ISSN No. 0976-5697

Volume 2, No. 6, Nov-Dec 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Effect of Black Hole Attack and Prevention in Mobile Ad-Hoc Network

Shaista Anjum*, Sarita Singh Bhadauria
Department of Electronics,
Madhav Institute of Technology and Science, Gwalior, India
shaianjum14@gmail.com
saritamits61@yahoo.co.in

Abstract- A Wireless ad-hoc network is a temporary network set up by wireless mobile nodes moving arbitrary in the places that have no network infrastructure. However, due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. One of these attacks is the Black Hole Attack against network integrity absorbing all data packets in the network. Since the data packets do not reach the destination node on account of this attack, data loss will occur. Our aim to protect the Mobile ad-hoc network through Black Hole Attack, Intrusion Detection System aimed to securing the AODV protocol using our Intrusion Detection system. We conclude that AODV performs well at all mobility rates and movement speed. In this, the work has been extended and the proposed protocol is called IDSAODV (Intrusion Detection System AODV).We proposed an IDS solution to eliminate the Black Hole effects in the AODV network. We implemented the solution into the NS-2.And evaluated the results as we did in Black Hole implementation.

Keywords: MANET, AODV, Black-Hole Attack, NS2 and Intrusion Detection System.

I. INTRODUCTION

Wireless ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. In this way, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network in place of a network which collapsed after a disaster like an earthquake. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. To support this connectivity, nodes use some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) and DSDV (Destination-Sequenced Distance-Vector).

Besides acting as a host, each node also acts as a router to discover a path and forward packets to the correct node in the network. As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the Black Hole attack. In the Black Hole attack, which lead to dropping of messages. Attacking node first agrees to forward packets and then fails to do so. Initially the node behaves correctly and replays true RREP messages to nodes that initiate RREQ message. This way, it takes over the sending packets. Afterwards, the node just drops the packets to launch a (DoS) denial of service attack. Black Hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface. In any case, nodes in the network will constantly try to find a route for the destination, which makes the node consume its battery in addition to losing packets. In our study, we simulated the Black Hole attack in wireless ad-hoc networks and evaluated its damage in the network. We made our simulations using NS-2 (Network Simulator version 2) simulation program that consists of the collection of all network protocols to simulate many of the existing network topologies. . Thus, to simulate Black Hole attacks, we first added a new Black Hole protocol into the NS-2. We started our study by writing a new AODV protocol using C++, to simulate the Black Hole attack. Having implemented a new routing protocol which simulates the Black hole we performed tests on different topologies to compare the network performance with and without Black holes in the network. As expected, the throughput in the network was deteriorated considerably in the presence of a Black hole. Afterwards, we proposed an IDS solution to eliminate the Black Hole effects in the AODV network. We implemented the solution into the NS-2.And evaluated the results as we did in Black Hole implementation.

II. SECURITY ISSUES IN MANET

Vulnerabilities of operating systems and upper layer applications that belong to user programs such as databases, browsers or client-server applications are not considered as a security issue for ad-hoc networks. General attack types are the threats against the routing layer of the ad-hoc networks; such as physical, MAC and network layer which is the most important function of wireless ad-hoc network for the routing mechanism, orienting the packets after a route discovery process. Other vulnerabilities are application security, network security, database security which is studied in different works which are not explained in detail here. Attacks to the wireless ad-hoc network in the networking layer usually have two purposes: not forwarding packets or adding and changing some parameters of routing messages; such as sequence number and IP addresses.

III. VARIOUS TYPES OF ATTACKS

A. Passive Eavesdropping:

An attacker can listen to any wireless network to know what is going on in the network. It first listens to control messages to infer the network topology to understand how nodes are located or are communicating with another. Therefore, it can gather intelligent information about the network before attacking. It may also listen to the

information that is transmitted using encryption although it should be confidential belonging to upper layer applications. Eavesdropping is also a threat to location privacy [1]. An unauthorized node can notice a wireless network that exists within a geographical area, just by detecting radio signals. To combat this, traffic engineering techniques have been developed.

B. Selective Existence Attacks:

This malicious node which is also known as *selfish node* and which is not participating in the network operations, use the network for its advantage to enhance performance and save its own resources such as power. To achieve that, selfish node puts forth its existence whenever personal cost is involved. Therefore these selfish node behaviors' are known as *selective existence attacks* [2].

C. Gray-Hole Attack:

Gray-hole attack is an active attack type, which lead to dropping of messages. Attacking node first agrees to forward packets and then fails to do so. Initially the node behaves correctly and replays true RREP messages to nodes that initiate RREQ message. This way, it takes over the sending packets. Afterwards, the node just drops the packets to launch a (DoS) denial of service attack. If neighboring nodes that try to send packets over attacking nodes lose the connection to destination then they may want to discover a route again, broadcasting RREQ messages. Attacking node establishes a route, sending RREP messages. This process goes on until malicious node succeeds its aim (e.g. network resource consumption, battery consumption). This attack is known as routing misbehavior [4]. Dropping packets is also one of the behaviors' of failed or overloading nodes [1]. One should not evaluate every dropping packet action as a selective existence, gray or Gray-hole attack. Actually most routing protocols have no mechanism to detect whether data packets have been forwarded, DSR being the only exception [3].

D. Wormhole Attack:

In the wormhole attack an attacker uses a pair of nodes connected in some way. It can be a special private connection or the packets are tunneled over the Ad Hoc network. Every packet that one of the nodes sees is forwarded to the other node which in turn broadcast them out. This might create short circuits for the actual routing in the Ad Hoc network and thereby create some routing problems. Also, all the data can be selectively forwarded or not using this attack thereby controlling the Ad Hoc network to a large extent. This kind of attack together with a partitioning attack can gain almost complete control over the network traffic.

E. Dropping Routing Traffic:

It is essential in the Ad Hoc network that all nodes participate in the routing process. However, a node may act selfishly and process only routing information that are related to it in order to conserve energy. This behavior/attack can create network instability or even segment the network.

IV. LITERATURE SURVEY

A number of protocols were proposed to solve the black hole problem. It requires a source node to initiates a checking procedure to determine the reliability of any intermediate node claiming that it has a fresh enough route to the destination.

Payal N. Raj, Prashant B. Swadas [6] proposed DPRAODV (detection, prevention and reactive AODV) to prevent security of black hole by informing other nodes in the network. It uses normal AODV in which a node receives the Route reply (RREP) packet which first checks the value of sequence number in its routing table. The RREP is accepted if its sequence is higher than that in the routing table. It also check whether the sequence number is higher than the threshold value, if it is higher than threshold value than it is considered as the malicious node. The value of the threshold value is dynamically updated in the time interval. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. The node that is detected as the anomaly is black listed and ALARM packet is sent so that the RREP packet from that malicious node is discarded. The routing table for that node is not updated nor is the packet forwarded to others. Their solution increases the average end to end delay and normalized routing overhead.

Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park [7] proposed two different approaches to solve the black hole attack. The first solution the sender node needs to verify the authenticity of the node that initiates the RREP packet by utilizing the redundancy of the network. The idea of this solution is to find more than one route for the destination. The SN unicast the ping packet using different routes. The IN or destination node or malicious node will ping requests. The SN checks the acknowledgment and processes them to check which one is safe or having malicious node. In the meantime the SN buffered its packet until it found the safe route. When the route is identified the buffered packets will be transmitted to it. The drawback of the solution is the time delay. The second solution is to store the last sent packet sequence number and the last received packet sequence number in the table. It is updated when any packet is arrived or transmitted. When node receives reply from another node it checks the last sent and received sequence number. If there is any mismatch then an ALARM indicates the existence of a black hole node. This method is faster and more reliable and has no overhead.

Chang Wu Yu, Tung-Kuang, Wu, Rei Heng, Cheng, and Shun Chao Chang [8] proposed a distributed and cooperative procedure to detect black hole node. In this each node detect local anomalies. It collects information to construct an estimation table which is maintained by each node containing information regarding nodes within power range. This scheme is initiated by the initial detection node which first broadcast and then it notifies all one-hop neighbors of the possible suspicious node. They cooperatively decide that the node is suspicious node. Immediately after the conformation of black hole, the global reaction is activated to establish proper notification system to send warning to the whole network. The simulation result show the higher black hole detection rate and achieves better packet delivery.

Hongmei Deng, Wei Li, and Dharma P. Aggrawal [9] proposed a solution for single black-hole node detection. In this method, each intermediate node is used to send backs the next hop information when it sends back an RREP message. After getting the reply message, the source node does not send the data packets but extracts the next hop information from the reply packet and then it sends a Further- Request to the next hop to verify that it has a route to the intermediate node who sends back the Further reply message, and that it has a route to the destination node.

V. SIMULATION ENVIRONMENT

The MANET network simulations are implemented using NS-2 simulator [5]. Nodes in the simulation move according to a model that we call Random Waypoint Mobility model. Each node is then assigned a particular trajectory. The MAC layer protocol IEEE 802.11 is used in simulations with the data rate of 512 Mbps in UDP and of 1024 Mbps in TCP. The application used to generate is Constant Bit Rate (CBR) traffic and Internet Protocol (IP) is used as Network layer protocol. The performance evaluation, as well as the design and development of routing protocols for MANETs, requires additional parameters which is addressed in RFC developed by Internet Engineering Task Force (IETF). Table 1 show the simulation parameters when the number of Black Hole increases with the number of nodes.

In this study, the four performance metrics are used which is packet delivery ratio, routing load or overhead, packet dropped and throughput.

- ***a.*** ***Throughput*** is the measure of how fast we can actually send through network. The number of packets delivered to the receiver provides the throughput of the network.
- ***b.*** ***Packet Delivery Ratio:*** The ratio of the data packets delivered to the destinations to those generated by the CBR sources.
- ***c.*** ***Normalized Routing Overhead:*** The number of routing packets transmitted per data packet delivered at the destination. Each hop-wise transmission of a routing packet is counted as one transmission
- ***d.*** ***Packets Dropped****:* Some of the packets generated by the source will get dropped in the network due to high mobility of the nodes, congestion of the network etc.

$$\textbf{Packet loss} = \frac{\textbf{(Packets sent – Packets received)}}{\textbf{Packets sent}} \times 100$$

Table 1.Simulation Parameter

Number of nodes	30
Dimension of simulated area	800×600
Routing Protocol	AODV , black hole AODV , ids AODV
Simulation time (seconds)	100
Traffic type	CBR
Packet size (bytes)	1000
Number of traffic connections	20 , 8
Maximum Speed (m/s)	30

VI. SIMULATION RESULTS

In UDP analysis, the three cases has been taken in which it is shown that how many packets has been transmit, how many packets received and how many packets are dropped at the time of normal AODV, the same thing is analyzed at the time of Black-hole case and the time of IDS black-hole.
In TCP analysis, routing load analysis, PDF analysis and throughput analysis the same thing is analyzed at the time of normal AODV, at the time of Black-hole and at the time of IDS black-hole.
For all the simulations, the same movement models were used, the number of traffic sources was fixed at 30, the maximum speed of the nodes was set to 30m/s and the pause time was varied as 0,20, 40 ,60, 80 and 100 seconds.

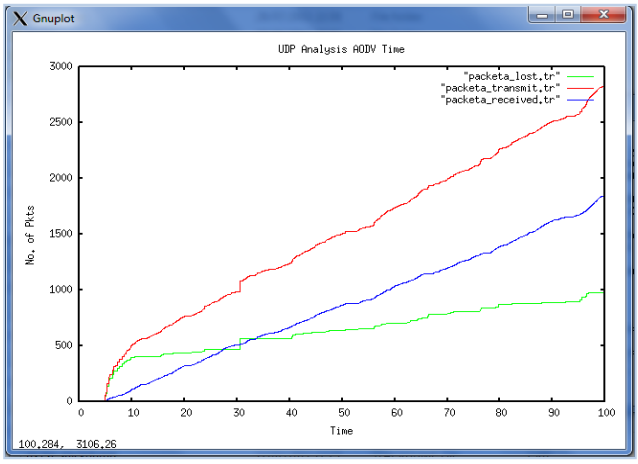

Figure.1

The Figure 1 shows the UDP analysis of normal AODV time, the total number of packets sends by the node is about 2880, the total number of packets received is about 1954 and the number of UDP packets dropped is 926.

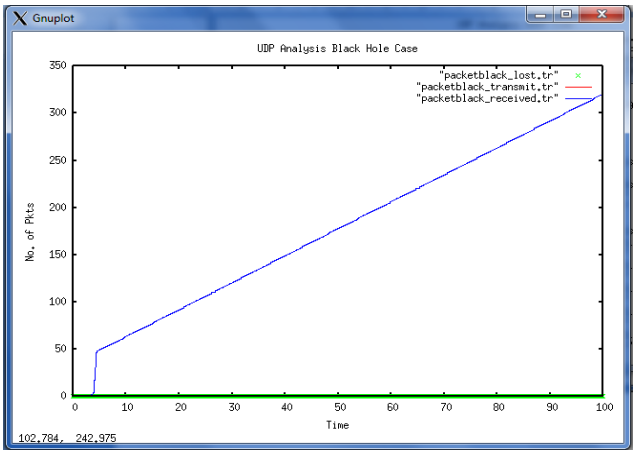

Figure.2

Here Result shows UDP Analysis in case Black hole Node present in our network, that time 340 packet transmit by transmitter node and 340 packet receive by the Black Hole Node, Genuine receiver can't be receive any UDP Packet.

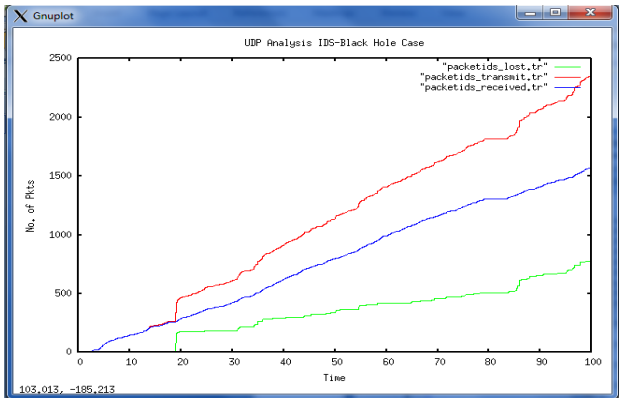

Figure.3

The Figure 3 shows the UDP analysis IDS and Black Hole node at the presence time, the total number of packets sends by the sender node number 18 and 20 is about 2457 packets, the total number of packets received by receiver 1579 and total number of UDP packets dropped by the two node i.e.18 and 20 is 840 packets. That means we conclude IDS Node Recover About 80 percent.

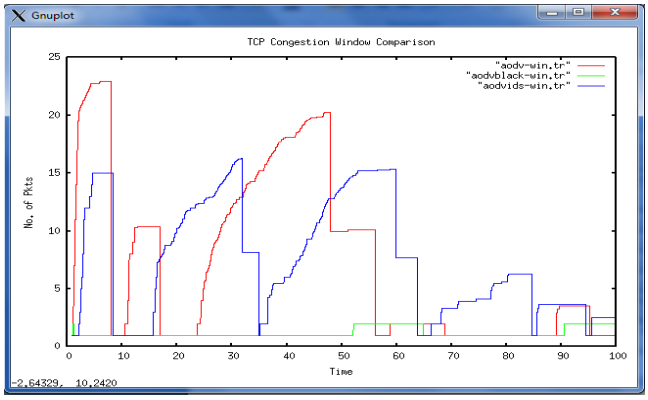

Figure.4

The Figure 4 shows the TCP congestion window comparison, the number of packets received is about 80-90% at the normal AODV time, the number of packets received at Black Hole time is about 10-20% and the number of packets received at IDS-Black-hole time is about 50- 60%.

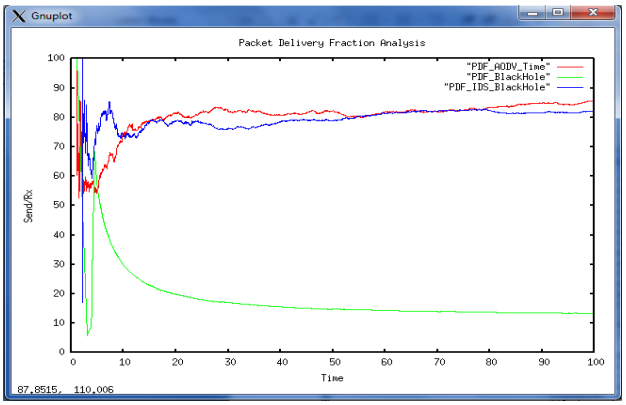

Figure.5

The Figure 5 shows the PDF analysis, at the time normal AODV the ratio of PDF is 85.6% which is shown by red line, at the time of Black-hole is 13.37% which is shown by green line and at the time of IDS Black-hole the ratio is 82.13% which is shown by blue line.

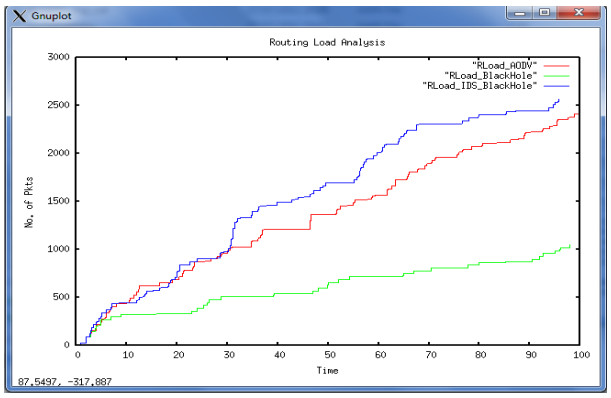

Figure.6

The Figure 6 shows the routing load analysis, in this the number of routing packets at the time of normal AODV is 2416 which is shown by red line, the number of routing packets at the time of Black-hole is 1051 which is shown by green line and the number of routing packets at the time of IDS Black-Hole is 2567 which is shown by blue line.

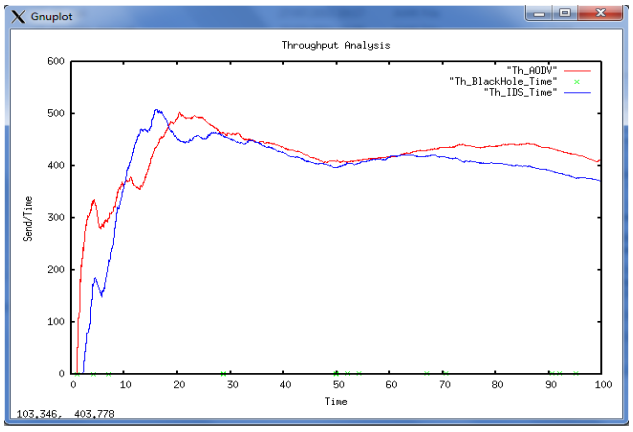

Figure.7

The Figure 7 shows the throughput analysis, throughput defines as how fast we can send through the network and at the time of AODV the number of packets delivered is 500 and at time of Black-hole none of the packets delivered and at the time of IDS Black-hole approximately 450 packets are delivered.

VII. CONCLUSION

In this study, we analyzed effect of the Black Hole in an AODV Network. For this purpose, we implemented an AODV protocol that behaves as Black Hole in NS-2. We simulated one scenario where each one has 30 nodes that use AODV protocol and also simulated the same scenario after introducing one Black Hole Node into the network. Moreover, we also implemented a solution that attempted to reduce the Black Hole effects in NS-2 and simulated the solution using the same scenarios. Our simulation results are analyzed above:

Having simulated the Black Hole Attack, we saw that the packet loss is increased in the ad-hoc network. In Appendix A and B , tables of simulation results show the difference between the number of packets lost in the network with and without a Black Hole Attack. This also shows that Black Hole Attack affects the overall network connectivity and the data loss could show the existence of the Black Hole Attack

in the network. If the number of Black Hole Nodes is increased then the data loss would also be expected to increase. It has been observed that in UDP analysis, that the number of packets lost at the time of normal AODV time is about 24.54%, at the time of Black-hole the number of packets lost is 95% and at the time of IDS-Black-hole is 35%.In TCP analysis, the number of packets lost at the time of normal AODV is 5.4%, at the time of Black-hole the number of packets lost extends up to 77.9% and at the time of IDS-Black-hole is 4.4%.

The same analysis has been done with different parameters such as routing load, packet delivery ratio and throughput. It has been calculated that number of packets lost at the Black-hole time is more and by adding IDS solution the recovery of packets of at least 50-60% is done means number of packets lost is less.

VIII. REFERENCES

[1]. P. Yau and C. J. Mitchell, "Security Vulnerabilities in Adhoc Network".

[2]. G. Vigna, S. Gwalani and K. Srinivasan, "An Intrusion Detection Tool for AODV-Based Ad hoc Wireless Networks", Proc. of the 20th Annual Computer Security Applications Conference (ACSAC'04).

[3]. D. Johnson, D. Maltz and J. Broch, "DSR the Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks". Ad Hoc networking, Chapter 5, page 139- 172. Addison-Wesley, 2001.

[4]. S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Ad Hoc Networks", Proc. 6th Annual Int'l. Conf. Mobile Comp. and Net., Boston, MA. pp. 255-265. August 2000.

[5]. Sukla Banerjee "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" Prceeodings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA

[6]. Payal N. Raj and Prashant B. Swadas,"DPRAODV: A dynamic learning system against black hole attack in AODV based Manet", International Journal of Computer Science Issues (IJCSI), Vol. 2, Issue 3, pp: 54-59, 2009.

[7]. Mohammad Al-Shurman and Seong-Moo Yoon and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks".

[8]. Chang Wu Yu, Tung-Kuang, Wu, Rei Heng, Cheng, and Shun Chao Chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks", PAKDD 2007 Workshops, pp. 538–549, 2007.

[9]. Hongmei Deng, Wei Li, and Dharma P. Agrawal,"Routing Security in Wireless Ad Hoc Network", IEEE Communications Magzine, vol. 40, Issue: 10, 2002

[10]. The network simulator ns-2, "www.isi.edu/nsnam/ns2".

[11]. Dokurer Semih, Erten Y.M. and Acar Can Erkin, "Performance analysis of ad-hoc networks under black hole attacks".

[12]. Saini Akanksha, Kumar Ashish, "Effect of Black Hole Attack on AODV Routing Protocol in MANET", IJCST, vol.1, issue 2, December 2010.

[13]. Saini Akanksha, Kumar Ashish, "Comparison between various black hole detection techniques in MANET" National Conference on Computational Instrumentation CSIO Chandigarh, INDIA, 19-20 March 2010.

APPENDIX-A

UDP Packet Analysis (Normal AODV Time)

Sender Node	Total udp Pkt Sends	Receiver Node	Total udp Pkt Receives	Drop Node	Total udp Pkt Drop
18	2179	3	188	1	1
20	278	10	1666	9	41
				17	30
				18	461
				20	61
				23	5
				26	2
Total Packet Sends	2457	Total Packet Receive	1854	Total udp Packet Drop	601

UDP Packet Analysis (Black Hole Time)

Sender Node	Total udp Pkt Sends	Receiver Node	Total udp Pkt Receives	Drop Node	Total udp Pkt Drop
18	2179	3	278	29	2136
20	278	10	43		
				Total udp Packet Drop	2136
Total Packet Sends	2457	Total Packet Receive	321		

UDP Packet Analysis (IDS-BlackHole Time)

Sender Node	Total udp Pkt Sends	Receiver Node	Total udp Pkt Receives	Drop Node	Total udp Pkt Drop
18	2179	3	136	1	129
20	278	10	1443	6	36
				16	1
				17	40
				18	571
				20	61
				29	2
Total Packet Sends	2457	Total Packet Receive	1579	Total udp Packet Drop	840

APPENDIX-B

TCP Packet Analysis (Normal Time)

Sender Node	Total TCP Pkt Sends	Receiver Node	Total TCP Pkt Receives	Drop Node	Total TCP Pkt Drop	Ack Node	Total TCP Pkt Ack	ACK Drop Node	Total TCP Ack Drop
0	378	7	931	0	21	0	330	1	3
2	327	11	304	2	11	2	284	2	2
5	555	12	268	5	22	5	495	7	32
6	288	19	353	6	8	6	223	8	3
22	946	21	533	7	4	22	899	11	8
25	263	24	220	8	4	25	214	12	39
				9	1			14	1
Total Packet Sends	2757	Total Packet Receive	2609	10	2	Total TCP ACK RX	2445	17	8
				14	5			19	23
				15	2			21	38
				17	7			23	4
				19	1			24	1
				20	8				
				22	7			Total ACK Drop	162
				23	2				
				25	27				
				27	11				
				29	3				
				Total TCP Packet Drop	146				

TCP Packet Analysis (Black Hole Time)

Sender Node	Total TCP Pkt Sends	Receiver Node	Total TCP Pkt Receives	Drop Node	Total TCP Pkt Drop	Ack Node	Total TCP Pkt Ack	ACK Drop Node	Total TCP Ack Drop
0	19	7	8	29	67	0	3		
2	27	11	6			2	6	Total ACK Drop	0
5	7	19	3	Total TCP Packet Drop	67	5	1		
6	6	21	1			22	8		
22	20	24	1			25	1		
25	7								
		Total Packet Receive	19			Total TCP ACK RX	19		
Total Packet Sends	86								

TCP Packet Analysis (IDS-BlackHole Time)

Sender Node	Total TCP Pkt Sends	Receiver Node	Total TCP Pkt Receives	Drop Node	Total TCP Pkt Drop	Ack Node	Total TCP Pkt Ack	ACK Drop Node	Total TCP Ack Drop
0	351	7	730	0	12	0	292	1	5
2	345	11	328	1	5	2	282	10	9
5	1342	12	151	5	19	5	1238	11	41
6	156	19	321	6	4	6	130	12	12
22	775	21	1322	7	10	22	730	15	5
25	309	24	279	9	6	25	269	19	22
				10	6			20	7
Total Packet Sends	3278	Total Packet Receive	3131	11	1	Total TCP ACK RX	2941	21	75
				14	3			24	11
				17	4			26	2
				20	7				
				21	6			Total ACK Drop	189
				22	37				
				23	1				
				25	24				
				Total TCP Packet Drop	145				