A protocol anomaly detection method based on optimized hidden Markov model

Qiu Wei[1,2], Yang Yingjie[1,2], Wang Yongwei[1,2], Chang Dexian[1,2], Liu Jiang[1,2], Hu Hao[1,2]

[1] Information Engineering University, Zhengzhou, 450001, China

[2]Henan Province Key Laboratory of Information Security, Zhengzhou, 450001, China

251197915@qq.com

Keywords: Intrusion detection; protocol anomaly; genetic algorithm; hidden Markov model; parameter optimization

Abstract. As to solve the issues of insufficient training data and initial parameters sensitive in existing protocol anomaly detection based on hidden Markov model, presenting a new protocol anomaly detection method based on improved genetic algorithm and hidden Markov model. First, the local competitive selection strategy, arithmetic crossover and adaptive non-uniform mutation operator were used to improve the genetic algorithm, in order to avoid the "premature" and "stagnation" problem in traditional genetic algorithm; then, the improved genetic algorithm was recommended to optimize the initial parameters of hidden Markov model to avoid the initial model parameters sensitive issue; and finally, the keyword and keyword interval were taken as training observations, describe the behavior of protocol details to expand the training sample space. Experimental results on DARPA 1999 data set show that the method has a high detection rate and low false alarm rate.

Introduction

Protocol anomaly detection [1][2] is the new technologies of anomaly detection [3][4]. it construct model based on the high degree rule and hierarchical of protocol. Since the protocol behavior is highly normative and invariant, the anomaly detection based on protocol can get higher detection rate and accuracy than conventional method. It has become a new hotspot in anomaly detection field.

Currently, the protocol anomaly detection techniques mainly can be divided into two methods: one is based on finite state machine; the other is based on Markov Model. The method based on finite state machine describes the normal protocol behavior by the status of protocol transfer process. All the behavior do not meet the state transition process will be treat as abnormal. Yoo[5] treats the protocol behavior which does not meet the protocol state transitions as abnormal by constructing TCP state machine. This method can visually display the protocol anomaly detection process, but the detection efficiency is not ideal. The Markov Model analysis protocol behavior through the flag sequence which is acquired in network stream. Bailin Xie[6] takes the different user's behavior as different model states based on the key sequence of protocol. Training the Half Hidden Markov Model for normal behaviors and the behavior deviate from the model is judged as abnormal. It achieves some certain results. However, the assumption of the initial state number is unfounded, different states setting will produce different results. Zhao[8] takes the quantization flag of TCP protocol as the observation sequence, and detects abnormal behavior based on the Hidden Markov Model. It gets high detection efficiency and accuracy. But the space of training observations sample is too small, and does not take the sensitive issue of model initial parameters into consideration. It would affect the detection efficiency and accuracy of the results seriously.

As to solve these problems, this paper proposes a new protocol anomaly detection method based on optimized Hidden Markov Model. First, the local competitive selection strategy, new arithmetic crossover and adaptive non-uniform mutation operator are used to improve the existing genetic operator, avoiding the local minima and convergence slow problem in traditional Genetic

Algorithm. Then, the improved genetic algorithm is taken into HMM to solve the sensitivity issue of initial parameter. Finally, the keywords and keyword Interval of protocol are acted as training observed value, expanding the training samples space and describing the feature of protocol behavior more detail. Experimental results show, this method has higher detection rate and lower false alarm rate compared with conventional method based on HMM.

Related Theory

Hidden Markov Model

The Hidden Markov Model[9][10] is a doubly stochastic process developed on the basis of Markov Chain. It contains hidden and observing states, and it is a probability model can parameterize the statistical properties of stochastic processes. The Hidden Markov Model can be represented by a quintuple $\lambda(N, M, A, B, \pi)$. Among them, N is the number of hidden model. M is the number of observed variables. π is the initial state distribution matrix, $\pi_i = P(m_t = s_i)$, m_t is the implicit state of model at time t. $A(A = a_{ij})$ is the transition probability matrix, $a_{ij} = P(m_t = s_j \mid m_{t-1} = s_i) = P(\frac{m_t = s_j, m_{t-1} = s_i}{m_{t-1} = s_i})$, wherein $a_{ij} \geq 0, \sum_{j=1}^{N} a_{ij} = 1$,it represents the probability of transfer state s_j at time t when the model in state s_i at previous time $t-1$. $B(B = b_{ij})$ is the distribution probability matrix of observations events under the order of all hidden states. $b_{ij} = P(O = o_j \mid m_t = s_i), i \in [1, 2 \cdots N], j \in [1, 2 \cdots M]$,it is the probability of observed variable o_j when the model is in a hidden state s_i.

Genetic Algorithms

The Genetic Algorithm[11] is a global optimization algorithm proposed by J.Holland and his students in 1975. It has good parallelism and global optimization capability. It can adaptively adjust the search path according to the objective function and optimize the search results. As the Genetic Algorithm is simple and easily operation, it is widely used in combinatorial optimization, pattern recognition and automatic control. The Genetic Algorithm mainly consists of the following three actions:

a. Choose. It can choose the most appropriate individuals to adapt to the environment for breeding the next generation based on the selection criteria. It will ensure the best genes can be inherited.

b. Cross. Selecting the different individual to interact gene and generate new individuals by simulating the evolutionary process. It can ensure the conduction of algorithm.

c. Variation. Performing the corresponding variation of individual genes to produce a new generation by simulating the evolution process. It can guarantee the diversity of individual.

Protocol anomaly detection based on optimized Hidden Markov Model

There are two protocol states when users communication with protocol, one is the observation state which can be directly obtain from protocol packets, the other is user's hidden behavior states. The two states do not get a one to one relationship. The HMM is a double random process, and can describe the association relationship between these two states well. It can detect the protocol abnormal behavior effectively.

The existing protocol anomaly detection methods based on the HMM use the protocol packet header flag as observations sample to train the model. But its observations space is limited, and cannot describe all the protocol behavior. Therefore, this paper takes the keywords and keywords intervals as the observations feature value. And the observations sample space can be extended. The keywords include protocol request commands and response state codes which can reflect the user communication interactions. Such as the keyword of FTP protocol is composed by commands codes USER, PASS, QUIT and response codes 120,211,350,451 and other components. Users' behave can be represented by different keywords sequences when using differently protocol to communicate.

However, the frequency of keywords is also different when using the same protocol for different activities. Namely the interval time between keywords is different. As to describe the interaction of protocol more detailed, this paper takes the <keywords, interval> attributes as the observation feature value. Expanding the training sample space of HMM models and improving the performance effectively. Furthermore, since the Baum-Welch algorithm of HMM in training, will get different results with different initial input parameters. It will lead model sick into a local optimum issue and drop the detection accuracy. But the initial parameters of existing HMM algorithm are randomly generating, they are not suitable for acting as input parameters.

This paper combines the global optimization ability of Genetic Algorithm with HMM to solve these problems. First, improving the genetic operator to avoid the easily converge of local minima issue and slow convergence defects in traditional Genetic Algorithm. Then, taking advantage of improved Genetic Algorithm adaptive ability to search the optimized initial input parameters after multiple iterations with a randomly input parameters set. Finally, detecting the protocol anomaly with the HMM model constructed by this paper.

The extraction of protocol packet feature

The network stream data need to be isolated into different protocol stream data before extracting the feature of protocol packets. This paper takes advantage of the opinion of reference article [13], using the regular expression to accelerate identification of application layer protocol, and improving the matching speed to meet real-time analysis effectively. For convenience, the relational orderings are defined as follows:

Definition 1 The observations o_i

$o_i =< keywords_i, interval_i >$ is the observation, wherein, $keywords_i$ represents the i th protocol keywords, $interval_i \in \{0,1,2\cdots\}$ represents the interval between i th and $i-1$ th keywords, $interval_i \in \{0,1,2\cdots\}$ and the units is second.

Definition 2 The observation sequence O

O is the observations sequence, and it is used to represent the visible symbol sequence of HMM.

This paper takes the observations attribute set<keywords, interval> as the training data for model training. The observations extraction method is as follows: First, extracting the regular expression pattern of protocol according to the RFC file. Then, the original stream data is preprocessed and converted the matching engine NFA to DFA for identification the protocol data. Finally, extract the keywords and keywords intervals of individual protocol data packets in one connection conversation through WinDump tool. The result is the observations value o_i and all observations constitute the final observation sequence O.

Parameter optimization based on improved GA

Due to the sensitive of training algorithm Baum-Welch for different initial input parameters in HMM, which would lead into a local optimum issue and affect the accuracy of detection results. By combining with the global automatically search ability of Genetic Algorithm, we can get the optimized initial input parameters of HMM after several iterations at a randomly input parameters set. It can solve those problems effectively. However, there are some defects in the existing Genetic Algorithm for the choice of selection, crossover and mutation operators. It will easily fall into local optimum and get poor convergence rate. The existing selection method based on roulette is easy lead the optimization process into a "premature" and "stagnation" state, badly impact the convergence process. The fixed cross operator and mutation operator probability values cannot guarantee offspring is better than their parent, leading the loss of good genes and decrease of individual diversity. To solve these problems, this paper improves the genetic operator. The local competitive selection strategy, new arithmetic crossover and adaptive non-uniform mutation operator are used to improve the convergence rate. It will ensure optimal results effectively. Then, the improved Genetic Algorithm is used for the initial parameter optimization of HMM to solve sensitive issue of initial parameters in Baum-Welch algorithm. The state transition probability matrix A, observation probability distribution matrix B and initial distribution matrix π will affect the

result of HMM significantly, so this paper is focuses on the optimization of the three initial parameters. The improved method and parameter optimization process is as follows:

(a) The selection of initial population

Due to different initial population size will get different optimal results, this paper found that when the initial population $M = 200$, it can get optimum results through the experiment.

(b) The coding of chromosome

$A(A = a_{ij})$ is the hidden state transition matrix, wherein $a_{ij} \geq 0, \sum_{j=1}^{N} a_{ij} = 1$. π is the initial state distribution matrix and $\pi_i \geq 0, \sum_{i=1}^{N} \pi_i = 1$. $B(B = b_{ij})$ is the observations value distribution matrix corresponding to the hidden state, $\sum_{j=1}^{m} b_{ij} = 1$ and $b_{ij} \in [0,1]$. As to ensure the generating new individuals will meet this condition, each new generation of individual parameters need to be normalized. Different A, B and π are represented by a different chromosomes and use the real matrix to encode.

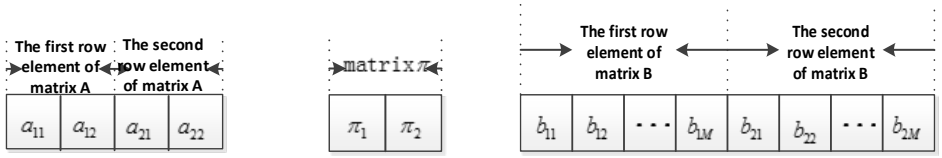

Fig.1. The initial parameter coding of HMM

(c) The determination of fitness function

The fitness function is the criteria of individual selection. It is important to guarantee the accuracy of Genetic Algorithm results. In order to ensure the consistency with results optimization, the objective function $P(O/\lambda)$ is used as the fitness function in HMM.

(d) The improvement of selection operator p_i

The selection operator of Genetic Algorithm plays an oriented role in model. It directly related to the quality of next generation and it is a crucial step in the algorithm. The existing roulette selection method has two major drawbacks. First, in the early evolution, the high adaptation individual will produce more offspring, the diversity of sample will gradually lose and get the algorithm into a local optimum, resulting in "premature". Second, the evolution fitness value will be similar in the late evolution, and the selection capability of algorithm become deteriorates, resulting in "stagnation". In this paper, the local competitive selection strategy is used to select proper individuals. It can reduce the complex of calculation and improve the algorithm efficiency by competing between individuals. Local competition selection is a method that random choose k individuals to compare, and the large fitness individual is selected as parent. The selection method fully considers the size of individual fitness value by local comparison, and do not use the relative ratio of the global fitness value. It can effectively avoid "premature" and "stagnation" issue in the Genetic Algorithm.

(e) The Improvement of crossover p_c

Crossover is the key to maintaining sample diversity of Genetic Algorithm. A good crossover can generate a lot of new winning individual by recombination. It can improve the global search ability and optimize search results. The existing fixed-based probability crossover operator cannot guarantee offspring is better than parent, leading to the loss of good genes. This paper proposes a new arithmetic crossover to solve these problems.

$$\begin{cases} X_A^{k+1} = \beta X_B^k + (1-\beta) X_A^k \\ X_B^{k+1} = \beta X_A^k + (1-\beta) X_B^k \end{cases} \quad (1)$$

Wherein, X_A^k and X_B^k represent the two parent of k th generation individuals, X_A^{k+1} and X_B^{k+1} are two new offspring, β is coefficients and $\beta \in (0,1)$.

(f) The improvement of mutation operator p_m

Mutation operator can increase the diversity of the sample by changing internal genes. It can overcome the "premature" issue. The large scale mutation operators can effectively maintain the diversity of the population in early evolution, but a small operator is able to improve the local search ability of the algorithm in later stage. This paper proposed an adaptive non-uniform mutation operator to improve mutation operator based on the above considerations.

$$p_m(k) = 1 - r^{(1-\frac{k}{N})^b} \qquad r \in (0,1) \tag{2}$$

Wherein, k is the current iteration algebra, N is the maximum number of iterations, b is the parameters of the system, and r is a random number.

(i) The termination condition

In this paper, the maximum evolution generation N is the termination condition. We know the experiment results tend to optimum from the experiment when $N = 150$.

(j)When the algorithm reaches the termination condition, the output result will be the optimal initial parameters of HMM. Otherwise, returning to continue the search.

Model Training

This paper takes advantages of improved Genetic Algorithm adaptive search ability to get the best result in a randomly input parameters set. And the result is act as the optimal initial parameters of HMM. It can get better training model. The optimal initial parameters $\lambda_0(N, M, A, B, \pi)$ of HMM are as follows:

a. The state space S. S are user hidden states of HMM. Because the data of anomaly detection model is the normal data, so the hidden state can be represented by normal state. But in order to ensure the completeness of state space, this paper introduces an unknown state as another hidden state. So the two states can be represented by $S = \{s_1, s_2\}$;

b. The initial distribution matrix π. $\pi = \{\pi_1, \pi_2\}$, in initial state, the probability of protocol packet in a normal state is π_1, and the probability of an unknown state is π_2;

c. The implicit state transition probability matrix A. After optimization of improved Genetic Algorithm, we obtained the optimal matrix $A = \begin{Bmatrix} a_{11}\, a_{12} \\ a_{21}\, a_{22} \end{Bmatrix}$. a_{11} is the probability of protocol state transfer from normal to normal. a_{12} is probability of protocol state transfer from normal to an unknown state.

d. The observations set is $O = (o_1 o_2 \cdots o_M)$, wherein, $o_i =< keywords_i, interval_i >$ and M is the total number of observed value.

e. $B(B = b_{ij})$ is the observation probability distribution matrix. It represents the probability that all the observations made in the normal or unknown state and it is $2 \times M$ order matrix. $B = \begin{Bmatrix} b_{11}\, b_{12} \cdots b_{1M} \\ b_{21}\, b_{22} \cdots b_{2M} \end{Bmatrix}$ is the optimal initial matrix under the optimization of Genetic Algorithm. b_{11} represents the probability of o_1 under normal state, b_{21} is the probability under an unknown state.

The Baum-Welch algorithm is used to train HMM after the determination of initial parameters λ_0. The Baum-Welch algorithm is an iterative algorithm with former probability $\alpha_t(i)$ and backward probability $\beta_t(i)$. Wherein, $\alpha_t(i)$ is the probability of implied state s_i under the observation sequence $o_1 o_2 \cdots o_t$ when the model is determined and $\alpha_t(i) = P(o_1 o_2 \cdots o_t, S_t = s_i / \lambda)$. $\beta_t(i)$ is the probability of implied state s_i under the observation sequence $o_{t+1} o_{t+2} \cdots o_T$ and $\beta_t(i) = P(o_{t+1} o_{t+2} \cdots o_T / S_t = s_i, \lambda)$. In addition, we define variables $\chi_t(i, j)$ and $\gamma_t(i)$. $\chi_t(i, j)$ is the probability of model when the hidden state is s_j at time $t+1$ and the hidden state is s_i at time t. $\gamma_t(i)$ is the probability of model when the hidden state is s_j at time t. Wherein ,

$$\chi_t(i,j) = P(S_t = s_i, S_{t+1} = s_j / O, \lambda) = \frac{\alpha_t(i) a_{ij} b_{jo_{t+1}} \beta_{t+1}(j)}{\sum_{i=1}^{M}\sum_{j=1}^{M} \alpha_t(i) a_{ij} b_{jo_{t+1}} \beta_{t+1}(j)} \quad (3)$$

$$\gamma_t(i) = P(S_t = s_i / O, \lambda) = \frac{\alpha_t(i)\beta_t(i)}{P(O/\lambda)} = \frac{\alpha_t(i)\beta_t(i)}{\sum_{i=1}^{M} \alpha_t(i)\beta_t(i)} = \sum_{j=1}^{M} \chi_t(i,j) \quad (4)$$

$$\gamma_t(i) = \sum_{j=1}^{M} \chi_t(i,j) \quad (5)$$

According to the above formula, we can get the revaluation parameter $\overline{\lambda} = (\overline{A}, \overline{B}, \overline{\pi})$.

$$\overline{\pi_i} = \gamma_t(i) \quad (6)$$

$$\overline{a_{ij}} = \frac{\sum_{t=1}^{T-1} \chi_t(i,j)}{\sum_{t=1}^{T-1} \gamma_t(i)} \quad (7)$$

$$\overline{b_{jk}} = \frac{\sum_{t=1}^{T} \gamma_t(j) * \sigma(o_t, \upsilon_k)}{\sum_{t=1}^{T} \gamma_t(j)} \quad \text{wherein,} \quad \sigma(o_t, \upsilon_k) = \begin{cases} \sigma(x,y) = 1 & x = y \\ \sigma(x,y) = 0 & x \neq y \end{cases} \quad (8)$$

After the iteration, comparing $P(O/\overline{\lambda})$ with the original one. If $P(O/\overline{\lambda}) \le P(O/\lambda)$, stop the algorithm and output the parameters. Otherwise, continue iterating until convergence with $\overline{\lambda}$ replace λ. Since $\alpha_t(i)[\alpha_t(i) \le 1]$ and $\beta_t(i)[\beta_t(i) \le 1]$ involve multiplied many times in iterative process. The recursive value will become increasingly smaller, even close to zero along with t increase. It is the underflow problems. In order to avoid this problem, we use the following formula to normalize for the results of each iteration, and the normalized results are treat as the input of next iteration.

$$\hat{\alpha}_t(i) = \alpha_t(i) / \sum_{i=1}^{M} \alpha_t(i) \quad (9)$$

$$\hat{\beta}_t(i) = \beta_t(i) / \sum_{i=1}^{M} \beta_t(i) \quad (10)$$

Anomaly Detection

In this paper, we detect application layer protocol anomaly based on improved Genetic Algorithm and HMM. We construct a corresponding HMM model for each protocol based on the separation protocol packets. The observation sequence $O = \{o_1 o_2 \cdots o_t\}$ is generated after data pretreatment. Then the Forward Algorithm[14] is used to calculate the value of corresponding model $P(O/\lambda)$. And the preset threshold P is the criterion to detect anomaly. When $P(O/\lambda) \ge P$, the current behavior is determined as normal, and the data will be added into training data for model updating. Otherwise, it is judged to be abnormal and give an alarm. Because there are normal data in model training, the smaller the $P(O/\lambda)$ is, the bigger the exceptions possibility is. As to ensure the different observation sequences of different lengths are comparable, the equation eight is used to normalization. The specific detection process is as follows:

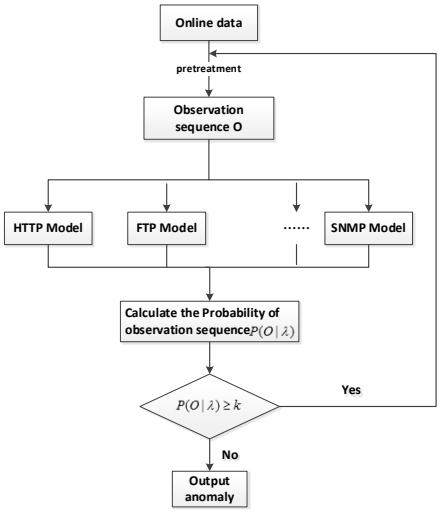

Fig.2. The framework of protocol anomaly detection

Experiments and results analysis

In order to verify the validity of the method, this paper does experiment on the data set of DARPA 1999 [17]. The DARPA 1999 data set is the benchmark assessment data which is widely used in the field of intrusion detection. There are five categories and 58 kinds of typical attacks data, including Probe, DOS, R2L, U2R and DATA. In the five weeks simulation data, the first and third week data without attacking are acted as training data, and the fourth and fifth week data are treated as test data. What more, we only detect the HTTP and FTP protocol behavior respectively.

As to describe the validity of this method better, we compare our method with the method of literature[2] which is based on HMM. And false alarm rate, detection rate and false negative rate are used as the testing criteria, which are defined as follows:

$$R_F = \frac{TF}{TN + TF} \tag{11}$$

$$R_T = \frac{FN}{FT + FN} \tag{12}$$

$$R_T = \frac{FT}{FT + FN} \tag{13}$$

Wherein, TN are the normal data which are detected as normal. FN are abnormal data which are detected as abnormal. TF are the normal data which are false detected as abnormal. FT are abnormal data which are missed detected as normal.

This paper detects the HTTP and FTP model by adjusting the detection threshold P, the experiment results are as follows:

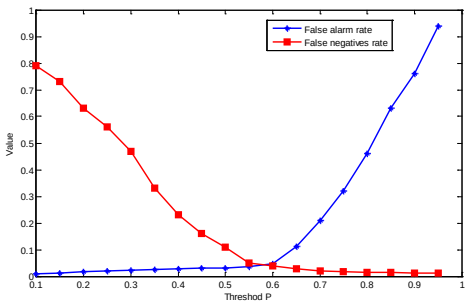

Fig.3. The relationship of false alarm rate and false negatives rate with the threshold P in HTTP model

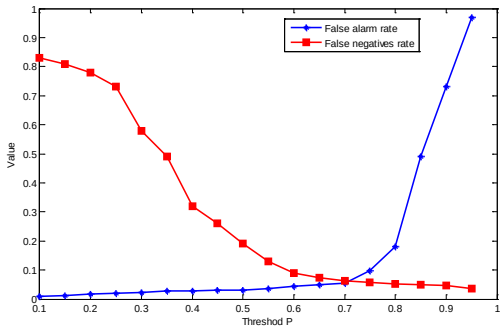

Fig.4. The relationship of false alarm rate and false negatives rate with threshold P in FTP model

As the experiment results show, the false alarm rate will increase with the addition of threshold value, but the false negative rate will increase in both HTTP and FTP model. That is because the models will judged more normal behavior as abnormal with the increase of the value P, which will

lead the addition of false positive rate. And the abnormal behavior was missed detected, leading the reduction of false negative rate. For the HTTP model, when the threshold $P = 0.6$, the false positives and false negatives can be maintained at an ideal interval. But for FTP model, when the threshold $P = 0.7$, the false positives and false negatives can be maintained at a more realistic range.

According to experiment results, the threshold of HTTP model is set as 0.6 and the threshold of FTP model is set as 0.7.The detection results of our method compare with classical method based on HMM are as follows:

Table 1 The comparison results of different methods

Data model	Detection criteria	Detection model	
		Improved HMM	HMM
FTP	Detection rate	93.67%	85.37%
	False positive	4.7%	8.4%
HTTP	Detection rate	97.8	90.1%
	False positive	3.2%	4.6%

From the above results, the detection rate, false positive rate and false negative rate of our method has improved compared with the traditional HMM. So the expansion of the sample space and optimize the initial parameters can improve the performance of HMM. And the performance of HTTP model is better than FTP model. Because the training data of HTTP is more than FTP in training process. It shows that the model has a certain dependence on the completeness of the training data.

Conclusion

The protocol anomaly detection has become a new hot in detection research. This paper proposes a protocol anomaly detection method based on improved genetic algorithm and HMM. We raise the Genetic Algorithm convergence speed and global optimal performance by improving the existing Genetic Algorithm selection, crossover and mutation operators. Solving the initial parameters sensitive issue of HMM through optimize the initial parameters with improved Genetic Algorithm. Finally, the experiments on DARPA 1999 verify the validity and reliability of this method.

Acknowledgement

In this paper, the research was sponsored by the 863 projects (Project No. 2012AA012704), National 973 Program (Project No. 2011CB311801) and leading scientists project of Zhengzhou City (Project No. 131PLJRC644).

References

[1] Satoshi Kagami,Tomonobu Kitagawa,Koichi Nishiwaki,Tomomichi Sugihara,Masayuki Inaba, Hirochika Inoue. A Fast Dynamically Equilibrated Walking Trajectory Generation Method of Humanoid Robot [J], 2002.

[2] VR Lakshmi,MK Kanth.Security Protocol in Network Traffic by Intrusion Detection[J].Journal of Current Computer Science,2015,vol(5):6-10.

[3] Sean Whalen,Matt Bishop,James P.Crutchfield. Hidden Markov Models for Automated Protocol Learning[C].SecureComm 2010, LNICST 50, 2010:415–428.

[4] Monowar H. Bhuyan, D.K.Bhattacharyya, I.K.Kalita. Network Anomaly Detection: Methods, Systems and Tools[C] //IEEE Communications Surveys &amp Tutorials (Impact Factor: 6.49). 2014,16(1):303-336.

[5] Tang Chenghua, Liu Pengcheng,Tang Shensheng. Anomaly Intrusion Behavior Detection Based

on Fuzzy Clustering and Features Selection[J]. Journal of Computer Research and Developmen. 2015:718-728

[6] Yoo I S .Protocol anomaly detection and verification [C] //Proc of the 2004 IEEE 5th Annual IEEE Workshop on Assu rence and Security.Piscataway,N J:IEEE,2004:74 -81

[7] Xie,Qiansheng. Apllication-layer Anomaly Detection Based on Application-layer Protocols' Keywords[C]. 2012 2nd International Conference on Computer Science and Network Technology, 2012 IEEE

[8] Zhao Jing, Huang Houkuan,Tian Shengfeng. Protocol Anomaly Detection Based on Hidden Markov Model[J]. Journal of Computer Research and Developmen. 2010,47(7)：621-627

[9] Wael Khreicha,Eric Grangera,Ali Mirib,Robert Sabourina. Adaptive ROC-based ensembles of HMMs applied to anomaly detection[J].Pattern Recognition,2012:208-230

[10] JJ Flores,F Caldern, A Antolino.Network Anomaly Detection by Continuous Hidden Markov Models-An Evolutionary Programming Approach[J].Flores 2015 network,2015:24-33.

[11] Vishakha V Patel,Kamal Sutaria.A Survey on Community Detection in Social Network using Genetic Algorithm[J].International Journal of Engineering Development and Research, 2015: vol(3):16-19.

[12] NK Dhillon, MU Ansari, Enterprise Network Traffic Monitoring, Analysis, and Reporting using Winpcap Tool a packet capturing API. International Journal of Advanced Research in Computer Science and Electronics Engineering, Volume 1, Issue 6, August 2012

[13] Shanshan,Minfei Zhang,Penglin Li.SVM-HMM Based Human Behavior Recognition.Springer International Publishing Switcerland.2015:93-103.

[14] Mahoney M V.Chan P K. An analysis of the 1999 DARPA/Lincoln Laboratory evaluation data for network anomaly detection[C]//Proc of the 6th Int Symp on Recent Advances in Intrusion Detection. Berlin: Springer, 2003:220-237.