Self-Organized Hash Based Secure Multicast Routing Over Ad Hoc Networks

Amit Chopra
PhD Research Scholar, CSE dept.
MMEC, M. M. University
Ambala, HARYANA, INDIA

Dr. Rajneesh Kumar
Professor, CSE dept.
MMEC, M. M. University
Ambala, HARYANA, INDIA

Abstract—**Multicast group communication over mobile ad hoc networks has various challenges related to secure data transmission. In order to achieve this goal, there is a need to authenticate the group member as well as it is essential to protect the application data, routing information, and other network resources etc. Multicast-AODV (MAODV) is the extension of an AODV protocol, and there are several issues related to each multicast network operation. In the case of dynamic group behavior, it becomes more challenging to protect the resources of a particular group. Researchers have developed different solutions to secure multicast group communication, and their proposed solutions can be used for resource protection at different layers i.e. application layer, physical layer, network layer, etc. Each security solution can guard against a particular security threat. This research paper introduced a self-organized hash based secure routing scheme for multicast ad hoc networks. It uses group Diffie-Hellman method for key distribution. Route authentication and integrity, both are ensured by generating local flag codes and global hash values. In the case of any violation, route log is monitored to identify the malicious activities.**

Keywords—Security; Multicast; Group Communication; MAODV; Key management; HASH

I. Introduction

Multicast based communication is a vital network service, which sends the data from a source to multiple destinations simultaneously by creating copies only when the links to the destinations split. Multicast routing tree can be constructed to transmit the data from the sender to all the destinations with a minimum multicast tree cost that is used to evaluate the utilization of network resources [1]. Multicast packets are transmitted to all members of a group with the same reliability as regular unicast packets. Multicasting can reduce the cost of communication, consumption of bandwidth, sender and router processing and delivery delay [2].

A. Security issues and challenges

Multicast Ad hoc networks operate in open environment having no access constraints to the network resources. Following are security issues related to network operations:

- Secure routing issues: Use of Shared medium, open network environment, Lack of Centralized Monitoring, Limited Resources, Physical vulnerability [3].
- Network Security Issues: Confidentiality, Integrity, Availability, Non-Repudiation [3].

B. Security Attacks over Multicast Ad Hoc Networks

Multicast communication supports both unicast and multicast operations, so various security attacks can be categorized as per these activities which are given below [6][12][20]:

- Unicast Operation Attacks: Black Hole Attack, Worm Hole Attack, Sybil Attack, Flooding Attack, Routing Table Attack, DoS Attack [33]
- Multicast Operation Attacks: MACT-Attacks, Group Lead Selection Attack, Link breakage Attack, Routing Table attack [20][21].

C. Security Constraints of Multicast Group Communication

It is quite complicated to enforce security rules for group communication due to various facts i.e. Dynamic Group Behavior, Group Operations: Join/Leave, Open Communication: Inside/Outside the Group etc. Security requirements should consider Group Member Authentication, secure key distribution/management, detection/prevention of any threat to the group or entire network, mobility and scalability, etc. Following are the different categories of security provision for group communication:

- Key-based Secure Multicast Routing: With this kind of security provision, any key distribution method based on cryptographic algorithms can be used to secure the group communication. Each group member exchanges the keys for communication. Key distribution faces some issues like key pair production, distribution and management, etc. Key-based communication becomes more challenging for scalable and dynamic groups. Shared Keys are used for node Identification purpose, called authentication which may be quite time-consuming process and its performance depends upon the number of keys to be processed and the number of participants involved in group communication [29][30][31[32].
- Key Generation: It is essential to secure data transmission over open shared medium which may have several security threats. Cryptography is a process that is used to secure data. One can use any cryptography method (Symmetric/Asymmetric) to maintain the level of confidentiality and integrity [11].
- Key Distribution: Key distribution is a process which assigns the generated keys to each node. There are

different ways for Public/Private Key generation and distribution [32]. After key pair generation, it is also essential to distribute them in a secure way to legitimate group members only. Key distribution process can be performed using key agreement protocols. For secure communication, one can use Diffie–Hellman/Needham–Schroeder protocol for symmetric key distribution or any certification authority for asymmetric key distribution [29].

- Key Management: For key pair management, one can use centralized, decentralized or distributed approach. All key management schemes enforce the rules for secure group communication by utilizing the basic concept of cryptography [32].

D. *Intrusion Detection and Prevention*

In this case, any unauthorized access to network resources can be referred as intrusion or attack and the methods those can identify its symptoms, called intrusion detection tools [21]. Intrusion detection depends upon various factors i.e. routing information, packet drop, extra control overhead, unavailability of services, flooding, over consumption of network resources, signal jamming, etc. Following are the categories security threats:

- Active attack: An intruder can directly modify the resources, and it can be detected.
- Passive attack: The Intruder just analyzes the network information without any alteration. Captured data may be further utilized to trigger another type of attack [3], and it is quite difficult to observe the passive attacks.

This article contains different sections i.e. Section-I introduce the basic requirements of secure multicast communication, Section-II explores the related research work in relevant fields. It provides brief overview of the key based security solutions, and also investigates some intrusion detection/prevention schemes, Section-III explains proposed scheme, Section-IV & V describes simulation setup/results, Section VI shows the security analysis and Section-VI concludes the outcome of the proposed scheme and its future use.

II. Related Work

A. *Key based security solutions*

As per above discussion, Researchers have developed various solutions to secure multicast network operations by introducing the concept of group key generation, Key distribution, mutual authentication for dynamic groups, secure group key exchange, intrusion detection and prevention algorithms etc. Hui Xia et al. [4] proposed a multicast trusted routing algorithm with QoS multi-constraints which is based on a modified ant colony algorithm. This algorithm combines the security trusted model and the modified tree based ant colony algorithm with the QoS multi constraints and this combination is used to explore the trustworthy multicast forward paths that prevents the network from various security threats.

Dr. N. Sreenath et al. [5] proposed an enhancement for the Secure Enhanced-On Demand Multicast Routing Protocol (EODMRP) to prevent it from various security attacks such as flooding and black hole attacks. Simulation results show that there is some improvement in packet delivery ratio in presence of black hole attack, with marginal rise in average end-to-end delay and normalized routing overhead and in case of flooding attack, it uses simple statistical packet dropping method that prevents the attacks from malicious nodes effectively.

Ahmed. M. Abdel et al. [6] explored the new possible security threats which can degrade the performance of multicast ad hoc routing which includes the different network operations i.e. election of group lead, link errors, repair and route management etc. To interrupt group lead selection process, intruder tries to select a node as lead that does not belong to multicast tree and later on group can be split into multiple groups. Intruder can also send the route repair requests for the routes which actually do not exists, in order to initiate real route maintenance for entire network. To protect the network against these attacks, hop by hop authentication method can be used to validate each route request and certificate based approach can be used to identify the group members and it can also be used for leader election process as well as for route maintenance. Simulation results show its performance in terms of improved PDR under the constraint of compromised network resources.

Ratna Dutta et al. [7] proposed and analyzed a generalized self-healing key distribution using a vector space access structure in order to reach more flexible performance of the scheme. Proposed method reduces storage, communication and computation costs over previous approaches, and is scalable to very large groups in highly mobile, volatile, and hostile wireless networks.

Sencun Zhu et al. [8] presented an overview of the various approaches that have been recently proposed to address the group key management issues and finally discussed several new research directions. Authors focused on ad-hoc and sensor networks and explored most common issues related to detection of compromised nodes, key distribution, Group rekeying schemes etc.

Zahraa Sabra et al. [9] proposed end user solution which is capable to provide secure environment for VoIP communication with respect to QoS parameters using hybrid ad hoc networks. They used AES, ECC192 to implement security features and Voice codec G.729b for simulation purpose.

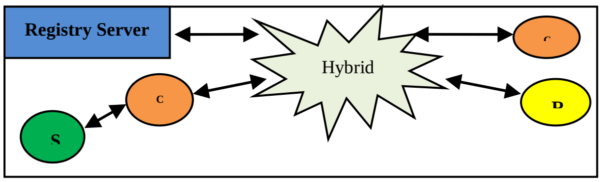

Fig. 1. Hybrid Network [9]

Fig. 1 above shows that as per the proposed scheme, Sender and receiver can communicate through cluster heads which are randomly selected and these are connected to hybrid networks. Shared keys are computed using SHA-512. Sender side cluster head sends query to Registry server which is forwarded to receiver side cluster head. If cluster heads share same keys, only then a link is established on the basis of authentication, after that sender and receiver can start VoIP communication. If a new cluster head is selected then registry server updates this information. Simulation results show that this scheme offers authentication against non-repudiation and traceability under QoS constraints.

Vennila Rajamanickam et al. [10] proposed an inter cluster communication and rekeying technique for multicast security in MANET using shared private keys generated by key manager. Low cost rekeying method is used when a node joins the cluster. Simulation results show the efficiency of proposed method in terms of low overhead and less computation cost.

E.A.Mary Anita et al. [11] designed a Worm Hole Secure ODMRP (WHS-ODMRP) that uses a certificate based authentication method in route discovery process. Authors also analyzed the performance of On Demand Multicast Routing Protocol (ODMRP) under the attack of worm hole using different scenarios. Simulation results show the comparison of WHS-ODMRP and ODMRP protocols and proved that proposed protocol can enhance the performance by reducing the packet loss caused by malicious nodes.

E.A.M. Anita [12] proposed a certificate based localized authentication scheme to prevent Sybil attack. Results show that the proposed method can sustain the Sybil attack and it is able to maintain the network performance in terms of throughput.

Jiwen Guo et al. [13] proposed a secure minimum-energy multicast (SMEM) algorithm to ensure multicast communication. In order to improve the stability of trust mechanism, the new trust values (calculated by the Bayesian theorem in CR networks) are modified by the iterative control criterion. Trust mechanism aims at guaranteeing the security of network environment, in which the trust information is encrypted to ensure the creditability of trust values. Results show that the time complexity of SMEM algorithm is polynomial.

Ding Wang et al. [14] investigated authentication related issues and presented a improved scheme to prevent the attacks over user credentials, called Kim-Kim scheme. Proposed Scheme offers three different phases i.e. first of all users are registered and key pairs (public & private keys) are produced as saved on server side. Whenever user wants to communicate with other, produced keys are saved on user’s device and to initiate communication, user side and server side credentials are used for mutual authentication purpose. Authors also investigated the potential threats for the proposed schemes i.e. compromise of node, keys, shared medium or server’s session etc. They performed cryptanalysis for each possible threat and they also raised some open issues like dependency of security goals over cryptography methods and offline security threats etc.

Babak Daghighi et al. [15] explored the various schemes which can be used for secure group communication and investigated the issues related to key exchange under the mobility constraints. They focused on the mobility of host as well as member in a group. It is quite complex to manage the validity of keys as any node can leave or join a group frequently. If a group member node leaves the group, that node should not be able to reuse the keys as well as the other resources of the group. If a node wants to join the group, authentication is required but if its keys have been expired, then there is need to reproduce the keys again but regenerated key should be unique. Frequently group updates may lead to extra overhead on group communication, storage key pool for group members and can affect the scalability, reliability and QoS etc. In order to develop a solution for secure group communication, all above factors are considered by researchers and they developed few solutions i.e. KMGM, GKMW, HKMS, TMKM, CDLM, HSK, FEDRP, GKMM, LKH, BALADE, KTMM, WSMM, M-IOLUS and SHKM etc. but each solution has its own limitations and there is requirement to explore Key management in highly mobile environment with the provision of QoS support which is essential for secure group communication.

Lin Yao et al. [16] developed a distributed key management scheme which can preserve the keys for nodes. Nodes can utilize the keys on the basis of their trust levels maintained by different nodes. Trust level of keys can protect from the various attacks and node can easily select the keys on the basis of their trust levels and it can eliminate the requirement of certification authority. Analytical and simulation models developed for this scheme show its performance in terms of less control overhead and efficient key management.

Lein Harn et al. [17] proposed an enhanced key management scheme using group Diffie–Hellman (GDH) key agreement protocol by introducing secret sharing method. Analytical model shows its performance in terms of its resistance against the well-known attacks over shared keys.

B. Security solutions forIintrusion Ddetection and Prevention

V.Srihari et al. [18] did a survey of the security threats and their remedies for VoIP/SIP protocols. As per their studies, security attacks can be introduced on session management, signaling, call control and credits etc. For detection and prevention, service providers can use intrusion detection system, fake call monitoring system, call analysis and pattern recognition etc.

Jiazi Yi et al. [19] did vulnerability analysis of Relay Set Selection (RSS) algorithms for the Simplified Multicast Forwarding (SMF) Protocol which is used in mobile ad hoc networks. Study shows that network topology can be compromised by misconfigured routers or malicious nodes by using spoofing. Attackers can also inject information conflicts for RSS decision making process. To enable the security provision, authors explained the various attack vectors for different RSS algorithms.

A.m. Pushpa et al. [20] propose multicast activity-based overhearing technique to identify this attacker node in the multicast group. They analyzed the multicast announcement packet fabrication to keep the track of group behavior and on the basis of threshold value, nodes can be isolated from network. Each node collects the feedback for a specific node and also considers the feedback status about that node to make the final decision. If all feedback collected about a particular node below then the threshold, then it is finally isolated from entire network. Simulation results indicate the impact of attack on the performance metrics such as Packet Delivery Ratio (PDR) and delay of PUMA and MAODV multicast routing protocols. Results show the efficiency of proposed scheme in terms of detection of malicious nodes w.r.t. less control overhead and false negative alarm rate. Proposed scheme can be extended to identify the attacks over parent selection method, which is used by tree based multicast routing protocols.

J.K.Harika et al. [21] proposed a secure multicast protocol for intrusion detection systems that uses hybrid cryptography to isolate the unwanted network overhead. In hybrid scheme, nodes can negotiate the session key for secure communication that fulfils the requirement of Authentication. Results show that the proposed scheme can defend the network from various attacks such as reply attack, rushing attack, IP spoofing and man in the middle attack etc.

A. Fidal castro et al. [22] proposed an artificial intelligence based solution which utilizes the analytical equations for network intrusion detection and prevention and can guard against several attacks i.e. black hole, Neighbor, route disruption etc. It builds the new rule as per the identified attack and this information is shared with each node. Simulation results show its performance in terms of rate of intrusion detection and response under the constraints of different mobility/traffic patterns.

Hui Xia et al. [23] proposed a scheme which estimates the route as per the assigned trust value and this value can be used to identify the attacker nodes. Trust level can be calculated for nodes as well as for routes also. For genuine and intruder nodes, different threshold values can be set and if any node's trust value is less than the recommended threshold, this can be identified as intruder. Node's trust level is used to build route's trust levels with route's state. Threshold value is updated, if there are variations in trust values and idle routes are identified and ignored by routing table. Performance of proposed scheme is evaluated by varying speed and density of intruders. This work can be extended further by considering various factors such as delay, threshold variations etc.

T. Stephen John et al. [24] developed an agent based method to identify the intruder nodes in network. Mobile agents are introduced by the sender node and they can adopt any forwarding route to find out any intruder. Broken routes are managed by intermediate nodes. ODMRP and D-ODMRP routing protocols were used for simulation purpose and results show ODMRP's performance is better than D-ODMRP in terms of delay, control overhead, PDR, energy utilization w.r.t. network size and node density etc. Proposed scheme can be extended ty introducing the concept of inter communication process for mobile agents.

Wei Yuan et al. [25] developed a routing scheme, called topology hidden multicast routing (THMR) which can isolate the routing information to prevent the network from well-known attacks over routing. Receiver insures the identification of sender and shared keys. Route information is isolated for intermediate nodes, in order to avoid the attack on routing table. To make a route request, first of all node produces shared keys for session using RSA algorithm and then generates broadcast messages which are validated by intermediate nodes. At the destination end, received packets are verified on the basis of the relevant keys and all are discarded, if their keys are already compromised. If packets are accepted then a replay is prepared using shared keys and this is again validated by intermediate nodes and finally it is accepted by source node. In case of route errors, short lived public keys are used to propagate broken link information and finally a new route is built, if it can't be repaired. It shows its resistance against various attacks i.e. impersonation, DoS, packet analysis, fabrication and routing attacks etc. Simulation results show its performance in terms of key computation time, delay and latency as compared to MAODV.

A. Menaka Push et al. [26] explored the packet drop/fabrication attack and introduced a watchdog algorithm based scheme to analyze it. For authentication purpose, it calculates the node's distance from core and each node keeps the track of its neighbor and in case of excessive packet drop, identified node is eliminated from group communication. If value of core's distance is altered by malicious node, then it can be identify by the neighbors by verifying the actual distance of core and its surrounding neighbors. If there is any difference between hop count and distance value, then current parent node can be identified as malicious node and finally it is neglected by group. Simulation results show it is able to maintain PDR and control overhead under the compromised situations but improvement in network performance and the impact of security threat, both depend upon the actual location of malicious nodes from the core and these two factors are inversely proportional to each other. Proposed scheme can be further enhanced for another multicast routing protocol.

P. Anitha et al. [27] developed a dynamic pre-keys distribution scheme to protect the network from Sybil attack and they Integrate the proposed scheme with On-Demand multicast routing, called S-ODMRP. Key distribution utilizes the relevant information of each node and common keys are used to establish a secure session and key can be easily validated, if it is common between two nodes. Simulation results show its performance in terms of improved PDR under the constraints of security threat.

N.M. Saravana kumar et al. [28] proposed a key management solution for multicast group operations. It can adopt dynamic behavior of group members as they can join/leave the group at any time using member authentication based on their signatures. Key pairs contain different subset of keys for inside or outside group communication. Key pairs enforce the rules for various operations i.e. group join/leave and data exchange etc. If any other node forcefully joins the group, that cannot access the information due to the absences of previously generated session/group keys. If ex-group member wants to re-join the group, as per the record of session keys, authentication can be done before group joining. Proposed method performs well under Security QoS constraints i.e. integrity, confidentiality, key calculation time, data processing time etc.

Xiao Wang et al. [29] explored the possible threats over multicast group communication and developed the solution by considering various factors i.e. mobility, scalability and key management etc. All nodes are arranged into self-organized form having one hop distance to each other and a Group manager (GM) is defined for multiple members. Diffie–Hellman key agreement protocol is used for key management and it uses different keys i.e. session key which is common for GM and group members, mobility key and a field keys are used when nodes move to another groups. Keys are generated for a particular group only. Keys are updated as per different network operations i.e. node movement, group join/leave, link breakage etc. Analytical and simulation models show the performance of proposed method in terms of consumed energy for key calculations, control overhead and efficient key management for groups etc.

III. Proposed Scheme

This paper presents a Secure MAODV Routing Solution based on Group Diffie-Hellman (GDH) Key distribution algorithm. Following are the basic steps of GDH algorithm (including Phase-I, II & III). Phase IV is used for node authentication before group joining.

```
Phase I: **Proc init (p,g)** {
//initialize all nodes and assign p,g values
            Initilize Node(s):=n;
            Calculateg();
           For each node $N_i$ {
          Assign ($N_i \rightarrow p, N_i \rightarrow g$) }                    (1)
**Proc Calculateg ()** {        p= getPrime()
//All nodes calculate the value of universal g on the basis
of initial value of G using private key i, for key exchange.
initial G=getPrimitiveRoot(p)
$Univeral\ g = \{N_i \rightarrow G^{a,b,c,d,e,f,\ldots n}\}$     }                (2)
Phase II: **Proc KeyExchange** ($N_i, N_j$) {
        $A_i = N_i \rightarrow g^a\ mod\ N_i \rightarrow p$                        (3)
        $B_j = N_j \rightarrow g^b\ mod\ N_j \rightarrow p$                        (4)
        $N_i \rightarrow key_i = B_j$                                  (5)
        $N_j \rightarrow key_i = A_i$            }                     (6)
Phase III: **Proc KeyAgreement** ($N_i, N_j$) {
         $s_i = N_i \rightarrow key_{i\square}^{a}\ mod\ p$                          (7)
         $s_j = N_j \rightarrow key_{i\square}^{b}\ mod\ p$                          (8)
         $N_i \rightarrow skey_{i\square}^{\square} = s_j$                              (9)
        $N_j \rightarrow skey_{j\square}^{\square} = s_i$    }                        (10)
Phase IV: **Proc Join_Group** ($N_i$) {
         If (IsAuthentic($N_i \rightarrow p, N_i \rightarrow g, N_i \rightarrow skey_{i\square}^{\square}$ )
         {        Set $N_i \rightarrow Join_{\square}$=True;
                  Update(Multicast Table, $N_i$)
         } else { Set $N_i \rightarrow Join_{\square}$=False; } }
```

A. Key Assignment and Node Authentication

To establish shared keys, all nodes participate in GDH algorithm key generation process to produce a universal value of g which cannot be reproduced by individual node. All candidates submit their private keys i.e. $\{N_1 \rightarrow G^a\}$, $\{N_2 \rightarrow G^b\}$, $\{N_3 \rightarrow G^c\}$,..$\{N_i \rightarrow G^n\}$ to produce g. After generating g, first node becomes group lead and starts key negotiation with upcoming members to generate key pairs for distribution purpose.

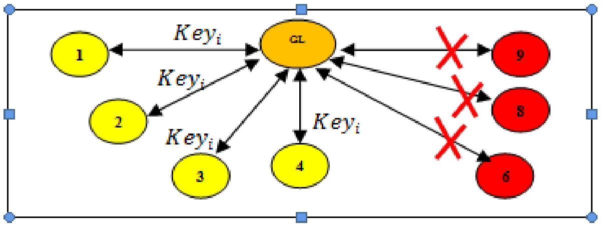

Fig. 2. Key assignment and node authentication

Once keys are assigned to each candidate node, group join process is initiated. During key negotiation and distribution process, if nonmembers try to join a group, they are authenticated on the basis of their $\{N_i \rightarrow G^i\}$ values and finally their group join requests are discarded. After successful key distribution process, local flag codes and global HASH values are generated and each member node is aware of these codes. If any member node does not verify the incoming and outgoing requests, activity logger generates alerts for authentication violations.

B. Control Message Authentication

A node can generate four different types of Route Requests: RREQ is used for route discovery and maintenance, RREQ-J for group joining, RREQ-R and RREQ-JR for tree merge. Only authorized nodes can generate RREQ messages with unique local flag codes. On the basis of these codes, incoming RREQ messages can be verified along with the encrypted flag to ensure route integrity and it is discarded, if local flag code of received RREQ does not match with the calculated local flag code.

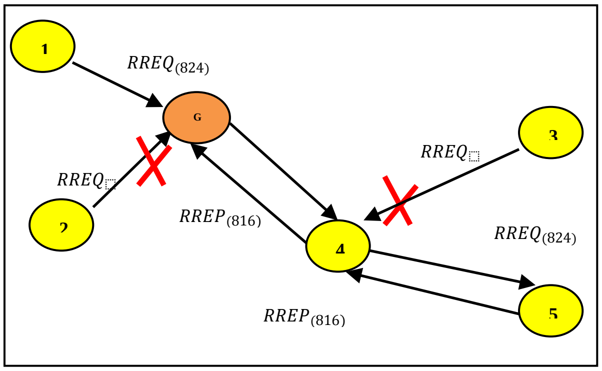

Fig. 3. Local Flag Codes

Table I. shows the list of local flag codes generated by one way HASH function during network operations. Following are the procedures used to verify the authenticity and integrity of messages. In case of any violation, Log alert messages are generated.

```
Proc setFlags (Msg, $S_i$)
{
Get_Local_Flag_Code($Msg \rightarrow Type, 1w\_Hash()$);    (11)
Get_Global_Hash_Value($Msg \rightarrow Type, SHA512()$);    (12)
        $encrypt(Msg \rightarrow flag, S_i \rightarrow key_i)$    (13)

LogInfo('Outgoing_Msg_From Node= $S_i$ at $Time = T_i$');
LogInfo('Outgoing Local Flag Code= $Msg \rightarrow Lfc$ at $Time = T_i$');
LogInfo('Outgoing Global Hash Value= $Msg \rightarrow Gh$' at $Time = T_i$);
}

Proc CheckFlags (Msg, $R_i$)
{
$Lf$ = Chk_Local_Flag_Code($Msg \rightarrow Type, 1w\_Hash()$);

$Gh$ = ChkGlobal_Hash_Value($Msg \rightarrow Type, SHA512()$);
                                                            (14)
      $d = decrypt(Msg \rightarrow flag, R_i \rightarrow key_j)$    (15)
       If ($Lf$ = $Gh$ = $d$ =True)
       {
         Accept=1;
       }
       else {
              Accept=0;
LogAlert ('Invalid_Msg_sent by Node= $S_i$ at Time=T' );
LogAlert ('Incomming Local Flag Code= $Msg \rightarrow Lfc$ at Time=T');
LogAlert ('Incomming Global Hash Value= $Msg \rightarrow Gh$' at $Time = T_i$); }
         return Accept;
       }
//Send a Message
        $S_i \rightarrow Send(setFlags(Msg, S_i), R_i,)$    (16)

//Receive a Message
       If ($R_i \rightarrow Recv$(CheckFlags($Msg$), $S_i$)==1)    (17)
        {
          $R_i \rightarrow accept(Msg)$
        }
        else {
        $R_i \rightarrow discard(Msg)$
        }
```

Where $Sender = S_i$, $Receiver = R_i$, in a particular group G_i, $at\ Time = T_i$, Msg indicates data to be sent, $Msg \rightarrow Type$ contains Request/Response control messages, $1w\_Hash()$ calls one way Hash function to calculate local flag code, $SHA512()$ calls SHA512 function to calculate global HASH values

Flag code based verification can filter the fake route requests and their replies. Unauthorized nodes cannot calculate local flag codes because these codes are available for group members only. SHA512 algorithm generates global HASH values which are used to ensure integrity of control messages.

TABLE I. LOCAL HASH CODES

MAODV Control Messages	Local Flag Codes
RREQ	824
RREQ-R	3208
RREQ-J	3976
RREQ-JR	6920
RREP	816
RREP-R	3200
RREP-J	3968
RREP-JR	6912
MACT-J	3998
MACT-P	3294
MACT-GL	7486
MTF-UP	3096
MTF-DOWN	15400
GRPH	932
GRPH-U	3316
GRPH_M	4084
HELLO-MSG	28938
Multicast Table Entry	22780518

If any node wants to a join multicast group, its keys are verified and a global HASH value is used for message authentication further. In case of invalid keys, all RREQ and RREP are discarded and if keys are valid but global HASH value based authentication fails, even then node cannot join the group. After successful joining of the group, activities of each node are logged and warning messages are generated for all unmatched flag codes and HASH values.

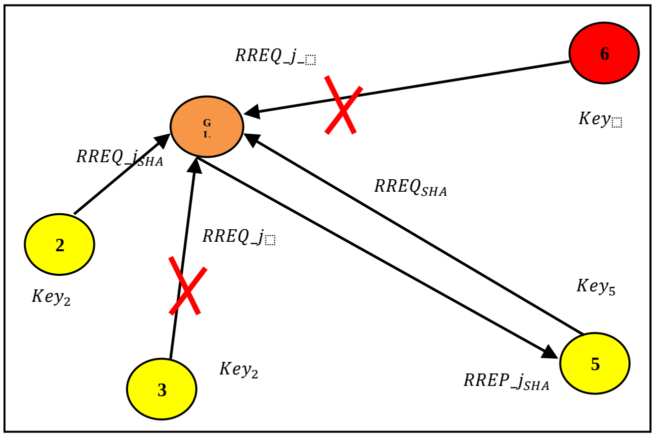

Fig. 4. Global HASH Values

Fig.4 above sows that RREQ_J of node 6 is discarded due to invalid keys, RREQ_J of node 3 is also rejected due to invalid global HASH value. REQ_J of node 2 and 5 is accepted due to successful message authentication.

C. Key Revocation

If any member node leaves a particular group, all assigned keys are revoked and that node cannot rejoin the group till further key negotiation.

TABLE II. GLOBAL HASH CODES

MAODV Control Messages	Global HASH Values
RREQ	8f9e705ccf9bbd05349fd0940428822385ddfd73e9321f9c28f008db7527bd6e881e22a418ca1562cdaf16df33ad332d13bf0744737b7f406b7c5b893d31fcc9
RREQ-R	63b2d0c9b925dd6c8820798099ae6c099245d9c4eaaeb6a3b604c09bebe30b39a62b9c99162922ebc05fed156a45ebd849ed088cef6abe6f87f010bbded5e37a
RREQ-J	f56c4416632652f2b3469ffdada9c9f245a8c025e128e471d05f75e625320024ee61bd29bbbd7dc1454102107ffe7b6fb288c1f0e0a56132f5b7c8cc3eb2be18
RREQ-JR	151e550443631e80078cca115ee978e0498dd5942661f5389e39694e5f8f619bc6a100cc9ebf60fafdad83c44b49e64e86595a530a06ac1ed1d537273968eee9
RREP	fd92856a81d58d4abd15a032b3a47d5df24d178b6142dcd86cd888a7902206089e052c082c0bbe0d7fd20731e773e2f0a57cb009ec68dd97c8d6dfc3483cbac2
RREP-R	168c5626507d1e5e892a5b0dad06c3da6fa82ee52cc80be7f6ec0f39320ffdc6e57a8f4dbbfa9b26f2f17d573e0a931c06a5ec28b8110b84e53dab4138199bec
RREP-J	d45e6c5407eb39095a27092c79cfb140d1e4f17950d9c377122f2fb03a14a21d529edb2f1b066795e8efb2007cdfe806390b329c340a0b50a3b351892bbefa8f
RREP-JR	ac9586c62d99bbcbef4e5eddaa30253d51ecaec779236ed8fce7f310c6759789a5e37b7e54ec16972331120227bdc560a4abe86257bc48ad3e3e23ba73e772de
MACT-J	60019dad8270475155c29098b47f3c075636440fe1debc428ca0d681763e0eb7c432267888bf05a3655564045049f8a747cf3e8bbbe896625f59855e6f4d1065
MACT-P	d35108b3c2ccacf75650125f208c955c7819a3ca454162a99997585e6e3b4154e661a74a0fb5d2fb544432a8cd0836e14d2551069489fa5583fdc71e937c0279
MACT-GL	7c60039bbc556772b9ab8728228291a9e7b6c333624bd94aaa38b6b8b327feda74e1934e75d9a48f5ff98917906720b503f94e2f261e264495a422d5ce17076b
MTF-UP	8701d222c072f43a4b70b049bc6a5db86e8fd014db4f218206d63496e7e8c25e9f496a9da7682959fb20cc7ddb7538cbed60197be68769ea8b01190dd1c03d43
MTF-DOWN	de1a48482d525753dac00107508d155b2d03a7610a96d740a6e81ffa89df92dfb1de6e428ed573ca61e63dfaf1557a850946444ad1e24e788454fb006802d8e7
GRPH	d13248a6fc8be1710e1c4a01b574c1f57cb2ffed8715f14cdc3917ba0d99982894dc5c5b8960ec71efc64c8455323d9e89c7c91956f43d98a1c97d6d6ac12cec
GRPH-U	c16b48e4cdde2b1030d578a3a36bcd766ce9cac04e8303d30a0252c707fbdfaf30864859f945246cb9e8267e37a2098390eede801b7790975ff44df5952899a2
GRPH_M	4db9c2544085faef3ba1bfba49044a254ae1e8662cef8f2ae8e6f4e1e3df53974f94ef106b821f874b6b8afdca9004009977726854f8d5f52a686f3c2234b5e6
HELLO-MSG	ec3256d70176dbd67b5370135ac3432a8654436b984ecd61de1fce8faf258326402a0d2bba95f82375c1c10a2e1895fb754e4160bbdb9583719e3a0ecbf39b13
Multicast Table Entry	ae2e360c2c7c3342a03aed80de66f3ac2afd89dca20d04824beb9a44a3124a667b91f2bd6178b52cd69b4a5371e6ee3d4f9e8c03f200b33fb9c42ea2447d7b55

Local flag codes and global HASH values both are verified for various network operations i.e. Tee construction/Tree Merge/Tree Pruning (MACT-J/MACT-P/MACT-GL), Group Leader selection etc. Without authentications of these codes, no multicast operation can be performed.

IV. SIMULATION SETUP

TABLE III. SIMULATION SCENARIO

Simulation Scenario	
Total Nodes	30
Sender Node(s) Density variation	1,5,10,15
MAC Protocol Standard	802.11
Key Distribution Algorithm	Group Diffie-Hellman (GDH)
Wierless Terrain	1200x1200
Multicast Ad Hoc Routing Protocol	MAODV
Simulation Time	10 Minutes
Group Size	1
Propagation Model	TwoRayGround
Traffic Type	CBR
Packet Size	512 Bytes
Sampling Interval	0.1 Second
Network Simulator	NS-2.35
One way HASH Funtion	For Local Flag Codes
SHA512 HASH Funtion	For Global HASH Values
Mobility Model	Random WayPoint

Table III. above shows the simulation scenario used for analysis purpose.

V. SIMULATION RESULTS

Following graphs show the performance of entire network using different parameters, i.e. Throughput, Packet Delivery ratio and Routing Load etc.

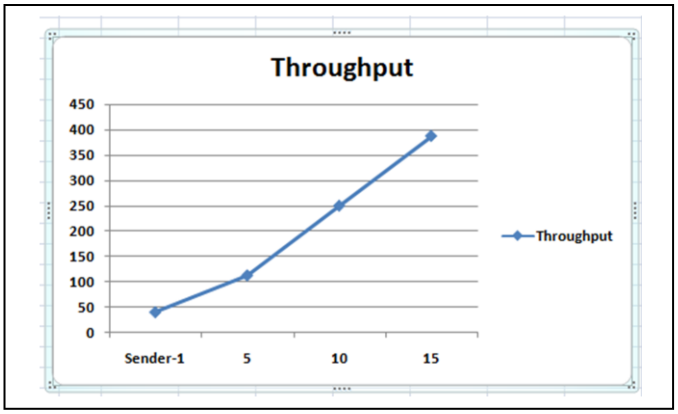

Fig. 5. Throughput

Fig.5 Above shows Throughput of the network with the sender density 1,5,10 and 15. It shows the improvement in Throughput, which is increasing w.r.t. sender's density.

Fig.6 Above shows Routing Load of the network with the sender density 1,5,10 and 15. It shows that Routing Load is decreasing w.r.t. sender's density. Fig.7 shows the significant improvement in Packet delivery Ratio of the network with the sender density 1,5,10 and 15.

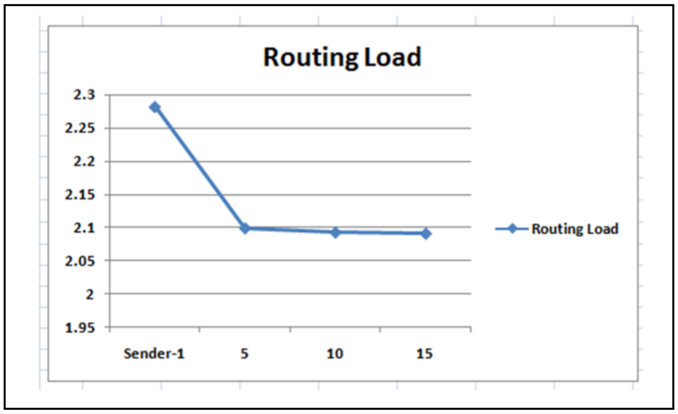

Fig. 6. Routing Load

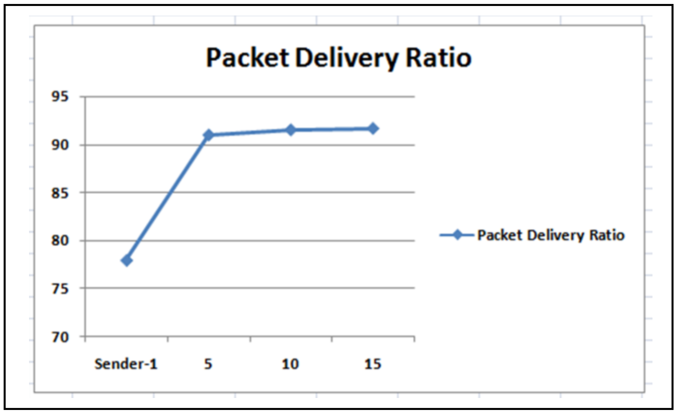

Fig. 7. Packet Delivery Ratio

VI. Security Analysis

A. *Secure Key management and node authentication*

GDH algorithm supports secure communication based on group authentication. At the initial stage, it requires a large prime number P and its primitive root G. All candidate nodes participate to generate a universal g on the basis of their private keys using P and G.

$$Univeral\ g = \{N_i \rightarrow G^{a,b,c,d,e,f,\ldots n}\} \quad (18)$$

If an intruder generates:

$$g^j = \{N_i \rightarrow G^{a,b,c,d,e,f,\ldots n+x}\} \text{ or} \quad (19)$$

$$g^j = \{N_i \rightarrow G^{a,b,c,d,e,f,\ldots n-x}\} \quad (20)$$

Then $g^j \neq g$, that means to generate exact value of universal g, intruder must use the key combination equivalent to original participant keys and it depends upon the number of candidate those want to form a group. Shared group key s_i can be generated, only if $(a,b) \in N_i \rightarrow g^{a,b}$

$$s_i = N_i \rightarrow key_i{}^a \ mod\ p \quad (21)$$

$$s_j = N_j \rightarrow key_i{}^b \ mod\ p \quad (22)$$

$$s_i = s_j \text{ , only if } (a,b) \in N_i \rightarrow g^{a,b} \quad (23)$$

If node leaves the group, then s_i is revoked and it cannot rejoin the group without key negotiation.

B. *Secure Multicast Tree construction and maintenance*

Local flag codes and global HASH values cannot be intercepted because all these are produced at the time of group formation and regeneration of exact codes by malicious nodes is not feasible. RREQ and RREP are used for route discovery. Intermediate nodes verify them on the basis of local flag codes and forward those by embedding an encrypted flag in their header with global HASH values. All messages without valid flag codes, global HASH values and encrypted flags are declared as unauthorized messages are declared as unauthorized messages and finally discarded. During RREQ propagation phase, intermediate authorized nodes set their status ON_TREE, if they are not on the tree and update multicast routing table and multicast packets are further propagated. RREQ/RREP messages from unauthorized nodes are not entertained.

An encrypted flag is merged with Multicast Route Activation (MACT) header. MACT-J is used for tree construction or when a node wants to join group. After receiving MACT-J, its flag is decrypted and local flag code and global HASH values are verified to update multicast routing table. Unauthorized MACT-J is rejected and routing table is not updated. MACT-GL is used for new group lead selection and MACT-P for Tree pruning. For new group leader selection, all shared keys of eligible candidate are verified and an encrypted flag is merged with MACT-GL header for authentication purpose. If the selected group leader cannot decrypt the flag, next candidate is selected for leadership and so on. Tree pruning is invoked when a node leaves the multicast tree and after that upstream node becomes a leaf node. Tree pruning is controlled by verifying the shared keys and HASH values of upstream/downstream nodes. After successful verification, MACT-P is processed otherwise it is filtered out. Finally, it can prevent group leader selection attack/MACT fabrication attack.

The only authorized group leader is allowed to generate periodic Group Hello messages (GRPH). After receiving a GRPH message, intermediate nodes update their multicast table after message authentication. Upstream and downstream node authentication is performed on the basis of shared key and HASH value for processing of GRPH-U, GRPH-M, RREQ-JR and RREP-JR etc.

VII. Conclusion

In this paper, GDH algorithm for key generation and distribution was used along with MAODV routing protocol. Key negotiation starts at the time of the group joining. All candidates use their private keys to calculate the universal value of g. After that shared key pair is generated and distributed to each participant node only. Fist node becomes the group leader and generates local flag codes and global HASH values, and embeds them with each message. These codes are used to verify the authenticity and integrity of all messages. Local flag codes/global HASH values are used to verify critical multicast operations i.e. Group Leader Selection, Tree Construction and Maintenance etc. All invalid requests and responses are rejected.

As per security analysis, it can be observed that reproduction of shared key is not feasible due to the absence of private keys of each node. In the case of compromised keys, the intruder cannot intercept the local flag codes and global HASH values and without using codes, all routing messages are discarded. Simulation results show that in the presence of multiple senders, Throughput and PDR of the network increase w.r.t. Sender's density, whereas routing load is reduced. Finally, simulation and analysis results conclude that proposed scheme can protect the routing information without generating extra control overhead, and it can be further extended to adopt the compromised network environment using different multicast routing protocols.

REFERENCES

[1] Hui Cheng et al., “Hyper-mutation based Genetic Algorithms for Dynamic Multicast Routing Problem in Mobile Ad Hoc Networks”, 11th International Conference on Trust, Security and Privacy in Computing and Communications-2012 IEEE, pp. 1586-1592.

[2] N. Bhalaji et al., “Performance Comparison of Multicast Routing Protocols under Variable Bit Rate Scenario for Mobile Ad hoc Networks”, Recent Trends in 19 Network Security and Applications Communications in Computer and Information Science vol. 89, 2010, Springer-2010, pp. 114-122.

[3] C. Siva Ram Murthy, B.S. Manoj, “Ad Hoc Wireless Networks”, 14 impression- Pearson-2012, Chapter (5-11), pp. 191-641.

[4] Hui Xia et al., “Multicast Trusted Routing with QoS Multi-Constraints in Wireless Ad Hoc Networks”, International Joint Conference of IEEE, TrustCom-IEEE-2011, pp. 1277-1282.

[5] Dr. N. Sreenath et al. “Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs”, ICCCI-IEEE -2012, pp. 1-7.

[6] Ahmed. M. Abdel Mo’men, Haitham. S. Hamza, IEEE Member, and Iman. A. Saroit, "New Attacks and Efficient Countermeasures for Multicast AODV", IEEE-2010, pp.51-57

[7] Ratna Dutta et al. “Computationally secure self-healing key distribution with revocation in wireless ad hoc networks”, Ad Hoc Networks, vol. 8 (6), August 2010, Elsevier 2010, pp.597-613

[8] Sencun Zhu et al., “Scalable Group Key Management for Secure Multicast: A Taxonomy and New Directions”, Network Security, 2010, Springer-2010, pp. 57-75.

[9] Zahraa Sabra and Hassan Artail,"Preserving Anonymity and Quality of Service for VoIP Applications over Hybrid Networks", IEEE Mediterranean Electro-technical Conference, 2014, pp.421-425

[10] Vennila Rajamanickam, Duraisamy Veerappan, "Inter cluster communication and rekeying technique for multicast security in mobile ad hoc networks", IET Information Security, IEEE, 2013, pp.234-239

[11] Anita, E.A.M. Bai, V.T., Raj, E.L.K., Prabhu, B, “Defending against worm hole attacks in multicast routing protocols for mobile ad hoc networks”, Advances in Computing and Communications in Computer and Information Science vol. 190, 2011, Springer-2011, pp. 1-5.

[12] E.A.M. Anita, “Sybil Secure Architecture for Multicast Routing Protocols for MANETs”, Advances in Computing and Communications in Computer and Information Science vol. 190, 2011, Springer-2011, pp. 111-118.

[13] Jiwen Guo et al., “Secure Minimum-Energy Multicast Tree Based on Trust Mechanism for Cognitive Radio Networks”, Wireless Personal Communications November 2012, vol. 67 (2), Springer-2012, pp. 415-433.

[14] Ding Wanga, Nan Wang, Ping Wang, Sihan Qing, "Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity", Information Sciences, Elsevier-2015

[15] Babak Daghighi, LaihaMatKiah, Shahaboddin Shamshirsband, Muhammad abib Ur Rehman, "Toward secure group communication in wireless mobile environments: Issues, solutions and challenges", Journal of Network and Computer Applications, Vol. 50, Elsevier -2015, pp. 1-14

[16] Lin Yao, Jing Deng, JieWang, Guowei Wu, "A-CACHE: An anchor-based public key caching scheme in large wireless networks", Computer Networks, Elsevier-2015, pp.78-88

[17] Lein Harn, Changlu Lin, "Efficient group Diffie–Hellman key agreement protocols", Computers and Electrical Engineering, Elsevier-2014, pp. 1972–1980

[18] V. Srihari, P. Kalpana, "Security Aspects of SIP based VoIP Networks: A Survey", ICCTET, IEEE-2014, pp-143-150

[19] Jiazi Yi et al., “Vulnerability Analysis of Relay Set Selection Algorithms for the Simplified Multicast Forwarding (SMF) Protocol for Mobile Ad Hoc Networks”, 15th International Conference on Network-Based Information-IEEE-2012, pp. 255-260

[20] A. Menaka Pushpa, Dr. K. Kathiravan, "Secure Multicast Routing Protocol against Internal Attacks in Mobile Ad Hoc Networks", IEEE GCC Conference and exhibition, 2013, pp-245-250

[21] J.K.Harika, Dr.C.Jayakumar, "An Acknowledgement Based Secure Data Transmission in MANETS", ICICES,IEEE-2014, pp-1-5

[22] A. Fidalcastro, E. Baburaj, "An Advanced Grammatical Evolution Approach for Intrusion Detection on multicast routing in MANET", ICICES, IEEE-2014, pp.1-4

[23] Hui Xia, Jia Yu, Zhi-yong Zhang, Xiang-guo Cheng, Zhen-kuan Pan, "Trust-enhanced multicast routing protocol based on node's behavior assessment for MANETs", International Conference on Trust, Security and Privacy in Computing and Communications, IEEE-2014, pp.473-480

[24] T. Stephen John and A. Aranganathan, "Performance analysis of proposed mobile autonomous agent for detection of malicious node and protecting against attacks in MANET", International Conference on Communication and Signal Processing, IEEE-2014, pp.1937-1941

[25] Wei Yuan, Liang Hu,Kun Yang, "A Topology Hidden Anonymous Multicast Routing for Ad Hoc Networks", GlobeCom, IEEE-2013, pp.599-604

[26] A. Menaka Pushpa, K. Kathiravan, "Resilient PUMA (Protocol for Unified Multicasting through Announcement) against Internal Attacks in Mobile Ad Hoc Networks", ICACCI, IEEE-2013, pp.1906-1912

[27] P. Anitha, G. N. Pavithra, P. S. Periasamy, "An Improved Security Mechanism for High-Throughput Multicast Routing in Wireless Mesh Networks Against Sybil Attack", PRIME, IEEE-2012, pp.125-130

[28] N.M. Saravanakumar, R. Keerthana and G.M. Mythili, "Dynamic Architecture and Performance Analysis of Secure and Efficient Key Management Scheme in Multicast Network", Artificial Intelligence and Evolutionary Algorithms in Engineering Systems Advances in Intelligent Systems and Computing Vol. 324, 2015, pp.775-784

[29] Xiao Wang, Jing Yang, Zetao Li, Handong Li, "The energy-efficient group key management protocol for strategic mobile scenario of MANETs", EURASIP Journal on Wireless Communications and Networking, Springer-2014, pp.1-22

[30] Mahalingam Ramkumar and Nasir Memon, "An Efficient Key Pre-distribution Scheme for Ad Hoc Network Security", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, Vol.23 (3),IEEE-2005, pp.611-621

[31] Sourabh Chandra, Smita Paira, S k Safikul Alam, Goutam Sanyal, "A comparative survey of symmetric and asymmetric key cryptography", ICECCE, IEEE, 2014, pp.83-93

[32] Youssef BADDI, Mohamed Dafir ECH-CHERIF El KETTANI, "Key Management for Secure Multicast Communication: A Survey", IEEE-2013, pp.1-6

[33] R. Di Pietro, S. Guarino, N.V. Verde, J. Domingo-Ferrer, "Security in wireless ad-hoc networks – A survey", Computer Communications, Vol. 51,Elsevier-2014, pp.1-2