ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

DDOS Attack Detection on Wireless Sensor Network: A Review

Amandeep Kaur[1], Daljeet Kaur[2], Gagandeep[3]

M. Tech Student, Department of Computer Science and Engineering, Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab, India[1]

Associate Professor, Department of Computer Science and Engineering, Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab, India[2]

Assistant Professor, Department of Computer Science and Engineering, Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab, India [3]

ABSTRACT: In this sense, DoS, especially DDoS, not only threatens the Internet, but also threatens the civil security, due to its prevalent usage in cyber-crimes. Thus to understand well the characteristics of DDoS problems and investigate corresponding defense mechanisms have significant contributions not only for academia and industry, but also for the social security and emergency management agencies, since they can use such knowledge to enhance their abilities of risk assessments and help the stakeholders to make appropriate decisions when facing DDoS threats. In the existing research work the different types of problems, such perspective in terms of detecting DoS attacks is to view the problem as that of a classification problem on network state (and not on individual packets or other units) by modeling normal and attack traffic and classifying the current state of the network as good or bad, thereby detecting attacks when they happen. Another is the Transmission failures or deadline misses may result in disturbances to the process, degradation of the overall control performance. In future All these are resolved with the help of a DDoS attack detection and DSR Algorithm with Cryptography on Wireless Sensor network and the WSN with BS, CH

KEYWORDS: DDoS, BS, CH, WSN, Attacks etc.

I. INTRODUCTION

Nowadays, distributed denial of service (DDoS) attacks pose one of the most serious security threats to the Internet [1]. DDoS attacks can result in a great damage to the network service. The DDoS attackers usually utilize a large number of puppet machines to launch attacks against one or more targets, which can exhaust the resources of the victim side. That makes the victim lose the capability to serve legitimate customers and prevent legitimate users from accessing information or services. Since DDoS attacks can greatly degrade the performance of the network and are difficult to detect, they have become one of the most serious security challenges to the current intrusion detection systems (IDS) [2]. Concerning the current state of the network, every corner of the world is likely to be the target of DDoS attacks. However, as long as they are detected early, the loss can be reduced to the minimum. Therefore, DDoS attack detection and defense still attract much concern from researchers. During a typical attack period, an attacker controls the compromised hosts to send requests to a target site and those combined packet flows will overwhelm the target due to the limited resources. The target can be machine, network link or even network links of ISPs. According to the typical communication pattern of DDoS attacks, they can be divided into two main categories, which are called direct attacks and indirect attacks, respectively. In order to launch an attack, attackers have to build a network first. Such kind of networks usually contains three components, which are attackers, masters and agents. The attacker controls one or more masters and each master controls thousands of agents to initialize the attacks. The attacker itself does not send packets to victims directly. It makes the puppets to send attack packets in order to hide its malicious activities. By this way, it is difficult to track the attack source during attacks.[2]

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

II. DIRECT AND REFLECTOR-BASED ATTACKS

During a direct attack, spoofed IP addresses are usually involved to prevent attackers from being discovered. As shown in Fig. 1, the attacker directly sends packets with forged source IP addresses to the victim side and tries to periodically establish connections with the victim to exhaust the victim's resources. Such kind of attacks utilizes the inherent weaknesses of some communication protocols, which require the receiver to send feedback to the sender side when it receives packets from senders. The attacker can take advantage of such feedback mechanism to launch an attack. One of the most prevalent DDoS attacks in the past decade is SYN flood attack which belongs to direct attacks.[3] According to the three-way handshake mechanism of TCP initialization process, the victim server needs to send an acknowledge packet to the sender side. Since source IP addresses of malicious packets are spoofed, the server will never get responses from sender's side. At the same time, the victim server still keeps a large amount of memory and CPU resources for those broken connections. By exhausting the resources of the server, legitimate users cannot access normal services. Fig. 2.shows a typical flow distribution during a DDoS reflector attack. Compared with the direct attack, the attackers do not send packets directly to the victim but to some reflectors.
Both routers and DNS servers can be utilized as the reflectors. The attacker sends packets, which are required to be responded to the reflectors. However, those packets which are sent to the reflectors contain the victims' IP addresses. The reflectors will then send a large number of packets to the victims. The large number of packets will saturate the ingress link of the victim. Such kind of attacks is more dangerous since all the responding packets have no difference compared with legitimate packets and thus it is more difficult to detect.[4]

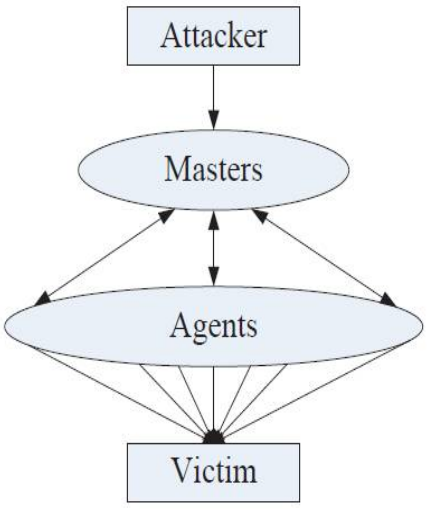

Figure 1: Direct attack [4]

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

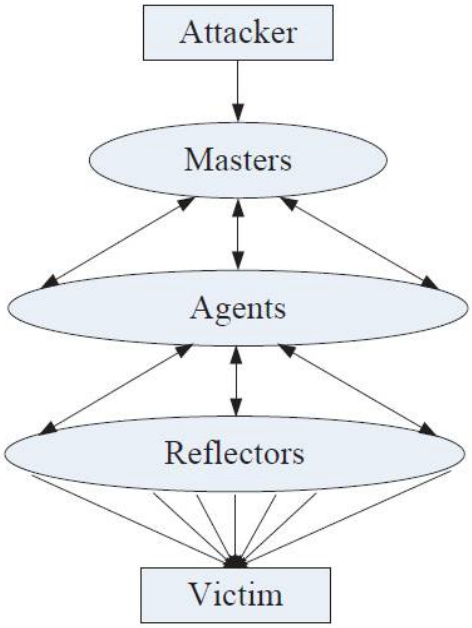

Figure 2: Reflector-based attack [4]

III. DDOS DETECTION

Systems used to detect DDoS attacks are considered as a type of Network Intrusion Detection Systems (NIDs). The latter employ two distinct approaches to detect malicious activities: signature-based detection and anomaly-based detection [2]. Signature-based detection is used to detect known security threats (e.g., a virus or malformed packets) looking for specific patterns (signatures) to appear in individual packets. On the other hand, anomaly-based NID is used to detect potential security threats based on abnormal behaviors over a set of packets. Due to the nature of flooding-based DDoS attacks, where every malicious packet may seem legitimate if analyzed individually but where the overall traffic behavior may suffer abrupt variations (e.g. abrupt increases of traffic volume), anomaly-based detection is always used to detect flooding-based DDoS attacks. In the recent decade, many anomaly-based detection methods were proposed to identify DDoS attacks from network traffic. Basically, these detection methods can be classified into two categories: off-line DDoS mining and on-line DDoS detection. Off-line DDoS mining usually try to find attacks by analyzing the main characteristics of feature distributions of the network traffic with some systematic methods, such as PCA (Principal Component Analysis)) [4, 5] and dominate states analysis [5]. The basic idea of PCA is to embed the multidimensional data into lower dimensional subspace in which normal instances and the anomalies appear significantly different. The basic idea of the dominate states analysis is to explore the interaction or dependence among the dimensions of the data by identifying subset of values (dominate states) to represent or approximate the original data in their probability distribution. Anomalies can be identified since their dominate states deviate significantly from the normal ones. When the network anomalies are identified, data clustering methods, such as k-means clustering [6], are applied to group different types of anomalies together for further identification, correlating anomalies to attacks. To achieve accurate analysis results, the processing procedures of off-line methods are executed on the whole data trace, and these methods usually involve expensive computations, e.g PCA involves matrix computations for computing principal components of the data. So the off-line DDoS mining methods can hardly be used in online detection, due to time and space complexities. However, the analysis results from the off-line anomaly mining can help build the base-line profile for the real time detection. Considering the big scale of the DDoS attacks, detection over big volume of traffic (e.g. multi-10Gbps) is really challenging [7]. Computation over massive data

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

streams is being studied in the emerging field of data streaming, aiming at methods for processing massive amounts of data in a real-time fashion, such that each tuple in the data stream is only processed once. Data streaming computation has been adopted in applications such as financial markets and mobile phones or credit card fraud detection applications [8]. Recently, data streaming has also been proposed for DDoS detection at high-speed network links, where streams of packets are processed by continuous queries to find anomalous DDoS-related traffic patterns in real time. Data streaming queries are referred to as continuous as they are constantly "standing" over the streaming tuples and continuously producing output results. Most data-streaming based DDoS detection methods focus on using space efficient and time-efficient algorithm to keep track of the heavy hitters, e.g. a source sending lots of packets to many destinations, in the monitored traffic. One particular algorithm used is sketch algorithm [9]. Sketch is a probabilistic summary technique which can sustain large streaming datasets. It keeps the summary updates using projection along random vectors to achieve space efficiency with guaranteed probabilistic reconstruction accuracy. However, sketch based solutions do not support continuous monitoring with sliding window, since the random vectors used for maintaining the sketches are reset when some anomalies are detected or some predefined period expires. Thus sketch-based solution may miss the anomalies spanning consecutive periods. Considering the types of DDoS attacks that are in the focus of the previous work in DDoS detection, SYN flooding is the most common one, since such attacks usually cause imbalance between the number of SYN packets and the SYN/ACK or FIN packets [10]. However, monitoring such imbalance to detect SYN flooding may require the monitor to be deployed at the edge routers, due to the routing asymmetry. So solutions which can detect DDoS attacks at the early stage, i.e. at the backbone links, are desired. However, monitoring high speed traffic in backbone links is challenging [11]. To detect bandwidth flooding attacks, change-point detection [11] and wavelet analysis [8] were proposed. Change-point detection maintains a moving average of each flow and compares the current flow rate against the moving average; if the changing ratio exceeds the threshold, then the flow is identified as suspicious. Wavelet detection maps the series of the flow rates into a spectral domain. Since the attack flows and the legitimate flows have distinguishable frequency components, the presence of attack flows can be detected[12]. However, most of the change-point based and wavelet-based detections only focus on detecting the abrupt changes of the traffic rate, so they may be insufficient for detecting connection requests flooding, like SYN flooding, since the traffic rate may not increase so much in such attacks.[11]

IV. RELATED WORK

Akash Mittal et.al.[2011] have studied Internet is the primary medium for communication which is used by number of users across the Network. At the same time, its commercial nature is causing increase vulnerability to enhance cyber crimes and there has been an enormous increase in the number of DDOS (distributed denial of service attack) attacks on the internet over the past decade. In this paper basically summarizing different techniques of DDoS and its countermeasures by different methods such as Bloom Filter, Trace Back method, Independent Component Analysis and TCP Flow Analysis.[1]

Divya Kuriakose et.al.[2013] have studied Network is collection of nodes that interconnect with each other for exchange the Information. This information is required for that node is kept confidentially. There are many security attacks in network. One of the major threats to internet service is DDoS (Distributed denial of services) attack. DDoS attack is a malicious attempt to suspending or interrupting services to target node. Various schemes are developed defence against to this attack. Main idea of this paper is present basis of DDoS attack. Types of DDoS attack, components of DDoS attack, need for Distributed defense system, comparative study of different defense mechanism.[2]

Saurabh Ratnaparkhi et.al.[2013] have studied DoS/DDoS attacks are a strong, comparatively new type of Internet attacks, they have basis some Biggest web sites on the world -- owned by the mainly famous E-Commerce companies such as Yahoo, eBay, Amazon -- became unreachable to customers, partners, and users; the financial losses are very huge. While former security threats could be faced by a tight security policy and active measures like using recalls, vendor patches etc. these DDoS are novel in such way that there is no totally pleasing protection yet. In this paper we classify diverse Forms of attacks and give an indication over the most common DDoS tools. The goal of this paper to is present the idea behind various protecting technique against the DDOS attack.[3]

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Darshan Lal Meena1 et.al.[2014] have studied Distributed denial-of-service (DDoS) is a rapidly growing problem. The multitude and variety of both the attacks and the defense approaches is overwhelming. This paper is a survey on the problem of denial-of-service (DoS) and Distributed Denial of Service (DDoS) attacks and proposed ways to deal with it. We describe the nature of the problem and look for its root causes, further presenting brief insights and suggested approaches for defending against DDoS. We point out both the positive and negative sides of each potential solution. Future work identifies and justifies open research issues. This provides better understanding of the problem and enables a security administrator to effectively equip his arsenal with proper prevention mechanisms for fighting against DDoS threat.[4]

Shenam Chugh et.al.[2015] have studied a review on the problem of denial-of-service (DoS) attacks and proposed ways to deal with it. Broadcast authentication is an important application in sensor networks.Public Key Cryptography (PKC) is desirable for this application,but due to the resource constraints on sensor nodes, these operations are expensive, which means sensor networks using PKC are susceptible to Denial of Service (DoS) attacks: attackers keep broadcasting bogus messages, which will incur extra costs, thus exhaust the energy of the honest nodes. In addition, the long time to verify each message using PKC increases the response time of the nodes; it is impractical for the nodes to validate each incoming message before forwarding it.We describe the nature of the problem and look for its root causes,further presenting brief insights and suggested approaches for defending against DoS.[5]

Raksha Upadhyay et.al.[2015] have studied Open nature of wireless sensor networks (WSN) makes it vulnerable to outside attacks. Many security threats like denial of service, black hole, sinkhole etc. may affect the network performance. Distributed denials of service (DDOS) attacks are defined as attacks that are launched by a set of malicious entities towards a node or set of nodes. In this work we propose a solution to prevent WSN from DDOS attack using dynamic source routing (DSR). Energy of concerned nodes has been used for detection and prevention of attack. Qualnet 5.2 simulator is used for implementation of the proposed solution.[6]

V. PROBLEM FORMULATION

In the research work big data processing on wireless sensor network different problems are faced that are given below:

- An important such perspective in terms of detecting DoS attacks is to view the problem as that of a classification problem on network state (and not on individual packets or other units) by modelling normal and attack traffic and classifying the current state of the network as good or bad, thereby detecting attacks when they happen.
- There is a resource overloading problem due to DDoS attacks.
- Another problem is the down security problem due to attacks.
- Transmission failures or deadline misses may result in disturbances to the process, degradation of the overall control performance.

VI. CONCLUSION AND FUTURE WORK

Distributed Denial of Service (DDoS) attack is now became a great challenge for the various ISP's (Internet Service Providers) as well as researchers who are working in the field of network security in the word. To handle this great challenge a lot of research and work have been done and based on that a lot of recommended models and mechanisms are there. Complete elimination of denial of service threats is infeasible given the current Internet infrastructure. Internet, being an open environment with no limits set in stone on the number of users, is inherently vulnerable to attacks of the denial of service type. There is no way to predict the parameters of the largest possible flood. Here in this all the above problems are reviewed. In the future these problems are resolved with the help of DSR and Cryptography to achieve better results.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

REFERENCES

[1] Akash Mittal, Prof. Ajit Kumar Shrivastava, Dr. Manish Manoria "A Review of DDOS Attack and its Countermeasures in TCP Based Networks" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011.
[2] Divya Kuriakose,V.Praveena "A Survey on DDoS Attacks and Defense Approaches" International Journal of Innovative Research in Computer and Communication Engineering ,Vol. 1, Issue 8, October 2013.
[3] Saurabh Ratnaparkhi , Anup Bhange " Protecting Against Distributed Denial of Service Attacks and its Classification: An Network Security Issue" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, January 2013
[4] Darshan Lal Meena, Dr. R. S. Jadon " Distributed Denial of Service Attacks and Their Suggested Defense Remedial Approaches" International Journal of Advance Research in Computer Science and Management Studies , Volume 2, Issue 4, April 2014.
[5] Shenam Chugh, Dr. Kamal Dhanda " Denial of Service Attacks" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 8, August 2015
[6] Raksha Upadhyay, Uma Rathore Bhatt, Harendra Tripathi "DDOS Attack Aware DSR Routing Protocol in WSN" International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015.
[7] Liang Hu, Xiaoming Bi, "Research of DDoS Attack Mechanism and Its Defense Frame,"Computer Research and Development (ICCRD), 3rd International Conference, pp. 440–442, March 2011.
[8] Robert Vamosi, "Study: DDoS attacks threaten ISP infrastructure," Online at http://news.cnet.com/8301-1009_3-10093699-83.html, CNET News, Nov. 2008.
[9] Elinor Mills, "Radio Free Europe DDOS attack latest by hactivists," Online at http://news.cnet.com/8301-10784_3-9933746-7.html, CNET News, May. 2008.
[10] Christos Douligeris and Aikaterini Mitrokotsa, "DDoS Attacks And Defence mechanisms: A Classification," in Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology, (ISSPIT'03), pp. 190-193, Dec 2003.
[11] Nisha H. Bhandari, "Survey on DDoS attacks and its detection defense approach," International Journal of Science and Modern Engineering,Vol.1, Issue.3, pp.67-71, Feb 2013.
[12] S.A.Arunmozhi, Y.Venkataramani,"DDoS attack and Defense in wireless ad-hoc Network," International Journal of Network Security & Its Applications Vol.3, No.3, pp.182-187, May 2011.
[13] Monika Sachdeva, Gurvinddr Singh, Krishnan Kumar, Kuldip Singh, " A comprehensive Survey of Distributed Defense Techniques against DDoS Attack," International Journal of Computer Science and Network Security, Vol.9, No.12, pp.7-15, Dec 2009.
[14] Shibiao Lin Tzi-cker Chiueh," A Survey on Solutions to Distributed Denial of Service Attacks", Department of Computer Science Stony Brook University, pp.1-38, Sep 2006.
[15] Shuchi Juyali, Radhika Prabhakar, "A Comprehensive Study of DDOS Attacks and Defense Mechanisms," Journal of Information and Operations Management, Vol.3, Issue.1, 2012.
[16] Quan Jia, Kun Sun, Angelos Stavrou, "CapMan: Capability-based Defense against Multi-Path Denial of Service (DoS) Attacks in MANET,"proceedings of the 20th international conference on computer communication and networks, pp 1-6, 2011.
[17] Antonio Challita, Mona El Hassan, Sabine Maalouf, Adel Zouheiry, " A Survey of DDoS Defense Mechanisms ," The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.
[18] Anurekha, R.,K. Duraiswamy, A. Viswanathan, V.P. Arunachalam, K. Ganesh Kumar, A. Rajivkannan" Dynamic Approach to Defend Against Distributed Denial of Service Attacks Using an Adaptive Spin Lock Rate Control Mechanism," Journal of Computer Science, pp.632-636, 2012.
[19] Puneet Zaroo," A Survey of DDoS attacks and some DDoS defense mechanisms," Advanced Information Assurance (CS 626), 2003.
[20] Guangsen Zhang, Manish Parashar,"Cooperative Defense against DDoS Attacks," Journal of Research and Practice in Information Technology, pp.1-6, 2006.
[21] Wei Ren, Dit-Yan Yeung, Hai Jin, Mei Yang, "Pulsing RoQ DDoS Attack and Defense Scheme in Mobile Ad Hoc Networks," International Journal of Network Security, Vol.4, No.2, pp.227-234, Mar. 2007.
[22] Jelena MIrkovic, Max Robinson, Peter Reither, George Oikonomou, "Distributed Defense against DDoS Attacks," Available:http"//www.isu.edu/~mirkovic/publication/udel_tech_report_2005.pdf, 2005.
[23] Haining Wang Cheng Jin Kang G. Shin" Defense Against Spoofed IP Traffic Using Hop-Count Filtering," Networking, IEEE/ACM Transactions on Networking, vol. 15, pp 1-13, 2007.
[24] A.Anna lakshmi, Dr.K.R.Valluvan "A survey of Algorithms for Defending MANETs against the DDoS Attack," International Journal of Advanced Research in Computer Science and Software Engineering, vol.2, Issue 9, pp.155-164, Sep 2012.