International Journal For Technological Research In Engineering
Volume 5, Issue 10, June-2018 *ISSN (Online): 2347 - 4718*

ANALYSIS OF SECURITY ISSUE FROM DOS& DDOS ATTACK IN WSN THROUGH ENERGY CONSTRAINTS

Ankit Garg
M.Tech. (CSE), Neelam College Of Engineering And Technology, Agra

ABSTRACT: ***The growing popularity of wireless sensor networks increases the risk of security attacks. One of the most common and dangerous types of attack that takes place these days in any electronic society is a distributed denial of service attack. Due to the resource constraint nature of mobile sensors, DDoS attacks have become a major threat to its stability. In this paper, we established a model of a structural health monitoring network, being disturbed by one of the most common types of DDoS attacks, the flooding attack. Through a set of simulations, we explore the scope of flood-based DDoS attack problem, assessing the performance and the lifetime of the network under the attack condition. To conduct our research, we utilized the Quality of Protection Modeling Language. With the proposed approach, it was possible to examine numerous network configurations, parameters, attack options, and scenarios. The results of the carefully performed multilevel analysis allowed us to identify a new kind of DDoS attack, the delayed distributed denial of service, by the authors, referred to as DDoS attack. Multilevel approach to DDoS attack analysis confirmed that, examining endangered environments, it is significant to take into account many characteristics at once, just to not overlook any important aspect. We introduce the DOS and DDOS attack in WSN and calculate the energy level and number of dead node in time domain analysis over the successive iteration. This proposed energy depreciation form of network energy as the communication round increases. The level goes down and near the end scenario it tends to zero. Energy loss comparison earlier and proposed concludes that there is rapid decrement of energy loss after dos and DDoS attack on WSN. Hence abnormal decrement of energy tells that DOS and DDOS attack should be done on our network.At the end of simulation one another executed button on GUI which is the comparative result of earlier work of DoS and the proposed work. It has clear that the proposed work has much improver result than earlier work.***

Key Word: DOS, DDOS, WSN, MATLAB

I. INTRODUCTION

A DoS attack can be carried out either as a flooding or a logic attack. A flooding DoS attack is based on brute force. Real-looking but unnecessary data is sent as much as possible to a victim. As a result, network bandwidth is wasted, disk space is filled with unnecessary data (such as spam e-mail, junk files, and intentional error messages), fixed size data structures inside host software are filled with bogus information, or processing power is spent for unusual purposes. To amplify the effects, DoS attacks can be run in a coordinated fashion from several sources at the same time (Distributed DoS, DDoS).A logic DoS attack is based on an intelligent exploitation of vulnerabilities in the target. For example, a skillfully constructed fragmented Internet Protocol (IP) data-gram may crash a system due to a serious fault in the operating system (OS) software. Another example of a logic attack is to exploit missing authentication requirements by injecting bogus routing information to prevent traffic from reaching a victim's network. There are two major reasons that make DoS attacks attractive for attackers.

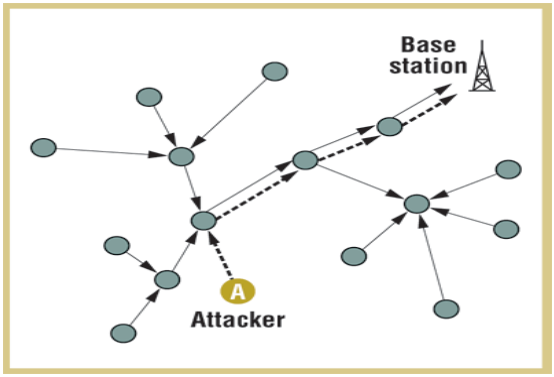

Fig 1.2: DOS attack in WSN

II. DISTRIBUTED DENIAL OF SERVICE ATTACK

An attempt to prevent or degrade availability of any resources by using multiple source hosts at the same time to send attack traffic. Typically the participants in a DDoS attack form a hierarchical DDoS network where an attacker controls a few masters (or handlers), which in turn control a much higher number of agents (or daemons or zombies or bots) to carry out a real attack against a victim. These are defined as follows.

- Agent (or daemon or zombie or bot): A compromised host used to send attack traffic in a DoS attack.
- Master (or handler): A compromised host used to control the operation of a large set of agents.
- DDoS network: A hierarchically structured set of masters and a gents to make it easier to control a DDoS attack by an attacker. DoS attacks may be either destructive or derivative.
- Destructive DoS attack: Prevents the availability of a resource completely.
- Degradative (non-destructive) DoS attack: Reduces the performance of a resource. A destructive DoS attack can, for example, crash a system or fill disk partitions. In these cases human intervention is typically needed for recovery. A degradativeDoS

attack will typically cause only temporary problems, and a system will recover automatically as soon as an attack terminates. An example of a degradativeDoS attack is a flooding attack overloading a network link or a host central processing unit (CPU). A prolonged high-bandwidth flooding attack, however, may have unexpected results, such as system crashes.

- Deployment phase: Installation of a malicious program on a set of compromised hosts to be used later as a source for DoS attack traffic.
- Attack phase: Coordinated transmission of attack traffic against a victim.

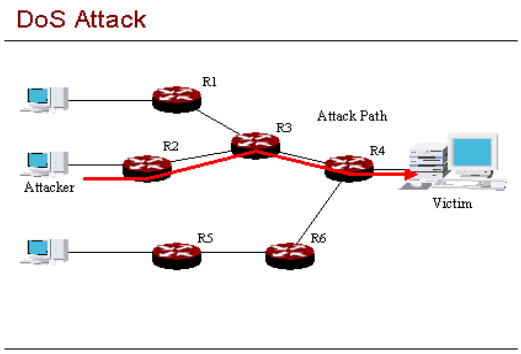

Fig 2.1: DOS attack through different routers

2. An Overview of DoS Attacks

Those who have been denial of service (DoS) attacks have proven to pose serious and continuing threats to consumers, organizations and infrastructure. The major reason of these attacks is to block access to specific resources, such as Web servers. Many defenses against Davies have been wished-for in the literature, but none provide reliable protection.

2.1 DoS Attacks in Real-Life

The actual DoS incident on the Internet from 1989 to 1995 was investigated. Three of the large amount typical impacts are as follows: 51% of incidents filled up disk, 33% of incidents degraded network services, and 26% of incidents were deleted. A single event can also lead to multiple types of damage (the sum of the percentages exceeds 100%).

III. RESEARCH PROBLEM

Defining DoS Invaders is particularly difficult due to the following problems. There has been much more to compare and contrast different ideas about DoS attacks and defense. Consequently, it is difficult to understand what the user's data needs to do and reduce the risk of Davis attacks. There are no effective defense mechanisms against many important DoS attacks.

3.1 Research Investigation

This study is designed to help all network users to mitigate DoS attacks and DDoS attacks in IP-based networks. This article focuses on the following aspects. We should understand the existing attack mechanisms and available defense mechanisms and have a rough idea of the benefits of each type of defense mechanism (at best). People should recognize the possible situations in the defense mechanism and can choose the most appropriate defense when several defense mechanisms for a specific attack type are available.

3.2 Research Methodology

The research method used in this definition is largely based on different situations of attack, but measuring, calculating statistics based on sports ideas and description of demand is also used in books. The used search method will be described in detail in this paper to describe each donation.

IV. PROPOSED WORK

The work offered under the LEACH and CBCR protocols contains defense mechanisms against the Davis attacks in WSN. There is a very relevant question that has not yet been discussed. It is possible to ensure that any defense mechanism should apply to an organization or user to reduce these attacks. This is primarily risk management responsibility, as this article has been stressed in the past. However, there are many practical problems in risk management to achieve the highest level of security. Other relevant issues have not yet been agreed, the results of directions and mathematical modeling are reliable. The following three sections will discuss these issues. At the end of this article, focus was on improving the following problems in the literature survey.

4.1 Detection Algorithm for DOS and its distributed form in WSN.

Step 1: Source code (SN) sends a restricted IP (RRIP) request to the backbone code (BBN).
Step 2: On receipt of the restricted IP address (RIP), it sends from RNN RREQ for the destination as well as RIP simultaneously and awaits response (RREP)
Step 3: When you receive RREP, each node passes RREP to the sender to the RREP nodes with the nodes contained in the Harmful Node and Blacklist table that are held at each node in the network. If the nodes in RREP do not match the entries in the two tables, RREP is forwarded to the sender node S.

Removal process: Step 1: If RREP is received only to the destination and not to the limited IP (RIP), the node performs the normal function by sending data via the route.
Step 2: If RREP is received during the review period, it initiates the black hole / DDoS detection process by sending a request to BBN to enter promiscuous mode
Step 3: BBN now starts monitoring the nodes in the RREP path and sends a PMODE_ON message to the sender node to announce that the promiscuous mode is ON for BBN.
Step 4: When you receive the PMODE_ON message from BBN, the sender node S sends a dummy packet via the same route run (RREP) for destination D.
Step 5: BBN Assign all neighbors of Nrrep (by node send message reply to S) to vote for the next node to which Nrrep forwards packets derived from S and is intended for D.
Step 6: Upon receipt of node ID from neighbors to Nosepiece, BBN selects the next node as Nero forwards the

package based on reported reference accounts.
Step 7: If the dummy packet is sent to the next node in the path, which is the same node as the selected node, we replace the selected node as the Nrrep node and we verify the next node for the new Nrrep node using neighbors of new Nrrep.
Step 8: About the selected node is a zero point, Nrrep is missing all packages. We cross verifying the malicious behavior of the selected node while dropping dummy packages with the same node in the network.
Step 9:Upon detection of malicious node, its node ID is sent to the remaining nodes on the network including the sender node. The other nodes in the network then add this malicious node device to the harmful node table held at each node on the network and its bill is set to S.

4.2 DoS and DDoS in LEACH Protocol

LEACH Low-Energy Adaptive Clustering Hierarchy uses collection shapes to access data and transfer to the base channel. Supports sensor flow sensor to WSN by adding important membership to the LEACH protocol. Packaging loss and power consumption in this protocol, however, were higher. It is designed to support movement of apps where understandable nodes are integrated with mobile numbers. Specifies the membership as it moves, and ensures that sensory tracks can communicate with a particular header. This protocol consists of two sections, one of which is the input category and the other relevant national level. During the installation phase, each sensor node selects the appropriate collection of headings according to the signal power detected, and then sends a message to the headset.LEACH Low-Energy Adaptive

4.3Simulation Parameters

Parameter	Value
Network Size	(100, 100, 50, 175)
Number Of Sensor Nodes	100
Sensor Node Deployment	100
Percentage Of Cluster Head	0.1
Energy.aggr =	5*0.0000000010
Energy. Free Space	10*0.0000000000010
Total energy	0.50
Energy. Multipath	0.0013*0.0000000000 010;
Energy Transmitted	5*0.0000000010
Energy. Receive	50*0.0000000010;

V. SIMULATION LAYOUT AND EXECUTION RESULT

Below is the figure after the implementation of MATLAB. The simulation runs on MATLAB2013b and the results are shown below, which clearly justifies the proposed scenario and techniques.

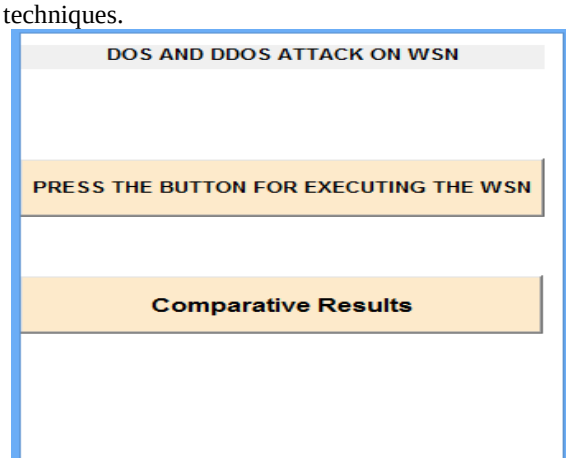

Fig 5.1: Basic layout constructed in MATLAB 2010 that has two buttons.

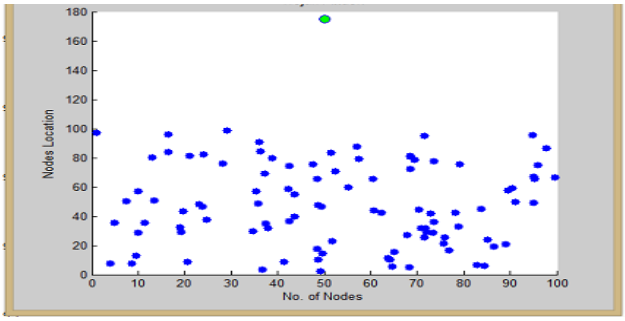

Figure 5.2 –No. of nodes 100 for Malicious Attack Using AODV protocol.

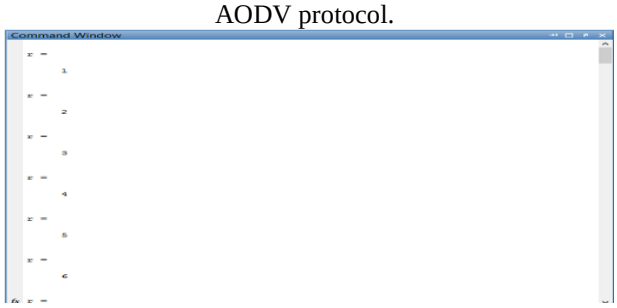

Figure 5.3 –No. of Rounds from 1 to 6 which is shown here for Malicious Attack.

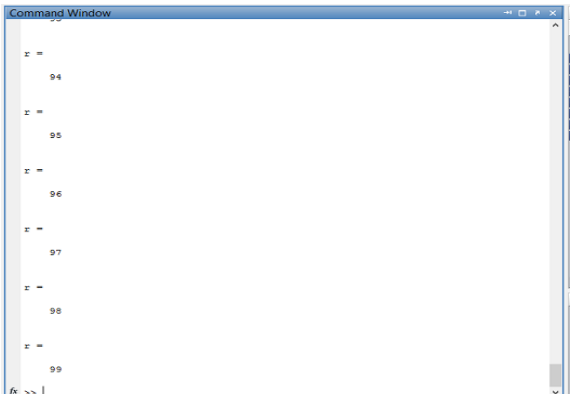

Figure 5.4 - No. of Rounds from 94 to 99 which is shown here for Malicious Attack (Total No. of Rounds 99)

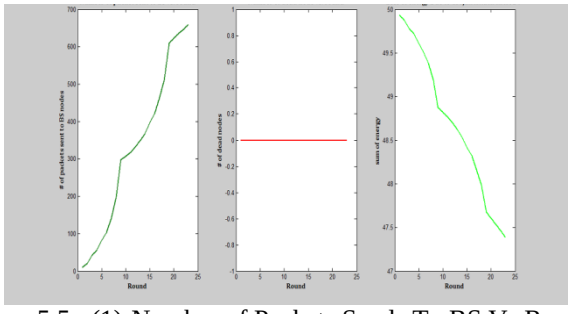

Figure 5.5: (1)-Number of Packets Sends To BS Vs Rounds (2) Number of Dead Nodes vs. Round (3) Loss of Energy Due to Malicious Attack in Different Round

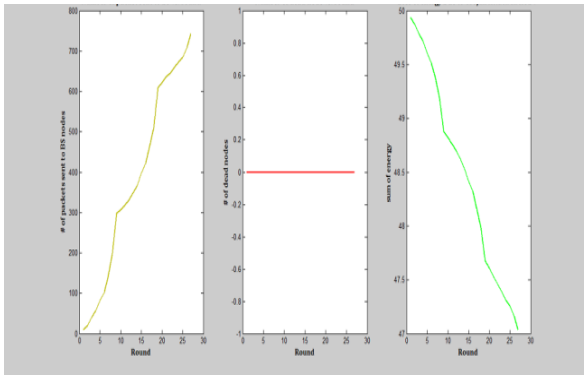

Figure 5.6: (1)-Number of Packets Sends To BS Vs Rounds (2) Number of Dead Nodes vs. Round (3) Loss of Energy Due to Malicious in Different Rounds

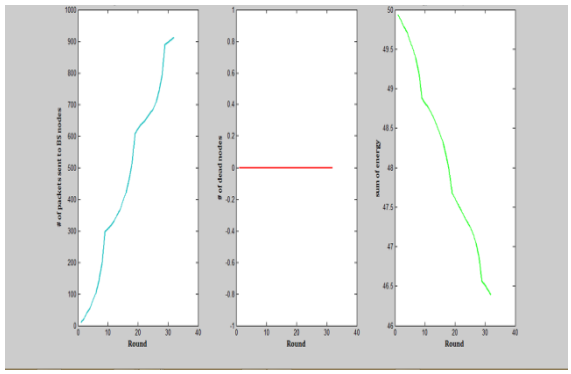

Figure 5.7: (1)-Number of Packets Sends To BS Vs Rounds (2) Number of Dead Nodes vs. Round (3) Loss of Energy Due to Malicious in Different Rounds

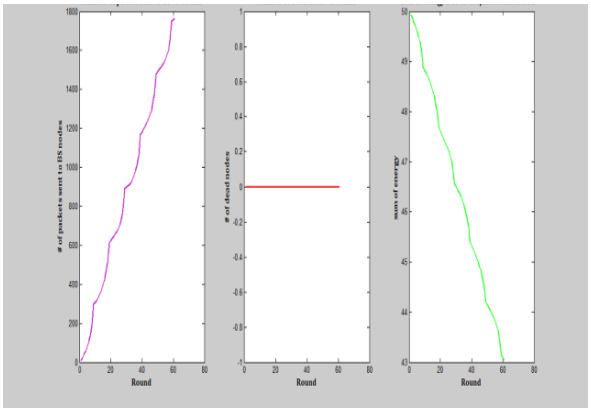

Figure 5.8: (1)-Number of Packets Sends To BS Vs Rounds (2) Number of Dead Nodes vs. Round (3) Loss of Energy Due to Malicious in Different Rounds.

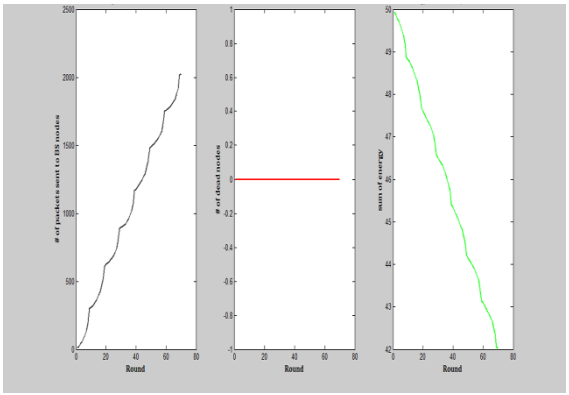

Figure 5.9: (1)-Number of Packets Sends To BS Vs Rounds (2) Number of Dead Nodes vs. Round (3) Loss of Energy Due to Malicious in Different Rounds.

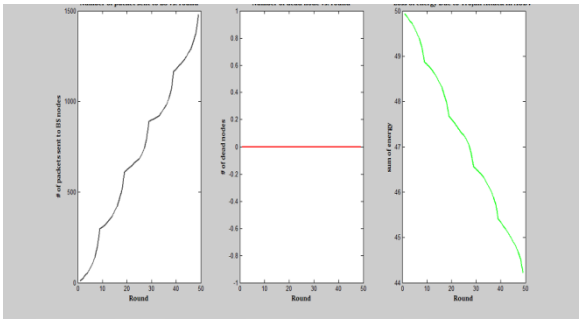

Figure 5.10: (1)-Number of Packets Sends To BS Vs Rounds (2) Number of Dead Nodes vs. Round (3) Loss of Energy Due to Malicious after 99 Rounds.

As a result of increasing the communication period, tracking the energy of this proposed energy prices. The surface is near to the bottom and near to the zero that reaches zero.

Table 5.1: before DOS attack

Before Dos and DDOS attack				
S .No.	No of Rounds	No of packet transmission	NO of dead node	Energy loss
1	200	12000	10	25
2	400	16000	45	12.5
3	600	17000	60	6.25

Table 5.2: After Dos Attack

After Dos and Ddos attack				
S .No.	No of Rounds	No of packet transmission	NO of dead node	Energy loss
1	200	6000	50	10
2	400	10000	80	2.5
3	600	13000	95	0.1

Compared to the energy loss between the two tables, we concluded that DDoS and DoS attacks on WSN have a sharp reduction in energy shortages. Therefore, unusual reduction in energy shows that on our network DoS and DDoS should be attacked.

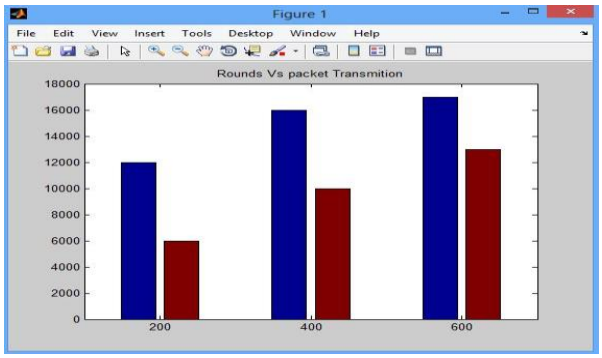

Fig 5.11: Comparison Result of Round VS packet Transmitted (Blue Earlier Work-red Proposed Work)

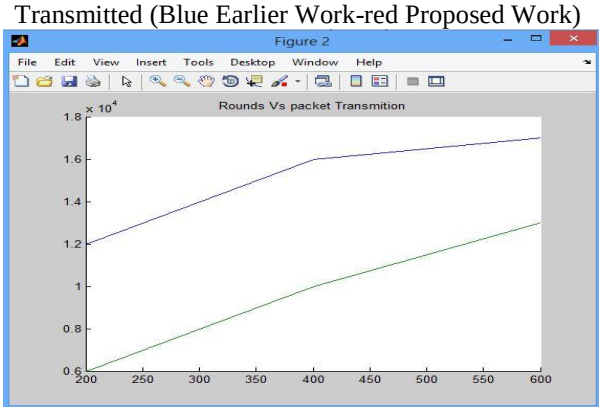

Fig 5.12: Comparison Result of Round VS packet Transmitted (Line Graph) (blue Line-proposed Work, Green Line-Earlier work)

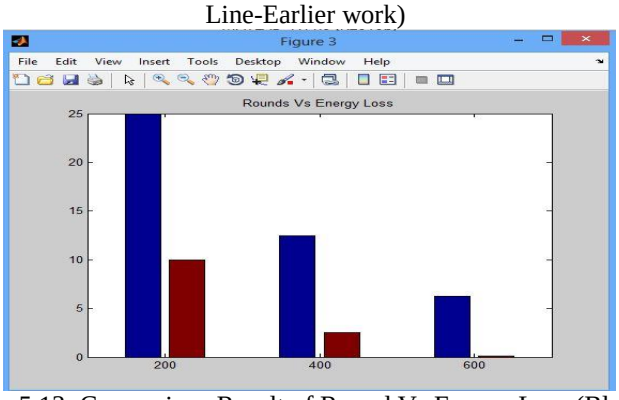

Fig 5.13: Comparison Result of Round Vs Energy Loss (Blue Earlier Work-red Proposed Work)

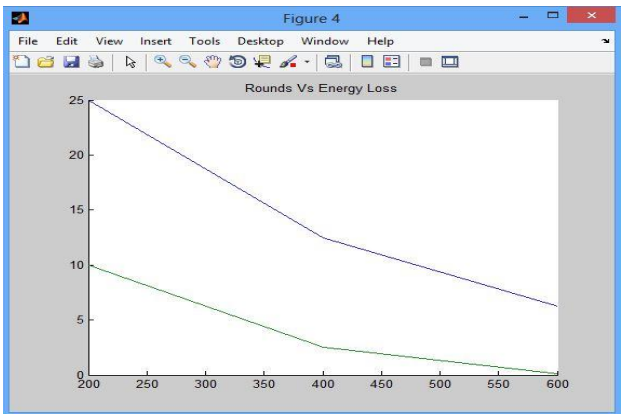

Fig 5.14: Comparison Result of Round Vs Energy Loss (Line Graph) (blue Line-proposed Work, Green Line-Earlier work)

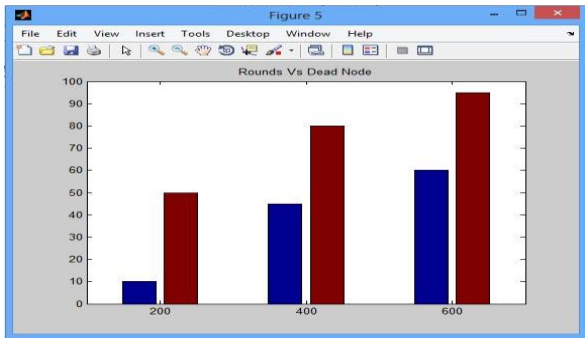

Fig 5.15: Comparative result of round Vs Dead Nodes (Blue Earlier Work-red Proposed Work)

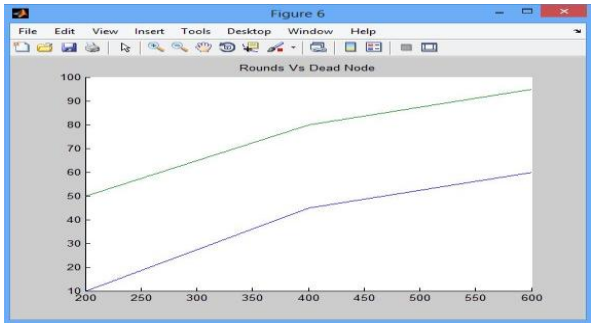

Fig 5.16: Comparative result of round Vs Dead Nodes (Line Graph), (blue Line-proposed Work, Green Line-Earlier work)

The above figure comes out after the end of the simulation and this is the comparative result of previous work with DoS and the proposed work. It is obvious that the proposed work has much better results than previous work.

VI. CONCLUSION AND FUTURE WORK

DoS attacks and distributed Davis are part of an overall risk management strategy for an organization. Each organization must identify the digital most important threat and due to the highest risk of continuity of operations, the effective mechanism of defense mechanisms against these types of attacks must be implemented. According to the studies and news about truth, Davis attacks indicate that these attacks not only exceed network security threats, but the attack will be carried out to the entire organization of the organization for the entire organization. Can end the risk of Davis attacks should not be minimized in this way, but even the maximum. In the future, the problem of DoS attacks can be very high as the number of hostages connected to the Internet increases, access lines are crisp, and the softener product is more complex, and the common home user and even more organizations. Most Internet hosts, most of which can be used for DoS purposes. There may also be an increase in Davis attacks, as a large number of hosts can create more traffic on the Internet connection lines faster. As the software becomes more complicated, the risk of using for compromised hostages will be higher. The new revision does not make the fastest situation easy. Finally, it is difficult for the current computer system to assess security risks, especially by the public.

This paper studied the issue of Davis attack and studied a distributed analysis from multiple perspectives. Individual defense mechanisms were described and analyzed, the choice of defense was studied and the broader standard of defense mechanism assessment was given. The following are the main components of each publication.

REFERENCE

[1] P. J. Criscuolo, Distributed Denial of Service, Tribe Flood Network 2000, and Stacheldraht CIAC-2319, Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory, February 14, 2000.

[2] J. Mirkovic and P. Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, ACM SIGCOMM Computer Communications Review, vol. 34, no. 2, pp. 39-53, April 2004.

[3] S. Ranjan, R. Swaminathan, M. Uysal, and E. Knightly, DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection, IEEE INFOCOM'06, 2006.

[4] R. K. C. Chang, Defending against flooding-based distributed denial of service attacks: A tutorial, Computer journal of IEEE Communications Magazine, Vol. 40, no. 10, pp. 42-51, 2002.

[5] R. Puri, Botsand Botnet an overview, Aug.08, 2003, [online] http://www.giac.org/practical/GSEC/Ramneek Puri GSEC.pdf

[6] B. Todd, Distributed Denial of Service Attacks, Feb. 18, 2000, [online] http://www.linuxsecurity.com/resource files/intrusion detection/ ddos–whitepaper.html

[7] CERT, Denial of Service Attacks, June 4, 2001, [online] http://www.cert.org/tech tips/denial of service.html

[8] J. Liu, Y. Xiao, K. Ghaboosi, H. Deng, and J. Zhang, Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures, EURASIP Journal on Wireless Communications and Networking, vol. 2009, Article ID 692654, 11 pages, 2009.

[9] Yahoo on Trial of Site Hackers, Wired.com, Feb. 8, 2000, [online] http://www.wired.com/news/business/0,1367,34221, 00.html

[10] Powerful Attack Cripples Internet, Oct. 23, 2002, [online] http://www.greenspun.com/bboard/q–and–a–fetch–msg.tcl?msg id=00A7G7

[11] Mydoom lesson: Take proactive steps to prevent DDoS attacks, Feb. 6, 2004, [online] http://www.computerworld.com/s/article/89932/My doom lesson take proactive steps to prevent DDoS attacks? Taxonomy ID=017

