_u(S_b)$

$N_c \rightarrow S_k(N_{a,b,c}) S_k(N_{a,b,c}) \leftarrow P_r(S_c) * S_k(N_{a,b})$

Step 5 : $N_c$broadcasts intermediate key to N_a, N_b

$N_c \xrightarrow{\text{sends } P_u(S_{c,a})} N_b$

$N_c \xrightarrow{\text{sends } P_u(S_{c,b})} N_a$

Step 6 : Calculate

$N_a \rightarrow S_k(N_{a,b,c}) S_k(N_{a,b,c}) \leftarrow P_r(S_a) * P_r(S_c) * P_u(S_b)$

$N_b \rightarrow S_k(N_{a,b,c}) S_k(N_{a,b,c}) \leftarrow P_r(S_b) * P_r(S_c) * P_u(S_a)$

The above algorithm shows joining of new node into the multicast group. Suppose, if a node N_c wants to join in a group. First it sends join request message to group manager. Group manager will grant permission to new node N_c. node N_c selects one private key $P_r(S_c)$ and generate public key $P_u(S_c)$. Group manager sends all the intermediate keys to new node N_c. After receiving all the keys from GM, N_c acts as a new group manager and calculate the new keys by using the intermediate keys which are received by old GM. Finally it broadcast the keys into remaining group members. Those perform computations on received keys and generate a new group key.

Algorithm: Joining of n new nodes into the multicast group

Round $i \in [0, n-2]$

$$N_i \xrightarrow{G*\left(\prod P_r(N_k)|k\in[0,i]\wedge k\neq j|j\in[0,i]\right),G*S_k(N_{0.....i})} N_{i+1}$$

$$N_{n-1} \xrightarrow{G*S_k(N_{0.....i-1\ i+1.....n-1})} N_i$$

In a large group, if a node wants join in that group previous node sends all the intermediate keys to joining node and broad cast to remaining group members. The above equations represents sending and broadcasting in round i.

Algorithm: Leaving the node from the multicast group

These two topological protocols are differ in redundancy of the paths between source and destination. Whereas tree-based multicast protocols [15] provide only a single path and mesh-based protocols provide multiple paths between source node to destination nodes. In multicasting, robustness and reliability both are very important and these parameters are high in mesh based networks. Examples of mesh based protocols are [16] PUMA and ODMR, CAMP.

Algorithm:

Step 1 : $N_l \xrightarrow{\text{quit REQ}} N_{gm}$

Step 2 : $N_{gm} \leftarrow \text{new } P_r(S_{gm})$

Step 3 : Calculates

$N_{gm} \rightarrow P_u(S_{gm})$

$P_u(S_{gm}) \leftarrow \text{new}P_r(S_{gm}) * G$

Step4 : N_{gm} broadcasts intermediate key values to all group nodes

Step5 : Nodes generates group key using their P_r

The above algorithm discusses how the node leaves from the multicast group. Node N_l want to leave from a group First it sends quit request (QuitREQ) to group manager N_{gm}. Group manager grant permission and changes his private key. Next, Group manager calculates public key, intermediate keys and broadcast to all group member. Group members generate group key by using their private keys.

If Group manager wants to leave

Step 1 : $N_{gm} \xrightarrow{\text{quit REQ}} \text{previous } N_{gm}$

Step 2 : Call leaving algorithm

Special case: Suppose, if group manager wants to leave from a group it sends quit request to previous group manager. New Group manager grant permission and changes his private key. Next, Present group manager calculates both public key and intermediate keys which broadcast to all group members in a group. Finally, all thegroup members will generate group key using their private keys.

5.3. Securing PUMA multicast routing protocol using ECGDH

PUMA is a receiver initiated approach and also establishes a mesh network to communicate among the group. The attacker will exploit the weakness of PUMA (a node can join in a group without any constraint) to launch MITM attack [17]. The attacker has a chancetoenterintothegroupandmaydropor alter the packets without forwarding to their neighboring nodes. We proposed Elliptic curve group diffie-hellman security mechanism to protect the multicast communications. In this proposed work, in a group one node will be elected as a group controller using ECGDH [18] mechanism, which is discussed in section V. We also proposed securely joining and leaving algorithms for authentication of mobile nodes in a group.Moreover, all the nodes in a group will communicate with a single group key which is generated by all the group nodes. This proposed ECGDH provides backward and forward secrecy when the nodes want to join or leave from the group.In backward secrecy, new node cannot obtain past communication. Whilein forward secrecy leaving node cannot access present group communication. Hence, in both the cases past and present information cannot be obtained by the nodes. On the other hand, if any of the node misbehaves unauthorized functions like not forwarding the data packets to the neighboring node and giving false information such as shortest hop count. In such cases the group controller will observes and discarded from the multi cast group.

6. SIMULATION RESULTS

In this paper, we compare PUMA with 4 parameters: Throughput, Packet delivery fraction, Control overhead, Total overhead with respect to Number of nodes in a group. In Figure 2 shows the graph of packet delivery fraction Vs number of nodes in a group from 5 to 100 respectively under legitimate, man in the middle attack and after providing security against attack situations. Legitimate situations gives high pdf compare to remaining situations. But other side man in the middle attack degrades the performance of pdf so for defending this attack we propose a security mechanism called ECGDH explained in Section V. After providing the security to PUMA routing protocol, the performance of Packet delivery has increased and given better results compared to man in the middle attack situation.

Figure 3 shows the graph of PUMA routing protocols throughput Vs number of nodes in a group from 5 to 100 without attack, with man in the middle attack and in security. If throughput is high then it indicates that maximum packets deliver to receiver. As usually throughput is higher in normal situations but it is degraded when the attack has happened. ECGDH improves the throughput performance even attack has happened or not. ECGDH security mechanism provides better throughput in attack scenario.Throughput is directly proportional to PDF. If PDF increases throughput also increases.

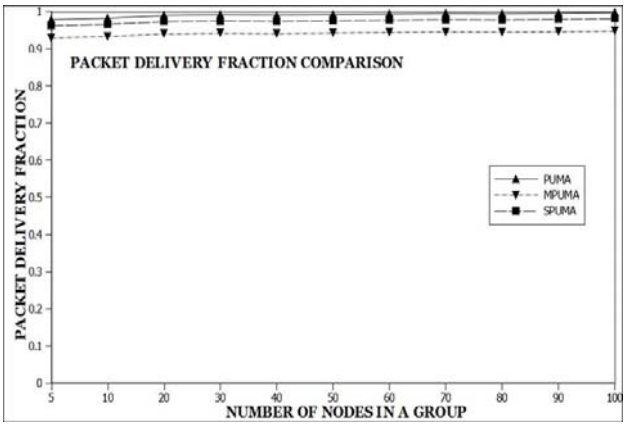

Figure 2. Packet delivery fraction of PUMA With and Without MITM AttacK Vs Secure PUMA

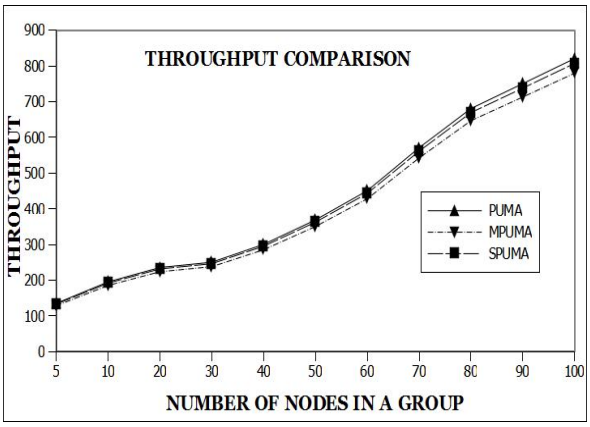

Figure 3. Throughput of PUMA With and Without MITM AttacK Vs Secure PUMA

Figure 4 depicts the control overhead Vs number of nodes in a group.Control overhead has increased when we provide security mechanism to our protocol compared to legitimate and normal situations. In normal situation control overhead maintains better results compared to attack scenario. Control overhead increases even though we provide the security. The main aim of security is controlling the attacks and traffic flow so control overhead has increased in after providing security.

Figure 5 depicts about total overhead Vs number of nodes in a group. Control overhead directly proportional to total overhead.If control overhead has increased then total overhead also increases. Like control overhead, total overhead also higher in after security compared to legitimate and attack scenario. But in contrast to control overhead, total overhead decreases when number of nodes in a group increases.

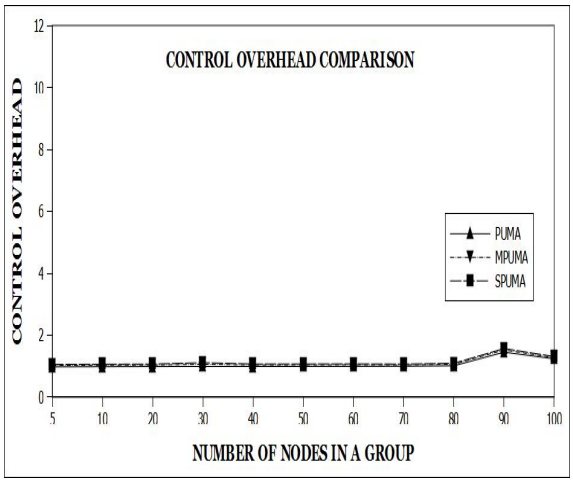

Figure 4. Routing Overhead of PUMA With and Without MITM AttacK Vs Secure PUMA

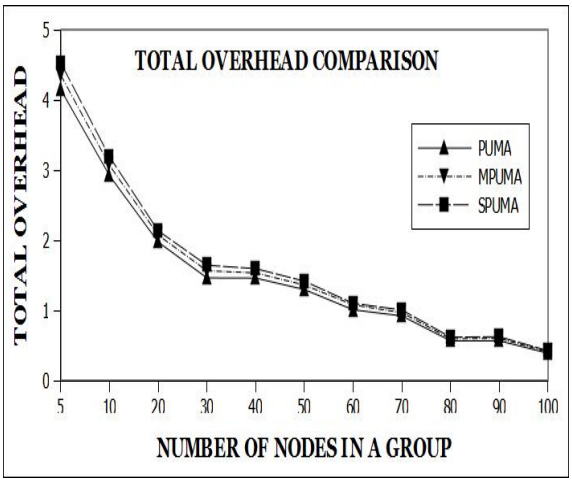

Figure 5. Total overhead of PUMA With and Without MITM AttacK Vs Secure PUMA

7. CONCLUSION

Mobile adhoc network is an infrastructure less network that has no trusted authority. In such type of networks, group communication is one of the important communications for various applications. Multicasting Mechanism can be applied to achieve this group communication. In this paper, we used PUMA routing protocol which provides better results compared to other mesh protocols.However, This routing protocols suffers from man in the middle attack. To defend this attack, we proposed a novel method Elliptic Curve Group Diffie Hellman (ECGDH). Finally, we compared PUMA routing protocol under normal situation, under attack scenario and defending with ECGDH security.

REFERENCES

[1] R. Vaishampayan and J. J. Garcia-Luna-Aceves, "Protocol for unified multicasting through announcements (PUMA)," in *Proceedings of the IEEE International Conference onMobile Ad- Hoc and Sensor Systems (MASS '04)*, 2004.
[2] IEEE, "IEEE Standard 1363-2000: Standard specifications for public key cryptography," IEEE, 2000.
[3] E. Babu, *et al.*, "An Implementation and Performance Evaluation Study of AODV, MAODV, RAODV in Mobile Ad hoc Networks," vol. 4, pp. 691-695, 2013.
[4] E. Babu, *et al.*, "An Implementation Analysis and Evaluation Study of DSR with Inactive DoS Attack in Mobile Ad hoc Networks," vol. 2, pp. 501-507, 2013.
[5] F. Blake, *et al.*, "Advances Elliptic Curves in Cryptography," Cam-bridge University Press, 2005.
[6] J. Liu and J. Li, "A better improvement on the integrated diffie-hellman-dsa key agreementprotocol," *International Journal of Network Security*, vol/issue: 11(2), pp. 114–117, 2010.
[7] E. Babu, *et al.*, "Inspired Pseudo Biotic DNA based Cryptographic Mechanism against Adaptive Cryptographic Attacks," *International Journal of Network Security*, vol/issue: 18(2), pp. 291-303, 2016.
[8] E. Babu, *et al.*, "Light-Weighted DNA-Based Cryptographic Mechanism Against Chosen Cipher Text Attacks," *Advanced Computing and Systems for Security,* Springer India, pp. 123-144, 2016.
[9] Y. Wang, *et al.*, "The Performance of Elliptic Curve Based GroupDiffie-Hellman Protocols for Secure Group Communication over Ad Hoc Networks," *IEEE International Conference on Communication*, vol. 5, pp. 2243–2248, 2006.
[10] E. Babu, *et al.*, "Light-Weighted DNA Based Hybrid Cryptographic Mechanism Against Chosen Cipher Text Attacks," *International Journal of Information Processing and Indexed With arXiv*, Indian Citation Index, 2015. ISSN-0973-821.
[11] M. J. Moyer, *et al.*, "A Survey of Security Issues in Multicast Communication", *IEEE Network*, pp. 12–23, 1999.
[12] O. S. Badarneh and M. Kadoch, "Review Article Multicast Routing Protocols in Mobile Ad Hoc Networks: AComparative Survey and Taxonomy," *EURASIP Journal on Wireless Communications and Networking*, 2009. Article ID764047, 42 pages doi: 10.1155/2009/764047.
[13] S. Kumar, *et al.*, "An Empirical Critique of On-Demand Routing Protocols against Rushing Attack in MANET," *International Journal of Electrical and Computer Engineering*, vol/issue: 5(5), 2015.
[14] A. Gopi, *et al.*, "Designing an Adversarial Model Against Reactive and Proactive Routing Protocols in MANETS: A Comparative Performance Study," *International Journal of Electrical and Computer Engineering*, vol/issue: 5(5), 2015.

[15] H. Deng, *et al*., "Routing security in wireless adhocnetworks," *IEEE Commun. Mag*., vol/issue: 40(10), pp. 70–75, 2002.
[16] P. Sinha, *et al.*, "CEDAR: aCoreExtraction Distributed Ad hoc Routing algorithm," *IEEE INFOCOM'99*, 1999.
[17] E. Babu, *et al.*, "An Implementation and Performance Evaluation of Passive DoS Attack on AODV Routing Protocol in Mobile Ad hoc Networks," *International Journal of Emerging Trends & Technology in Computer Science*, vol/issue: 2(4), pp. 124-129, 2013.
[18] E. Babu, *et al.*, "Efficient DNA-Based Cryptographic Mechanism to Defend and Detect Blackhole Attack in MANETs," in *Proceedings of International Conference on ICT for Sustainable Development*, Springer Singapore, pp. 695-706, 2016.