I. J. *Computer Network and Information Security*, 2013, 2, 29-35
Published Online February 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.02.04

Selection of Next Generation Anti-Virus against Virus Attacks in Networks Using AHP

Sounak Paul
Department of Information Technology
Birla Institute of Technology, Mesra, Ranchi, India
paul.sounak@gmail.com

Bimal Kumar Mishra
Department of Applied Mathematics
Birla Institute of Technology, Mesra, Ranchi, India
drbimalmishra@gmail.com

Abstract — Defending against virus attacks in network is a vital part of network security. With the rapid evolution of viruses, its defense mechanism has also been evolved over the years. But given the diversity and complexity of virus propagation and its attack behavior, no defense mechanism is equipped fully to protect the network from such attacks. Several antiviruses are available in the market. But none can give full proof solution to malicious attacks in communication networks. In this paper we present a mechanism to measure and compare the relative ability of antivirus against various kinds of viruses. We construct a hierarchical structure for different virus defense mechanism. Using Analytical Hierarchy Process (AHP) we construct a pair wise comparison matrix and find the value of corresponding Eigen vectors; we then apply the theory of AHP to calculate weight of each defense index. We validated our technique with an example. Our method can provide a strong reference to design an optimal network security solution.

Index Terms — Virus, Antivirus, AHP, Network security, Weight, Defense index

I. INTRODUCTION

The last decade has seen a phenomenal growth of internet and communication technology. However it has also offered a platform for rapid evolution of different malicious code including viruses. To challenge new defense mechanism, modern computer viruses use various mutation techniques such as encryption, polymorphism or metamorphism to evade detection [1][17]. We can classify mutation of virus in the following ways: 1) Encryption- Virus encrypt its body and carry a decryptor module with itself. In early viruses similar encryption key were used in each infection. With decryptor remain same in every generation; detecting the virus was relatively easy using signature of the decryptor [2]. 2) Polymorphism: Polymorphic viruses mutate their decryption engine in newer generation. They changes their payload dynamically to look different in every infection, though they function exactly same, making it difficult for traditional signature based detection scheme to detect them [3][17]. 3) Metamorphism: “Metamorphics are body Polymorphics”[4]. Metamorphic virus does not use encryption, instead they mutate their code structure using various code obfuscation techniques; such as garbage code insertion, swapping interchangeable instruction, control flow obfuscation to create child viruses [5]. Child viruses thus created not only appear different but they also function differently [17].

With the evolution of virus from simple encrypted code to much complex mutated code on every replication, the antivirus must become very sophisticated to defend against virus attack. Several methods of detecting the viruses have been deployed. But given the diverse structure and behavior of viruses, a single method is not sufficient to defend against complex attacks. Modern computer antivirus uses different defense mechanisms together to detect known as well as unknown viruses. For example Symantec antivirus [18] collaborate different defense mechanism to detect malicious code efficiently and effectively. Their file-based protection technology uses signature and heuristic based detection algorithm to scan files for known as well as unknown threats. Their Network-intrusion prevention system (Network-IPS), browser protection and unauthorized download protection system analyzes all incoming data stream before allowing into user’s system. The behavioral based protection of Symantec uses machine learning based/artificial intelligence based classification engine to learn the difference between malicious code and innocuous traffic [18].

Each defense mechanism has their advantages and limitations. Therefore it is very important to determine and compare the ability of defense mechanism used in antivirus in network environment. Determining the ability of the antivirus has great significance in virus research such as propagation dynamics, immunization, detecting and blocking known and unknown viruses.

Most of the research on computer virus focuses on virus propagation model, evolution of virus structure and virus detection and prevention. Measuring and comparing antivirus defense capabilities is a difficult task, because of the dynamics of virus attack. Ming Liu et al. proposed an evaluating model for antivirus ability [9]. In this paper the ability of antivirus has been measured and compared based on relative weight of operating system characteristics, anti-virus and other application characteristics and user characteristics. The focus of this work is on external affecting factor of antivirus. To our best of knowledge a very few research has been done so far on measurement and comparison of antivirus ability based on performance of different defense mechanism used in antivirus. The objective of this paper is to measure and compare antivirus's defense ability based on the relative weight of different defense mechanism used in core of antivirus. For this purpose we use here in this paper a multiple criteria decision making mechanism called Analytical Hierarchy Process (AHP)[6][7][8][9].

The rest of the paper is organized as follows. We present few related definitions, principles in section II. In section III, we present classification of virus defense mechanism. In sections IV we present our proposed scheme. Section V discusses the calculation of antivirus ability, finally we draw conclusion in section VI.

II. Definitions, Principles, And Antivirus Performance Metrics

Discrete classification of defense mechanism is a difficult task. The following definition, principles and metrics form the basis of measuring and comparing the antivirus ability. We define the ability of a computer antivirus as the ability to detect, prevent and eliminate virus from computer system. By computer system we mean associated network, hardware, software and operating system. The more viruses especially new viruses an antivirus detect, higher the ability it has [9][11].

To measure and compare antivirus ability, the classification of antivirus should follow the following principles [9].

- The defense ability must be measurable and comparable. The impact of the defense mechanism should be measurable.
- The classification of the defense mechanism should be comprehensive, so as to cover broader range of antiviral factor.
- The structural and functional boundaries of each defense mechanism should be well defined. It should not overlap with each other.

The following metrics are used to evaluate the performance of a defense mechanism [10] of an antivirus.

- True Positive (TP): Number of programs correctly classified as virus code.
- True Negative (TN): Number of programs correctly classified as benign program.
- False Positive (FP): Number of benign programs incorrectly classified as virus code.
- False Negative (FN): Number of virus codes classified as benign programs.
- Detection Rate $(DR) = \frac{TP}{TP+FN}$
- False Positive Rate $(FPR) = \frac{FP}{TN+FP}$
- Accuracy $(ACY) = \frac{TP+TN}{TP+TN+FP+FN}$

III. Classification of Defense Mechanism Against Computer Virus

People use various methods to detect, prevent and remove computer virus attack. Basically there are three main approaches of virus detection that may be used in modern antivirus software to defend from simple to much sophisticated and complex viruses.

- Signature scanning and emulation based
- Machine learning based
- Immune based

3.1. Signature Scanning and Emulation

3.1.1. Static Analysis Based Detection

In this technique, first the virus binary is disassembled to recover assembly level instructions. Then determine procedural boundaries and obtain control flow graph (CFG) of the instructions. Data flow analysis is done on the CFG to identify the instructions which modify memory locations.

Finally a directed graph based on the code is compared with final representation of suspicious activities to establish whether a program is benign program or virus [12].

3.1.2. Heuristic Analysis

This technique uses the behavioral characteristics of computer viruses combining with past experience to analyze and detect unknown viruses [12][13]. Heuristic based detection detects new/unknown viruses by searching for suspicious instructions within static files before they get a chance of activation. Heuristic based method use context to adjust sensitivity, e.g. a new downloadable program is more suspicious than an already installed and running program [18]. Heuristic analysis is prone to false positives.

3.1.3. Emulation Based Detection

In this technique antivirus implements a virtual machine to simulate processor, operating system and memory activities. This technique is useful especially for encrypted and polymorphic virus. Such virus decrypts in memory. The viruses are examined in virtual environment. One disadvantage of code emulation is that it sometimes takes long time if the decryption loop is very long [14].

3.1.4. Pattern Based Detection

This technique looks for "virus signature", which is a unique sequence of bits from known viruses. This unique signature is organized into a database for use as a fingerprint to match while scanning viruses [15]. Recently some Zero-day (unknown) signature scheme has been proposed. Based on their characteristics, these schemes are broadly divided into two categories; Exploit based and vulnerabilities-driven. While the first category captures the features specific to a worm implementation, the second category captures characteristics of vulnerability the worm exploits [19]. Examples of exploit based signature scheme are polygraph [20], Hamsa [21], PADS [22], CFG [23], Taint Check [24]. Some of vulnerability-driven signature scheme are LESG [19], COVERS [25].

3.1.5. Nearly Exact and Exact Scanning

The second generation scanner use “smart scanning” by ignoring junk instruction such as nop. To achieve higher accuracy and speed near exact identification uses two search strings, hash functions or cryptographic checksums. Exact identification use checksums of all constant bits found in virus [15].

3.2. Machine Learning Based Detection

3.2.1. Hidden Markov Models (HMM) based

HMM is a Virus detection tool requires training to represent a set of data, which is usually in the form of observation sequence and unique symbols. These data are derived from various viruses of a family. The observation symbols are unique assembly opcodes of all viruses. The opcodes of all viruses are concentrated to produce one long observation sequence. Given any observation sequence, we can watch it against a trained HMM to determine the probability of seeing such a sequence. The probability will be high if the sequence is “similar” to the training sequence [15].

3.2.2. Data Mining based

This technique [10] is used to detect unknown viruses. The key to data mining approach is feature extraction. The feature vectors are used to train classification model for virus detection. When compared to a traditional signature or emulations based algorithms, data mining based detection technique reports higher detection rate but resulted in higher false positive rate.

3.2.3. Neural Network based

This technique is primarily used to detect virus- both known and new viruses. IBM has implemented this technique in their antivirus [15]. Feature they have used were short byte string called trigrams. Network is trained to identify training set which consist of both viral and legitimate boot sectors [16].

3.3. Immunity based Model

This technique first extracts vaccine genes (computer virus signature code) and put them into vaccine gene library. After that it generates specific antibodies from known virus vaccine gene, and non-specific antibodies created based on vaccine gene using crossover, mutation and other possible operations. If an unknown virus is identified by non-specific antibodies, its vaccine gene will be added in vaccine gene library [11]. Another method of vaccination is being proposed by Wang et al. in [26]. The method is called Packet Vaccination.

IV. The Proposed Scheme:Measurement And Comparison Of Antivirus Ability By AHP

The measurement and comparison of antivirus is a multifactor optimization process and can be achieved by AHP. AHP decomposes a complex problem into hierarchy of simple subproblems. These subproblems are weighted according to their relative importance to the problem. The bottom hierarchy is the solution alternatives. AHP synthesizes their weight to the problem and finds the best solution. AHP selects the solution alternative with the largest synthesized weight. AHP performs following steps [7][8][9].

Step1: Structuring Hierarchy: Model a problem into hierarchy is the first step of AHP implementation. In this step decision criteria and sub-criteria layer are identified and organized in hierarchy. Overall goal is placed at the root/topmost level of hierarchy. Subsequent levels present option or decision factor to achieve the goal.

Step2: Constructing the pairwise comparison matrix: Comparison matrix of decision factors of same parents are generated through series of judgment.

Step3: Local weight calculation: Calculate the relative weight of decision parameters with respect to parent node using AHP equations.

Step4: Checking for judgment consistency and calculating global weight: Consistency of the judgment is checked. If it passes then only we proceeds for calculating weight of sub-criteria layer decision factor’s weight with respect to the goal layer. Sum weight of decision factors may be calculated thereafter.

A. Structuring AHP hierarchy for defense mechanism

By decomposing the defense mechanism as stated in section 3 we can structure the problem as a hierarchy of multiple factor in Figure 1.

In our problem, at the top level of hierarchy we have goal of the problem – “Antivirus Ability”- this level is designated as a goal layer. In the next level of hierarchy we have three decision criteria. We designate this level as decision criteria layer. The next level child nodes present the decision sub criteria layer.

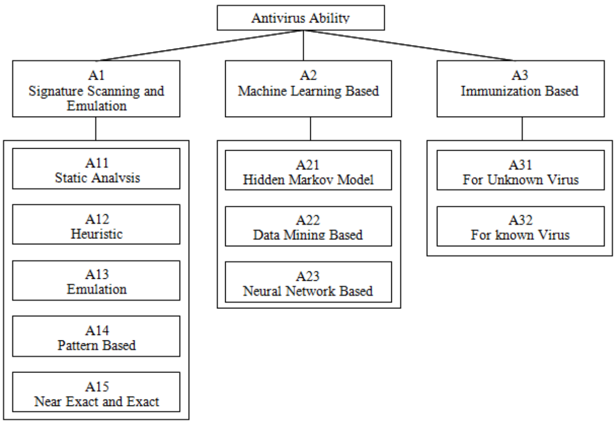

Figure 1. Structuring AHP hierarchy

B. Pairwise comparison

Each factor in a layer is compared with all other factors in the same layer against the goal. The comparison within same parent is done by asking two questions in sequence “which is more important” and “by how much”. The comparison result within same parent is presented with a matrix

$$A=(a_{ij})_{n*n} \qquad (1)$$

Matrix A meet two conditions

i) $a_{ij}>0$

ii) $a_{ji}=\frac{1}{a_{ij}}$

Where element a_{ij} gives the ratio of judgement value of i^{th} factor weight to the j^{th} factor maximum weight. a_{ij} takes the value from 1 to 9 according to AHP as shown in the Table I[7].

TABLE I. FUNDAMENTAL SCALE OF 1 TO 9

a_{ij}	Importance of factor i and j
1	Equal
3	Moderate
5	Strong
7	Very Strong
9	Extreme Importance
2,4,6,8	Moderate between the adjacent values

On the basis of the above scale we present an example of judgment comparisons matrix of criteria layer as follows. The real judgment matrix can be formed only after studying individual antivirus in detail.

$$A=\begin{array}{c|ccc|} & A_1 & A_2 & A_3 \\ \hline A_1 & 1 & 1/4 & 1/2 \\ A_2 & 4 & 1 & 2 \\ A_3 & 2 & 1/2 & 1 \\ \hline \end{array} \qquad (2)$$

This implies that Signature scanning and emulation (A_1) is equal important of itself, Machine learning based method (A_2) is 4 times (refer Figure 1 and Table I) more important than A_1 and 2 times more important than Immunization based (A_3). A_3 is 2 times more important than $A_{1.}$

Similarly for sub criteria of A_1, A_2, and A3 as in Figure I we present an example of judgment comparison matrix in (3), (4) and (5) respectively, as follows.

$$A_1=\begin{array}{c|ccccc|} & A_{11} & A_{12} & A_{13} & A_{14} & A_{15} \\ \hline A_{111} & 1 & 1/4 & 1/3 & 5 & 3 \\ A_{12} & 4 & 1 & 2 & 7 & 5 \\ A_{13} & 3 & 1/2 & 1 & 6 & 4 \\ A_{14} & 1/5 & 1/7 & 1/6 & 1 & 1/2 \\ A_{15} & 1/3 & 1/5 & 1/4 & 2 & 1 \\ \hline \end{array} \qquad (3)$$

$$A_2=\begin{array}{c|ccc|} & A_{21} & A_{22} & A_{23} \\ \hline A_{21} & 1 & 1/3 & 1/5 \\ A_{22} & 3 & 1 & 1/2 \\ A_{23} & 5 & 2 & 1 \\ \hline \end{array} \qquad (4)$$

$$A_3=\begin{array}{c|cc|} & A_{31} & A_{32} \\ \hline A_{31} & 1 & 6 \\ A_{32} & 1/6 & 1 \\ \hline \end{array} \qquad (5)$$

C. Local Weight Calculation

For a reciprocal $n*n$ matrix A, we find the eigen value equation

$$A=\lambda_{max}W \qquad (6)$$

where W is non-zero eigen vector and λ_{max} is the largest eigen value. After standardizing the eigen vector W, we consider the vector element W as local weight of each decision factor approximately, denoted as:

$$W_j^T=\{w_1,w_2,w_3,\dots\dots w_n\} \qquad (7)$$

n is the number of decision factor.

According to (6) and (7) we calculate the weight of three factors in decision criteria layer against goal layer i.e. antivirus ability, and weight of specific defense mechanism in decision sub-criteria layer against the criteria layer. Finally we can get the weight of each specific defense mechanism toward goal layer.

We present below the in Table II the eigen vector for the comparison matrices above.

TABLE II. EIGEN VECTOR OF THE ABOVE MATRICES

Matrix	Eigen Vector (W_A)
A	(0.14285, 0.57142, 0.28571)
A_1	(0.15716, 0.43672, 0.28782, 0.04415, 0.07412)
A_2	(0.10958, 0.30915,0.58126)
A_3	(0.57142, 0.095238)

D. Checking for judgment consistency

Judgment errors are inevitable, since comparisons judgment matrices are subjective, and have to be detected through the following equations.

$$CI=(\lambda_{max}-n)(n-1) \qquad (8)$$

Where λ_{max} is the maximum eigen value and CI is consistency index.

$$\lambda_{max}=\left(\frac{1}{n}\right)\sum_{i=1}^{n}(AW)_i/W_i \qquad (9)$$

AHP matrix is perfect if $CI\geq 0$

Next consistency ratio (CR) is calculated as $CR=CI/RI$. RI is random index and has the following value as shown in Table III. [6][7].

TABLE III. RANDOM INDEX VALUE

n	R1
1	0
2	0
3	0.58
4	0.90

5	1.12
6	1.24
7	1.32
8	1.41
9	1.45
10	1.49

It is mentioned in [6], [7] that the judgment error is acceptable if CR ≤ 0.1. Substituting λ_{max} value in (8) we find CI and CR value calculated using Table III.

The results are listed below in Table IV.

TABLE IV. CI AND CR VALUE OF THE MATRICES

Matrix	CI	CR
A	0.000	0.000
A_1	0.065	0.059
A_2	0.002	0.004
A_3	0.000	0.00

Thus all matrices pass the consistency check. We can now find out the combinational weight or priority of each defense index in decision sub criteria layer to the goal layer using weight ratio of criteria layer to the goal layer and weight ratio of sub-criteria layer to the parent in criteria layer[6] [9] in the following Tables.

TABLE V. PRIORITY OF ELEMENTS OF A1 MATRIX

Defense Factor	A_{11}	A_{12}	A_{13}	A_{14}	A_{15}
Priority	0.02245	0.06239	0.04111	0.00630	0.01058

TABLE VI. PRIORITY OF ELEMENTS OF A2 MATRIX

Defense Factor	A_{21}	A_{22}	A_{23}
Priority	0.06262	0.17666	0.33215

TABLE VII. PRIORITY OF ELEMENTS OF A3 MATRIX

Defense Factor	A_{31}	A_{32}
Priority	0.16326	0.02721

For a given antivirus, we should analyze and decompose the defense mechanisms it has used. We should calculate the weight of each defense mechanism of figure 1. We can calculate the sum weight of defense index with the following equation.

$$W_{av} = \sum_{ij} W\left(A_{ij}\right) * f_{av}\left(A_{ij}\right) \qquad (10)$$

$W(av)$ indicates the sum weight of defense index in antivirus where $\left(A_{ij}\right)$ is the defense index, $W(A_{ij}\ )$ indicates corresponding weight of $(A_{ij}\ )$, $f\left(A_{ij}\right)$ indicates the score of defense mechanism $\left(A_{ij}\right)$ in an antivirus, which can be estimated by the average virus detection rate of the particular defense technique minus its false positive rate.

E. Calculation of Antivirus Ability

We can calculate and measure the antivirus ability in the following way. Priorities of defense indexes of antivirus X and Y are listed in Table VIII, IX and X.

TABLE VIII. PRIORITY AND SCORE OF ELEMENTS OF A1 MATRIX FOR ANTIVIRUS X AND Y

Defense Factor	A11	A12	A13	A14	A15
Priority	0.02245	0.06239	0.04111	0.00630	0.01058
Score of X	80	0	75	73	0
Score of Y	0	78	0	82	70

TABLE IX. PRIORITY AND SCORE OF ELEMENTS OF A2 MATRIX FOR ANTIVIRUS X AND Y

Defense Factor	A_{21}	A_{22}	A_{23}
Priority	0.06262	0.17666	0.33215
Score of X	0	79	0
Score of Y	0	0	73

TABLE X. PRIORITY AND SCORE OF ELEMENTS OF A3 MATRIX FOR ANTIVIRUS X AND Y

Defense Factor	A_{31}	A_{32}
Priority	0.16326	0.02721
Score of X	50	88
Score of Y	65	75

Using (10) we can find the value of sum weight of defense of antivirus X as

$W_{av}(X) =$ 80*0.02245+75*0.04111+73*0.01058+79*0.17666+50*0.16326+88*0.02721 =30.16513

And value of sum weight of defense of antivirus Y is calculated as

$W_{av}(Y) =$ 78*0.06239+82*0.00630+70*0.01058+73*0.33215+65*0.16326+75*0.02721 =43.02322

From the above calculation we can conclude that antivirus Y is stronger than antivirus X.

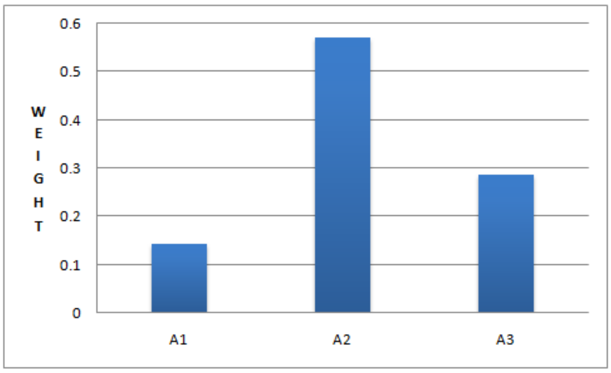

Figure 2. Wight of criteria layer decision factors

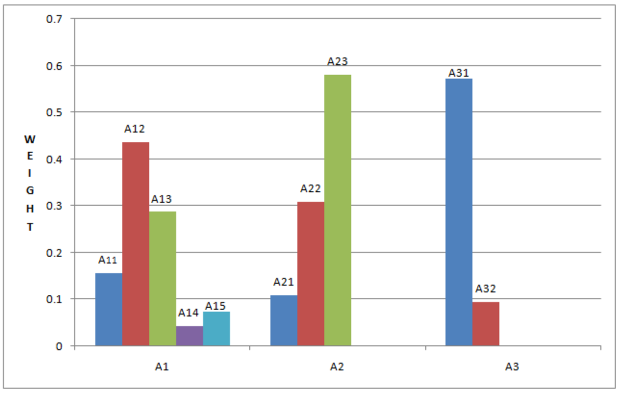

Figure 3. Weight of sub-criteria layer decision factors w.r.t respective parents

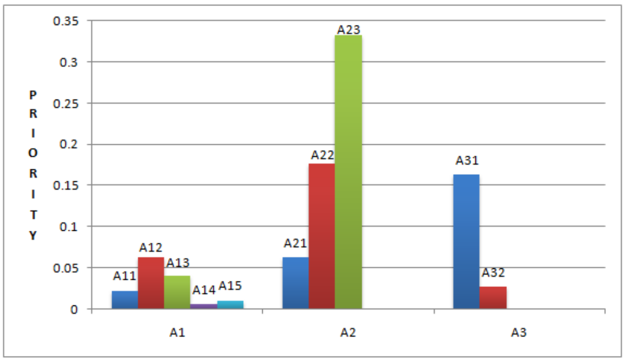

Figure 4. Priority of sub-criteria layer decision factors w.r.t goal layer.

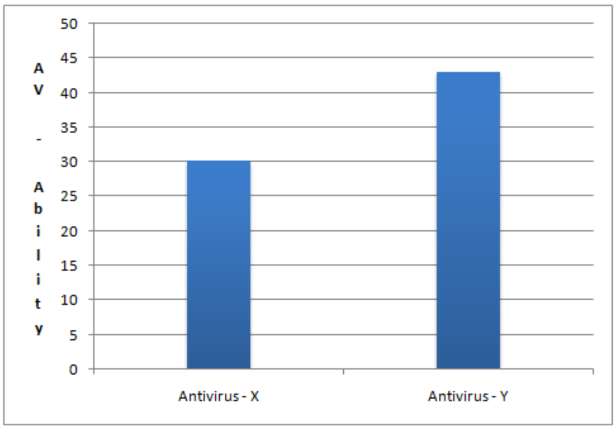

Figure 5. Anti-virus ability

Figure 2 shows relative weight of criteria layer decision factors, against goal layer. Figure 3 shows the relative weight of sub-criteria layer decision factors against their respective parents as calculated in Table II. Figure 4 presents the priority of sub-criteria layer decision factors against goal layer; as shown in Table V, VI and VII. The comparison of ability of two anti-viruses has been shown in Figure 5.

V. Conclusion and Future Work

With the growing menace of computer virus, the antivirus industry is also gearing up to provide sustainable defense from virus attack. There exist several established methods for detecting known and unknown viruses. But given the diversity and complexity of new viruses, a single defense mechanism may not be sufficient to protect the computer and network from such complex attacks. Modern antivirus uses combination of two or more efficient defense mechanisms to defend against much sophisticated attacks in communication network. Each defense mechanism has their advantages and limitations. Therefore it is very important to determine and compare the ability of defense mechanism used in antivirus in network environment. In this paper we propose a mechanism to measure and compare the relative ability of different antivirus using a multiple criteria decision making process called AHP. The method gives the relative weight of each defense mechanism. It can also calculate the sum weight of defense index in an antivirus. The proposed method gives a strong reference to design an optimal security solution against diversified virus attack in networks. The proposed method is scalable; in the sense that it can accommodate any new defense mechanism released in future. We need to include it in the AHP hierarchy in Figure 1 and compute the comparison matrix accordingly.

In our future work, we plan to evaluate our proposed method in a live environment. We need to evaluate performance metrics related to a particular defense mechanism. The research in this direction will provide a more robust and reliable system to designing a stronger security solutions.

Acknowledgements

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions on this paper. The authors also thank Neminath Hubballi and Praveen James Sanga, for their constructive comments and feedback in this work.

References

[1] Xiaoqi Jia, Xi Xiong, Jiwu Jing, and Peng Liu, Using Purpose Capturing Signatures to Defeat Computer Virus Mutating. In the proceeding of ISPEC, LNCS 6047, pp. 153–171, 2010.

[2] Virus-scan-software.com, “A history of computer viruses”, http://www.virus-scan-software.com/virus-scan help/answers/the-history-of-computerviruses.shtml

[3] Venkatesan, Ashwini, Code Obfuscation and Virus Detection, Master’s Projects. 2008, Paper 116.http://scholarworks.sjsu.edu/etd_projects/116

[4] I.Muttik, Silicon Implants, Virus Bulletin, pp. 8-10, May 1997.

[5] Venkatachalam, Sujandharan, Detecting Undetectable Computer Viruses, Master’s Projects,

2010 Paper 156. http://scholarworks.sjsu.edu/etd_projects/156

[6] T.L. Saaty, Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process, RWS Publications, U.S.A., 2000.

[7] Q. Y. Song and A. Jamalipour, A network selection mechanism for next generation networks, IEEE Int. Conf. Communication (ICC). Vol.2, pp.1418-1422, 2005.

[8] Sounak Paul, Sukumar Nandi, Indrajeet Singh, A Dynamic Balanced-Energy Sleep Scheduling Scheme in Heterogeneous Wireless Sensor Networks, In the proceeding of IEEE 16th Intl. Conf on Networks(ICON), 2008.

[9] Ming Liu, Lansheng Han, M.Zou, Qiwen Liu, An Evaluating Model for Anti-virus Ability Based on AHP. , in the proceeding of IEEE Intl Conf on Computational Science & Engineering, 2009.

[10] Jau-Hwang Wang, Peter S. Deng, Virus Detection Using Data Mining Techniques, in the proceeding of IEEE 37th Intl Conf on Security Technology, pp 71-76, 2003.

[11] Yu Zhang, Tao Li, Renchao Qin, A Dynamic Immunity-based Model for Computer Virus Detection, in the proceeding of IEEE International Symposiums on Information Processing, 2008.

[12] Venkatesan, Ashwini, Code Obfuscation and Virus Detection, *Master's* Projects 2008, Paper 116. http://scholarworks.sjsu.edu/etd_projects/116

[13] Li Peng, Wang Ru-chuan , Zhang Wei, Key technologies of new malicious code developments and defensive measures in communication networks, The Journal of China Universities of Posts and Telecommunications, Elsevier, 2010.

[14] P.Szor, P.Ferrie, The art of computer virus research and defense, Addison-Wesley, 2005.

[15] Wing Wong, Analysis and detection of metamorphic viruses. Master's Thesis, 2006.

[16] G. Tesauro, J.O. Kephart, G.B. Sorkin, “Neural networks for computer virus recognition”, IEEE Expert, vol. 11, no. 4, pp., 1996.

[17] P. Li, M. Salour, and X. Su, "A survey of internet worm detection and containment,” Communications Surveys & Tutorials, IEEE, vol. 10, pp. 20-35, 2008.

[18] Symantec Anti-virus: www.symantec.com

[19] Lanjia Wang, Zhichun Li, Yan Chen, Zhi Fu , Xing Li, Thwarting zero-day polymorphic worms with network-level length-based signature generation, IEEE/ACM Transaction on Networking, vol 18, no. 1, pp, 53-66, 2010.

[20] J. Newsome, B. Karp, and D. Song, Polygraph: Automatically generating signatures for polymorphic worms, in Proc. IEEE S&P, 2005, pp. 226–241.

[21] Z. Li, M. Sanghi, Y. Chen, M. Kao, and B. Chavez, Hamsa: Fast signature generation for zero-day polymorphic worms with provable attack resilience, in Proc. IEEE S&P, 2006, pp. 33–47.

[22] Y. Tang and S. Chen, Defending against Internet worms: A signature based approach, in Proc. IEEE INFOCOM, 2003, pp. 1384–1394.

[23] C. Kruegel et al., Polymorphic worm detection using structural information of executables, in Proc. RAID, 2005, pp. 207–226.

[24] J. Newsome and D. Song, Dynamic taint analysis for automatic detection, analysis, and signature generation of exploits on commodity software, presented at the NDSS, 2005.

[25] Z. Liang and R. Sekar, Fast and automated generation of attack signatures: A basis for building self-protecting servers, in Proc. ACM CCS, 2005, pp. 213–222.

[26] X. Wang et al., Packet vaccine: Black-box exploit detection and signature generation, in Proc. ACM CCS, 2006, pp. 37–46.

Sounak Paul is an Assistant professor in the Department of Information Technology, Birla Institute of Technology (BIT), Mesra, Ranchi, India, presently deputed at Birla Institute of Technology, International centre, Muscat, Oman (Waljat College of Applied Sciences). He received his Master in Technology (M.Tech) in Computer science and Engineering from Indian Institute of Technology (IIT), Guwahati, India. He earned his Master in Computer Applications (MCA) from Birla Institute of Technology, Mesra, Ranchi, India. His research interests include network security specially malware analysis and defense, intrusion detection and wireless sensor networks.

Bimal Kumar Mishra is an Associate Professor in the Department of Applied Mathematics, Birla Institute of Technology (BIT), Mesra, Ranchi, India. He received his Master degree in Operational Research from University of Delhi, India (1992) and Masters in Mathematics too. He earned his Ph. D. degree from Vinoba Bhave University, Hazaribag (1997) and subsequently earned his D.Sc. Degree from Berhampur University, Orissa, India in 2007. His research interests include Nonlinear Analysis specifically mathematical modeling of cyber attack and its defense. He is editor in chief of International Journal of mathematical modeling, Simulations & Applications and International Journal of mathematical modeling and Computing. He is the member in editorial board of several international Journals. He has published more than 90 research papers in journals of repute and conference proceedings. Presently he is working in the area of cyber attack/crime and its defense mechanism.