International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 2, Issue 8, August 2015)

# Outbreak Detection of Denial of Service

Anoop Kolsur
Telecommunication
Dayananda Sagar College of Engineering
VTU, Belgaum, India
Bangalore, India
anoopkolsur@gmail.com

H C Srinivasaiah
Telecommunication
Dayananda Sagar College of Engineering
VTU, Belgaum, India
Bangalore, India
hcsrinivas@ieee.org

***Abstract*—Interconnected systems, such as Web servers, database servers, cloud computing servers etc, are now under threads from network attackers. As one of most common and aggressive means, Denial-of-Service (DoS) attacks cause serious impact on these computing systems. In this paper, proposed system 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. Furthermore, a triangle-area-based technique is proposed to enhance and to speed up the process of MCA. 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. The results show that our system outperforms two other previously developed state-of-the-art approaches in terms of detection accuracy.***

***Index Terms*— Denial of service, multivariate correlation analysis, anomaly-based detection.**

## I. INTRODUCTION

A Wireless Sensor networks is distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. DENIAL-OF-SERVICE (DoS) attacks are one type of aggressive and menacing intrusive behavior to online servers. DoS attacks severely degrade the availability of a victim, which can be a host, a router, or an entire network. They impose intensive computation tasks to the victim by exploiting its system vulnerability or flooding it with huge amount of useless packets. The victim can be forced out of service from a few minutes to even several days. This causes serious damages to the services running on the victim. Therefore, effective detection of DoS attacks is essential to the protection of online services. Work on DoS attack detection mainly focuses on the development of network - based detection mechanisms. Detection systems based on these mechanisms monitor traffic transmitting over the protected networks. These mechanisms release the protected online servers from monitoring attacks and ensure that the servers can dedicate themselves to provide quality services with minimum delay in response. Moreover, network-based detection systems are loosely coupled with operating systems running on the host machines which they are protecting. As a result, the configurations of network based detection systems are less complicated than that of host-based detection systems. Generally, network-based detection systems can be classified into two main categories, namely misuse based detection systems [1] and anomaly-based detection systems [2]. 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.

## II. EXISTING SYSTEM

Interconnected systems, such as Web servers, database servers, cloud computing servers etc, are now under threads from network attackers. As one of most common and aggressive means, Denial-of-Service (DoS) attacks cause serious impact on these computing systems.

This makes our solution capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only.

## III. PROBLEM STATEMENT

The objective of DoS attacks s to consume resources, such as memory, CPU processing space, or network bandwidth, in an attempt to make them unreachable to end users by blocking network communication or denying access to services.

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 2, Issue 8, August 2015)

## IV. PROPOSED SYSTEM

In this 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. Furthermore, a triangle-area-based technique is proposed to enhance and to speed up the process of MCA. 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. The whole detection process consists of three major steps as shown in Figure.1. The sample-by-sample detection mechanism is involved in the whole detection phase (i.e., Steps1, 2 and 3) and is detailed.

**In Step1**, basic features are generated from ingress network traffic to the internal network where protected servers reside in and a reused to form traffic records for a well-defined time interval. Monitoring and analyzing at the destination network reduce the overhead of detecting malicious activities by concentrating only on relevant in bound traffic.

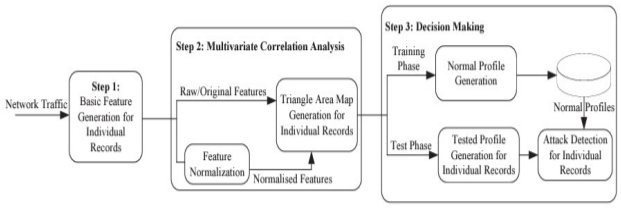


Figure 1: Framework of the proposed denial–of-Service attack detection system.

This also enables our detector to provide protection which is the best fit for the targeted internal network because legitimate traffic profiles used by the detectors are developed for a smaller number of network services.

**Step 2** is Multivariate Correlation Analysis, in which the "Triangle Area Map Generation" module is applied to extra ct 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 (Step2).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 the n used tore place 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.

**InStep3**, the anomaly-based detection mechanism is adopted in Decision Making. It facilitates the detection of any DoS attacks without requiring any attack relevant knowledge. Furthermore, the labor-intensive attack analysis and the frequent update of the attack signature data base in the case of misuse-based detection are avoided. Meanwhile, the mechanism enhances the robustness of the proposed detectors and makes them harder to be evaded because attackers need to

**Figure1**: Block diagram of outbreak detection of veto of service.

generate attacks that match the normal traffic profiles built by a specific detection algorithm. This, however, is a labor-intensive task and requires expertise in the targeted detection algorithm. Specifically, two phases (i.e.,the "Training Phase" and the "Test Phase").

**Advantages**

The results show that our system outperforms two other previously developed state-of-the-art approaches in terms of detection accuracy. To find various attacks from the user to avoid Network Intrusion.

## V. INTRUSION DETECTOR IN OSI LAYER

Intrusion detection system is placed on a network to analyze traffic in search of unwanted or malicious events. Network traffic is built on various layers; each layer delivers data from one point to another.

The OSI model and transmission control protocol (TCP)/IP model show how each layer stacks up. Within the TCP/IP model, the lowest link layer controls how data flows on the wire, such as controlling voltages and the physical addresses of hardware, like mandatory access control (MAC) addresses. The Internet layer controls address routing and contain the IP stack. The transport layer controls data flow and checks data integrity. It includes the TCP and user datagram protocol (UDP). Lastly, the most complicated but most familiar level is the application layer, which contains the traffic used by programs. Application layer traffic includes the Web (hypertext transfer protocol [HTTP]), file transfer protocol (FTP), email, etc. Most NIDSs detect unwanted traffic at each layer, but concentrate mostly on the application layer.

## VI. GENERATION OF HASHED BASED MAC

Cryptography, a keyed hash message authentication code (HMAC) is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authentication of a message. Any cryptographic hash function, such as MD5 or SHA1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMACMD5 or HMACSHA1 accordingly. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output, and on the size and quality of the key. An iterative hash function breaks up a message into blocks of a fixed size and iterates over them with a compression function. For example, MD5 and SHA1 operate on 512bit blocks. The size of the output of HMAC is the same as that of the underlying hash function (128 or 160 bits in the case of MD5

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 2, Issue 8, August 2015)

or SHA1, respectively), although it can be truncated if desired. The definition and analysis of the HMAC construction was first published in 1996 by Mihir Bellare, Ran Canetti, and Hugo Krawczyk, who also wrote RFC 2104. This paper also defined a variant called NMAC that is rarely, if ever, used. FIPS PUB 198 generalizes and standardizes the use of HMACs. HMACSHA1 and HMACMD5 are used within the IPSec and TLS protocols.

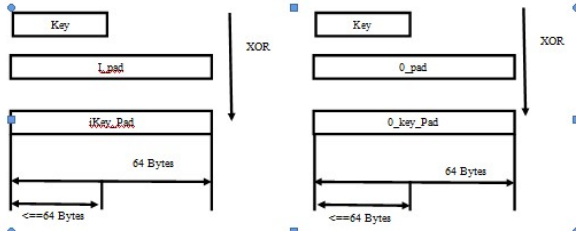


**Figure3**: Generation of Hash based mac

## VII. KDD CUP'99

The task for classifiers learning contest organized in conjunction with KDD'99 conference was to learn a predictive model (i.e. classifier) capable of distinguishing between legitimate and illegitimate connections in a computer network.

**KDD'99 Task Description**

Software to detect network intrusions protects a computer network from unauthorized user including perhaps insiders. The intrusion detector learning task is to build a predictive model (i.e. classifier) capable of distinguishing between "bad" connections, called intrusions or attacks, and "good" normal connections.

A connection is a sequence of TCP packets starting and ending at some well defined times, between which data flows to and from source IP address to target IP address under some well defined protocol. Each connection is labeled as either normal, or an attack, with a exactly one specific attack type. Each connection record consists of 100bytes.

Attacks fall into four main categories:

1. DOS: Denial- of – service e.g.: Syn Flood.
2. R2L: Unauthorized access from a remote machine e.g.: Guessing password
3. U2R: Unauthorized access from a superuser (root) privileges e.g.: Various "buffer overflow" attacks
4. Probing: surveillance and other probing e.g.: Port scanning

It is important to note that the test data is not from the same probability distribution as the training data, and it includes specific attack types not in training data. This makes the task more realistic. Some intrusion experts believe that most novel attacks are variants of known attacks and the "signature" of known attacks can be sufficient to catch novel variants. The datasets contains a total of 24 training attack types, with additional 14 types in test data only.

For each phase of development, different techniques for detecting and eliminating errors that originate in that phase are used. This is done so that the errors from a module do not carry on, into the system affecting further development.

## VIII. IMPLEMENTATION

**Functional:**

Control the Congestion in Router; Hmac Key generation, Shortest Distance Path selection in the router ,Protects the Files from Malicious data injected node or traffic node , The data will collect by using data aggregate router**,** Identifying the intrusion in IDS manager. Find the malicious or traffic node forwards the control to Test phase, Filtering the traffic/malicious content in the attacker database.

**Non Functional Requirement:**

**Security**: The system should allow a secured communication between Sender and Router and Receiver.

**Energy Efficiency:** The Time consumed by the Router to transfer the File's Packets from the Receiver.

**Reliability:** The system should be reliable and must not degrade the performance of the existing system and should not lead to the hanging of the system.

## IX. CONCLUSION

This paper has 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 behaviors. The latter technique facilitates our system to be able to distinguish both known and unknown DoS attacks from legitimate network traffic.

## REFERENCES

[1]. V Paxson, "Bro: A System for Detecting Network Intruders in Realtime", ComputerNetworks, vol.31,pp.2435-2463,1999
[2]. P Garca-Teodoro, J Daz-Verdejo, G Maci-Fernndez, and E. V zquez, "Anomaly based Network Intrusion Detection: Techniques, Systems and Challenges, "Computers & Security ,vol.28, pp.18-28,2009
[3]. D E Denning, "An Intrusion detection Model, "IEEE Transactions on Software Engineering, pp.222-232, 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 Communications, vol.31, no. 17 pp.4212-4219, 2008.
[7]. 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.
[8]. 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.
[9]. 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.
[10]. S T Sarasamma, Q.A.Zhu, and J.Huff, "Hierarchical Kohonenen Net for Anomaly Detection in Network Security," Systems, Man, and

Cybernetics, PartB: Cybernetics, IEEE Transactions on, vol.35, pp.302-312,2005
[11]. S Yu W Zhou, W Jia S Guo,Y Xiang, and F Tang, "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient," Parallel and Distributed Systems, IEEE Transactions on,vol.23,pp.1073-1080,2012.
[12]. S Jin D S Yeung, and X Wang, "Network Intrusion Detection in Covariance FeatureSpace,"PatternRecognition, vol.40, pp. 21852197, 2007.
[13]. CF Tsaiand C Y Lin, "A Triangle Area Based Nearest Neighbors Approach to Intrusion Detection, "Pattern Recognition,vol.43,pp. 222-229,2010.
[14]. A Jamdagni, Z Tan, X He P Nanda, and R P Liu, "RePIDS: A multitier Real-time Payload based Intrusion Detection System," Computer Networks,vol.57,pp.811-824,2013.
[15]. Z Tan, A Jamdagni,X He P Nanda and R P Liu, "Denial of-Service Attack Detection Based on Multivariate Correlation Analysis," Neural Information Processing,2011,pp.756-765.
[16]. Z Tan, A Jamdagni, X He, P Nanda, and R P Liu, "Triangle Area-Based Multivariate Correlation Analysis for Effective Denial of-Service Attack Detection, "The 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liver pool, United Kingdom, 2012, pp.33-40.
[17]. S J Stolfo, W Fan, W Lee, A Prodromidis, and P.K.Chan, "Cost based modeling for fraud and intrusion detection: results from the JAM project, "The DARPA Information Survivability Conference and Exposition 2000(DISCEX'00),Vol.2,pp.130-144,2000.
[18]. G V Moustakides, "Quickest detection of a brupt changes for a class of random processes," Information Theory, IEEE Transactions on, vol.44, pp.1965-1968, 1998.
[19]. A A Cardenas J S Baras and V Ramezani, "Distributed change detection for worms, DDoS and other network attacks, "The American Control Conference,Vol.2,pp.1008-1013,2004.
[20]. 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.
[21]. M. Tavallaee, E Bagheri, L Wei, and A A Ghorbani, "A Detailed Analysis of the KDDC up99 Data Set", The Second IEEE International Conference on Computation al Intelligence for Security and Defense Applications,2009,pp.1-6.

## ABOUT AUTHORS

**Anoop Kolsur** born on March 10, 1990 in Gulbarga, India. Pursuing Masters in Digital Communication and Networking at Dayananda Sagar College of Engineering, Bangalore, India. Completed bachelor of engineering in Electronics and Communication at APPA Institute of Engineering And Technology, Gulbarga, India.

Published his extreme project work on 'Military emergency alert system Using Raspberry Pi', 2014 National conference, ISBN- 978-81-921740-3-7. , 'Hurt Locker- An Explosive disposal robot' in IJEEE ISSN: 2348-4748, Volume 1, Issue 6, June 2014, 'POV: Persistence of Vision' in IJEEE ISSN: 2348-4748, Volume 1, Issue 6, June 2014. "3D PLS- An high secure polygon lock technology", volume 1, Issue 7, July 2014, ISSN: 2348-4748.Anoop. "Virtual data center powered virtual machine", volume 1, Issue 7, July 2014, ISSN: 2348-4748.

**H C Srinivasaiah** is a professor at Dayananda Sagar College of engineering, Bangalore, India. His area of interest is into antennas, microwave, radar as well as telecommunication as well.