International Journal of Computer and Communication Technology

Volume 5 | Issue 2 Article 4

April 2014

Secure Efficient On-Demand Insider Attacks Multicast Routing Protocol in Wireless Networks

K. Vishnu Vardhan
Department of Computer Science and Engineering CMR College of Engineering and Technology, Hyderabad,India, vishu3688@yahoo.co.in

G. Ravi Kumar
Department of Computer Science and Engineering CMR College of Engineering and Technology, Hyderabad,India, ravicmrcse@gmail.com

Badi. Rajani
Department of Computer Science and Engineering CMR College of Engineering and Technology, Hyderabad,India, subodh2rajani@gmail.com

Y. sarada Devi
Department of Computer Science and Engineering CMR College of Engineering and Technology, Hyderabad,India, sarada.roja@gmail.com

Recommended Citation

Vardhan, K. Vishnu; Kumar, G. Ravi; Rajani, Badi.; and Devi, Y. sarada (2014) "Secure Efficient On-Demand Insider Attacks Multicast Routing Protocol in Wireless Networks," *International Journal of Computer and Communication Technology*: Vol. 5 : Iss. 2 , Article 4.
DOI: 10.47893/IJCCT.2014.1226
Available at: https://www.interscience.in/ijcct/vol5/iss2/4

Secure Efficient On-Demand Insider Attacks Multicast Routing Protocol in Wireless Networks

K. Vishnu Vardhan, G. Ravi Kumar, Badi. Rajani, Y.sarada Devi
Department of Computer Science and Engineering
CMR College of Engineering and Technology, Hyderabad,India
E-mail : vishu3688@yahoo.co.in , ravicmrcse@gmail.com, subodh2rajani@gmail.com, sarada.roja@gmail.com

Abstract— Wireless multicast routing send and receives the data source to destination. High error rates, unfixed and changeable self of the signal power and broadcast change with time and environment regularly result in not effective links. These services more weak to internal attacks coming from compromised nodes that behave randomly to disrupt the network, also referred to as Inside attacks. Our method ensures that as long as a fault-free path exists between two node or multi nodes in multicast group they can communicate reliably even if an destroy majority of the network acts in a complex mode. Multicast Group is the link on different Multicast Group's Group Leader in multi hops networks.

Index Terms*—mobile computing, Multi hop wireless networks, Byzantine resiliency, Byzantine attacks.*

I. INTRODUCTION

Wireless networks are facing difficult situation of problems facing in ad-hoc networks every node maintained own infrastructure and with in the networks communicate to the multicast wireless networks. Each and every node can communicate to another node or group of nodes, problem attacking nodes can be in the network of groups or single node path.

Multicast nodes are moving the message to target nodes in that way any situation of nodes can facing and difficulty's like that insider attacks block hole, worm hole and flood rushing. In this situation common for wireless networks and routing protocol can performed and detected to that complex attacks. Because some kinds of nodes are acts like genuine. Multicasting nodes between two nodes are any another group of nodes may be acts like that within the group. Wireless networks broadcasting the signals. Multigroup nodes are multicasting in multi hop nodes in group of nodes every group node become a member of group leader nodes. A group leader node can maintained every node previous information and signature of the nodes. When node to node or node to group of nodes broadcast the message passing verify to the database for every group leader and source node, trusted nodes only can received source messages. Our protocol ensures that multicast data is delivered from the source to the members of the multicast group, even in the presence of Byzantine attackers, as long as the group members are reachable through non-adversarial path.

Here an authentication framework is used to eliminate outside adversaries and ensure that only authorized nodes perform certain operations (only tree nodes can perform tree operations and only group nodes can connect to the corresponding multicast tree). SEIMR mitigates inside attacks that try to prevent a node from establishing a route to the multicast tree by flooding both route request and route reply. Tree nodes monitor the rate of receiving data packets and compare it with the transmission rate indicated by the source in the form of an MRATE message [1].

II. SIMILAR WORK

MANET two mechanisms that detect misbehaving nodes reflecting dropping nodes and past information of the nodes are bad report to send the next node of neighbor. There are two mechanisms Secure data forwarding, detected misused nodes reports and metric level calculation of other nodes have been to ease damaging effect of packet dropping.

Honesty of the forwarded packet, upon detection of an unruly node, a report is generated and nodes update the rating of the reported bad node. The ratings of nodes along a good route are every so often incremented, at the same time as reception of naughtiness alert radically decreases the node rating. When a new route is necessary, the source node calculates a path metric equivalent to the standard of the ratings of the nodes in each of the route replies, and selects the route with the peak metric [3].

An addition of the Ad Hoc On-demand Distance Vector (AODV) routing protocol has been proposed to protect the routing protocol messages. The Secure-AODV scheme assumes that each node has certified public keys of all network nodes, so that in-between nodes can authenticate all in-transit routing packets. As the message traverses the network, middle nodes cryptographically authorize the signature and the hash value, create the k^{th} element of the mix up sequence, with k being the number of traversed hops, and place it in the packet. The route replies are provided either by the destination or intermediate nodes having an active route to the required target, with the latter mode of process enabled by a dissimilar type of control packets [6].

MAODV is a reactive protocol that energetically creates and maintains a multicast tree for each group. It is an altered copy of AODV, a unicast routing protocol. Due to constraints of space, we present in this section a brief overview of only those aspects of MAODV relevant to our implementation. A detailed description of MAODV can be found in. Each node running MAODV maintains two routing tables: Route Table (RT) and Multicast Route Table (MRT). The Route Table is used for recording the next hop for routes to other nodes in the network. Each entry in RT contains a destination IP address, a destination sequence number, hop count to the destination, IP address of next hop, and the lifetime of this entry [1].

A. Node Authentication

The authentication framework prevents unauthorized nodes to be part of a multicast tree or of a multicast group. Each node authorized to join the network has a pair of public/private keys and node certificate that binds its public key to its IP address. Each node authorized to join a multicast group has an additional group certificate that binds its public key and IP address to the IP address of the multicast group.

Nodes in the multicast tree are authenticated using a tree token, which is periodically refreshed and disseminated by the group leader in the multicast tree with the help of pair wise shared keys established between every direct tree neighbors. Only nodes that are currently on the tree will have a valid tree token. To allow any node in the network to check that a tree node possesses a valid tree token, the group leader periodically broadcasts in the entire network a tree token authenticator [2].

Hop count authentication is to prevent tree nodes from claiming to be at a smaller hop distance from the group leader than they actually are, we use a technique based on a hash chain. The group leader in GroupHello messages, which are broadcast periodically in the entire network, also includes the hop count anchor. This allows a tree node to prove its hop distance from the group leader to any node in the network.

B. Route Discovery

SEIMR’s route discovery allows a node that wants to join a multicast group to find a route to the multicast tree. To prevent outsiders from interfering, all route discovery messages are authenticated using the public key corresponding to the network certificate. Only group authenticated nodes can initiate route requests and the group certificate is required in each request. Tree nodes use the tree token to prove their current tree status. The requesting node broadcasts a route request (RREQ) message that includes the node identifier and its weight list, the multicast group identifier. The RREQ message is flooded in the network until it reaches a tree node. Only new requests are processed by intermediate nodes [1].

When a tree node receives a RREQ from a requester, it initiates a response. The node broadcasts a route reply (RREP) message that includes that node identifier, the requester’s identifier and weight list from the request message. The RREP message is flooded in the network until it reaches the requester.

C. Multicast Route Activation

The requester signs and unicasts on the selected route an multicast activation message that include its identifier, the group identifier, and the sequence number used in the RREQ phase. The MACT message also includes a one-way function applied to on the tree token extracted from RREP, f(requestor, tree token), which will be checked by the tree node that sent the RREP message to verify that the nodes activated the route is the same as the initial requestor.

An intermediate node on the route checks if the signature on MACT is valid and if MACT contains the same sequence number as the one in the original RREQ. The node then adds to its list of tree neighbors the previous node and the next node on the route as downstream and upstream neighbors, respectively, and sends MACT along the forward route. During the propagation of the MACT message, tree neighbors use their public keys to establish pair wise shared keys, which will be used to securely exchange messages between tree neighbors.

The requester and the nodes that received MACT could be prevented from being grafted to the tree by an adversarial node, selected on the forward route, which drops the MACT message.

D. Multicast Tree Maintenance

Routing messages exchanged by tree neighbors, such as pruning messages are authenticated using the pair wise keys shared between tree neighbors. Tree pruning occurs when a group member that is a leaf in the multicast tree decides to leave the group. A node initiates pruning from the tree by sending a message to its parent. The group leader periodically broadcasts in the entire network a signed Group Hello message that contains the current group sequence number, the c, and the hop count anchor. A signed Group Hello message containing a special flag also ensures that when two disconnected trees are merging, one of the group leaders is suppressed [1].

III. IMPLEMENTATION

A. Data flow mechanism

Each multicast handset stores the source in order in the Member Table. For each multicast group the node is participating in, the source ID and the time when the last Join Request is received from the source is recorded. If no Join Request is received from a source within the refresh stage, that entry is removed from the Member Table. A Routing Table is created on demand and is maintained by each node. An entry is inserted or up dated when a non-duplicate Join Request is received the node stores the destination the source of the Join Request and the next hop to the target the last node that propagated the Join Request. The Routing Table provides the next hop information when transmitting Join Tables.

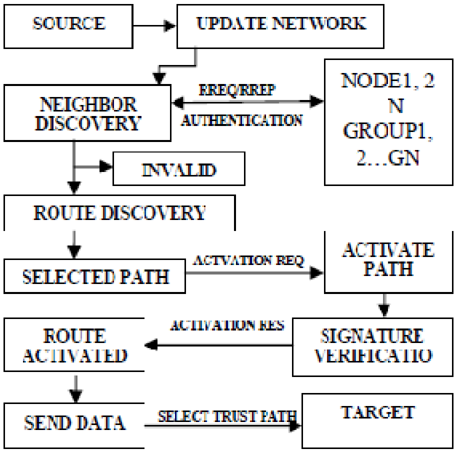


Figure 1. Multi group's Multicast Routing Protocol

When a node is a forwarding group node of the multicast group, it maintains the group information in the Forwarding Group Table. The multicast group ID and the time when the node was last refreshed are recorded.

The Message collection is maintained by each node to identify duplicates. When a node receives a new Join Request or data, it stores the source ID and the sequence number of the packet. Note that entries in the Message store need not be maintained permanently. Schemes such as LRU (Least Recently Used) or FIFO (First in First Out) can be employed to expire and remove old entries and prevent the size of the Message store to be general **Fig1**. After the group establishment and route construction process, A multicast source can transmit packets to receivers via selected routes and forwarding groups. Periodic control packets are sent only when outgoing data packets are still present.

B. Multigroup nodes communication

Implication shown that in Multicast Routing protocol, message from one Multicast group to the other doesn't exist. **Fig2** Represents the Groups form of types of nodes that can appear in Multicast settings or Multicast Groups.

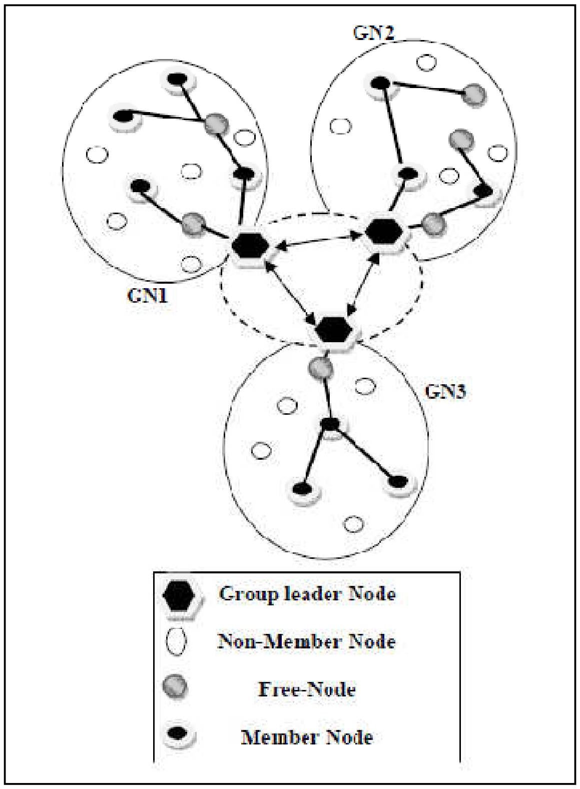


Figure 2. Nodes in Multi hop for Multicast Groups.

Let’s think a Multicast Group say in which the Group Leader needs to send a data to its Group member nodes D1, D2 and a member node A1 in another Multicast Group say GN2, then it has to send the data through the Group Leader of GN2. So, this explains the nature of Multicast Group Leaders to get connected and form Groups. We should also remember that when the data is transmitted to GN2 from GN1, GN1 will communicate with the GN2 and pass the token information after which GN2 checks the member node for the Destination.

Once the shortest path has been found, the encrypted data from the GN1 will be transmitted to the destination A1 in GN2 and will be decrypted only in the destination assuring data security while transmitting. Tree nodes can be either member nodes or nonmember node [5].

IV. GENERAL PROBLEMS

Byzantine attacks share certain features with the “selfish” node problem not forwarding the data packets of others. Attacks where the adversary has full control of an authenticated device and can perform arbitrary behavior to disrupt the system are referred to as Byzantine attacks. In difference, the goal of a Byzantine node is to disrupt the communication of other nodes in the network, without regard to its own resource use [4].

1. **Black hole attack.** A basic Byzantine attack is a black hole attack where the adversary stops forwarding data packets, but still participates in the routing protocol correctly.

2. **Wormhole attack.** If more than one node is compromised, it is reasonable to assume that these nodes may interact in order to gain an additional advantage. This allows the adversary to perform a more effective attack. Indeed, one such attack is a Byzantine wormhole, where two adversaries collude by tunneling packets between each other in order to create a shortcut (or wormhole) in the net work.

3. **Flood rushing attack.** One or several adversaries rush an authenticated flood through the network before the flood traveling through a legitimate route. This allows the adversaries to control many paths. Flood rushing can be used to increase the effectiveness of a black hole or wormhole attack.

IV. DATA FLOW AND GROUPS LEADERS MECHANISM

A. *New Joining Nodes*

Group Leader (GL1) maintained the information about the nodes (GN1) and other group leaders (GL1, 2...N). Each and every group leader maintained the information about the nodes individually. When new node N’ trying to join under the group leader, all group leader nodes broadcast the message to new nodes the new node searching for short distance circle group node and reply to nearest group leader.

The node information ID and signature verifying hop counting neighbor nodes using method for hello messages to broad cast send and received. Once join the non member node to group leader, node responsible and all kind of information send and received the group leader nodes.

Every group leader verifying the node information signature and ID past and present neighbor nodes metric calculation and finding the insider attacks nodes avoiding the group to that bad nodes. Group leader nodes when received the messages to broadcast before checking all previous and present timing.

B. *Multi Nodes and Groups Leaders*

Source Node Updating the network, then Neighbor discovery sending RREQ to nodes and Group Leaders all nodes activate and RREP sending to Neighbor Nodes, group leader and nodes authentication checking, its invalid the node it is a malicious attacking node avoiding the neighbor discovery, its valid then continues the process.

Time based metric calculation hop by hop nodes. Any node not response to previous time or more time to reaching the neighbor node, the time metric recognized its unwanted node immediate sending the information to all nodes and group leader avoiding the links to neighbor nodes, regenerating process starts the activated new path.

Route Discovery Selected the path activate request the path verifying its Id of group leader and nodes previous information checking. Signature verifying the nodes and group leaders, sending activation response message to Route is activated. Source Node gets the trusted route path to target nodes or group leaders.

Algorithm for multicast group communication protocol

NEW JOINING NODES

Create group leaders GL.

Maintained information (GL1, 2…, N...).

Individual GL node to node communication

New node N’ joining the nearest group.

Message passing N to N’ within the GL

GL nodes N information Maintained

GL verify N RREQ/ RREP and authentication.

MULTI NODES AND GROUPS LEADERS

Source S updating the network

Neighbor discovery send RREQ to and GL, requester id, group id

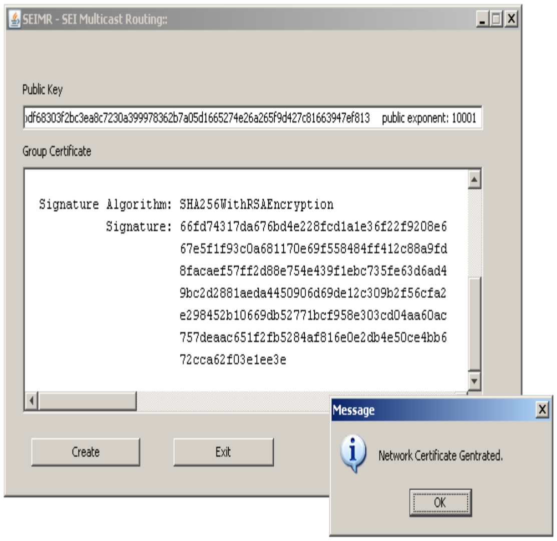
Broadcast (req)

If (req is not found in requests list) then Verify Signature of req If (node's group is same as req's group) then Verify Signature of req in group Res = Create Signature with RREP, node id, group id requester id, weight list Broadcast (res)

Else

```
Broadcast (req)
      Update Requests List (req)
Update = true; prev_node = responder_id; total_weight = 0
If ((node. group == res.group) AND (node.seq >= res.seq)) then
      Exit
Update hop_count and res.total_weight
   prev_res = Find (response_list, res.req_id, res.group)
   If ((prev_res) AND (res. total_weight > prev_res. total_weight)) then
      Update = false;
   If (update) then
      VerifyHopCount (res)
      VerifySign (res)
            If (node == res.req_id) then
Authentication checking GL
Its not value avoiding the route stop
Else
W_timer ≠ (Node, GL) avoiding
Else
W_timer = (Node, GL)
Signature verifying (GL, Node)
Then
Route activated to Target
Source Send to Target GL Node.
```

VI. TESTING AND RESULTS



SEIMR - SEI Multicast Routing::

Public Key

df68303f2bc3ea8c7230a399978362b7a05d1665274e26a265f9d427c81663947ef813 public exponent: 10001

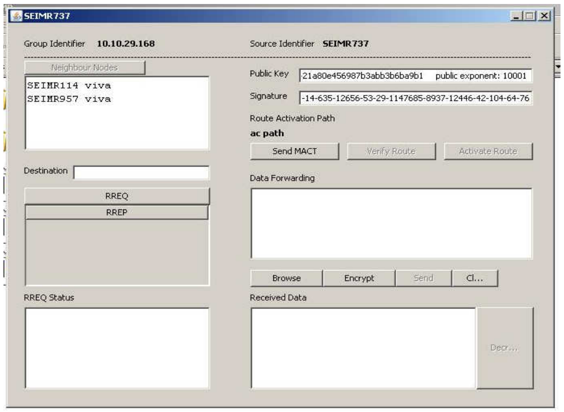
Group Certificate

```
 Signature Algorithm: SHA256WithRSAEncryption
          Signature: 66fd74317da676bd4e228fcd1a1e36f22f9208e6
                     67e5f1f93c0a681170e69f558484ff412c88a9fd
                     8facaef57ff2d88e754e439f1ebc735fe63d6ad4
                     9bc2d2881aeda4450906d69de12c309b2f56cfa2
                     e298452b10669db52771bcf958e303cd04aa60ac
                     757deaac651f2fb5284af816e0e2db4e50ce4bb6
                     72cca62f03e1ee3e
```

Message

Network Certificate Gentrated.

Figure 3. Network Certificate Generated



SEIMR737

Group Identifier **10.10.29.168**

Source Identifier **SEIMR737**

```
SEIMR114 viva
SEIMR957 viva
```

Public Key 21a80e456987b3abb3b6ba9b1 public exponent: 10001

Signature -14-635-12656-53-29-1147685-8937-12446-42-104-64-76

Route Activation Path

ac path

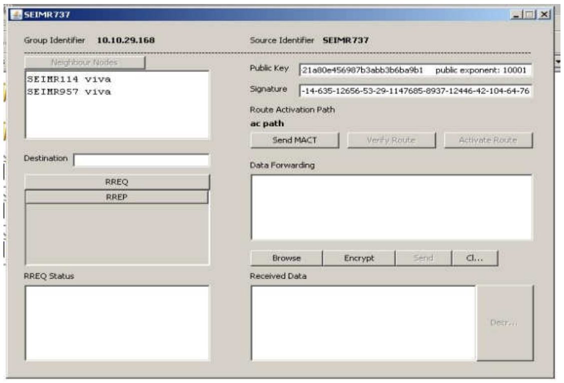
Destination

Data Forwarding

RREQ Status

Received Data

Figure 4. Node1



SEIMR737

Group Identifier **10.10.29.168**

Source Identifier **SEIMR737**

```
SEIMR114 viva
SEIMR957 viva
```

Public Key 21a80e456987b3abb3b6ba9b1 public exponent: 10001

Signature -14-635-12656-53-29-1147685-8937-12446-42-104-64-76

Route Activation Path

ac path

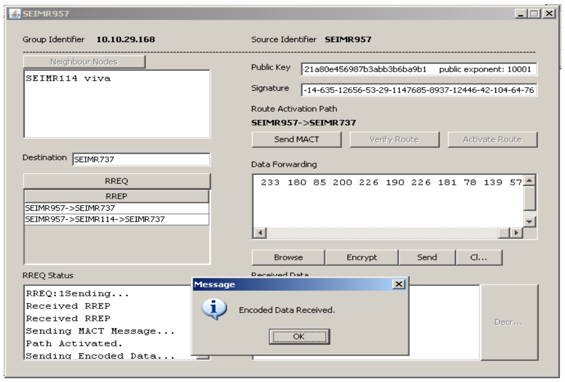
Destination

Data Forwarding

RREQ Status

Received Data

Figure 5. Node2



SEIMR957

Group Identifier 10.10.29.168

Source Identifier SEIMR957

SEIMR114 viva

Public Key 21a80e456987b3abb3b6ba9b1 public exponent: 10001

Signature -14-635-12656-53-29-1147685-8937-12446-42-104-64-76

Route Activation Path

SEIMR957->SEIMR737

Destination SEIMR737

SEIMR957->SEIMR737
SEIMR957->SEIMR114->SEIMR737

Data Forwarding

```
233 180 85 200 226 190 226 181 78 139 57
```

RREQ Status

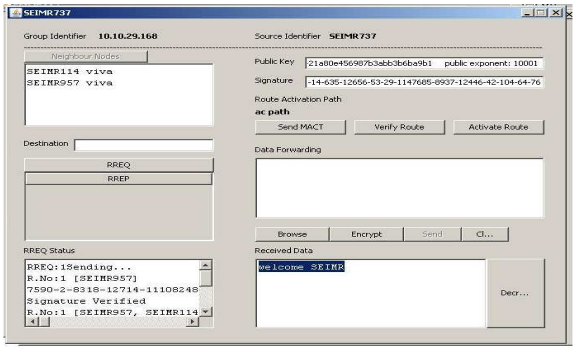
```
RREQ:1Sending...
Received RREP
Received RREP
Sending MACT Message...
Path Activated.
Sending Encoded Data...
```

Received Data

Message

Encoded Data Received.

Figure 6. Encription, Data Send To Target Node



SEIMR737

Group Identifier 10.10.29.168

Source Identifier SEIMR737

SEIMR114 viva
SEIMR957 viva

Public Key 21a80e456987b3abb3b6ba9b1 public exponent: 10001

Signature -14-635-12656-53-29-1147685-8937-12446-42-104-64-76

Route Activation Path

ac path

Destination

Data Forwarding

RREQ Status

```
RREQ:1Sending...
R.No:1 [SEIMR957]
7590-2-8318-12714-11108248
Signature Verified
R.No:1 [SEIMR957, SEIMR114
```

Received Data

welcome SEIMR

Figure 7. Decryption, Receives Original Data

VII. CONCLUSION AND IMPLEMENTATION

Mutigroup multicast routing strategy is effective against strong insider attacks such as black holes, worm hole and flood rushing. Identifies and avoids adversarial links and it provides efficient authentication for nodes, as well as maintaining the tree at each stage data securely send source to destination. This implementation is only software based.

REFERENCES

[1] R. Curtmola and C. Nita-Rotaru, “BSMR: Byzantine-Resilient Secure Multicast Routing in Multi-Hop Wireless Networks,” Proc.Fourth Ann. IEEE Conf. Sensor, Mesh and Ad Hoc Comm. And Networks (SECON ’07), 2009.

[2] Syed Rehan Afzal, Subir Biswas, Jong-bin Koh, Taqi Raza, Gunhee Lee, and Dong-kyoo Kim, "RSRP: A Robust Secure Routing Protocol for Mobile Ad hoc Networks", in proc. of IEEE Conference on ireless Communication and Networking, pp: 2313- 2318, March 31- April 3,Las Vegas, NV, 2008, Doi: 0.1109/WCNC.2008.408.

[3] Baruch Awerbuch, Reza Curtmola, David Holmer “ODSBR: An On-Demand Secure ByzantineResilient Routing Protocol for Wireless Ad Hoc Networks” ACM Journal Name, Vol. V, No. N, Month 20YY

[4] L. Xie and S. Zhu, “Message Dropping Attacks in Overlay Networks: Attack Detection and Attacker Identification,” Proc. Second Int’l Conf. Security and Privacy in Comm. Networks (SecureComm), 2006.

[5] R. Kalaidasan,Mrs. V.Hemamalini,Anoop K Babu,"SORB: Secure On Demand Resilient to Byzantine Multicast Routing in Multihop Wireless Networks" Rajiv Gandhi College of Engg. & Tech,Department of CSE.

[6] R. Curtmola and C. Nita-Rotaru, “BSMR: Byzantine-Resilient Secure Multicast Routing in Multi-Hop Wireless Networks,” Proc.Fourth Ann. IEEE Conf. Sensor, Mesh and Ad Hoc Comm. And Networks (SECON ’07), 2007.

◈◈◈