American Journal of Engineering Research (AJER)
e-ISSN : 2320-0847 p-ISSN : 2320-0936
Volume-02, Issue-10, pp-214-220
www.ajer.org

Research Paper Open Access

Analysis of Black Hole Effect and Prevention through IDS in MANET

Nisha[1], Simranjit Kaur[2], Sandeep Kumar Arora[3]
[1](ECE, S.S.C.E.T Badhani/ PTU, India)
[2](ECE, S.S.C.E.T Badhani/ PTU, India)
[3](ECE, LPU Phagwara/LPU, India)

Abstract: - A mobile ad hoc network (MANET) is an autonomous network. It is a collection of mobile nodes that communicate with each other over wireless links. From last few years, the interest in the area of Mobile Ad-hoc Network (MANET) is growing due to its practical applications and requirement of communication in mobile devices. In the comparison to wired or infrastructure-based wireless network, MANET is vulnerable to security attacks due to its fundamental characteristics, e.g., the open medium, dynamic network topology, lack of clear lines of defense, autonomous terminal, lack of centralized monitoring and management. There are various types of attacks in MANET which drops the network performance. Black hole attack is one of them. Ad hoc On-demand Distance Vector routing (AODV) is a popular routing algorithm MANET. In this paper we investigated the effects of Black Hole attacks on the network performance. In our work we simulated black hole attacks in Network Simulator 2 (ns-2) and measured the throughput, PDF and routing load in the network with and without a black hole. We also proposed a solution against black hole attacks using intrusion detection system (IDS).

Keywords: - *MANET, RP-AODV, Black hole attack, IDS.*

I. INTRODUCTION

Wireless network is the combination of mobile computer nodes or stations that are not physically wired. The main advantage of this type of network is communicating with rest of the world while being mobile or wireless. But disadvantage is their limited bandwidth, memory, processing capabilities and open medium [1]. Wireless networks consist two basic system models are fixed backbone wireless system i.e. infrastructure based network and Wireless Mobile Ad hoc Network (MANET) i.e. known as infrastructureless network. The infrastructure based networks uses fixed and wired gateways. The bridges for these networks are known as base stations which are responsible for coordinating communication between the mobile hosts (nodes). The other type of network is infrastructureless mobile network commonly known as an ad-hoc network. In this type of network the mobile nodes communicate with each other without any fixed infrastructure between them. An ad hoc network is a collection of mobile nodes that do not rely on a predefined infrastructure to keep the network connected. So all functioning of networks is dependent on the trust and co-operation between nodes. Nodes are the mobile systems or devices i.e. mobile phone, laptop, PDA (personal digital assistance), MP3 player or personal computer that is participating in the network. They can form arbitrary or dynamic topologies depending on their connectivity with each other in the network. Nodes are very helpful to conveying information about the topology of the network and share the responsibility of managing the network. Hence in addition to acting as hosts, each mobile node does the function of routing as well as relaying messages for other mobile nodes [2]. However, due to its inborn characteristics of dynamic topology, lack of centralized management security and limited physical security, MANET is vulnerable to various kinds of attacks than wired networks. As shown in figure 1, ad hoc network consist several home-computing devices including cellular phones, laptops, PDAs and so on. Communication can be done directly between nodes within its transmission range.

Most important networking operations include routing and network management [3]. There are many routing protocols that provide efficient routing in the network. Routing protocols can be divided into three classes i.e.

proactive, reactive and hybrid protocols, depending on the routing topology. Proactive protocols are basically known as table-driven routing protocol. In this each node maintains predetermined routing information. Examples of this type include DSDV, WRP and CGSR. Reactive protocol also known as source-initiated on-demand protocols, in contrary, do not periodically update the routing information. Whereas in reactive routing protocols, routes are established whenever it is necessary. Example of this type includes DSR, AODV, TORA SSR and ABR. Hybrid protocols have features of both reactive and proactive approaches. Example of this type includes ZRP. Security is a major concern in all kinds of communication networks, but ad hoc networks face the greatest challenge due to their inherent nature. As a result, there exist various kinds of attacks that can be performed on an Ad hoc network. [4]. In this work, we discuss one such attack known as Black Hole Attack on the widely used AODV (Ad -hoc On-demand Distance Vector) routing protocol in MANETs. A mechanism presented shows the method to detect & prevent from black hole attack in Mobile ad hoc network and also protection through black hole attack activity using intrusion detection system (IDS) in AODV routing protocol. Intrusion detection systems (IDS) are mainly used to detect and call attention to suspicious behavior.

The rest of this paper is organized as follows. In section II, we discuss the some related work for security of MANET by routing attacks. Section III, describes overview of AODV protocol. Section IV (A) we discuss Black hole Attack and in IV (B) describe solution to black hole attack. Section V presents the simulation environment. Sections VI discuss important results obtained in simulation. Section VII describes the conclusion of the paper and future work.

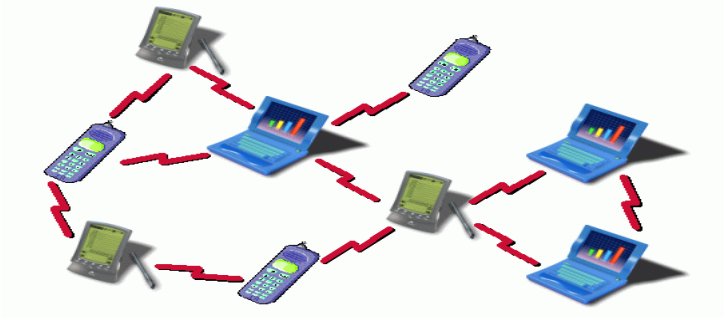

Figure 1: Wireless Ad-Hoc Network

II. LITERATURE REVIEW & RELATED WORK

The first intrusion detection model was developed in 1987 in which Denning proposed a model based on the hypothesis that security violations can be detected by monitoring a system check records for abnormal patterns of system usage [5]. In contrast to securing the routing layer of ad hoc networks, some researchers have also focused on simply detecting and reporting misleading routing misbehavior. In contrast to securing the routing layer of ad hoc networks, some researchers have also focused on simply detecting and reporting misleading routing misbehavior. Researchers have proposed solutions to identify and eliminate a single black hole node [1]. In [6], Marti, Giuli, Lai and Baker describe misbehavior detection and its effects. The paper presents two extensions to the DSR algorithm: the watchdog and the path rater. The watchdog identifies function of misbehaving nodes by listening promiscuously to the next node transmission. This technique is imperfect due to collisions in routes, limited transmission power and partial dropping. In [7], Sen et al. have presented a scheme for detection of malicious packet dropping nodes in a MANET. He provides a mechanism i.e. based on local misbehavior detection and flooding of the detection information in a controlled manner in the network so that the malicious node is detected even if moves out a local neighbourhood. In [8], black hole attack is mitigated by analyzing the destination sequence number in the RREP packet. If the destination sequence number in the RREP packet is higher than the destination sequence number at the source, then the node sent RREP packet is assumed to a malicious node. In [9], he proposes a modified protocol viz. MR-AODV based on our previous finding viz. R-AODV that eliminates limitations of existing mechanisms. MR-AODV isolates Blackhole and Grayhole nodes during route discovery phase as R-AODV and sets up a secure route for data transmission. In his simulation results prove that MR-AODV is a reliable solution which gives significant improvement in PDR with acceptable average end-to-end delay and normalized routing overhead under various network parameters and traffic conditions.

III. AODV-RP

In this paper we use AODV as the routing protocol. AODV is a reactive routing protocol and it is an adaptation of the DSDV protocol for dynamic link conditions [10]. Basically it has combined properties of both DSR and DSDV. It uses on-demand approach to find available routes, i.e. a route is established only when it is

required by a source node to transmit the data packets. AODV protocol operates in two phases: route discovery and route maintenance. It uses three types of control messages namely Route-Request (RREQ), Route-Reply (RREP), Route Error (RERR) are used for establishing and maintaining the routing path from source to destination. Route discovery process is used by node when the packet sender has no route to destination in its Routing Table. When the source node wants to make a connection with the destination node, it broadcasts an RREQ message over the network. This RREQ message received by neighbours or intermediate nodes of the source node. Each node receives a RREQ will check its Routing Table to see whether it has a path to the requested destination. It replies if there is one with RREP packet to source node. Source node receives multiple RREP packets via different paths. Source node selects fresher and shorter path among them to send the application data. If there is no route to destination, the RREQ is forwarded. Before forwarding, it keeps a reverse path to the source node in its routing table. The Routing Table records the route information of the next hop, the distance and the current highest sequence number it has seen. Route maintenance starts when its one hop neighbours go out of its range. Then the node invalidates a cached route. It is used to notify the source node or to trigger a new route discovery.

Sequence numbers are also used in the RREP messages. The sequence number is a 32-b it unsigned integer. When a node sends any type of routing control message, it automatically increases its own sequence number. Higher sequence number indicates more accurate information. When a node sends the highest sequence number, its information is considered most up to date and route is established over this node by the other nodes. So, more the sequence number means more is the freshness. A destination node updates its own sequence number either a node initiates a route discovery process or a destination node responds to RREQ with a RREP.

IV. BLACK HOLE ATTACK

A Black Hole attack [11] is a kind of DoS attack where a malicious node can attract all packets to pretend to have a fresh route to the destination and then absorb the network traffic and block data packets by dropping them. Black Hole nodes are difficult to find if they start using sequence number comparable to the current sequence number of networks. In Figure 2, we assume that Node M is the malicious node (Black Hole Node). Node S is a source node initiates route discovery by broadcast RREQ packet to all nearest neighbour. If this RREQ packet is received by malicious node M, it sends faked RREP packet by inserting high sequence number in the attention of having valid or fresh route. AODV-RP relies on sequence number to check freshness of the route. Then source gets deceived by the faked RREP packet and ignore all other replies from other nodes. The node S sends data packets in that route. The malicious node, instead of forwarding data to destination it simply drops. In this way black hole attack decrease the packet delivery percentage of the network significantly. In this work, to see the effect of an attack on the network we modify RP-AODV to BLACKHOLEAODV. In this we configure blackhole node to perform the attack in the network.

V. INTRUSION DETECTION SYSTEM

Intrusion detection is based in collection and analysis of system and network audit data. Upon detection, intrusion should be reported to security management. It continuously monitors activities like packet traffic. Each mobile node runs IDS independently to observe behaviour of neighbouring nodes, looking signs of intrusion locally, making decision to prevent the system from attack or it can also request for data and actions from neighbouring nodes if needed [12].

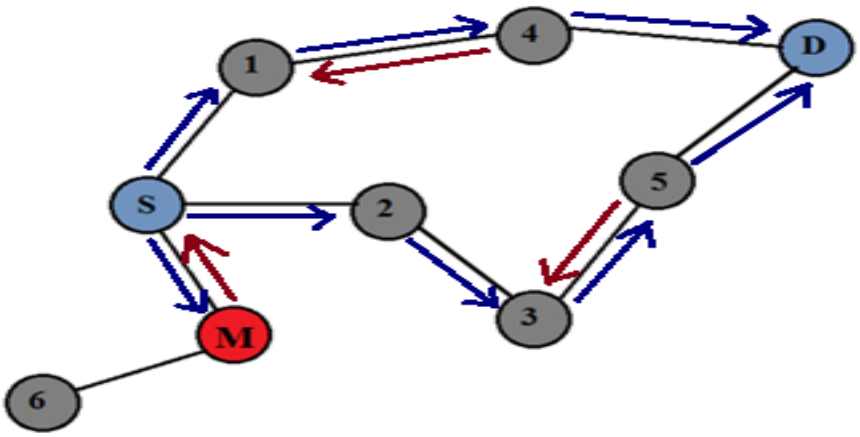

Figure 2: Black Hole Attack scenario

Intrusion detection systems in the Ad Hoc networks are divided into various categories from different viewpoints. The most important IDS systems are network based intrusion detection (NIDS) and host based intrusion detection (HIDS). In NIDS detecting attacks and malicious actions are done with the help of neighbouring nodes by their cooperation between each other. It runs on a gateway of a network and obtained audit data from traffic and then analyzed the data collected. In HIDS data acquires through hope rating system's log files that run on the node. In ad hoc network, a combination of the HIDS and NIDS can be used to discover attacks. This combination makes a powerful and distributed intrusion detection system. In this system, packets are exchanged in the network and also data collected from the network nodes are considered as a basis for intrusion detection.

As we know black hole attack is very difficult to detect than other attacks. To minimize the effect of blackhole node and improve the performance of network we use IDS and also modify RP-AODV to IDSAODV. As we see in III (A), black hole send an RREP message without checking the tables, it is more likely for the first RREP to arrive from the Black Hole. But with the help of IDSAODV Protocol it will check the RREP packet from Black Hole node for minimum path to destination and choose maximum destination sequence number. The IDSAODV Protocol will discard the first RREP packet from Black Hole node and choose second coming RREP packet from destination. The IDSAODV Protocol will also find another path to destination. To see the effect of IDSAODV, we configure the nodes as IDSAODV Protocol in our work and observed various performance parameters. We used same scenarios for IDSAODV as we used for normal RP-AODV and for Black hole attack to do the comparison.

VI. SIMULATION AND RESULTS

In this section, we describe simulation environment and simulation results.

6.1 Simulation Environment

We use NS-2 (v-2.35), a network simulation tool to simulate wireless and wired communication network. NS2 is discrete event simulator developed by the University of California in Berkeley. It provides a good platform for MANET simulation. We simulate our model for 20, 30 and 40 nodes. The random waypoint model is selected as a mobility model in a rectangular field (600 x 600 m^2). RP-AODV is used for simulation at network layer. Nodes send constant bit rate (CBR) traffic at varying rates over UDP connections. Each packet is of size 512 bytes. We have repeated the experiments by changing the number of node 20, 30 and 40 to see the performance of network under attacks. The simulation parameters are given in Table I.

Table I. Network Simulation Parameters

Parameter	Definition
Protocol	AODV, BLACKHOLEAODV, IDSAODV
MAC layer	IEEE 802.11
Simulation duration	500s
Node placement	Random
Simulation area	600m *600m
Size of data packet	512 bytes
Traffic sources	CBR/UDP
Number of nodes	20, 30, 40
Version NS-2	2.35

6.2 Result analysis

A simulation study was carried out to evaluate the performance of MANET in presence of attacks using metrics such as throughput, packet delivery ratio and normalized routing load.

6.2.1 Throughput

It is defined as amount of data transferred from sender to receiver in a given amount of time. It is measured in bits per second or packets per second. Throughput is calculated for the network in normal condition, then in the presence of the black hole attack and in the presence of IDS to improve the performance of network. Throughput values for 20, 30 and 40 nodes for normal AODV, BLACKHOLEAODV and for IDSAODV are plotted in X-graph as shown in figure 3.

6.2.2 Packet delivery function

Packet delivery fraction is calculated by dividing the number of packets received by the destination

through the number of packets originated by the application layer of the source (i.e. CBR source). It specifies the packet loss rate, which limits the maximum throughput of the network. The better the delivery ratio, the more complete and correct is the routing protocol. PDR is calculated by considering number of nodes 20, 30 and 40 for different routing protocols are plotted in graph as shown in figure 4. PDR characterize both correctness and efficiency of network. It is observed from simulation that PDR value of network in normal condition is higher than the network under attack but when we use IDS (intrusion detection system) in the presence of attack, the PDR ratio again rise. PDR values for 20, 30 and 40 nodes for normal AODV, BLACKHOLEAODV and for IDSAODV are plotted in X-graph as shown in figure 4.

6.2.3 Normalized routing load

Normalized routing load is the ratio between the total numbers of packets transmitted from routing layer of the source to the total number of packets received at the application layer of the destination. It characterizes the protocol routing performance under congestion. Normalized routing load values for 20, 30 and 40 nodes for normal AODV, BLACKHOLEAODV and for IDSAODV are plotted in X-graph as shown in figure 5.

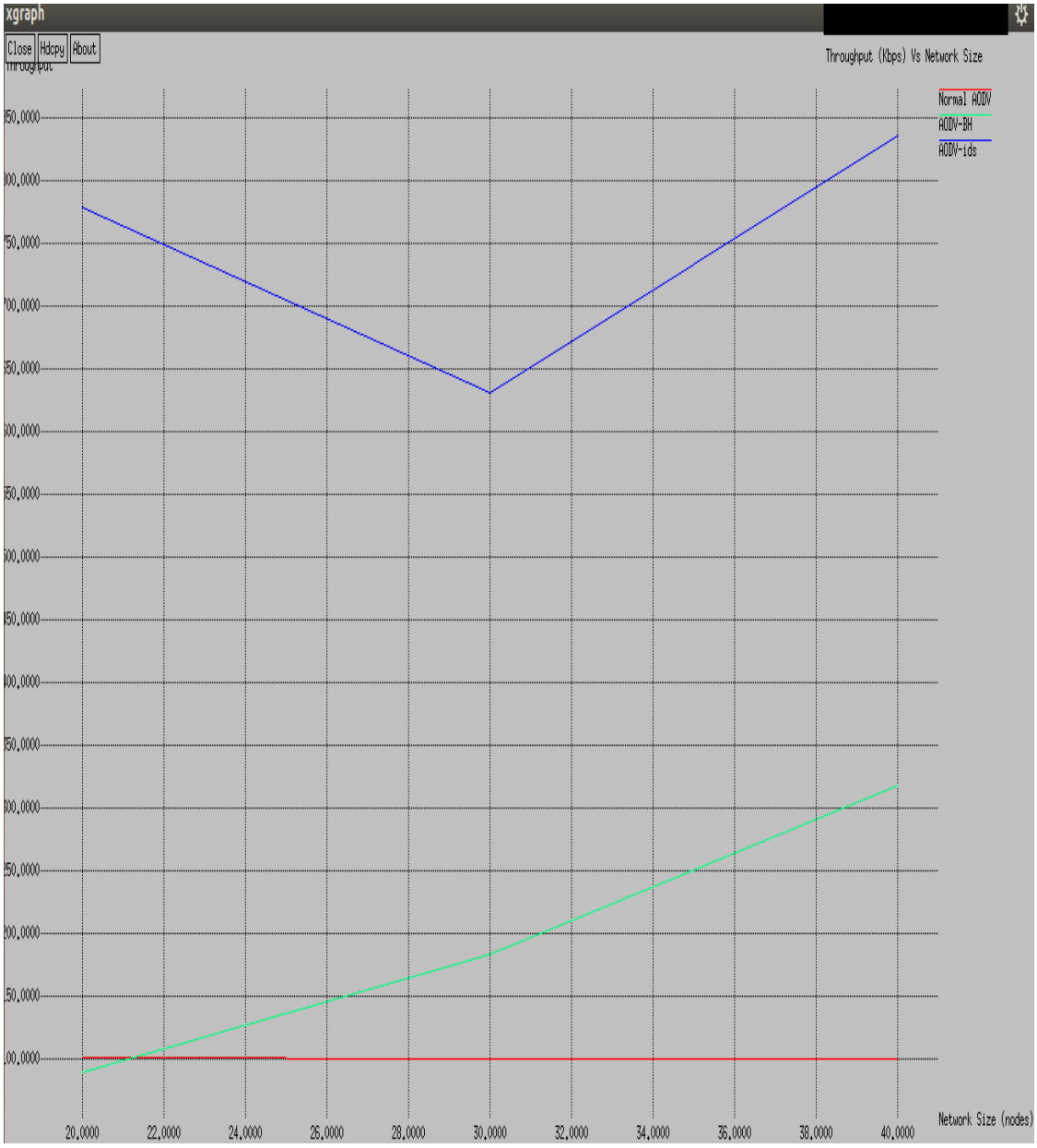

Figure 3: Throughput values for different routing protocols

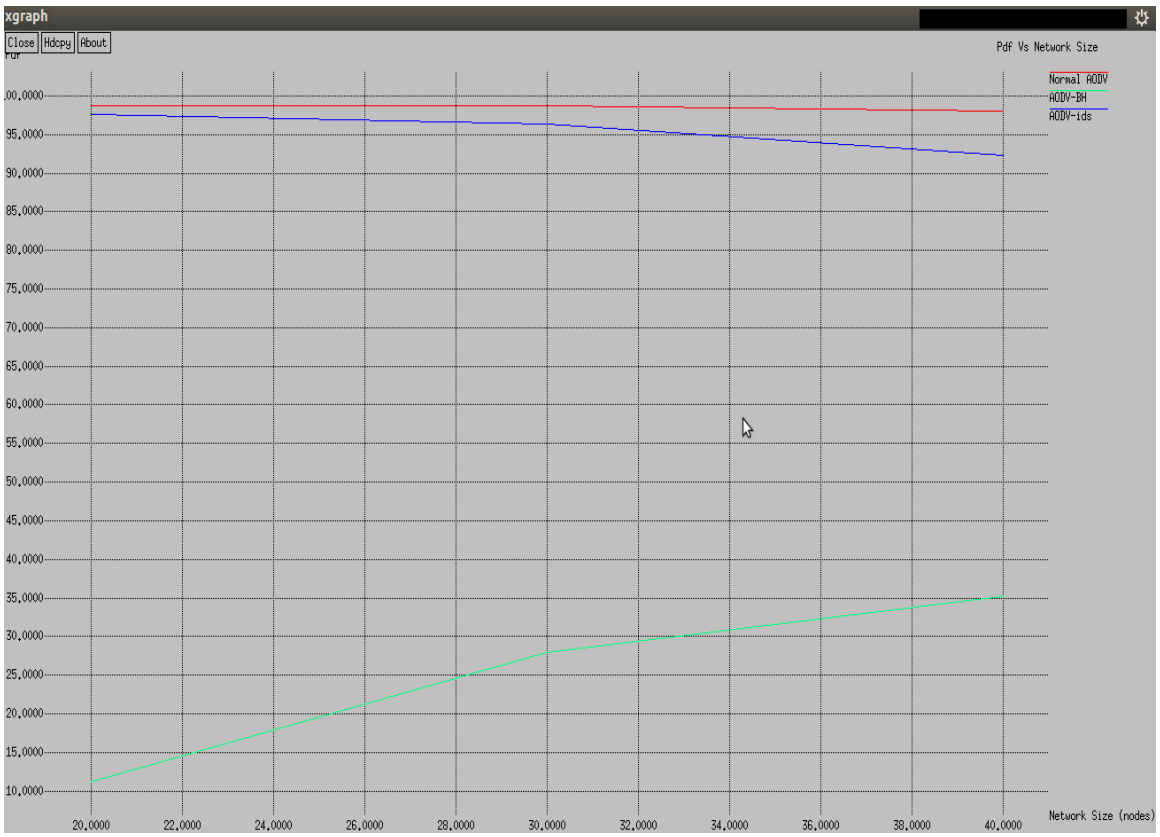

Figure 4: PDR values for different routing protocols

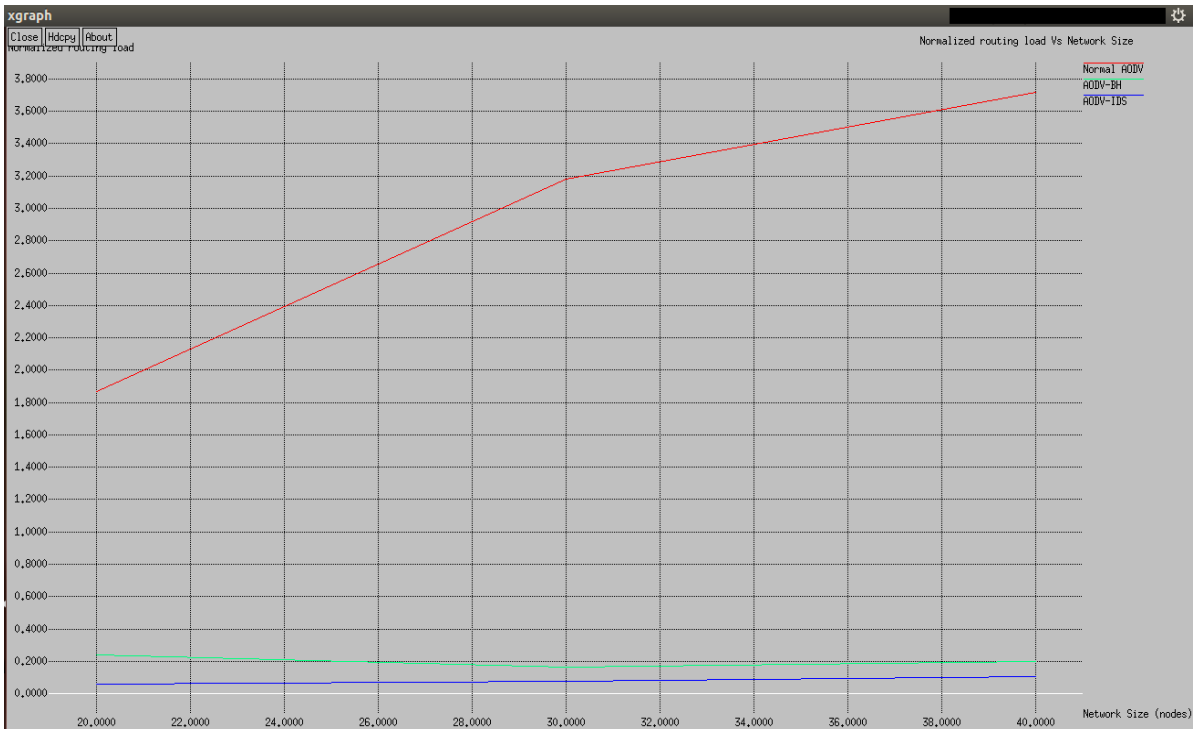

Figure 5: Normalized routing load values for different routing protocols

VII. CONCLUSION

In this paper we are discussed the routing security issues of MANETs. Black hole attack can easily deploy against the MANET. We introduced a black hole in each scenario and compared the performance of the networks with and without a black hole. We also introduced a prevention of black hole attack through IDS. For this we implemented an IDSAODV protocol. The observation and results shows that throughput increases in the presence of IDS. The PDF in the presence of black hole attack varies from 10% to 40% but when we used IDS to prevent the system from attack, the value rises and varies between 90 – 98%. The value for routing load increases in the presence of black hole attack but drops when we applied IDS. The advantage of using this approach is that IDSAODV does not require any additional overhead and require minimum modification in AODV protocol and other one is that it does not make any modifications in the packet format hence can work together with the AODV protocol.

REFERENCES

[1] Hongmei Deng, Wei Li, and Dharma P. Agarwal, "Routing Security in Wireless Ad Hoc Networks", University of Cincinnati, IEEE communication magazine, October 2002

[2] C.Siva S Ram Murthy and B.S.Manoj," Ad hoc Wireless Networks – Architectures and Protocols", Pearson Education, 2007.

[3] V. Karpijoki, "Security in Ad Hoc Networks", Seminar on Net Work Security, HUT TML 2000.

[4] Lidong Zhou, Zygmunt J. Haas, "Securing Ad Hoc Networks", IEEE network, special issue, November/December 1999.

[5] L. Prema Rajeswari, R. Arockia Xavier Annie, A. Kannan, "Enhanced Intrusion Detection Techniques For Mobile Ad Hoc Networks", Uk International Conference on Information and Communication technology in Electrical Sciences (ICTES 2007), Dec. 20-22, 2007. Pp. 1008-101.

[6] S. Marti, T. J. Giuli , K. Lai, and M. Baker mitigating routing Misbehaviour in mobile ad hoc networks. In mobile Computing and Networking (MOBICOM), Pp.255–265, 2000. Available on:citeseer.ist.psu.edu/marti00mitigating.html.

[7] J. Sen, M. Girish Chandra, P. Balamuralidhar, S.G. Harihara, and H. Reddy, "A distributed protocol for detection of packet dropping attack In mobile ad hoc networks", in Proceedings of IEEE International Conference on Telecommunications (ICT'07), May 2007, Penang, Malaysia.

[8] N. Mistry, D. C. Jinwala, and M Z averi, "Improving AODV protocol against black hole attacks, " Proceeding of International Muiti Conference of Engineers and Computer Scientists vol. II, IMECS 2010, pp. 1034-1039, Hong Kong, March 17-19, 2010.

[9] Rutvij H. Jhaveri, "MR-AODV A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs", Third International Conference In Advanced Computing & Communication Technologies (ACCT), pp.254 – 260, 6-7 April 2013.

[10] Charles E. Perkins, Elizabeth M. Belding- Royer, Samir R. Das, Mobile Ad Hoc Networking Working Group, Internet Draft, February 2003.

[11] Yi-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy May/June 2004.

[12] Niyati Shah and Sharada Valiveti, "Intrusion Detection Systems for the Availability Attacks in Ad hoc network", International Journal of Electronics and computer science engineering, Vol.1, pp.1850-1857.