I. J. Computer Network and Information Security, 2013, 10, 1-10
Published Online August 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.10.01

Security Algorithms for Mitigating Selfish and Shared Root Node Attacks in MANETs

J.Sengathir
Research Scholar, Department of Computer Science and Engineering,
Pondicherry Engineering College, Pondicherry, India,
j.sengathir@gmail.com

R.Manoharan
Associate Professor, Department of Computer Science and Engineering,
Pondicherry Engineering College, Pondicherry, India,
rmanoharan@gmail.com

***Abstract*—** Mobile ad hoc network is a type of self configurable, dynamic wireless network in which all the mobile devices are connected to one another without any centralised infrastructure. Since, the network topology of MANETs changes rapidly. It is vulnerable to routing attacks than any other infrastructure based wireless and wired networks. Hence, providing security to this infrastructure-less network is a major issue. This paper investigates on the security mechanisms that are proposed for Selfish node attack, Shared root node attack and the Control packet attack in MANETs with the aid of a well known multicast routing protocol namely Multicast Ad hoc On Demand Distance Vector (MAODV). The security solutions proposed for each of the above mentioned attacks are evaluated with the help of three evaluation parameters namely packet delivery ratio, control overhead and total overhead. The algorithmic solutions thus obtained are analysed in the simulation environment by using ns-2 simulator.

***Index Terms*—** MANETs, Selfish nodes, Shared root node, MADOV, Control packet, Sequence numbers

I. Introduction

A mobile ad hoc network is a self-organizing distributed network in which each and every mobile node performs routing autonomously without any centralized authority [1]. In this Wireless network, the packets are relayed in a multi-hop fashion from the source node to the multicast group members based on the reliability of the nodes present in the routing path. Thus, routing in MANETs necessitates the cooperation of each and every node for successful packet delivery [2]. But the presence of non co-operating nodes i.e., selfish nodes reduces the throughput of the entire network, so an algorithm has to be devised for handling selfish nodes [3]. In this paper, we propose a reactive mechanism called Secure Destined Packet algorithm which can detect and prevent the selfish behaviour based on the calculation of both the cut off ratio and the packet delivery ratio computed on each of the mobile nodes in the network.

In MANETs, the transmissions of data between the groups of hosts are identified through a unique group destination address. But still, the security issues of MANETs in group communications are more challenging because of the commitment of multiple senders and multiple receivers [4]. Although several types of security attacks in MANETs have been studied in the literature, the focus of earlier research was only on unicast (point-to-point) applications [5-7]. The impact of security attacks on multicast scenario of MANETs has not yet been explored. Especially in case of MAODV protocol, the reliability of the data transfer depends on the shared root node or the rendezvous point of each multicast group. Hence securing shared root node becomes a necessary task. In order to make the shared root node more secure, the group leader election algorithm becomes essential.

The protocol used for our study is the MAODV Protocol. Some of the striking features of the protocol are enumerated below. Multicast Ad hoc On-demand distance vector protocol (MAODV) is an enhanced multicast version of AODV Protocol, where all the members of the multicast group are formed into a multicast shared tree [8]. The tree formation includes the non-members and the root of the tree is called the group leader. Multicast data packets are relayed among the tree nodes [9]. The salient feature of the MAODV protocol is about how they form the tree, repair the tree when link break occurs and to join the existing is disconnected tree into a new tree. The four types of packets supported by MAODV are RREQ, RREP, MACT and GRPH [10]. A node broadcasts a RREQ only when it is a member node and if it wants to join the tree or when it is a non-member node but has a data

packet to be delivered to the group [11]. When the node receives the RREQ, it sends the reply by sending the RREP using unicast routing. GRPH is the group hello packet, which is send periodically by group leader to know whether the group members are within the range of communication [12]. MACT packet originates only when there is a need for group communication.

The rest of the paper is organized as follows: In section 2 we discuss on the literature a survey and the list of possible attacks in MANET. In section 3, 4 and 5, we discuss elaborately on the proposed detection and mitigation algorithm of selfish node, shared root node attack and control packet attack respectively. The detailed performance analyses for the proposed algorithms relative to the existing traditional MAODV are discussed in section 6. Finally, we conclude in section 7 with future scope.

II. Literature Review

From the recent past, many secure mitigation algorithms were proposed varying from trust based solution to energy based algorithms for selfish node behavior and shared root node attack. These algorithms were implemented based on the confidence level that a each and every node possesses about their neighbour nodes and they are mainly employed to tackle energy, congestion or bandwidth allocation. Some of the works present in the existing literature are enumerated below.

Ching-Chuan Chiang et al [13] proposed a multicast routing protocol that needs only minimal infrastructure. This protocol makes its profit by exploiting the broadcast facilities of the wireless channel which is present implicitly in the network. The design protocol is a hybrid protocol that shows the property of both flooding and shortest multicast tree.

S. Kumar Das et al [14] proposed a reactive multicast routing protocol which performs its routing by building and maintaining a shared meshes. This shared mesh is formed by the group of core based trees.

H. Yang et al [15] determined the genuineness of the mobile nodes with the help of one way hash function. This one way hash function was manipulated based on the initial input iteratively. The obtained output can be used for authentication. This mechanism also enables to find any fault in the network using explicit acknowledgement

S.Roy, V.G.Addada, S.Setia and S.Jajodia [16] proposed detection and prevention solutions to various attacks on multicast tree maintenance. The various attacks against route discovery and establishment are RREP-INV, MACT (J) –MTF and RREP-INV, MACT (P) –PART. They elaborated on the shared root node attack, how they occur and how they can be mitigated. They have explained about the clear scenario of how the shared multicast tree are formed and how a node or a group of nodes join a source multicast tree.

C.Demir and C.Comaniciu et al [17] proposed an auction based routing methodology for MANETs. The auction based methodology was implemented with the following properties in mind, the first one is that the route can be selected depending upon minimum cost calculated from individual node bids. The second one is that the payment allocated to the winning route should be the one requested by the second smallest biding route. The mechanism is implemented during route discovery following the route discovery process the payment is carried out the specific amount of currency is paid to the intermediate routes.

Chi-Yuan Chang et al [18] proposed an efficient bootstrap router which was designed based on the rendezvous point mechanism. This proposed mechanism can provide a solution to the RP recovery in case of shared tree network. This work also emphasizes the need of PIM multicast network, which provides one-to-many services like videoconferencing and chat applications.

D. Patel et al [19] addressed various security issues against Worm Hole attack. They used the parameter called time of flight which calculates the RTT for each and every node. This work also determines whether mobile nodes are within the communication range or not by using directional antennas.

Bing Wu et al [20] suggested mechanism like Watch Dog, Pathrater and IDS for monitoring, so that the attacks could be prevented with an aid of a reactive solution. This solution mainly concentrates on the key manipulations performed on the mobile node. These computations help to determine whether a node is genuine or not.

A. Similar Types of Attacks

There are a number of routing attacks which may reduce the performance of the MAODV protocol. Short descriptions of some of such attacks are given below:

Neighbouring Attack:

In a normal scenario, each and every participating node first records the id of the packet received. In case of neighbor attack the compromising node simply forwards the packet without recording the packet id assuming that they are neighbours even though they are not in the same radius of communication.

Blackmail Attack:

In case of black mail attack, the attacker node advertises a genuine node as a compromised node which may carry out some malicious behaviour during routing mechanism. Such attacks could prevent the source to choose the best path to the destination there by reducing the overall efficiency and throughput in the network.

Jelly fish Attack:

In this kind of attack, an attacker delays the data packet unnecessarily for some quantum of time before forwarding them. Thus disturbing the performance of the multicast group results in high end to end delay in the networks

Sybil Attack:

In case of Sybil attack, the malicious nodes present in the network topology generates a large number of fake identities to disturb the normal functioning of MANET applications.

Resource consumption Attack:

In this attack, the malicious node tries to consume the resources like battery power and bandwidth of the other nodes available in the network. This could be established by triggering unnecessary route request control messages, beacon messages packets or stale information to nodes.

Sinkhole Attack:

In this specific kind of attack, the compromised attacker node tries to get the attraction of the data packet to itself from all other neighboring nodes. This could make all the data flow to flow to particular node and hence the packet may be altered or eavesdropped.

Byzantine Attack:

In this byzantine attack, an attacked intermediate node or a set of compromised attacker nodes works in collusion and carries out the attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets which results in disruption or degradation of the routing services. It is hard to detect byzantine failures. The network would seem to be operating normally in the viewpoint of the nodes, though it may actually be showing Byzantine behavior.

Gray hole Attack:

The gray hole attack has two phases. In the first phase, a malicious node exploits the protocol to advertise itself having an optimal route to a destination node, with the intention of intercepting packets, even though the route is not optimal. In the second phase, the node drops the intercepted packets with a certain probability. This kind of attack is more difficult to detect than the black hole attack where the malicious node drops the received data packets with certainly. A gray hole may exhibit its malicious behavior different ways. It may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of gray hole node may behave maliciously for some time duration by dropping packets but may switch to normal behavior later. A gray hole may also exhibit a behavior which is a combination of the above two, thereby making its detection even more difficult.

B. Extract of the Literature Review

The review of the literature on the security mechanisms available for MAODV protocol are lacking in the following issues:

i. The methodology by which a shared root node attack can be detected and if detected how to isolate the shared root node is not yet proposed.

ii. The algorithm for choosing a node as the group leader, when the existing shared root node is compromised is not yet explored.

iii. Non-reputation mechanisms for identifying a selfish node in a group are not available.

iv. The use of the sequence number for identifying the control packet attack are not yet established for in this protocol

v. The preventive mechanism that has to be carried out, when the control packets like RREQ, RREP, MACT or GRPH are attacked has not been implemented.

Thus it is motivated to detect and provide solution to these attacks on MAODV, in order to enhance the security and the performance of the network.

III. Selfish Node Attack

Selfish nodes are defined as the mobile nodes that deny forwarding other nodes' packets but relays the packets originated from them. This behaviour is intentionally for maximizing their resources at the expense of all other neighbor nodes. Hence, Selfish nodes are found to be the most vulnerable in MANET environment. Due to the presence of selfish nodes the packet delivery ratio of the network drastically drops and leads to poor performance of the network. Suitable trust solution is required to mitigate the above said attack. Here we propose an algorithm called Secure Destined Packet Algorithm to secure the MAODV protocol against non cooperating nodes and make the protocol more robust. In Secure Destined Packet Algorithm, the detection of selfish behaviour present in the network topology is identified at two different levels. In the primary level, the selfish nodes are identified based on information obtained from neighbours using two hop acknowledgement mechanisms. In the secondary level, the mobile nodes which are already identified as selfish nodes are screened based on inbound and outbound data Counter.

The optimal Packet transmission ratio obtained for each and every node is compared with the cut-off Packet Delivery Ratio. If the optimal Packet transmission ratio is lower, a selfish node is found.

Algorithm 1 Pseudo code for Primary Level Secure Destined Packet Algorithm

Notations
SRCN: Source Node
IMN: Intermediate Node
DSN: Destination Node
THACK: Two hop acknowledgement
FQ: Further Request
FP: Further reply
DTR: Data routing Information
NH_Node: Next Hop Node
Id_Node: Identity of node
SRCN broadcasts **RREQ** to all possible paths
SRCN receives **RREP** as an acknowledgement from DSN
If (RREP is from DSN or any other reliable node) then
Route data packet (Optimal-Route)
Else
Send FQ to all the NH_node
Receive FP and update DTR entry obtained from the current NH_node
End if
If (NH_node is not a reliable node and FP, DTR is not updated) then
Check IMN for selfish node using THACK
End if
If (IMN is not a selfish node) then
Data packet (safer route)
Else
Insecure route
IMN is a selfish-node
Do
Advanced secure destined packet algorithm ()
Do
Current IMN= NH_node
End if.

Algorithm 2 Pseudo code of Secondary Level Secure Destined Packet

Inbound Data Counter: The number of data packets that a source node or any node present in the network (k) receive from a next hop node (m) is determined by DCI(k,m), where $1 \leq k \leq N$, $1 \leq m \leq N$ and N is the node density of the network .

Outbound Data counter: The number of data packets that a mobile node k transmits to the next hop nodes m is termed as DCO (k, m), Where $k \geq 1$, $m \leq N-1$.
Here, the optimal Packet transmission ratio is termed as the ratio between DOC (k, m) of each node 'k' for its next hop node 'm' to the DCO (k, m), where $1 \leq k \leq N$, $1 \leq m \leq N$.

For each data dissemination,
DCI (k, m) = DCI (k, m) +1 (1)
DCO (k, m)= DCO (k, m)+ 1 (2)

The optimal packet transmission ratio for any node 'k' is
Pdr (k, m)=DCO(k,m)/DCI(k, m) (3)
If (Pdr(k,m)> cutoffPdr(k,m))
Mark the k^{th} next hop as selfish node
Inform the source node.
Call Rehabilitate( )
End if.

A. Illustration for Selfish Node Behaviour.

Consider a multicast scenario in MAODV as illustrated in the Fig.1. Here 'S' is the source node, 'M' is the selfish node and 'R1', 'R2', 'R3' are the receiver nodes in the group. When the source 'S' present in the first multicast group transmits the data packets to the receiver nodes present in the next multicast group. Since the node 'M' is selfish, the packets routed through the S-RV1-RV2-M-R2 path are dropped by that node. Since the receiver 'R2' node has not received any packets, it sends RREQs to its neighbors. Further if any RREPs are not received, it sends THACK i.e., two hop acknowledgement for detecting the reliable route and marks the node 'M' as the selfish node in the routing table.

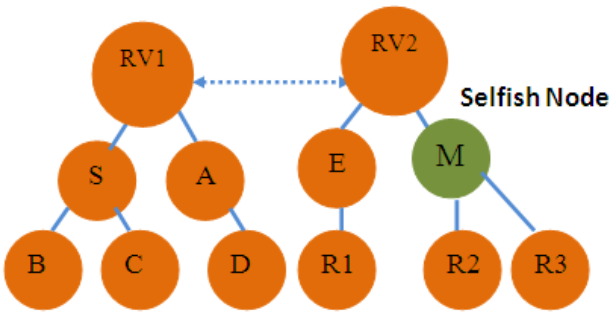

Figure 1: The Presence of Selfish Node in the Multicast Scenario of MAODV

The second level of selfish node detection is achieved by comparing the Packet Transmission Ratio of each and every node with the cut-off ratio computed distributive in each and every node. The mitigation of selfish node is achieved through the help of Rehabilitate ( ).

IV. Shared Root Node Attack

In case of shared root node attack, the attacker node disguises a tree node and sends a MACT (P) packets i.e., a tree prune control packet to all the nodes' present in the multicast tree. If a downstream node has one and only downstream link and if it is a non member, it prunes itself and sends a prune message to its entire downstream node. This may cause multicast tree to be pruned. So the multicast pruning may disturb the group communication by not relaying the packets to the multicast members as well as the non members. Here, we propose a Detecting Shared Root Node algorithm to identify the mobile nodes which tries to exhibit shared root node behaviour. The identified attacker nodes are removed and new zone leader is elected by means of the secure zone leader election algorithm. The newly elected zone leader will update its entries in the multicast table. The zone is reconstructed with the help of newly elected zone leader

Algorithm 3: Pseudo code for mitigating Shared root node attack.

***Notations*:**
SRCN: Source Node
IMN: Intermediate Node
DSN: Destination Node
NH_Node: Next hop Node
Fp: Further Replay
RTN: Root node
ID_Node: Identity of the node
SRCN sends the RREQs to all the routes
The first receiver or the leader of the multicast group RTN receives RREQs
If the RTN Reply's with RREPs then
Send the data packet(safer route)
Else
Call Secure Zone leader Election Algorithm ()
End if

Algorithm 4 Secure Zone leader Election algorithm

***Notations*:**
EZL: Elected zone leader
RP: Reputation Probability
HS: Historical Behaviour of individual nodes.
PC: Present Context Behaviour of Nodes.
If (RTN is attacked)
Begin
For each node present in the multicast group ***do***
Compute

$$RP = \alpha * HS^{t}_{n-1}(m,n) + PC^{t}_{n-1}(m,n)$$

End for
for k nodes do
Compare RP value
End for
Choose node with the maximum RP value as EZL
End if

A. *Illustration for Shared Root Node Behaviour.*

The source node D present in the first multicast tree wants to send data to receivers R1, R2 and R3, the rendezvous point RV of group 1 or group 2 may be compromised as shown in Fig. 2.

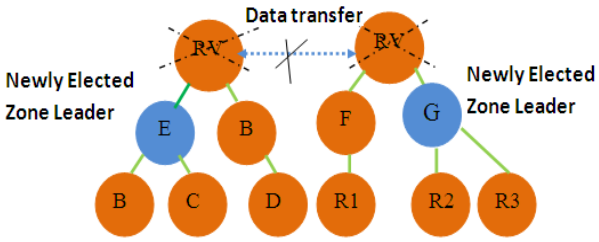

Figure 2: The Presence of Shared Root Node Attack in the Multicast Scenario of MAODV

This can be counteracted by electing a zone leader which has maximum reputation Probability in the multicast group. In this scenario, the newly elected zone leader is E in group 1 and G in group 2 according to their Reputation Probability factor.

V. Control Packet Attack

In case of MAODV, the route establishment between the source node and the receiver nodes in group communication is achieved through control packets namely RREQ, RREP, GRPH and MACT. In our proposed solution, we have devised an algorithm mainly for detecting RREQ and RREP control packet attack. This algorithm makes use of the sequence number for detecting the control packet attack, where sequence number is the monotonically increasing number when the packet relays from one hop to the other hop. The following algorithm detects the control packet attack using sequence number.

Algorithm 5: Pseudo code for detecting control packet attack

Notations:
SRCN: Source Node.
T_o: Current Time.
C: Control Packet
PN: Predecessor Node
DN: Destination
SNo: Sequence Number
RREQ: Route Request Packet.
RREP_ACK_TIME: Duration for getting RREP.
SRCN ***floods*** RREQs to all possible routes.
While (Simclock = T_0+RREP_ACK_TIME)
Begin
Store PN_id, PN_C_SNo, C_DN_SNo, C_Orgid and C_OrigMactid in MACT_ACK_Table
If (PN_C_SNo< C_DN_SNo)
Then Route Data Packets in the path established in Reverse Route
Else
Set PN_id as Malicious in MACT Table
Call Isolate (PN)
Retransmit RREQ
End if
End while

A. *Illustration for Control Packet Attack .*

Initially the source node S sends RREQs to all possible routes and waits for time period called Simclock for RREPs through reverse route as shown in Fig. 3.

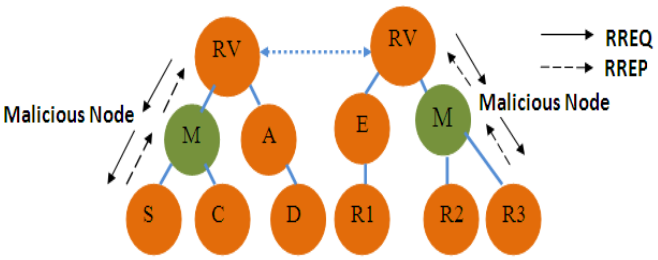

Figure 3: The Presence of Control Packet Attack in the Multicast Scenario of MAODV

If M is not malicious RREPs are acknowledged, it stores the predecessor node id, current sequence number, destination sequence number and Multicast identifier in the Multicast Table. In case, the node M behaves as malicious node then the detection of control packet attack is performed by comparing the current node's sequence number with destination node's sequence number present in the control packet. If the current node sequence number is less than the destination node sequence number, the source node initiates the forwarding of data packets. If not, identify the predecessor node M is identified as malicious node and isolated. Finally call for retransmission of RREQs by the source node S.

VI. Simulation and Results

The simulation environment used for our study is ns-2.26.This simulation environment is chosen because of possessing the feature of high scalability especially for large scale wireless communication networks. We have used the above mentioned simulation platform for analyzing the influence of the selfish, root node and control packet attack based on the evaluation parameters like packet delivery ratio, control overhead and total overhead. In our simulation environment, 50 mobile nodes are placed in a terrain size of 1000X1000. Each source transmits packets of size 512 bytes each at various time intervals. The refresh interval time is set as 20 seconds while the channel capacity is 2 Mbps.

A. Performance Metrics

The performance analysis of multicast ad-hoc on demand distance vector protocol was carried out with the help of the following evaluation parameters.

Packet Delivery Ratio:

Packet delivery ratio may be defined as the ratio of the total number of data packets received to the total number of the data packets sent towards the multicast group in a multicast session.

Control Overhead:

Control overhead may be defined as the ratio of the sum of control data bytes needed by the source to explore the optimal route between the source and the receiver group to the total number of application data bytes transmitted.

Total Overhead:

Total overhead may be defined as the ratio of total number of packets comprising of both the control packets and data packets required for establishing a multicast session to the number of data packets sent towards the group.

B. Simulation Parameters

The following table 1 illustrates the parameters for simulation study.

Table 1 Simulation Parameters

Parameter	Value	Description
No. of mobile nodes	50	Simulation node
Type of channel	Wireless	Channeltype
Type of propagation	Two Ray Ground	Radio-propagation model
Type of network interface	Phy/WirelessPhy	Network interface type
Type of interface queue	Queue/DropTail/ PriQueue	Interface queue
Type of antenna	Antenna/OmniA ntenna	Antenna model
Type of protocol	MAODV	Multicast Adhoc on demand distance vector
Simulation time	50m	Maximum simulation time
Packet size	512bytes	Data packet size
Terrain dimension	1000m 1000m	x-dimension of motion y-dimension of motion

C. Performance Evaluation of Secured Packet Destination Algorithm for Selfish Nodes

Packet Delivery Ratio:

In ideal conditions, the maximum packet delivery ratio of MAODV protocol is 97%. The performance of the protocol crumbles based on the number of selfish nodes present in the multicast scenario and reaches a minimum of 58%. The Fig. 4 shows the performance analysis of Secured Destination Packet Algorithm based on Packet Delivery Ratio

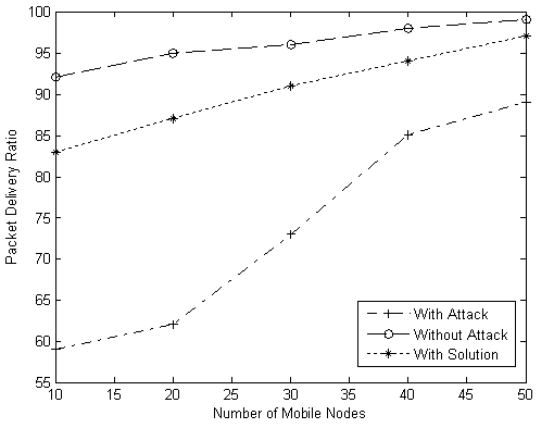

Figure 4: Performance Analysis of Secured Destination Packet Algorithm based on Packet Delivery Ratio.

But When Secure Destination Packet Algorithm is deployed, the packet delivery ratio increases to an extent of 21%.

Control Overhead

The presence of the selfish node behavior increases the control overhead in the MAODV protocol, which

reduces the effective group communication. Hence the control overhead has to be reduced for ideal performance of the protocol. The Fig. 5 shows the Performance Analysis of Secured Destination Packet Algorithm based on Control Overhead.

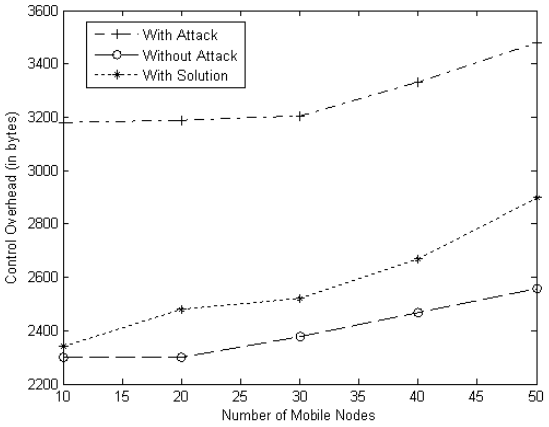

Figure 5: Performance Analysis of Secured Destination Packet Algorithm based on Control Overhead.

Control overhead considerably increases in the presence of the selfish node attack to an extent of 27% but when mitigation algorithm is deployed it shows a decrease of 25%.

Total Overhead

The presence of the selfish node increases the total overhead in the MAODV protocol, thus by affecting the effective group communication. Hence the total overhead has a greater impact on the performance of the protocol. The Fig. 6 shows the performance Analysis of Secured Destination Packet Algorithm based on Total Overhead.

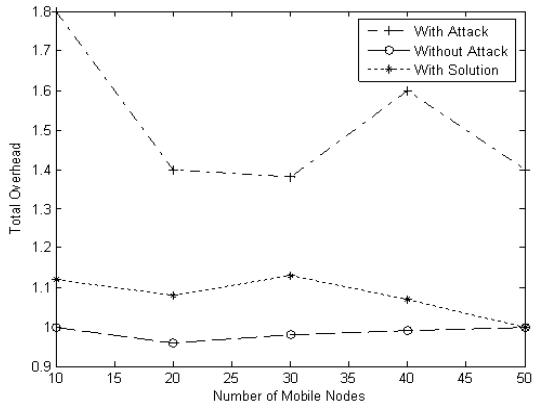

Figure 6: Performance Analysis of Secured Destination Packet Algorithm based on Total Overhead.

The total overhead considerably increases in the presence of the Selfish node attack to an extent of 32% but when mitigation algorithm is deployed it shows a decrease of 30%.

D. Performance Evaluation of Secured Zone Leader Election Algorithm.

Packet Delivery Ratio

In ideal conditions, the maximum packet delivery ratio of MAODV protocol is 97%. The performance of the protocol crumbles based on the number of selfish nodes present in the multicast scenario and reaches a minimum of 57%. The Fig. 7 shows the Performance Analysis of Secured Zone Leader Election Algorithm based on Packet Delivery Ratio.

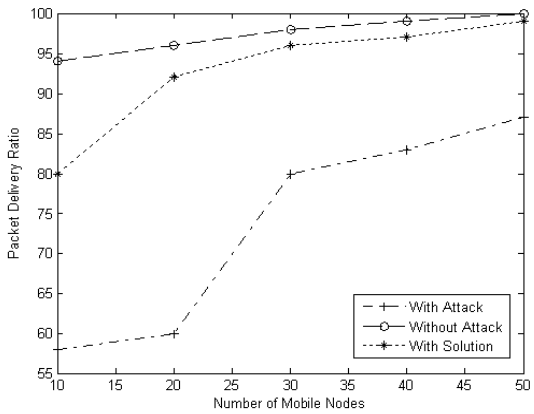

Figure 7: Performance Analysis of Secured Zone Leader Election Algorithm based on Packet Delivery Ratio.

But When Secure Zone leader election Algorithm is deployed, the packet delivery ratio increases to an extent of 33%.

Control Overhead

The presence of the shared root node attack increases the control overhead in the MAODV protocol, which reduces the effective group communication. Hence the control overhead plays a vital impact on the performance of the protocol. The Fig. 8 shows the Performance Analysis of Secured Zone Leader Election Algorithm based on Control Overhead.

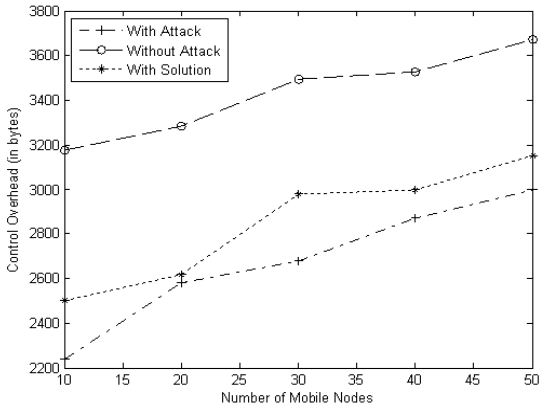

Figure 8: Performance Analysis of Secured Zone Leader Election Algorithm based on Control Overhead.

The control overhead considerably increases in the presence of the selfish node attack to an extent of 27% but when mitigation algorithm is deployed it shows a decrease of 25%.

Total Overhead

The presence of the selfish node attack increases the total overhead in the MAODV protocol, which reduces the effective group communication. Hence the total overhead has a greater impact on the performance of the protocol. The Fig. 9 shows the Performance Analysis of Secured Zone Leader Election Algorithm based on Total Overhead.

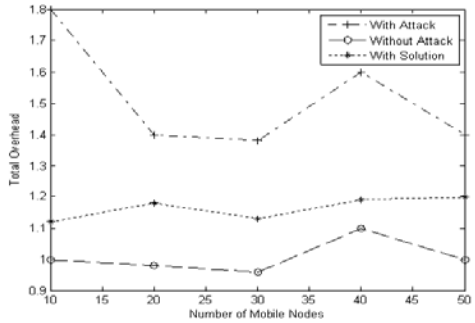

Figure 9: Performance Analysis of Secured Zone Leader Election Algorithm based on Total Overhead.

The total overhead considerably increases in the presence of the Selfish node attack to an extent of 32% but when mitigation algorithm is deployed it shows a decrease of 30%.

E. Performance Evaluation of Sequence Number based Detection Algorithm for Control Packet Attack.

Packet Delivery Ratio

In ideal conditions, the maximum packet delivery ratio of MAODV protocol is 97%. The Fig. 10 shows the performance Analysis of Control Packet Attack Detection Algorithm using Sequence Number based on Packet Delivery Ratio.

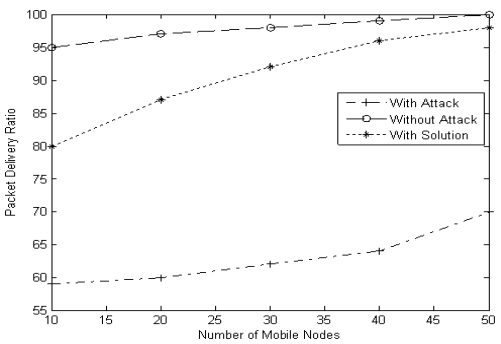

Figure 10: Performance Analysis of Control Packet Attack Detection Algorithm using Sequence Number based on Packet Delivery Ratio.

The performance of the protocol crumbles based on the number of selfish nodes present in the multicast scenario and reaches a minimum of 57%. But when is sequence number based detection algorithm was deployed, the packet delivery ratio increases to an extent of 21%.

Control Overhead

The presence of the control packet attack increases the control overhead in the MAODV protocol, which reduces the effective group communication. Hence the control overhead plays a vital impact on the performance of the protocol. The Fig. 11 shows the performance analysis of Control Packet Attack Detection Algorithm using sequence number based on Control Overhead.

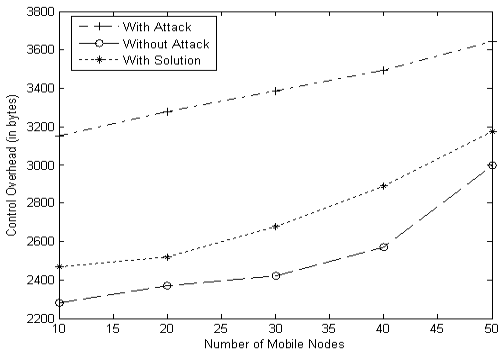

Figure 11: Performance Analysis of Control Packet Attack Detection Algorithm using Sequence Number based on Control Overhead.

The control overhead considerably increases in the presence of the control packet attack to an extent of 29% but when mitigation algorithm is deployed it shows a decrease of 26%.

Total Overhead

The presence of the control packet attack increases the total overhead in the MAODV protocol, which reduces the effective group communication. Hence the total overhead has a greater impact on the performance of the protocol. The Fig. 12 shows the Performance Analysis of Control Packet Attack Detection Algorithm using Sequence Number based on Total Overhead.

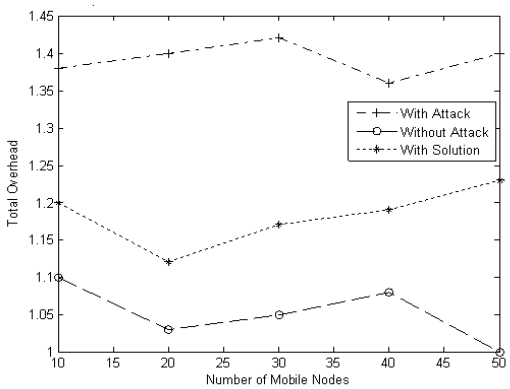

Figure 12: Performance Analysis of Control Packet Attack Detection Algorithm using Sequence Number based on Total Overhead.

The total overhead considerably increases in the presence of the control packet attack to an extent of 30% but when mitigation algorithm is deployed it shows a decrease of 27%.

VII. Conclusion and Future Enhancements

This paper provides an elaborate description about the existing reactive and tree based multicast protocol MAODV and how the security can be provided for the same by detecting and mitigating the attacks like shared root node attack, selfish node attack and control packet attack. The Performance of the algorithm has been analyzed by varying the number of mobile nodes with respect to the metrics like packet delivery ratio, Control overhead and total overhead.

This work can be further proceeded to establish multiple level security, so as to propose security as one of the QOS in group communication. New Security metrics can be framed and the above proposed algorithms can be analyzed with those metrics.

References

[1] E.M.Royer and C.E.Perkins. Multicast Operation of the Ad hoc On-Demand Distance Vector Routing Protocol. Proceedings of ACM MOBICOM 2002, pp.207-218, Aug 2002.

[2] Seungjoon Lee and Chongkwon Kim. Neighbor Supporting Ad Hoc Multicast Routing Protocol. In Proceedings of ACM the First ACM International Symposium on Mobile Ad Hoc Networking and Computing, pages 37–44, August 2000.

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

[4] S.Buchegger and J-Y L.Boudec. Nodes bearing Grudges: Towards routing security, Fairness, and Robustness in Mobile Ad-Hoc Networks preseented at tenth Eurominicro workshop on Partallel. Distributed and Networkbased Processing , Canary Islands, spain, 2002.

[5] L.Buttyan and J-P, Hubaux, Stimulating Cooperation in Self –organizing Mobile Ad hoc Networks, Mobile Computing and Networking. Pp 255-265, 2003.

[6] S.Marti, T.J Giuli, K.Lai, and M.Baker. Mitigating routing misbehavior in mobile ad hoc networks. Mobile Computing and Networking, pp 255-2656, 2000.

[7] P.Michiardi and R.Molva, CORE: A collaborative reputation mechanism to enforce node cooperation mobile ad hoc networks. presented at Communication and Multimedia security, Protoroz, Solvenia, 2002.

[8] S.Buchegger and J-Y L.Boudec. Performance Analysis of the CONFIDANT protocol: Cooperation of Nodes – Fairness in Distributed Ad-hoc Networks. Presented at tenth Eurominicro workshop on Partallel, Distributed and Network based Processing , Canary Islands, spain, 2002.

[9] F.Kargl A.Klenk , S.Schlott and M.Weber. Advanced Detection of selfish or Malicious Nodes in Ad hoc Networks. Presented at 1st European Workshop on Security in Ad-Hoc and Sensor Network. Heidelberg Germany,2004.

[10] Md. Amir Khusru Akhtar & G. Sahoo. Mathematical Model for the Detection of Selfish Nodes in MANETs. International Journal of Computer Science and Informatics (IJCSI) ISSN (PRINT): 2231 – 5292, Volume-1, Issue-3.

[11] A.H Azni, Rabiah Ahmad,Zul Azri Muhamad Noh, Abd Samad Hasan Basari, Burairah Hussin. Correlated Node Behavior Model based on Semi Markov Process for MANETS. IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, January 2012.

[12] C.A.V.Campos and L.F.M.de Moraes. A Morkovian Model Representation of Individual Mobility Scenarios in Ad Hoc Networks and Its Evaluation. EURASIP Journal on Wireless Communicationsand Networking.,Pp231 –5292, Volume-1, Issue-3.

[13] Ching-Chuan Chiang, Mario Gerla, and Lixia Zhang. Forwarding Group Multicast Protocol (FGMP) for Multihop, Mobile Wireless Networks. Cluster Computing, Springer Special Issue on Mobile Computing, 1(2):187–196, 1998.

[14] Subir Kumar Das, B.S. Manoj, and C. Siva Ram Murthy. Dynamic Core-Based Multicast Routing Protocol for Ad Hoc Wireless Networks. In Proceedings of the Third ACM International Symposium on Mobile Ad Hoc Networking and Computing, pages 24–35, June 2002.

[15] H. Yang, H. Y. Luo, F. Ye, S. W. Lu, and L. Zhang, Security in mobile ad hoc networks: Challenges and solutions. IEEE Wireless Communications, vol. 11, pp. 38-47, 2004.

[16] S. Roy, V.G. Addada, S. Setia and S.Jajodia, *Securing MAODV: Attacks and countermeasures,* in Proceedings of. SECON'05, IEEE,2005.

[17] Demir, C and Comaniciu C. An Auction based AODV Protocol for Mobile Ad Hoc Networks with Selfish Node. Communications ICC'07. IEEE International Conference in June 2007.

[18] Chi-Yuan Chang, Yun-Sheng Yen. Chang-Wei Hsiesh Han-Chieh Chao An Efficient Rendezvous Point Recovery Mechanism in Multicasting Network. International Conference on Communications and Mobile Computing, 2007.

[19] Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah. MANET Routing Protocols and Wormhole Attack against AODV. IJCSNS International Journal of Computer Science and Network Security, Vol.10 No.4, pp. 12-18, April 2010.

[20] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei. A Survey on Attacks and Counter measures in Mobile Ad Hoc Networks. WIRELESS/MOBILE

NETWORK SECURITY Y. Xiao, X. Shen, and D.-Z. Du (Eds.) 2006 Springer.

J.Sengathir is a Research Scholar in the Department of Computer Science and Engineering, Pondicherry Engineering College, Pondicherry, India. His main research area includes Mobile Ad hoc Network Security, Cloud Security and Software Engineering.

Dr. R.Manoharan is an Associate professor in the Department of Computer Science and Engineering, Pondicherry Engineering College. His main research area includes Mobile Ad hoc Networks, Wireless Sensor Network, Cloud Security, LTE and Software Engineering.

