Secure Multicast Routing in MANETs for PBM Protocol

A. Amuthan
Associate professor
Department of CSE
Pondicherry Engineering
College, Puducherry, India

S. Parthiban
Senior Technical Assistant
Department of CSE
Pondicherry University
Puducherry, India

R.Kaviarasan
Assistant Professor
Department of CSE
Alpha College of Engg & Tech
Puducherry, India

ABSTRACT

A Mobile Ad-hoc NETwork (MANET) consists of Mobile Nodes (MNs) without any centralized authority. Mobile nodes form a network over radio links due to its infrastructure less environment. Multicast routing plays a significant role in MANETs. Due to its features, such as dynamic network topology, limited bandwidth, and limited battery power, routing in MANETs becomes a tedious task. In the presence of malicious nodes, the MANET is vulnerable to various kinds of attacks. The MANET protocol is found to be more vulnerable due to the lack of centralized authority and also due to its dynamic nature. Position Based Multicast (PBM) protocol does not require any distribution structure and it avoids flooding of control packets. It uses the geographical locations of the intermediate nodes and the destination node to make the message forwarding decisions. Position-based routing is commonly regarded as highly scalable and very robust against frequent topological changes. However, there are several potential security issues for the development of position-based routing protocols. In this paper, we examine the various multicast routing attacks and a suitable countermeasure is provided against attacks using game theory in the existing Position Based Multicast (PBM) protocol in MANETs. The proposed countermeasure is evaluated using the performance metrics namely packet delivery ratio, End to End Delay and Control Overhead.

Keywords

MANETs, PBM, MN, impersonation attack, replay attack, denial of service, Flooding attack.

1. INTRODUCTION

With the development of wireless communication technology, two basic wireless network models have been developed for the same. The fixed backbone wireless model consists of a large number of Mobile Nodes (MNs) and relatively fewer, but more powerful, fixed nodes. MANETs are collection of mobile nodes without any infrastructure the communication between a fixed node and an MN within its range occurs via the wireless medium. However, this requires a fixed permanent infrastructure. Another system model, a Mobile Ad-hoc NETwork (MANET), is a self-organizing collection of MNs that form a temporary and dynamic wireless network on a shared wireless channel without the aid of a fixed networking infrastructure or centralized administration. A communication session is achieved either through single-hop transmission if the recipient is within the transmission range of the source node, or by relaying through intermediate nodes. For this reason, MANETs are also called multi-hop packet radio network. However, the transmission range of each low-power node is limited to each other’s proximity, and out-of-range nodes are routed through intermediate nodes.

The applications of MANETs are used in the field of disaster relief management, military system, group communication. MNs in MANETs are capable of communicating with each other without the use of a network infrastructure or any centralized administration. As the transmission range of wireless network is much smaller, the mobile nodes have to depend upon the intermediate nodes for data transmission. Each MN operates not only as a host but also as a router, forwarding packets for other MNs in the network that may not be within direct wireless transmission range of each other. Each node participates in an ad-hoc routing protocol that allows itself to discover multi-hop paths through the network to any other node.

This paper discusses on the issues and challenges in multicast protocols. MANETs are prone to many security attacks. So devising a suitable countermeasure to mitigate the attacks and make the protocol becomes more challenging. The PBM protocol from the literature is found to be vulnerable to many attacks a mitigating technique is devised and evaluated on the performance of the network and result is observed.

2. ISSUES AND CHALLENGES IN MANETs

The MANET network has number of issues regarding the topology. The issues like Energy consumption, QOS, security and scalability due to the dynamic nature of the networks. The utilization in more energy level of the nodes results in network congestion of the nodes

2.1 Topology, Mobility, and Robustness

A multicast routing protocol should be robust enough to react quickly with the mobility of the nodes and should adapt to topological changes in order to prevent dropping up of packets during data transmission would create a low packet delivery ratio.

2.2 Capacity and Efficiency

Routing protocols should provide less number of control packets transmitted through the network relative to the number of data packets reaching their destination, and methods to improve and increase the available capacity need to be considered

2.3 Energy Consumption

Energy saving techniques aimed at minimizing the total power consumption of all nodes in the multicast group (minimize the number of nodes used to establish multicast connectivity, minimize the number of overhead controls, etc.) and at maximizing the multicast life span should be considered.

2.4 Quality of Service (QoS) and Resource Management

Multicast routing protocols should be able to reserve different network resources to achieve QoS requirements such as, capacity, delay, delay jitter, and packet loss. It is very difficult to meet all QoS requirements at the same time because of the peculiarities of ad hoc networks.

2.5 Security and Reliability

Security provisioning is a crucial issue in MANET multicasting due to the broadcast nature of this type of network, the existence of a wireless medium, and the lack of any centralized infrastructure. This makes MANETs vulnerable active as well as passive attacks. Multicast routing protocols should take this into account, especially in some applications such as military (battlefield) operations, national crises, and emergency operations. Reliability is key a key factor in determining the packet delivery ratio of the network.

2.6 Scalability

A multicast routing protocol should be able to provide an acceptable level of service in a network irrespective of the number of nodes present in the network. It is very important to take into account the nondeterministic characteristics (power and capacity limitations, random mobility, etc.) of the MANET environment in coping with this issue.

3. VULNERABITIES IN MANETs

The attacks [2] can be categorized on the basis of the source of the attacks i.e. Internal or External, and on the behavior of the attack i.e. Passive or Active attack.

- External attacks, in which the attacker advertises fake routing information to the nodes and causes congestion.
- Internal attacks, in which the adversary wants to gain the normal access to the network and in order to participate in the network activities by impersonation or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.
- In passive attacks, the attackers typically involve eavesdropping of data, thus disclose the information of the location and move patterns of mobile nodes. This kind of attack is very difficult to detect, because the attacker seldom exhibits abnormal activities.
- Active attacks, on the other hand, involve actions performed by intruder. The target of the attack can be either data traffic or routing traffic. The intruders floods large volumes of unwanted data packets which results in network congestion. They can also intentionally drop, corrupt and delay data packets passing through it.

In the following, the main attacks that emerge in the mobile ad hoc networks are discussed.

3.1 Impersonation Attack

Malicious nodes use the identity of other nodes in the network. Impersonation attack is the first step for most of the attacks and it is used to launch further more sophisticated attacks. Impersonation attacks are launched by using other node's identity, such as IP or MAC address. If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic as a result it will advertise fake routing packets, gain access to some confidential data, modify the contents or drop the packets.

3.2 Replay Attack

The attacker collects data as well as routing packets and replays them at a later moment in time. In other words, it is the propagation of old routing messages, which do not reflect current topology, in the network to affect routes and to increase the network routing traffic. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions. This can result in a falsely detected network topology or help to impersonate a different node identity. It can be used to gain access to data which was demanded by replayed packet. This type of attack can be prevented by using the concept of sequence number technique.

3.3 Denial of Service

This attack aims to attack the availability of a node or the entire network. If the attack is successful the services will not be available. The attacker generally uses radio signal jamming and the battery exhaustion method. Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network.

3.4 Flooding Attack

Flooding attack is classified into RREQ, RREP, control packet and data packet flooding. This attack aims in exhausting the network resources, such as bandwidth and to consume a node’s resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance.

All these vulnerabilities cause a drop in the performance of the protocols in MANETs.

4. POSITIONBASEDMULTICAST (PBM) PROTOCOL

Position-Based Multicast (PBM) [1] [3] is a multicast routing algorithm for Mobile Ad-hoc NETworks which does require a tree or mesh based hierarchy. Instead forwarding node uses information about the positions of the destinations and its own neighbors to determine the next hops that the packet should be forwarded to and is thus very well suited for highly dynamic networks. PBM is a generalization of existing position-based unicast routing protocols such as face-2 or GPSR. The key contributions of PBM are rules for the splitting of multicast packets and a repair strategy for situations where there exists no direct neighbor that makes progress toward one or more destinations. Position-based routing can be divided into two main functional elements: the location service and position based forwarding. The location service is used to map the unique identifier (such as an IP address) of a node to its geographical position. Position-based forwarding is performed by a node to select one of its neighbors in transmission range as the next hop the packet should be forwarded to. This protocol uses the geographic positions to determine its position. With this information, the forwarding node selects one of its neighbors as a next hop such that the packet makes progress towards the geographical position of the destination. It is possible that there is no neighbor with progress towards the destination while there still exists a valid route to the destination. The packet is then said to have reached a local optimum. In this case a recovery strategy is used to escape the local optimum and to find a path towards the destination.

In order to extend position-based routing to multicast two key problems have to be solved. First, at certain nodes multicast packet has to be split into multiple copies in order to reach all destinations, the challenge being to decide when such a copy should be created. Second, the recovery strategy used to escape from a local optimum needs to be adapted to take multiple destinations into account.

Node that forwards a packet has access to the following information:

- The node's own geographical position:
- The position of all neighbors within transmission range:
- The positions of the destinations

Given this information the main task of a forwarding node in PBM is to find a set of neighbors that should forward the packet next. If the current node selects more than one next hope node, then the multicast packet is split. There are two distinct cases that can occur when a forwarding node selects the next hop nodes: either for each destination exists at least one neighbor which is closer to that destination than the forwarding node itself. In this case greedy multicast forwarding is used. Otherwise the node employs perimeter multicast forwarding.

4.1 Greedy Multicast Forwarding

Optimizing the progress of the packet can be done in the following way. Let k be the forwarding node, N the set of all neighbors of k, W the set of all subsets of N, Z the set of all destination nodes, and d(x,y) a function which measures the distance between nodes x and y. Given a set of next hop nodes w belongs to W the overall remaining distance to all destinations of a multicast packet can be calculated as shown in Equation 1. In this equation for each destination the next hop node in the set w is chosen which is closest to that destination. Using Equation 1 as the sole optimization criterion would lead to a splitting of the multicast packet as soon as there is no single neighbor which provides the largest progress towards all destinations. This may be undesirable since it ignores the bandwidth usage.

$$fd(w) = \sum_{z \in Z} \underset{m\epsilon W}{\min(d(m,z))} \qquad (1)$$

In order to consider the bandwidth usage we include the number of next hop nodes as a second element into the optimization criterion. The overall optimization criterion that determines which set of next hop nodes w belongs to W should be selected as next forwarding nodes is given in Equation 2.

$$f(w) = \frac{|w|}{|N|} + (1-\gamma)\,\frac{fd(w) = \sum_{z \in Z} \underset{m\epsilon W}{\min(d(m,z)}}{\sum_{z \in Z}(d(m,z)} \qquad (2)$$

The first part of the equation determines the number of next hop neighbors and normalizes it to a value between [0,1] by dividing it by the total number of neighbors of k. The second part determines the remaining overall distance from the next hop nodes towards the destinations and normalizes this to a value between [0,1] by dividing it by the remaining overall distance calculated from the forwarding node k to the destinations. $\lambda\epsilon$ [0,1] determines the weight of each objective. If λ is close to 0 multicast packets will be split early, while for λ close to 1 the multicast packet will only be split if this is enforced by the restriction that there must be progress for each destination. λ determines how early a packet should be split.

4.2 Perimeter Multicast Forwarding

Applying greedy multicast forwarding may lead to a situation where the packet arrives at a node that does not have neighbors providing progress for one or more destinations. An example of this is depicted in Fig: 1 the copy of the multicast packet which is on its way to D2, D3, and D4, as well as the copy for D5 get stuck in a local optimum.

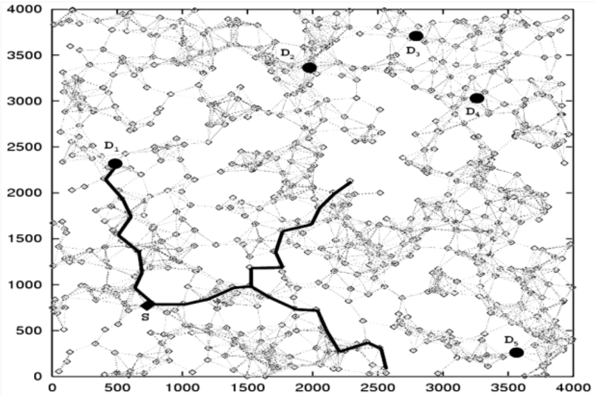

Fig 1: Greedy Multicast Routing Failure

This problem has been solved by applying a modification of the right hand rule. The basic idea is to traverse the boundaries of gaps in the network until greedy forwarding can be resumed. To this end the graph formed by the connections (edges) between mobile nodes is planarized, i.e., intersecting edges are removed. If a node in PBM detects that it has no neighbors with forward progress for one or more destinations, then multicast perimeter mode is initialized for these destinations. For all other destinations greedy multicast forwarding is used. On the planarized graph, the virtual edge is calculated as the connection between the current node and the position representing the average of the positions of the affected destination nodes. The multicast packet is then transmitted over the first edge counter-clockwise of the virtual edge. A multicast packet transmitted this way is said to be in perimeter mode. When a node receives a perimeter multicast packet, it checks for each destination, if it is closer to that destination than the node where the packet entered perimeter multicast mode. For all destinations where this is the case greedy multicast forwarding can be resumed, for all other destinations perimeter multicasting is continued by transmitting the packet over the next edge counter-clockwise of the edge where the packet arrived. Automatically splitting a packet into copies that are to be forwarded in greedy multicast mode and a copy that is to use perimeter multicast may cause the transmission of the same packet to two nodes which are located in the same direction, or even to the same node twice. In order to reduce the load on the network PBM includes an optional combination of greedy and perimeter multicast forwarding: if some, but not all, destinations of a packet require perimeter multicast forwarding, then the next hop is determined using the perimeter rules from above. All copies of the packet with destinations for which greedy forwarding could be used also select this node as the next hop, if it provides progress towards the copy's destination. This reduces the number of copies of the same packet in the network. It comes at the cost of a potentially increased path length towards the individual destinations. Fig 2 shows how the problem depicted in Fig 1 is solved using perimeter multicast routing with and without combining perimeter and greedy packets.

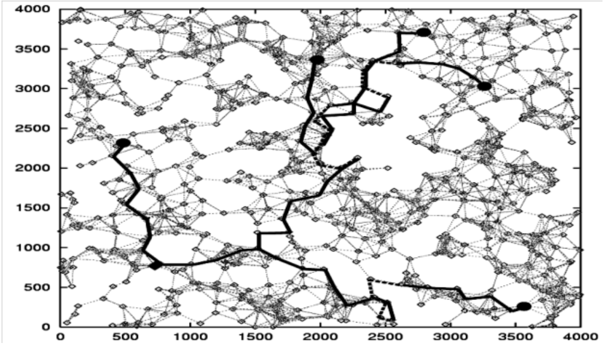

Fig 2(a): Paths taken without combining perimeter and greedy packets

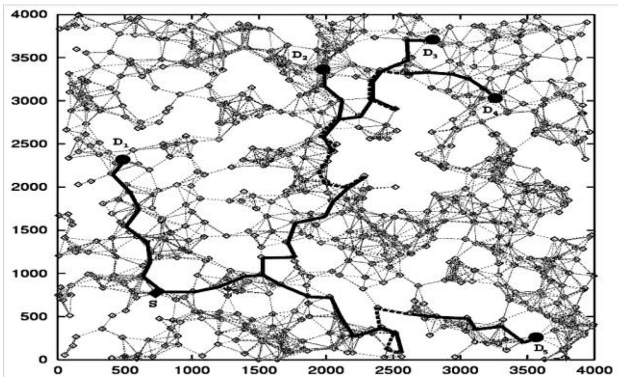

Fig 2(b): Paths taken with combining perimeter and greedy packets

5. PROPOSED SOLUTION

5.1 Attack and Flee Mechanism:

In MANETs, a malicious node would plan to attack the network and flee from its position whenever it has been detected, so that it can start again with a clean history when it re-appears in the network after a prescribed amount of time. This paper focuses on this scenario and the regular node raises an alarm whenever a node flees. There are two possibilities when a node flees-

- When a malicious node flees.
- When a regular node flees.

The alarm must be raised only in the first situation. This scenario is shown in the figure below. The malicious nodes at any given point in time have three possible actions to take- co-operate, attack or decline, while the regular node has two options- raise an alarm or not. The nodes must choose between these options in such a way as to maximize it s goal strategy. The nodes are split into logical regions called clusters and the nodes in a cluster co-operate with each other in the detection of malicious nodes. The various cost factors involved for the actions are taken into consideration in the stage game between the regular and malicious nodes.

The existing work suggests [5] that the malicious node must attack with a probability p=(Ca – Cc)/Ga, where Ca is the cost to attack and Cc is the cost to co-operate and Ga is the gain as a result of the attack. A report must be made about the malicious activity with a factor of O(1-u), where O is the belief on the node and u is the uncertainty in this belief. Since the malicious node will also be aware of the probability with which the other nodes in the cluster will report, it can choose its own probability to flee.

A few mechanisms used to prevent this type of mechanism are as follows. One of them is dynamic threshold which must be chosen by all the members in the cluster by taking into consideration the cost required to raise an alarm. Belief dissemination (authentication mechanism) suggests to decrease the probability so that the malicious nodes become more conservative and also to enable communication between the nodes in the cluster.

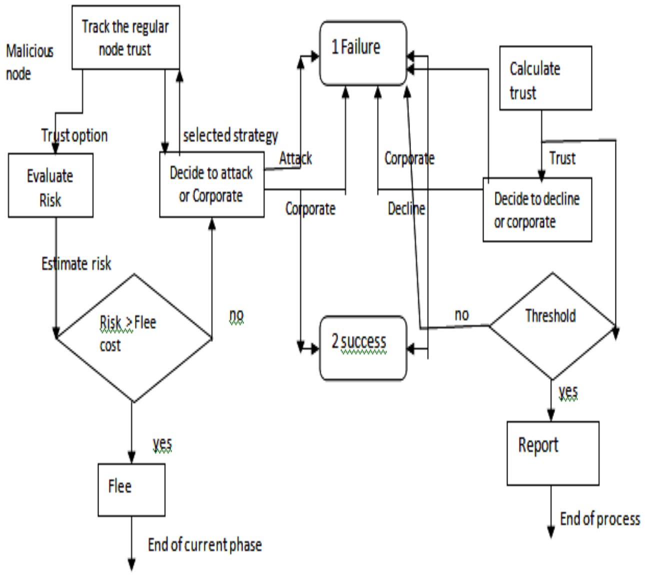

Fig 3: Attack and flee mechanism

The other mechanisms include tit-for-tat mechanism, system without uncertainty and a never fleeing equilibrium. The main disadvantage of this solution is that the malicious node is well aware of the regular node's strategies and it can make use of this knowledge to cause maximum damage to the network. It also does not deal with the co-operative strategy of the malicious nodes.

5.2 Location Guided Steiner Tree

The Steiner tree is commonly used as a multicast packet distribution tree for efficient delivery of multicast packets in a fixed network. It spans over all nodes in a multicast group and minimizes the overall cost of the tree. Finding a Steiner tree in a network is a NP-hard optimization problem. Under the well-known Takahashi-Matsuyama heuristic, the multicast routing protocol generates a Steiner tree by an incremental approach. Initially the tree contains only the source node. At each iteration, the nearest unconnected destination to the partially constructed tree is found and the least-hop path between them is added to the tree. The distance is usually measured by the number of network-level hops. This tree construction process is repeated until all destinations are included in the tree. In a router-assisted multicasting approach, every node in a network can become a tree node to forward packets, in which case the constructed Steiner tree is near optimal.

The location-guided Steiner (LGS) tree is constructed using a modified version of the Takahashi-Matsuyama heuristic. The differences are: 1) we use geometric distance as a measurement of closeness; 2) only the group nodes can be used as tree nodes. Between the group nodes, data packets are encapsulated in unicast packets and forwarded via the underlying unicast routing protocol. Below we use the same set of nodes in the earlier example to illustrate the construction of a LGS tree, as shown in Figure 3.4

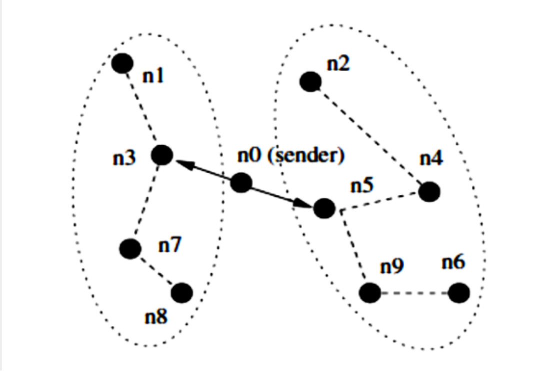

Fig 4: LGS algorithm

Initially, the tree only contains the sender node n0. Within the remaining set of nodes {n1, n2. . . n9}, node n3 is geometrically closest to n0. Therefore, n3 is added into the tree with edge n0n3. In the second step, the remaining set of unconnected nodes is examined and the node closest to the partially constructed tree is selected. In the example, we compare the distance from n0 to each of the nodes in the un-connected set {n1, n2, n4, . . . , n9}, as well as the distance from n3 to that set, and select the shortest distance which is between n0 and n5. Therefore, n5 is added to the tree with edge n0n5. This process repeats until all the nodes have been included in the tree as shown in the figure. Subsequently, the sender node n0 forwards a copy of the data packet to each of its children nodes, i.e. n2, n3, and n5, with their corresponding subtrees as destinations. Thus the packets sent by the sender reaches all the members of the multicast group.

5.3 Solution for Attack and Flee Mechanism

The common objective of a malicious node is maximizing the damage to the network while avoiding being caught. In order to minimize the impact of malicious nodes and to simulate cooperation, regular nodes will monitor and continuously evaluate its neighbors. But malicious nodes have the strategy of fleeing to avoid punishment in MANETs. There exists Bayesian Nash equilibrium in the game between the normal and malicious nodes. Therefore, a malicious node can start its malicious behavior all over again with clean history in a new location by fleeing before being caught. We propose a modified multicast tree formation algorithm such that the suspicious nodes are placed at the bottom of the multicast tree (leaf nodes). When a node tries to flee from the multicast session, we find out the position of that node in the multicast tree. If the node is a split node, we do not take any action. If it is a leaf node, depending on the threshold value, either perform a Denial of Service attack on the fleeing node or inform the network that the node is suspicious.

5.4 Trust Calculation

The continuous monitoring of the neighboring nodes is done based on the trust value determination. The trust value equation is as follows:
TV=W*TV1 + (1-W)*TV2 ---- (3)
Where TV1 is the first part of the trust value determined using the maturity value of the node. It is determined based on the links held by the nodes at present and the time of establishment of the link taking into consideration the node's mobility.

$\mathrm{TV}_1 = \left(\sum_1^{l}(\mathrm{pt} - \mathrm{ct})\right) * \mathrm{s}$ ---- (4)

pt- time of determination of trust value
ct- time of link creation
l- Number of links held by the node
s- speed with which the node moves in the network
TV2 is the second part of the trust value which is calculated as the ratio of the packets forwarded by the node to the number of packets received by the node.
TV2=pf/pr ---- (5)

pf- number of packets forwarded by the node
pr- number of packets received by the node
W is the weightage. It determines how much each part of the trust value contributes to the final value. In other words, it determines how the two methods of trust calculation are combined to get the final trust value.

5.5 Tree Formation

The Location Guided Steiner tree formation algorithm is modified to improve the efficiency of the protocol. In LGS, while determining the children of a particular node in the multicast tree, only the distance is taken into consideration. Whereas in the modified approach, the trust value of the nodes along with the distance between the nodes is considered for tree construction.
In fig 4, if the trust value of n7 is greater than that of n3 and the distant between n0 and n7 is not very large when compared to that between n0 and n3, then the formation of the multicast tree varies. Node, n7 is made the child of the source node (n0) and n3 will become the child of n7 as shown in the figure below

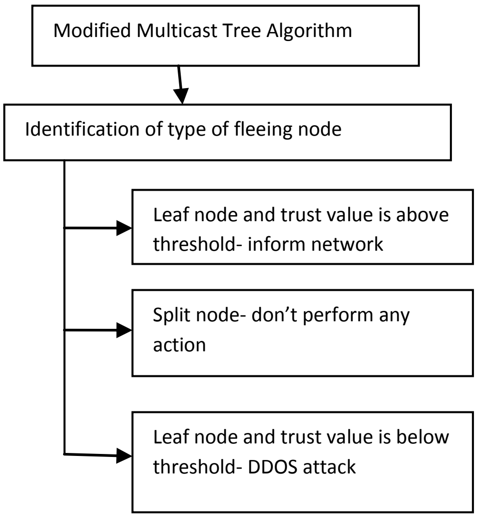
Modified Multicast Tree Algorithm
Identification of type of fleeing node
Leaf node and trust value is above threshold- inform network
Split node- don't perform any action
Leaf node and trust value is below threshold- DDOS attack

Fig 6: Solution

The threshold value is determined based on the uncertainty in the determination of trust value.

Threshold = TV (1-u) ---- (6)

Where u is the uncertainty is the trust calculation.

6. SIMULATION SETUP

The proposed work is simulated in ns-2.28 environment. The simulation scenario consists of 50 nodes out of which some nodes are configured to be attackers are randomly deployed in a terrain dimension of 500m X 500m with the following simulation environment shown in the table below:

Table 1. Simulation Settings

PARAMETER	VALUE	DESCRIPTION
Channel	Channel/Wirelesschannel	Channel Type
Propagation	Propagation/TwoRayGround	Radio Propagation Model
Network Interface	Phy/WirelessPhy	Network Interface Type
MAC	Mac/802_11	Medium Access Control Type
Interface Queue	Queue/DropTail	Interface Queue Type
Link Layer	LL	Link Layer
Antenna	Antenna/OmniAntenna	Antenna Model
Interface Queue Length	50(in packets)	Maximum packet in interface Queue
Routing Protocol	SPBM	Routing Protocol
Data Rate	11Mbps	Data Transfer Rate
Terrain Dimension	500m X 500m	Terrain Dimension of the network
Simulation Time	100 Seconds	Total duration of the simulation
Packet Size	128Bytes	Size of the CBR traffic packet
Number of Nodes	50	Number of nodes in the Scenario

7. SIMULATION RESULTS

The proposed solution is evaluated in terms of Packet Delivery Ratio, Average delay, control overhead and total overhead.

7.1 Packet Delivery ratio

Packet delivery ratio(PDR) is the ratio of the number of packets received and the number of packets expected to be received. For the multicast packet delivery, the ratio is equal to the total number of received packets over the multiplication of the group size and the number of originated packets. The packet delivery ratio is determined for varying number of nodes and the graph is generated as shown below. The graph shows a decrease in the delivery ratio in the presence of attackers. After implementation of the solution, the delivery ratio increases by around **10%** with respect to the delivery ratio in the presence of attacks.

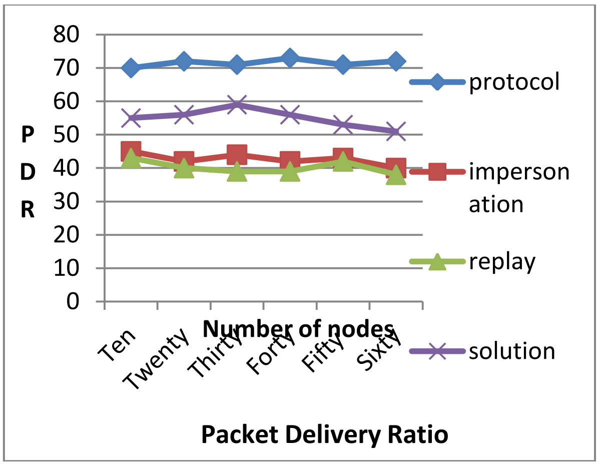

Fig 7: Packet Delivery Ratio

7.2 Average delay

Average delay is the total latency experienced by a packet to traverse the network from the source to destination. In other words it is the time taken for a packet to travel from the source to destination. The average delay is determined for varying number of nodes and the graph is generated as shown below. The delay increases with the presence of malicious nodes. With the implementation of the solution, the delay is reduced by a value of 1.5ms with respect to replay attack and a value of 0.3 with respect to impersonation attack.

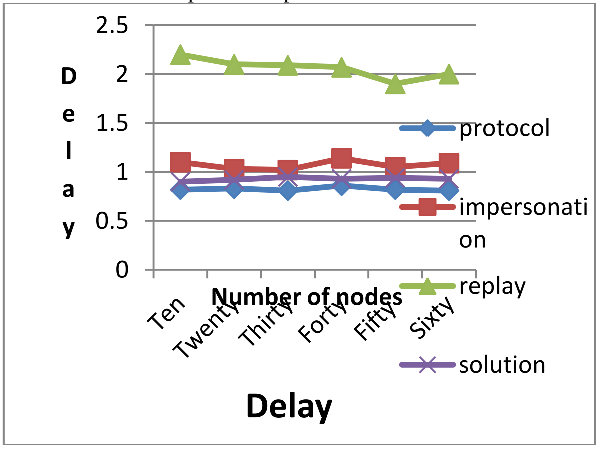

Fig 8: Average delay

7.3 Control overhead

Control packet overhead is the ratio of the number of control data bytes which is used by the sender to discover the secure route between sender and receiver and the total number of application data bytes transferred between sender and receiver. The control overhead is determined for varying number of nodes and the graph is generated as shown below. The overhead increases with the presence of malicious nodes. With the implementation of the solution, it is reduced by around **5%** with respect to the control overhead in the presence of the attacks.

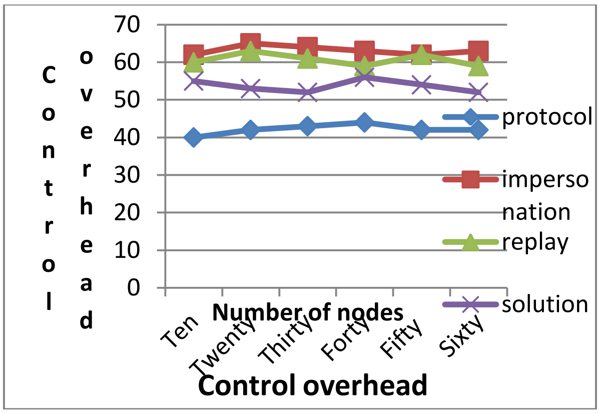

Fig 9: Control overhead

7.4 Total overhead

Total overhead can be defined as the total number of routing (control) packets that have been transmitted at time t by the nodes in the network. The total overhead in the network is determined for varying number of nodes and the graph is generated as shown below. The overhead increases with the presence of malicious nodes. With the implementation of the solution, it is reduced by **12%** with respect to both the total overhead in the presence of the attacks.

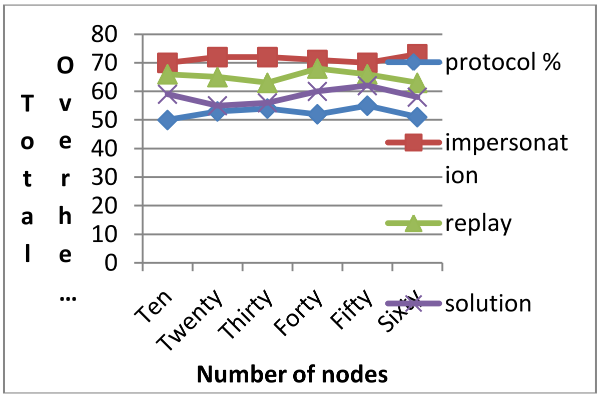

Fig 10: Total overhead

Thus the efficiency of the solution is has been analyzed using the four metrics. The solution shows an increase in the performance of the protocol.

8. CONCLUSION

The nodes in the MANETs are dynamically without any infrastructure or pre-configuration. So a base station or access point. MANETs can be deployed and operated without depending on a fixed backbone. However, their features of open medium, absence of infrastructure, dynamic changing network topology, cooperative algorithms, lack of centralized monitoring and management point, resource constraints and lack of a clear line of defense, which make MANET vulnerable to many kinds of security attacks. Therefore, there is a major concern about their security.

Among the various security issues in MANETs, an analysis is made on the attack and flees mechanism in SPBM protocol and a solution has been stated for the same. The key feature of this protocol is the lack of distribution structure like a tree or mesh. The packets are forwarded to the node which is closest to the destination based on the position of the nodes in the network. The position is determined using Global Positioning system. This protocol divides the network into squares, and the members belonging to the same square are stored in the neighbor table. Routing between the nodes in the same square is easier when compared to routing between nodes belonging to different squares. The attack and flee mechanism enables the malicious nodes to cause damage to the network repeatedly by fleeing from the multicast group after causing enough damage to the network. The node can re-join the network with fresh trust values and thus cause repeated damage without being caught.

The performance of the solution has been studied using metrics such as packet delivery ratio, delay, control overhead and total overhead. The protocol's performance is reduced in the presence of attackers and the performance is better after the implementation of the solution. This solution can be applied for any type of attack and for any protocol. Prediction of the fleeing node can be done using game theoretic approach. A Bayesian-Nash game can be simulated between the neighboring nodes in the network and preventive measures can be applied before the node flees from the multicast group. Also other tree formation algorithm can be used as LSG does not perform well when the location information is outdated due to its computational complexity.

9. REFERENCES

[1] Luo Junhai, Ye Danxia, Xue Liu, and Fan Mingyu, "A Survey of Multicast Routing Protocols for Mobile Ad-Hoc Networks", In the proceedings of IEEE Communications Surveys & Tutorials, Vol. 11, No. 1, pp.78-9, ISSN : 1553-877X, March 2009.

[2] N.Shanthi, L.Ganesan And K.Ramar, "Study Of Different Attacks On Multicast Mobile Ad Hoc Network, Journal of Theoretical and Applied Information Technology", Vol.9 No.2, pp. 45-51, 2005.

[3] Martin Mauve, Holger Fubler, J¨org Widmer and Thomas Lang, "Position-Based Multicast Routing for Mobile Ad-Hoc Networks" In the proceedings of ACM SIGMOBILE Mobile Computing and Communications, Vol.7 No.3, pp.53-55, DOI: 0.1145/961268.961288, 2003.

[4] Chen.K and Nahrstedt.K ,"Effective location-guided tree construction algorithms for small group multicast in MANET", Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies

[5] Feng Li, Yinying Yang, Jie Wu,"Attack and Flee: Game-Theory-Based Analysis on Interactions Among Nodes in MANETs", In the proceedings of IEEE transactions on systems, man, and cybernetics part b: cybernetics, vol. 40, no. 3, ISSN : 1083-4419, June 2010