World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:7, No:7, 2013

Selective Forwarding Attack and Its Detection Algorithms: A Review

Sushil Sarwa and Rajeev Kumar

***Abstract*—**The wireless mesh networks (WMNs) are emerging technology in wireless networking as they can serve large scale high speed internet access. Due to its wireless multi-hop feature, wireless mesh network is prone to suffer from many attacks, such as denial of service attack (DoS). We consider a special case of DoS attack which is selective forwarding attack (a.k.a. gray hole attack). In such attack, a misbehaving mesh router selectively drops the packets it receives from its predecessor mesh router. It is very hard to detect that packet loss is due to medium access collision, bad channel quality or because of selective forwarding attack. In this paper, we present a review of detection algorithms of selective forwarding attack and discuss their advantage & disadvantage. Finally we conclude this paper with open research issues and challenges.

***Keywords*—**CAD algorithm, CHEMAS, selective forwarding attack, watchdog & pathrater, wireless mesh network**.**

I. Introduction

A wireless mesh network (WMN) [1] is a communication network made up of radio nodes organized in a mesh topology. As shown in Fig 1, Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The mesh clients are often laptops, cell phones and other wireless devices while the mesh routers forward traffic to and from the gateways which may, but need not, connect to the Internet. WMNs are emerging as a promising solution to provide high-speed Internet access due to the advantages of scalability, self-management, and low up-front cost [2]. U.S. military forces are currently using WMNs to connect their computers in field operations. Several universities deployed WMN in their campuses to provide high speed internet access without need to bury cables in old buildings. WMNs are applicable in isolated locations, rugged terrain etc. where implementing a wired network is very hard. However, compared to wired networks, the WMNs are more likely to suffer from various security attacks, due to the nature of open medium, distributed architecture and dynamic topology [1], [3]-[6]. A mesh network is reliable and offers redundancy. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes.

Sushil Sarwa is postgraduate student at Computer Science and Engineering Department in National Institute of Technology Hamirpur (H.P.), India 177005 (e-mail: sushilsarwa87@gmail.com).

Rajeev Kumar is with Computer Science and Engineering Department In National Institute of Technology Hamirpur (H.P.), India 177005 (e-mail: eminentpearl@gmail.com).

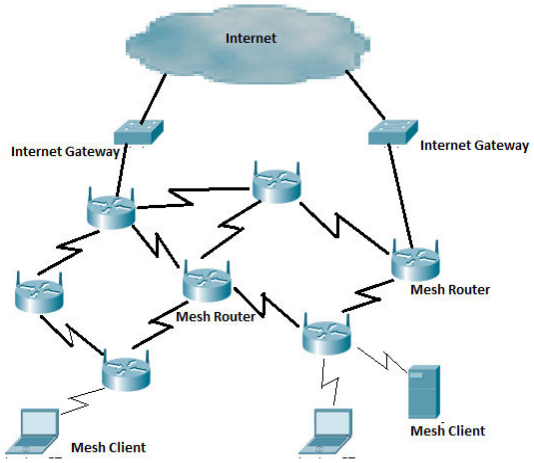

Fig. 1 Wireless Mesh Network

WMNs are vulnerable to passive attacks such as eavesdropping [4], as well as to active attacks such as DoS attack [3]. If routers are collaborated with each other successfully than the network become strong and reliable. We can use cryptography solutions to protect the mesh routers from most of routing protocols attacks- selective forwarding, black hole, sinkhole and wormhole attacks [3], [4], [6]-[8]. But if any router in network is compromised, the attacker will easily gain access to the public/private keys of the compromised routers and use them to break the cryptographic system.

In this paper we concentrate on a special case of DoS attack which is selective forwarding attack first propose by karlof [4]. In this attack a malicious router selectively drop the data packets from the packets it received. When any data packet comes to the source router from mesh client for sending to the destination then the source router first check its routing table and if it could not find any route then it will broadcast the ROUTE REQUEST (RREQ) message. When destination node or intermediate node gets this message all of them send the ROUTE REPLY (RREP) to the source router. Source router can select the RREP from attacker node as it is showing that it have the fast and reliable path from source to destination. Once the source router sends the data packets to the attacker node, the attacker node sends the subset of the packet it received to the destination.

Most of the prior works related to selective forwarding attacks were studied in the area of ad hoc and sensor networks. These works can be used in the area of WMNs too. But since WMNs are mainly targeting the broadband usage, these type

of attack will be more common in WMNs as compare to other two networks.

In this paper we describe the selective forwarding attack and how it can be implemented in WMN. The remainder of this paper is organized as follow. Sections II, III and IV will give a brief introduction of three different techniques to detect selective forwarding attack and their advantage & disadvantage. In final section we conclude this paper with open research issues and challenges.

II. Watchdog & Pathrater Scheme

The watchdog & pathrater [3] algorithm was designed for detecting selective forwarding attack in mobile ad hoc networks but the same can also be used for WMNs. In this algorithm the network is modified by installing extra facilities to detect and mitigate routing misbehavior. These facilities are introducing two new extensions to the Dynamic Source Routing algorithm (DSR) [9] to mitigate the effect of routing misbehavior, the watchdog and pathrater.

A. Proposed Scheme and Implementation

1.Watchdog

The watchdog used to identifies misbehaving nodes. When a packet is forwarded by a node, the node's watchdog verifies that the next node in the path also forwards the packet. Promiscuous mode should be enabled for this so that node can listen the transmissions of next node. If the next node does not forward the packet then it is misbehaving. Pathrater use this information to decide the network path that can deliver packets.

2.Pathrater

The pathrater runs by each node in the network. This facilitates to combine knowledge of misbehaving nodes with link reliability data to pick the route most likely to be reliable. Each node in the network maintains a rating about every other node it knows. This rating is used to calculate the path metric by averaging the node ratings in the path. This metric provide the comparison of the overall reliability of different paths and allows path rater to emulate the shortest length path algorithm when no reliability information has been collected. It is different from standard DSR as in that shortest path in the route cache is chooses. Since the path rater depends on knowing the exact path a packet has traversed it must be implemented on top of a source routing protocol.

The watchdog technique has some advantage and weaknesses when used with DSR. The advantage of watchdog is that it can detect the misbehavior of a node at forwarding level. Watchdog's weaknesses are that it might not detect a misbehaving node in the presence of 1) ambiguous collisions, 2) receiver collisions, 3) limited transmission power, 4) false misbehavior, 5) collusion, and 6) partial dropping [3]. This algorithm also increases the overhead transmission. Pathrater used to send some extra route request packets and watchdog also adds small amount of extra overhead.

III. CHEMAS: Checkpoint-Based Multi-Hop Acknowledgement Scheme

This scheme was especially given for selective forwarding attack in wireless sensor networks but it is also applicable in WMNs. According to Checkpoint-based Multi-hop Acknowledgement Scheme (CHEMAS) [4], multipath forwarding technique can be used to decrease the impact of selective forwarding attack. In this scheme, each intermediate node can detect abnormal packet loss and identify malicious nodes in its forwarding path according to the amount of acknowledgements it received from the downstream checkpoint nodes. The source node collects alert information from intermediate nodes containing suspect nodes' ID and position.

A.Proposed Scheme and Implementation

In this detection scheme three types of packets are used. Packet format of each packet is shown in Tables I-III [4]. Event packets are generated whenever a special event or a query from a base station is detected. After an event packet is generated, it is forwarded hop-by-hop from the source node to the base station.ACK packets are generated at checkpoint nodes in a forwarding path. When a checkpoint node receives an event packet, an ACK packet is generated for the event packet and then delivered to the upstream nodes. The path followed by ACK packet remain same as followed by the previous event packet only in opposite direction. Alert packets are generated at intermediate nodes when suspect nodes are detected. Once generated, alert packets will be sent to the source node or the base station through multiple hops. The basic idea of this scheme is as follows. Intermediate nodes, which come in the forwarding path is selected as checkpoint node. The path then is divided into several segments by these checkpoint nodes. Whenever a special event is detected by source node, an event packet is generated.

TABLE I
Event Packet Format

DstID(2 Byte)	SrcID(2 Byte)	Packet_ID(2 Byte)	Payload(50 Byte)	Checkpoint_Seed(2 Byte)

TABLE II
ACK Packet Format

Packet_ID(2 Byte)	Node_ID(2 Byte)	OHC_number(2 Byte)
MAC_{OHC}(4 Byte)		TTL(1 Byte)

TABLE III
ALERT PACKET FORMAT

DstID(2 Byte)	SrcID(2 Byte)	Suspect_Node_ID(2 Byte)
Lost_Packet_ID(2 Byte)		MAC(4 Byte)

This event packet will be forwarded hop-by-hop toward the base station, and each intermediate node saves the event packet in its cache after forwarding it to the next downstream node. When a checkpoint node receives an event packet from an upstream neighbor, it generates an ACK packet and then sends the ACK packet back to the upstream neighbor. The ACK packet is transferred toward the source node. If an intermediate node cannot receive ACK packets from downstream, it will generate an alert packet, specifying the next downstream-neighboring node as the suspect node.

Some of the key disadvantages of this algorithm is that the algorithm suffers from high overhead as intermediate node need to send an acknowledgement packet to source node on receiving each packet. Also this algorithm assumes that there is no loss because of bad channel quality and if any packet is dropped than it is due to presence of malicious nodes.

IV. Channel Aware Detection Algorithm

The Channel Aware Detection (CAD) [2] algorithm is based on two procedures, channel estimation and traffic monitoring [2]. Channel estimation is the procedure to estimate normal loss rate due to bad channel quality or medium access collision while traffic monitoring is used to monitor actual loss rate. If the monitored loss rate at certain hops exceeds the estimated loss rate, those nodes involved will be identified as attackers.

A. Proposed Scheme and Implementation

The basic principle of CAD is as follows. Each intermediary node along given a path implements both downstream and upstream monitoring and Observing the behavior of a downstream node to determine whether the node is dropping or tampering the data packets is called downstream monitoring while observing the behavior of its upstream node by measuring the loss rate is called upstream monitoring. These observations are then compared against the upstream/downstream detection thresholds to detect misbehaviors.

In CAD, each mesh node maintains a history of packet counts such as how many packets it receives from its upstream node and how many packets it overhears from its downstream node which are forwarded. Based on these observations, each node maintains a probability of distrust for its downstream node. Two types of packets known as the PROBE packet and PROBE ACK packet are introduced for the detection of malicious routers. The source sends a PROBE packet after a bunch of data packets which contains total number of packets send to the destination. When this PROBE packet reached at all nodes in the path, each node add its traffic monitoring parameters along with PROBE packet. Now it is the work of destination node to check the packet loss if any by using the information send by each node in PROBE packet. On receiving a PROBE packet, destination node need to send PROBE ACK packet to source node. If destination node detect packet loss then it send a negative PROBE ACK to source which contains a list of suspicious routers based on CAD. Now source uses another path in route cache to forward the remaining data packets. If no packet loss detected then destination send a positive PROBE ACK packet to source. The source node just continues the normal data transmission upon the positive PROBE ACK.

The main advantages of the algorithm are that each node's behavior in the path is observed by its upstream and downstream neighbors, and the thresholds are dynamically adjusted with the normal loss rates to maintain the detection accuracy when network status changes. Disadvantage of this algorithm is that extra packets are transmitted to detect the attack and also downstream traffic monitoring increase the traffic overhead.

V. Conclusion

In recent years, DoS attacks become one of the most common attacks on network and also a most important area of research, and there have been existed large number of research. In this paper, we concentrated on selective forwarding attack and its detection algorithms in different types of wireless networks. CAD algorithm can detect the attackers efficiently and thus increase the packet delivery ratio. Nevertheless, there still exist a series of challenges in this algorithm. We need a mechanism that can preserve our network from attacks and also increase the efficiency.

References

[1] I. F. Akyildiz and X. Wang, "A survey on wireless mesh networks," IEEE Commun. Mag., vol. 43, no. 9, pp. S23-S30, Sept. 2005.
[2] D. M. Shila, Yu Cheng, and T. Anjali. Mitigating selective forwarding attacks with a channel-aware approach in WMNS. Wireless Communications, IEEE Transactions on , 9(5):1661 –1675, may 2010.
[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. International Conference on Mobile Computing and Networking, Boston, MA, 2000.
[4] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Elsevier's AdHoc Networks J., vol.1, no. 2-3, pp. 293-315, Sept. 2003.
[5] B. Xiao, B. Yu, and C. Gao, "CHEMAS: identify suspect nodes in selective forwarding attacks," J. Parallel and Distrib. Computing,vol. 67, no. 11, pp. 1218-1230, Nov. 2007.
[6] D. Manikantan Shila and T. Anjali, "Defending selective forwarding attacks in mesh networks," in Proc. 2008 Electro/Information Technology Conference , Ames, IA, May 2008.
[7] R. Curtmola and C. Nita-Rotaru, "BSMR: Byzantine-resilient secure multicast routing in multi-hop wireless networks," in Proc. Sensor, Mesh and Ad Hoc Communications and Networks, June 2007.
[8] A. Perrig, R. Canetti, D. Tygar, and D Song, "The TESLA Broadcast Authentication Protocol," in RSA Crypto Bytes, Summer 2002.

[9] A. D. Johnson, D. A. Maltz, and 3. Broch. "The Dynamic Source Routing Protocol for Mobile Ad-Hoc Networks" (Internet-Draft). Mobile Ad-hoc Network (MANET) Working Group, IETF, October 1999.D. Johnson. Personal Comm- unication. February 2000.