МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2007
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2007
Proceedings of the Thirty Sixth Spring Conference of
the Union of Bulgarian Mathematicians
St. Konstantin & Elena resort, Varna, April 2–6, 2007

BCJR ALGORITHM, GRADIENT METHOD AND ANOMALY BASED INTRUSION DETECTION SYSTEMS*

Evgeniya P. Nikolova, Veselina G. Jecheva

Hidden Markov Models (HMM) are probabilistic models suitable for various recognition problems, particularly for intrusion detection. The present paper investigates the capabilities of the BCJR algorithm, based on log-likelihood ratios (LLR) in anomaly detection method. The BCJR application is preceded by the HMM training using ML criterion, namely gradient based method. Some experimental results of this algorithm were represented compared to the results of the same algorithm over training using ML criterion.

1. Introduction. Computer security is an important challenge in the contemporary world. The intrusion detection system (IDS) is aimed to find attacks exploiting illegal usages or misuses. To protect the network, an IDS must generate alarms when it detects intrusive activity. Different IDSs trigger alarms are based on different types of network activity. The two most common triggering mechanisms are the following: anomaly detection and misuse detection [3].

Misuse detection IDSs generate the alarms based on specific attack signatures. These attack signatures encompass specific traffic or activity that is based on known intrusive activity. Their major drawback is their little possibility of detecting an attack at its first appearance. Anomaly based IDS assume that an intrusion will always reflect some deviations from normal system work. They build models of normal user activity and then attempt to detect some deviations from the normal model in the observed data. If any user activity deviates too much from the normal user data, then the IDS assumes an intrusion is present and generates an alarm. One of the most important advantages of the anomaly based IDS is the ability to detect attacks regardless of whether or not the IDS has observed them before.

There are different approaches to describe normal user activity and the deviations from this baseline – finite automata [15, 11], machine learning [2], Hidden Markov Model [8, 12], genetic algorithms [5, 9, 14], statistics [4], etc. Our work is based on the anomaly detection at program level, introduced by Forrest, Hofmeyr, Somayaji, and Longstaff [6]. They examined the short sequences of system call traces produced by the execution of the privileged programs at Unix system.

The present paper introduces a comparison between two approaches, based on the HMM and BCJR algorithm. The system model is created using the Hidden Markov

*Key words: intrusion detection, Hidden Markov Models, maximum likelihood criterion, BCJR algorithm, gradient based method, Log-Likelihood ratios

Model (HMM) – a finite state machine which transforms the input system call sequences into sequences of hidden states. The initial HMM is tuned using a gradient based method and the BCJR decoding algorithm is then applied. The results obtained from the two described approaches – BCJR algorithm and BCJR algorithm applied after HMM training, are introduced.

2. The system model. Our system model is created using the Hidden Markov Model (HMM) (see [13]), which contains the set of states $S = (s_1, s_2, \ldots, s_N)$ and the set of observable states (intrusions) $V = (v_1, v_2, \ldots, v_M)$. The elements of the set S are the states the system passes through its work in the discrete moments of time $t = 1, 2, \ldots, T$. Let $O = (O_1, O_2, \ldots O_T)$ be the incidents sequence in the moments $t = 1, 2, \ldots, T$, where each O_i is equal to some v_j $(i = 1, \ldots, T;\ j = 1, \ldots, M)$. The HMM is completely specified by:

1. the initial probability distribution $\pi = (\pi_1, \pi_2, \ldots, \pi_N)$, where π_i is the probability the system is in state s_i, $i = 1, \ldots, N$ at the initial moment $t = 1$;

2. the state transition probability matrix A=$\{a_{ij},\ 1 \leq i \leq N,\ 1 \leq j \leq N\}$, $0 \leq a_{ij} \leq 1$ and $\sum\limits_{j=1}^{N} a_{ij} = 1$, where a_{ij} is the transition probability from the state s_i to the state s_j holding the intrusion type $v_k \in V$ constant;

3. the observable probability distribution matrix $B = \{b_j(k) = P(k^{th}$ observed $|$ system is in state j), $1 \leq j \leq N$, $1 \leq k \leq M\}$, $0 \leq b_j(k) \leq 1$ and $\sum\limits_{k=1}^{M} b_j(k) = 1$.

We consider the system process as a first order hidden Markov process, described by the model $\theta = (A, B, \pi)$.

The parameters of the model can be optimized according to the gradient based method [2] which is based to the standard formula

$$\theta_{\text{new}} = \theta_{\text{old}} - \eta \left[\frac{\partial J}{\partial \theta} \right]_{\theta = \theta_{\text{old}}},$$

where J is a quantity to be minimized and η is the learning rate. In our case we set $J = -\log p(O|\theta)$. Since there are two main parameter sets, transition probabilities a_{ij} and observation probabilities $b_j(k)$, we can find the gradient $\dfrac{\partial J}{\partial \theta}$ for each of the parameter sets.

We use the BCJR decoding algorithm [1] to estimate random parameters with a prior distributions. The algorithm scans the traces of the system activity and compares with the patterns of normal user activity. Its results have the form of log-likelihood ratios (LLR), which are represented as follows

$$\Lambda_i = \ln \frac{P(m_i = 1 | y_i)}{P(m_i = 0 | y_i)},$$

where $P(m_i = k | y_i)$ is the a posteriory probability in which the bit, determining the presence of attack, is equal k, k =0,1.

3. Experimental results. Experiments, based on the algorithms described, were accomplished using corresponding software in C++. The data in these experiments were

obtained from University of New Mexico's Computer Immune Systems Project [16]. The method of their obtaining is described in [6] and [7]. The experiment data consists of two main sets: normal activity patterns, including main process patterns (sendmail, ftp, named and lpr), as well as their child processes patterns which compose the set S, i.e. the system states. The experiment data also contain intrusive activity patterns, generated by some common intrusion tools (sm565a, syslog-local, syslog-remote, sscp, decode) which compose the set V of the HMM. Each data file consists of pairs of numbers, one pair per line. The first number in each pair is the process ID (PID) of the process executed, and the second one is the system call number. The correspondence between system call numbers and the actual system call names is stored in an additional file. The intrusion data are put into sequence which elements constitute the observation sequence O with length T from the HMM. In our experiments T takes the following values: 10, 15 and 20.

A method for intrusion detection during the system work using the BCJR decoding algorithm was propounded in our previous work [10]. The intrusion detection problem is considered as decoding problem. Figure 1 shows some of the results and the LLR's calculated. Each LLR is the logarithmic ratio from the probability of attack presence to the probability of normal activity at specific moment t. It can be seen, that if LLR is positive, then it implies that we most likely have attack.

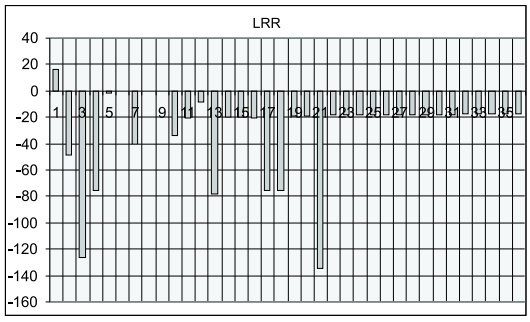

Fig. 1. LLR's calculated using the BCJR decoding algorithm

Another strategy for checking whether the particular activity data is normal or anomalous, is a prior to determine the model parameters A, B for given an HMM θ and given sequence of observations O using standard gradient method, and then to apply the BCJR decoding algorithm. For standard gradient method we use learning rate η from $0.00001 - 0.001$ for both observation and transition probabilities. Some of the results obtained by the BCJR decoding algorithm for T=10 and $\eta = 0.00001 - 0.00005$ are shown in Figure 2. It can be seen, that IDS most probably checks O_6 as attack.

We accomplished an evaluation of the algorithm performance in terms of detection accuracy. The detection accuracy of IDS is the percentage of attack samples detected as attacks. The false rate of IDS accounts for the detection of normal sample as an attack. We compare the work of BCJR algorithm against its work over training which is performed using the gradient based method. Based on our calculations, some of which are presented graphically in Figures 3, 4 and 5, the values of the LLRs which apply by BCJR algorithm, are compared to those of the values of the LLRs, which apply by BCJR algorithm over gradient training for $T = 10.15$ and 20 and $\eta = 0.00005$. Figure 5

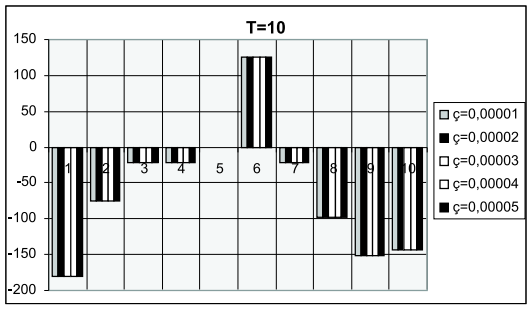

Fig. 2. LLR's calculated using the BCJR decoding algorithm depending on the values of η

represents the second method most likely checks O_6, O_{14}, O_{19} and O_{20} as attacks, while the first method considers them as normal system work. The best results for the second method were 83% accurate while the best results for the first method were 78%. It is worth mentioning that the decoding based on BCJR algorithm is more consistent with preceding gradient training.

Finally, potential future work includes investigation of the reasons for false rate and investigation of the efficiency of this algorithm.

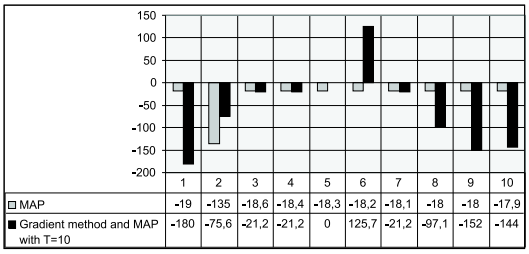

Fig. 3. Comparison between the results of independent BCJR algorithm and BCJR algorithm combined with gradient based method when $T = 10$

4. Discussions. An advantage of the described method is its potential to detect an unknown attack the first time it appears, as it is based on the BCJR decoding algorithm, which results in calculation of the probability of attack presence instead of one-to-one mapping between the current patterns and those in the database. A disadvantage of the algorithm is its considerable price, as it has (N^2) complexity. As N is the number of the states, i.e. the number of normal user activity patterns in the database, its value could be significant in the case of a large system. Another disadvantage of the anomaly based IDS, in general, is the creation of the database containing the user profiles, which could be a task of considerable difficulty, especially during the ML training.

5. Conclusions and future work. The present paper is an extension of our previous work [10]. It introduces an approach for intrusion detection in anomaly based IDS. Since we considered the attack presence recognition as a decoding problem, we applied the BCJR algorithm combined with a gradient based method. The drawback of this algorithm

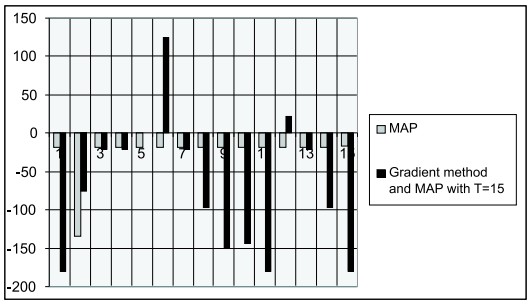

Fig. 4. Comparison between the results of independent BCJR algorithm and BCJR algorithm combined with gradient based method when $T = 15$

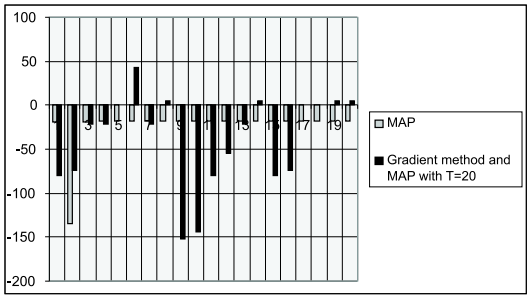

Fig. 5. Comparison between the results of independent BCJR algorithm and BCJR algorithm combined with gradient based method when $T = 20$

is its considerable computational complexity. So, the purpose of some future work directions could be some other probabilistic and decoding methods application in intrusion detection systems.

REFERENCES

[1] L. Bahl, J. Jelinek, J. Raviv, F. Raviv. Optimal Decoding of Linear Codes for minimising symbol error rate. *IEEE Transactions on Information Theory*, **IT-20** (1974), 284–287.

[2] P. Chan, M. Mahoney, M. Arshad. Learning Rules and Clusters for Network Anomaly Detection, Workshop on Statistical and Machine Learning Techniques in Computer Intrusion Detection, George Mason University, Technical Report CS-2003–06, 2003.

[3] S. Chebrolu, A. Abraham, J. P. Thomas. Feature Deduction and Ensemble Design of Intrusion Detection Systems. *Computers & Security*, **24**, (2005), 295–307.

[4] M. Christodoresku, S. Jha. Static Analysis of Executables to Detect Malicious Patterns. In: Proceedings of the 12th USENIX Security Symposium, August 2003, 169–186.

[5] M. Crosbie, G. Spafford. Applying Genetic Programming to Intrusion Detection. *Working Notes for the AAAI Symposium on Genetic Programming*, 1995, 1–8.

[6] S. Forrest, S. A. Hofmeyr, A. Somayaji, T.A. Longtaff. A Sense of Self for Unix Processes. In: Proceedings of the 1996 IEEE Symposium on Security and Privacy, IEEE Computer

Society Press, Los Alamitors, CA, 120–128.
[7] S. Forrest, S. A. Hofmeyr, A. Somayaji. Intrusion Detection Using Sequences of System Calls. *Journal of Computer Security*, **6** (1998) 151–180.
[8] X. D. Hoang, J. Hu, P. Bertok. A Multi-layer Model for Anomaly Intrusion Detection Using Program Sequences of System Calls. 11th IEEE International Conference on Networks (ICON 2003), Sydney, Australia, 2003.
[9] H. Hou, G. Dozier. Immunity-Based Intrusion Detection System Design, Vulnerability Analysis, and GENERTIA's Genetic Arms. In: Symposium on Applied Computing Proceedings of the 2005 ACM symposium on Applied computing, 2005, 952–956.
[10] V. Jecheva, E. Nikolova. About Some Applications of Raviv Algorithm in Anomaly-Based Intrusion Detection Systems. In: Proceedings of the Conference Mathematics, Informatics and Computer Science, V. Tarnovo, 2006, 131–136.
[11] C. C. Michael, A. Ghosh. Simple, State-Based Approaches to Program-Based Anomaly Detection. *ACM Transactions on Information and System Security*, **5** (2002), 203–237.
[12] Y. Qiao, X. W. Xin, Y. Bin, S. Ge. Anomaly intrusion detection method based on HMM. *IEEE Electronic Letters Online* № 20020467, 2002.
[13] L. R. Rabiner. A tutorial on Hidden Markov Models and selected applications in speech recognition. *Proc. IEEE*, **77** (1989), 257–286.
[14] Y. B. Reddy. Genetic Algorithm Approach for Intrusion Detection. In: Proceedings of Modelling, Simulation, and Optimization MSO, 2004, Hawaii, ISBN: 0-88986-424-1, 2004.
[15] R. Sekar, M. Bendre, Dhurjati, P. Bullineni. A Fast Automaton-Based Method for Detecting Anomalous Program Behaviours. In: IEEE Symposium on Security and Privacy, S&P 2001, 144–155.
[16] University of New Mexico's Computer Immune Systems Project, `http://www.cs.unm.edu/~immsec/systemcalls.htm`.

Evgeniya P. Nikolova
Veselina G. Jecheva
Burgas Free University
Faculty for Computer Science and Engineering
62 San Stefano Str.
8001 Burgas
e-mail: enikolova@bfu.bg
vessi@bfu.bg

BCJR АЛГОРИТЪМ, ГРАДИЕНТЕН МЕТОД И ПРИЛОЖЕНИЕТО ИМ В СИСТЕМИ ЗА ОТКРИВАНЕ НА НАРУШЕНИЯ,БАЗИРАНИ НА АНОМАЛИИ

Евгения П. Николова, Веселина Г. Жечева

Скритите Маркови Модели (СММ) са вероятностни модели, приложими за различни разпознавателни проблеми, в частност за откриване на нарушения. Целта е да се определи вероятността за атака в редица от наблюдения върху работата на един компютър. В настоящата работа се представят възможностите на BCJR алгоритъма, основан на логаритмично частно на правдоподобие, за откриване на нарушения базирани на аномалии. Сравнява се неговата работа с работата му върху СММ, чиито параметри са оптимизирани чрез критерия за максимално правдоподобие, основан на градиентен метод.