International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 11, ISSN No. 2455-2143, Pages 1-6
Published Online September-October 2016 in IJEAST (http://www.ijeast.com)

APPLICATION OF FUZZY COMPREHENSIVE EVALUATION METHOD IN AN ENTERPRISE BASED ON NETWORK SECURITY

Timothy Osaigbovo,
Aduvie International School/ICT Department, Jahi
FCT Abuja, 234, Nigeria

Garba Suleiman
College of Education/ Computer Science
Department Zuba FCT Abuja, 234, Nigeria

Abstract— **When computer networks was introduced few decades ago, they were primarily used by researchers in academic institution for sending electronic mail and by corporate organizations for sharing printing devices. In these circumstances, security was not a threat and did not get a lot of attention. But today, as millions of individuals world over are using networks for financial transaction, e-commerce, and processing their tax returns, network security is surfacing on the horizon as a potentially massive problem. With the advent of computer systems the need for computerized tools for protecting programs and files stored on the computer became obvious, this is especially the case for a shared system and is even more important for systems that can be logged into from a voice or a data network. In this study, an actual implementation to validate the performance of the designed network defence mode was carried out. The experimental data indicated that the entire system had an average successful detection rate of 87.15%, which met the design requirements. However, a certain margin of error still existed.**

Keywords— **Intrusion Detection System, Honeynet, Firewall, Fuzzy Comprehensive Evaluation**

I. INTRODUCTION

Network and information security is a critical link in a country's overall national security system. Once a war breaks out, the network will become a part of the battlefield. When a cyber-war starts, no one—from governments to private enterprises—will be spared, similar to a war in real life. Cyber terrorism may not cause human casualties or fatalities, but the amount of damages that it can bring will definitely result in a wider scope. The disaster that it will cause is also likely to be a more devastating one. Hence, the security of networks and information systems to an enterprise is as important as military security. Along with the growing popularity of the Internet, the importance of network security has become increasingly prominent. Users' requirements and expectations of network security have also become more sophisticated, leading to the development and growth of network security technologies.

II. NETWORK DEFENCE MODEL

The test subject for our study is a classified and sensitive network laboratory that belongs to the academic network. Its network security model was developed from scratch and gradually built into a complete system. The attempt was to establish a truly effective network defence method. The related procedure is as follows.

- Design a hybrid firewall module. This serves to segregate the intranet from the main gateway to the external network and imposes strict control over access to the intranet resources by external users.
- Install an Intrusion Detection System (IDS) at a critical node of the network (e.g., the server farms). The purpose of this step is to conduct real-time monitoring and detection of a variety of network activities and create appropriate records and issue early warnings when attacks occur.
- Adopt the honeynet technology to link up the network's hybrid firewall, IDS, and virtual honeynet, and then enable the three components to interact with one another. This creates an early warning system for network security. The system administrators will be promptly alerted when there are intrusions or system vulnerabilities; thus, timely repairs and maintenance can be carried out.

The topology of the network defence model adopted in this study is shown in Fig. 1.

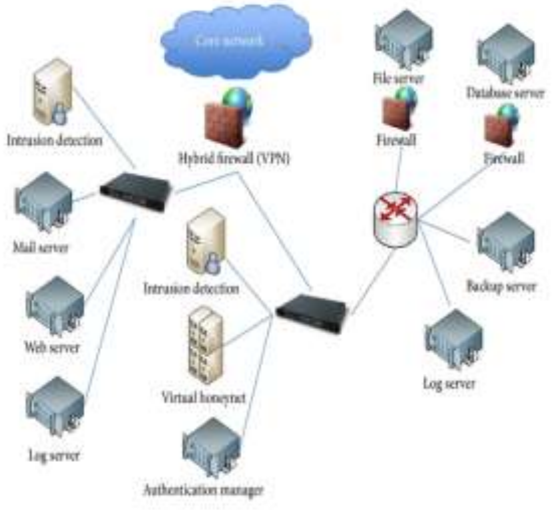

Fig. 1. Network Defence Model

III. Research Method and Theory

The module for screening data packets consists of the screening program (which can be operated at the gateway to the firewall) and two backend programs. This module functions as the security router between the network and the data link layers. It intercepts data packets that pass through the gateway of the firewall and verifies whether these contain application protocols that match the preinstalled security regulations, before deciding whether to forward, block, or discard the packets.

The firewall system uses the Netfilter/Iptables framework of the Linux environment. Appropriate modifications were made so that the system meets the requirements of connectivity and interactivity between the internal components of the computer. This study used Iptables, packets selection tool based on the Netfilter framework, to develop a firewall subsystem with various functions. These Iptables include network address translation (dynamic NAT) during the screening of data packets, proxy servers, and others.

Further, the implementation of the firewall system under the Linux environment consists of two aspects. First, Netfilter provides a scalable and structured underlying framework, on top of which Iptables are implemented. The latter is a selection tool, responsible for the filtering and management of incoming and outgoing data packets. Second, Netfilter and Iptables jointly form the main Linux firewall system.

IV. Fuzzy Representation of the IDS Features

The fuzzy theory is suited for use in intrusion detection because it can easily combine input data from various sources. Since many types of intrusions cannot be clearly defined, the advance warnings that they trigger are usually vague too.

Fuzzy mathematics is used for describing, researching, and managing the mathematical relationships found in things with fuzzy characteristics. A comprehensive fuzzy evaluation is an important application of fuzzy mathematics. When the circumstances involve very complex factors, it can be used for selecting the best program for execution or making a choice after ranking the system detection results after the evaluation.

The main steps of the fuzzy evaluation method are as follows: (i) determine the factors and comments sets for evaluation, and then establish the fuzzy sets of the various factors (membership function); (ii) establish the fuzzy relationship between the evaluation factors and the comments, and then determine the weight that the respective factors have during evaluation; and (iii) derive a conclusion on the basis of calculations using a specific operand. Flexibility in the handling of attacks and the use of reasonable judgment are required for identifying a strict boundary between the normal and the abnormal.

We have used the fuzzy sets technique in this study. The fuzzy sets of basic variables are represented by the following quintuple:

Fuzzyset ::= <Object,Attribute.FC,Domain,ML>

Here, Object refers to the item being described; Attribute, a particular property of the object; FC, the fuzzy concept; Domain, the location of the attribute; and ML, the membership list.

The procedure for conducting a fuzzy evaluation is as follows.

Step 1. Determine the factors and comments sets for evaluation, and then establish the fuzzy sets of the various factors. Internet access can be described using various characteristics such as the duration of the connection, communication volume, source and destination addresses, and types of service (i.e., the target port number). A compilation of these characteristics is known as the factors set. The evaluation vector is the bituple E=<U, W>, where U denotes the factors set U= {u1, u2…,un} and W represents the weight vector. Every component of corresponds to the degree of importance of a factor during evaluation and can be represented as follows: $W = \int_u w/u$. Corresponding to the factors set is the comments set, which refers to the set of linguistic variables of the condition “degree of abnormality.”

The method of describing each factor is consistent. Therefore, the density distribution function of these factors can be treated as their membership function. During this step, the task is to calculate the density distribution function of each factor using the existing data.

Step 2. Evaluate the fuzzy relation between the factors and comments sets, and then determine the weight to be ascribed to the various factors during evaluation. This is the most important step in intrusion detection based on fuzzy evaluation. The detection model can be established once the fuzzy relation between the two sets has been determined. The fuzzy relation between the factors ui and comments indicates the degree of membership that the respective factors have with the various degrees of abnormality. The determination of the fuzzy relation between the factors ui and comments ej is based on f (ui), which is the density distribution function of ui . If the comments set is {e1, e2…,em}, then the density distribution function of ui will be mapped onto m number of fuzzy relations. The relationship between the membership functions of a fuzzy relation is shown in Fig. 2. The following two characteristics of the fuzzy relation between the factors and the comments can be identified from Fig. 2.

(i) The smaller the density of a particular eigenvalue is, the greater the degree of membership of the comment is to a higher degree of abnormality.

(ii) The higher the degree of abnormality of a comment is, the larger the membership function slope is.

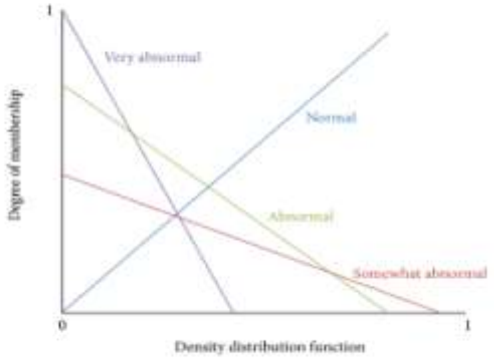

Fig. 2. Membership function of the various comments

In order to determine the weight of each factor, it is necessary to assess and rank the importance of all the factors. In this study, a judgment matrix established through the expert evaluation method (EEM) was used. The EEM is an important fuzzy mathematics tool used for creating fuzzy sets, fuzzy relations, and other mathematical models. It relies mainly on the experience of experts in the related fields. The sequence to establish a judgment matrix using EEM is as follows.

(i) Invite number of experts to establish a comparative judgment matrix A1, A2…,An for a particular type of intrusion, on the basis of their own experiences and the concept of fuzzy relations.

(ii) Set up a group of weights W1, W2…,Wn, W1+ +W2+…,Wn=1 in accordance with the authority ranking of the experts, where Wi represents the authority ranking of expert number i, i E 1,2,…,n.

(iii) Represent the final judgment matrix as A=W1XA1 +…, WnXAn.

Step 3. The conclusion from the evaluation and calculations carried out using a particular operand is derived as follows.

(i) Use the comments set to assess each eigenvalue that was determined by the aforementioned fuzzy relations, and then compose the evaluation matrix.

(ii) Carry out a compositional operation of the fuzzy matrix using the weight vector of the factors list and the evaluation matrix, thereby deriving a comprehensive evaluation vector.

(iii) Determine the comments for this particular set of eigenvalues on the basis of the principle of the maximum degree of membership.

V. Proactive and Early Security Warning Mechanism

The warning mechanism used in this study is a structurally implemented network based on a closed-ended virtual honeynet. Except for the managing platform, the virtual honeynet does not carry out any interactive data transmission with any external host or device. The closed-ended virtual honeynet comprises a virtual intruder, a virtual honeynet gateway, and two virtual honeypot systems. Its network topology is shown in Fig. 3.

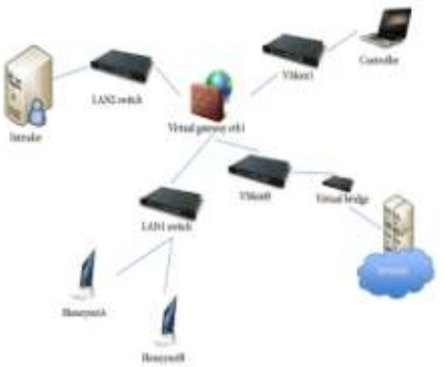

Fig. 3. Membership function of the various comments

Within the virtual honeynet, the LANl, LAN2, VMnet0, and VMnetl switches are all virtual Layer 2 switching equipment. The LANl and LAN2 switches control the exchange of data between the virtual devices.

The VMnet0 and VMnetl switches exercise similar controls but between the virtual devices and the host (managing platform). The VMnetl switch uses the host mode to ensure that the homed host (managing platform) can manage the honeynet gateway; that is, information from the homed host can be transferred to Interface Number 2 (eth2) of the honeynet gateway. On the other hand, the VMnet0 switch uses the bridging mode (normally not used in a closed-ended virtual honeynet) to ensure that the data pass directly through the physical network interface of the homed host (managing platform) to the real network.

There is a bridge between Interface Numbers 0 (eth0) and 1 (ethl); hence, these do not have any IP address. When data packets pass through the gateway, their time-to-live (TTL) values are not reduced. As such, the honeynet gateway is not visible to virtual intruders.

A virtual honeynet system can provide system administrators with the ability to monitor, defend, and document the security of all segments of the network and can play a significant role in enhancing the security management of network systems.

VI. Tests for Different Types of Intrusion

The types of network intrusion used for the experiment are shown in Table 1.

Table- 1 Types of Intrusion

Category	Type	Activities
0	**Normal**	**Normal**
1	**Probe**	**Probes on system vulnerabilities, for example, port scans**
2	**DoS (Denial-of-Service)**	**DoS attacks, for example, SYN flooding**
3	**R2L (Remote-to-Local)**	**Unauthorized access by remote machine, for example, password guessing**
4	**U2R (User-to-Root)**	**Unauthorized access by locally managed accounts, for example, buffer overflow attacks**

The comments set created for the experiment comprises four comments, namely, “Normal,” “Somewhat abnormal,” “Abnormal,” and “Very abnormal”.

All comments assessed as “Abnormal” and above are classified as intrusions. At the start of the experiment, the tcp dump within the gateway was activated to collect the network data. The outputs of this process were multiple records of network communication. These records were divided into four groups. Group 1 was the baseline, which contained network data that did not relate to intrusion activities. In this group, 80% of the data were treated as training data, while the remaining 20% were used for testing the misreported rate. The data for Groups 2–4 were contained in network1, network2, and network3, respectively. Each group was subjected to three different types of attacks. After processing, the four groups of data used for testing the detection rates were stored in the database. The names of the network connection tables were “Normal,” “Intrusion1,” “Intrusion2,” and “Intrusion3,” respectively.

During the experiment, network connections were divided into three categories: (i) outgoing network connections from the local network; (ii) incoming network connections from the extranet; and (iii) connections within the local area network (LAN). The results of the experiment are shown in Table 2.

Table- 2 Intrusion Ratio of Normal and Abnormal Data

Network connection table	Ratio of network connections evaluated as intrusions		
	Outgoing connections	Incoming connections	Connections within the LAN
Normal	**0.62**	**0.23**	**0.88**
Intrusion 1	**3.09**	**15.44**	**18.96**
Intrusion 2	**3.81**	**12.83**	**12.42**
Intrusion 3	**2.41**	**20.03**	**9.51**

Selective data were used for testing. The statistics related to the intrusion detection subsystem are shown in Tables 3 and 4. The former is based on the information collected and the latter on the intrusion type.

Table 3- Statistics Based on Information Collected

Performance indicator %	Type of attack				
	Probe	DoS	R2L	U2R	Mean
Detected	**96.99**	**84.51**	**86.52**	**80.56**	**87.15**
Misreported	**1.71**	**9.03**	**13.48**	**33.33**	**14.39**
Under-reported	**3.01**	**14.84**	**13.48**	**22.22**	**12.36**

Table 4- Statistics Based On Intrusion Type

Type	Number of cases			
	Detected	Misreported	Under-reported	Total
Probe	**226**	**4**	**7**	**233**
DoS	**131**	**14**	**23**	**155**
R2L	**77**	**12**	**12**	**89**
U2R	**29**	**12**	**8**	**36**

The system performance indicators of the network security early warning system were derived through further calculations and analysis. The data are shown in Table 5, and the graphical representation is presented in Fig. 5.

Table 5- Table 5: System Performance Indicators.

Performance indicator %	Type of attack				
	Probe	DoS	R2L	U2R	Mean
Detected	**96.99**	**84.51**	**86.52**	**80.56**	**87.15**
Misreported	**1.71**	**9.03**	**13.48**	**33.33**	**14.39**
Under-reported	**3.01**	**14.84**	**13.48**	**22.22**	**12.36**

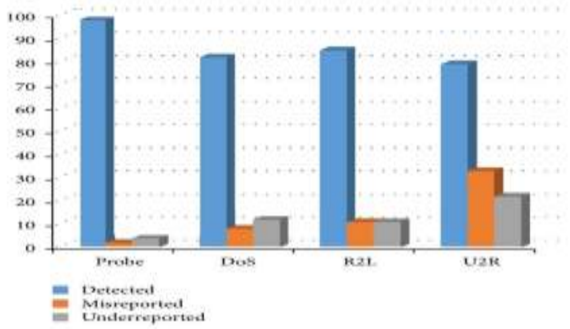

Fig. 5: System performance indicators

VII. CONCLUSION

Computed using the above data, successful detection rate was 87.15%. The requirements that we set for the experiment were met to a certain extent. The firewall system and IDS were stable in their operations and fully functional. The analysis of the two sets of experimental data indicated that the security protection of the system was further enhanced through the connectivity and interactivity between the firewall, IDS, and virtual honeynet. As long as the proposed network security architecture study initiated a connection, the system responded in a timely manner, irrespective of the mode of attack. The connection was also recorded and documented in the system log. This provided a comparative analysis to the system administrators and enabled them to take appropriate measures promptly.

With the above notwithstanding, the experiment reflected a number of shortcomings:

(i) although the IPSec protocol of the firewall could protect the security of the data packets, it reduced their transmission speeds;
(ii) there was room for further strengthening of the system's self-adaptability.

In this study, an actual implementation to validate the performance of the designed network defence mode was carried out. The experimental data indicated that the entire system had an average successful detection rate of 87.15%, which met the design requirements. However, a certain margin of error still existed. Further, the firewall system, IDS, and virtual honeynet system had stable operations, were fully functional, and could fulfil the design requirements.

The contributions of this study could be summarized as follows. (i)The concept of a network defence model was proposed shortly after a systems analysis of a sensitive and classified network was carried out. This systems analysis was an important prerequisite of and the basis for systems design. In this study, a model for an intelligent early warning system was designed. Based on the systems methodology and a combination of the theories of network security and the principles of automatic control, the proposed model was self-adaptive and could respond to network security issues in a dynamic manner in an enterprise. (ii) IPS technology was used for establishing a distributed network security architecture comprising the following components.
(a) Hybrid firewall: A hybrid firewall system was designed on the basis of packet filtering and proxy and VPN technologies. (b) IDS: Snort tools were used for creating a network intrusion detection system that used a fuzzy comprehensive evaluation to determine the intrusion detection eigenvalues.(c) Virtual honeynet system: The approach of a virtual network trap was adopted, together with the implementation of a close-ended virtual honeynet, to give a proactive and early security warning to the network.(d) Connectivity and interactivity were established between the firewall, intrusion detection, and virtual honeynet, which further proved the practicality and usability of the system.
Distributed network security architecture can effectively prevent network intrusions and provide direct protection for key data. It plays an important supporting role in the construction of a network security system. Not only can it be applied to the development of an academic network, but it can also be used for constructing and improving the networks of private corporations and governmental network. The results of this study can provide new ideas and solutions, as well as serve as a reference for future network security topology design and related studies.

VIII. References

[1] D. P. Fidler, "Was Stuxnet an act of war? Decoding a cyberattack," *IEEE Security and Privacy, vol. 9, no. 4, pp. 56– 59, 2011.*

[2] M. Taddeo, "An analysis for a just cyber warfare," *in Proceedings of the 4th IEEE International Conference on Cyber Conflict* (CYCON '12), pp. 1–10, 2012.

[3] R. A. Clarke and K. Robert, Cyber War: *The Next Threat to National Security and What to Do about It*, HarperCollins, 2010.

[4] J. A. Lewis, *Assessing the Risks of Cyber Terrorism*, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, 2002.

[5] X. Chun-Tao, D. Xue-Hui, C. Li-Feng, and C. Hua-Cheng, "An algorithm of detecting and defending CC attack in real time*," in Proceedings of the International Conference on Industrial Control and Electronics Engineering (ICICEE '12),* pp. 1804– 1806, 2012.

[6] S.Chen, J. Xu,R.K. Iyer, andK.Whisnant, "Evaluating the security threat of firewall data corruption caused by instruction transient errors," *in Proceedings of the International Conference on Dependable Systems and Networks (DNS '02),* pp. 495–504, June 2002.

[7] S. Mirzaie, A. K. Elyato, and M. A. Sarram, "Preventing of SYN flood attack with iptables firewall," *in Proceedings of the 2nd International Conference on Communication Software and Networks (ICCSN '10),* pp. 532– 535, February 2010.

[8] H. Salehi, H. Shirazi, and R. A. Moghadam, "Increasing overall network security by integrating signature-based NIDS with packet filtering firewall," *in Proceedings of the 1st IITA International Joint Conference on Artificial Intelligence (JCAI '09),* pp.357–362, April 2009.

[9] M.Marchi, R. Penzo, and A. Provetti, "Policy-based parametric firewall configuration: a real-case application*," in Proceedings of the 8th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'07)*, p. 276, June 2007.

[10] S. M. Bridges and M. U. Rayford, "Fuzzy data mining and genetic algorithms applied to intrusion detection*," in Proceedings of the 23rd National Information Systems Security Conference,* National Institute of Standards and Technology, 2000.

[11] M. Botha and R. von Solms, "Utilising fuzzy logic and trend analysis for effective intrusion detection," *Computers and Security, vol. 22, no. 5, pp. 423–434*, 2003.

[12] L. Zhang and Q.Wang, "A network security evaluation method based on FUZZY and RST*," in Proceedings of the 2nd International Conference on Education Technology and Computer (ICETC '10),* vol. 2, pp.V240–V244, June, 2010.

[13] L. Rui and Y. Yi, “Network security assessment based on fuzzy sets and rough sets*,” in Proceedings of the 5th International Conference on Wireless Communications*, Networking and Mobile Computing (WiCOM ’09), pp. 1–4, September 2009.

[14] J. E. Dickerson, J. Juslin, O. Koukousoula, and J. A. Dickerson, “Fuzzy intrusion detection*,” in Proceedings of the 9th IFSA World Congress and 20th NAFIPS International Conference*, vol. 3, pp.1506–1510, July 2001.

[15] G. Florez, S. M. Bridges, and R. B. Vaughn, “An improved algorithm for fuzzy data mining for intrusion detection*,” in Proceedings of the Annual Meeting of the North American on Fuzzy Information Processing Society (NAFIPS ’02),* pp. 457–462, 2002.

[16] H. Jin, J. Sun, H. Chen, and Z. Han, “A fuzzy data mining based intrusion detection model,” *in Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS ’04),* pp. 191–197, May 2004.

[17] A. Jadhav, A. Jadhav, P. Jadhav, and P. Kulkarni, “A novel approach for the design of network intrusion detection system (NIDS*),” in Proceedings of the International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS ’13)*, pp. 22–27, 2013.