Securing Corporate Networks against Denial-of Service Attack Detection Using Multivariate Correlation Analysis

Roopadevi B N[1], A.NarayanaRao [2]

[1] PG Student, Dept. of CSE, Shree Institute of Technical Education, Tirupati, A.P, India1
[2] Associate Proffessor, HOD. Dept. of CSE, Shree Institute of Technical Education, Tirupati, A.P, India2

Abstract— Interconnected systems such as Web servers, database servers etc, are now under threads from network attackers. As one of most common attack is Denial-of-Service attacks cause serious problem on these computing systems. In this we present a DoS attack detection system that uses Multivariate Correlation Analysis(MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. Our MCA-based DoS attack detection system employs the principle of anomaly-based detection in attack recognition. This makes our solution capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only. The effectiveness of our proposed detection system is evaluated using KDD Cup 99 dataset, and the influences of both non-normalized data and normalized data on the performance of the proposed detection system are examined.

***Keywords*—Denial-of-Service attack, Network traffic characterization, Multivariate correlations, Triangle area, KDD cup 99 dataset.**

I. INTRODUCTION

Denial of service attack is a malicious attempt to make a server or a network resource unavailable to the users, usually by temporarily interrupting the services of a host connected to the internet. When this attack is caused the user is deprived of services of resource they would normally expect to have current computer networks are effected by major threats that are caused by these denial of service attacks. This attack does not result in theft of information or other security losses. This type of attack on network is designed to bring network to its knees by flooding it with useless traffic.Early DoS attacks were technical games played among underground attackers. For example, an attacker might want to get control of an IRC channel via performing DoS attacks against the channel owner. They sometime coordinately expressed their views via launching DoS attacks against organizations whose policies they disagreed with. DoS attacks also appeared in illegal actions. Companies might use DoS attacks to knock off their competitors in the market.

In recent years, DDoS attacks have increased in frequency, sophistication and severity due to the fact that computer vulnerabilities are increasing fast (CERT 2006, Houle *et al.* 2001), which enable attackers to break into and install various attacking tools in many computers. Wireless networks also suffer from DoS attacks because mobile nodes (such as laptops, cell phones, etc.) share the same physical media for transmitting and receiving signals; and mobile computing resources (such as bandwidth, CPU and power) are usually more constrained than those available to wired nodes. In a wireless network, a single attacker can easily forge, modify or inject packets to disrupt connections between legitimate mobile nodes and cause DoS effects. In this article, we will provide an overview on existing DoS attacks and major defense.

II. DOS ATTACKS IN THE INTERNET

a. Attack Techniques

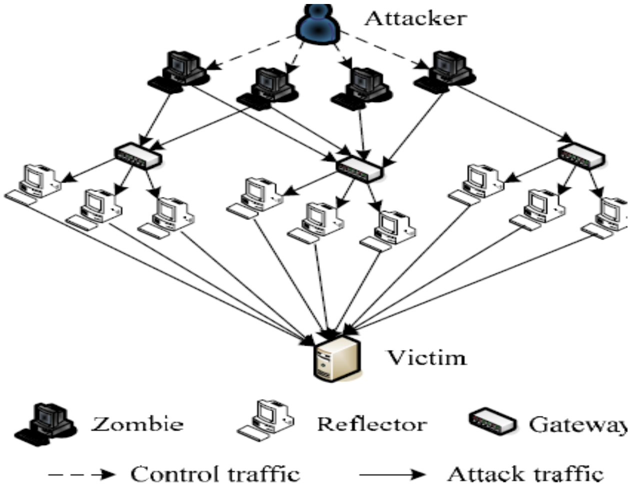
Many attack techniques can be used for DoS purpose as long as they can disable service or downgrade service performance by exhausting resources for providing services. Although it is impossible to enumerate all existing attack techniques, we describe several representative network based and host based attacks.

b. Network Based Attacks

TCP SYN Flooding. DoS attacks often exploit stateful network protocols, because these protocols consume resources to maintain states. TCP SYN flooding is one of such attacks and had a wide impact on many systems. When a client attempts to establish a TCP connection to a server, the client first sends a SYN message to the server. The server then acknowledges by sending a SYN-ACK message to the client. The client completes the establishment by responding with an ACK message. The connection between the client and the server is then opened, and the service-specific data can be exchanged between them.

ICMP Smurf Flooding. ICMP is often used to determine if a computer in the Internet is responding. To achieve this task, an ICMP echo request packet is sent to a computer. If the computer receives the request packet, it will return an ICMP echo reply packet. In a smurf attack, attacking hosts forge ICMP echo requests having the victim's address as the source address and the broadcast address of these remote networks as the destination address (CERT 1998). As in the below Figure, if the router of the remote network does not filter the special crafted packets, they will be delivered to all computers on that network. These computers will then send ICMP echo reply packets back to the source carried in the request packets. The victim's network is thus congested. So there is no proper transfer of data between the client and the server.

The most common type of Denial of service attack involves flooding target resource with external communication requests. This overload prevents the resource from responding to legitimate traffic or slows its response so significantly that is rendered effectively unavailable.



By patching or redesigning the implementation of TCP and ICMP protocols, current networks and systems have incorporated new security features to prevent TCP and ICMP attacks. Note that UDP flooding is similar to flash crowds that occur when a large number of users try to access the same server simultaneously. However, the intent and the triggering mechanisms for DDoS attacks and flash crowds are different.

c. Intermittent Flooding

Attackers can further tune their flooding actions to reduce the average flooding rate to a very low level while achieving equivalent attack impacts on legitimate TCP connections. In shrew attacks attacking hosts can flood packets in a burst to congest and disrupt existing TCP connections. When a QoS enabled server receives a burst of service requests, it will temporarily throttle incoming requests for a period until previous requests have been processed.

Thus, attackers can flood requests at a pace to keep the server throttling the incoming requests and achieve the DoS effect. Guirguis's study showed that a burst of 800 requests can bring down a web server for 200 seconds, and thereby the average flooding rate could be as low as 4 requests per second.

d. Host Based Attacks

Besides misusing network protocols, attackers can also launch DoS attacks via exploiting vulnerabilities in target's applications and systems. Different from network based attacks, this type of attacks are application specific, i.e., exploiting particular algorithms , memory structure, authentication protocols , implementation (CERT 1997), etc. Attacks can be launched either from a single host as a conventional intrusion or from a number of hosts as a network based DDoS attack. The traffic of host based attacks may not be as high as network based attacks, because application flaws and deficiencies can easily crash applications or consume a tremendous amount of computer resources. Consequently, mutual authentication cannot be done quickly and service performance is downgraded. Researchers also found that attackers could exploit algorithmic deficiencies in many applications' data structures to launch low-bandwidth DoS attacks.

In the worst case where all n inputs collide, O(n^2) computation will be required. It is found that attackers can easily figure out such collision inputs in some hash algorithms, and demonstrated that attackers could bring down two versions of Perl, the Squid web proxy, and the Bro intrusion detection system via inputting strings that collide to crash the critical hash tables in these applications.

III. EXISTING SYSTEM:

Network-based detection systems can be classified into two main categories, namely misuse-based detection systems and anomaly-based detection systems. Misuse-based detection systems detect attacks by monitoring network activities and looking for matches with the existing attack signatures. In spite of having high detection rates to known attacks and low false positive rates, misuse-based detection systems are easily evaded by any new attacks and even variants of the existing attacks. Furthermore, it is a complicated and labor intensive task to keep signature database updated because signature generation is a manual process and heavily involves network security expertise.

Disadvantages of Existing System:

- Most existing IDS are optimized to detect attacks with high accuracy. However, they still have various disadvantages that have been outlined in a number of publications and a lot of work has been done to analyze IDS in order to direct future research.

- Besides others, one drawback is the large amount of alerts produced.

IV. PROPOSED SYSTEM:

Here, we present a DoS attack detection system that uses Multivariate Correlation Analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. Our MCA-based DoS attack detection system employs the principle of anomaly-based detection in attack recognition.

The DoS attack detection system presented in this paper employs the principles of MCA and anomaly-based detection. They equip our detection system with capabilities of accurate characterization for traffic behaviors and detection of known and unknown attacks respectively. A triangle area technique is developed to enhance and to speed up the process of MCA. A statistical normalization technique is used to eliminate the bias from the raw data.

Advantages of proposed system:

- To find various attacks from the user to avoid Network Intrusion.
- This makes the solution capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only.
- More detection accuracy.
- Accurate characterization for traffic behaviors and fewer false alarms.

V. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and its constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Implementation of any software is always preceded by important decisions regarding selection of the platform, the language used, etc. These decisions are often influenced by several factors such as the real environment in which the system works the speed that is required, the security concerns, other implementation specific details etc. There are two major implementation decisions that have been made before the implementation of this project. The implementation phase is required to run the project.

a. Multivariate Correlation Analysis:

In this Multivariate Correlation Analysis, in which the “Triangle Area Map Generation” module is applied to extract the correlations between two distinct features within each traffic record coming from the first step or the traffic record normalized by the “Feature Normalization” module in this step. The occurrence of network intrusions cause changes to these correlations so that the changes can be used as indicators to identify the intrusive activities. All the extracted correlations, namely triangle areas stored in Triangle Area Maps (TAMs), are then used to replace the original basic features or the normalized features to represent the traffic records. This provides higher discriminative information to differentiate between legitimate and illegitimate traffic records.

Algorithm for Multivariate Correlation Analysis:

```
**Require:** Observed traffic record $x^{observed}$, normal profile $Pro : (N(\mu, \sigma^2), \overline{TAM^{normal}_{lower}}, Cov)$ and parameter $\alpha$
Generate $TAM^{obsverved}_{lower}$ for the observed traffic record $x^{observed}$
$MD^{observed} \leftarrow MD(TAM^{obsverved}_{lower}, \overline{TAM^{normal}_{lower}})$
**if** $(\mu - \sigma * \alpha) \leq MD^{observed} \leq (\mu + \sigma * \alpha)$ **then**
    **return** Normal
**else**
    **return** Attack
**end if**
```

b. Evaluation of Attack detection

During the evaluation, the 10 percent labeled data of KDD Cup 99 dataset is used, where three types of legitimate traffic (TCP, UDP and ICMP traffic) and six different types of DoS attacks (Teardrop, Smurf, Pod, Neptune, Land and Back attacks) are available. All of these records are first filtered and then are further grouped into seven clusters according to their labels. We show the evaluation results in graph of receiver operating characteristics(ROC) curves.

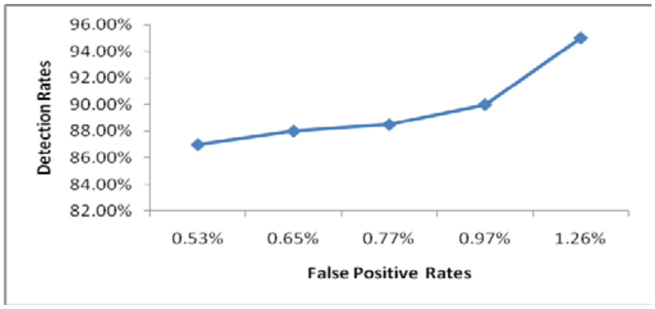


Fig a: ROC curve for analyzing original data

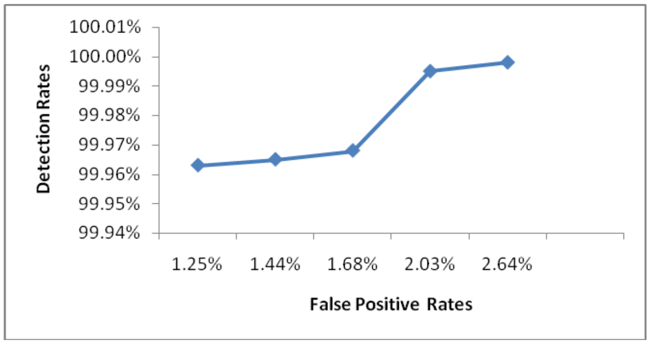
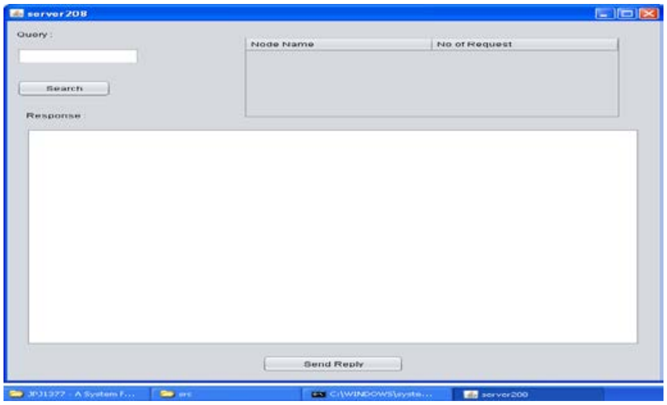


Fig b: ROC curve for normalized data

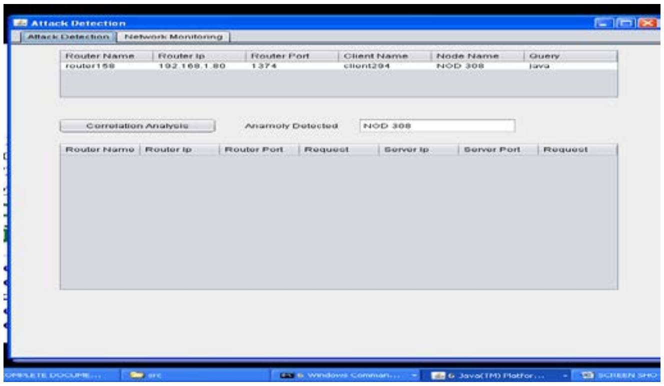
This graphs shows DoS detection for original data and for normalized data. The false positive rates are recorded against the detection rates and analyzed for both original data and normalized data.

VI. RESULTS



Node Name	No of Request

Fig 1: First initialize the server node by running server



Router Name	Router Ip	Router Port	Client Name	Node Name	Query
router158	192.168.1.80	1374	client294	NOD 308	java

Anamoly Detected: NOD 308

Router Name	Router Ip	Router Port	Request	Server Ip	Server Port	Request

Fig 2: IDS system finds anomaly occurred or not also performs data aggregation

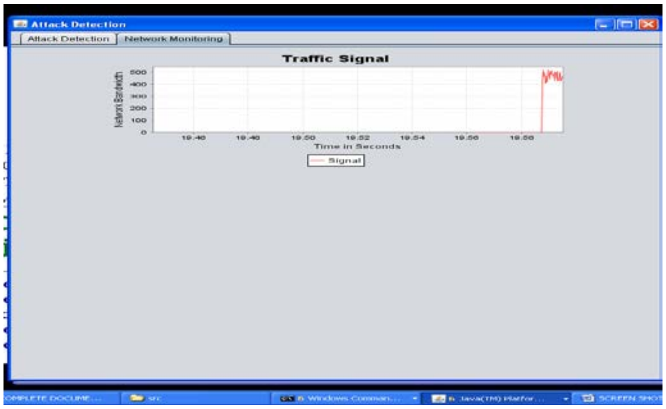


Fig 3: Traffic signal is shown at the IDS system.

VII. CONCLUSION:

Here presented a MCA-based DoS attack detection system which is powered by the triangle-area based MCA technique and the anomaly-based detection technique. The former technique extracts the geometrical correlations hidden in individual pairs of two distinct features within each network traffic record, and offers more accurate characterization for network traffic behaviours. The latter technique facilitates the system to be able to distinguish both known and unknown DoS attacks from legitimate network traffic. The results have revealed that when working with non-normalized data, our detection system achieves maximum 95.20% detection accuracy. The proposed system achieves equal or better performance in comparison with the two state-of-the-art approaches.

REFERENCES:

[1] C. Yu, H. Kai, and K. Wei-Shinn, "Collaborative Detection of DDoS Attacks over Multiple Network Domains," Parallel and Distributed Systems, IEEE Transactions on, vol. 18, pp. 1649-1662, 2007.

[2] W. Wang, X. Zhang, S. Gombault, and S. J. Knapskog, "Attribute Normalization in Network Intrusion Detection," The 10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN), 2009, pp. 448-453.

[3] G. Thatte, U. Mitra, and J. Heidemann, "Parametric Methods for Anomaly Detection in Aggregate Traffic," Networking, IEEE/ACM Transactions on, vol. 19, no. 2, pp. 512-525, 2011.

[4] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient," Parallel and Distributed Systems, IEEE Transactions on, vol. 23, pp. 1073-1080, 2012.

[5] V. Paxson, "Bro: A System for Detecting Network Intruders in Realtime," *Computer Networks*, vol. 31, pp. 2435-2463, 1999

[6] P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E. Vzquez, "Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges," *Computers & Security*, vol. 28, pp. 18-28, 2009.

[7] D. E. Denning, "An Intrusion-detection Model," *IEEE Transactions on Software Engineering*, pp. 222-232, 1987.

[8] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, "DDoS attack detection method using cluster analysis," Expert Systems with Applications, vol. 34, no. 3, pp. 1659-1665, 2008.

[9] A. Tajbakhsh, M. Rahmati, and A. Mirzaei, "Intrusion detection using fuzzy association rules," Applied Soft Computing, vol. 9, no. 2, pp. 462-469, 2009.

[10] J. Yu, H. Lee, M.-S. Kim, and D. Park, "Traffic flooding attack detection with SNMP MIB using SVM," Computer Communications, vol. 31, no. 17, pp. 4212-4219, 2008.

[11] W. Hu, W. Hu, and S. Maybank, "AdaBoost-Based Algorithm for Network Intrusion Detection," Trans. Sys. Man Cyber. Part B, vol. 38, no. 2, pp. 577-583, 2008.

[12] S. T. Sarasamma, Q. A. Zhu, and J. Huff, "Hierarchical Kohonenen Net for Anomaly Detection in Network Security," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 35, pp. 302-312, 2005.

[13] S. Jin, D. S. Yeung, and X. Wang, "Network Intrusion Detection in Covariance Feature Space," *Pattern Recognition*, vol. 40, pp. 2185- 2197, 2007.