International Journal For Technological Research In Engineering
Volume 4, Issue 10, June-2017 *ISSN (Online): 2347 - 4718*

A NOVEL TECHNIQUE OF DETECTION DDOS AND DOS ATTACK THROUGH VARIABLE ENERGY ANALYSIS IN WSN:A FINAL RESEARCH

Ramesh Kumar Shukla
M.Tech (ECE), Dept of Electronics & Communication Engg., GITAM, Kablana

Abstract: In this paper a new scheme early detection of DDoS attack in WSN has been introduced for the detection of DDoS attack. It will detect the attack on early stages so that data loss can be prevented and more energy can be reserved after the prevention of attacks. Performance of this scheme has been seen on the basis of throughput and remaining energy of the network. The duration of a simulation is thus predetermined by the total simulation time which is clearly stated in all simulation-based publications. 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.

I. INTRODUCTION TO DENIAL OF SERVICE ATTACKS

Denial of Service (DoS) attacks has proved to be a serious and permanent threat to users, organizations, and infrastructures. The primary goal of these attacks is to prevent access to a particular resource like a web server. A large number of defenses against DoS attacks have been proposed in the literature, but none of them gives reliable protection. There will always be vulnerable hosts in the Internet to be used as sources of attack traffic. It is simply not feasible to expect all existing hosts in the Internet to be protected well enough (in July 2005 it was estimated that there were approximately 350000000 hosts in the Internet). In addition, it is very difficult to reliably recognize and filter only attack traffic without causing any collateral damage to legitimate traffic.

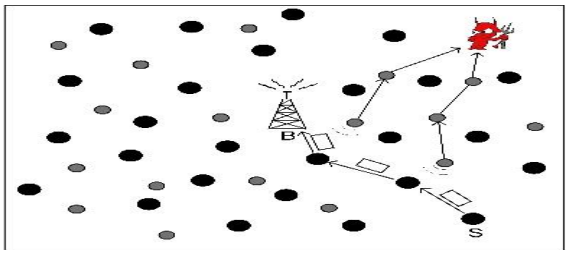

Fig1.1: Basic Of WSN while intruders

1.1 DoS Attacks in Real-Life: Real DoS incidents in the Internet between the years 1989 and 1995 were investigated in. The three most typical effects were the following: 51% of these incidents filled a disk, 33% of the incidents degraded network service, and 26% of the incidents deleted some critical files. A single incident was able to cause several types of damages at the same time (the sum of percentages is more than 100%).

1.2 Research Problem

Mitigating DoS attacks is difficult especially due to the following problems. Very little has been done to compare, contrast, and categorize the different ideas related to DoS attacks and defenses. As a result it is difficult to understand what a computer network user needs to do and why to mitigate the threat from DoS attacks. There are no effective defense mechanisms against many important DoS attack types.

II. LITERATURE SURVEY: DDOS ATTACK: SCOPE AND CLASSIFICATION

The distributed nature of DDoS attacks makes them extremely difficult to combat or trace back. Attackers normally use spoofed (fake) IP addresses in order to hide their true identity, which makes the trace back of DDoS attacks even more difficult. Furthermore, there are security vulnerabilities in many Internet hosts that intruders can exploit. Moreover, incidents of attacks that target the application layer are increasing rapidly. One of the necessary steps towards deploying a comprehensive DDoS defense mechanism is to understand all the aspects of DDoS attacks. Various classifications of DDoS attacks have been proposed in the literature over the past decade. In this survey, we are interested in providing a classification of DDoS flooding attacks based on the protocol level at which the attack works. We review various DDoS flooding incidents of each category, some of which have been well reviewed/analyzed in [1], [2], [3][4], [6] and the rest are recent trends of DDoS flooding attacks. In this paper, we mainly focus on DDoS flooding attacks as one of the most common forms of DDoS attacks. Vulnerability attacks, in which attackers exploit some vulnerabilities or implementation bugs in the software implementation of a service to bring that down, are not the focus of this study. As we mentioned earlier, DDoS flooding attacks can be classified into two categories based on the protocol level that is targeted: A. Network/transport-level DDoS flooding attacks: These attacks have been mostly launched using TCP, UDP, ICMP and DNS protocol packets. There are four types of attacks in this category [2], [6]: A.1 Flooding attacks: Attackers focus on disrupting legitimate

user's connectivity by exhausting victim network's bandwidth (e.g., Spoofed/non-spoofed UDP flood, ICMP flood, DNS flood, VoIP Flood and etc. [2], [5]). A.2 Protocol exploitation flooding attacks: Attackers exploit specific features or implementation bugs of some of the victim's protocols in order to consume excess amounts of the victim's resources (e.g., TCP SYN flood, TCP SYN-ACK flood, ACK & PUSH ACK flood, RST/FIN flood and etc. [2], [5]). A.3 Reflection-based flooding attacks: Attackers usually send forged requests (e.g., ICMP echo request) instead of direct requests to the reflectors; hence, those reflectors send their replies to the victim and exhaust victim's resources (e.g., Smurf and Fragile attacks) [2], [6]. A.4 Amplification-based flooding attacks: Attackers exploit services to generate large messages or multiple messages for each message they receive to amplify the traffic towards the victim. Botnets have been constantly used for both reflection and amplification purposes. Reflection and amplification techniques are usually employed in tandem as in the case of Smurf attack where the attackers send requests with spoofed source IP addresses (Reflection) to a large number of reflectors by exploiting IP broadcast feature of the packets (Amplification) [2], [3]. All of the above attack types with their details have been well presented in [2], [32], [3], [3]. Hence, we skip further explanation of these attacks; instead we focus on the application-level DDoS flooding attacks as they are growing rapidly and becoming more severe problems as they are stealthier than the network/transport-level flooding attacks and they masquerade as flash crowds. B. Application-level DDoS flooding attacks: These attacks focus on disrupting legitimate user's services by exhausting the server resources (e.g., Sockets, CPU, memory, disk/database bandwidth, and I/O bandwidth) [3]. Application-level DDoS attacks generally consume less bandwidth and are stealthier in nature compared to volumetric attacks since they are very similar to benign traffic. However, application-level DDoS flooding attacks usually have the same impact to the services since they target specific characteristics of applications such as HTTP, DNS, or Session Initiation Protocol (SIP). Here we briefly describe the DNS amplification flooding attack and the SIP flooding attack as two of the famous application-level reflection/amplification flooding attacks embracing DNS and SIP protocols. Then we classify various flavors of application-level flooding attacks that employ the HTTP protocol since these attacks are consistently reported as the major types of recent DDoS flooding attacks [3]. B.1 Reflection/amplification based flooding attacks [2], [3]: These attacks use the same techniques as their network/transport-level peers (i.e., sending forged application-level protocol requests to the large number of reflectors). For instance, the DNS amplification attack employs both reflection and amplification techniques.

III. EARLEIR

In this research is to help any network user in mitigating DoS attacks and DDoS in IP-based networks. This dissertation concentrates especially on the following areas. One should understand existing attack mechanisms and available defense mechanisms, and have a rough idea about the benefits (best-case performance) of each defense mechanism. One should acknowledge possible situation dependency of defense mechanisms, and be able to choose the most suitable defense when more than one defense mechanisms are available against a specific attack type.One should evaluate defense mechanisms in a comprehensive way, including both benefits and disadvantages (worst-case performance), as an attacker can exploit any weakness in a defense mechanism. Knowledge of all of these issues is necessary in successful mitigation of DoS and DDOS attacks. Without knowing how a specific defense mechanism works under different possible conditions and what the real benefits and weaknesses are, it is not possible to assure the suitability of a defense mechanism against a certain type of a DoS and DDOS attack.

IV. PROPOSED WORK

All simulations used in this dissertation are terminating simulations with a finite time horizon. The duration of a simulation is thus predetermined by the total simulation time which is clearly stated in all simulation-based publications. 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.

4.1 Simulation 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*0.000000001
Energy.free Space	10*0.000000000001
Total energy	0.5
Energy.multiPath	0.0013*0.000000000001;
Energy Trasnmitted	5*0.000000001
Energy.receive	50*0.000000001;

4.2 The proposed GUI constructed in MATLAB

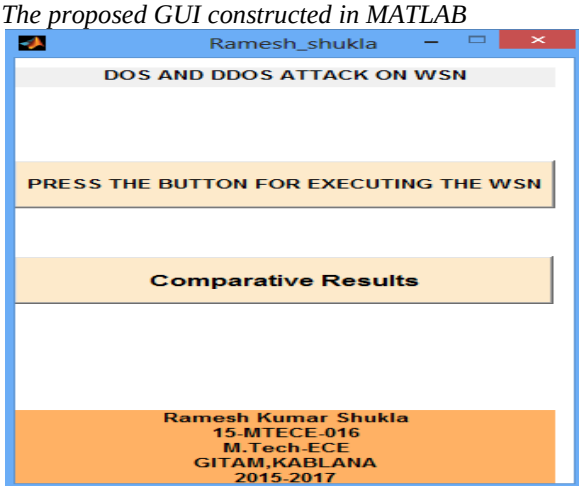

Fig 4.1: basic layout having the push button for executing the code (In Matlab 2010)

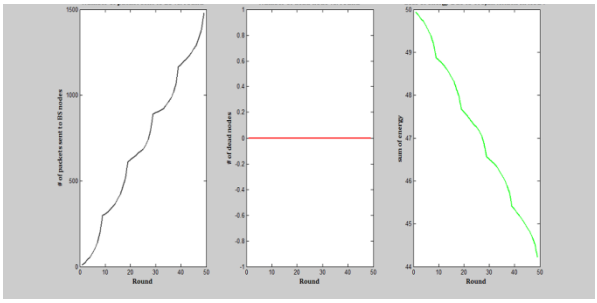

Figure 4.2: (1)-Number of Packets Sends To BS Vs Rounds (2) Number of Dead Nodes vs. Round (3) Loss of Energy Due to Malicious after 99 Rounds

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.

Table 1.1: 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 4.2: 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

Energy loss comparison between above two tables we conclude 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.

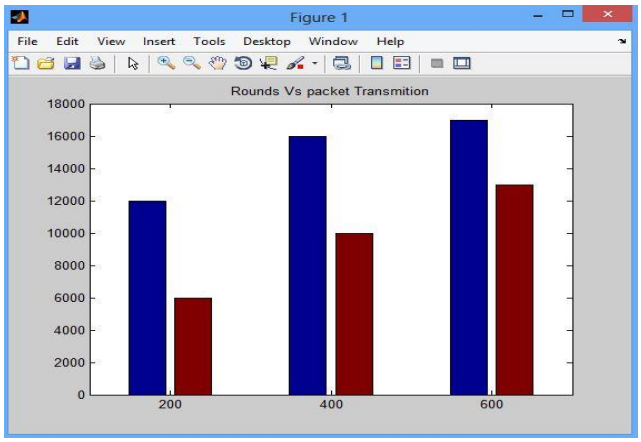

Fig 4.3: Comparison Result of Round VS packet Transmitted (Blue Earlier Work-red Proposed Work)

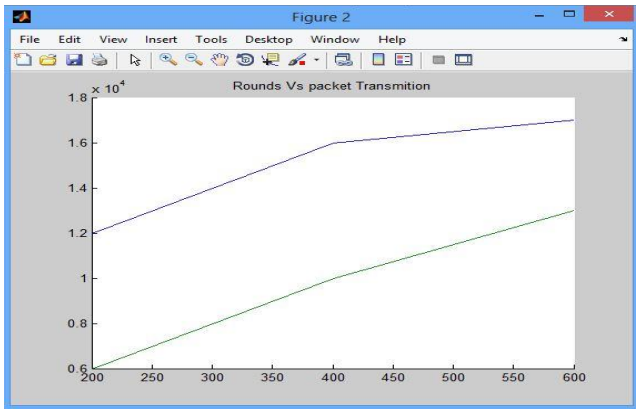

Fig 4.4: Comparison Result of Round VS packet Transmitted (Line Graph) (blue Line-proposed Work, Green Line-Earlier work)

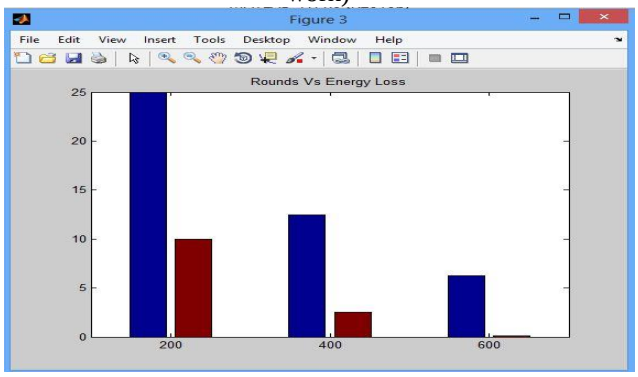

Fig 4.5: Comparison Result of Round Vs Energy Loss (Blue Earlier Work-red Proposed Work)

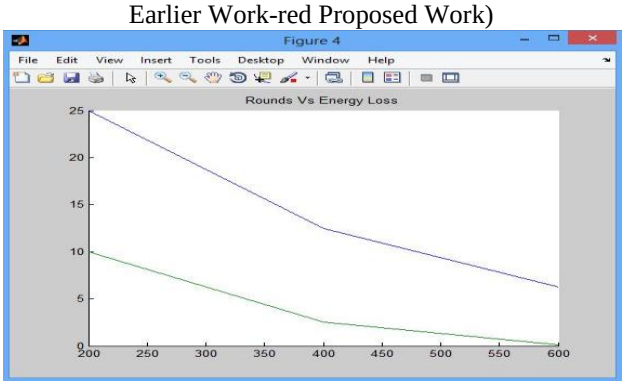

Fig 4.6 : Comparison Result of Round Vs Energy Loss (Line Graph) (blue Line-proposed Work, Green Line-Earlier work)

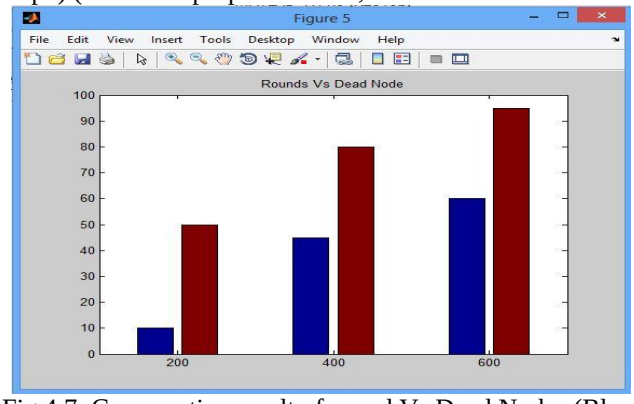

Fig 4.7: Comparative result of round Vs Dead Nodes (Blue Earlier Work-red Proposed Work)

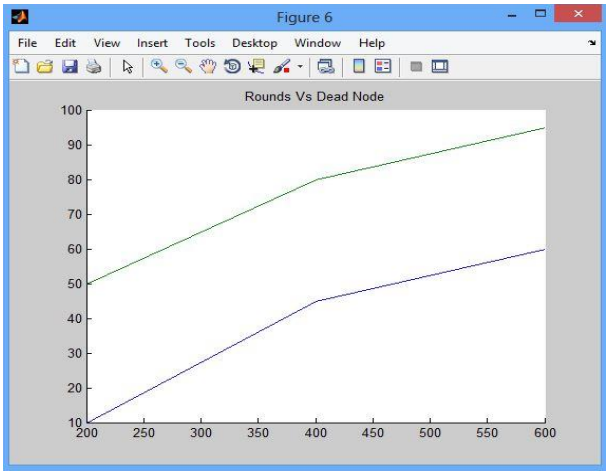

Fig 4.8: Comparative result of round Vs Dead Nodes (Line Graph), (blue Line-proposed Work, Green Line-Earlier work)

Above figure come out after the end of simulation and this 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. DoS attacks and distributed DoS are a part of an overall risk management strategy for an organization. Each organization must identify the most important DoS risks, and implement a cost-effective set of defense mechanisms against those attack types causing the highest risk for business continuity. Studies and news about real-life DoS attacks indicate that these attacks are not only among the most prevalent network security risks, but that these attacks can also block whole organizations out of the Internet for the duration of an attack. The risk from DoS attacks should not thus be underestimated, but not overestimated, either. In the future the problem from DoS attacks will most probably increase because the number of hosts connected in the Internet increases, access lines get faster, soft-ware products get more complex, and security continues to be difficult for an ordinary home user and even many organizations. The more there are hosts in the Internet, the more of them can potentially be used for DoS purposes. The intensity of DoS attacks can also increase, as a higher number of hosts can produce more traffic over faster Internet access lines. As software gets more complex, more vulnerability will reside in them to be used for compromising hosts. The fast pace of new revisions does not make the situation easier. Finally, it will continue to be difficult to evaluate security risks in existing computer systems, especially by ordinary people.

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/Mydoom lesson take proactive steps to prevent DDoS attacks? Taxonomy ID=017

[12] Lazy Hacker and Little Worm Set off Cyberwar Frenzy, July 8, 2009, [online] http://www.wired.com/threatlevel/2009/07/mydoom /

[13] New" cyber-attacks" hit S Korea, July 9, 2009, [online] http://news.bbc.co.uk/2/hi/asia-pacific/8142282.stm

[14] Operation Payback cripples MasterCard site in revenge for Wiki Leaks ban, Dec. 8, 2010,[online]http://www.guardian.co.uk/media/2010/dec/08/operation–payback– MasterCard–website–Wiki Leaks

[15] T. Kitten, DDoS: Lessons from Phase 2 Attacks, Jan. 14, 2013, [online] http://www.bankinfosecurity.com/ddos-attacks-lessons-from-phase-2-a-54 20/op-1

[16] Forrester Consulting, The Trends And Changing Landscape Of DDoS Threats And Protection, A commissioned study conducted by Forrester Consulting on behalf of VeriSign, Inc., July 2009.

