Mitigation of Multiple Blackhole Attack in WMN

Arijita Bhowmik
Department of Computer Science & Engineering
Tripura University
Suryamaninager

Abhishek Majumder
Department of Computer Science & Engineering
Tripura University
Suryamaninager

ABSTRACT

Wireless Mesh Networks (WMNs) is an emerging technology. Amongst number of challenging issues, security is a very serious issue in WMNs. If the network is not secured, network will be confined to a limited and controlled environment. In WMNs, the static mesh routers (MRs) cooperate with each other to forward packets. The routing protocols assume that all the routers in the network are reliable. Due to open architecture of the WMNs, it suffers from various types of denial of service attacks like collision attacks, packet dropping and misdirection, blackhole attack and multiple blackhole attack. In black hole attack, the routers advertise itself to have a valid route to a destination router, though the route is unauthentic. Some routers can also co-operate with each other to implement multiple blackhole attacks. Many Intrusion Detection Systems (IDSs) such as use of honeypot and routing protocols like modified Ad hoc On-Demand Distance Vector Routing (AODV) have been introduced. In this paper, an algorithm for intrusion detection against multiple blackhole attacks has been proposed. The proposed scheme uses the Data Routing Information Table (DRI) to accurately diagnose multiple black hole attack**.**

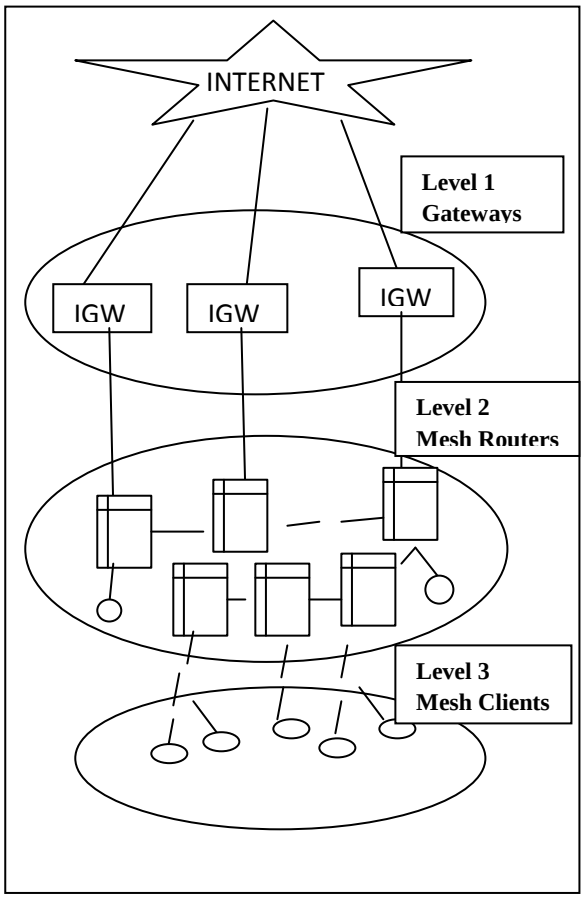
Keywords

Blackhole, Data Routing Information, Intrusion detection, Multiple blackhole, Wireless mesh networks.

1. INTRODUCTION

Wireless Mesh Networks (WMNs) are emerging as a new upcoming technology in providing fast broadband internet services to a large number of mobile users [1].The WMNs are arranged in a hierarchical manner and it consists of Mesh Routers (MRs), Mesh Clients (MCs) and Internet Gateways (IGWs) as shown in Fig. 1. The IGWs are connected to the wired network. They form the upper most level (Level 1) of the hierarchy. The MRs (Level 2) are the static Access Points (APs). They are connected to each other through wireless links. The MRs route the traffic from the MCs to the IGWs in a multi-hop fashion. The MCs (Level 3) are connected to the nearest available MRs in a single or multi hop fashion.

Mesh networking provides solutions to the applications such as building automation, small and large scale internet connectivity, etc [1]. As it is more advantageous over other wireless networks, WMNs are emerging as a new solution for rapid progress and inspiring many applications [2].
However, due to the factors like open wireless channels, cooperative routing algorithm, lack of centralized monitoring, etc. the WMNs results in increased risk and opportunity of network intrusion [1]. So, a safety measure to detect and clear



intruders is a very important and urgent issue in WMNs. But it is very difficult to prevent completely the networks from being attacked. So, an intrusion detection system is needed to detect intrusion and to take appropriate measures to overcome the intruded network [3].

An intrusion detection system (IDSs) is a device or software application that monitors network or system activities. It detects the malicious activities or policy violations and produces reports to a management station for the necessary action. An Intrusion detection and prevention systems (IDPSs) primarily aims at identifying the possible incidents, logging information about them and reporting attempts [4]. Traditional approaches are based on the pre-knowledge of misbehavior patterns. There are two major drawbacks of traditional approaches. First, the discovery of signatures whenever there is a new attack. So IDSs need to be updated frequently. Second, if the signature matches, it is recognized only as an attack. There is no signature for new attacks [5]. Also traditional approaches do not have the ability to detect the multi-patterns of misbehavior or cooperative misbehavior. So, a new intrusion detection system that can overcome such pitfall is necessary.

This paper presents an IDSs based on DRI. The scheme can detect misbehaviours directly using the routing protocol. The mesh routers maintain an additional DRI table along with the routing table. The information stored in the DRI table is used to detect single as well as multiple malicious attackers that cooperate with each other.

The paper is organized as follows. Section II gives the definition of the black hole and multiple black hole attack. Section III reviews existing work in this area. Section IV presents the scheme and algorithm. V shows the working of the algorithm. Section VI compares the proposed scheme with other schemes. Finally, section VII draws the conclusion and future work.

2. BLACK HOLE

This section gives an overview of black hole attack. The black hole routers advertise to have a valid route to a destination router. The route through that router is unauthentic. It has the intention to capture the packet and perform malicious activity [6]. Many researchers have proposed solutions to identify and eliminate a single black hole node [6]. However, to the best of our knowledge, the case of multiple black hole nodes acting in cooperation has not been addressed effectively in wireless mesh network. In a multiple black hole attack the malicious nodes cooperate with each other in such a way that simple intrusion detection system fails to detect them.

3. RELATED WORK

This section describes few of the relevant schemes for solving black hole attack.

Prathapani et. al [1] proposed a novel strategy by employing mobile honeypot agents that utilizes the topological knowledge and detects spurious route advertisements. Honeypot agents are deployed as roaming software agents that tour the network and lure attackers by sending route request advertisements. Agents collect valuable information on attacker's strategy from the intrusion logs gathered at a given honeypot.

Ramaswamy et. al [6] proposed modified Ad hoc On-Demand Distance Vector (AODV) protocol and made the use of the Data Routing Information (DRI) table along with the cached and current routing tables. In the protocol, the source node (SN) broadcasts a Route Request (RREQ) message to discover a secured route to the destination node. The Intermediate Node (IN) generating the Route Reply (RREP) is to provide its Next Hop Node (NHN) and its Data Routing Information (DRI)) entry for the NHN. Upon receiving RREP message from IN, the source node will check its own DRI table to see whether IN is a reliable node or not. The power constraints and low processing speeds in the wireless ad hoc and sensor networks limit the use of this solution.

Black-hole attack is a type of denial-of-service attack which when carried out can disrupt the services. Shree et. al [7] has implemented RID-AODV, a security solution for multiple black-hole attack in WMNs. Based on the backbone of AODV, RID-AODV combines the ability of route skipping of Intrusion Detection System AODV (IDSAODV) and route failure correction using reverse route establishment of Reliable Ad hoc On-demand Distance Vector (RAODV). But it is difficult to maintain a reverse route.

R.Suryawansi et. al [8] had investigated that a collection of honeypots trap the attacker more effectively. The authors proposed a honeynet, which is a collection of honeypots. Honeynet is able to trap the attackers by analyzing their attacking techniques. Honeynet send the logs to a centralized repository to analyze those logs so as to better understand the technique used for attacking. The analysis is based on the pre-knowledge of the attack. So, it cannot detect multi-patterned attack.

Rawat et. al [9] proposed to create a honeypharm for trapping the activities of hacker in order to build more secured WMNs. It is based on a clustered honeypot approach where the entire network is divided into clusters. Each cluster consists of at least one honeynet that comprises of two or more low interaction honeypots (i.e. honey mesh routers). This low interaction honeypot detects the attackers and traps all the activities of attacker. It then sends the attacker's information to the high interaction honeypot that are acting as a Remote Gateway (RG) which is a central place for collecting all the malwares. These low interaction honeypots when encounters an attack, activates a trigger on high interaction honeypots. The high interaction honeypot analyzes all the activities of the attacker and stores it in a log files. After the analysis, all these files are normalized and stored in a central database in the form of tables from where readable information can be presented in a proper way to the end users. Though it is efficient but it cannot detect malicious attackers that cooperate with each other.

L. Santhanam et. al [10] investigated the detection of route floods by using a machine learning technique. A perceptron training model as a tool for intrusion detection has been used. The perceptron model is trained by feeding various network statistics and then used as a classifier.

4. PROPOSED APPROACH AND ALGORITHM

WMNs consist of the static mesh routers. The proposed scheme is based on the DRI table that is maintained by the static mesh routers. Each router maintains an additional DRI table. In the DRI table, 1 stands for "true" and 0 for "false". The first bit "From" stands for information on routing data packet from the router and the second bit "Through" stands for information on routing data packet using the router. Using the DRI table, we check the reliability of the interacting routers. Through cross-checking multiple blackhole attacks can be detected. Crosschecking is done using Further Reply (FRq) which includes DRI entry for Intermediate Router (IR), the next hop router of current next hop router (NHR) and the DRI entry for the current NHR's next hop. As the mesh routers are static in nature the cross-checking results can be used for a longer time. This leads to fast packet transfer and less bandwidth problem.

In the protocol, the source router (SR) broadcasts a RREQ message to discover a secured route to the destination node. The IR that receives RREQ informs who is its NHR, and its DRI table entry for the NHR. Upon receiving RREP message from IR, the source router will have to check its own DRI table to find whether IR is a reliable node. If source router has used IR before to route data, IR is a reliable router and source router starts routing data through IR. Otherwise, IR is

unreliable and the source router sends FRq message to NHR to check the identity of the IR, and asks NHR: 1) if IR has routed data packets through NHR [9]) who is the current NHR's next hop to destination, and 3) has the current NHR routed data through its own next hop. The NHR in turn responds with FRq message which include 1) DRI entry for IR [9]) the next hop router of current NHR and 3) the DRI entry for the current NHR next hop. Based on the FRp message from NHR, source node checks whether NHR is a reliable node or not. If source node has routed data through NHR before, NHR is reliable; otherwise, unreliable. If NHR is reliable, source node will check whether IR is a black hole or not. If the second bit is equal to 1 i.e. IR has routed data through NHR of the DRI entry from the IR, and the first bit of the DRI entry from the NHR is equal to 0, IN is a black hole. If IR is not a black-hole and NHR is a reliable node, the route is secured, and source node will update its DRI entry for IR with 01, and start routing data via IR. If IR is a black-hole, the source node identifies all the nodes along the reverse path from IR to the node that generated the RREP as black hole nodes. Source node ignores any other RREP from the black holes and broadcasts the list of cooperative black holes. If NHR is an unreliable node, source node treats current NHR as IR and sends FRq to the updated IR's next hop router.
The notations used in the algorithm are shown in table I. Fig. [9] presents the algorithm.

Table 1. Notation used in the algorithm

SR	Source Router
IR	Intermediate Router
DR	Destination Router
NHR	Next hop router
FRq	Further Request
FRp	Further Reply
RREQ	Route Request
RREP	Route reply
Reliable Router	The Router through which the SR has routed data
DRI	Data Routing Information
ID	Identity of the node

1. Source Router (SR) broadcasts Route Request (RREQ)
2. SR receives Route reply (RREP)
3. IF (RREP is from Destination Router (DR) or a reliable router)
   Route data packets (Route is secure)
4. ELSE
   1. Send FRq and ID of IR to NHR.
   2. Receive FRp
   3. IF (NHR is a reliable node)
      1. Check IR for black hole using DRI entry
      2. IF (IR is not a black hole)
      1. Route data packets (Secure Route)
      3. ELSE
      1. All the nodes along the reverse path from IR to the node that generated RREP are black holes.
   4. ELSE
      1. Current IR = NHR
      2. Send FRq to the updated IR's next hop router

Fig. 2 Algorithm for black hole detection

5. WORKING

This section discusses about working of the proposed black hole detection scheme. Once the DRI is formed it is used for a certain interval of time. After timeout the process is repeated. Fig. 3 shows an example scenario.

i) Let Router S wants to send a packet to router D.
ii) Router S broadcasts a RREQ.
iii) Now, S receives RREP from router B1 (RREP contains ID of NHR and its DRI entry for NHR).
iv) S checks its DRI table. If router B1 is reliable, it forwards the packet. If router B1 is found unreliable, it sends FRq to router B1's next hope neighbour i.e. router B[9], through router 1 and router [9].
v) FRq query for the DRI entry of router B1, its NHR i.e. 3 and if it has routed data packet to router 3.

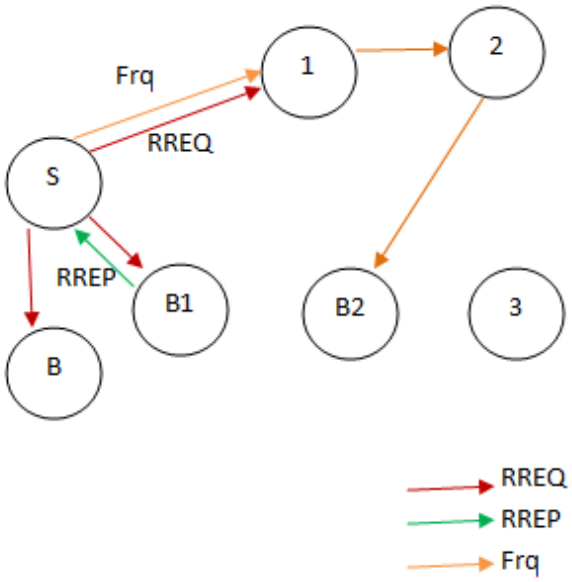


Fig. 3. Working diagram of DRI based IDS

vi) If router S has routed data through router 3 before, router 3 is reliable; otherwise, unreliable. If router 3 is reliable, source node will check whether B[9] is a black hole or not. If the second bit (i.e. IR has routed data through NHR of DRI) entry from the router B1 is equal to 1, and the first bit (i.e. NHR has routed data from IR of the DRI) entry from the router B[9] is equal to 0, IN is a black hole.

vii) If router B1 is not a black-hole and router B[9] is reliable node, the route is secured, and router S will update its DRI entry for router B1 with 01, and starts routing data via B1.

viii) If router B1 is a black-hole, the source node identifies all the nodes along the reverse path from router B1 to router S that generated the RREP as black hole nodes. S ignores any other RREP from the black holes and broadcasts the list of cooperative black holes.

ix) If router B[9] is an unreliable node, source node treats current router B[9] as IR and sends FRq to the updated IR's next hop node and goes on in a loop till the last hop count or till the destination is reached.

x) Since the routers are fixed, the DRI table can be used for a certain interval of time.

xi) Update will also occur when a new MR is added.

6. REFERENCES

[1] A. Prathapani, L. Santhanam, and D.P. Agrawal, "Intelligent honeypot agent for blackhole attack detection in wireless mesh networks", in Proc. of IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, pp. 753—758, 2009.

[2] N. Patil, "Service Discovery in Wireless Mesh Networks", Department of Information Technology, IIIT Allahabad, Allahabad, 2005. 22

[3] J. Wang et al. , "An Intrusion Detection System Approach for Wireless Mesh Networks Based on Finite State Machine". Draft available at: http://www.cs.ucla.edu/~wangzy/inestablishment/resource/IDS_draft.pdf (last accessed March 24, 2012)

[4] http://en.wikipedia.org/wiki/Intrusion_detection_system

[5] T. M. Chen, G.S. Kuo, Z.P. Li, and G.M. Zhu,"Intrusion detection in wireless mesh networks," Security in wireless mesh networks, Auerbach Publication, pp. 145-167, 2008.

[6] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon and K. Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks" in Proc. of International Conference on Wireless Networks, pp. 1-7, 2003.

[7] O. Shree, F. J. Ogwu, "A Proposal for Mitigating Multiple Black-Hole Attack in Wireless Mesh Networks", Wireless Sensor Network, vol. 5, no. 4, pp-76-83, 2013.

[8] R. Suryawanshi, S. Tamhankar, "Performance Analysis And Minimization Of Black Hole Attack In MANET", IJERA, vol. 2, no. 4, pp. 1430-1437, 2012.

[9] P. Rawat1, S. Goel, M. Agarwal3 and R. Singh, "Securing WMN Using Hybrid Honeypot System," IJDPS, vol. 3, no. 3, pp. 29-34, 2012.

[10] L. Santhanam, A. Mukherjee, R. Bhatnagar, and D. P. Agrawal, "A Perception based Classifier for Detecting Malicious Route Floods in Wireless Mesh Networks", in Proc. of the International Multi-Conference on Computing in the Global Information Technology, pp. 35, 2007.