ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

An Efficient Way of Detecting Denial-Of-Service Attack Using Multivariate Correlation Analysis

S.Gomathi[1]

M E (CSE), Muthayammal Engineering College, Rasipuram, Tamilnadu, India[1]

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 attack is Denial of Service (DoS) these attacks cause serious impact on computing systems. The shared nature of the medium in wireless networks makes it easy for an adversary to launch a Wireless Denial of Service (WDoS) attack. To give a simple example, a malicious node can continually transmit a radio signal in order to block any legitimate access to the medium and/or interfere with reception. This act is called jamming and the malicious nodes are referred to as jammers. Jamming techniques vary from simple ones based on the continual transmission of interference signals, to more sophisticated attacks that aim at exploiting vulnerabilities of the particular protocol used. 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.

Key words: Wireless Denial of Service, jamming, malicious node, jammer, learning patterns.

I. INTRODUCTION

In recent days, security has been a priority during the transmission of data in wireless network, be it through adhoc, Wi-Fi or wireless sensor network (WSN). This is because of the existence of hacking and other malicious activities that occur just like any other common day-to-day routine. Due to the progress in technology, wireless networks are coming into existence as they've become more affordable and easily accessible through the off-the-shelf components. So they are some equipment to disrupt these advancements. Since wireless networks are more accessible for the use of internet in the near past and future, it is more vulnerable to attacks than any wired network.

The widely known actuality about the wireless network is its easy accessibility and sharable nature of medium. This actuality is both the pro and con when it comes to a wireless network i.e., it is very easy for the rival to initiate an attack. This attack can be the disruption of network operations and flooding the user and kernel buffers. It is termed as Denial of service attack or jamming, depending on whether one looks at the consequence or the cause of attack. A most common example of such an attack is while browsing the internet, the page that is to be opened is not getting loaded properly and the refresh button is clicked several times than necessary. This is an example of jamming or the Denial of Service attack that is done inadvertently. This attack can also be done deliberately. For example, one can use a mobile device to send volume of SMS in hinterland. This is enough to block communication between any two wireless nodes.

In fact, it has become more like a race between the adversary to attack a network and the security experts to invent efficient methods to block the attack. The network must be capable of transmission of data between the legitimate nodes irrespective of the attack induced by the adversary. There must not be any interruption between the legitimate users. An intimation about the presence of an attacker must be given to the head of the network. It is also not ethically and morally

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

accepted if the legitimate node/ user communicate with the attacker. At such times the node involved in such a scam must be identified and warned of any other misleading activities in the network may compromise both the network and the data.

Our paper is organized as follows: In section II, we discuss the related theory about the jamming and various techniques. Section III comprises of the system design and proposed system. Section IV describes about the algorithms for Multivariate Correlation Analysis. Section V will conclude the paper.

II. RELATED THEORY

Denial of service attack is basically done in order to block a node from receiving legitimate data or to block the node completely from another legitimate node. This blocking can be done either with the data sent continually or by sending radio signals or by any other means of transmission signal jamming. We have several authors who have discussed about the various jamming techniques and their detection and/ or prevention techniques.

In [1], the authors, Pelechrinis K, Iliofotou M and Krishnamurthy S V, University of California have surveyed the various types of denial of service attacks and the performance issues due to the DoS attack in each network. They have provided several intrusion detection techniques in their survey and have mentioned that there must be system implementation to avoid real world adversaries. In all of the jamming techniques and the detection algorithms, throughput is 0 which effectively reduces the performance of the network.

In [2], the authors have detailed about the selective jamming where the adversary chooses the data to jam preferentially a high priority data when it concerns security and privacy. They do so by performing packet classification at the physical layer. The authors have evaluated the effects of packet hiding by measuring the effective throughput of the TCP connection in the following scenarios:

1. No packet hiding (N.H.).
2. MAC-layer encryption with a static key (M.E.).
3. SHCS (C.S.).
4. Time-lock CPHS (T.P.).
5. Hash-based CPHS (H.P.).
6. Linear AONT-HS (L.T.).
7. AONT-HS based on the package transform (P.T.).

In [3], data forwarding without any delay in the defending jamming in a wireless sensor network is proposed. This proposal consists of sensor nodes as clusters for a particular frequency. Here when a frequency where data forwarding occurs is jammed, the cluster of sensor nodes in that frequency becomes inoperative and the other clusters act as backup.

[4] Discusses the technique of game theory. Game theory provides powerful tools to model and analyze such attacks. This article discusses a class of such jamming games played at the MAC layer among a set of transmitters and jammers. The equilibrium strategies resulting from these jamming games characterize the expected performance under DoS attacks and motivate robust network protocol design for secure wireless communications. A key characteristic of the distributed wireless access networks is that users do not have complete information regarding the other user's identities, the traffic dynamics, the channel characteristics, or the costs and rewards of other users.

Various forms of uncertainty can be present as illustrated in Fig. 2, including:
• User types: Users may not know each other's type, where type refers to whether a node is a transmitter or jammer.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

• Physical presence: Users may not know whether or not the opponent is physically present to transmit.
• Packet traffic: Users may not know traffic dynamics of the opponent, that is, whether or not the opponent's queue is backlogged.
• System parameters: Users may not know each other's utilities (reward and cost functions).
• Physical channel: Users may not know physical channel characteristics, such as channel gains, channel noise, or packet capture probability.

III. SYSTEM DESIGN AND PROPOSED SYSTEM

The overview of our proposed DoS attack detection system architecture is given in this section, where the system framework and the sample-by-sample detection mechanism are discussed.

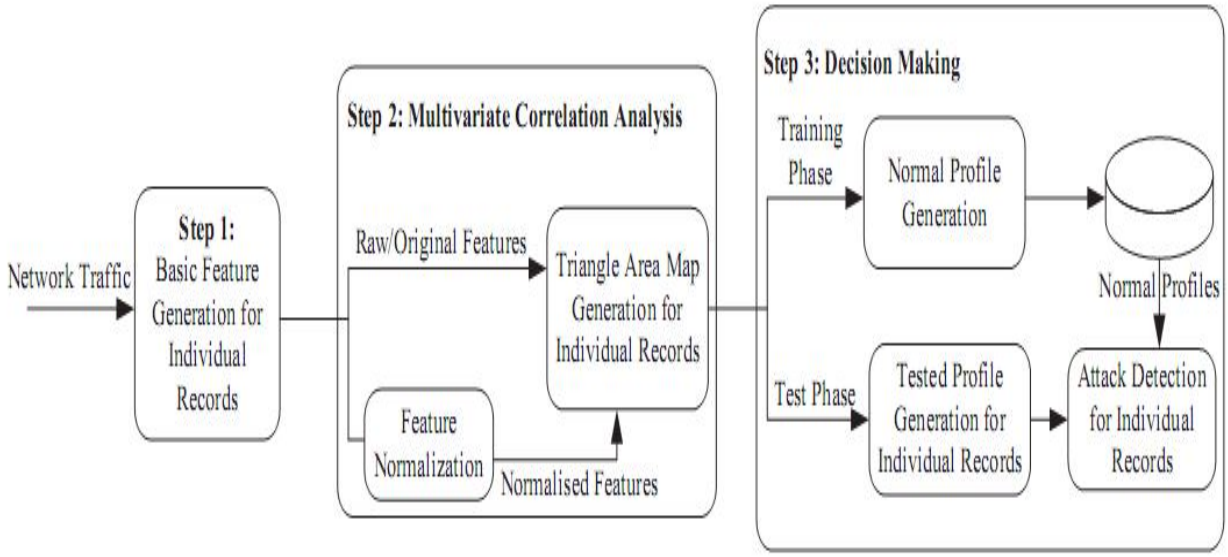

Figure 1: SYSTEM ARCHITECTURE

3.1 Framework

The whole detection process consists of three major steps as shown in Fig. 1.
Step 1: The basic features are generated from ingress network traffic to the internal network where protected servers reside in and are used 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 inbound traffic. 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: 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 (Step 2). 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

basic features or the normalized features to represent the traffic records. This provides higher discriminative information to differentiate between legitimate and illegitimate traffic records. Our MCA method and the feature normalization technique are explained in Sections 3 and 5.2 respectively.

Step 3: 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 database 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 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") are involved in Decision Making. The "Normal Profile Generation" module is operated in the "Training Phase" to generate profiles for various types of legitimate traffic records, and the generated normal profiles are stored in a database. The "Tested Profile Generation" module is used in the "Test Phase" to build profiles for individual observed traffic records. Then, the tested profiles are handed over to the "Attack Detection" module, which compares the individual tested profiles with the respective stored normal profiles. A threshold-based classifier is employed in the "Attack Detection" module to distinguish

DoS attacks from legitimate traffic.

a. MULTIVARIATE CORRELATION ANALYSIS

DoS attack traffic behaves differently from the legitimate network traffic and the behavior of network traffic is reflected by its statistical properties. To well describe these statistical properties, we present a novel Multivariate Correlation Analysis (MCA) approach in this section. This MCA approach employs triangle area for extracting the correlative information between the features within an observed data object (i.e., a traffic record).

IV. DETECTION MECHANISM

In this section, we present a threshold-based anomaly detector, whose normal profiles are generated using purely legitimate network traffic records and utilized for future comparisons with new incoming investigated traffic records. The dissimilarity between a new incoming traffic record and the respective normal profile is examined by the proposed detector. If the dissimilarity is greater than a pre-determined threshold, the traffic record is flagged as an attack. Otherwise, it is labeled as a legitimate traffic record. Clearly, normal profiles and thresholds have direct influence on the performance of a threshold-based detector. A low quality normal profile causes an inaccurate characterization to legitimate network traffic. Thus, we first apply the proposed trianglearea- based MCA approach to analyze legitimate network traffic, and the generated TAMs are then used to supply quality features for normal profile generation.

4.1 Normal Profile Generation

Assume there is a set of g legitimate training traffic records Xnormal = {xnormal 1 , xnormal 2 , · · · , xnormal g }.The triangle-area-based MCA approach is applied to analyze the records. The generated lower triangles of the TAMs of the set of g legitimate training traffic records are denoted by Xnormal TAMlower ={TAMnormal,1lower , TAMnormal,2lower , · · · , TAMnormal,glower }.

Mahalanobis Distance (MD) is adopted to measure the dissimilarity between traffic records. This is because MD has been successfully and widely used in cluster analysis, classification and multivariate outlier detection techniques. Unlike Euclidean distance and Manhattan distance, it evaluates distance between two multivariate data objects by taking the correlations between variables into account and removing the dependency on the scale of measurement during the calculation.

4.2 Threshold Selection

The threshold is used to differentiate attack traffic from the legitimate one.

Threshold = $\mu + \sigma * \alpha$. (16)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

For a normal distribution, α is usually ranged from 1 to 3. This means that detection decision can be made with a certain level of confidence varying from 68% to 99.7% in association with the selection of different values of α. Thus, if the MD between an observed traffic record xobserved and the respective normal profile is greater than the threshold, it will be considered as an attack.

4.3 Attack Detection

To detect DoS attacks, the lower triangle (TAMobservedlower) of the TAM of an observed record needs to be generated using the proposed triangle-area-based MCA approach. Then, the MD between the TAMobserved lower and the TAMnormal lower stored in the respective pre-generated normal profile Pro is computed. The detailed detection algorithm is shown in Fig. 2.

Require: Observed traffic record xobserved, normal profile
Pro : (N(μ, σ2), TAMnormal
lower , Cov) and parameter
α
1: Generate TAMobserved
lower for the observed traffic
record xobserved
2: MDobserved ← MD(TAMobserved
lower ,TAMnormal
lower)
3: if $(\mu - \sigma * \alpha) \leq$ MDobserved $\leq (\mu + \sigma * \alpha)$ then
4: return Normal
5: else
6: return Attack
7: end if

Fig. 2. Algorithm for attack detection based on Mahalanobis distance.

V. 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] Konstantinos Pelechrinis, Marios Iliofotou and Srikanth V. Krishnamurthy(2011), "Denial of Service Attacks in Wireless Networks:The Case of Jammers" Communications Surveys & Tutorials, IEEE, vol 13: issue:2, nos 245- 257.

[2] Proano, A.; Lazos, L.;(2011) "Packet-Hiding Methods for Preventing Selective Jamming Attacks" Dependable and Secure Computing, IEEE, vol. 9 issue 1. Nos 101- 114.

[3] Ghosal, A.; Halder, S.; Mobashir, M.; Saraogi, R.K.; DasBit, S.;(feb- 28th to march 3rd 2011)" A jamming defending data-forwarding scheme for delay sensitive applications in WSN" Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference, nos 1- 5.

[4] Sagduyu, Y.E.; Berry, R.A.; Ephremides, A.;(aug 2011)" Jamming games in wireless networks with incomplete information", Communications Magazine, IEEE, vol 49, issue 8, nos 112- 118.

[5] Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda, Member, IEEE, and Ren Ping Liu, Member, IEEE," A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. , NO. , 2013 1