Weeding Wormhole Attack in MANET Multicast Routing using Two Novel Techniques - LP^3 and NAWA^2

S.Vijayalakshmi
Department of Computer Applications
IFET College of Engineering,
Anna University, Chennai,
Tamilnadu, India.

S.Albert Rabara
Department of Computer Science
St.Joseph's College
Bharathidasan University, Trichy,
Tamilnadu, India

ABSTRACT
Mobile Adhoc Network (MANET) with its unique and special characteristics is prone to a host of security threats from within and outside the network. The MANET architecture is well suited for conducting multicast communications as this greatly reduces the number of multicast packets traversing the network. The replication of multicast packets by the intermediate downstream multicast router is demand based and is determined by the number of fresh receivers in the group. This greatly paves way for network resource optimization and a good trail of performance parameters like MPDR, Throughput, Jitter and End-to-End Delay. It is literally bogging down to construe a localized MANET as a single flat larger group. So the concept of orchestrating hierarchical group architecture within MANET dawned which led to the definition of Iolus framework. The hierarchical secure multicast distribution tree created within MANET backed by Iolus framework is prone to a array of attacks. One such prominent insider attack is wormhole attack where the two colluding adversaries conspire to short-circuit the flow of packets to a foreign network through an out-of-band high bandwidth link. The implication of this attack in unicast routing of MANET is less pronounced due to the limited number of participating entities. But this attack has a large telling effect on multicast routing as it involves multiple receivers and numerous intermediate multicast routers. The possibility of compromising the internal group node as a wormhole colluding agent is more common in multicast than in unicast. This threat marks an unprecedented intensity by divulging more faction of data thereby rendering the remedial process a huge flop. The real intent of the attacker is not to disrupt the multicast communication but in abetting the mass divulgence of multicast data to unauthorized group members. Two novel solutions viz., Limiting Packet Propagation Parameter (LP^3) and Neighbor Aware Wormhole Adversary Axing (NAWA^2) has been proposed to counter this menace.

***Keywords*: Rushing attack, Iolus framework, Multicast communication, RIMR, ROMR.**

1. INTRODUCTION

A mobile ad hoc network is a self – organizing system of mobile nodes that communicate with each other via wireless links with no infrastructure or centralized administration such as base stations or access points. A node in a MANET operates both as hosts as well as routers to forward packets to each other. MANETS are suitable for applications such as military, emergency rescue and mining operations. In these applications, communication and collaboration among a given group of nodes are necessary. Instead of using multiple unicast transmissions, it is advantageous to use multicast in order to save network bandwidth and other resources, since a single message can be delivered to multiple receivers simultaneously. Multicast routing protocols can be classified into two groups: tree based and mesh based. In a multicast routing tree, there is usually only one single path between a sender and a receiver, while in routing mesh, there may be multiple paths between sender – receiver pairs. Example of tree based multicast routing protocols are MAODV, AMRIS, BEMRP and ADMR. Typical mesh based multicast routing protocols are ODMRP, CAMP, DCMP and NSMP [1][11].

Among all the research issues, security is an essential requirement in ad hoc networks. Compared to wired networks, MANETS are more vulnerable to security attacks due to the lack of a trusted centralized authority, easy eaves dropping because of shared wireless medium, dynamic network topology, low bandwidth, battery power and memory constraints of the mobile devices. The security issue of MANETS in group communication is even more challenging because of multiple senders and multiple receivers. Security in multicast is thus considerably more complicated than in the unicast case. Most unicast solutions are prohibitively inefficient for multicast scenarios. Factors affecting security [10] are group type, group size, member (node) characteristics (power, storage, availability), membership dynamics, membership control, number and type of senders, volume and type of traffic and routing algorithm used. Attacks on routing mechanisms are becoming widespread. Thus multicast security is a fairly complex multi-faceted, multi-layered problem.

These requirements are even more difficult to fulfil in ad hoc networks where bandwidth, storage and energy constraints of the nodes pose additional problems when coupled with mobility and dynamically changing topology in the absence of a centralized infrastructure. Several types of security attack in MANETS have been studied in the literature, and the focus of earlier research is on unicast applications. The impacts of security attacks on multicast in ad hoc networks have not yet been solved. This paper highlights the impact of wormhole attack on multicast routing in MANET.

The rest of the paper is organized as follows. **Section 2** presents a holistic approach to multicast communication. In **Section 3**, we provide reviews about the wormhole attack and the repercussion on multicast routing in MANET. **Section 4** highlights the existing and proposed solutions to combat wormhole attack in MANET. **Section 5** presents the results and discussions of the study using NS graphs. Finally, we make some conclusions and future direction in **Section 6**.

2. INTRODUCTION TO MULTICAST COMMUNICATION

2.1 Introduction

The increasing diffusion of one-to-many and many-to-many network services such as stock market applications, news distribution, video conferencing, software updates distribution, video on demand, tele-medicine, has lead to the design and implementation of new communication primitives that make a more efficient use of the network resources. The multicast primitive is now available in several commercial implementations of the TCP/IP stack and many different protocols have been proposed by the computer network community. Multicast is an internet work service that provides efficient delivery of data from a source to a group of recipients. Multicast transmission can reduce the network load since a single packet transferred by the source is replicated and forwarded to the desired group of host receivers while minimizing the number of copies of the packet that traverses the network. It reduces the sender's transmission overhead, the network bandwidth usage, and the latency observed by receivers. The set of principals sending and/or receiving data on a particular multicast channel is called a multicast group.

The traditional mechanism used to support multicast communication is IP multicast. In IPv4, the class D addresses (ranging from 224.0.0.0 through 239.255.255.255) are reserved for multicast communication [2]. Multicast-enabled hosts and routers participate in the Internet Group Management Protocol (IGMP) to manage and control the group formation, modification and termination. Multicast-enabled routers also participate in one or more multicast routing protocols. Deployment of multicast technology in MANET reduces the overhead of unwanted transmission of duplicate packets as the replication is purely receiver based and is enough if one packet travels which eases the resource constrained internet thereby ensuring optimal usage of network bandwidth. Here, the bandwidth for one receiver is equal to bandwidth for all receivers.

The security constraints experienced by MANET is severely accentuated while deploying multicast communication. Iolus framework, which insist in the creation of secure distribution tree for multicast group employ Group Security Agents (GSA) like Group Security Intermediaries (GSI) and Group Security Controller (GSC) for effective coordination of the group [12]. The compromise of GSAs by the Byzantine attack can cause severe implications. The GSI in charge of a subgroup serves two purposes:

- Mediate all communication between its subgroup and other subgroups
- Manage its subgroup's keys.

2.2 Security Requirements of Multicast Communication

The wedding of multicast with MANET senses a surge in security incidents which propels to provide a defense in depth solution to thwart the attacks faced by this duo. A Synergetic and strategic security approach is required to circumvent the threats stemming out of this knot. The multicast communication over MANET should not only satisfy the basic security requirements like Confidentiality, Authentication, Non Repudiation, and Integrity but also advanced security requirements.

• ***Limiting members:*** Controlling who can be a member of the multicast group as well as who can send data to the group and who can receive data sent to the group.
• ***Revoking membership:*** Offering a mechanism to expel a member from a group and preventing this member from joining the group again.
• ***Data secrecy:*** Preventing any outsiders (i.e., non group-members) from accessing the data sent to the multicast group.
• ***Sender and data authentication:*** Providing a mechanism to members for ensuring that the data originated from an authorized sender and has not been modified on the way.
• ***Member privacy:*** Preventing outsiders and other members, from knowing the identities of the current members.
• ***GAC (Group Access Control)****:* Checks whether group access is by authorized and authenticated group members.
• ***GKM (Group key Management)****:* Ensures that the group key is periodically refreshed and kept updated to prevent the old members from accessing the future communication (Forward secrecy) and new members from interpreting the past data (Backward Secrecy) using Internet Security Association Key Management Protocol (ISAKMP) [3] and Internet Key Exchange (IKE) protocol.

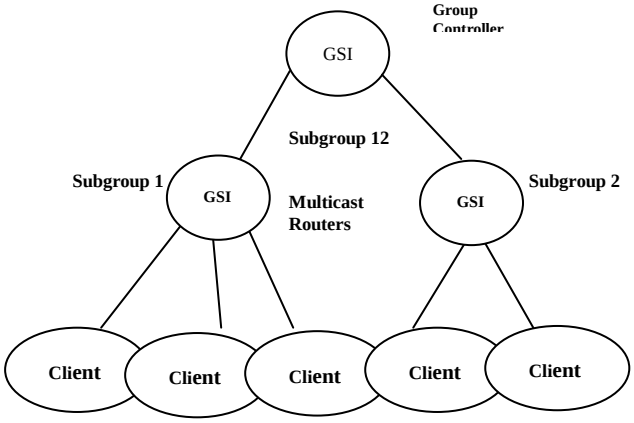


Figure 1: Iolus Framework

These services typically require the establishment of a security association between the source and the recipients of the multicast channel. The security association defines the set of cryptographic keys and algorithms used for each service. The establishment of a security association for a multicast channel is inherently more complex than with unicast. In the unicast case, a security association is static in that the source, the recipient, and the dataflow do not vary during the association. In a dynamic multicast group, session are ever-evolving entities as recipients can be added to or removed from the group through join and leave operations, respectively. Therefore, an efficient re-keying mechanism is mandatory to ensure a robust multicast system. Rekeying is defined as the process by which the Keying material must change each time the set of users in a multicast group changes [4]. The group key must be revoked and redistributed to all the remaining nodes in a secure, reliable, and timely fashion whenever there is change in group membership status [13].

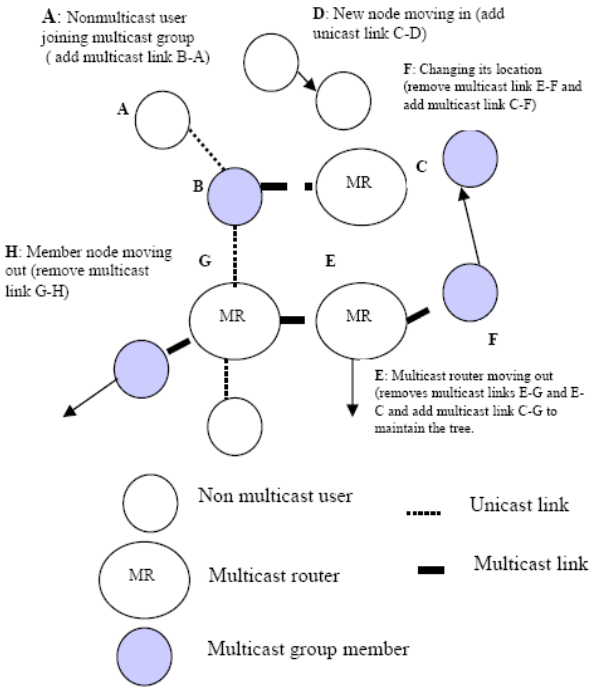


Figure 2: Multicast Routing in MANET

3. A GENTLE INTRODUCTION TO WORMHOLE ATTACK

A wormhole attack typically requires the presence of at least two colluding nodes in an ad hoc network. The malicious nodes need to be geographically separated in order for the attack to be effective. In this attack, a malicious node captures packets from one location and "tunnels" these packets to the other malicious node, which is assumed to be located at some distance. The second malicious node is then expected to replay the "tunneled" packets locally. There are several ways in which this tunnel can be established. We consider two possible methods below [5].

3.1 Types of Wormhole Attack

In the first method for establishing the tunnel shown in Figure 4, a malicious node denoted X in the figure, encapsulates a packet received from its neighboring node A. Node X then sends the encapsulated packet to the colluding malicious node Y. Node Y then replays the packet in its neighborhood after decapsulating the packet. Thus, the original packet transmitted by node A in its neighborhood is replayed by node Y in its neighborhood, which includes node B. For example, if the original packet transmitted by node A (and tunneled by node X) was a hello packet, then node B on receiving this packet would assume that node A is its neighbor, which is not true. As another example, if node A transmits a route request packet for node B, then node X can "tunnel" such a packet to node Y by encapsulating the packet. As a result, this route request packet will arrive at the destination node B with a lower hop count than the other Route Request packet going through the other route. This happens in spite of using any secure routing protocol such as the ones given earlier. Note that nodes between X and Y that relay the packet cannot interpret the packet as it is encapsulated. Therefore, they cannot increment the hop count.

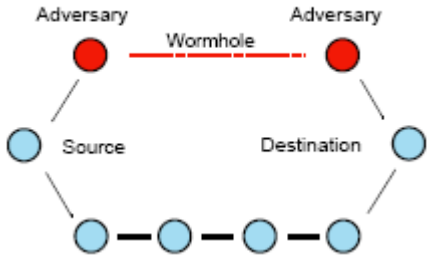


Figure 3: Simple Wormhole Configuration

In the second method for establishing the tunnel shown in Figure 5, the two malicious nodes X and Y are assumed to have access to an out-of-band high bandwidth channel. This could be achieved for example by having a wired link between the two nodes or by having a long range high bandwidth wireless link operating at a different frequency. Thus, this method requires specialized hardware capability and hence is more difficult than the previous method. In this case also, a hello packet transmitted by node A can be retransmitted in the vicinity of node B. As a result node B infers that node A is its neighbor. Similarly, a route request packet, from node A for node B, can also reach node B (which is the destination for the route request packets) faster and possibly with fewer hops, since a high-bandwidth direct link is being used between the two malicious nodes [14]. As a result, the two endpoints of the tunnel can appear to be very close to each other. To see this, consider Figure 5. Here node B receives three route requests. It is clear that the route request received through the wormhole will have the least hops.

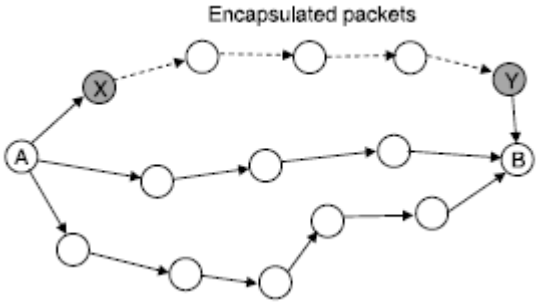


Figure 4: Wormhole Attack (Encapsulated Packet)

It seems as if the malicious nodes are performing a useful service by tunneling the packets. This would be so if the nodes were performing this service without any malicious intent, but malicious nodes could use this attack to undermine the correct operation of various protocols in ad hoc networks. The most important protocol that is impacted is the routing protocol, as we can see from the examples given earlier. Data aggregations, protocols that depend on location information, data delivery, and so on, are some other examples of services that can be impacted. Note that the wormhole attack can be successful even without access to any cryptographic material on the nodes [6][7].

3.2 Security Challenges of Wormhole Attack in MANET

As MANETs are unwired network with dynamic topology associated with them, they are vulnerable to a series of attacks. In protocol stack, Physical layer has security issues like Denial of Service (DoS) attacks and preventing signal jamming. Network layer has to deal with security of ad-hoc routing protocol and

related parameters. Transport layer has issues with end to end data security with encryption methods and Authentication. Application layer has security concerns with prevention, worms, malicious codes, application abuses as well as virus detection. There can be two kinds of attacks: passive and active. A passive attack does not disturb the normal network operation while an active attack does it. In passive attack, attacker sneaks data without altering it. Passive attacks are difficult to detect as there is no change in the functionality of the network. Active attacks can be internal or external. Internal attacks are carried out by nodes within the network while external attacks are carried out by nodes outside the network. Modification, Impersonation and Fabrication are some of the most common attacks that cause a big security concern for MANET. Wormhole attack is perpetuated by adopting fabrication technique.

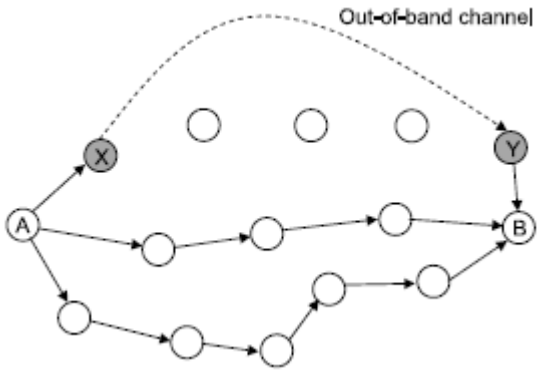


Figure 5: Wormhole Attack (Out of Band channel)

Providing security cover for a multicast group prevailing on a MANET throws open interesting and intriguing challenges. One such attack is wormhole attack whose modality is to short-circuit the normal multicast traffic to an external entity through high profile tunnel being orchestrated by the colluding insiders. This is in fact using the network against itself. The security issue of MANETS in group communication is even more challenging because of multiple senders and multiple receivers. The wormhole attack in unicast is simple and less tricky as it involves only a single sender and a receiver.

The repercussion caused due to wormhole attack in multicast routing is a challenging phenomenon as it is backed by multiple intermediate multicast routers along with the sender and receivers. The secure multicast distribution tree is at stake as the colluding wormhole adversaries jeopardize the multicast services rendered to the downstream nodes thus leading to unnecessary network partition and pruning. There is an equal possibility for the subversion of group member and group head by the wormhole adversary. The impact caused by the wormhole adversary on the group member is docile than the impact on group head. Mitigating the wormhole impact in group member becomes manageable as the group head periodically monitoring the group activities grew suspicious about a node which is not complying with the routing protocol specification and eventually strips it off the status.

The repercussion caused by the subversion of group head has a massive telling effect on the network performance as it permits the voluntary disclosure of group activities and information to external entities. The wormhole infected group head mars the inter group and intra group communication. The pruning of group head is more complex because the associated group members have to be reassigned to a genuine group head availing the group service causing multicast tree reconfiguration [15].

4. A COMPREHENSIVE STUDY ON WORMHOLE ATTACK

4.1 Existing Solutions for Wormhole Attack

There have been some proposals recently to protect networks from wormhole attacks by detecting such attacks. The concept of leashes is introduced to detect wormhole attacks. A leash is any information added to a packet in order to restrict the distance that the packet is allowed to travel. A leash is associated with each hop. Thus, each transmission of a packet requires a new leash. Two types of leashes are considered, namely geographical leashes and temporal leashes. A geographical leash is intended to limit the distance between the transmitter and the receiver of a packet. A temporal leash provides an upper bound on the lifetime of a packet. As a result, the packet can only travel a limited distance. A receiver of the packet can use these leashes to check if the packet has traveled farther than the leash allows and if so can drop the packet.

Another approach for detecting wormhole attacks is deploying directional antennae. The approach here is based on the use of packet arrival direction to detect that packets are arriving from the proper neighbors. Such information is possible due to the use of directional antennae. This information about the direction of packet arrival is expected to lead to accurate information about the set of neighbors of a node. As a result, wormhole attacks can be detected since such attacks emanate from false neighbors [8].

To illustrate this idea consider Figure 6. Here two nodes, A and B are shown. The directional antenna with six zones explicitly for both nodes is depicted. Each node is assumed to have knowledge of the zone from where a packet is received. Given this, the basic idea that is used to determine the set of authentic neighbors is that, if a node is in a given direction of another node, then the latter node is in the opposite direction of the former node. For example, in Figure 6, node B is in zone 6 of node A while node A is in the opposite zone, which is zone 3 of node B. An implicit assumption here is that the directional antennae on the various nodes are perfectly aligned [9].

The authors present a graph theoretic framework for modeling the wormhole attack. They provide a necessary and sufficient condition that any solution to the wormhole problem needs to satisfy. In addition, the authors also propose the use of local broadcast keys whereby the keys in different geographic regions are different. As a result, an encrypted message replayed via the wormhole in a different location cannot be decrypted by the receivers in that region.

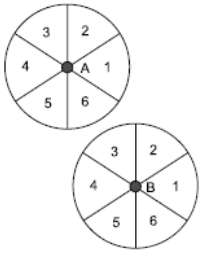


Figure 6: Zones on Directional Antenna

4.2 Simulation of an Attack Scenario

Figure 7 conceptualizes the wormhole attack model where the wormhole adversaries in the multicast distribution tree be it either the group member or group head conspiring to bypass the normal flow of multicast packets to a foreign network populated by a group of unauthorized members wishing to avail the group services through illegitimate way.

4.3 Two Novel Solutions Proposed to Combat Wormhole Attack

4.3.1 Limiting Packet Propagation Parameter (LP^3)

There are host of security antidote/solutions available for a node to recover from the wormhole impact which has been discussed in section 3. Another novel technique proposed is Limiting Packet Propagation Parameter (LP^3) which is embedded with the multicast packet just like Time to Live (TTL) field. This field is a once assigned random value which will constrain the endless outward journey of the multicast packet through the sophisticated resource enriched out of band tunnel. The expiry of this field value entails the dissolvance of the packet. This field value is designed/calibrated in such a way that it safely reaches the destination before its expiry. If the packet is taking an excessive network trip then the LP^3 value diminishes to zero culminating in cessation of packets. The possibility of an attacker cracking this field is ruled out as it is encrypted/digitally signed by the sender. Although this added attribute/field results in increase of packet size and length it is of paramount importance to curtail the occurrence of wormhole attack. This attribute also imposes a performance penalty as it incurs more overhead for the field processing at every hop.

The prime target of the wormhole attack is multicast routing protocol. An optimal multicast route is selected in the absence of a wormhole attack after ascertaining the round trip propagation delay and time, number of intermediate node between the multicast sender and receiver. The wormhole adversary after acquiring its potential position and status in multicast routing in MANET issues a bogus route advertisement with promising hop count value, round trip propagation delay and time factor. The multicast sender instead of blindly accepting the dubious offer forwards a multicast trace route test packet to confirm the existence of a valid multicast route through MANET. This technique attributes a bleak chance for multicast sender falling gullible to the wormhole adversary.

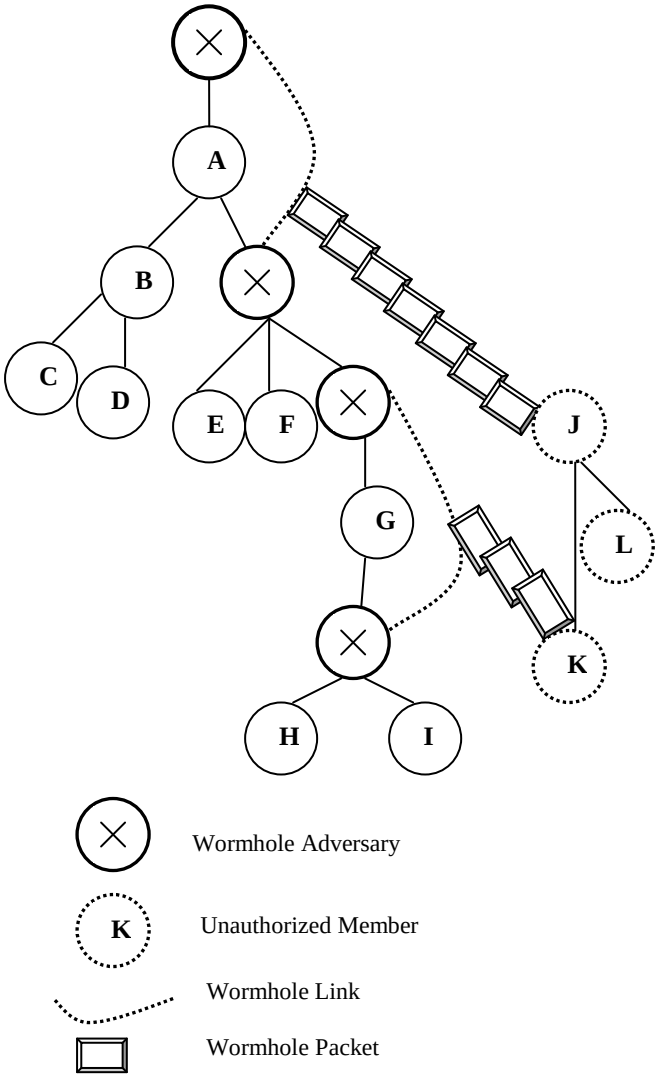


Figure 7: Simulated Wormhole Attack Model

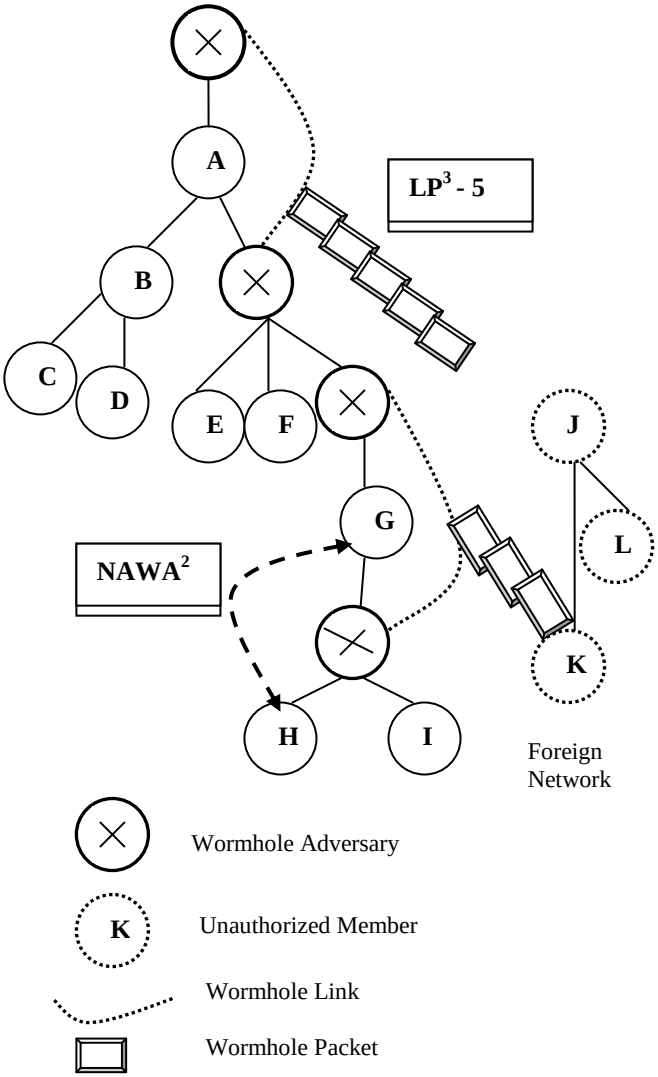


Figure 8: Adoption of Solution Technique

4.3.2 Neighbor Aware Wormhole Adversary Axing (NAWA^2)

The colluding wormhole adversaries enjoy a hassle free attack spree until spotted by the genuine multicast neighbors. The two genuine multicast neighbors of the wormhole adversary sense a surge in deterioration of multicast performance metric like Multicast Packet Delivery Ratio (MPDR) and jitter. These two legitimate suspicious neighbors join hand in unison to spot the culprit node and its colluder and assist in appending them to the Node Conviction List (NCL). This genuine multicast neighbor to neighbor interaction message prevailing near the attack infected zone and their relentless coordination helps to dismantle the conspiracy hatched between the two colluding wormhole attackers. This method is resilient to false positive reports/falsified/fabricated reports since in MANET each node is constantly under the scanning, monitoring and inspection of its neighbor. Even if the immediate neighbor tries to safeguard the colluding wormhole attackers it is instantly handcuffed by their genuine neighbors who act as watchdog overhearing their neighbor's transmission. This deliberation has led to the definition of a novel technique by name Neighbor Aware Wormhole Adversary Axing (NAWA^2).

This technique helps to instantly prune the misbehaving wormhole perpetuators culminating in cordoning off the attack infected zone. The mapping of attack infected zone by the genuine neighbors assist the multicast group members in choosing a non adversarial multicast route to securely forward the packets to its destination. Figure 8 depicts the adoption of two novel techniques like LP^3 and NAWA^2 in the wormhole infected MANET Multicast distribution tree. Figure 9 registers the reaction of the solution techniques in arresting the wormhole adversaries and appending them to NCL.

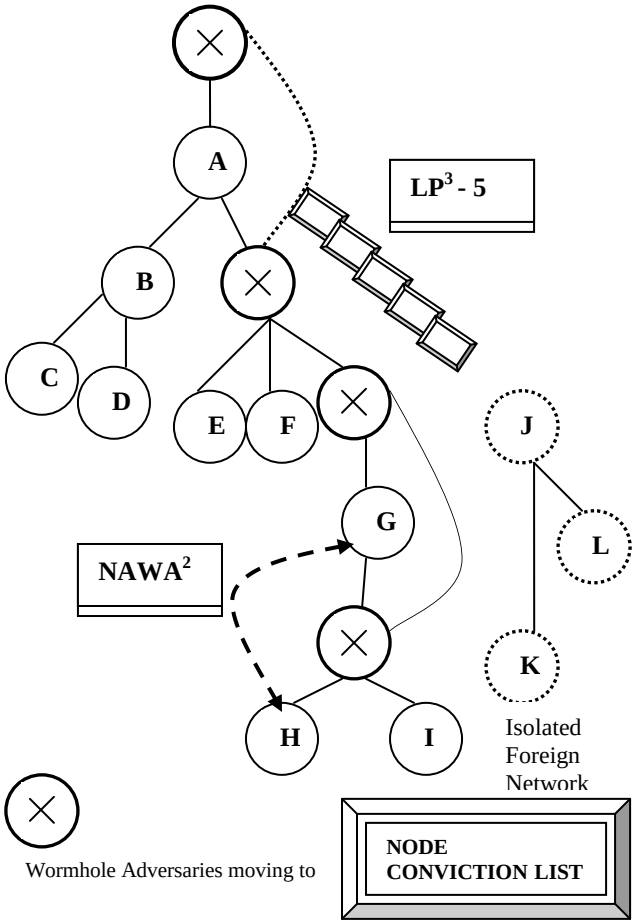
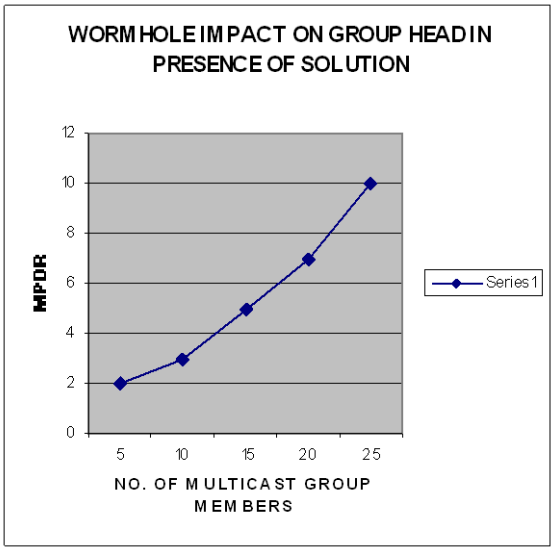


Figure 9: Wormhole Adversaries Appended to NCL

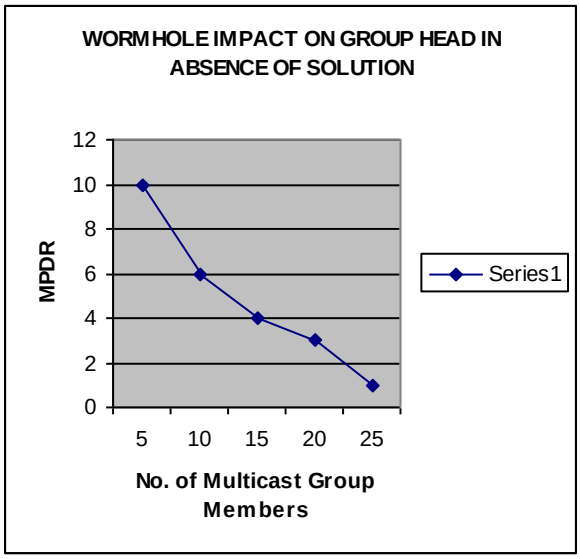
5. RESULTS AND DISCUSSION

Various graphs have been simulated using Network Simulator to study the impact of this attack on Multicast Packet Delivery Ratio (MPDR) with the presence and absence of the proposed solution technique. The implication stemming from the compromise of the group member by the wormhole adversary is less severe than the group head. The colluding nature exhibited in group head mars the inter group communication and in group member mars the intra group communication. The off-shoot of the group head falling prey to wormhole attacker senses a deflation in MPDR values in the absence of these two novel techniques. The attack intensity and magnitude is less pronounced in the colluding context of group member as it is continuously and consistently monitored by the genuine group head which constrain the plummeting nature of MPDR values. With the deployment of these two techniques in the wormhole infected zone one can realize the spiralling nature of MPDR values in both scenarios (Group head and Group member).

Graph 1 and 3 portrays the impact of wormhole attack on multicast group head and group member in the presence of these two novel techniques. These graphs show a steady increase in the MPDR values with the attack counter strategy proposed by these two techniques. Graphs 2 and 4 depict the impact of wormhole attack on multicast group head and group members in the absence of these two techniques. These graphs highlights a steady fall in the MPDR values due to the flippant nature of the network not complying with these proposed robust solutions.



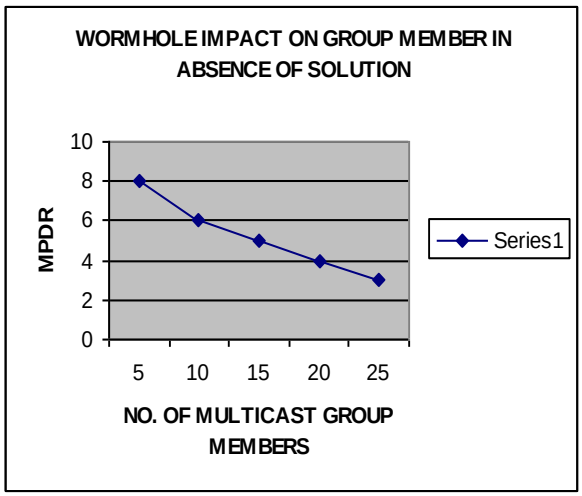
Graph 1: Wormhole Impact on Group Head in Presence of Solution.



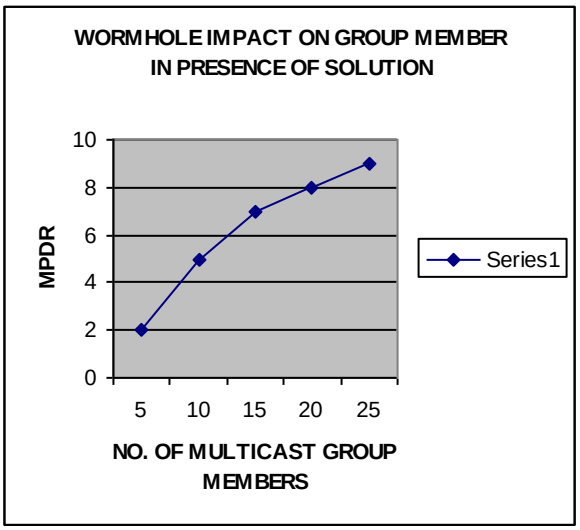
Graph 2: Wormhole Impact on Group Head in Absence of Solution.

6. CONCLUSION

Despite the ample vulnerabilities associated with the MANET group communication the proposal for modeling stringent security architecture becomes a daunting task. MANET with its intriguing characteristics invites a host of security threats which has to be countered effectively. The wormhole attack is one such attack where the compromised insider colludes with an outside wormhole adversary to bypass the normal flow of packets to a foreign network through an out-of-band enriched tunnel exclusively dedicated for this purpose. The attack perpetuated on multicast communication has a substantial effect than the unicast communication as the cardinality of participating entities is of lower degree than the former. This paper strongly recommends the induction of two novel techniques viz. Limiting Packet Propagation Parameter (LP^3) and Neighbor Aware Wormhole Adversary Axing ($NAWA^2$) which sustainably maintains the network performance parameter like Multicast Packet Delivery Ratio (MPDR) at a constant level despite the severity of the attack. Various graphs are simulated to highlight the significance of the proposed solutions on MPDR.



Graph 3: Wormhole Impact on Group Member in Absence of Solution.



Graph 4: Wormhole Impact on Group Member in Presence of Solution.

7. REFERENCES

[1] V.Varadharajan, R.Shankaran and M.Hitchens, "Security for Cluster Based Ad hoc Networks", Elsevier Computerscience.com, Computer Communications, October 2003.

[2] T.Ballardie, J.Crowcroft, "Multicast-Specific Security Threats and CounterMeasures".

[3] C.M.MCorderio, H.Gossain, D.P.Agarwal, "Multicast Over Wireless Mobile Adhoc Networks: Present and Future Directions", IEEE Network, January/February 2003.

[4] S.Xu., and V.B. Boppana, " On Mitigating In-band Wormhole Attacks in Mobile Adhoc Networks", ICC, IEEE Communications Society 2007.

[5] J.D.Parmar., A.D.Patel., R.H.Jhaveri and B.I.Shah., " MANET Routing Protocols and Wormhole Attack against AODV", International Journal of Computer Science & Network Security, Vol.10, No. 4, April 2010.

[6] N.Shanti., L.Ganesan and K.Ramar., "Study of Different Attacks on Multicast MANET", Journal of Theoretical and Applied Information Technology, 2005-09.

[7] F.Anjum and P.Mouchtaris., "Security for Wireless Adhoc Networks", Wiley Interscience, A. Johnwiley & Sons, Inc., Publication 2008.

[8] D.Brushi and E.Rosti., "Secure Multicast in Wireless Networks of Mobile Hosts: Protocols and Issues", Milano, Italy, 2009.

[9] Roy S., Addada V.G., Setia S. and Jajodia S., "Securing MAODV: Attacks and Countermeasures", Centre for Secure Information Systems, George Mason University, Fairfax, VA 22030.

[10] Mohapatra, P., Gui, C., and Li, J., "Group Communications in Mobile Ad Hoc Networks", University of California, Davis.

[11] Awerbuch, B., Holmer, D., Rotaru, C.N., and Rubens, H., "An On-Demand Secure Routing Protocol resilient to Byzantine Failures", Dept. of Computer Science, Johns Hopkins University, Baltimore MD 21218 USA.

[12] Athanasiou, G., Tassiulas, L., and Yovanof, G.S., "Overcoming Misbehavior in Mobile Ad Hoc Networks: An Overview".

[13] Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L., "Security in Mobile Ad Hoc Networks: Challenges and Solutions", UCLA Computer Science Department.

[14] Marti, S., Giuli, T.J., Lai, K., and Baker, M., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Department of Computer Science, Stanford University.

[15] Nguyen, H.L. and Nguyen, U.T., "A Study on Different Types of Attacks on Multicast in Mobile Ad hoc Network", Adhoc Networks 6(2008) pages 32-46.

AUTHOR BIOGRAPHIES

VIJAYALAKSHMI.S is Lecturer of Computer science, Dept. of MCA, IFET College of Engineering, Villupuram, Anna University. She is a Ph.D candidate currently doing research work on security in ad hoc networks. She holds M.C.A degree from SR College, Bharathidasan University, Trichirapalli and M.Phil degree from Alagappa University, Karaikudi. She has a teaching experience of 6 years in the field of Computer Science. She has authored 10 research papers which are published in refereed national and international journals and conferences.

Dr.S.ALBERT RABARA is working as an Associate Professor in the Dept. of Computer Science, St.Joseph's College (Autonomous), (Bharathidasan University) Tiruchirappalli. He obtained his Ph.D Degree in Computer Science from Bharathidasan University. An expert in the field of Information and Communication Technology and Security, he is a consultant for several colleges in Tamil Nadu. He has 22 years of teaching and research experience and guided four Ph.D Scholars. Published more than 40 papers in Journals, International and National Conference Proceedings, his research contribution is significant in IEEE, ACM and springer science publications and DBLP library catalogues. He is a member of editorial board of several International Journals.