Scientific Journal Impact Factor (SJIF): 1.711
e-ISSN: 2349-9745
p-ISSN: 2393-8161
International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Implementation of Homeostasis at Network Level

Ranjita Patil [1], Dr. V. R. Ghorpade[2]
[1] *Student*, [2] *Professor*
[1,2] *D Y Patil College of Engineering and Technology*

Abstract— In last few years, the complexity at computer networks is increasing exponentially. These complex network architectures have resulted in increased demands of information security measures. Compared to the traditional central and static networking control mechanisms, the biologically inspired network security mechanisms are becoming a promising approach for fulfilling current (and future) network requirements. Hence the proposed system is inspired from the biological process or metaphor Homeostasis. *Homeostasis* is a biological system able to maintain a stable status by taking actions upon the observed continuous changes in their internal and external environments. Using this concept the network will be able to detect the malicious anomalies (change in external environment) and to generate the response (such as traffic rate limiting, node quarantine) to maintain the stable status of system. Anomaly based detection technology has the high rate of false alarms but the ability of anomaly-based technology to integrate with other security products will create a security elements that can effectively work together. This detection does not end the task but it's a start of taking steps towards the mitigation of impact of malicious anomaly and to generate the signature for future use. When solution for any anomaly is unavailable it takes time to make it available. This time period can be utilized by the anomaly to affect the system. Thus mitigation steps will enhance ability of system to maintain the stability of system. In this way the proposed system may play an important role in network security technology.

Index Terms— Anomaly, Connection features, False Alarm, Homeostasis, Network profile, Node Quarantine, Signature.

I. INTRODUCTION

Homeostasis is the biological term. It is the ability of the cell organism to maintain a constant internal environment in response to environmental changes. This biological concept must be implemented at computer networks because the computer networks are becoming more complex with the ever-increasing demands for network services and the additional new security challenges (such as DoS, DDoS,..etc) are introduced.

An anomaly-based system treats any network connection violating the normal network profile as a network anomaly. A network anomaly is revealed if the incoming traffic pattern deviates from the normal profile significantly. However, anomaly detection may result in higher false alarm.The false alarms can be false positive alarm or false negative alarm. The false positive ratio is defined as the number of normal-traffic streams misclassified as malicious variants divided by the total number of normal-traffic streams used in the experiment. The false negative ratio is defined as the number of malicious variants misclassified as normal traffic divided by the total number of malicious variants used in the experiment.The proposed approach is to minimize the false alarm ratio and mitigate the impact of attack to maintain stability of system by using concept of homeostasis.

To take any action in response to network anomaly, detection of most significant anomaly is required. This can be achieved by using union of different methods used for anomaly detection. These methods

when used at single level helps to detect the anomaly at its own level but when combined and used as a union may lead to the confirmation of the anomaly. The traditional signature-based system leverages manually characterized attack signatures to detect attacks in real-time traffic but it fails to detect the newly generated attacks. Thus signature-based systems are unable to maintain the stability of system under the unknown attacks. This limitation can be removed by using anomaly-based systems to detect the unknown attacks. Anomaly-based system observes the variation in network traffic patterns.

Even though system detects the malicious anomaly, the solution to tackle this anomaly cannot be made immediately available. Thus till the solution is made available, the system may get badly affected by the malicious anomaly or even may get crashed.

So there is need to devise the network security process which can detect the anomalies and maintain the stability of system. Hence attempt should be made to detect the malicious anomalies with less false positive alarm and to mitigate the impact of such malicious activities

II. RELATED WORK

*Homeostasis*is the phenomenon of biological systems maintaining their own stable status by reacting to sensed continuous changes in their internal and external environments. This kind of phenomena can be observed in mechanisms like body temperature regulation or blood pressure maintenance. According to ChenyuZheng,and Douglas C. Sicker,[1] the metaphor of homeostasis can be applied to the problem of networked system status control in continuously changing environments in future research. The systems suitable to employ this metaphor have high priority in maintaining a stable status, guarantee sustainable functionality. The control mechanisms for the systems are the key components in these applications. They must be defined so that decisions on homeostatic responses based on changing environments can effectively adjust the systems toward a regular state.

The homeostasis metaphor has been applied already to the field of security in operating systems. Somayaji et al. [2] introduced a Linux kernel extension that maintains homeostasis in the operating system's security in an autonomously responding fashion. Attacks are effectively stopped by monitoring active processes at the system-call level in real-time, and delaying (i.e., reducing the CPU cycles received by unusually behaving processes based on the monitored anomalies of system call sequences) or aborting the execution of compromised programs.At the same time, legitimate computation proceeds with minimal impact on performance.

Biological phenomena show characteristics that are desirable for new network application designs compared to the traditional central and static networking control mechanisms. F. Hashim, K. S. Munasinghe, and A. Jamalipour [3]also proposed biologically inspired security framework. It has the Danger Theory based anomaly detection framework. For security control measures Danger Zone (DZ) concept is used. Implementation of biological concepts at computer network had added robustness to the system to maintain its stability. But while inhibiting the anomaly propagation, it is required to address the impact of the rate limiting strategy on the delay performance of legitimate traffic.

The different mechanisms used for the bio-inspired system are the key components in these applications. Such as H. Wang, D. Zhang and K. Shin [4] presented the mechanism called Change-Point Monitoring (CPM) to detect denial of service attack. CPM makes use of strong positive correlation between requests and corresponding replies in Internet. This Correlation is due to the inherent protocol behavior. It only keeps track of few packet counts. By applying the nonparametric CUSUM method, CPM detects the flooding attacks in a timely manner with low computational overhead. Thus CPM can be combined with the anomaly inhibition mechanism. And K. Hwang, M. Cai, and Y. Chen [5] have combined the advantages of intrusion detection system (ISD) and anomaly detection system (ADS). Thus hybrid intrusion detection system have low false positive rate and can detect the novel unknown attacks. Network

traffic data mining is done to generate the signature over Internet connection episodes. This gives the idea about the signature generation over the anomalous behavior of computer networks.

III. PROPOSED SYSTEM

To minimize the false alarm in network anomaly detection system and add response to prevent the propagation of malicious anomaly, for this the homeostasis concept at network level is being proposed. Here anomaly detection will be done at three levels such as check for deviation, analysis and detection, and identifying significance. Figure 1 shows in detail architecture of the system.

A. Analyze Data for Deviation

The deviation in network traffic pattern can be noticed by making use of basic 41 attributes like number of packets and byte counter per observation interval. If these 41 features are used for processing the network traffic patterns then it will comsume more time. Intentionaly use of some significant features helps to improve the performance. Identification of significant features out of these 41 features is a difficult task. These features will play important role to detect the volume anomalies as Denial of Service attack.

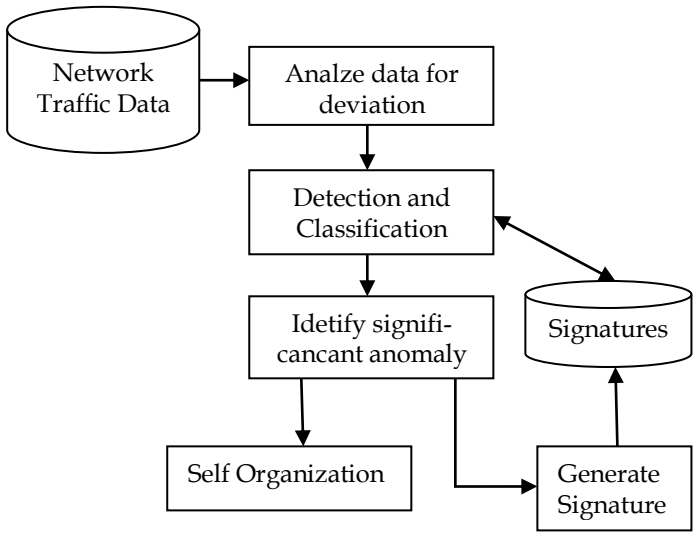

Figure 1: System Architecture

B. Detection and Classification

In this module network traffic will be analyzed to identify the malicious anomaly. It can use the information generated while observing the network traffic at regular intervals. Analysis can be done by using spectral analysis method. Detection can be done by utilizing the efficient detection approaches like rate based detection (the history of previous observed data rates is used to compute an estimate for the current interval.) or frequency information based detection (packet rates are transposed into the frequency domain and analyzed for anomalies.) or entropy-based detection (traffic is split into different classes and anomalies in traffic rates are determined by change in the entropy compared to base line.). All these techniques of detection are based on the network traffic patterns. The basic 41 features used to study

network traffic patterns are enlisted in TABLE 1,2,3 give by Salvatore J. Stolfo et al. [9]. These features generate the high dimentional data which is very complex and consumes more processing time. Thus reduction algorithm PCA (Principle Component Analysis) is prefeared for data reduction by number of researchers.

C. Identify Significant Anomaly

In this module cross examination of previous two detection processes will be done. It will find whether the suspicious anomaly is significant enough or not to create a danger condition at node. If it detects that the deviation is originated by the malicious attack then it will trigger the signal.

D. Self Organization

Under Self Organization the system will generate the response to the changing external environment. This module will inhibit the malicious anomalies. The strategies like node quarantine (it is aggressive action which significantly hinders the normal communication), traffic rate limiting (it is less aggressive as it allows the suspicious node to enter the network but at a slower pace) and process homeostasis (it monitors every executing process in computer at the system level) can be used to inhibit the anomaly propagation. Here the localization of anomaly is very important. The advanced PCA algorithms, such as JSPCA (Jointly Sparse PCA) or GJSPCA (Graphical Jointly Sparse PCA), work efficiently to localize the anomaly.

Table 1: Basic features of individual TCP connections.

Sr. No.	Feature name	Discription
1	duration	length (number of seconds) of the connection
2	protocol_type	type of the protocol, e.g. tcp, udp, etc.
3	service	network service on the destination, e.g., http, telnet, etc.
4	src_bytes	number of data bytes from source to destination
5	dst_bytes	number of data bytes from destination to source
6	flag	normal or error status of the connection
7	land	1 if connection is from/to the same host/port; 0 otherwise
8	wrong_fragment	number of ``wrong'' fragments
9	urgent	number of urgent packets

Table 2: Traffic features computed using a two-second time window.

Sr. No.	Feature name	Discription
10	count	number of connections to the same host as the current connection in the past two seconds
Note: The following features refer to these same-host connections		
11	serror_rate	% of connections that have ``SYN'' errors
12	rerror_rate	% of connections that have ``REJ'' errors
13	same_srv_rate	% of connections to the same service
14	diff_srv_rate	% of connections to different services
15	srv_count	number of connections to the same service as the current connection in the past two seconds
Note: The following features refer to these same-service connections.		
16	srv_serror_rate	% of connections that have ``SYN'' errors
17	srv_rerror_rate	% of connections that have ``REJ'' errors
18	srv_diff_host_rate	% of connections to different hosts
Note: Features from 19 to 28 are host-based traffic features		

Table 3: Content features within a connection suggested by domain knowledge.

Sr. No.	Feature name	Discription
29	hot	number of ``hot'' indicators
30	num_failed_logins	number of failed login attempts
31	logged_in	1 if successfully logged in; 0 otherwise
32	num_compromised	number of ``compromised'' conditions
33	root_shell	1 if root shell is obtained; 0 otherwise
34	su_attempted	1 if ``su root'' command attempted; 0 otherwise
35	num_root	number of ``root'' accesses
36	num_file_creations	number of file creation operations
37	num_shells	number of shell prompts
38	num_access_files	number of operations on access control files
39	num_outbound_cmds	number of outbound commands in an ftp session
40	is_hot_login	1 if the login belongs to the ``hot'' list; 0 otherwise
41	is_guest_login	1 if the login is a ``guest''login; 0 otherwise

E. Generate Signature

When it will receive the signal from anomaly detection method, confirmation of malicious anomaly would have been done. Thus it will extract all the information from spectral analysis to generate the traffic signature of the newly encountered attack. This signature can be stored and passed over the network for early identification of attack in future. This module helps to combine the advantages of intrusion detection system (ISD) and anomaly detection system (ADS).

F. Methodology

The dataset required as an input to the system is the network traffic.Internet is a large source of all kind of datasets. Many web sites provide large datasets for anomaly detection (Such as KDD). There are many methods available which can be useful in many ways for the proposed system. These are: i) Pattern Matching Techniques for identifying potentially problematic traffic. ii) Entropy based anomaly detection for adding significance in anomaly detection. iii) Mining algorithm like base-support algorithm can be used to mine the normal traffic records and generate the signature

IV. PERFORMANCE ANALYSES

Performance analysis can be done with the help of metrics like anomaly detection rate, false alarm rate and receiver operating characteristic (ROC) curve. Anomaly detection rate is ratio between the number of correctly detected anomalies and the total number of anomalies used in experiment. It is used to measure the correctness of the system. Similarly false alarm rate which can be either false positive rate or false negative rateis used to measure the misclassification done by the system. And receiver operating characteristic (ROC) curve is a trade-off between detection rate and false alarm rate.

V. CONCLUSIONS

The large amount of work has been done on network anomalies detection. This work is further extended to find the location of anomalies so that mitigation techniques can be used effectively to stop the anomalies from degrading the network services. The PCA helps to add robustness to network analyzing system by detecting the new anomalies (whose signature is not available). In addition the use of signature based detection minimizes the false alarm rate. Besides this, the high dimensionality nature of network traffic pattern cannot be neglected as it affects the performance of whole system.

REFERENCES

[1] ChenyuZheng, and Douglas C. Sicker, “Survey on Biologically Inspired Algorithms forComputer Networking”, *IEEE Communications Surveys & Tutorials*, ref. no.1553-877X/13/$31.00 c_ 2013.

[2] A. B. Somayaji, “Operating System Stability and Security through Process Homeostasis” July 2002.

[3] F Hashim, K. S. Munasinghe and A.Jamalipour, “Biologically InspiredAnomaly Detection and Security Control Frameworks for Complex Heterogeneous Networks,” *IEEE Transactions onNetwork and Service Management*, vol. 7, no 4, pp. 268-281, December 2010.

[4] H. Wang, D. Zhang, and K. G. Shin,”Change-point Monitoring for the Detection of DoS Attacks,”*IEEE Trans. On Dependable and Secure Comput*., vol. 1, no. 4, pp. 193-208, Oct 2004.

[5] K. Hwang, M. Cai, Y. Chen, and M. Qin, “Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes,” *IEEE Trans. On Dependable and Secure Comput.*, vol. 4, no. 1, pp. 41-55, January 2007.

[6] M. Burgess, “Computer Immunology”, in Proc. Sys. Administration conf. pp. 283-297, Dec 1998.

[7] MaizuraMokhtar, Jon Timmis, Andy M. Tyrrell and Ran Bi, “An Artificial Lymph Node Architecture for Homeostasis in Collective Robotic Systems”, Symbiotic Evolutionary Robot Organisms Project.

[8] Matthew M. Williamson “Biologically Inspired Approaches to Computer Security”, Copyright Hewlett-Packard Company 2002.

[9] https://kdd.ics.uci.edu/databases/kddcup99/task.html

