BYZANTINE BEHAVIOUR (B^2) – MITIGATING MIDWAY MULTICAST MISBEHAVIOUR (M^4) IN ADHOC NETWORK

S. Albert Raebra[1] and S.Vijayalakshmi[2]

[1]Department of Computer Science, St.Joseph's College, Bharathidasan University,
Trichy, a_rabara@yahoo.com
[2]Department of Banking Technology, Pondicherry University, Pondicherry
anviji_lakshmi@yahoo.co.in

ABSTRACT

Ad-hoc networks are an emerging area of mobile computing and an efficient paradigm for multicast communication. The security challenges faced by the network due to their inherent unique characteristics are exacerbated in case of multicast communication. Group communication in ad hoc network is susceptible to a host of outsider and insider attacks. The security solutions proposed for the outsider attack cannot be directly applied to the insider attack due to their disparate behavior. The compromise and subversion of the authenticated, trusted and participating node in the network leads to Byzantine attack or behavior. Attacks where adversaries have full control of a number of authenticated devices and behave arbitrarily to disrupt the multicast routing are referred to as Byzantine attacks. Online auction network inherently embracing multicast technology has been taken as the case study. The implications of the Byzantine attack in the online auction Network have been studied. Besides the existing network performance parameters like delay, jitter, throughput, Packet Delivery Ratio (PDR) another parameter by name Immediate Neighbor Aware Vouch Count (INAVC) is included to proactively select a fault free multicast route. This proactive parameter is dynamic and reflects the true multicast architecture in adhoc network thereby enabling to instantly prune the Byzantine adversary. Providing robust and resilient defense solutions to subvert this attack in auction Network becomes the focus of this paper.

KEYWORDS

Ad-hoc networks, Multicast Communication, Byzantine Behavior, Online Auction Network

1. INTRODUCTION

Many important applications for ad hoc networks are group oriented in nature, and can therefore benefit from a multicast communication service. Example applications include mobile conferencing, battlefield communications, and disaster recovery operations. Ad hoc networks are composed of autonomous nodes that are independent of any fixed infrastructure. Mobile ad hoc networks (MANET) have a fully decentralized topology and they are dynamically changing. Besides these challenges, the wireless transmission medium introduces limitations in communication. Efficient support of group communications is critical for most ad hoc network applications. However, MANET group communications issues differ from those in wired environments for the following reasons: The wireless communications medium has variable and unpredictable characteristics and the signal strength and propagation fluctuate with respect to time and environment. Further, node mobility creates a continuously changing communication topology in which routing paths break and new ones form dynamically. Because MANET has

DOI : 10.5121/ijnsa.2010.2308

limited bandwidth availability and battery power, their algorithms and protocols must conserve both bandwidth and energy [1].

Many multicast routing protocols that support group-oriented communication have been described in the literature. These protocols assume a trusted, non adversarial environment and their design do not take security issues into account. Nodes that can not be authenticated do not participate in the multicast routing protocol, and are not trusted. Any intermediate node on the path between the source and destination can be authenticated and can participate in the routing protocol but the authenticated node may exhibit byzantine behaviour [2]. The Byzantine behavior is defined as any arbitrary action by an authenticated node that results in disruption or degradation of the routing service and such an adversary is called a Byzantine adversary.

An intermediate node can exhibit such routing misbehavior either alone or in collusion with other nodes. The routing protocol in MANET which encompasses all-node-as router idea assume that the nodes will fully participate. Unfortunately, node misbehavior is a common phenomenon. Misbehavior is due to selfish, malicious, overload or broken reasons. The Byzantine behavior culminates in scrambling of the auction services which leaves online trading community in lurch. Unlike networks using dedicated nodes to support basic functions like packet forwarding, routing, and network management, in ad hoc networks these functions are carried out by all available nodes. Unlike wired networks where an adversary must gain physical access to the network wires or pass through several lines of defense at firewalls and gateways, attacks on a wireless network can come from any direction and target all nodes. Therefore MANETs, do not have a clear line of defense, and every node must be prepared for encounters with an adversary directly or indirectly [3].

In MANETs, nodes are receptive to being captured, compromised, and hijacked since they are units capable of roaming independently. Attacks by compromised nodes are far more damaging and much harder to detect. Furthermore, the lack of a centralized authority gives ground to adversaries to exploit new types of attacks. This research paper aims at analyzing the impact of Byzantine attack posed on online auction and highlighting various mitigation strategies to thwart this attack. Online auction has been taken as the case study since it inherently advocates secure group multicast communication [4][5].

The rest of the paper is organized as follows. **Section 2** surveys the security challenges of Byzantine behavior in multicast routing in ad hoc network. In **Section 3**, we present the Ebay Online auction application and discuss the implications and impact of the Byzantine behavior in this network. **Section 4** suggests possible robust and resilient defense solutions to circumvent this menace. Simulated Graphs highlighting the impact in multicast performance metrics are discussed in **Section 5**. Finally, we make some conclusions and future direction in **Section 6.**

2. RELATED WORKS

Awerbuch, B. et al [3] implements On-Demand Secure Byzantine Routing Protocol (ODSBRP) to handle some Byzantine Behaviors such as Flood Rushing Attack, Byzantine Wormhole attack, Black hole etc. and to analyze their mechanisms and to describe the major mitigation techniques. Through simulation, they perform a quantitative evaluation of the impact of these attacks on an insecure on-demand routing protocol. The relative strength of the attacks is analyzed in terms of the magnitude of disruption caused per adversary.

Awerbuch, B. et al [6] propose an on-demand routing protocol for ad hoc wireless network that provides resilience to byzantine failures caused by individual or colluding nodes. Their adaptive probing technique detects a malicious link after log *n* faults have occurred, where *n* is the length of the path. These links are then avoided by multiplicatively increasing their weights and by using an on-demand route discovery protocol that finds a least weight path to the destination.

Curtmola, R. et al [7] propose Byzantine Resilient Secure Multicast Routing (BSMR), a novel secure multicast routing protocol that withstands insider attacks from colluding adversaries. This protocol is a software-based solution and does not require additional or specialized hardware.

Lin, X. et al [15] tries to solve the problem from a different perspective by targeting the node compromise revocation, i.e., isolating and breaking off the misbehaving nodes. To mitigate the security breaches from internal compromised nodes and eventually eliminate compromised nodes from the wireless ad hoc networks, they propose an energy efficient malicious node removal mechanism.

Tan, H. et al [16] propose a novel Network Protocol to address the imperative issues that have been ignored in existing literature. The scalability evaluation of the network protocol through the simulation in NS2 is also presented. The complete analytical model behind the design is also projected.

Sathyamoorthy, E. et al [18] aimed at the stipulations which arise in the traditional online auctions as a result of various anomalies in the reputation and trust calculation mechanism. They try to improve the scalability and efficiency of the online auctions by providing efficient trust management methodology considering several factors into consideration. A comparison between the performance of the auctions system with and without the agent methodology is done with good results.

2. SECURITY CHALLENGES OF BYZANTINE BEHAVIOR IN MULTICAST ROUTING

Security in Mobile Ad Hoc Network (MANET) has attracted growing interest in recent years. An ad hoc wireless network is an autonomous self-organizing system of mobile nodes connected by wireless links where nodes not in direct range can communicate via intermediate nodes. A common technique used in routing protocols for ad hoc wireless networks is to establish the routing paths on demand, as opposed to continually maintaining a complete routing table. A significant concern in routing is the ability to function in the presence of byzantine failures which include nodes that drop, modify, or mis-route packets in an attempt to disrupt the routing service.

2.1. Introduction to Multicast Communication

Multicasting is a point to multipoint communication mechanism in which the source forwards the traffic to a group of host receivers. 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. The recent growth of the World Wide Web has sparked new research into using the Internet for novel types of group communication, like multiparty videoconferencing, distance learning, distribution of software upgrades/patches and real-time push-based information delivery systems such as stock quote services. The set of principals sending and/or receiving data on a particular multicast channel is called a multicast group [6].

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. Multicast-enabled hosts and routers participate in the Internet Group

Management Protocol (IGMP) [l] to manage and control the group formation, modification and termination. Multicast-enabled routers also participate in one or more multicast routing protocols like DVMRP, MOSPF, PIM and MAODV. 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 [7][8]. 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.

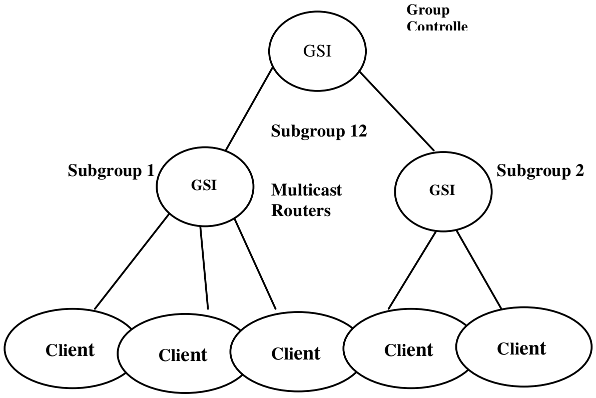


Figure 1. Iolus Framework

2.2. Byzantine Behavior

Multicast routing protocols deliver data from a source to multiple destinations organized in a multicast group. Several protocols were proposed to provide multicast services for multi-hop wireless networks. These protocols rely on node cooperation and use flooding, gossip, geographical position, or dissemination structures such as meshes, or trees. A major challenge in designing protocols for wireless networks is ensuring robustness to failures and resilience to attacks. Wireless networks provide a less robust communication than wired networks due to frequent broken links and a higher error rate. Security is also more challenging in multi-hop wireless networks because the open medium is more susceptible to outside attacks and the multi-hop communication makes services more vulnerable to insider attacks coming from compromised nodes[9][10]. Although an effective mechanism against outside attacks, authentication is not sufficient to protect against insider attacks because an adversary that compromised a node also gained access to the cryptographic keys stored on it. Insider attacks are also known as Byzantine attacks and protocols able to provide service in their presence are referred to as Byzantine resilient protocols.

In ad hoc networks, where mobile nodes communicate with each other through multi-hop wireless links, the corresponding routing and medium access control protocols were designed under the assumptions that all hosts would obey the protocols specifications. However, in such an open and dynamic environment, misbehaving hosts could compromise the network functionality by either attacking the physical layer, the MAC layer, or the network layer. Accordingly, these adversaries may have devastating effects on the performance of the network by degrading end-to-end throughput, increasing unfairness by starving multi-hop flows, indefinitely increasing delays, depleting channel capacity and preventing access to the wireless channel. The inherent feeble characteristic of the ad hoc group has simplified its surrender to the Byzantine threat trap [11].

Consider the case where a device or a set of devices could be compromised and be under the control of an adversary or set of adversaries that can collude. Once an adversary has control of an authenticated device, protocols which rely on authentication to provide security services become of little use. Authentication and data integrity mechanisms, although needed in order to prevent injection, fabrication and impersonation attacks, do not provide protection against insider attacks since they cannot force a node to behave according to the protocol. The adversary has full control of an authenticated device and exhibit arbitrary behavior to disrupt the system.

From a more general perspective, a Byzantine attack is any attack that involves the leaking of authentication cryptographic secrets so that an adversarial device is indistinguishable from a legitimate one. The security protections, however, break down when even a single legitimate node is compromised. It turns out to be relatively easy to compromise a legitimate node, which is to extract all the security information from the captured node and to make malicious code running for the attacker's purpose [12]

2.3. Considered Byzantine Attacks in Multicast Routing

Several Byzantine attacks in ad hoc multicast routing protocols have been proposed.

Black Hole Attack: A basic Byzantine attack is a black hole attack where the adversary stops forwarding data packets, but still participates in the routing protocol correctly. As a result, whenever the adversarial node is selected as part of a path by the routing protocol, it prevents communication on that path from taking place. Most existing secure and insecure routing protocols are disrupted by black hole attacks because they render the normal methods of route maintenance useless.

Gray Hole Attack: It is a special case of a black hole where an attacker could create a gray hole, in which it selectively drops some packets but not others, for example, forwarding routing packets but not data packets.

Flood Rushing Attack: A flood rushing attack exploits the flood duplicate suppression technique used by many routing protocols. This attack takes place during the propagation of a legitimate flood and can be seen as a "race" between the legitimate flood and the adversarial variant of it. If an adversary successfully reaches some of its neighbors with its own version of the flood packet before they receive a version through a legitimate route, then those nodes will ignore the legitimate version and will propagate the adversarial version. This may result in the continual inability to establish an adversarial-free route, even when authentication techniques are used.

Byzantine Wormhole Attack: This attack occurs when two adversaries cooperate to tunnel packets between each other in order to create a shortcut (or wormhole) in the network. Such a tunnel can be created by using a private communication channel (such as wired communication or a pair of radios and directional antennas), or by even using the existing ad hoc network infrastructure. Since the adversaries are using authenticated devices, they have complete access to use the ad hoc network. As a result, the adversaries can send a route request and discover a route across the ad hoc network. The adversaries can then tunnel packets through the non-adversarial nodes to execute the attack. This is in essence using the network against itself.

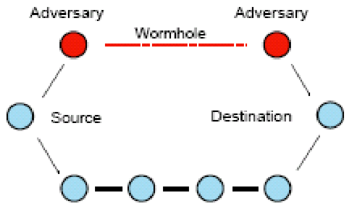


FIGURE 1 SIMPLE WORMHOLE CONFIGURATION

Apart from these listed attacks, other threats like Blackmail attack, N/w partition, Routing loop, detour, gratuitous detour, change in route selection metric has a substantial impact on the performance of the routing. Byzantine attack can manifest itself in routing disruption, resource consumption and packet dropping attack. An adversary can attack control messages corresponding to the route discovery, route activation and tree management components of the multicast routing protocol, or can attack data messages. The multicast route discovery can be disrupted by outside attackers by injecting, replaying, or modifying control packets. Malicious nodes that are not in the tree can mislead correct nodes into believing that they found and are connected to the tree. Nodes can flood the network with bogus requests for joining multicast groups. A Byzantine node can prevent a multicast route from being established by dropping the request and/or response, or can influence the route selection by using wireless specific attacks such as wormhole and flood rushing.

A Byzantine node can also modify the packets carrying the route selection metric such as hop count or node identifiers. Outsider nodes can inject bogus route activation messages, while Byzantine nodes can prevent correct route activation messages to reach correct nodes. Nodes can maliciously report that other links are broken or generate incorrect pruning messages resulting in correct nodes being disconnected from the network or tree partitioning. In the absence of authentication, any node can pretend to be the group leader. Although many routing protocols do not describe how to select a new group leader when needed, we note that the leader election protocol can also be influenced by attackers. Attacks against data messages consist of eavesdropping, modifying, replaying, injecting data, or selectively forwarding data after being selected on a route [13][14].

3. IMPLICATIONS OF BYZANTINE BEHAVIOR IN ONLINE AUCTION NETWORK

3.1 Online Auction Model - Case Study

An online auction is simply defined as a virtual marketplace hosted on the Internet to match buyers and sellers of goods around the globe regardless of the physical limitations of traditional auctions such as geography, presence, time, and space. Live Auctions provides real-time online bidding on items being sold on the sales floor of the world’s leading auction houses. Live Auctions empowers traditional auctioneers to extend their sales beyond the auction house floor and reach millions of potential buyers online through a proprietary technology developed by eBay. Buyers gain easy access to exclusive, high-end property with the convenience and comfort of bidding from their home or office [11][18].

The advent of mobile wireless devices has prompted the conduct of online auction in an effective way. MAODV (Multicast Ad hoc On Demand Distance Vector), a well-known protocol that is representative of tree-oriented multicast routing protocols for ad hoc networks is deployed here. Online auction inherently insist the formation of a transient group where the group members are active during the auction activity. The auctioneer who is acting as a group head for the online auction session coordinates the group activities of the members. The group head has to ensure the secrecy of the data and that it reaches only to authorized members who have joined the group after validating their credentials.

3.2 Impact of Byzantine Attack in Online Auction Network

The resource rich online auction transaction invites a host of security challenges to the sensitive group head which mandates the need to improve its resiliency to various attacks. The highest profile attack is the Byzantine attack where an adversary compromising the group head and impersonating it. There is an equal chance of the group member and as well as the group head falling prey to the Byzantine attack. The victimization of the group head mars the inter group communication whereas the victimization of the group member paralyzes the intra group communication [15].

The inter group communication faces more brunt than the intra group communication as the misbehaving group member can be stripped off its membership by the genuine group head whereas the subversion of group head due to a Byzantine attack can cause a host of attacks. We will confine our study to highlight the plight of the subverted group head alone (GSI). Online auction scenario demands the creation of secure multicast distribution tree as advocated by Iolus framework where GSI and GSC control the group activities. The subversion of intermediate GSI’s in the tree by Byzantine attack jeopardizes the normal multicast routing process. Consider a case where there are three GSI’s namely GSI1, GSI2 and GSI3. The GSI1 is adjacent to GSI2 and GSI2 is adjacent to GSI3. However there is no direct link between GSI1 and GSI3.

When GSI1 wants to send the message to GSI3, GSI1 sends the message to GSI2, and GSI1 make sure the ID of GSI2 by a provided method. At the same time, GSI1 expects GSI2 to forward the message to GSI3. Under the assumption that there is bidirectional link for all the adjacent nodes, GSI1 is supposed to hear the signal from GSI2 when GSI2 sends the message to GSI3 because of broadcasting nature in wireless environment. Now assume the abnormal situation when node GSI2 a Byzantine adversary had compromised the node GSI3 by launching a DoS (Denial of Service) attack on it thereby illegally acquiring the possession of the GSI3’s ID. When the node GSI2 receives the message from GSI1, GSI2 does not need to forward the message to GSI3 because GSI2 holds the ID of GSI3 also. This implies that GSI2 does not broadcast the forwarding signal, and the node GSI1 does not hear any signal from GSI2. Thus, GSI1 can assume this situation as anomaly.

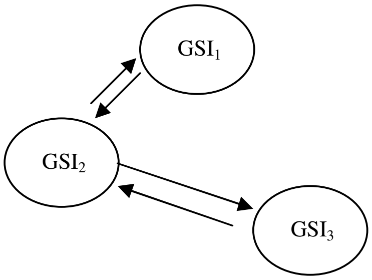


FIGURE 2 CONCEPTUAL ATTACK VIEW

GSI2 can fabricate factual data about the shadow identity and tries to blacklist it. The misrepresentation of the blacklisted node is manifested in several ways like creating routing loop, partitioning the network, misdirecting the traffic to a non existent node, tampering the data, pretending to forward the data to the intended destination. This eventually leads to unwanted pruning of the authenticated node. GSI2 can also collude with GSI3 to gain an undue mileage in the ongoing group communication by swapping their identities and presenting simultaneously wherever is required. The colluding entities can also short circuit the traffic to other non group members though an out of band channel which poses serious challenges as the home network itself is not aware of the divulgence of the sensitive auction data. This scenario creates the least of suspicion by other GSIs as the identity is active anywhere at any given time [19].

4. ROBUST SOLUTIONS FOR CIRCUMVENTING BYZANTINE ATTACK IN ONLINE AUCTION NETWORK

Multicast Routing in adhoc network is a cooperative process seeking the assistance of immediate and intermediate neighbors to forward packets for nodes that are out of transmission range. At any instant of time a node in ad hoc network maintains a constant vigil on its immediate neighbor and establishes a trustable relationship to securely route multicast data on the multicast route. Packet Propagation latency time, end –to – end delay, Throughput, Jitter, Packet Delivery Ratio are touted as reactive/post performance parameter (Po^3)as it present the serious lacunae in the multicast tree after the attack incidence. This parameter cannot be fully relied upon because of the fault reporting lag time. This provides room for the culprit to have a high hand over the transmitted multicast packets and manipulate it at will and wish. The pre performance parameter (Pr^3) like Immediate Neighbor Aware Vouch Count (INAVC) which is proactive and instant precludes the selection of a faulty path and if the path appears less promising in midway, a switch/swap to a correct functional multicast route is facilitated. This parameter guarantees the selection of robust, reliable and responsive (R^3) neighbor which warrants the creation of secure multicast route.

The online auction network inherently embracing multicast technology is prone to a host of outsider and insider attack. The antidote suggested for outsider attack cannot be directly applied for insider attack due to architectural, functional, technical and deployment disparity. Byzantine attack is a very serious attack where the trusted internal participants of the home network behave arbitrarily to cause wide scale disruption and cause performance degradation. This is similar to network acting against itself through some compromised hostile members that are touted as attack launchers. The adversary wishing to gain illegal possession of network information conquers the trusted internal nodes by instigating innumerable attacks like Denial of Service (DoS attack), Wormhole attack, Rushing attack and Sleep Deprivation and torture attack [16].

There are ample opportunities for the Byzantine attacker to compromise any number of intermediate multicast routers in the established multicast tree. These subverted internal multicast routers serve as attack vehicle/launchers jeopardizing the normal multicast flow in the online auction network. The task of penalizing and prosecuting the corrupted/compromised multicast routers and nodes is left at the mercy of genuine, still trusted group members/group head (multicast router). The genuine multicast nodes in the tree continuously and consistently monitor their neighbor's performance metric like delay, throughput, jitter, PDR (Packet Delivery Ratio).

This paper envisage the addition of another performance metric by name INAVC maintained by the genuine group members about their neighbors. The genuine node acting as a watchdog by overhearing the transmission of neighbor's packet already sent by it helps to set the count value accordingly. The neighbor behaving in a consistent and correct manner culminates in the count value increment or otherwise. For any multicast route to be activated the neighbors with a maximum count value is chosen ensuring a non adversarial multicast path. The midway misbehaviour can also be thwarted by sensing the plummeting nature of INAVC value thereby promoting instant pruning of the inconsistent and incompliant nodes. The salvation of troubled/discontinued route occurs by selecting a neighbor with next maximum INAVC value ensuring the persistence of the multicast route.

The process of populating this field is a gradual phenomenon and it incurs less initial overhead at the cost of magnified maintenance in repairing the culprit nodes later. This subtle and suave mechanism is robust in spotting the fault free functional multicast route in the beginning itself. The nodes periodically handshake with their neighbours to exchange the INAVC report for three requirements - In search of a better quality and an optimal route - To forecast a pruning process in multicast tree to nail the Byzantine/compromised nodes - For conducting a thorough study on network topology and learning about neighbours neighbour.

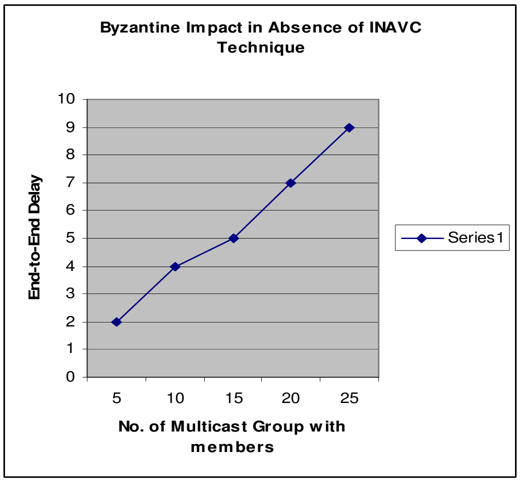
The proposed mechanism has its own share of setbacks. This mechanism inherently suffers a delay factor because it requires neighbourhood scanning to entrust the task of onward routing of multicast packet. It is also subjected to storage, computation and communication complexities. The need to store vouch count value of the neighbours pose Storage complexity. The MANET with frequently changing topology demands the re computation of INAVC values to suit the existing network setup thereby inflating computation complexity. The computed vouch count value has to be disseminated to their neighbours for optimal route selection and to bypass the faulty multicast route etc. leading to surge in communication complexity [17].

The node in possession of INAVC report can cause a blackmail attack or generate false reporting about their genuine neighbors. The multicast group node at any instant of time is likely to receive multiple INAVC reports for the same neighbor through other civilian nodes. The correctness and completeness of the report is assessed by using two techniques like authorization stamp and authentication token embedded along with this report. The report devoid of these recommended techniques is deemed spurious and is unfit for scanning and scrutinizing the neighbors thus thwarting the blackmail occurrence.

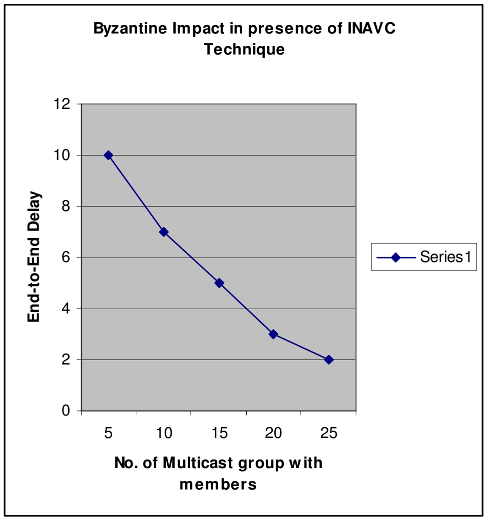
The deterioration in multicast service due to the alleged involvement of the adversary in Byzantine behavioral activities degrades/undermines the promising status of it. The Byzantine attacker is busy manifesting malicious network activities that acts detrimental to the normal multicast routing process. This malicious/spurious misbehaving network entity earns the wrath of the destined nodes (next hop nodes) which are deprived of its normal share of multicast packets. The affected neighbors of the Byzantine adversary join hands in unison and send a Multicast Node Nefarious Report (MN^2R) to the multicast sender/civilian node which maintains the INAVC value.

5. RESULTS AND DISCUSSION

The Byzantine attack in ad hoc network accentuates the security risks faced by multicast routing. The security challenges encountered by the unique wedding of multicast routing in MANET are exacerbated in presence of Byzantine adversary. The deficiency in formation of functional multicast route, incorrect pruning of genuine group nodes, routing loop, directing packets to non existent nodes or collusion between the Byzantine adversaries to cause gratuitous detour and forcing a node to use suboptimal route are the Byzantine attack trail. Two graphs are plotted with the end-to-end delay metric on y axis and no. of multicast groups with members on x axis with the presence and absence of INAVC solution. This robust mechanism foils the attempts made by Byzantine adversary and ensures the maintenance of fault free multicast path through a substantial number of compromised nodes [9]. Graph 1 depicts the surge in end-to-end delay value as the compromised nodes join hands in unison to subvert the normal multicast routing process in the absence of this robust, adaptive solution. Graph 2 represents a slowdown in end-to-end delay value as the compromised Byzantine nodes are prosecuted and penalized accordingly by this INAVC technique.



Graph 1: Byzantine Impact in Absence of INAVC



Graph 2: Byzantine Impact in Presence of INAVC

5. CONCLUSION

Online auction network embracing multicast technology in ad hoc network encounters serious threats from within and outside. The security impact stemming from the compromise of group head/group member is more intense and severe than the outsider attack. This unique novel solution INAVC proactively determines and isolates the faulty node and helps in the formation of non adversarial multicast route. This robust, flexible and adaptive technique helps not only in ensuring the quality and optimality of multicast route but also the persistence of the route in presence of Byzantine adversary. Two graphs are simulated with end-to-end delay performance metric on y axis and the no. of multicast group with members on x axis. Adopting this technique to curtail the occurrence of other variants of Byzantine attack like Rushing, Wormhole, Blackhole and Blackmail attack become foreseeable enhancement.

REFERENCES

[1] 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.

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

[3] 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.

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

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

[6] Awerbuch, B., Curtmola, R., Holmer, D., Rotaru, C.N., and Rubens, H., " Mitigating Byzantine Attacks in Ad Hoc Wireless Networks", March 2004, Technical Report Version.

[7] 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.

[8] Curtmola, R., and Rotaru, C.N., "BSMR: Byzantine-Resilient Secure Multicast Routing in Multi-hop Wireless Networks", Dept. of Computer Science, Purdue University.

[9] Lee, S., and Choi, Y.H., "A Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks", Department of Computer Engineering, Hongik University, Korea.

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

[11] www.onlineauctions.com

[12] Perlman, R., "Network layer protocols with Byzantine robustness".1988, Massachusette Institute of Technology: Boston.

[13] Perlman, R., "Interconnections: Bridges, Routers, Switches and Internetworking Protocols". 2nd ed. 1999:Addision-Wesley Publishing Company.

[14] Awerbuch, B., et al., "Mitigating Byzantine Attacks in Ad Hoc Wireless Networks", 2004, Johns Hopkins University.

[15] Avramopoulos, I.C., H.Kobayashi, and R.Y.Wang., "A Routing Protocol with Byzantine Robustness", Sarnoff Symposium, 2003.

[16] Lin, X., Zhu, H., Lin, B., Ho, P.H., and Shen, X., "A Novel Voting Mechanism for Compromised Node Revocation in Wireless AdHoc Networks", IEEE Communications Society, GLOBECOMM, 2006.

[17] Tan, H., "On Mitigating Malicious Behaviour against Routing in Wireless Network", IEEE Communications Society, WCNC proceedings, 2007.

[18] Sathiyamoorthy, E., Narayana, N.C.S., and Ramachandran, V., "Agent Based Trust Management Model Based on Weight Value Model for Online Auctions", International Journal of Network Security & Its Applications (IJNSA), Vol 1, No.3, October 2009.

[19] Roy, D.B., Chaki, R., and Chaki, N., "A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-hoc Networks", International Journal of Network Security & Its Applications (IJNSA), Vol 1, No.1, April 2009.

Authors

ALBERT RAEBARA. S is Associate Professor of Department of Computer Science, St. Joseph's College, Bharathidasan University Trichy. He obtained his Ph.D from Pondicherry University. He has authored one research book and has written about 30 research papers in leading national and international journals. His research interests coincide with domains like High speed network, Optical networks, Information Security and Nano Sensors. Dr. Albert Raebara is on the editorial board of several reputed journals as well as in government committees.

VIJAYALAKSHMI.S is Lecturer of Computer science, Dept. of Banking Technology (School of Management), Pondicherry 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 5 years in the field of Computer Science. She has authored 5 research papers which are published in refereed national and international journals and conferences.