Enhancing Efficiency of Intrusion Detection Based on Intelligent Immune Method in MANET

Lai-Cheng Cao
School of Computer and Communication, Lanzhou University of Technology/Lanzhou 730050, China
Email: caolch@lut.cn

Sheng Dong and Wei Han
School of Computer and Communication, Lanzhou University of Technology/Lanzhou 730050, China
Email: hanwei14810831@126.com

***Abstract*—In order to enhance efficiency of intrusion detection in the Mobile Ad hoc NETwork (MANET), an intrusion prediction method based on intelligent immune threshold matching algorithm was presented. Using a dynamic load-balancing algorithm, wireless network data packet was distributed to a set of analysis subsystem by the balance subsystem; it could avoid packet loss and false negatives in high-performance wireless network with handling heavy traffic loads in real-time. In addition, adopting the dynamic threshold value, which was generated from variable network speed, the mature antibody could better match the antigen of the database subsystem, and consequently the accuracy of detection was increased. Experiment shows this intrusion detection method has relatively low false positive rate and false negative rate, so it effectively resolves the shortage of intrusion detection in MANET.**

***Index Terms*—Mobile Ad hoc NETwork (MANET), intrusion detection, false alarm rate, false negative rate, intelligent immune threshold matching algorithm.**

I. INTRODUCTION

Mobile Ad hoc NETwork (MANET) is becoming more and more widely implemented in the industry [1-3]. A large number of mobile nodes can be deployed in an ad hoc fashion to form a MANET for many civil and military applications [4-5]. However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious [6]; attackers can easily compromise MANETs by inserting malicious or noncooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs. Many research efforts have been devoted to such research topic [7-12]. Paper [13] puts forward a method based on intelligent immune to improve efficiency for intrusion prediction, this method is quoted to resolve intrusion detection in this paper, it obtains relatively low false positive rate and false negative rat.

Intrusion detection implies how effectively an intruder can be detected by the MANET. Obviously, sooner the intruder can be detected, better is the intrusion detection capability of the MANET. In the extreme, the intruder can be detected immediately after it enters the field of interest, which is densely deployed with mobile nodes and has full sensing coverage.

While these existing methods can obtain a high detection rate (DR), they often suffer from a relatively high false alarm rate (FAR) and false negative rate (FNR), which wastes a great deal of manpower. Meanwhile, their computational complexities are also oppressively high, which limits their applications in practice. In this paper, we adopt an intelligent immune threshold matching algorithm, if the bites of continuous matching between the antibody and the antigen are greater than or equal to threshold m, which can be dynamic adjusted in order to enhance detection performance, the antibody and the antigen are matching. In addition, we adopt a dynamic load-balancing algorithm, which can avoid packet loss and false negatives in high-performance network with handling heavy traffic loads in real-time.

The remainder of this work is organized as follows. In Section II we describe the intrusion detection model. In Section III we introduce our dynamic load-balancing algorithm. In Section IV we present intelligent immune threshold matching algorithm. In Section V we finish experiments analysis about our method. The conclusion is presented in Section VI.

II. INTRUSION DETECTION MODEL

Manuscript received August 2013; revised September 2013; accepted November 2013.
The Gansu Provincial Natural Science Foundation of China under Grant No. 0916RJZA015, corresponding author: Cao Lai-Cheng.

doi:10.4304/jcp.9.7.1577-1581

Because MANET IDS frequently have problems with handling heavy traffic loads in real-time, which result in packet loss and false negatives [14], in a configured IDS node, we mend the balance-paralleling architecture of paper[14] and combine intelligent immune method to enhance the efficiency of intrusion detection, this architecture (as shown in Fig. 1) is made up from four subsystem: a balance subsystem, a set of analysis subsystem, an antigen database subsystem, and a detecting result notice subsystem.

- *Balance subsystem*: is responsible for collecting wireless network packets and forwarding these packets to subsequent analysis subsystem. It aggregates the incoming traffic load to multiple analysis subsystem, and carries out load balancing between a number of analysis subsystem to base on a dynamic load-balancing algorithm (namely dynamic least load first algorithm), which divides the data stream based on the current value of each analysis subsystem's Load function. The incoming data packets, which belonged to a new session, are forwarded to the analysis subsystem that has least load currently.
- *Analysis subsystem*: it uses intelligent immune threshold matching algorithm to detect intrusion incident.
- *Antigen database subsystem*: it uses to store the antigen, which contain the feature of intrusion incident.
- *Detecting result notice subsystem*: it uses to classify that network packets are normal or anomalous by the bites of continuous matching between the antigen of antigen database and the antibody that is generated from analysis subsystem.

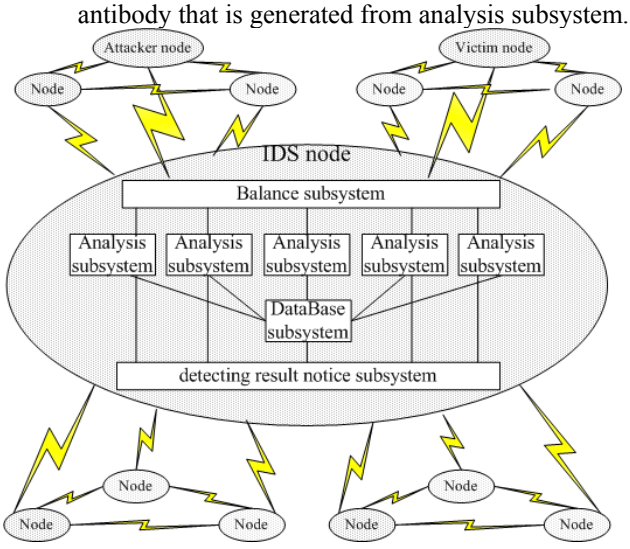

Figure 1. The Architecture of the IDS node.

III. Dynamic Load-Balancing Algorithm

In order to avoid packet loss and false negatives in high-performance wireless network with handling heavy traffic loads in real-time, a dynamic load-balancing algorithm is used in the balance subsystem. This algorithm is described below:

$$L_i(t)=a_1S_i(t)+a_2P_i(t)+a_3U_i(t)+a_4M_i(t)+a_5N_i(t)\ (i=1,2,\cdots,N) \quad (1)$$

Where the number of analysis subsystem is N, analysis subsystem's Load functions is $L_i(t)$ $(i=1,2,\cdots,N)$, the value of Load function stands for the size of the analysis subsystem's load at time t. Meanwhile, the following functions are used:

- $S_i(t)$ $(i=1,2,\cdots,N)$ denotes as analysis subsystem's Session function. The value of Session function stands for the relative number of sessions being processed by an analysis subsystem at time t.
- $P_i(t)$ $(i=1,2,\cdots,N)$ denotes as analysis subsystem's Packet function. The value of Packet function stands for the relative number of packets that are already distributed but not yet processed by an analysis subsystem at time t.
- $U_i(t)$ $(i=1,2,\cdots,N)$ denotes as distributed to the analysis subsystem's CPU function. The value of CPU function stands for the percent utilization of an analysis subsystem's CPU at time t.
- $M_i(t)$ $(i=1,2,\cdots,N)$ denotes as distributed to the analysis subsystem's Memory function. The value of Memory function stands for the percent utilization of an analysis subsystem's Memory at time t.
- $N_i(t)$ $(i=1,2,\cdots,N)$ denotes as distributed to the analysis subsystem's NIC speed function. The value of NIC speed stands for the percent speed of an analysis subsystem's NIC at time t.

Weight coefficients a_1,a_2,a_3,a_4,a_5 represent the relative impact of different parameters on the Load function value. The sum of all weight coefficients should be equal to 1:

$$\sum_{i=1}^{5} a_i = 1 \quad (2)$$

Based on a lot of experimental results and analyses, we may suggest a set of weight coefficients are $a_1=0.3$, $a_2=0.3$, $a_3=0.1$, $a_4=0.2$, $a_5=0.1$. However, the same parameter may have different impact on Load function value in different network traffic environments. For example, the number of sessions would have more impact in FTP traffic environments than in HTTP traffic environments, because an FTP session would be likely to last longer and have more loads than a HTTP session. Hence, we can adjust the weight coefficients to optimize the dynamic load-balancing algorithm based on specific network traffic environments.

Using the dynamic load-balancing algorithm, the data stream on the high-speed wireless network link is divided into several smaller streams that are fed into a number of different, paralleling analysis subsystems. Each analysis subsystem is only responsible for a subset of all detectable intrusion scenarios and can therefore manage to process the incoming volume in real-time.

IV. Intelligent Immune Threshold Matching Algorithm

Definition 1. The self and the nonself:

On the Field $D = \{0,1\}^l$, if antigen set $Ag \subset D$, $self \subset Ag$, $nonself \subset Ag$, then $self \bigcup nonself = Ag$, $self \bigcap nonself = \phi$.

Where *Ag* denotes the binary character string, whose length is *l*, it is obtained by extracting features (namely the feature of network packet of IP address, port number and protocol type) of IP message through the analysis subsystem. Self set is normal network services transaction, and nonself set is illegal activity or network attack.

Definition 2. The antibody and the antigen:

In immunity, antibody is classified three types [15], namely immature antibody, mature antibody and memory antibody. Antibody cell set is

$$B = \{< d, age, count > | \ d \in D \wedge age \in N \wedge count \in N\}$$

Where *d* denote antibody, its length is *l* of the binary character string, age denotes the age of antibody, *count* denotes the count of affinity of antibody, and *N* denotes the set of natural numbers.

Immature antibody is the antibody of nonself tolerance:

$$I_b = \{< d, age > | \ d \in D \wedge age \in N\}$$

Predicting antibody set is $B = M_b \bigcup T_b$.

Where $T_b = \{x \mid x \in B, x \quad count \le \rho\}$ (ρ is matching threshold), this set is mature immune antibody set. $M_b = \{x \mid x \in B, x \quad count > \rho\}$, namely memory immune antibody set, it is generated by evolving from active mature antibody.

- *Intelligent immune threshold matching algorithm*

Supposing the antigen binary character string in antigen database subsystem is $x = (x_i, x_{i+1}, \cdots, x_j)$, and the mature antibody from the analysis subsystem is $y = (x_i, x_{i+1}, \cdots)$, the algorithm, which the Classifier divides that this wireless network visit is normal or anomalous, is shown as follow:

$$f_{match}(x,y) = \begin{cases} 1 & iff \exists i, j(x_i = y_i, x_{i+1} = y_{i+1}, \cdots x_j = y_j, \\ & j - i \ge m, 0 < i \le j \le l, i, j, t \in N) \\ 0 & otherwise \end{cases} \quad (3)$$

Where *m* is threshold, 1 denotes match, and 0 denotes no-match, *l* is the length of character string.

If the match bits are equal or greater than threshold *m*, $f_{match}(x,y) = 1$, the detecting result notice subsystem divides that this network visit is anomalous.

In the process of detecting of the analysis subsystem, if the network speed, which the balancer allocates to the analysis subsystem based on dynamic load-balancing algorithm, is slower, threshold value *m* will be increased to restrain matching speed, it will make that generated mature antibody can more correctly match the antigen of antigen database subsystem, thus detecting accuracy will be enhanced. When the wireless network speed increases, *m* will be decreased; it will make generating mature antibody more quickly, this algorithm is shown as follow:

1) Initialization: $m_0 = l$

2) Generating dynamic threshold m:

$$m_{t+1} = m_t - \text{int}((v_{t+1} - v_t)/n) \quad (4)$$

Where *t* denotes time, *m* denotes the threshold value *m* of t time; v_t denotes the network speed of t time, *n* denotes the amount of self set, function int(z) denotes computing integer part of z.

- *Generating mature immune antibody set Tb*

1) *Initialization:* $T_b(0) = \{\}$

2) Generating dynamic mature immune antibody set

$$T_b(t+1) = T_b(t) + T_{new}(t+1) - (T_{active}(t) + T_{dead}(t))$$

Where

$T_{new} = I_b - \{d \mid d \in I_b \wedge \exists y \in self \wedge f_{match}(d,y) = 1\}$,

$T_{active} = \{x \mid x \in T_b \wedge x \quad count \ge \rho \wedge x \quad age \le \sigma\}$,

$T_{dead} = \{x \mid x \in T_b \wedge x \quad count < \rho \wedge x \quad age > \sigma\}$,

ρ denotes TTL (Time To Live) of antibody.

3) Generating dynamic memory immune antibody set

$$M_b(t+1) = M_b(t) + M_{new}(t+1) - M_{dead}(t+1)$$

Where $M_{new}(t+1) = M_{active}(t+1)$,

$$M_{dead}(t+1) = \{x \mid x \in M_b(t+1), f_{match}(x, self(t)) = 1\}$$

V. Experiment Results

A. Empirical Datum

The detecting is performed based on the system calls data. Table I summarizes the different data sets and program. Intrusions were taken from public advisories posted on the internet. The processes involved are Login, Ps, Xlock, Inetd, Stide, Named and Ftp and intrusions types include buffer overflows, symbolic link attacks, Trojan agents, etc. To validate our method, extensive detecting was also performed based on the data sets collected from the computer network system of our own lab. Several normal and abnormal Http and Ftp system call sequences are collected. The "attacker" and the "victim" consist of denial of service, symbolic link, symbolic, trojanized login, trojanized ps and buffer overflow, etc.

B. Experiment Analysis

TABLE I.
THE SYSTEM CALLS DATA

Data set	Intrusions		Normal data available	
	Attack type	Number of traces	Number of traces	Number of system calls
MIT lpr	Symbolic link Symbolic	1001 1001	2703 4298	2926304 2027468
UNM lpr	Buffer overflow Buffer overflow	2 2	27 72	9230572 16937816
Named	Trojanized login Trojanized ps	9 26	12 24	8894 6144
Xlock	Denial of service	31	3	541
Login Ps Inetd Stide	Denial of service	105	13726	15618237

The evaluation criterion of experiment is False Positive Rate (FPR) and False Negative Rate (FNR).

False Positives—the number of valid traffic samples classified as attacks.

False Negatives—the number of attacks classified as valid traffic.

FPR—the percentage between False Positives and total number of valid traffic samples, namely

$FPR = ((\text{False Positives}) / (\text{Total number of valid traffic samples})) * 100\%$.

FNR—the percentage between False Negatives and the total number of attack samples, namely

$FPR = ((\text{FalseNegatives}) / (\text{Totalnumberof validtrafficsamples})) * 100\%$.

The binary character string antigen $l = 90$, initialization self set $n = 60$, matching threshold $\rho = 60$, experiment time is two weeks, same experiment is repeated five times.

4) Fixed value of threshold m

When threshold m is fixed, in our experiment, m=10, m=15, m=20, m=25, m=30, FPR and FPR are shown as in Fig. 2 and Fig. 3.

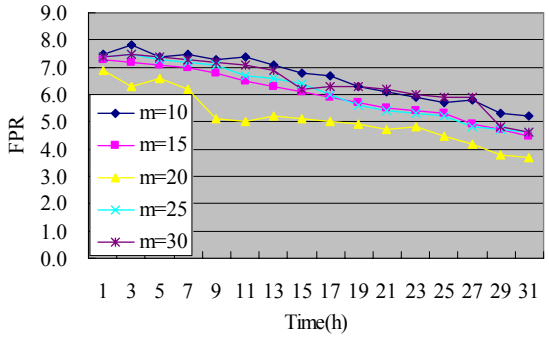

Figure 2. FPR in fixed value of threshold m.

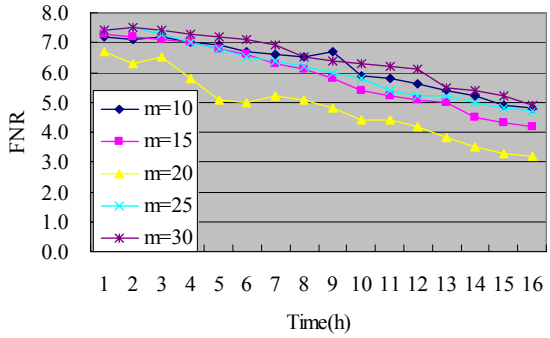

Figure 3. FPR in fixed value of threshold m.

Finding from experiment, when m is lesser (n<20), FPR and FNR are higher. FPR and FNR gradually become smaller with m gradually increase, the reason is that the maturity of antibody gradually increase so that detection precision also gradually increase. When m=20, detection precision reaches optimum, but when m continuously becomes larger (n>20), FPR and FNR gradually become higher, the reason is that computing complex gradually increase.

5) Variable value of threshold m

When threshold m is variable, m is generated based on formula (4). Using two weeks, we repeat same experiment. In comparing between fixed m=20 (optimum value of above experiment) and variable m, FPR and FPR are shown as in Fig.4, here m-Va denotes m-Variable. Because threshold m better adapts variation of network speed, it leads to increase the efficiency of processing data packets, thus variable value of threshold m is better than fixed one.

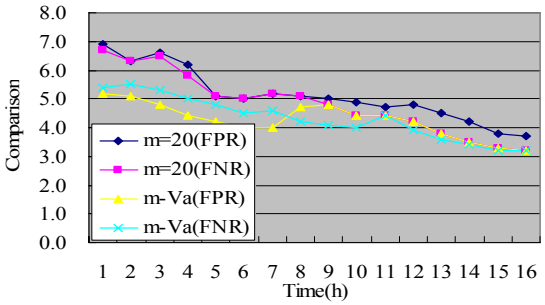

Figure 4. Comparing fixed m to variable m.

VI. Conclusions

Intrusion detection technology clears the way for possible real time response to hostile intrusions to computer network systems, and provides a powerful guarantee, which effectively prevents farther harm for MANET. In this paper, an intrusion detection method based on intelligent immune threshold matching algorithm is presented, this method takes on better real-time detection and relatively low false positive rate and false negative rat, and thus it has an extensive worthiness of applications and theories in network security field.

Acknowledgment

This work is supported by the National Natural Science Foundation of China under Grant No. 60972078; the Gansu Provincial Natural Science Foundation of China under Grant No. 0916RJZA015.

References

[1] Elhadi M. Shakshuki, Nan Kang, Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs," IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS. vol.60, no.3, MARCH 2013.

[2] K. Kuladinith, A. S. Timm-Giel, and C. Görg, "Mobile ad-hoc communications in AEC industry," J. Inf. Technol. Const., vol. 9, pp. 313–323, 2004.

[3] K. Stanoevska-Slabeva and M. Heitmann, "Impact of mobile ad-hoc networks on the mobile value system," in Proc. 2nd Conf. m-Bus., Vienna, Austria, Jun. 2003.

[4] J.N. Al-Karaki and A.E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," IEEE Wireless Comm., vol. 11, no. 6, pp. 6-28, Dec. 2004.

[5] S. Tilak, N.B. Abu-Ghazaleh, and W. Heinzelman, "A Taxonomy of Wireless Micro-Sensor Network Models," ACM Mobile Computing and Comm. Rev., vol. 6, no. 2, pp. 28-36, Apr. 2002.

[6] L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[7] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technol," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[8] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[9] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[10] J. G. Rocha, L. M. Goncalves, P. F. Rocha, M. P. Silva, and S. Lanceros-Mendez, "Energy harvesting from piezoelectric materials fully integrated in footwear," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 813–819, Mar. 2010.

[11] A. Singh, M. Maheshwari, and N. Kumar, "Security and trust management in MANET," in Communications in Computer and Information Science, vol. 147. New York: Springer-Verlag, 2011, pt. 3, pp. 384–387.

[12] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.

[13] Cao, Lai-Cheng, "Enhancing efficiency of intrusion prediction based on intelligent immune method," Lecture Notes in Computer Science, vol. 6216, pp.599-606, 2010.

[14] Wenbao Jiang, Hua Song, and Yiqi Dai, "Real-time intrusion detection for high-speed networks", Computer & Security, Vol 24, No 4, pp. 287-295, 2005.

[15] HE Shen, LUO Wen-Jian, WANG Xu-Fa: A Negative Selection Algorithm with the Variable Length Detector, vol. 18, no. 6, pp. 1361-1368, 2007.

Lai-Cheng Cao, born in 1965, is an associate professor in the School of Computer and Communication at Lanzhou University of Science and Technology. He holds a M.S. degree in the School of Information Science and Technology from Lanzhou University. His research interests include Artificial Intelligence, Communication Systems and Networks, Safety and Security Critical Software.

Sheng Dong, born in 1982, is a graduate student in the School of Computer and Communication at Lanzhou University of Science and Technology. His research interests include the Software Engineering, intrusion tolerance technology, intrusion prediction public-key cryptography algorithm and algorithm optimization.

Wei Han, born in 1983, is a graduate student in the School of Computer and Communication at Lanzhou University of Science and Technology. Her research interests include intrusion prediction public-key cryptography algorithm, Communication Systems and Networks, Safety and Security Critical Software.