"IMPLEMENTATION OF ATTACK DETECTION USING THE MAHALOBIS TECHNIQUE"

[1]UJWAL MUDE
Department of Computer Science & Engineering, Abha Gaikwad-Patil Collage of Engineering Nagpur, India
ujjwalmule@gmail.com

[2]SAKSHI GOTEKAR
Department of Computer Science & Engineering, Abha Gaikwad-Patil Collage of Engineering Nagpur, India

[3]MAYURI SURYAWANSHI
Department of Computer Science & Engineering, Abha Gaikwad-Patil Collage of Engineering Nagpur, India
Mayurisuryawanshi1999@gmail.com

[4]SANJIVANI LIKHAR
Department of Computer Science & Engineering, Abha Gaikwad-Patil Collage of Engineering Nagpur, India
sanjivanilikhar03@gmail.com

PROF. YUVRAJ SURYAWANSHI
Department of Computer Science & Engineering, Abha Gaikwad-Patil Collage of Engineering Nagpur, India

ABSTRACT: *An Intrusion Detection System is a system for detecting intrusions and reporting them accurately to the proper authority. Intrusion Detection Systems are usually specific to the operating system that they operate in and are an important tool in the overall implementation an organization's information security policy, which reflects an organization's statement by defining the rules and practices to provide security. In this project design an intrusion detection system to detecting the all types of attack in the network. i. e. IP Address Spoofing, DDOS Attacks, packet Sniffer Attack etc. and implementing the solution to one of these attack.*

Keywords: Intrusion Detection System, IP Address Spoofing, DDOS Attacks, packet Sniffer Attack

1. INTRODUCTION

A packet sniffer, sometimes referred to as a network monitor or network analyzer, can be used legitimately by a network or system administrator to monitor and troubleshoot network traffic. Using the information captured by the packet sniffer an administrator can identify erroneous packets and use the data to pinpoint bottlenecks and help maintain efficient network data transmission. In its simple form a packet sniffer simply captures all of the packets of data that pass through a given network interface. Typically, the packet sniffer would only capture packets that were intended for the machine in question. However, if placed into promiscuous mode, the packet sniffer is also capable of capturing ALL packets traversing the network regardless of destination.

2. PROBLEM DEFINITION

As a network administrator who needs to identify, diagnose, and solve network problems, a company manager who wants to monitor user activities on the network and ensure that the corporation's communications assets are safe, or a consultant who has to quickly solve network problems for clients. It is difficult to identify the problems if the network traffic is not tracked, as an administrator in general we depend on the analyzer provided by the operating system (if any) or the antivirus software that is installed to provide real-time network security. However, it is identified that these systems provide specific set of reports which may not be enough for an administrator to trace all the problems. To handle these types of issues we want to implement a specific network analyzer that can track all the incoming and outgoing calls.

3. OBJECTIVES

- The main objective of this system shows how real time network connection behavior can be modeled.
- The objective of the system is to create a new set of rules during run time. So the intruder cannot be able to attack the system with virus
- Detection of attack in the network.

4. RELATED WORK

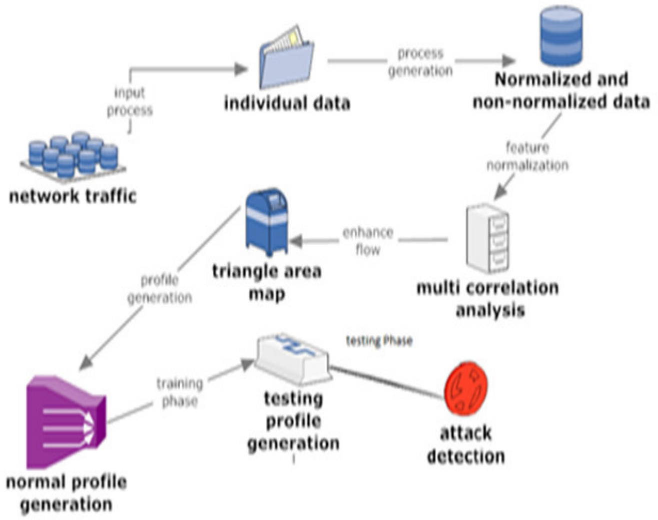
Garcı´a-Teodoroa et. al. [1] begins with a review of the most well-known anomaly-based intrusion detection techniques. Then, available platforms, systems under development and research projects in the area are presented. Finally, we outline the main challenges to be dealt with for the wide scale deployment of anomaly-based intrusion detectors, with special emphasis on assessment issues.

Signature and anomaly-based systems are similar in terms of conceptual operation and composition. The main differences between these methodologies are inherent in the concepts of ‘‘attack’’ and ‘‘anomaly’’. An attack can be defined as ‘‘a sequence of operations that puts the security of a system at risk’’. An anomaly is just ‘‘an event that is suspicious from the perspective of security’’. Based on this distinction, the main advantages and disadvantages of each IDS type can be pointed out.

Yu Chen ET. AL. [2] presents a new distributed approach to detecting DDoS (distributed denial of services) flooding attacks at the traffic flow level. The new defense system is suitable for efficient implementation over the core networks operated by Internet service providers (ISP). At the early stage of a DDoS attack, some traffic fluctuations are detectable at Internet routers or at gateways of edge networks. We develop a distributed change-point detection (DCD) architecture using change aggregation trees (CAT). The idea is to detect abrupt traffic changes across multiple network domains at the earliest time. Early detection of DDoS attacks minimizes the flooding damages to the victim systems serviced by the provider.

The system is built over attack-transit routers, which work together cooperatively. Each ISP domain has a CAT server to aggregate the flooding alerts reported by the routers. CAT domain servers collaborate among themselves to make the final decision. To resolve policy conflicts at different ISP domains, a new secure infrastructure protocol (SIP) is developed to establish the mutual trust or consensus. We simulated the DCD system up to 16 network domains on the DETER test bed, a 220-node PC cluster for Internet emulation experiments at USC Information Science Institute. Experimental results show that 4 network domains are sufficient to yield 98% detection accuracy with only 1% false-positive alarms. We prove that this DDoS defense system can scale well to cover 84 AS domains. This security coverage is wide enough to safeguard most ISP core networks from real-life DDoS flooding attacks.

5. PROPOSED SYSTEM



The proposed system categories of four modules

- Loading and preprocessing dataset
- Mahalanobis Distance
- Threshold Selection
- Attack detection

5.1 Loading and preprocessing dataset:

In this module we are going to select the input spatial dataset. After the load the spatial dataset which contains geometric relevant information. After loading, view the required data. In this process we remove the unwanted values like null, missing tuples etc.

5.2 Mahalanobis Distance

Mahalanobis distance (MD) used to extract the correlations between the selected packet payload features It works with network packet payloads. Mahalanobis distance is adopted to measure the dissimilarity between traffic records Attack detection based on Mahalanobis distance.

5.3 Threshold Selection:

In this module is to distinguish DoS attacks from legitimate traffic The threshold given is used to differentiate attack traffic from the legitimate one. Normal profile is greater than the threshold, it will be considered as an attack.

It is powered by the triangle-area based MCA technique and the anomaly-based detection technique.

5.4 Attack detection

Attack detection system that uses multivariate correlation analysis (MCA) for accurate network traffic. It characterization by extracting the geometrical correlations between network traffic features. It compares the individual tested profiles with the respective stored normal profiles.

6. RESULT ANALYSIS

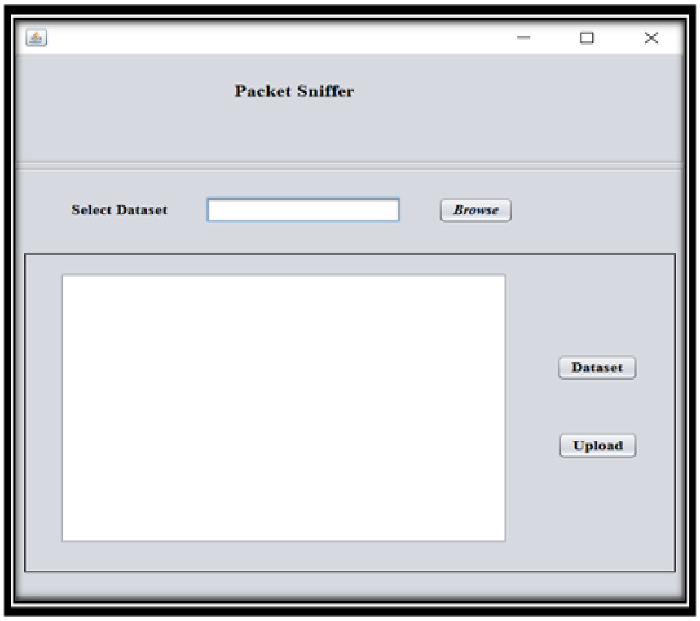
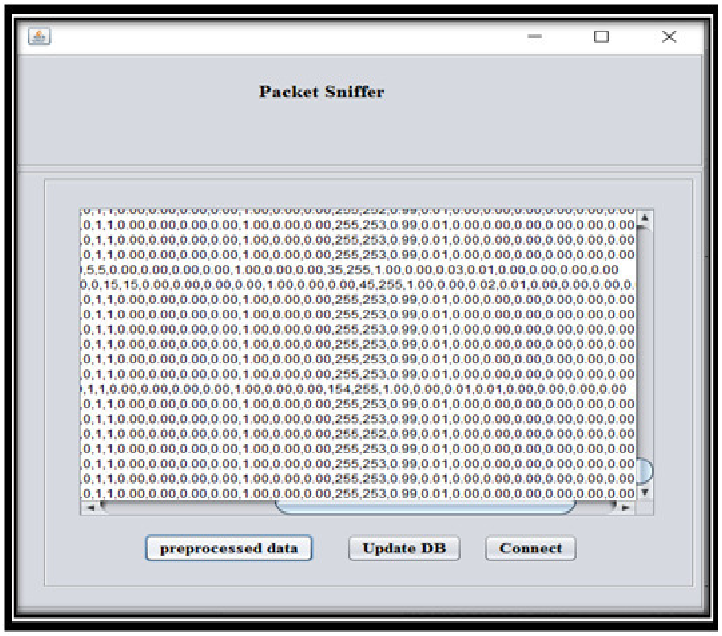
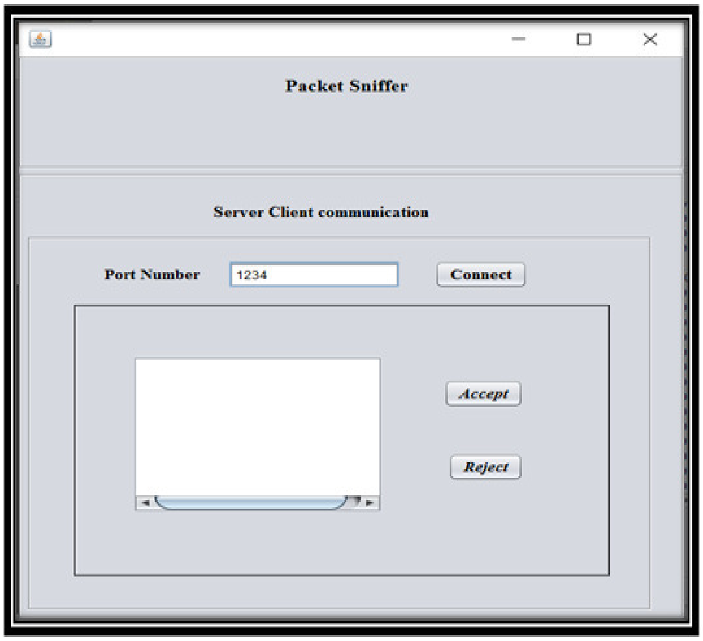


Figure 1: Database Selection



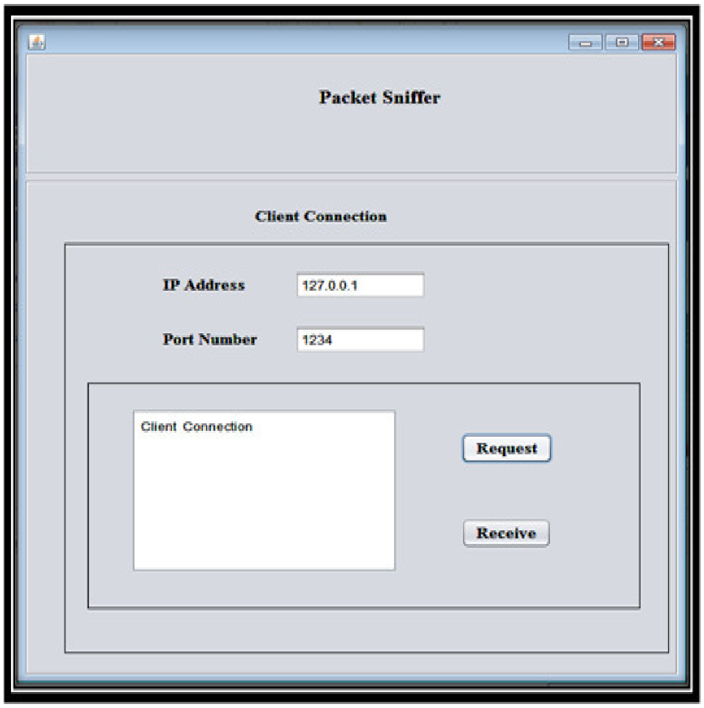
```
,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,252,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.00
,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,253,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.00
,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,253,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.00
,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,253,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.00
,5,5,0.00,0.00,0.00,0.00,1.00,0.00,0.00,35,255,1.00,0.00,0.03,0.01,0.00,0.00,0.00,0.00
0,0,15,15,0.00,0.00,0.00,0.00,1.00,0.00,0.00,45,255,1.00,0.00,0.02,0.01,0.00,0.00,0.00,0.
,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,253,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.00
,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,253,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.00
,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,253,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.00
,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,253,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.00
,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,253,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.00
,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,253,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.00
,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,154,255,1.00,0.00,0.01,0.01,0.00,0.00,0.00,0.00
,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,253,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.00
,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,253,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.00
,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,252,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.00
,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,253,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.00
,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,253,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.00
,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,253,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.00
,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,253,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.00
```

Figure 2: Data Preprocessing



Port Number: 1234

Figure 3: Server Client Communication

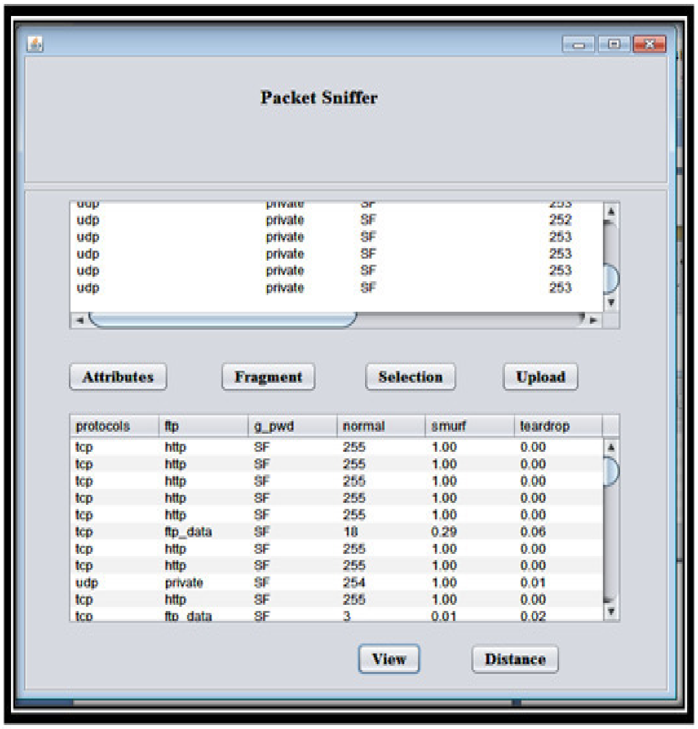


IP Address: 127.0.0.1

Port Number: 1234

Client Connection

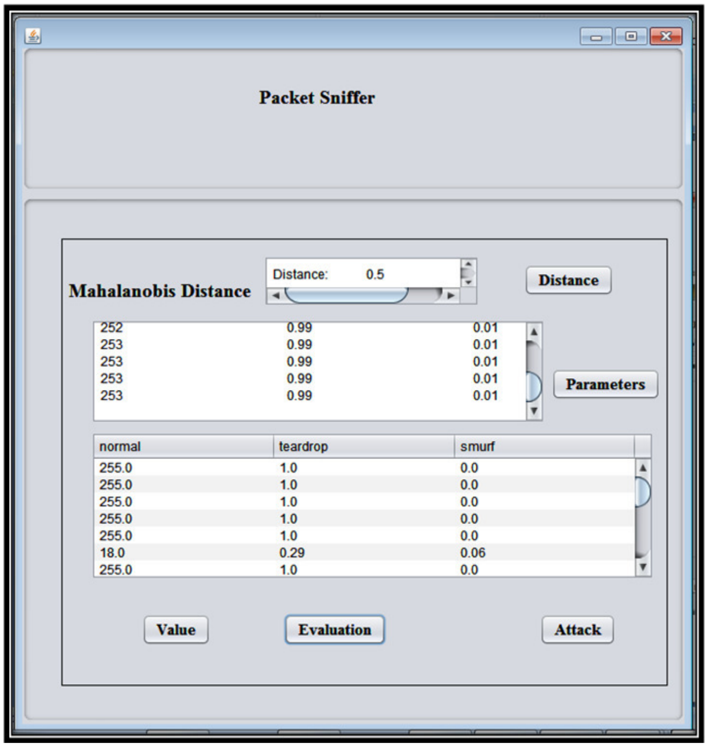
Figure 4: Client Connection



udp	private	SF	253
udp	private	SF	252
udp	private	SF	253
udp	private	SF	253
udp	private	SF	253
udp	private	SF	253

protocols	ftp	g_pwd	normal	smurf	teardrop
tcp	http	SF	255	1.00	0.00
tcp	http	SF	255	1.00	0.00
tcp	http	SF	255	1.00	0.00
tcp	http	SF	255	1.00	0.00
tcp	http	SF	255	1.00	0.00
tcp	ftp_data	SF	18	0.29	0.06
tcp	http	SF	255	1.00	0.00
tcp	http	SF	255	1.00	0.00
udp	private	SF	254	1.00	0.01
tcp	http	SF	255	1.00	0.00
tcp	ftp_data	SF	3	0.01	0.02

Figure 4: Attribute Selection

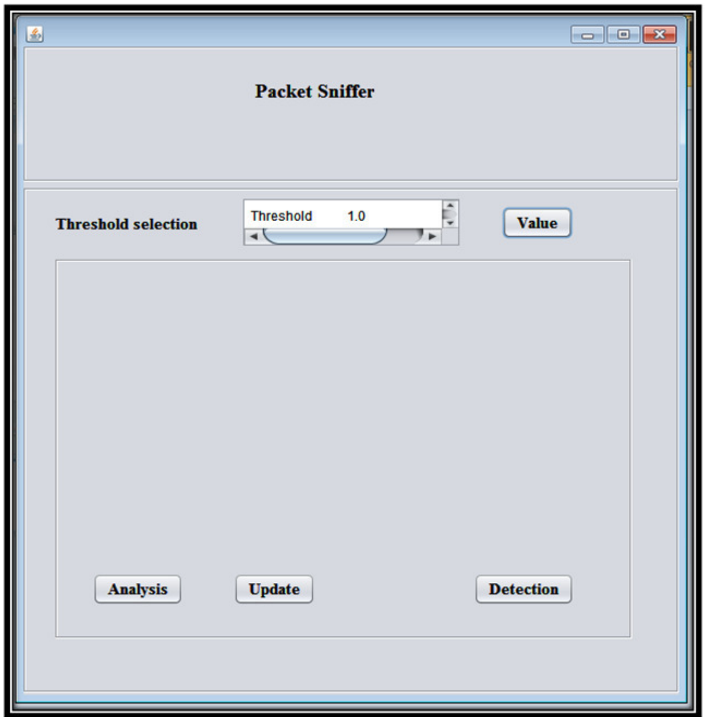


Distance: 0.5

252	0.99	0.01
253	0.99	0.01
253	0.99	0.01
253	0.99	0.01
253	0.99	0.01

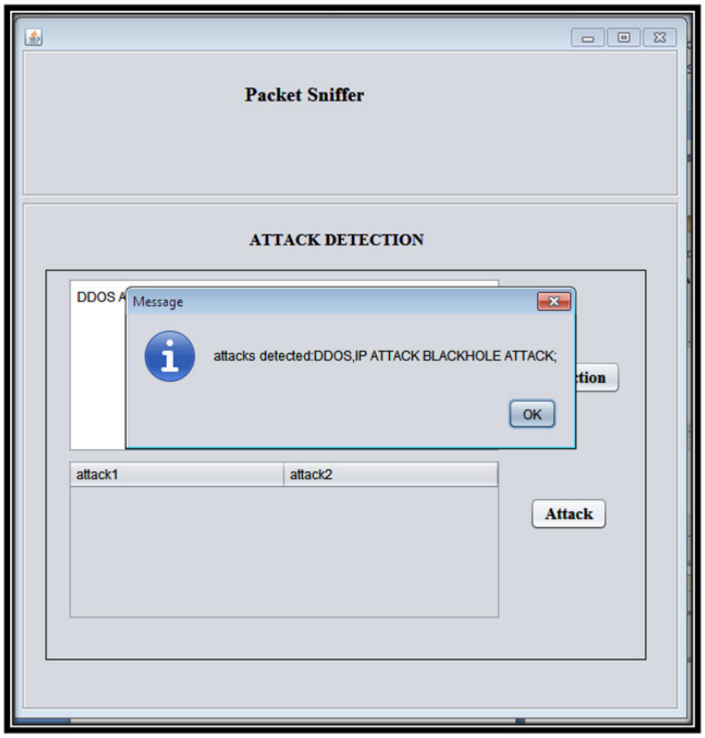
normal	teardrop	smurf
255.0	1.0	0.0
255.0	1.0	0.0
255.0	1.0	0.0
255.0	1.0	0.0
255.0	1.0	0.0
18.0	0.29	0.06
255.0	1.0	0.0

Figure 5: Mahalanobis Distance



Threshold 1.0

Figure 6: Threshold value



attacks detected:DDOS,IP ATTACK BLACKHOLE ATTACK;

attack1	attack2

Figure 7: Detected Attack

7. CONCLUSION

This paper has presented an 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 behaviors. The latter technique facilitates our system to be able to distinguish both known and unknown DoS attacks from legitimate network traffic. Such a system can be as simple as a straightforward system based on packet thresholds: Only N SYN packets are allowed to hit the server in unit time and excess SYN packets may not be allowed. The system can also be as complex as a probabilistic system which models various probability distributions for the various TCP flags.

8. REFERENCES

[1] P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E. Vzquez, “Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges,” Computers and Security, vol. 28, pp. 18-28, 2009.

[2] V. Paxson, “Bro: A System for Detecting Network Intruders in Real-Time,” Computer Networks, vol. 31, pp. 2435-2463, 1999.

[3] D.E. Denning, “An Intrusion-Detection Model,” IEEE Trans. Software Eng., vol. TSE-13, no. 2, pp. 222-232, Feb. 1987.

[4] 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.

[5] A. Tajbakhsh, M. Rahmati, and A. Mirzaei, “Intrusion Detection Using Fuzzy Association Rules,” Applied Soft Computing, vol. 9, no. 2, pp. 462-469, 2009.

[6] J. Yu, H. Lee, M.-S. Kim, and D. Park, “Traffic Flooding Attack Detection with SNMP MIB Using SVM,” Computer Comm., vol. 31, no. 17, pp. 4212-4219, 2008.

[7] W. Hu, W. Hu, and S. Maybank, “AdaBoost-Based Algorithm for Network Intrusion Detection,” IEEE Trans. Systems, Man, and Cybernetics Part B, vol. 38, no. 2, pp. 577-583, Apr. 2008.

[8] C. Yu, H. Kai, and K. Wei-Shinn, “Collaborative Detection of DDoS Attacks over Multiple Network Domains,” IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 12, pp. 1649-1662, Dec. 2007.

[9] G. Thatte, U. Mitra, and J. Heidemann, “Parametric Methods for Anomaly Detection in Aggregate Traffic,” IEEE/ACM Trans. Networking, vol. 19, no. 2, pp. 512-525, Apr. 2011.

[10] S.T. Sarasamma, Q.A. Zhu, and J. Huff, “Hierarchical Kohonenen Net for Anomaly Detection in Network Security,” IEEE Trans. Systems, Man, and Cybernetics, Part B: Cybernetics, vol. 35, no. 2, pp. 302-312, Apr. 2005.

[11] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, “Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient,” IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 6, pp. 1073-1080, June 2012.

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