International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Survey on Multivariate Correlation Analysis for Denial of Service Attack Detection

Sana Chaugale[1], Dr. Tanuja Dhope[2]

[1]sanachaugale7@gmail.com

[2] G. H. Raisoni College of Engineering and Management Wagholi, Pune, India,
tanuja.dhope@raisoni.net

Abstract: ***Denial of Service attacks (Dos) cause serious effect on systems. Due to shared nature of the medium in wireless networks it makes the situation too easy to make possibility of an attack. DoS attack detection system uses Multivariate Correlation Analysis (MCA) for most accurate network traffic characterization. MCA extract the geometrical correlations between network traffic features. MCA DoS attack detection system employs the principle of anomaly-based detection during attack recognition. This makes more easy for detecting known and unknown DoS attacks by simply learning the patterns of legitimate network traffic.***

Keywords: Denial of Service, KDD cup99, multivariate correlation, triangle area.

1. Introduction

Nowadays, security has been a major concern during the transmission of data in wireless network, it may be through Wi-Fi, ad-hoc or may be in wireless sensor network. This is because of the existence of hacking and other hostile activities that happens like any other common daily routine. So there is some equipment to disrupt these advancements [1].Since, wireless networks are most accessible for use of internet in the near past and future; it is more difficult to attacks than any wired network. The widely known about the wireless network is its ease of accessibility and nature of medium which is mostly sharable. These make possible both the pro and con when it comes to a wireless network that mean, it is too easy for the attacker to initiate an attack. This attack can be the flooding the user buffers and kernel buffers, and disruption of network operations.

Most common example of such an attack is while browsing the internet, the page that we want to open is not loaded properly and the reloading will be done many times than necessary. This is an example of jamming. This attack can also be done intentionally. Example, one can use a mobile device to send volume of SMS. This is enough to block the communication in between two wireless nodes. It has become like a race between the adversary to attack and the security methods to block that attack. The network must capable for data transmission between the legitimate nodes irrespective of the attack. Legitimate users must not be any interruption in between them. Information about the presence of an attacker must be given to the network head. It is also not ethically accepted if the legitimate user communicates with the attacker. At this time the user that involved in such a scam must be identified and warned. [2]

Related Work

In [3] paper , surveyed the different types of denial of service attacks and the effect of Dos attack on the performance In this paper several intrusion detection techniques are studied. All jamming techniques and the algorithms for Dos detection, throughput is 0 which reduces the performance of the network.

In [4] paper, shown, KDD'99 dataset that is used in Dos attack detection. KDD'99 dataset most wildly used data set for the evaluation of anomaly detection methods. It is prepared by Stolfo [5] and is built on the bases of data capturing in DARPA'98 IDS evaluation [6]. DARPA'98 is compressed raw (binary) tcp dump data of 7 weeks of network traffic of about 4 gigabytes.

In [7] paper, Discussed Multivariate correlation (MCA) approach. MCA extract the correlation between the features observed in traffic record. Triangle area Map generation (TAM) is purposely used to extract the correlation between the features.

In [8] paper, Introduced the technique of game theory. This technique provides powerful tools to model and analyse such attacks. It discussed about jamming games at the MAC layer among a set of transmitters and jammers. Result comes out from this game theory provide robust network protocol design for secure wireless communication and characterize the expected performance under DoS attacks. In distributed wireless access networks system users do not have complete information about the other user's identities, the channel characteristics, the traffic dynamics, the rewards and the costs of other users.

Proposed System

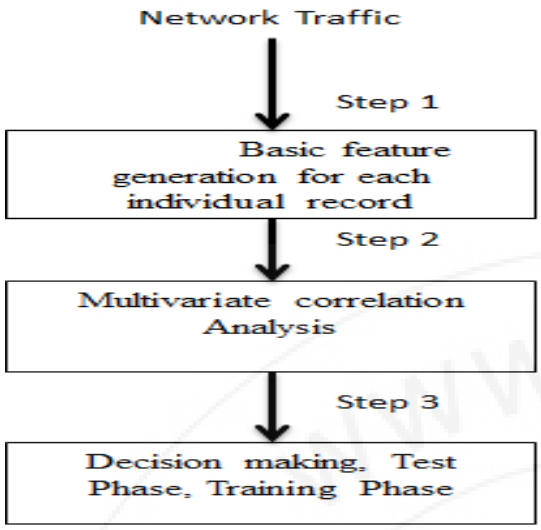

Figure 1: Framework of denial-of-service Attack detection system

In this section the overview of DoS attack detection system architecture, system framework and sample-by-sample detection mechanism are enlighten. The detection process consisting three major steps as shown in Fig. 1.Step 1: Very First basic features are generated from ingress network traffic to the internal network where protected servers reside in and they are used to form traffic records. Analysing and Monitoring at the destination network side reduce the overhead of detecting hostile activities by concentrating only on related traffic. This also provides protection to detector which is the best fit for the targeted network because legitimate traffic profiles that are used by detectors are developed for a very smaller number of network services. Step 2: Multivariate Correlation Analysis, in this step the "Triangle Area Map Generation" module is applied.

It helps to extract the correlations between two distinct features within each traffic record coming from the first step. And also extract the correlation between the traffic records normalized by the "Feature Normalization" module. If there any presence of intrusion then it causes to change in these correlations .So the changes can be caused as indicators to identify the intrusive activities. All extracted correlations, named as triangle areas stored in Triangle Area Maps, are then used to replace the original basic features to represent the traffic records. This provides valuable information i to differentiate between legitimate and illegitimate traffic records. Step 3: In this step the anomaly-based detection mechanism is there in Decision Making. It is used to detect any type of DoS attacks without requiring any attack related information. Further, the danger attack analysis and the frequently updating of the attack signature database, in the case of misuse-based detection are avoided. The mechanism enhances the robustness of the proposed detectors. And also makes them harder to be evaded because attackers need to generate attacks that match the normal traffic profiles.

This is very difficult task and it requires expertise in the targeted detection algorithm. Generally, two phases are involved in Decision Making. In "Training Phase ""The "Normal Profile Generation" module is operated in to generate profiles for various types traffic records, and the generated profiles are stored in a database. In "Test Phase" the "Tested Profile Generation" module is used to build profiles for individual traffic records. After this, the tested profiles are handed over to the "Attack Detection" module. This module compares the individual tested profiles with the stored normal profiles. A threshold-based classifier is used in the "Attack Detection" module. [9]

3.1 Multivariate Correlation Analyses

The behavior of traffic that is attacked by DoS is different from the legitimate network traffic. And the behavior of any network traffic is reflected by its statistical properties. To understand these statistical properties of network traffics, A Multivariate Correlation Analysis approach is there, This MCA approach uses triangle area for extracting the correlative information between the features within an observed traffic records. [10]

3.2 Detection Mechanism

This section represents a threshold-based anomaly detector, whose normal profiles are generated using purely legitimate network traffic records. And then can be used for future comparisons with new incoming traffic records. The changes between a new incoming traffic record and the normal profile are examined by the detector .The traffic record is flagged as an attack, If the dissimilarity is greater than a determined threshold. Otherwise, it labeled traffic as a legitimate traffic. Normal profiles and thresholds have direct impact on the performance of a threshold-based detector. A low quality normal profile may cause an inaccurate characterization to network traffic. Therefore, first apply the proposed triangle area- based MCA approach to analyse legitimate network traffic, and the generated Triangular area map generations are then used to supply features for normal profile generation.

3.3 Detection Mechanism

Assume there is a set of g legitimate training traffic records, Xnormal = {xnormal 1, xnormal 2, · · ·, xnormal g}. A triangle-area-based MCA approach is applied to analyse the records. The generated lower triangles of the set of g legitimate training traffic records are denoted by Xnormal TAMlower = {TAMnormal, 1lower, TAMnormal, 2lower, ··, TAMnormal, glower}. Mahalanobis Distance is under concern to measure the dissimilarity between traffic records. Because MD has been widely used in cluster analysis, classification and multivariate detection techniques. It calculates distance between two multivariate data objects by taking the correlations between variables and removing the dependency.

3.4 Detection Mechanism

Threshold is specially used to differentiate attack traffic from the legitimate one. Threshold = $\mu + \sigma * \alpha$. Where α denotes normal distribution and usually ranged from 1 to 3. Detection decision can be made with a certain level of confidence, varying from 68% to 99.7% by the selection of different values of α. Finally, if the MD between an observed traffic record and the respective normal profile is greater than the threshold, it will be considered as an attack.

3.5 Attack Detection

For the detection of DoS attacks, the lower triangle (TAMobservedlower) of the TAM of an observed record needs to generate using the MCA approach. After this, the MD between the TAM observed lower and the TAMnormal lower stored in the corresponding normal profile is computed. The detailed detection algorithm is: [10]

Requirement: Observed traffic record yobserved, normal profile: (N (μ, σ2), TAMnormal lower, Cov) and parameter α

1: Generate TAM observed lower for the observed traffic record x observed
2: MDobserved ← MD (TAM observed Lower, TAMznormal lower)
3: if $(\mu - \sigma * \alpha) \leq$ MDobserved $\leq (\mu + \sigma * \alpha)$ then
4: return Normal
5: else
6: return Attack
7: end if

3.6 Naive Bayes

These networks are like graphical models that are useful to represent and handle uncertain information. Bayesian networks are specially specified by two components. [11]

1. First component is graphical component which is composed of a directed acyclic graph (DAG) where edges show relations between events, vertices represent events
2. Second component is numerical component consisting in a quantification of different links in the DAG by a conditional probability distribution of each node in the context of its parents.

The Naive Bayes method Bayesian classification, there is a hypothesis that the given data belongs to a particular class. Then the probability for the hypothesis is calculated that should be true. This is among the most practical methods for certain types of problems. The approach requires only one scan of the whole data that involves under. And also, if at some stage there are additional training data will there, then each training example can incrementally Increase or decrease the probability that a hypothesis is correct. Thus, a Bayesian based network is used to model a domain that containing any uncertainty. [12]

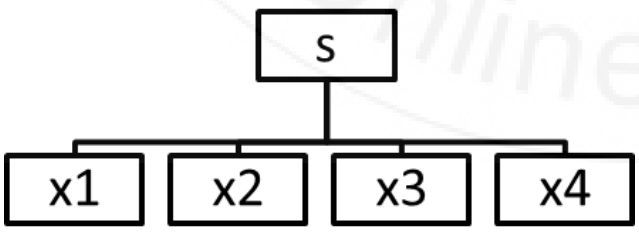

Figure 2: Naive Bayes structure

As shown in Figure 2, Naive-Bayes structure has the class node S act as a parent node of all other nodes, other than this no connections are allowed in this structure. Naive-Bayes method assumes that all the network features are independent of each other.

Conclusion

This paper presented a MCA-based DoS attack detection system which uses the triangle area based MCA technique and the anomaly-based detection technique. This technique is useful to extracts the geometrical correlations in each individual pairs of two distinct features within each network traffic record. And it gives more accurate characterization for network traffic behaviors. The technique facilitates our computing system to be able to compare both known and unknown DoS attacks from network traffic. Data mining will research under research and more beneficial results will come from the implementation of data mining based intrusion detection systems. To verify the effectiveness and performance of the Denial of Service attack detection system has been conducted by using KDD cup 99 dataset.

References

[1] S.Gomathi "An Efficient Way of Detecting Denial-Of-Service Attack Using Multivariate Correlation Analysis", International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 1, March 2014
[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] 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.
[4] "Nsl-kdd data set for network-based intrusion detection systems." Available on: http://nsl.cs.unb.ca/NSL-KDD/, March 2009.
[5] S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. K. Chan, "Costbased modeling for fraud and intrusion detection: Results from the Jam project," discex, vol. 02, p. 1130, 2000.
[6] R. P. Lippmann, D. J. Fried, I. Graf, J. W. Haines, K. R. Kendall, D. McClung, D. Weber, S. E. Webster, D. Wyschogrod, R. K. Cunningham, and M. A. Zissman, "Evaluating intrusion detection systems: The 1998 drape off- line intrusion detection evaluation," discex, vol. 02, p. 1012, 2000.
[7] J.Welkin Eyes, S.Karthiprem, E.Thangadurai "High Accuracy detection of Denial of Service Attack based on Triangle Map Generation" IJCSMC, Vol. 3, Issue. 1, January 2014.
[8] 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 & Electronics Systems Technology (Wireless VITAE)," 2011 2nd International Conference, nos 1- 5.

[9] K.Sujithra1, V.Vinoth Kumar "A Survey On Triangle Area Map Based Multivariate Correlation Analysis To Detect Denial-Of Service Attack" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 10, October 2014
[10] Zhiyuan Tan, Aruna Jamdagni, Xiangjian He‡, Senior Member, IEEE, 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:25 no:2 year 2014
[11] Nahla Ben Amor, Salem Benferhat and Zied Elouedi "Naive Bayesian Networks in Intrusion Detection Systems," Institut Sup_erieur de Gestion Tunis, 41 Av. de la libert_e, 2000 Le Bardo, Tunisie
[12] Z. Muda, W. Yassin, M.N. Sulaiman, N.I. Udzir. "Intrusion Detection based on K-Means Clustering and Naïve Bayes Classification," 7th International Conference on IT in Asia (CITA), 2011.