Real-Time Detection for Network Systems Malware Attacks and Prevention Attack Using Artificial Immmune System Algorithm

Ubochi C. I., Amanze B.C., Igbe C.M., Agbakwuru A.O., Agbasonu V.C
Department of Computer Science, Faculty of Physical Sciences,
Imo State Univesrity, Owerri , Nigeria
amanzebethran@yahoo.com

DOI: 10.56201/ijcsmt.v9.no4.2023.pg80.88

Abstract
Malware threats detection and prevention has improved with age, but this improvement seems to be a continuous process as advancement in the technology opens the door with a loop-hole for intruders every time. To develop a system that will intelligently provide real-time detection of network systems malware attacks and prevent the attack using Artificial Immune System (AIS) algorithm and machine learning techniques. During the literature review, it was observed that recently, many researchers were and is still performing their experiment to increase the effectiveness of intrusion prevention in standard datasets. When the amount of data in the network started to grow, this led to a significant challenge in malware threats detection. Therefore, there was need of dealing with these huge datasets. Many IDS still lack the ability to detect all kinds of new attacks in the network, so researchers are inclined towards modeling the normal instances to increase their system effectiveness. Anomaly detection based on outlier has always been a challenging task for real-time detection. In this research work, artificial immune system and machine learning was used to detect the malware threats on the data network. In summarizing the whole research, the work mainly focused on malware threat detection, packets analysis and modeling the normal instances in presence of malicious attack information. Our approach overcomes the drawbacks of one associated with the rule-based approaches and is efficient. One has discussed about the effectiveness of this work on basis on performance metrics, and accuracy. Thus, this work provides a practical solution for construction of better malware threats detection and prevention system based on artificial immune system and machine learning.

Keywords: *IDS, Firewall, Data Network, AIS*

Introduction

Malware is a contraction of malicious programming codes, scripts, active content, or intrusive software that is designed to destroy intended computer systems and programs or mobile and web applications using different forms including computer viruses, worms, ransomware, rootkits, trojan, dialers, adware, spyware, keyloggers, or malicious Browser Helper Objects (BHOs) [1]. Malware is the short form of malicious software or application which is not limited to computer system rather extend to the internet and related fields. Network security refers to activities designed to protect a network. These activities ensure usability, reliability, and safety of a business network

infrastructure and data. Effectual network security focuses on a variety of threats and hinders them from penetrating or spreading into the network [2]. A firewall is a device or software that controls the traffic of a network to block or allow the packets [3]. Depending on the protocol layer they operate at, firewalls can be classified into packet filters, circuit proxies, and application level proxies [4]. However, only two types of firewalls dominate the market today; application proxies and packet filtering gateways (and some hybrid combination of both). Application level firewalls, these goes one step beyond a packet filter. A packet filtering gateway is a firewall technique used to control network access by monitoring outgoing and incoming packet and allowing them to pass or half based on the source and destination internet protocol (IP) addresses, protocols and port [5]. Application level firewalls these check the data that is being sent and authenticate that the particular protocol is being used perfectly [5]. Traditional firewalls have degenerated in terms of ability to resist an attack against them and protect hosts behind them. More challenges like the management of manually configured firewall rule is complex, they are error prone [6]. They also rely on topology restrictions and controlled network entry points to enforce traffic filtering. Hachana emphasizes firewall testing as a very vital step to discover and exposure faulty points plus vulnerabilities existing in the firewall [6]. [7] proposed an integrated firewall, which uses firewall management plane (FMP) and cross layer mechanism and this approach managed to gather data about malicious or suspicious packets and also update the IP packet filter table whenever a certain malicious source was identified [7]. However, the approach cannot detect whether an incoming packet is malicious or not, the approach can only check if the packet belongs to an existing connection and if the source address is already blocked therefore the approach did not fully solve the challenges faced with traditional firewalls.

Intrusion detection and prevention process requires set of different systems to be integrated. To contribute towards the integration, [8] proposed an automated firewall rule set generation system which increased on the accuracy of generated rule sets, solved time wastage which was faced when creating rule sets however useful rule sets can be neglected [8]. Similarly, [9] suggested combination of firewalls, antivirus monitoring tools and IDS to be put in place in order to detect attacks on a network. In both studies, the proposed method can detect packets on the network but a lot of negative and positive false alarms can be generated and genuine packets can be denied to go through the network. Detection of any attack is a decision-making process. Complexity of the process requires intelligent mechanisms to make successful decisions. Saied et al. proposed the use of an artificial neural network (ANN) algorithm to analyze traffic and the approach managed to detect attacks and also separate genuine traffic from DDOS attacks basing on specific features (patterns). [10] also integrated IDSs and an intelligent mechanism as a denial of service intelligent detection system (DoSID) in a similar way [10]. Another important study was carried out by [11] and the study proved fruitful because it added intelligence to firewall systems by using firewall logs and neural networks to analyze traffic on a network [11]. Though the method used is different from the existing traditional firewall, more studies are required to fully work on the challenges of traditional firewall. Method of an agent based early warning system (A-EWS) as proposed in this research work aimed at detecting any attacks or intrusions on a network as early as possible. By using IDS successfully managed to detect any attacks or intrusions on a network as early as

possible. Even though different systems and mechanisms are developed against threads, [12] conducted a study to typically utilize firewalls to be used as the main layer of security in the network framework [12]. This study designing an intelligent firewall agent to address two issues; that is to add intelligence to the traditional firewall and also provide an effective defensive mechanism against network attacks. IDS and the agent will be integrated for increasing performance of decision process.

Review of Related Work

[13] proposed a model of stateful firewalls, which is used to store some packets that the firewall has accepted previously and needs to remember in the near future. They designed a model of stateful firewalls that has several favorable properties. It allowed inheriting the rich results in stateless firewall design and analysis. Moreover, it provides backward compatibility such that a stateless firewall can also be specified using our model. Second, they presented methods for analyzing stateful firewalls that are specified using their model. [14] showed how to eliminate a large percentage of misconfigurations in advance of attempted accesses using a data-mining technique called association rule mining. Their methods can reduce the number of accesses that would have incurred a costly time-of-access delay by 43% and can correctly predict 58% of the intended policy. [15] proposed a new scheme for conflict resolution, which is based on the idea of adding resolve filters. Their main results are algorithms for detecting and resolving conflicts in a filter database. They have tried their algorithm on 3 existing firewall databases, and have found conflicts, which are potential security holes, in each of them. A general solution is presented for the k -tuple filter, and an optimized version is described for the more common 2-tuple filters consisting of source and destination addresses. They also showed how to use the 2-tuple algorithm for the 5-tuple case in which the other three tuples have a restricted set of values. *M.* [16] described an algorithm that contains both intellectual and practical contributions. On the intellectual side, after the basic notion of binary searching on hash tables, they found that they had to add markers and use precomputation, to ensure logarithmic time in the worst-case. Algorithms that only use binary search of hash tables are unlikely to provide logarithmic time in the worst case. They single out mutating binary trees as an aesthetically pleasing idea that leverages off the extra structure inherent in their particular form of binary search. On the practical side, they have a fast, scalable solution for IP lookups that can be implemented in either software or hardware. their software projections for IPv4 are 80 ns and they expect 150– 200 ns for IPv6. Our average case speed projections are based on the structure of existing routing databases that they examined. The overall performance can easily be restricted to that of the basic algorithm which already performs. [17] showed on their paper how to leverage largely commodity Ethernet switches to support the full aggregate bandwidth of clusters consisting of tens of thousands of elements. Similar to how clusters of commodity computers have largely replaced more specialized SMPs and MPPs, they argued that appropriately architected and interconnected commodity switches may deliver more performance at less cost than available from today's higher-end solutions. Their approach requires no modifications to the end host network interface, operating system, or applications; critically, it is fully backward compatible with Ethernet, IP, and TCP. [18] presented an automated process for

detecting and resolving such anomalies. The anomaly resolution algorithm and the merging algorithm should produce a compact yet anomaly free rule set that would be easier to understand and maintain. These algorithms can also be integrated into policy advisor and editing tools. They also established the complete definition and analysis of the relations between rules. [19] represented an innovative mechanism that facilitates systematic detection and resolution of XACML policy anomalies. A policy-based segmentation technique was introduced to achieve the goals of effective anomaly analysis. Also, described an implementation of a policy anomaly analysis tool called XAnalyzer. The results showed that a policy designer could easily discover and resolve anomalies in an XACML policy with the help of XAnalyzer.

System Architecture

The system architecture of the proposed malware threats detection System using an artificial immune system based on the machine learning algorithm is displayed in the diagram in figure 1 .

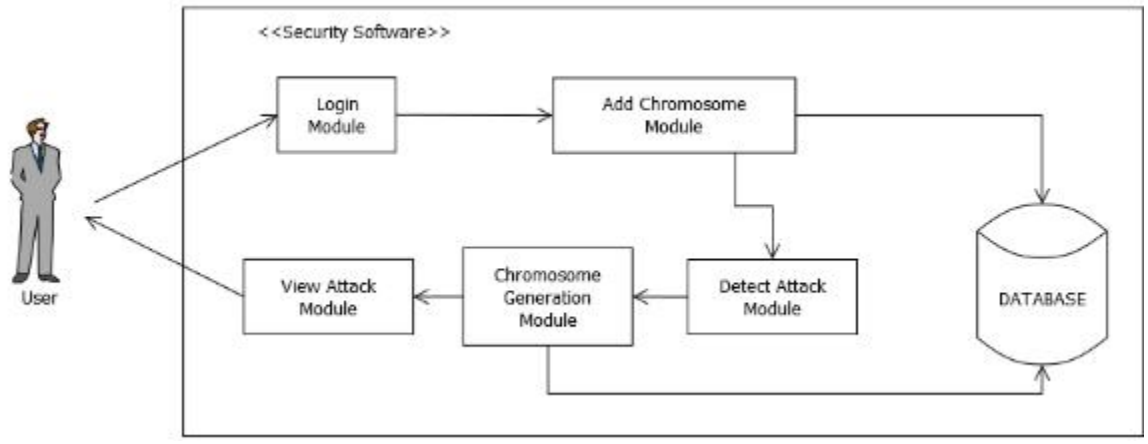

Figure 1: System Architecture of proposed system

High Level Model of the Proposed System

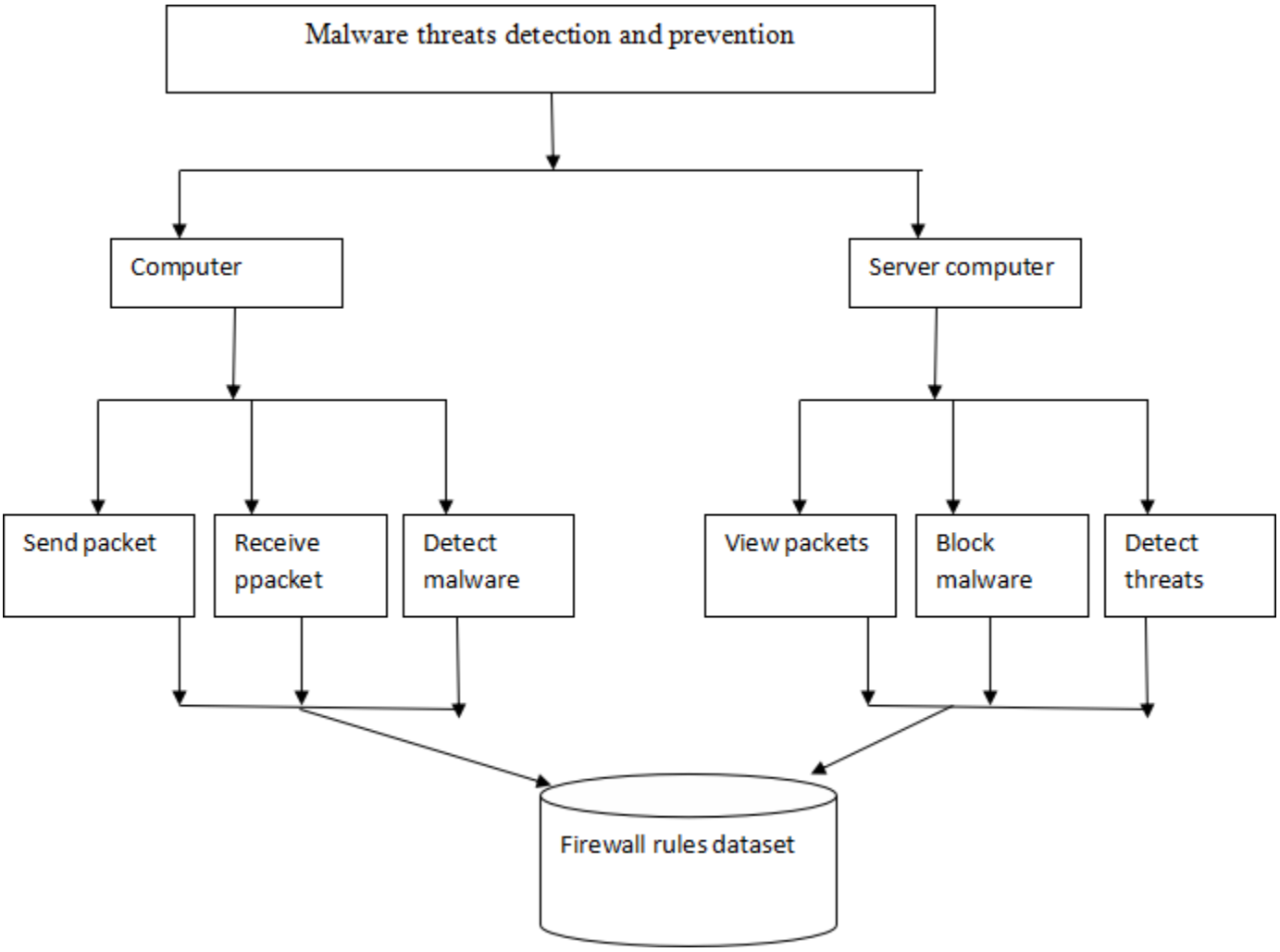

Figure 2: High Level Model of the Proposed System

Algorithm

Algorithm

Algorithm: Treshold-based Artificial Immune

/* Main loop */

FOR each source Node (s) /* Concurrent activity */

Set t to be current time

WHILE t≤T /*T is the total experiment time */

Select destination node to be d;

Set T*sd* to zero /*T*sd*travel time from s to d*/

IF (G^{d} =Yes)

Launch Check Artificial Immune (s, d); /* From s to d */

ELSE

Launch Forward Artificial Immune (s, d);/* From s to d */

IF(T*sd*<= *T_Goodsd*) /* extracted from T-Good table */

Set G^{d} to 'yes'

END IF

END IF

END WHILE

END FOR

Launch Check Artificial Immune (source node: s, destination node: d)

T*sd*= 0

WHILE (current_node≠ destination_node

Select next node using routing table; /* node with highest probability */

Get travel_time from the routing table of the source node;

/* from current node to next_node */

Set T*sd*to be (T*sd*+travel_time);

Set current_node to be next_node;

END WHILE

IF (T*sd*>T_Goods*sd*) SetG^{d} to be 'No'

CHECK malware threats

Launch Forward Artificial Immune (Source node: s, destination node: d)

WHILE (current_node≠ source node)

Select the next node using routing table

Push on stack (next_node, travel_time);

Set current_node=next_node;

END WHILE

Launch backward Artificial Immune (d, s);

Die

END FORWARD Artificial Immune

Launch BACKWARD Artificial Immune (source: s, destination node: d)

WHILE (current node ≠ source node)

Choose next node by popping the stack

Update the malware threat dataset

Update the dataset table (T*sd*)

END WHILE

END BACKWARD Artificial Immune

UPDATE THE malware dataset (T*sd*)

IF (T*sd*<=T_Good*sd*)

←P*hd*1

P*nd*0 ,ɣ n ≠ h, n ε Nk /* h is the node "come from" , k is the current node, Nkis the set of neighbors nodes and packet is the path or sub path destination */

ELSE

←P*hd*1P*hd* +

Generate malware threat alert

Block the packet transmission

end

Conclusion

A malware detection and prevention system were built using immune-inspired algorithms and machine learning. The system developed was carried out using php-Mysql and java script. The software developed was tested and it was able to achieve 91.85% accuracy in malware threats detection and prevention in a network. It is recommended that more research be conducted on how to improve the security in a network system using other methods.

References

[1]. Ahmad, M. (2020). Malware in computer systems: Problems and solutions, IJID (International Journal on Informatics for Development), vol. 9, p. 1,
[2]. Hu, H., Ahn, G. and Kulkarni, K. (2012). Detecting and resolving firewall policy anomalies, IEEE Transactions on Dependable and Secure Computing, 9:318–331
[3]. Ko, H. (2008). Special Issues for Penetration testing of Firewall, Journal of Security Engineering, vol. 5, no. 4, pp. 303-308,
[4]. Leporati, A. and Ferretti, C. (2010). Modeling and Analysis of Firewalls by (Tissue-like) P Systems," Science And Technology, vol. 13, no. 2, pp. 169-180
[5]. Lee, J., Bagheri, B. and Kao, H.-A. (2015). A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems," Manufacturing Letters, vol. 3, p. 18–23
[6]. Hachana, S. , Cuppens-Boulahia, N. and Cuppens, F.(2015). Mining a high level access control policy in a network with multiple firewalls, Journal of Information Security and Applications, no. 20, pp. 61-73

[7]. Langendoerfer, P., Piotrowski, K., Peter, S. and Lehmann, M. (2017). Crosslayer firewall interaction as a means to provide effective and efficient protection at mobile devices, Computer Communications, vol. 7, no. 30, pp. 1487-1497

[8]. Pranschke, G. C., Irwin, B. and Barnett, R. (2009) .Traffic Inspection for Automated Firewall Rule Set Generation, in Information Security South Africa Conference 2009, Johannesburg

[9]. Bsufka, K., Kroll-Peters, O. and Albayrak, S. (2016) . Intelligent network-based early warning systems," in Lecture Notes in Computer Science, Springer, 2016, pp. 103-11.

[10]. Alfantookh, A. A. (2016) .DoS attacks intelligent detection using neural networks, Journal of King Saud University- Computer and Information Sciences, no. 18, pp. 31-51,

[11]. Kumaranayaka, D., Rathnayaka, S. C., Dilhara, M. D. R., Perera, J., Abeysinghe, N. and Wijesundara, M. (2012) .Intelligent Firewall Rule Generating System based on Passive Data Gathering," PNCTM, vol. 1, pp. 63-67

[12]. aur, H., Ebadati, E. M. and Alm, M. A. (2011). Implementation of Portion Approach in Distributed Firewall Application for Network Security Framework," International Journal of Computer Science, vol. 8, no. 2, pp. 207-217

[13]. Gouda, M.G. and Liu, A.X. (2005). A model of stateful firewalls and its properties, in: Proceedings of the IEEE International Conference on Dependable Systems and Networks (DSN-05), 2005, pp. 320–327.

[14]. Garriss, S., Bauer, L. and Reiter, M. K. (2008). Detecting and resolving policy misconfigurations in access-control systems", In Proc. of the 13th ACM Symposium on Access Control Models and Technologies, pages 185–194, Estes Park, CO

[15]. Hari, B., Suri, S. and Parulkar, G. (2010). Detecting and Resolving Packet Filter Conflicts, Proceedings of IEEE INFOCOM'00, March 2010.

[16]. Waldvoge, M. (1997) .Scalable High Speed IP Routing Lookups, Proc. ACM SIGCOMM '97, Cannes, France, Sept. 1997; http://www.acm.org/sigcomm/ sigcomm97.

[17]. Al-Fares, M**.,** Loukissas, A. and Vahdat. A. (2008) .A scalable, commodity data center network architecture". In SIGCOMM

[18]. Abedin, M., Syeda, N., Latifur, K., Bhavani, T. (2006). Detection and Resolution of Anomalies in Firewall Policy Rules, In Proc. 20th IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec 2006), Springer-Verlag, July 2006, SAP Labs, Sophia Antipolis, France (2006).

[19]. Hu, H., Ahn, G. and Kulkarni, K. (2011) .Anomaly discovery and resolution in web access control policies", In Proceedings of the 16th ACM symposium on Access control models and technologies, pages 165–174. ACM