An Analysis of DDoS Attack Detection and Mitigation Using Machine Learning System

R.Sindhu Nayaki[1]
(Research Scholar)
Dept. of Computer Science,
Tamil University,Thanjavur,
Thanjavur Tamil Nadu, India.
e-mail:cs.sindhu2014@gmail.com

A. Senthil Kumar[2]
(Asst. Professor)
Dept of Computer science,
Tamil University, Thanjavur,
Thanjavur Tamil Nadu, India.
e-mail: erodsenthilkumar@gmail.com

Abstract: Nowadays, many companies and/or governments require a secure system and/or an accurate intrusion detection system (IDS) to defend their system service and the user's private information. In network security, developing an accurate discovery system for distributed denial of service (DDos) attacks is one of challenging tasks. DDos attacks jam the network service of the target using multiple bots hijacked by crackers and send frequent packets to the target server. Servers of many companies and/or governments have been victims of the attacks. In such a command by multiple bots from another network and then leave the bots quickly after command execute. The proposed strategy is to develop an intelligent detection system for DDos attacks by detecting patterns of DDos attacks using system packet analysis and exploiting machine learning techniques to study the patterns of DDos attacks. In this study, we analysed large numbers of network packets provided by the Center for applied internet data analysis and Applied the detection system using an Ad-hoc On-demand distance Vector (AODV) and Adaptive information dissemination (AID) protocols. The discovery system is accurate in detecting DDos.

Keywords: *wireless mobile ad-hoc network, security goal, security goal, security attacks, defensive mechanisms, DDoS attack.*

*****

I INTRODUCTION

A. SECURITY OVERVIEW

The term computer security encompasses many related, yet separate, topics. These can be stated as security objectives, and include: control of physical accessibility to the computer (s) and/or network. Prevention of accidental erasure, modification or compromise of data. Detection and prevention of intentional internal security breaches. [1] Detection and prevention of unauthorized of unauthorized external intrusions (hacking).

Network security solutions are loosely divided into categories: hardware, software and human. In this chapter will provide an overview of basic security concepts. Then, it will examine the four security objectives and look at each of the three categories of security solutions. This [2] defection is perhaps a little misleading when it comes to computer and networking Security, as it implies a degree of protection that it is inherently impossible in the modern connectivity-oriented computing environment. This is why the same dictionary provides another definition specific to computer science: "the level to which a program or device is safe from unauthorized use." Implicit in this caveat that the objectives of security and accessibility- the two top priorities on the minds of many network administrators- are, by their very natures, diametrically opposed. The more accessible your data is, the less secure it is. Likewise, the more tightly you secure it, the more you impede accessibility. Any security plan is an attempt to strike likely to encounter in the IT security field.

B. Intrusion Detection System:

An Intrusion [3] Detection System is an application used for monitoring the network and protecting it from the intruder. With the rapid progress on the internet based technology new application areas for computer network have emerged. In instances, the fields like business, financial, industry, security and healthcare sectors the LAN and WAN application have progressed. Allof these application areas made the network an attractive target for the abuse and a big vulnerability for the community. Malicious users or hackers use the oraganization's internal systems to collect information's and cause vulnerabilities like software bugs, lapse in administration, leaving systems to default configuration. As the internet emerging into the society, new stuffs like viruses and worms are imported. The malignant so, the users use different techniques like cracking of password, detecting unencrypted text are used to cause vulnerabilities to the system. Hence, security is needed for the users to secure their system from the intruders. Firewall technique is one of the popular protection techniques and it is used to protect the private network from the public network. IDS are used in network related activities, medical applications, credit card frauds; insurance agency. The goal of nitration detection is to monitor the network assets to detect anomalous behaviour and misuse in network. [4] Intrusion detection concept was introduced in early 1980's after the evolution of internet with surveillance end monitoring the threat. There was a sudden rise in reputation and incorporation in security infrastructure. Since then. Several events in IDS technology have advanced intrusion detection to its current state. James andreson's wrote a paper for a government organization and imported an approach that audit trails contained important information that could be valuable in tracking misuse and understanding led to terrific improvements in the subsystems of every operation system. IDS and Host based intrusion detection system (HIDS) were first defined. In 1983, SRI international and Dorothy dinning began working on a government project that launched a new effort into intrusion detection system development. Around 1990s the revenues are generated and intrusion detection market has been raised. Real secure is an intrusion detection network developed by ISS. After a year, Cisco recognized the priority for network intrusion detection developed and purchased the wheel group for attaining the security solutions. The government actions like federal intrusion detection networks (FID Net) were designed under presidential decision directive 63 is also adding impulse to the IDS.

II SYSTEM ANALYSIS

A. *Existing System:*

Compared with other DDoS[5] detection methos, detecting by entropy is proved to have many advantages, such as simpler, higher sensitivity, lowew rate of false positives. Many attackers in different locations continuously send a great deal of packets at the same time, which is out of the target device's processing ability, making the legitimate user out of service. This enables attackers can launch DDos attacks towards SDN network from multiple layers. It works well when the attack traffic is very huge.

Demerits:

The sub channels are allocated to optimize throughput and maintain the proportional stream rate ratios. It may cause bottleneck problem in the wireless network. Sometimes it leads to network shut down with whole date loss. The Performance consequently depends on the scheduling strategy employed.

B. Proposed System:

Wireless communication technologies have made great progress the experience of mobile users.SDN can greatly facilitate big data acquisition, transmission, storage, and processing and big data will impact the design and operation of SDN.Distributed denial of service(DDoS) flooding attacks is the main methods to destroy the availability of the sever or the network

Advantages:

The problems in the existing approach are overcome by using efficient scheduling algorithm. Relay [6] cooperation mechanisms allow multiple receivers to simultaneously transmit the multicast data on the same transmission resource. It helps retain the

broadcast nature of the traffic on the access hop, making cooperation a critical component in improving multicast performance.

III MODULES

A. Node Formation:

Neighbouring node IDs are presented with a constant size using a Bloom filter. The Bloom filter output (BFO) is used as a proof. A newly deployed node generates different proofs according to the collected neighbouring node IDs. Until collecting the entire neighbouring node IDs. The proofs are delivered to a randomly selected node in the network. Here, the delivery frequency increases proportionally to the number of the collected neighbouring node IDs. The strategy nslowly increases traffic between the neighbouring nodes and their randomly selected nodes.

B. Route Discovery Phase:

The route discovery phase is to establish an end-to-end route, the source node broadcasts the Route Request Packet (PPEQ) containing the identities of the source (IDS) and the [7] destination (IDD)nodes where the destination node will send the Acknowledgement to the source from that message the route will be discovered and maintained that route for communication till all packets get transmitted.

C. Flow Label Propagation:

This module classifies traffic flows based on the flow level statistical properties. A flow consists of successive IP packets having the same 5-tuple :{ source ip, source port, destination ip, destination port, transport protocol}. Traffic flows are constructed by inspecting the headers of IP packets captured by the system one computer network. For the purpose of classification, each flow can be represented using a set of flow level statistical properties such as number of packets and packet size.

D. Nearest Cluster Based Classifier:

Nearest cluster based classifier (NCC) due to its good performance. The k-means clustering aims to partition traffic flows into k clusters (k<\T\0,C={C1,C2,….,CK}, so as to minimize the within –cluster[8] sum of squares. The traditional k-means algorithm uses an iterative refinement technique. This replacement can significantly reduce the amout of unknown clusters and produce more complete traffic classes.

E. Compound Classification:

The compound classification on the correlated flows[9] modelled by a bog-of-flows (BOF) instead of classifying individual traffic flows. All flows sharing the same 3-tuple are generated by the same application and should belong to the same traffic class. The correlation information can be utilized to improve the classification accuracy. This observation becomes the motivation of conducting compound classification.

IV Conclusion

A DDoS detection method based on fuzzy synthetic evolution decision-making model. Also make a comparable experiment to show its advantage to other DDoS detection algorithm based on single factor. DDoS attacks divide the attacks into three levels and used these levels of attacks data to initialize the parameters of the DDoS [4] detection method. Host-based DDoS detection framework called BRAIN is proposed that adds another dimension to detect DDoS attacks in reds-time. The results illustrate that the inclusion of hardware behaviour into detection increases accuracy significantly. BRAIN is a low cost, adaptive and highly accurate DDoS detection framework with 99.8% accuracy.[10] Anomaly detection in BRAIN is doctrine around behaviour derived from hardware events. It may be even possible to model and detect other network attacks using behaviour derived from these hardware events.

V Future Enhancement

The DoS is a pure hardware targeted attack which can be much faster and requires fewer resources that using a bonnet or a root/server in a DDoS attacks. Because of these features, and the potential and high probability of security exploits on network enabled embedded devices (NEEDs), this technique has come to the attention of numerous hacking communities. Using entropy as a summarization tool, it is able to show that the analysis of feature distributions leads to significant advances on two fronts: (1) it enable highly sensitive detection of a wide range of anomalies, augmenting detections by volume-based methods, and (2) it enables automatic classification of anomalies via unsupervised learning. It is demonstrated the utility of treating anomalies as events that alter traffic feature distributed shown that treating anomalies, in understanding the structure of anomalies, and in classifying anomalies. The work proposed that entropy is an effective metric to capture unusual changes induced by anomalies in traffic feature distributions. The work in has demonstrated the utility of treating anomalies as events that alter traffic feature distributions. It shows that treating anomalies in this manner yields considerable diagnostic power, in detecting new anomalies, in understanding the structure of anomalies, and in classifying anomalies. It also shows that entropy is an effective metric to capture unusual changes induced by anomalies in traffic feature distributions.

References

[1] v. jyothi, s . k. addepalli, and R. karri, “ deep packet field extraction engine DPFEE A pre-processor for network instrusion detection and Denial-of-service detection systems,” IEEE ICCD,PP.287-293,2015.

[2] Imperva, “Q2 2015 Global DDoS threat landscapt: assaults resemble advanced persistent threats”, https://www.incapsula.com/blog/ddos-globalthreat-landscape-report-q2-2015.html.

[3] X. wang and R. karri ,” numchecker/; detecting kernel control-flow modifying roolits by using hardware performance counters,”IEEE DAC,PP.1-7,2013.

[4] K.Kato and v.klyuev, “An intelligent DDoS attacks detection system using packet analysis and support vector machine,”IJICR,PP.478-485,2014.

[5] K. Devi, G. Preetha, G. Selvaram, and S.M. Shalinie, “An impact analysis:Real time DDoS attacks detection and mitigation using machine learning,”ICRTIT,PP.-7,2014.

[6] a. Ramamoorthi, T. subbulakshmi, and S. M Shaline, “ Real time detection and classification of ddos attacks using enhanced svm with string kernels,”ICRTIT,PP 91-96,2011.

[7] Z. Li ,c. Wilson, Z jiang, y . zhao, c. jin,Z.-L zhang, and Y. Dai, “Efficient batched synchronization in drop box-like cloud storage services,” In proc. ACM/IFIP/USENIX 14th int. middleware conf,2013,pp.307_327.

[8] A.Li.X. yang,S. Kandula,and M.Zhang, “cloudcmp: comaring public cloud providers,” in proc.ACM SIGCOMN Internet meas. Conf, 200,pp.1-4.

[9] A Bessani, M. cotteia, B. Quaresma, F.Andr_e, and p. souse, “depsky. Dependable and secure stoage in a cloud-of-clouds,” in proc 6th conf. comut system, 2013, pp. 31-46.

[10] P.Wendell, J. W. Jiang, M. J. Freedman, and j. Rexfod, “Donar: Decentralized server selection for cloud sevices,” in proc. ACM SIGCOMM conf.,2010,pp.23-242.