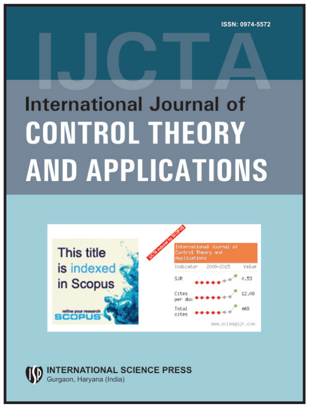

International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 10 • Number 12 • 2017

Efficient Analysis of Malignant Packet Detection in Distributed Firewall

P. Senthil Kumar[a], S. Arumugam[b] and P. Rama Subramanian[c]

[a] *Assistant Professor, Department of Computer Science & Engineering, Excel College of Technology, India. Email: psenthilexcel@gmail.com*
[b] *Professor, Department of IT,, Nandha Engineering College, Erode, Tamil Nadu, India. Email: arumugamdote@yahoo.co.in*
[c] *Principal, Annai Vailankanni College of Engineering, India. Email:2005.rams@gmail.com*

Abstract: Security in networking plays a vital role in protecting user data from unauthorized access. The traffic from various domain networks are passed through the distributed firewall system which checks the packets flow from one domain network to another domain environment. In this paper, Similarity Index Algorithm is proposed to detect the malignant packets in firewall architecture. The proposed algorithm is based on the energy index and similarity index value. The performance of the proposed firewall system is analyzed using Network simulator version 2 environments in terms of latency and malicious packets detection rate with respect to number of nodes or computers in network. The latency and malicious packet detection rate of the proposed firewall architecture is 14.74 ms and 87%, respectively.

Keywords: Malignant Packets, Detection Rate, Latency, Distributed Firewall.

1. INTRODUCTION

Firewall is a networking device to filtrate the packet based on the firewalls access rules and regulation over through the Internet connections. The firewall placed on the edge of the every computer connects through internet over the networks of the organization. Based on the predefined firewalls access rules the public network and private networks can be segregated. Firewall is one of the system securities that protects from hackers and malignant attack. It also provides high flexible security to online computer users. The security of the system is dependent on the rules of the firewall configuration; else undesired packet traffic may enter or may block the desired packets.

The distributed firewalls allows of network policy on a computer network without inhibit its topology on an inside or outside the network. To implement a Distributed firewalls concept needs a security firewall access rule that can describe which connections are allow or disallow.

Firewalls are categorized as Packet-filtering firewalls, Circuit-level gateways, Stateful inspection firewalls and Multilayer inspection firewalls. Packet-filtering firewalls are a firewall which filters the packets coming from unauthorized network domain environments. Circuit-level gateways provides the data connection, Stateful inspection firewalls provides the network security based on the filtering the unauthorized details from the unique network domain environment. Multilayer inspection firewalls provides the security between local server and remote server in multi domain network environment.

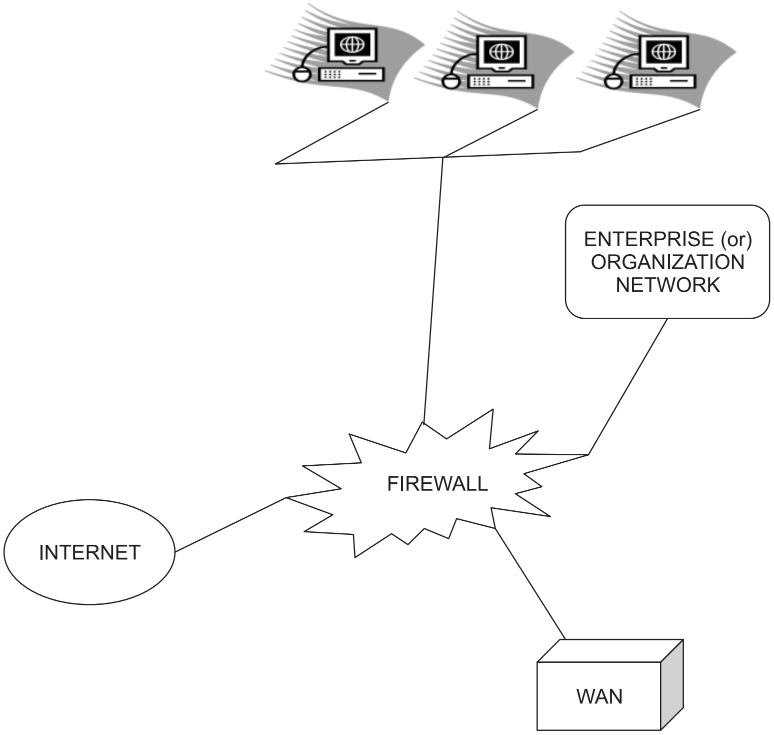

Figure 1: Firewall interfacing between network domains

Figure 1 shows the interfacing structure between different network domain environments such as Local Area Networks (LAN) and Wide Area Networks (WAN). The packets from LAN are sent to WAN network through the firewall architecture which verifies and filters the unauthorized packets. In this paper, an efficient methodology is proposed to detect the malicious packets from remote network domain environment. This paper is organized as Section II describes the methodologies used in conventional firewall design; Section III proposes an efficient methodology for malicious packet detection in firewall architecture, Section IV discusses the experimental results of the proposed method with conventional methods and Section V concludes this paper.

2. LITERATURE SURVEY

Xuan et. al., (2016) designed and analyzed application layer firewall to detect and capture different kind of attacks in networking. The authors proposed Erlangian queuing model in firewall to detect the malware packets which were passed throughout the network. This proposed methodology supported both static and dynamic networking architectures. The proposed firewall architecture supported the malicious packets detection systems in the layers such as network, transport, and application layers. Rakesh Yadav et. al., (2016) proposed a firewall tool to detect the anomalies or unauthorized patterns in network system. The authors set the rule to find the anomalies in networking which supported both static and dynamic network environment. Wenli Shang et. al., (2016) designed and implemented Industrial Firewall to automate the security of industrial network using the protocol Modbus/TCP. The authors effectively analyzed the intercept illegal data stream with respect to various network security parameters.

Jing Li et. al., (2015) developed an efficient framework for Multi-Firewall to prevent the unauthorized entry of the packets from other domain networks. The author's analyzed multi-firewall rule set to protect the network architecture system from un-authorized events. Sahithi Dandamudi et. al., (2015) implemented firewall system to detect unauthorized entry of the packets in network. The data integrity and confidentiality of the network system was analyzed with respect to various parameters in network domain environment. S. Lar et. al., (2011) designed a firewall system using Proactive Security Mechanism in which the packets from various domain networks were analyzed using their proactive logic with their primary address of the firewall system. The fuzzy controller was designed in firewall to maximize the performance of the proposed firewall mechanism design.

The following points are derived from the conventional methods of firewall design for various network domain environments.

- The conventional firewall system supported only static network environment.
- The packets from malicious nodes/devices were not detected by the conventional firewall system.
- The performance in terms of latency and malicious packets detection rate were not optimum for network security.

3. PROPOSED METHODOLOGY

The malicious packets are detected in firewall architecture using similarity index algorithm. The proposed algorithm is explained in the following section.

Step 1: Determine the Energy Index of the individual port in Firewall using the following equation as,

$$\mathrm{E}_1 = \sum_{i=1}^{\mathrm{N}} w_i \times (1 - din_i) \tag{1}$$

where, w_i is the weight of the individual port in firewall and din_i is the number of data bits in an individual packet i.

The energy index is based on the weight of the individual port in firewall system. The weight of the individual port in firewall is computed based on the number of packets correctly and wrongly received in firewall and it is stated as,

$$w_i = \frac{\alpha + 1}{\sqrt{\mathrm{R}^2 - 1}} \tag{2}$$

where, α is the number of packets received correctly at an individual port and β is the number of packets wrongly received at an individual port in firewall architecture and

Step 2: Determine the rational factor (r) of the individual port in firewall as,

$$r_i = \frac{\sum_{i=1}^{\mathrm{N}} \mathrm{E}_i \times (\mathrm{SA})_{\text{packet } i} + (\mathrm{DA})_{\text{packet } i}}{\mathrm{N}} \tag{3}$$

The rational factor determines the originality of the source and destination address and it is correlated to the number of ports in firewall system. In this paper, the length or size of the source and destination address is 10 bits long and the data length is 16 bits long. The performance of the proposed firewall system is high when the value of rational factor is high and the performance of the proposed firewall system is low when the value of rational factor is low.

Step 3: Determine the connectivity factor of the individual port using the following equation as,

$$\mathrm{C}_i = \frac{\mathrm{E}_i}{r_i} \times \sqrt{\frac{(\mathrm{E}_i - 1) \times (r_i - 1)}{\mathrm{N}}}; \quad i = 1 \text{ to } \mathrm{N} \tag{4}$$

The connectivity factor of the port in firewall decides the behaviour of the incoming packets from various source ports in various domain networks. The value of connectivity factor must lie between 0 and 100. If the computed connectivity factor is not in the range, then the firewall system performance is low and there may be number of malicious packets.

Step 4: Find the similarity difference index of the individual port as stated in below equation as,

$$\mathrm{D}_i = \frac{\mathrm{E}_i + r_i}{(\mathrm{C}_i - 1) \times \mathrm{N}} \tag{5}$$

The similarity index shows the resemblance of the received packets in different individual port in firewall system with respect to the energy index and rational factor. Low similarity index illustrates the presence of malicious packets in the individual port and high similarity index illustrates the originality of the packets received from various domain networks.

Step 5: Find the minimum of similarity difference index as

$$\mathrm{M} = \mathrm{Min}\ (\mathrm{D}_1, \mathrm{D}_2, \mathrm{D}_3, \mathrm{D}_4) \tag{6}$$

If M is D_1, then the packets received from port 1 of the firewall is malicious. If M is D_2, then the packets received from port 2 of the firewall is malicious. If M is D_3, then the packets received from port 3 of the firewall is malicious. If M is D_4, then the packets received from port 4 of the firewall is malicious.

4. RESULTS AND DISCUSSION

The performance of the proposed firewall system is analyzed using Network simulator version 2 environments in terms of latency and malicious packets detection rate with respect to number of nodes or computers in network. The initial setup of the simulation tool is described in Table 1. The maximum number of packets for each network used in this paper is 1500 and each node or computer transfers the packets at the rate of 100 kb/s with the energy consumption of 100 mJ per cycle. In this paper, two LAN and two WAN networks are connected with the designed firewall architecture. Each LAN contains 25 computers and each WAN contains 30 computers. Total number of computers used in this paper is 110 (both LAN and WAN).

Table 1
Initial Network parameters setup

Parameters	*Initial Value*
Maximum packets	1500
Throughput	100 kb/s
Energy consumption	100 mJ per cycle
No. of LANs	2
No. of computers in Each LAN	25
No. of WAN s	2
No. of computers in Each LAN	30

A. Latency

It defines the time taken by the designed firewall architecture to identify the malicious packets which are passing through the firewall unit. It is measured in milliseconds. The latency should be low for the better network environment. Table 2 describes the latency of the proposed firewall architecture for different number of computers or nodes. The latency will be increased when the number of computers increases. The latency of the proposed firewall is 2.17 ms when there are 10 numbers of computers connected to the firewall system. The latency of the proposed firewall is 14.74 ms when there are 100 numbers of computers connected to the firewall system.

Table 2
Analysis of Latency

No .of computers/nodes	*Latency (ms)*
10	2.17
20	3.92
30	4.18
40	7.39
50	8.72
70	9.47
80	10.76
90	12.84
100	14.74

Figure 2 shows the graphical illustration of the latency analysis for the proposed firewall architecture using Similarity Index Algorithm. Figure 3 shows the graphical illustration of the malicious packets detection rate analysis for the proposed firewall architecture using Similarity Index Algorithm.

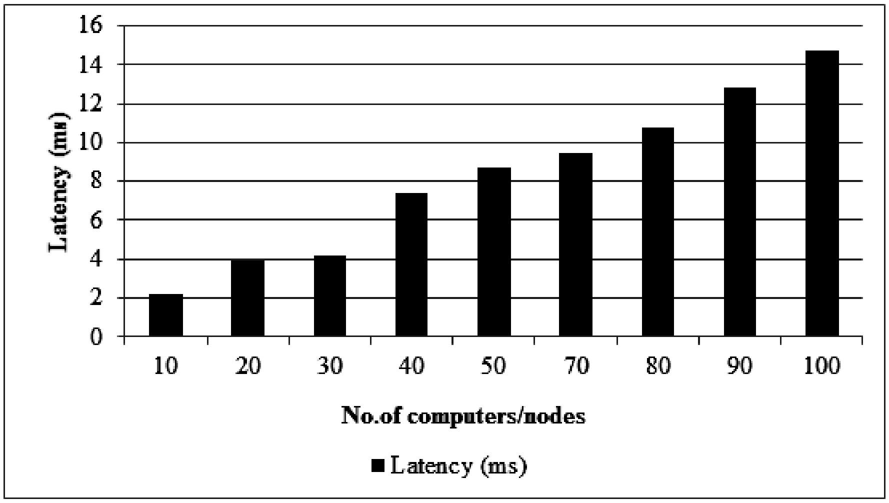

Figure 2: Graphical illustration of latency analysis

B. Malicious Packets Detection Rate

It defines the rate at which the malicious packets are detected by proposed firewall architecture. It the ratio between the number of malicious packets detected by firewall and the total numbers of malicious packets in network environment. It is measured in percentage. The detection rate should be high for the better network environment. Table 3 describes the detection rate of the proposed firewall architecture for different number of computers or nodes. The detection rate will be decreased when the number of computers increases. The detection rate of the proposed firewall is 98% when there are 10 numbers of computers connected to the firewall system. The latency of the proposed firewall is 87% when there are 100 numbers of computers connected to the firewall system.

Table 3
Analysis of malicious packet detection rate

No. of computers/nodes	*Detection rate (%)*
10	98
20	97
30	96
40	95
50	93
70	92
80	91
90	89
100	87

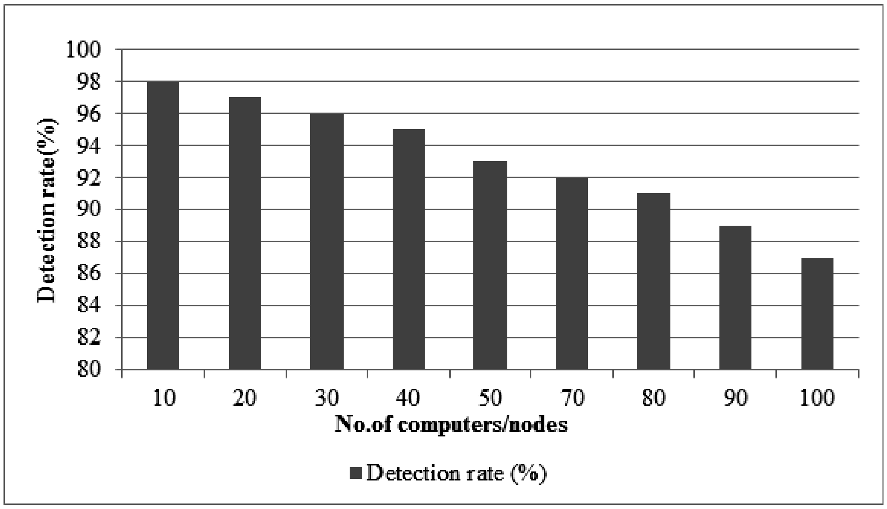

Figure 3: Graphical illustration of malicious packets detection rate analysis

Table 4 compares the performance of the proposed firewall system with conventional methodologies as Xuan et. al., (2016), Rakesh Yadav et. al., (2016) and Lar et. al., (2011). The proposed firewall system achieves 14.74 ms of latency and 87% of detection rate, while the conventional methodologies as Xuan et. al., (2016) provided 17.54ms of latency, 81% of detection rate, Rakesh Yadav et. al., (2016) achieved 18.95 ms, 85% of detection rate, Lar et. al., (2011) achieved 19.38 ms of latency and 80% of detection rate.

Table 4
Comparisons between proposed and conventional firewall system

Methodologies	*Latency (ms)*	*Detection rate (%)*
Proposed method	14.74	87
Xuan et. al., (2016)	17.54	81
Rakesh Yadav et. al., (2016)	18.95	85
Lar et. al., (2011)	19.38	80

5. CONCLUSION

In this paper, malignant packet detection algorithm is proposed in firewall architecture which efficiently detected the malignant packets from various network domains. This proposed algorithm is based on the computation of the energy index of the individual port in firewall architecture. The performance of the proposed system is analyzed in terms of latency and malicious packet detection rate. This proposed firewall architecture achieves 14.74 ms of latency and 87%, of malicious packet detection rate, respectively.

REFERENCES

[1] Xuan S, Yang W, Dong H, Zhang, J., “Performance Evaluation Model for Application Layer Firewalls”, *PLoS ONE*, Vol. 11, No. 11, 2016.

[2] Jing Li, “The Research and Application of Multi-Firewall Technology in Enterprise Network Security”, *International Journal of Security and Its Applications,* Vol. 9, No. 5, pp. 153-162, 2015.

[3] Rakesh Yadav, Harjeet Kaur, Aman Saurabh,” Design of Tool to Detect Anomalies in Firewall Rules”, *Indian Journal of Science and Technology*, Vol. 9, No. 47, 2016.

[4] Sahithi Dandamudi, Tarik Eltaeib, “Firewalls Implementation in Computer Networks and Their Role in Network Security”, *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*, Vol. 2, No. 3, 2015.

[5] S. Lar, X. Liao, A. Rehman and M. Qinglu, “Proactive Security Mechanism and Design for Firewall,” *Journal of Information Security*, Vol. 2, No. 3, pp. 122-130, 2011.

[6] Wenli Shang, Quansheng Qiao, Ming Wan, Peng Zeng, “Design and Implementation of Industrial Firewall for Modbus/TCP”, *Journal of Computers*, Vol. 11, No. 5, 2016.

[7] El-Atawy, A., K. Ibrahim, H. Hamed, and E. Al- Shaer, ‘‘Policy Segmentation for Intelligent Firewall Testing,’’ *1st Workshop on Secure Network Protocols (NPSec 2005)*, 2005.

[8] “A Study on Existing Protocols and Energy-Balanced Routing Protocol for Data Gathering in Wireless Sensor Networks” published in International Journal of Computing and Technology on Nov 10, 2013..Impact Factor 1.213(Refereed Journal). www.cirworld.com/index.php/ijct/article/view/2780/pdf_293

[9] “Challenges and Authentication in Wireless Sensor Networks by using promising Key Management Protocols” at International Conference in Kristu Jayanthi College, Bangalore on Feb 19th & 20th 2015 and Published in International Journal of Computer Applications.Impact Factor 0.814.www.ijcaonline.org/icctac2015/number1/icctac2005.pdf

[10] W. Weiping, C. Wenhui and Z. Wei, “Firewall Technology Analysis”, *Information Security and Communications Confidential*, Vol. 8, pp. 24-27, 2006.