International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Detection of Distributed Denial of Service Attack

Danveer Singh, Kalicharan Sahu

[1]PG Scholar, Computer Science and Engineering, Galgotias University, Greater Noida, U.P, India

[2]Assistant Professor, Computer Science and Engineering, Galgotias University, Greater Noida, U.P, India

Abstract: ***Availability is one of the three main objectives of computer security, along with confidentiality and integrity. Availability can be defined as the ability to use the information or resource desired. Denial of service attack is a most popular attack which effect the availability. In our research we mainly focus on the analyzing two denial of service attacks specially gray hole attack and black hole attack. Wireless networks mainly consist of both mesh clients and mesh routers. We constrain our analysis to mesh routers which are static. We have accept both black hole attack and gray hole attack in mesh routers and analysis the network without and with the presence of attack routers. We examines the delivery ratio of packets and observe how the network is affecting in the existence of an attack router by simulating the scenario with AODV protocol. By keeping the history of number packets transmitted and the number of packets received the algorithm defines the number of packets dropped and defines the probability of attack. We test our algorithm in the existence of an attack router and identify the attack router.***

Keywords: DoS, service, attacks, availability, security.

1. Introduction

Providing solution to the security challenges is a major research area in recent years. We are facing two broad categories of attacks such as passive attacks and active attacks. In the case of passive attack, the attackers simply analyze and listen to the network traffic with the objective of capturing sensitive information which can be used later to launch an active attack on the network [1]. Active attacks are which will directly damage the network bandwidth either by tampering, modification or just by dropping of packets. The three important features of a secure network are confidentiality, integrity and service availability [2]. Confidentiality is compromised by passive attacks, integrity by active attacks and availability by the most severe form of active attack on internet namely Denial of Service (DoS) attacks. Since WMNs is mainly used in long distance internet access and other applications which uses internet, DoS attack is treated as the highest security risk for this network, as DoS uses internet as a platform to be launched. Network layer is highly vulnerable to different DoS attacks due to multi-hop routing, as the number of hop increases the routing overheads increase. DoS attack in network layer can affect the routing mechanism or can degrade the network performance by exhausting the network resources[3]. DDoS attacks in network layer can be black hole attack in which a malicious node absorbs all the packets forwarded towards the target node and dropping those packets or dropping all the packets go through the malicious node or gray hole attack in which the malicious node selectively dropping some packets or randomly dropping some packets.

2. Problem Formulation

In this work we focus our attention to two special type of Denial of Service (DoS) attacks called gray hole attack or selective dropping attack and black hole attack or sink hole attack. We consider these attacks on the almost stationary wireless mesh routers. Gray hole attack is a type of attack in which the attack router accepts the packets and refuses to forward certain packets by just dropping the packets. In black hole attack the attack router will advertise in the network that it has a fresh route to the destination and after that may drop all the packets that it receives. Cryptographic techniques are used to protect the physically unprotected mesh routers from various DoS attacks including gray hole and black hole attacks. But if the router is compromised the attacker will gain access to the private/public key pair of the router and can break through the cryptographic systems. Thus non-cryptographic methods will provide a second line of defense [4]. In this work we try to develop a non cryptographic type of defense by checking the forwarding of the upstream routers by overhearing their transmission. We consider AODV routing protocol to implement these attacks. AODV protocol is one of the commonly used in wireless mesh networks and is proposed as one of the protocol in the IEEE 802.11s standard [5]. AODV is a reactive distance vector routing protocol which will establish the path only when the router has some data to send. AODV borrows the basic route establishment and maintenance mechanisms from the Dynamic Source Routing protocol (DSR) and the hop-to-hop routing vectors from the Destination-Sequenced Distance-Vector protocol (DSDV). To avoid routing loops AODV makes use of the sequence number in the control packets.

3. Simulation

In the simulation we used random dropping of packets using the random function. While the packets are sending to destination, packets are dropped randomly by the malicious node. Simulation of Gray hole attack and Black hole attack are done on NS-2.35. In order to simulate Gray hole attack and Black hole attack on NS2 we had to modify and implement the existing AODV protocol.

3.1 Implementing Gray Hole Behavior

Implementation of the gray hole attack is done in AODV protocol and simulated in NS-2.35. To show the gray hole behavior, one node is selected as attack node and it will drop packets randomly. The attack node should be able to participate in the AODV messaging. For this the new protocol which exhibits gray hole attack should be able to participate in AODV messaging. Implementation of the new routing protocol which perform gray hole attack is explained below.

All routing protocols in NS2 are installed in the ns-2.35 directory. We start by duplicating the AODV protocol in this directory and named the directory as "GAODV "(all the header files and classes of AODV directory are modified). All the files in the AODV directory are modified with GAODV such as *gaodv:cc*, *gaodv:h*, *gaodv rqueue:cc*, *gaodv rqueue:h* etc except for *aodv packet:h*. The new protocol will use the same aodv packets and thus its possible for the new GAODV protocol to send the same AODV packets. So we have changed all the names of classes, structures, functions in all the files except for the struct names that belong to the AODV *packet:h* code. By creating all this we have designed AODV and GAODV protocols to send packets with each other. To integrate the GAODV protocol to the NS2, two common files has to be modified. Since we are using the same packets used in AODV, we don't have to modify the common files related to packet. Thus we had to modify two files [6].

The first modified file is the *ns lib:tcl*. It's in this file the protocol agents are coded in a procedure. So here we had to add the protocol agent for the newly created GAODV protocol. When a node is using GAODV protocol this agent is scheduled at the beginning of the simulation and is assigned to the nodes which use the protocol.

```
Simulator instproc create-grayholeaodv-agent { node } {
set ragent [new Agent/grayholeAODV [$node node-addr]]
$self at 0.0 "$ragent start" ;# start BEACON/HELLO
Messages
$node set ragent_ $ragent
return $ragent
}
```

Figure 3.1: *ns lib:tcl* GAODV modification

```
grayholeaodv/grayholeaodv_logs.o
grayholeaodv/grayholeaodv.o \
grayholeaodv/grayholeaodv_rtable.o
grayholeaodv/grayholeaodv_rqueue.o \
```

Figure 3.2: *makefile:in* GAODV modification

The next file modified is the *makefile:in* in the root directory of ns-2.35. This file is modified for creating the object files for the cpp coded files. After all the implementations are ready, we have to recompile NS-2 again to create the object files.

3.2 Implementing Black Hole Behavior

Implementation of the black hole attack as a protocol is similar to that of gray hole attack implementation and the library changes are similar and we used the name BAODV instead of GAODV. The *gaodv:cc* file is modified such that instead of dropping packets randomly it will drop all the packets using if else condition and saved the file as *baodv:cc*.

4. Proposed Algorithm

When a node wants to send a packet it will send the RREQ packet and if it receives a route reply first from a normal behaving node, then everything will work fine. But if it gets reply from an attacker node in which implements selective dropping all the packets will not reach the destination. Some packets will be dropped by attacker node. If the selective dropping attack reduces the delivery ratio drastically an algorithm should be implemented to identify such nodes. A RREP from an attacker node can reach the source node earlier than a normal node if it is near to the source node or in other words the shortest path from the source to the destination. In this work we focus on developing an algorithm which focus on multiple dropping attackers in wireless mesh network and concentrate our study on the static routers which are present in hybrid wireless mesh networks.

In our algorithm at each mesh router, the router will maintain a packet count history of the number of packets it has forwarded to the downstream node. When a router forwards a packet to the downstream node, the number of packet sent (*Nt*) is incremented. When sent packet received by the destination the number of packets (Nr) is increased. If the packet forwarding is not heard within the time period the algorithm assumes that the packet is dropped by the downstream node. After that, the number of packets dropped (*Nd*) is calculated.

According to these observations each router will maintain a *PDR* value, which is obtained by the number of packets received by the downstream node (*Nr*) to the number of packets forwarded by the router to the downstream (*Nt*).
$PDRa = Nr / Nt$
The obtained *PDRa* value is compared with PDR value of gray hole attack (*PDRg*) and if *PDRg* is found in between 70% - 97% then a possibility of gray hole attack is identified.

When this condition fails *PDRa* is compared with PDR value of black hole attack (*PDRb*), and if *PDRb* is found in between 0% - 20% then a possibility of black hole attack is identified. If these conditions become true within the *interval* an attack is identified.

We have implemented the protocol which will implement gray hole attack in ns2. Now we have to do simulate the scenario to check whether the protocol is working properly or not. To test whether the implementation of GAODV and BAODV is working correctly or not we have created a scenario in which 21 routers are connected randomly and checked the data traffic when all routers are using the original AODV protocol.

After that two of the routers are set to use GAODV protocol and four routers are set to use BAODV protocol and compared the data traffic in both occasions. As expected the delivery ratio of data is decreased when we use GAODV and BAODV protocol.

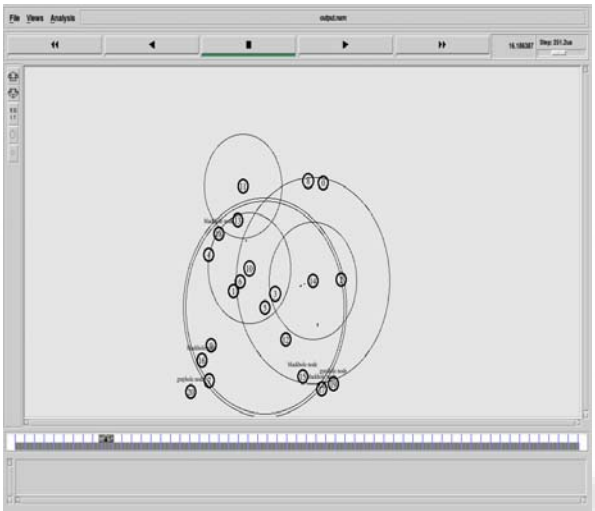

Figure 4.1: Simulation in NS2 without presence of any attack

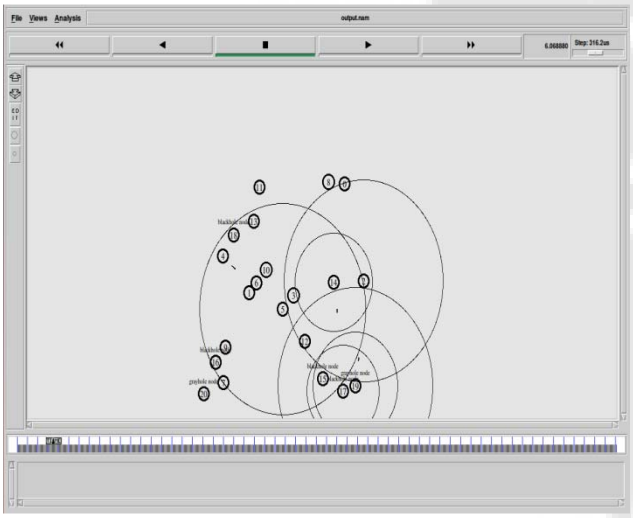

Figure 4.2: Simulation in NS2 with presence of Gray hole attack

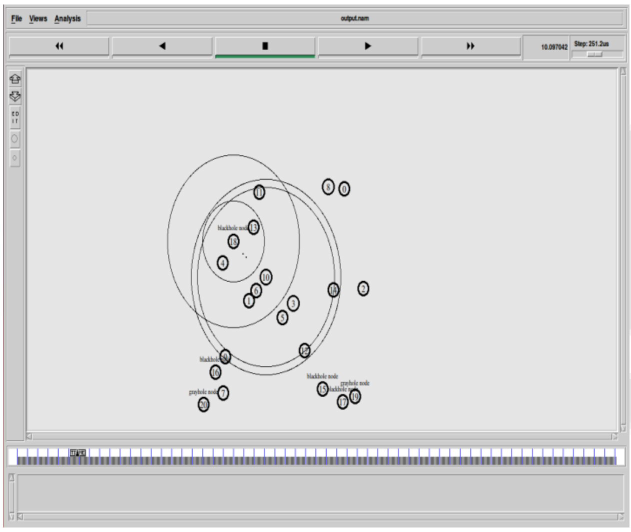

Figure 4.3: Simulation in NS2 with presence of Black hole attack

4.4 Simulation of the Proposed Algorithm

Previously we implemented both gray hole and black hole attack in ns-2.35 and obtained the results. Since we were not able to implement the promiscous mode of operation in ns-2.35 it become impossible to overhear the transmission of the neighbouring router. So we have written our algorithm in Perl language and using the trace files obtained during the previous simulation. Our algorithm will take the trace file as input. Since we are not using simulator for the evaluation of the algorithm, some assumptions are taken while evaluating the algorithm.

We assume that once the attack is detected by the neighboring routers, no time is required for the packet reporting the attack to reach the source and to establish a new path to the destination. This assumption is taken because once we detect the attack in the router we assume that all the remaining packets are routed towards the destination without any drop.

Table 4.1: Attack Table

Nt	*Nr*	*PDR*	*Nd*	*Attack Type*
4408	4408	100%	790	No Attack
4498	4256	94%	1040	Gray Hole Attack
2330	371	15%	2846	Black Hole Attack

5. Result of Simulation

First we simulated the network with no attack node and checked the delivery ratio of the data sent. Delivery ratio is the performance metric used and is the ratio of the data received by destination to the data sent which is expressed in percentage.

In the absence of attack the delivery ratio obtained in between 97% - 100%. Then we introduced a malicious node in the network which will implement gray hole attack and drop packets in a random fashion as explained earlier. Router 19 and 20 is selected as the gray hole attack router which is in the path of the transmission. Since the delivery ratio is calculated using the data received by destination nodes to the data sent by source nodes. As expected nodes drops some packets randomly and the delivery is decreased from 100% to a range of 70% - 97% .

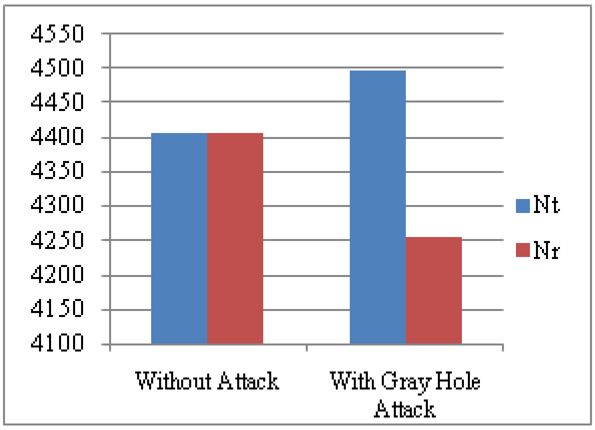

Figure 5.1: Comparison between delivery ratio of network with and without gray hole attack

Similarly we implemented the black hole attack to router 15 to 18 and checked the delivery ratio and the ratio was coming down from 100% to less than 20%.

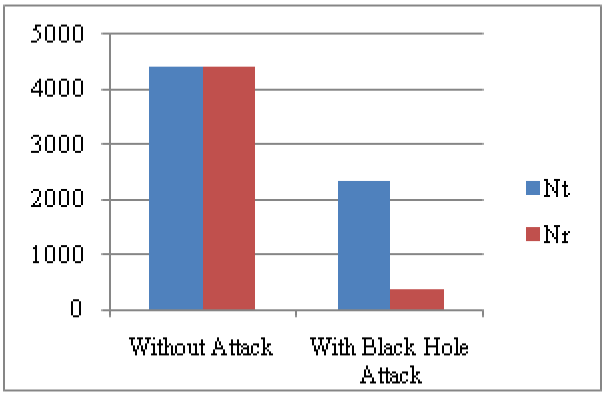

Figure 5.2: Comparison between delivery ratio of network with and without black hole attack

5.2 Comparison of Proposed Algorithm wth Cad Algorithm

Table 5.1: Comparison of proposed algorithm with CAD algorithm

CAD Algorithm	*Proposed Algorithm*
Attack detection is done by the source router	Attack detection is performed by packet delivery behavior of nodes in the network
Needs to sent extra packet to initiate the detection	Need to send extra packets only for the detection of Gray hole attacks in the network
Attack node is identified only if the source router demands	Attack is identified by the observation of misbehavior of nodes.
Threshold values are dynamic and thus changes according to channel behavior	Threshold values are dynamic and thus changes according to the network behavior
Detection doesnt depend on the data traffic through a node	Detection proves to be more effective when applied on heavy traffic scenarios
Works well under dynamic channel behavior	Works well under Ad-hoc network conditions

6. Conclusion & Future Work

In future we plan to find the appropriate threshold values in the presence of normal loses due to wireless channel and MAC layer collisions and to work on the attacks when the attack routers collude together.

Since routers in WMNs work in a fully wireless environment the packet can be lost due to different factors. So finding an appropriate threshold value for detecting the gray hole attack in real environment is really difficult. Wireless mesh networks is having an open architecture and more prone to Denial of Service attacks due to its use in broadband internet access. Thus more research work has to be done to reduce the Denial of Service attacks and improve the network.

References

[1] Shafiullah Khan, Kok-Keong Loo, Tahir Naeem, and Mohammad Abrar Khan, "*Denial of service attacks and challenges in broadband wireless networks*"

[2] Farzad Sabahi, "*Cloud Computing Security Threats and Responses*", 2011, IEEE

[3] en.wikipedia.org/wiki/Denial–of service_attack

[4] A. Prathapani, L. Santhanam, and D.P. Agrawal, "*Intelligent honeypot agent for blackhole attack detection in wireless mesh networks*", In Mobile Adhoc and Sensor Systems, IEEE 6th International Conference on, pages 753 –758, Oct 2009

[5] Myung J.Lee and Jianliang Zheng, "*Emerging standards for wireless mesh technology*", IEEE Wireless Communications, April 2006

[6] Monika, "*Denial of Service Attacks in Wireless Mesh Networks*", IJCSIT, Vol. 3 (3), 2012,4516-4522

Author Profile

Danveer Singh received the Bachelor Degree in Computer Science and Engineering in 2011 from Mangalayatan University, Beswan (Aligarh). He is currently pursuing the Master Degree in Computer and Engineering from Galgotias University, Greater Noida, U.P, India. His area of interest is Cloud Computing.

Kalicharan Sahu received M. Tech. degree in Computer Science & Engineering from JNU, New Delhi, INDIA & has done B.E. in Information Technology from M.I.T.S. An autonomous institute under R.G.P.V. Bhopal, India. He is currently on the designation of Assistant Professor in Computer and Engineering from Galgotias University, Greater Noida, U.P, India.