Prevention of Shared Root Node Attack in MAODV

P.Ramesh[1],Dr.M.Sailaja[2],S.Koteswararao[3],V.Rajesh[4]

[1,3,4]Department of Electronics and Communication Engineering, RIT, Yanam,U.T.
[2]Department of Electronics and Communication Engineering,JNTUK,Kakinada,A.P.

Abstract
In MANETs, most of the research work carried out till now has not widely addressed the security of Mobile Ad hoc Distance Vector protocol (MAODV). In the existing multicast routing protocols maintenance of the multicast structure is very difficult due to mobility where path breakage occurs very frequently. Hence this protocol require periodic or event driven control packet updates for each member in the multicast group in order to maintain the multicast structure e.g., membership information, routes etc. This protocol works effectively with small-scale multicast groups they suffer from severe communication overhead caused by control packet floods (e.g., Join Query or Request packet flooding in MAODV) in a large-scale network with a large number of multicast groups. Such overhead would be unsustainable in a battle field scenario with multicast group consisting of dozens of teams where each team includes hundreds of units.

KEYWORDS:
MANETS,MAODV,Overhead,flooding,NS-2.

I INTRODUCTION

Multicasting can efficiently support a wide variety of application that are characterized by a close degree of collaboration typically for MANETs. The performance of a multicast session in a MANET under attack depends heavily on many factors such as the number of multicast senders, the number of multicast receivers, the number of attackers as well as their positions [1]. In this paper we provide a thorough description of the existing of the multicast protocol MAODV and how the protocol can be made more secure by providing solution on the attacks like shared multicast tree node attack, selfish behavior of nodes and control packet attack.

Mobile Ad hoc Distance Vector protocol (MAODV) is a reactive based protocol in which no pre defined path exists between nodes for transmission. Path is established only on demand [2]. Also MAODV is a tree based protocol where only one path exists between two nodes. So, if that path fails then communication between those nodes will be a problem, resulting in a security issue. Here we concentrate mainly on:

- Attacks on shared multicast tree root node
- Selfish behavior of nodes
- Attacks on control packets

II PROPOSED WORK

Both the shared root node attack and control packet attack can be detected by using two hop acknowledgements. These attacks can be prevented by reconfiguring. If the source node broadcasts the RREQs Packet, it is passed on all the routes from that source node and after the destination node receiving the RREQs then forwards the RREPs using the reverse route. If the RREPs comes from the reliable intermediate node then send the data packets else the root node has been attacked hence both the control packets and the data packets cannot be routed to the downstream node or to the neighbor multicast tree and the routing table are not updated. In case of root node attack, the root node must be rehabilitated based on the best neighboring node depending on the best range of communication. Then the killed node (RN node) can be rehabilitated in order to prevent the network being crippled by the root node attack. Shared root node is one that first actively joins with the source with the join flag set.

2.1 System Analysis:

System analysis is the most important part of any project study. This phase, system analysis gives us a perfect idea about our system. It also provides us with some additional information. It describes about the entire system, not only about the present system but also the overview of the present system, limitation of the present system and the proposed solution. So, the system study and analysis are the most important parts of a system study progress [3].

In this phase here we make the analysis of the system. That means in this phase mainly we do the study of the system which means what is the problem definition of the system. Alternate system solutions are studied and recommendations are made about omitting the resources required designing the system. Here in this phase apart from the problem definition we make the determination system performances the identification and evaluation of the potential system solutions and the analysis of alternate solutions. The reason for these activities is to pick the most cost effective system that meets the desired the performance requirement to the lowest cost. A study phase

Manuscript received September 5, 2012
Manuscript revised September 20, 2012

report is prepared and this is recommended to the user or users of the system at the most feasible solution to the problem [4]. The greater the participation of the user in the study the more likely the success of the subsequent phases.

III FUNCTIONAL R EQUIREMENTS

3.1 ATTACKS on shared multicast tree node

In this attack, a malicious node impersonates a tree node and sends a MACT (P) packet, i.e., a prune message, to the tree node's children in the multicast tree. If a downstream node is a non-member and has only one downstream link, it also prunes itself and sends a similar prune message to its downstream node. This may lead to the multicast tree pruning [5]. The multicast pruning may interrupt the group communication so that the packets may not be forwarded to the multicast members and non members.

3.2 Detection of shared multicast tree node attack

A shared multicast tree node attack may occur in the following scenario exists

- When an impersonated tree node sends a MACT-P packet to the tree node children in the multicast tree.
- When the root node cannot forward the packet to the other group members.

3.3 COUNTER MEASURE FOR SHARED MULTICAST TREE NODE ATTACK

Shared multicast tree node attack may cause other members of the multicast group to get compromise and hence deteriorate the group communication, thus high level algorithm is proposed to provide the solution for this the high level Algorithm is described below:
If a shared root node gets attacked in the multicast Tree.

- Then the group members of multicast tree also get compromised to the attack.
- The compromised network can be rehabilitated by reconfiguring the network with the new root node.
- The new root node can be selected by the optimal average distance from that node to the leaves.

3.4 SELFISH NODE BEHAVIOUR

These nodes aim to get the greatest benefits from the networks while trying to preserve their own resources, e.g. battery life or bandwidth. Selfish nodes attempt to maintain communications with the nodes it wants to send data packets to but may refuse to cooperate when it receives routing or data packets that it has no interest in. Therefore, it may either drop data packets or refuse to retransmit routing packets that it has no interest in[6].

Based on using Multicast Ad hoc On-Demand Distance Vector (MAODV) routing protocol, the selfish node can do the following possible actions in Ad hoc network:

- Turn off its power when it does not have active communications with other nodes.
- Does not re-broadcast Route Request (RREQ) when it receives a RREQ.
- Re-broadcasts RREQ but does not forward Route Reply (RREP) on reverse route, therefore the source does not know a route to the destination and it has to rebroadcast a RREQ.
- Re-broadcasts RREQ, forward RREP on reverse route but does not forward data packets.
- Does not uni-cast/broadcast Route Error (RERR) packets when data packets are received but there is no route.
- Selectively drop data packets. This in particular can be used to fight existing mechanisms to detect selfish nodes.

Based on the above threats we can see how damaging selfish nodes can be in MANET, particularly in terms of reducing the delivery rate by dropping packets and not forwarding them which lead to inefficiency in MANET. Improving the ratio of well-behaved nodes therefore results in better trust amongst nodes, better security, and hence better overall operation of the MANET.

3.5 Detection of SELFISH NODE BEHAVIOUR

A node is detected to exhibit selfish behavior if it is not relaying the received packets even if it is active in the network. It may be due to factors such as:

- low energy
- low data rate
- poor channel conditions

This can be detected by analyzing the routing table of the neighbor nodes of the malicious node. If the routing table information of the neighbor does not get updated then selfish behavior can be detected.

3.6 COUNTER MEASURE FOR SELFISH NODE BEHAVIOUR

Selfish behavior of nodes may cause network performance degradation and hence the high level algorithm is proposed to provide the solution for this he high level Algorithm is described below:

- If a mobile node does not relay the packets even if active in the network then.
- The node can be detected to be selfish by two hop acknowledgement.
- If the routing table is not updated in the neighbor nodes of malicious node.

- When the acknowledgement is not received within the time stamp.
- Then the nodes can be reconfigured so that the packets can be routed to the appropriate destination.

TType	***J***	***P***	***G***	***U***	***R***	***Reserved***	***Hop count***

3.7 ATTACK ON CONTROL PACKETS

In MAODV the group leader is typically the first node to join the group node which wish to join the group , if they have the address of the group leader (recorded by the node when the group leader joined the group), unicast a route request (RREQ) to the group leader if they do have any record of the address of the leader for a group they broadcast the RREQ packet this RREQ is rebroadcast by the node which are not members of the multicast tree (which also establish the reverse path and keep the state information consisting of the group address , requesting node id and next hope information).

Multicast Group ip address
source ip address
source sequence number

Type	***J***	***R***	***G***	***Reserved***	***Hop count***

Figure 1: Route Request (RREQ) Message Format.

The format of the Route Request message remains as specified:

Join flag(J) : set when source node wants to join a multicast group.

Repair flag (R) : set when a node wants to initiate a repair to connect two previously disconnected portions of the multicast tree.

When a node wishes to repair a multicast tree, it appends the Multicast Group Rebuild extension. When a node wishes to unicast the RREQ for a multicast group to the group leader, it includes the Multicast Group Leader extension. The route request (RREQ) is answered with the route reply (RREP) by a member of the multicast group. This RREP, containing the distance of the replying node from the group leader and the current sequence number of the multicast group, is unicast to the requesting node (which establish the forward path). Note that only the nodes which have recorded a sequence number greater than that in the RREQ packet can be reply. The receiver node selects the most recent and the shortest path from all the RREPs it receives and sends a Multicast Activation (MACT) messages [7].

Type	***R***	***Reserved***	***G***	***Prefix sz***	***Hop-count***

Figure 2: Route Reply (RREP) Message Format

MACT confirms to the intermediate relying node they would be part of the tree only after the MACT is received, is a forward path establish during the RREP propagation, activated. Nodes that wish to send data to the source use a similar procedure in only one respect: any node with recent route to the multicast group can reply to the non join RREQ.

Other fields

Figure 3: Multicast Activation (MACT) Message Format

Thus the control packets of MAODV like RREQ and RREP when attacked may cause serious effect in route discovery and route establishment.

3.8 deTECTION OF CONTROL PACKET ATTACK

The control packet is said to be attacked:

- If the acknowledgement is not received within the time stamps from the members and non group members of multicasting
- If reverse route is not established by the routing nodes
- If the RREQ-J flag is not set.

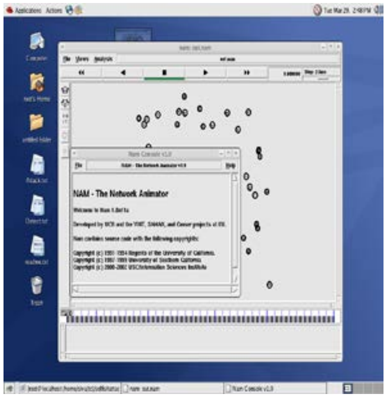
3.9 COUNTER MEASURE FOR CONTROL PACKET ATTACK

Control packet attack may cause network performance degradation due to the lack of connection establishment so that multicasting of information becomes impossible. Hence, the high level algorithm is proposed to provide the solution for this the high level Algorithm is described below:

- If a mobile node does not relay the packets even if active in the network then.
- The node can be detected to be selfish by two hop acknowledgement.
- If the routing table is not updated in the neighbor nodes of malicious node.
- When the acknowledgement is not received within the time stamp.
- Then the nodes can be reconfigured so that the packets can be routed to the appropriate destination.

IV SIMULATION RESULTS

Here NS-2 is used as a simulator.
Simulation Results are shown below.
NETWORK ANIMATOR:



NAM - The Network Animator

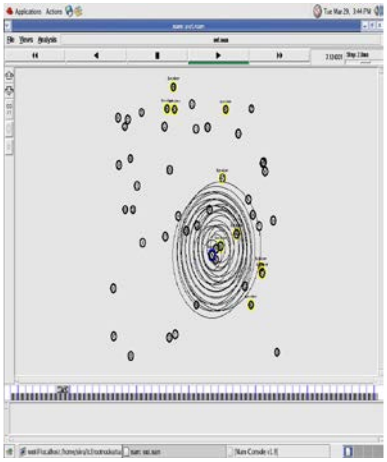
Welcome to Nam 1.0a11a

Developed by UCB and the VINT, SAMAN, and Conser projects at ISI.

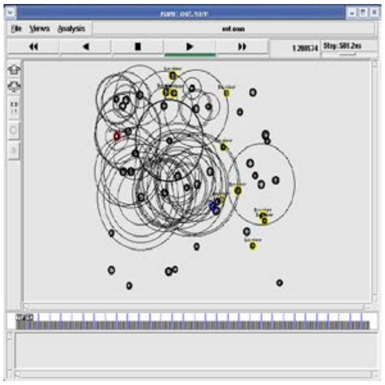
Nam contains source code with the following copyrights:

Copyright (c) 1991-1994 Regents of the University of California.
Copyright (c) 1997-1999 University of Southern California.
Copyright (c) 2000-2002 USC/Information Sciences Institute

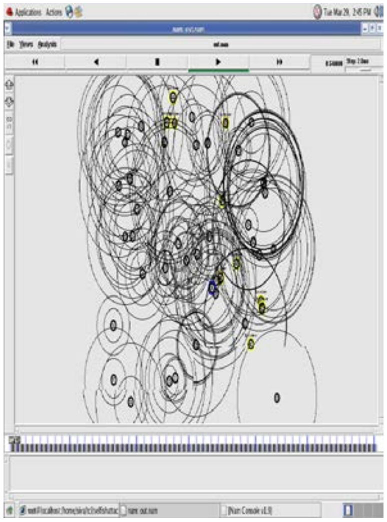
ROOT NODE ATTACK:



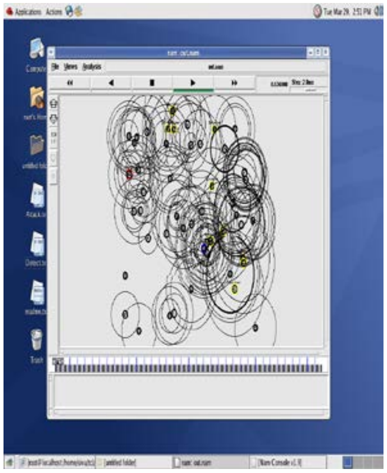
ROOT NODE DETECT:



SELFISH NODE ATTACK:



SELFISH NODE DETECT:



V CONCLUSION AND FUTURE ENHANCEMENTS

This Paper presents a new mechanism for detecting selfish behavior of nodes and implements the solution with higher level algorithm because the selfish behavior may cause network degradation during group communication. the various scenarios during which a node may behave to be selfish or analyzed. This also presents a new mechanism for detecting control packet attack and implements the solution with higher order algorithm because this kind of attack may fail to establish communication among the groups. This also presents the mechanisms for detecting shared root node attack and how to provide the solutions so that all the members and non members do not get compromised to the attack. The security of MAODV has been proposed for the above attacks will be integrated as a solution in the forthcoming future which will detect and countermeasure the above attacks for all scenarios.

The MAODV is being simulated and solutions are realized in Ns-2(Network Simulator) to prove assumptions considered in current work. Ns-2 is an object-oriented event-driven simulator with extensive support for simulation of MAODV. An initial study of network simulator has been done.

REFERENCES

[1] S. Roy, V.G. Addada, S. Setia and S.Jajodia “Securing MAODV: Attacks and countermeasures,” in Proc. SECON’05, IEEE, 2005.

[2] Demir, C and Comaniciu C, “An Auction Based AODV Prorocol for Mobile Ad Hoc Networks with Selfish Nodes,” Communication, 2007.ICC’07. IEEE International Conference in june 2007.

[3] M.Phani Vijaya Krishna, Dr M.P.Sebastain “HMAODV: History aware on Multicast Ad Hoc On Demand Distance Vector Routing” IEEE 2006

[4] Ben-Jye Chang and Yan-Min Lin , Ying-Hsin Liang “Distributed Wireless Links Repair for Maximizing Reliability and Utilization in Multicast MANET”, IEEE 2008

[5] TomoyukiOhta, Toshifumi Kawaguchi, and Yoshiaki Kakuda ,“A New Multicast Routing Protocol Based on Autonomous Clustering in Ad Hoc Networks” ,IEEE 2005.

[6] Bommaiah, McAuley and Talpade.AMRoute, “ADhoc Multicast Routing Protocol”, Internet draft,draft talpade-manet-amroute-00.txt,August 1998,Work in progress.

[7] Josh Broch, David B.Johnson, David A.Maltz, “ The Dynamic Source Routing Protocol for Mobile AdHoc Networks”, Internet Draft,draft-ietf-manet-dsr-00.txt,March 1998,Work in progress.

P. Ramesh graduated in Electronics & Communication Engineering from RMCE, Hyderabad (India) and post graduated in Embedded systems from VNRVJIET,Hyderabad. His research interests includes Cluster based routing for Wireless Sensor Networks and Digital Communication.

Dr.M.Sailaja obtained B.E in Electronics &Communication Engineering. She Completed M.S in USA and PhD from JNTU. Presently, she is working as HOD in ECE Department in JNTU Kakinada. Her Research interests include Parallel Processing and Computer Networks.

S.Koteswararao graduated in Electronics & Communication Engineering from Dr.S.G.I.E.T and post graduated in instrumentation and Control Systems from JNTUK,Kakinada and pursuing his PhD from JNTUK,Kakinada and research interests includes MAC Layer issues of Wireless sensor networks and Digital commmunication.

V.Rajesh graduated in Electronics Engineering from the Institution of Engineers(India) and post graduated in Instrumentation from SRTM and currently submitted his PhD Thesis from ECE dept, Andhra University and research interests includes measuring and processing of Bio-Electric Signals, Virtual Instrumentation and Image processing.