Evaluation of Network Attacks and its Mitigation Techniques

R.Priyanka
ECE department
Mahalingam College of Engineering and Technology
Coimbatore, India

T.Subashri
ECE department
Mahalingam College of Engineering and Technology
Coimbatore, India

A.Gowshalyadevi
ECE department
Mahalingam College of Engineering and Technology
Coimbatore, India

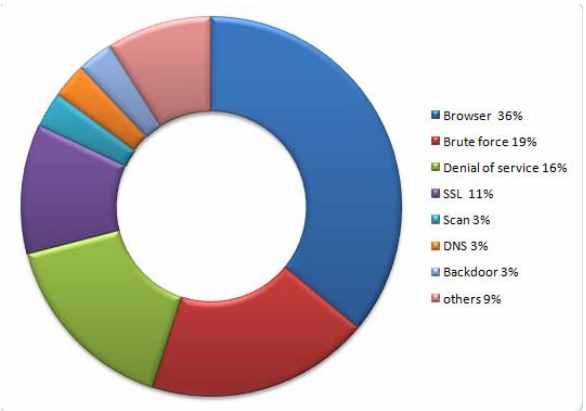
N.Sugirtham
ECE department
Mahalingam College of Engineering and Technology
Coimbatore, India

***Abstract*— Internet has become an infrastructure that affords the basis of highly networked information society. Moreover it has brought more convenience for the lives of people and has infiltrated general life deeply. As these two namely, internet and network applications are growing very faster, the delve for the desirable solution to offer the necessary salvation against the data infiltrator attacks along these services in time thrive faster. However, illicit computer access by malicious users is still a severe menace. This paper illustrates the mitigation techniques to subdue the one of the foremost denial of service network attacks namely cyber attack, black hole attack, jamming attack and flooding attack. A scenario is created and different attacks are implemented in that environment and mitigation techniques are applied to subdue these attacks. QoS parameters and performance metrics graphs are obtained. The proposed frameworks are implemented using the simulation tool OPNET version 17.5 RIVERBED MODELER.**

***Index Terms*— attacks, illicit, mitigation, salvation and RIVERBED**

I. INTRODUCTION

A Network is a cluster of computers, servers, network devices, mainframes, peripherals and other devices connected to one another that allow data to be share and used. A good archetype of a network is the Internet, which bind people all over the world [9]. It can be setup in a number of ways named as network topologies. Common configurations in the network are bus topology, ring topology, mesh topology, tree topology, star topology and hybrid topology. In computer networks, attacks is a endeavor to destroy, disable, expose, steal, alter or gain unauthorized access to or make illegal use of an asset[4]. An attack is usually carried out by someone with awful intentions to introduce calamity while others achieve penetration testing on organization systems to find out if all foreseen controls are placed. To employ against a business, the illicit can pick from a long list of various network attacking methods. Some types are more trivial in the networks, by knowing them; it is easier to prioritize the defenses. There is survey list below based on a chart from the 2016 McAfee Labs Threat Report which highlights the top 7 network attack types in 2016, based on data from millions of sensors across file, message, and web and network vectors.



Raziehmalekhoseini et al proposes countermeasures against syn flooding attack in the Next Generation Network (NGN) by applying a filtering and PSO algorithm to IP packets flowing from internet in to

NGN. Mitko Bogdanoski et al provide various countermeasures and simulation results regarding the effects of link failure recovery mechanism against ping flood dos attack. Nabie Y. Conteh et al discuss the role of social engineering in network intrusions and cyber-theft. They recommend some preventive measures and possible solutions to the threats and vulnerabilities of social engineering and supports to offer optimism by organizational education campaigns that social engineering attacks can be reduced. S.Suresh Kumar et al describes ways to provide security for various applications such as banking, education, public services as the vulnerabilities may happen by cyber-attacks. Authors used access controls, encryption, intrusion detection and honey pots as the countermeasures against cyber-attacks. Arif Sari et al proposes method for preventing and mitigating jamming attacks, implemented at the MAC layer that consist of a combination of PCF and RTS/CTS mechanisms. This mechanism minimizes the occurrence of collisions on the wireless network.H. A. Esmaili et al describes the effect of black hole attack on ad hoc network using AODV as a routing protocol. Simulation results show that packet delivery ratio in the presence of malicious nodes, reduces notably. TomislavShuminoski et al analyzed the effects of SYN flood attack are and they presented in OPNET simulation environment based on anomaly detection algorithms. Donna M. Gregg et al focuses on DoS attack such as Octopus, Snork, UDP Storm, distributed TCP SYN flood, and ARP Cache Poisoning and executed these attack models against a validated model of a target network. Mehdi Ebady Manna et al reviewed the state-of-the art of detection mechanisms for SYN flooding which is classified based on the router data structure, statistical analysis of the packet flow and artificial intelligence. Isha Sharma et al evaluate the performance of DSR Protocol under influence of black hole attacks and enhance its performance in MANET network for various parameters. Neeti Yadav et al improve the performance of mobile ad hoc networks under jamming attack by using CTS/RTS integrated approach. Nirali Modi et al propose algorithm by using the trust value which is used to identify the malicious node, after identifying this node it will be removed from the neighboring path and select the another path. Rajeev Raman et al proposes a novel idea for detecting jamming from jammer by using three parameters such as average request, variance and energy. Dilip Kumar D.P et al illustrate the advantages of selective squeeze in terms of network performance degradation and adversary effort by presenting two case studies such as selective attack on TCP and on routing. Saman Taghavi Zargar et al explore the scope of the DDoS flooding attack problem and attempts to combat it. They categorize the DDoS flooding attacks and classify existing countermeasures based on where and when they prevent, detect, and respond to the DDoS flooding attacks. Sylvain P. Leblanc et al represents a snapshot of the current state of the art in the simulation and modeling of cyber attacks. Here they discusses a number of simulations of cyber warfare, including live, virtual, and constructive simulations, that were found in the open literature and were conducted in the private sector, academia, and government. The rest of this paper is organized as follows. In section 2, discuss about cyber attack, section 3 discusses about jamming attack, section 4 discusses about black hole attack and section 5 discuss about flooding attack. In section 6 we explain the various simulation parameters, section 7 shows the results of every attack, and finally we conclude in section 8.

II. CYBER ATTACK

Cyber attack is a deliberate exploitation of computer information systems, computer networks, infrastructures and personal computer devices by either individual or whole organization by the various means of malevolent acts usually hail from a nameless source that either alters, steals or devastate a specified target by hacking into a susceptible system. These attack use malevolent code to alter the computer data, code or logic, resulting in disruptive consequences which can compromise data and lead to cyber crimes such as identity and information theft. Cyber attack is characterized as cyber terrorism and cyber warfare in different context. It can be range from installing spyware on PC to endeavors that destroy the infrastructure of whole nations. Cyber-attacks have become as sophisticated as the stunt sworn demonstrated. Cyber attacks are introduced against a state or an individual because of three main factors namely spectacular factor, fear factor and vulnerability factor [13]. Cyber security bulwarks the data and reliability of computing assets belonging to or connecting to network organizations. Its purpose is to defend those assets against all threat factors throughout the entire life cycle of a cyber-attack. First and foremost step is to detect and eliminate the intruder in the network environment. Unless adequate steps are taken to preserve data and conserve lateral movement, the recovery processes will not likely be triumphant. The mighty (ability) to detect and identify the source and assay the extent of a compromise is crucial part which rapids the

incident response, minimizing loss, mitigating exploited weaknesses, and restoring services. Early exposure of an incident can limit or even prevent possible damage to control systems and reduces the level of effort required to contain, eliminate, and restore affected systems [20]. Logging and auditing with host-level Domain Name Service (DNS) resolution capabilities are crucial for improving detection and determining the depth and breadth of any concession.

III . JAMMING ATTACK

Jamming attack thwart authentic users from accessing the channels or by disrupting the communication between a sender and a receiver. The jammer can choose to rupture selected control packets for a very short time and bring down the whole network. Such jammer, which jams the network with the help of the protocol, is termed as protocol aware jammers. The wireless networks are more vulnerable to Denial-of-Service (DoS) attacks [19]. Mostly jamming causes denial of service type attack to sender or receiver. The easiest plan for jamming a wireless network communication is to continuously endure unwanted information to the node where the server is overloaded. The network resource is inaccessible to its appropriate user by this attack[5]. Here the attacker always tries to forbid the message, that is sent by its target node and it points to the Denial-of-Service attack.

Jamming attacks affects the network in the sense that they prevent all kinds of information exchange. This problem remains an open problem in the communications field. To understand how a jammer attacks wireless networks and how to evade jamming to achieve efficient communication, we investigate three different aspects of wireless network jamming: 1) Types of existing jammers, 2) Jamming detection and countermeasure and 3) Protocols for localizing jammers. First, a network can be jammed in various ways using distinct types of jammers. To avoid jamming in networks, it is essential to know how a jammer works[8]. Simple solution to subdue this attack is to apply high transmission power on jammed channels rendering this jamming to be less of a menace. Another countermeasure of jamming is to use directional antennas instead of Omni directional antennas. However, none of existing detection or counteractant approach can address all types of jammers without giving false alarms[14]. Therefore, more research is essential for detecting and avoiding different types of wireless network jamming.

IV. BLACK HOLE ATTACK

Black hole attack is a deadfall routing layer attack in which data will not reach its intended recipient without informing the source. The transmission of packets on multiple nodes and dropping of packets is mostly accruing on routing layer. Routing protocol is targeted by the attack. This attack has a great influence on virtual mesh network [18]. It is mostly found in temporary networks which are difficult to find. It will cause dominant effect to the performance of mesh networks. In black hole attack, the sender node accepts the reply message from fault node and make smallest way to receiver node. Then sender node accepts the respond message from non-real node which is called fault node and transfers the packets. This type of attack is known as black hole attack [10]. In forwarding the packets from source to destination it is found that some packets are dropped without forwarding or just dumped. This is due to the black hole which is neighbour to the nodes in the mobile adhoc networks [7]. In this attack, the black hole node dumps all data packets, which is supposed to be forwarded. However, it participates devotedly in the route establishing process, which is initiated by other nodes so as to stay on the path of the connection. Such nodes are recognized from the simulation environment and the packet loss ratio is calculated. The throughput will be lower than that of the existing value due to the neighbour of black hole nodes [16].

V. FLOOD ATTACK

The flooding algorithm is quite easy to implement. Flood attack is similar to broadcasting that befalls when source packets are remitted to all the attached network nodes. It uses every path in the networks [2]. Flood attack is a denial of service attack that befalls when a plexus (network) becomes so weighed down with the packets initiating incomplete connection requests and the servers can no longer process the genuine connection requests [3]. Ping flood is a simple ddos attack where the attacker deluges the victim with ICMP Echo Request packets as soon as possible without waiting for replies. It is the most successful if the assailant has more bandwidth than the victim. The attacker hopes that the victim will retort with ICMP Echo Request packets, thus consuming both incoming bandwidth as well as outgoing bandwidth [1]. The size of the correctly formed IPv4 packet including the IP header is 65,535 bytes, including a total payload size of 84 bytes. Many antiquity computer systems simply could not wield ample packets and would crash if they received one. This flaw was easily exploited in

early TCP/IP implementations in a wider ambit of operating systems including Windows, Linux, Unix , Mac as well as network devices like printers and routers [6]. Since remitting a ping packet larger than 65,535 byte breach the Internet Protocol, assailants would generally remit malformed packets in fragments. When the victim system venture to reassemble the fragments and ends up with an oversized packet, memory overflow could occur and led to various system problems including crash. To avoid Ping attacks and its variants, many sites bulwark ICMP ping messages altogether at their firewalls. First, invalid packet attacks can be directed at any listening port like FTP ports and you may not want to bulwark all of these, for operational reasons. Moreover, by blocking ping messages, you prevent legitimate ping use .The smarter approach would be to selective block fragmented pings, allowing actual ping traffic to pass through unhindered. Incapsula DDoS Protection services intelligently and preemptively detect and filter out all abnormally large packets, even if they are fragmented, eradicate the threat of Ping of death and similar packet based attacks altogether.

IV. SIMULATION PARAMETER

Throughput: Throughput is the average rate of successful message delivery over a communication channel. It represents the total number of bits per second (bits/sec) forwarded from wireless LAN layers to higher level in all WLAN nodes of the network[17]. High throughput is always desirable in a communication system.

Delay: Represents the end to end delay of all packets received by the wireless LAN of all WLAN nodes in the network structure and forwarded to the higher level. A data packet may take longer time to reach the destination due to queuing and different routing paths.

Load: Represents the total load submitted to the wireless LAN layers by all high layers in all WLAN nodes of the network.

Traffic Sent: Total size of packets in bits that are generated and sent to lower layer by the source in one second.

Infected device count: This represents the number of infected device in the network over a period of time.

VII. SIMULATION

Cyber Scenario

In the cyber scenario, the two routers are connected to one another. Ethernet stations and Ethernet workstations are connected to the router via switches. One switch is connected to the system admin where scan and clean operation is specified. One router is connected to the attacker whereas another one to the server.1000 Base X links are used to connect all the objects, so that file sharing can take place between them.

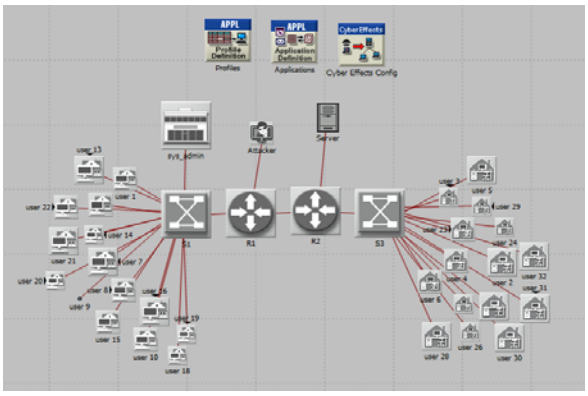


Figure 7.1 Cyber Scenario

After creating the above scenario, the parameters are to be altered in the above scenario to implement the attack and mitigation technique.

Jamming Scenario

In the jamming scenario, the server is placed in-between all the mobile workstation. Rx group configuration is placed to improve the network performance along with profile and application configuration. A jammer is introduced in the same scenario to implement the jamming attack.

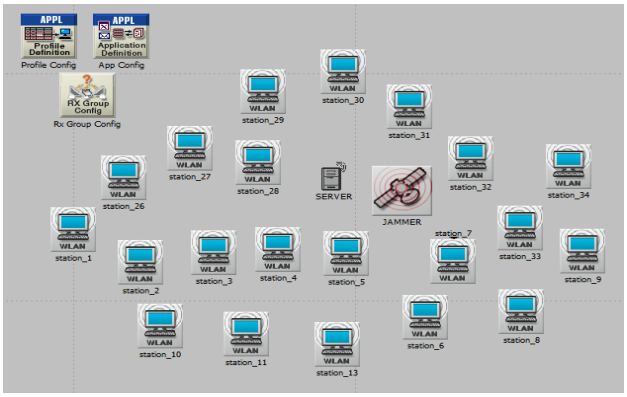


Figure 7.2 Jamming Scenario

In the above scenario, the following parameters are implemented to introduce and to recover that attack.

Black hole Scenario

In the black hole scenario, the server is placed in-between all the mobile workstation. Mobility configuration is placed to specify the mobility model along with profile and application configuration. An attacker is introduced in the same scenario to implement black hole attack on the network. Mitigation technique is employed to recover from the attack.

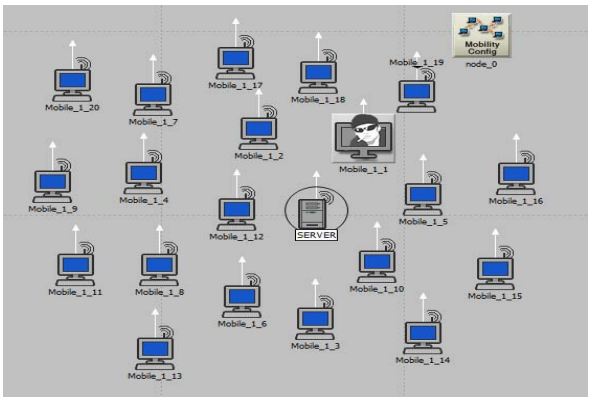


Figure 7.3 Black Hole Scenario

Flood Scenario

In the flooding scenario, the server is placed in-between all the mobile workstation. Rx group configuration is placed to improve the network performance along with profile and application configuration. A router is attacked by the three attackers and to subdue that attacks, the router is replaced by the firewall as shown in the figure 7.4.

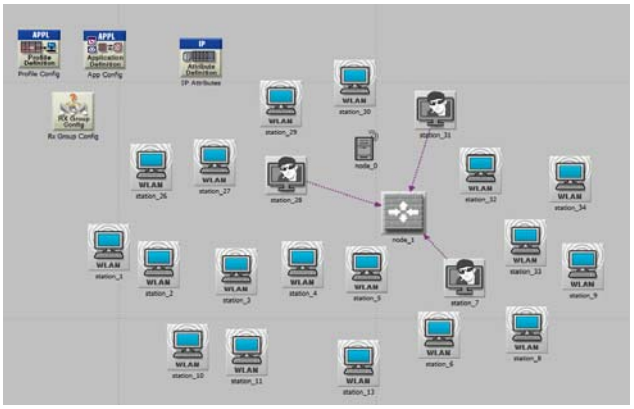


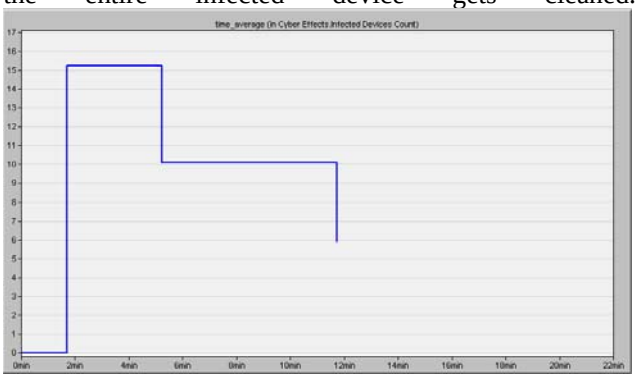
Figure 7.4 Flooding Scenario

VIII. Result

As mentioned various scenarios are created in this simulation using OPNET software and each scenario is simulated over a period of time. The output graphs for various parametric metrics are analyzed. The performance of the cyber, jamming and black hole attack are evaluated in this simulation based on the performance metrics chosen in global and node parameter. All the obtained graphs are compared against the performance metrics and results are obtained.

Cyber Infected Device Count

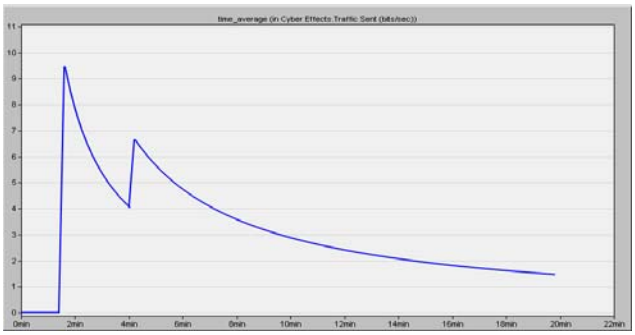
The figure 8.1 shows the graph of infected device count in the cyber scenario becomes higher when the attacker attacks (i.e.) during 100-110 seconds. The infected device count is stable until the scan and clean process gets started. It decreases during 300-310 sec when the scan and clean process started. At 700 seconds, the entire infected device gets cleaned.



Infected device Vs Time (min)
Figure 8.1 Infected device count

Cyber Traffic Sent-Attacker

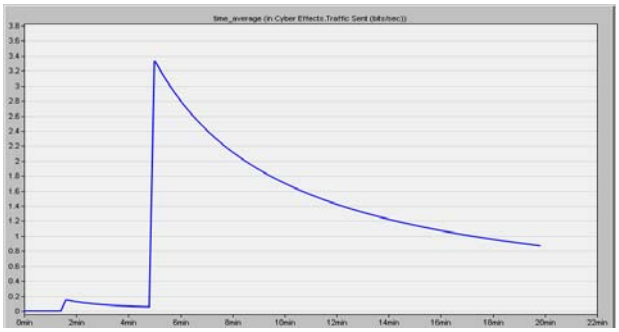
This graph shows the traffic sent by the attacker. As attacker is to attack the workstations during 100-110 seconds by sending packets. It is seen that the attacker has sent traffic to the nodes during 100-110 seconds as shown in the figure 8.2.



Traffic (bits/sec) Vs Time (min)
Figure 8.2 Traffic sent by Attacker

Cyber Traffic Sent-System Admin

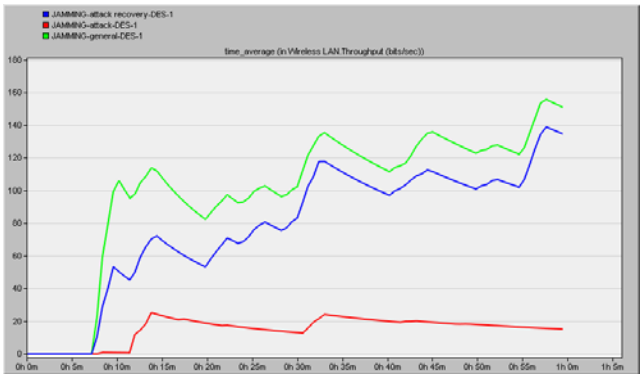
This graph shows the traffic sent by the system admin. As shown in the figure 8.3, system admin scans and cleans the workstations during 300-310 seconds. It is seen that it has sent some packets to the nodes during 300-310 seconds to clean all the infected nodes.



Traffic (bits/sec) Vs Time (min)
Figure 8.3 Traffic sent by System admin

Jamming Throughput

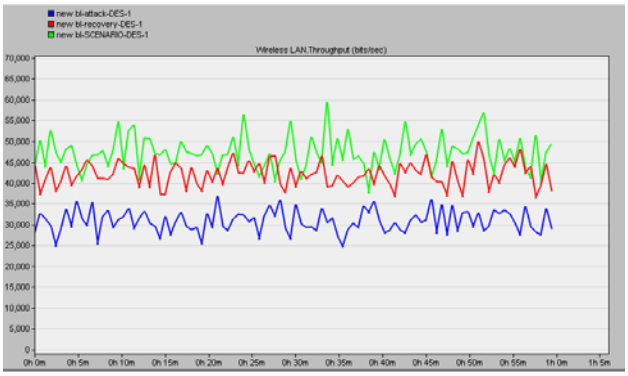
This graph compares three scenarios without attack, with attack and recovery of attack. It is seen clearly that the attack throughput is very less than the without attack throughput. It means the attacker degrades the network highly. The recovery throughput is not same as the without attack throughput but it is closer to that as shown in the figure 8.4.



Throughput Vs Time (min)
Figure 8.4 Jamming Throughput

Black hole Throughput

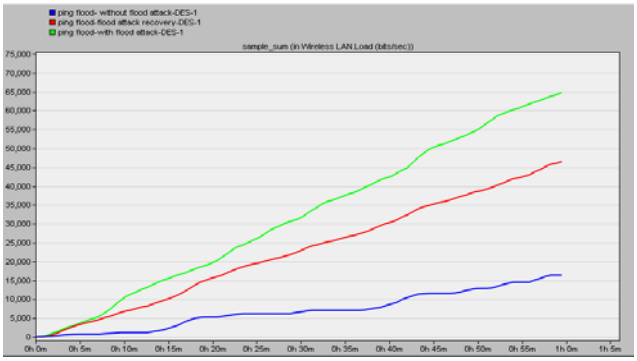
The figure 8.5 shows the graph which compares the three scenarios without attack and with attack along with the normal environment scenario. It is seen clearly that the attack throughput is very less than the without attack throughput, as the attack take place in the normal environment. It means the attacker degrades the network throughput performance highly. The recovery is managed to subdue the black hole attack.



Throughput Vs Time (min)
Figure 8.5 Black hole Throughput

Flood Load

The scenario where the flood attack is implemented is seemed to have a high load than others, because the attacker will send too many packets to flood the receiver. The recovery scenario load is lesser than the flood attack scenario, as there is a filtration of packets in the firewall as shown in the figure.



Load (bits/sec) Vs Time (min)
Figure 8.6 Flood Load

Delay Comparison

PARAMETER	Without Attack	With Attack	Attack Recovery
Jamming attack	0.00018	0.00083	0.00070
Black hole Attack	0.00072	0.00032	0.00068
Flood attack	0.00056	0.00080	0.00064

Table 8.1 Delay Comparison

This table 8.1 compares the delay of three attack's three scenarios without attack, with attack and recovery of attack. In both jamming and flood attack, the attacker delay is higher because the scenario is affected by the respective attacks and the attack recovery delay is also high compared to without attack as it takes some time to recover the attack made by the attacker. The without attack delay is always low as it is not affected by any external forces as shown in the table 8.1.But, in black hole attack, the concept is entirely different, the delay of the attack scenario is very low in contrast to other two attacks, as the attacker is pretending to have a shortest path when compared to all nodes in the environment.

IX. CONCLUSION

Security plays a very crucial factor in almost every field either it is an organization, a governmental entity, a country, or even in house. Computers, mobile devices, and internet are facing superfluent amount of security challenges day by day. Attacks that are catching the headlines can change significantly from one year to the next. The main goal of this project is to provide mitigation technique for some known existing attacks. In the network environment, attacks are insetted and mitigation techniques are also done to recover back the network to its normal state. Even though the attacks cannot be fully recovered, it is recovered to some good level in terms of throughput and delay which increases the network performance to a greater extent when compared with attacked environment.

Reference

[1] Aleksandar Risteski and Mitko Bogdanoski, "Wireless network behavior under ICMP ping flood DoS attack and mitigation techniques", *International Journal of Communication Networks and Information Security (IJCNIS)*, Vol.3, No.1,pp.17-24, April 2011.

[2] Aleksandar Risteski , Mitko Bogdanoski and Tomislav Shuminoski, "Analysis of the SYN flood DoS attack", *I. J. Computer Network and Information Security*, vol.8, pp.1-11, June 2013.

[3] Angela Amphawan and Mehdi Ebady Manna, "Review of syn-flooding attack detection mechanism", *International Journal of Distributed and Parallel Systems (IJDPS)*, Vol.3, No.1, pp.99-117,January 2012.

[4] Ankit Kumar and Priyanka Porwal, "Cloud Security Countermeasures against Distributed Denial of Service Attacks", *International Journal of Computer Systems*,ISSN: 2394-1065, Vol.2,Issue 11, pp. 494-499,November 2015.

[5] Arif Sari and Dr. Beran Necat,"Securing Mobile AD-HOC Networks Against Jamming Attacks Through Unified Security Mechanism", *International Journal of Ad hoc, Sensor & Ubiquitous Computing(IJASUC)*,Vol.3,pp.79-94,June 2012.

[6] David Tipper, James Joshi and Saman Taghavi Zargar, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks", *IEEE communication surveys and tutorials*,pp.1-24,February 2013.

[7] Debarati Roy Choudhury, Dr.LeenaRagha and Prof. Nilesh Marathe, "Implementing and improving the

performance of AODV by receive reply method and securing it from Black hole attack", *International Conference on Advanced Computing Technologies and Applications (ICACTA-2015)*, pp.564–570, March 2013.

[8] Dilip Kumar D.P and H. Venugopal, "Avoiding Selective Jam Attack by Packet Hiding Method in Wireless Sensor Network", *International Journal of Science and Research (IJSR)*, ISSN: 2319-7064, Vol.2, Issue 6, pp.324-328, June 2013.

[9] Donna C. Furnanage, Donna M. Gregg, David V. Heinbuch and William J. Blackert, "Analyzing denial of service attacks using theory and modeling and simulation", *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Academy*, pp.205-211, June 2001

[10] H.A.Esmaili, Hossein gharaee and M.R.Khalili Shoja, "Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator", *World of Computer Science and Information Technology Journal (WCSIT)*,ISSN: 2221-0741,Vol.1, pp.49-52, 2011.

[11] Hossein Soltani, MadiheSadat Yazdani and Seyed Hasan Mortazavi Zarch, "Attacks Simulation On Computer Networks By Simulator",*Journal of Engineering Computers & Applied Sciences(JECAS)*,ISSN: 2319-5606, Vol.3, No.6, pp.12-17,June 2014.

[12] Isha Sharma and Rajesh Kochher, "Performance Evaluation of Enhanced DSR Protocol under Influence of Black Attacks", *International Journal of Advanced Research in Computer and Communication Engineering*,Vol.4, Issue 12, pp. 313-318,December 2015.

[13] Nabie Y. Conteh and Paul J. Schmick, "Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks", *International Journal of Advanced Computer Research*,Vol 6(23), pp. 31-38,February 2016.

[14] Narendra Pal Singh Rathoren and Rajeev Raman , "A survey on energy efficient and secure infrastructure for MANET jamming attack", *International Journal of Engineering Trends and Technology (IJETT)* , ISSN:2231-5381, Vol.23, No.8, pp.388-390, May 2015.

[15] Navab Malekhoseini and Razieh Malekhoseini, "SYN flooding attack countermeasures in next generation network", *International Journal of Computer Science and Information Technology & Security* (IJCSITS), ISSN: 2249-9555, Vol.3, No.2, pp. 218-224, April 2013.

[16] Naveen Hemrajani and Swati Jain , "Detection and mitigation techniques of black hole attack in MANET:an overview, *International Journal of Science and Research (IJSR)*, ISSN: 2319-7064,Vol.2 , Issue 5, pp.70-73, May 2013

[17] Nirali Modi and Vinit Kumar Gupta, "Prevention of black hole attack using AODV routing protocol in MANET", *International Journal of Computer Science and Information Technologies (IJCSIT)*, ISSN: 0975-9646,Vol.5(3) , pp.3254-3258, 2014.

[18] Parminder Singh and Rupinder Kaur, "Blackhole and greyhole attack in wireless mesh network",*American Journal of Engineering Research(AJER)*,ISSN:2320-0936, Vol.3, Issue-10, pp.41-47,2014.

[19] Paru Raj and Pawani Popli, "Mitigation of Jamming Attack in Mobile Ad Hoc Networks", *International Journal of Innovative Research in Computer and Communication Engineering* ,ISSN: 2320-9798 ,Vol. 4, Issue 6,pp.10791 -10798, June 2016.

[20] S.Suresh Kumar and P.D.S.S.Lakshami Kumar, "A report on cyber security attacks and countermeasures", *International Journal of Advanced Computer Communications and Control*, Vol. 02, No. 03, pp.103-105,July 2014.

AUTHORS PROFILE

Priyanka Radhakrishnan, born in 1996. B.E pursuing candidate in Dr.Mahalingam College of Engineering and Technology from Tamil nadu,India.

Subashri Thirumalaisamy, born in 1995. B.E pursuing candidate in Dr.Mahalingam College of Engineering and Technology from Tamil nadu,India.

Gowshalyadevi Arjunan, born in 1995. B.E pursuing candidate in Dr.Mahalingam College of Engineering and Technology from Tamil nadu ,India.

Sugirtham N, born in 1983. Assistant professor in Dr.Mahalingam College of Engineering and Technology from Tamil nadu , India. Her main research interests include network security and cryptography.