ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 4, April 2013

Performance Evaluation of Various Countermeasures for Grayhole Attack in Wireless Mesh Network

Christy Thomas[1], Dhanya S Pankaj [2]

M. Tech Student, Department of Computer Science, Rajagiri School of Engineering & Technology, Kochi, India [1]

Asst. Professor, Department of Computer Science, Rajagiri School of Engineering & Technology, Kochi, India[2]

Abstract: Wireless mesh networks (WMNs) have been advancing as a solution for large scale high speed internet access through their self configuring, low cost and scalability. But as compared to wired networks, WMNs are likely to suffer from different security attacks due to its open medium nature, dynamic topology and distributed architecture. A special case of Denial of service (DoS) is called selective forwarding attack or Grayhole attack. This paper compares various counter measures for Grayhole attack in WMNs. The counter measures include Watchdog, Byzantine-Resilient Secure Multicast Routing (BSMR) and channel aware detection (CAD). From the comparison study, it can be concluded that CAD have high packet delivery ratio than Watchdog and BSMR.

Keywords: Wireless mesh networks, Selective forwarding attacks, Watchdog, BSMR, Channel-aware detection

I. INTRODUCTION

A wireless mesh network (WMN)[1] is an ad-hoc network that provides both redundancy and self healing as each node in the mesh network is connected at least to one other node. A WMN consists of mesh routers and mesh clients. Mesh routers are the backbone of WMN with minimal mobility which guarantees high connectivity and robustness. The gateway and bridge functionalities in mesh routers enable the integration of wireless mesh networks with various existing wireless networks, such as wireless sensor networks, WiMAX and wireless-Fidelity (Wi-Fi) [8].The mesh client nodes can be stationary or mobile whose backbone is provided by mesh routers.

A special kind of Denial of Service (DoS) attack is called selective forwarding attack or Gray hole attack [2]. In this attack, an opponent node first exhibits as an honest node during the route discovery process, and then it refuses some of the data packets sent to it even when no congestion occurs. Thus malicious nodes could degrade the network performance and disturb route discovery process. In a wireless network, it is hard to detect the presence of such adversary node because the packet loss over the wireless link can be due to bad channel quality, collisions, intentional dropping and so on. If an attacker node drops all the packets, the attack is called black hole attack [9].

To launch a selective forwarding attack, an attacker may compromise the mesh router in the network, known as internal attacks; or attack the network from outside, which is known as external attacks. To prevent external attacks, routers may use any authentication mechanism to keep away the attacks from unauthorized routers. But, internal attacks may constitute severe threats. So both cryptographic and non-cryptographic approach is used to defend the dropping misbehavior launched by internal attackers [3].

One of the methods to resist selective forwarding attack is Watchdog technique [4], where a node monitors its neighbors to determine whether they forward the packet to the intended destination. In [5], the authors propose another selective forwarding detection scheme Byzantine-resilient multicast protocol (BSMR) for multicast routing protocols. Another practical algorithm known as channel aware detection (CAD) that adopts two steps, hop-by-hop loss monitoring and traffic overhearing, to identify the mesh nodes subject to the attack is described in [6].

The rest of the paper is organized as follows. Section II describes the Watchdog technique to find the misbehaving node. The second method, Byzantine-Resilient Secure Multicast Routing (BSMR) is explained in Section III. Section IV discusses the third method, Channel Aware detection of gray hole attack. Section V compares the above three techniques. Finally this paper is concluded in Section VI.

II. WATCHDOG AND PATHRATER TECHNIQUE

Watchdog and Pathrater is a technique for detecting and mitigating routing misbehavior presented by S. Marti *et al.* [4].

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 4, April 2013

A. Watchdog

Watchdog is a method for detecting the misbehavior nodes. Suppose there exists a path from node S to D through intermediate nodes A, B, and C. Node A cannot transmit a node to C, but A can listen on node B's traffic. When A transmits a packet for B which is to be forward to C, A can tell whether B forwards the packet. A can also tell if B has tampered with the payload or the header if encryption is not performed separately for each link. The figure 1 illustrates the working of Watchdog. In the figure the solid line represents the intended direction of the packet sent by B to C and the dashed line indicates that A is within transmission range of B and can overhear the packet transfer.

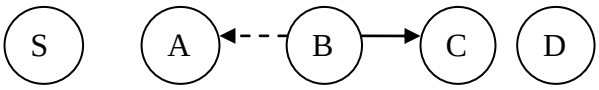

Figure 1.Watchdog Technique [4]

The watchdog can be implemented by maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to check whether there is a match. If there is a match, the packet in the buffer is removed by the watchdog, since it has been already forwarded. If a packet has in the buffer for longer than a particular timeout, the watchdog increments a failure tally for the node responsible for forwarding the packet. If the tally exceeds a particular threshold bandwidth, it concludes that the node is misbehaving and sends a message to the source notifying it about the misbehaving node.

B. Pathrater

The pathrater is run by each node in the network. It combines knowledge of misbehaving nodes with link reliability data to find a reliable path. Each node maintains a rating for every other node it knows about in the network. The pathrater assigns ratings to nodes. When a node in the network becomes known to the pathrater (through route discovery), 0.5 is assigned by the pathrater. A node always rates itself with a 1.0. This ensures that when calculating the path, the pathrater increments the ratings of nodes on all actively used paths by 0.01 at periodic intervals of 200ms[4]. A special highly negative value, -100 for example, is assigned to nodes suspected of misbehaving by the watchdog mechanism. A negative path value indicates the existence of one or more suspected misbehaving nodes in the path when the pathrater calculates the path metric. If the path metric value is negative the pathrater will find another path for forwarding the packets.

III. BYZANTINE- RESILIENT SECURE MULTICAST ROUTING (BSMR)

BSMR is secure multicast routing protocol that withstands insider attacks from colluding adversaries. BSMR is proposed by R. Curtmola and C. Nita-Rotaru [5].

A. BSMR Overview

BSMR ensures that multicast data is delivered from the source to the members of the multicast group, as long as the group members are reachable through non-adversarial paths and a non-adversarial path exists between a new member and a node in the multicast tree. This is done even in the presence of byzantine attackers.Outside attackers are prevented using authorization framework. Nodes have a method to determine the source authenticity of the received data (e.g., TESLA [7]). This allows a node to determine correctly the rate at which it receives multicast data.
Inside attacks that try to prevent a node from establishing a route to the multicast tree by flooding both route request and route reply are mitigated by BSMR. Each node has a weight list which is a list of link weight. High weights correspond to low reliability. This list is included in each route request to ensure that a new route to the tree avoids adversarial links. A link's reliability is based on the number of packets successfully delivered on that link over time.

B. BSMR Route Discovery

BSMR route discovery allows a newly added node to find a route to the multicast tree. The protocol follows the typical route request/route reply procedure used by on-demand routing protocols. All route discovery messages are authenticated using the public key corresponding to the network certificate to prevent the outside interferences. Only group authenticated nodes can initiate route requests. The group certificate is required in each request. Tree token are used to prove their current tree status.
Several mechanisms are used to counter internal attackers: (1) both route request and route reply are flooded in order to ensure that, if an adversarial-free path exists, it will be found; (2) the path selection relies on the weights list carried in the response flood and allows the requester to select a non-adversarial path; (3) the propagation of weights and path accumulation is performed using an onion-like signing to prevent forwarding nodes from modifying the path carried in the response.

IV. CHANNEL – AWARE DETECTION ALGORITHM

Channel Aware Detection (CAD) is proposed by D M Shila and T Anjali [6]. It identifies intentional selective dropping from "natural" wireless losses. A "natural" packet loss can occur due to bad channel quality or medium access

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 4, April 2013

collisions under the infinite buffer assumption. These two types of loss events are independent and are estimated as "natural" losses (L).

In CAD, each mesh node maintains a number of packets received by it to measure the loss rate of the link. Therefore, when a node receives a packet from the upstream (Previous-hop), it updates the packet count history with the corresponding packet sequence number and buffers the link layer acknowledgments (ACKs) received for each packet forwarded to downstream node (next hope).

The number of packets forwarded by source S to destination D is denoted as Ws and the number of packets received successfully by the intermediate node v_{i+1} from the upstream node v_i over a time window is denoted as $n_{v_{i+1}}^{v_i}$ [6].

When a router forwards a packet to the downstream node, it performs two operations: (i) For each packet relayed to the downstream, it buffers the ACKs. (ii) It also overhears the downstream traffic and determines whether the node forwarded or tampered the packet. Based on these observations, the node maintains two parameters for its downstream node, probability of trust, P_t and probability of distrust, P_{dt} where $P_t = 1 - P_{dt}$. Probability of distrust can be calculated as the number of packets tampered and dropped by the downstream node out of the total number of forwarded packets.

Two new packets known as the PROBE packet and PROBE ACK packet are used for the detection of malicious routers. The source, S, sends a PROBE packet after every Ws data packets. On receiving the PROBE, each node in the path marks the PROBE packet with the two detection parameters. This technique is known as packet marking. For each PROBE packet sent to destination, source marks the packet with the number of packets transmitted to destination (Ws) and each intermediate node v_{i+1} marks the packet with the number of packets received successfully from its upstream node v_i. Additionally, when the packet is passed along the path, each node v_i also attaches mark of its opinion to the downstream node v_{i+1} to indicate that the downstream node is misbehaving or not. Opinion is either 0 or 1 based on a threshold. In addition to opinion parameters, each node except the source and destination appends the parameter the behavior. Behavior represents the observation of node v_{i+1} about the behavior of upstream node v_i and is computed by determining the packet loss rate of the link $\{v_i, v_{i+1}\}$ by the node v_{i+1}. At each node, the PROBE message is attached with a message authentication code (MAC), which is generated with the node's private key and a nonce random number. The MAC signature can protect the message from being tampered. On reception of the PROBE message, the destination make a list of misbehaving nod using information added by each node in the path. Then the destination sends a PROBE ACK message to the source for every PROBE packet it receives from source. If the source gets a negative PROBE ACK from destination the source will find another route to destination. If the source gets apositive PROBE ACK from destination the source will resume the data transmission.

V. DISCUSSION

In the previous section, various counter measures for selective forwarding attack were discussed. In watchdog technique, a node acts as a monitor and observes its neighbors to find misbehaving node. BSMR protocol provides resilience against Byzantine attacks. CAD algorithm detect attackers effectively even in harsh channel condition.

Figure 2 gives a performance comparison of Watchdog (WD), BSMR, CAD techniques to defend gray hole attack. Horizontal line represents selective dropping rate and vertical line represents the Packet Delivery Ratio (PDR).

TABLE I
COMPARISON OF VARIOUS COUNTERMEASURES FOR GRAY HOLE ATTACK

Methods	Characteristics	Advantage	Disadvantage
Watchdog and Pathrater Technique	A node monitor its neighbors to detect misbehaving node	Detect misbehavior at the forwarding level	Do not detect a misbehaving node in the presence of ambiguous collisions, receiver collisions, limited transmission power, false misbehavior, collusion and partial dropping.
BSMR	Selective dropping detection scheme for multicast routing protocol	Identifies and avoids adversarial links based on a reliability metric	Assumes static detection threshold independent of channel quality and medium access collision
Channel Aware Detection Algorithm	Detects attacker node using hop-by-hop loss observation and traffic overhearing strategies	Detection of attacker node does not depend on the data traffic through a node and CAD works well under dynamic channel behavior because threshold values are dynamic	Needs to send extra packet to initiate the detection. Attack detection is done by the source router so attacker is identified only if the source router demands

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 4, April 2013

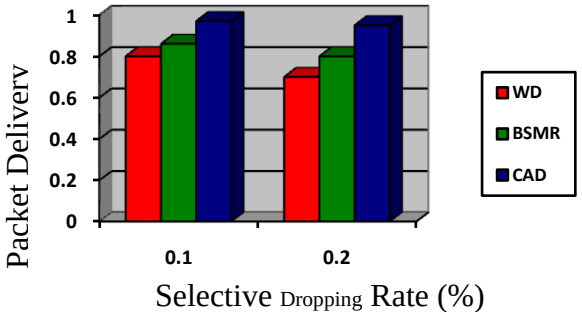

Figure 2.Comparison of PDR of WD, BSMR, CAD

It can be inferred from the figure that, CAD has better packet delivery ratio (PDR), approximately 0.96 at a dropping rate of 10% when compared to Watchdog that has only 0.8 PDR and BSMR 0.86 PDR [3]. BSMR employs static thresholds that are independent of "natural" losses where CAD sets the threshold values dynamically. Table 1 summarises the comparison of the above methods along with each method's advantage and disadvantage.

VI. CONCLUSION

Wireless Mesh Networks (WMNs) have emerged recently as a promising technology for next-generation wireless networking. It provides wide variety of applications that cannot be supported directly by other wireless networks. Security is a major concern of this network. This paper compares three different methods to counter one of the DoS attack called the gray hole attack in wireless mesh network. From the comparison it can be concluded that CAD algorithm performs better than Watchdog and BSMR algorithms since its detection of attacker node does not depend on the data traffic through a node. Also CAD works well under dynamic channel behavior because threshold values are dynamic.

REFERENCES

[1] I.F. Akyildiz and X. Wang, "A survey on Wireless Mesh networks," in *IEEE communication Magazine*, September 2005
[2] E. Cayirci and C. Rong. "Security Attacks in Ad Hoc, Sensor and Mesh Networks," in *Wiley-Interscience*, Jan. 2009
[3] Devu Manikantan Shila, Yu Cheng and Tricha Anjali, "Mitigating Selective Forwarding Attacks with a Channel-Aware Approach in WMNs", IEEE Transactions On Wireless Communications, VOL. 9, no 5, pp 1661 – 1675, May 2010..
[4]] S. Marti, T. J. Giuli, K. Lai and M. Baker "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. of MobiCom, Boston, Massachusetts, 2000.
[5] R. Curtmola, and C. Nita-Rotaru "BSMR: Byzantine-Resilent Secure Multicast Routing in Multi-hop Wireless Networks," in Proc. of Sensor, Mesh and Ad Hoc Communications and Networks, Jun. 18-21, 2007.
[6]] Devu Manikantan Shila, Tricha Anjali, "Defending Selective Forwarding Attacks in WMNs", IEEE International conference on electro/information technology 2008, EIT 2008, pp 96 – 101, May 2008.
[7] A. Perrig, R. Canetti, D. Song, and J. D. Tygar, "Efficient and secure source authentication for multicast," in Proc. Of NDSS'01, 2001.
[8] L. Santhanam, D. Nandiraju, N. Nandiraju, and D.P. Agrawal, "Active cache based defense against dos attacks in wireless mesh network," in Wireless Pervasive Computing, 2007,ISWPC '07. 2nd International Symposium on, Feb. 2007
[9] Choong Seon Hong Muhammad Shoaib Siddiqui, " Security issues in wireless mesh networks," in International Conference on Multimedia and Ubiquitos Engineering. IEEE Computer Society, IEEE, 2007S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

BIOGRAPHY

Christy Thomas is currently pursuing her Master of Technology in Computer Science and Engineering with Specialization in Information Systems from Rajagiri School of Engineering and Technology, Kochi, Kerala, India under M.G University. She received B. Tech degree from Govt. Engineering college, Idukki under Mahatma Gandi University.