ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

OPTIMISED SECURITY FRAMEWORK BASED ON TIME STAMP FOR DOS ATTACKS IN WIRELESS SENSOR NETWORKS

Munish Dhar*, Rajeshwar Singh

* P.G Student, Department of ECE, Doaba Institute of Engg. & Technology, Mohali, Punjab, India
Professor, Department of ECE, Doaba Khalsa Trust Group of Institutions, SBS Nagar, Punjab, India

ABSTRACT

Network performance always dependent on the perfect flow of the data processing packets in network but with attacks in network, performance halted a lot or just degraded at times. Denial of service attack is one of the most dangerous and real time attack which could slow down every service and network, especially when applied to ad-hoc networks such as wireless sensor networks. In this paper we designed optimized security framework for detection of dos attacks. This research focused on detection of time based denial of service attacks which work on timely bases and are not detected by normal process. The time difference between two nodes and the time stamp period variation is calculated. If two nodes are showing variation which tends to more timestamp period then it considered to be malicious node. Our proposed work provides better results in term of throughput recovery by avoiding mechanism.

KEYWORDS: Wireless sensor networks (WSN), security concerns, denial of service (DOS) attacks, time Stamp, network simulation tool

INTRODUCTION

Recent advances in semiconductor, networking and material science technologies are driving the ubiquitous deployment of large-scale wireless sensor networks (WSNs) [1]. Once the sensors are deployed in an unsecure environment, there are many critical security issues. The main issues related with the security of WSNs are key management, attack detection and prevention, secure routing and secure location [2]. Denial of service attack is one of the most dangerous and real time attack which could slow down every service and network, especially when applied to wireless sensor networks. The invader compromise sensor nodes and results in dos attacks by continuously sending bogus or false packets in the network [3]. Wireless sensor networks are susceptible to denial of service attacks as they are limited in energy and have no central monitoring point [4]. A denial of service (DoS) attack can be described in many forms and also there are different types of DoS attacks in the layered protocol of sensor network [5]. In [6], author defined DoS attack as an incident in which a user is deprived of the services of a resource he would normally expect to have, whereas in [7] it was defined as any event that diminishes or eliminates a network's Capacity to perform its expected function". Now attack may be from a single agent or from multiple agents. When attacker attacks from multiple agents that are distributed in the network, it is termed as distributed denial of service (DDOS) attack whereas when attacker attacks from a single agent, it is called as single-source denial of service (SDOS) attack [8]. A DDOS attack mainly occurs in 2000 & 2001 which harms various websites like Amazon.com, EBay, and Yahoo etc. Figure 1 describes the component of DDoS attack mechanism. The mechanism starts attack by taking system as agents and then uses botnest to exhaust the victim's system.

1) Master: The Original Attacker, who decides when to attack in the network and how it can be done.
2) Controller/Handler: Co-ordinates with original attacker to compromise other nodes to continue the DDoS attack
3) Agents or Bonets: Agents or slaves are programs that actually responsible to conduct attack on the victim or nodes in the network.
4) Victim/Target: A host on which attack has to be performed [9].

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

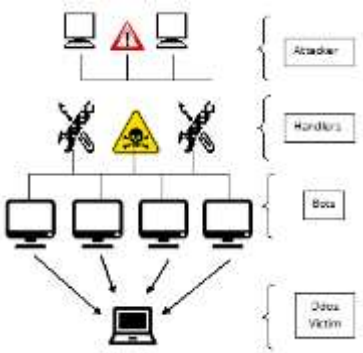

Figure 1: Components of DDOS attack

The rest of this paper is organized as follows: Section 2 covers previous work. In Section 3, present work is being discussed. Section 4 focus on result and discussions. Finally, Section 5 gives conclusion and future scope

RELATED WORK

This section charts out the overview on a plethora of existing DDOS defense schemes proposed in the literature.

We begin our discussion with the rate limit framework proposed by Jing [10]. It involves detection of attacks, deciding the rate limit and application of rate limiter. As attack is detected, attack detection agent (ADA) will send alert and defense request to defense service provider (DSP) who performs rate limit decision-making and sends rate limit commands to rate limiter (RL). RL then limits the rate of particular flow of traffic and sends real-time rate information to the local DSP.

Rahul Mahajan in 2002 introduced a pushback mechanism for detecting and controlling high bandwidth aggregates which is a collection of packets from one or more traffic flows having similar properties such as destination or source address prefix, TCP packets, ICMP packets, etc .The mechanism includes controlling of upstream network traffic. The congested router sends commands to its adjacent upstream routers to rate-limit the aggregate since those are responsible for sending major fraction of the aggregate traffic [11].

Walish proposed a defense by offense technique in which DDoS attacks can be prevented at application level by sending large volumes of traffic. The scheme assumes that, if the bad clients are already using most of their upload bandwidth, by encouraging the clients to send higher volume of traffic will change in the volume of good clients only. [12].

Xuan deployed Gateway architecture to detect attacks and control the traffic. It protects TCP friendly traffic using gateways which are deployed at different locations to detect attacks and perform the traffic access control. It filters the traffic based on the matching degree of the on-going flows to the ones in the TCP friendly flow list [13].

Abraham Yaar presents SIFF, a type of Filter, which permits a server-client to selectively stop individual flows from entering the network and divides traffic into two main parts, privileged and unprivileged. Privileged packets are those verified statelessly by the routers in the network, and are dropped when the verification fails. Privileged channel are formed using capability exchange handshake. Capabilities are verified with help of routers in the network, and can be cancelled by quenching update messages to an offending host [14].

In [15], Arunmozhi make use of medium access control information to detect the attack . It checks current and previous sending rate and any change in the congestion notification bit indicates congestion in the network. If rate is equal to or greater than the last one, then they are considered as bogus packets and all packet from that node is rejected. In the proposed scheme it uses two phase bandwidth Querying scheme and Data transmission scheme.

In [16], the author introduced spin lock rate control mechanism to identify the malicious traffic flow towards a target system which is based on the amount of traffic flowing towards the victim and selectively implement rate limiting based on flow of traffic and type of on flow towards victim. It involves divide and conquer approach and calculation of ratio of collective flow (RCF). The system adapts quickly to any changes in the rate of flow.

PROPOSED APPROACH

In this section, we will discuss proposed DDoS defense framework as shown in figure 2, which aims to provide successful detection of DDoS attacks based upon time stamp.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

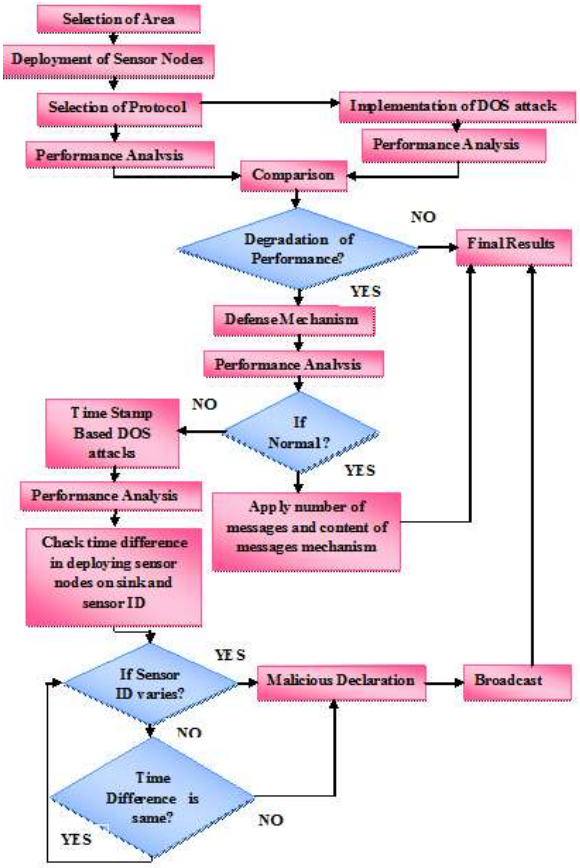

Figure 2: Architectural diagram for proposed security framework

The network analysis is done using NS2 Simulator. The deployment of network structure includes assignment of unique keys to the network nodes so that communication process will be secure. Proposed work has considered cluster head selection processes with unique ids.

Many mechanisms are good to adapt the content of the messages and judge on the bases of same. But as said most of the researches haven't considered time stamp based attacks. DOS attack which is time based is very difficult to detect through related concept. This research, focused on elimination of time based a denial of service attacks which work on timely bases and are not detected by normal process. Mechanism of proposed work enhanced security mechanism and further calculated the time difference between two nodes and calculates the time stamp period variation. If two nodes are showing variation which tends to more timestamp period then it considered to be malicious node. Our proposed work provides better results in term of throughput recovery by avoiding mechanism.

EXPERIMENTAL DESIGN AND PERFORMANCE ANALYSIS

Simulation Environment

The simulations have been done using NS2 (Network Simulator) which is an open source event-driven simulator designed especially for research in communication networks. It is based upon an object oriented simulator written in C++ and OTCL interpreter used to execute user scripts [17].

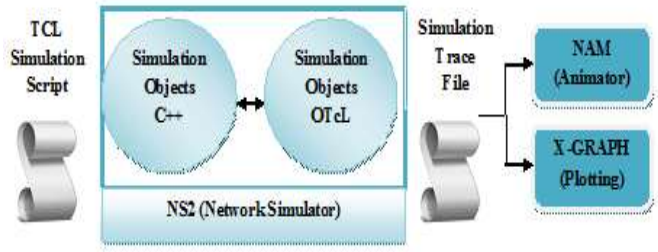

Figure 3: Basic architecture of NS2

System Implementation

We started with deployment of wireless sensor nodes in the field and unique keys are assigned to the wireless nodes. The simulation randomly generates 100 points in the range of 1500 m×1150 m plane and used 81 points for wireless communication. At initial phase basic functionality and collection of information (simulator, basic mobility functions etc) has been done. Three scenarios have been taken into consideration. In first normal traffic is passing through the network and there is no attack. In second scenario, particular node sends the malicious traffic causing the DOS attack and in last Scenario, dos attack is detected and new mechanism is implemented to remove the DOS attack. All these scenarios were implemented in NS2 simulator. We processed with basic structure in which 10 attacker traces have been used. Throughput shown in Normal scenario is decreased when we have applied attacker scenario to normal network and is recovered with implementation of proposed scheme for avoidance.

The communication between sensor nodes and cluster head and further between cluster head and base station is shown below. Also detection of malicious nodes using time stamp parameter is also shown.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

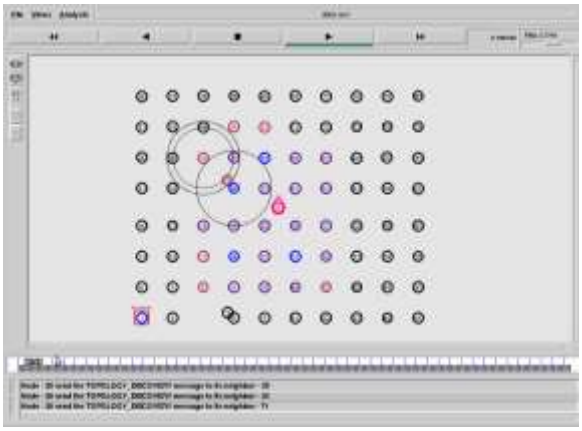

Figure 4: Simulation scenario for experimentation

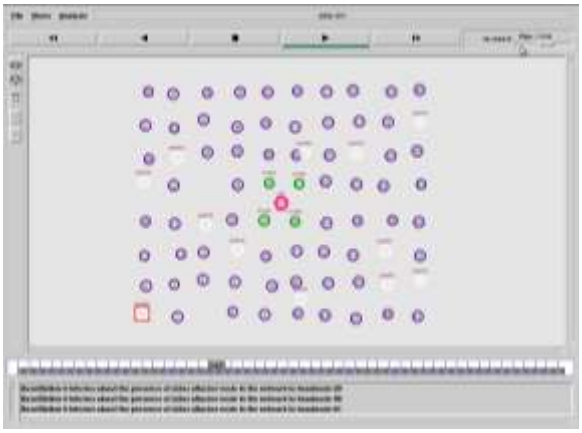

Figure 5: Detection of malicious attacker nodes along with normal nodes

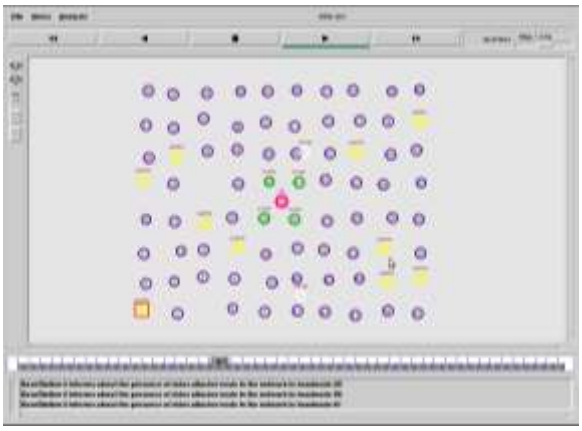

Figure 6: Attacker detection and filtering of normal nodes from the simulation

Table 1: Parameters used for simulation

Parameters	Value
Simulator	NS2
Simulation Time	80 sec
Number of Subnets	5
Number of Nodes	81
Traffic Model	CBR
Energy Consumption	50 nJ/bit
Speed	2 mps
Transmit Power	14mW
Receiving Power	12 mW
Initial battery power	100 J
MAC layer	802.11
Time Slots	Grid Distribution
Magnify Coefficient	10nJ/bit/ m^2
Data Fusion Consumption	5nJ/bit/signal

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Performance Evalution

In normal scenario, throughput value is around 415 kbps and it decreases with attacker scenario to 91 kbps. Recovery scenario recovered the basic throughput to 385 kbps. Experimentation shows, attacker scenario decreases performance by 78.07%, which is recovered by our proposed scheme by providing recovery of 70.85%. Total wastage of throughput during this process is around 7.22%.

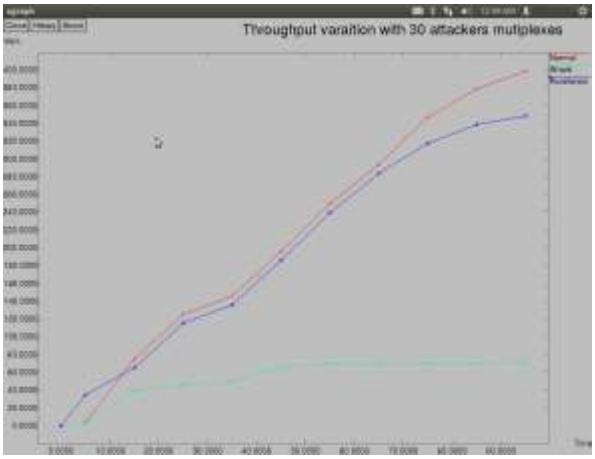

Figure 7: Throughput variation with 30 attackers

On similar note, when we experimented with 30 attacker traces, performance decreased by 88% and recovered around 72% throughput. When we experimented with 50 attacker traces, performance decreased by 87% and recovered around 63% throughput. When these values are compared with related study [3], it shows improvement in term of data lost during recovering mechanism.

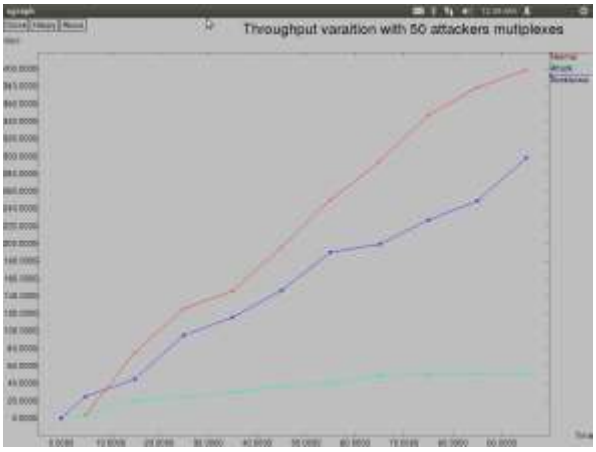

Figure 8: Throughput variation with 50 attackers

Conclusion And Future Scope

This paper proposed a security framework which focused on elimination of time based denial of service attacks which work on timely bases and are not detected by normal process. Experimentation shows that attacker scenario decreases performance which is recovered better by our proposed scheme. This work gives a good solution for reduction of effects of Dos attacks in WSN and increase in TCP throughput for communication in wireless network. Current experimentation is based on the WSNs only and we haven't tested it for Wi-Fi, WI-Max and content based networks due to time and resource limitation. In future, it would be very interesting to apply our concept to these networks for local area network infrastructures.

REFERENCES

1. Yusnani Mohd Yussoff, Habibah Hashima, Roszainiza Roslib, Mohd Dani Baba (2012), " A Review of Physical Attacks and Trusted Platforms in Wireless Sensor Networks" in International Symposium on Robotics and Intelligent Sensors, Vol.41, Issue.4, April 2012, pp.580-587.
2. TIAN Bin, YANG Yi-xian, LIDong, LI Qi and XIN Yang , "A security framework for wireless sensor networks" in The Journal of China Universities of Posts and Telecommunications, Vol.17, Issue.2, February 2010, pp.118–12
3. ZHANG Yi-ying, LI Xiang-zhen and LIU Yuan-an, "The detection and defence of DoS attack for wireless sensor network" in jcupt , 2012
4. Han G J, Shen W and Trung Q D, "A proposed security scheme against denial of service attacks in cluster-based wireless sensor networks" in Security and Communication Networks, 2011.
5. Li M, Koutsopoulos I and Poovendran R, "Optimal jamming attacks and network defense policies in wireless sensor networks" in Infocom, May 2007
6. Y. Zhou, Y. Fang and Y. Zhang, "Securing Wireless Sensor Networks: A Survey" in IEEE Communications Surveys & Tutorials", vol.10, issue 3, pp. 6 –28, 2008.
7. A. D.Wood and J. A Stankovic, "Denial of Service in Sensor Networks" in IEEE Computer.,vol. 35, no. 10, October 2002, pp. 54-62.
8. Scarfone, K., Grance, T., and Masone, K. , " Computer security incident handling

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

guide" in Special Publication 800-61, National Institute of Standards and Technology (NIST). March, 2008.
9. Shweta Tripathi1, Brij Gupta , Ammar Almomani , Anupama Mishra and Suresh Veluru , " Hadoop Based Defense Solution to Handle Distributed Denial of Service (DDoS) Attacks" in Journal of Information Security, 2013, 4, 150-164.
10. Yinan Jing, Zheng Xiao, Xueping Wang, and Gendu Zhang, "O2-DN: An Overlay-based Distributed Rate Limit Framework to Defeat DDoS Attacks" in Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006; 23-29 April 2006; pp. 79.
11. Ratul Mahajan, Steven M. Bellovin, Sally Floyd, John Ioannidis, Vern Paxson and Scott Shenker , "Controlling High Bandwidth Aggregates in the Network" in ACM SIGCOMM Computer Communication; Vol.32, No.3, July 2002; pp. 62-73.
12. Michael Walfish, Mythili Vutukuru, Hari Balakrishnan, David Karger and Scott Shenker, "DDoS Defence by Offense" in ACM SIGCOMM'06, Pisa, Italy; September 11-15, 2006
13. Dong Xuan, Riccardo Bettati, and Wei Zhao;, "A Gateway-based Defense System for Distributed DoS Attacks in High-Speed Networks" in IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5-6 June 2001; pp. 212-219.
14. Abraham Yaar, Adrian Perrig and Dawn Song, "SIFF: a stateless Internet flow filter to mitigate DDoS flooding attacks" in Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on 9-12 May 2004; pp.130 – 143.
15. S.A.Arunmozhi and Y.Venkataramani, "DDoS attack and Defense in wireless ad-hoc Network" in International Journal of Network Security & Its Applications Vol.3, No.3, pp.182-187, May 2011.
16. Anurekha, R., K. Duraiswamy, A. Viswanathan, V.P. Arunachalam, K. Ganesh Kumar and A. Rajivkannan, "Dynamic Approach to Defend Against Distributed Denial of Service Attacks Using an Adaptive Spin Lock Rate Control Mechanism" in Journal of Computer Science 8 (5): 632-636, 2012.
17. NS Documentation. Available: http://www.isi.edu/nsnam/ns.