通信情報保護學會論文誌
第7卷 第4號, 1997. 12

A Tuning of Intrusion Detection Model with Fuzzy Set

Young-Soo Kim*, Woo Hwang**, Sung-Ok Kim***

Abstract

This paper introduces a statistical approach of intrusion detection and tunes an intrusion detection model using fuzzy set. We describe the method of applying fuzzy set for NIDES intensity measure. By using fuzzy set, we improve the algorithm for evaluating score value of NIDES, and present a possibility of intrusion detection system.

1. Introduction

In this age of universal electronic connectivity of viruses and hackers, of electronic eavesdropping and electronic fraud, there is indeed no time at which security does not matter. The explosive growth in computer system and their interconnections via networks have increased the dependence of both organizations and individuals on the information stored and communicated using these systems. This in turn has led to a heightened awareness of the need to protect data and resources from disclosure and to protect systems from network-based attacks[1].

Additionally, a computer system should have confidentiality, integrity and assurance against denial of service. Especially on the internet, the vast spectrum systems are subject to attack by intruders because of increased connectivity. Thus, it is important that the security mechanisms of a system are designed so as to prevent unauthorized access to system resources and data. However, completely the preventing breaches of security appear, at present, unrealistic. We can, however, try to detect these intrusion attempts so that action may be taken to repair the damage later. This field of research is called Intrusion Detection[2].

Generally, intrusion detection techniques can be divided in two main classes[3][4][5][6][7]. The first technique is the anomaly detection technique. It contains statistical approaches,

* Electronics & Telecommunications Research Institute

** Yein Information Corporation

*** Hannam University

feature selection, combining individual measures, predicative pattern generation and neural network method. The second technique is the misuse detection technique. It contains conditional probability, production/expert systems, state transition analysis, keystroke monitoring and model-based intrusion detection[8].

We will discuss NIDES(Next Generation Intrusion Detection Expert System). NIDES developed by SRI is an interesting case study for the expert system approach. NIDES follows a hybrid intrusion detection technique consisting of a misuse detection component as well as an anomaly detection component. The anomaly detector is based on the statistical approach, and it flags events as intrusive if they are largely deviant from the expected behavior. To do this, it builds user profiles based on many different criteria(more than 30 criteria, including CPU and I/O usage, commands used, local network activity, system errors, etc.). These profiles are updated at periodic intervals. The expert system misuse detection component encodes known intrusion scenarios and attack patterns(bugs in old version of sendmail could be one vulnerability). The rule database can be changed for different systems. One advantage of the NIDES approach is that it has a statistical component as well as an expert system component. This means that the chances of one system catching intrusions missed by the other increase. Another advantage is the problem's control reasoning is cleanly separated from the formulation of the solution. We will use fuzzy set into statistical approach for NIDES.

2. NIDES(Next Generation Intrusion Detection Expert System)

The core component of the NIDES prototype are as follows[9];

- Audit-data generation component
- Audit-data collection component
- Statistical component
- Rulebased component
- Resolver component

The graph of the core component is shown in Figure 1. The audit-data generation component generates NIDES-format audit records of subject's activities on a target system from C2 auditing(TCSEC's C2 level) and UNIX accounting files. It is capable of being remotely started, stopped, and monitored.

The audit-data collection component is capable of gathering audit data generated by multiple target hosts as it is generated, provided the amount of audit data being generated is reasonable. This component guarantees that an audit record will be disposed only after it has been processed by the analysis components(statistical, rulebased, and resolver). The statistical component detects masquerading users. The rulebased component detects "well-known" types of intrusive or suspicious user behavior. The resolver component analyzes the alerts issued by the statistical and rulebased components and reports only non-redundant alerts. The security officer's user interface component enables the following.

- Real-time operation of NIDES, including displaying and reporting of alerts, selecting target hosts to be monitored, and reporting status of monitored target hosts.
- Processing of previously recorded audit data using NIDES, including logging of alerts and managing of persistent store information are used by NIDES.

The security officer user interface component depends on the resolver component for obtaining alerts, on the audit-data collection component for obtaining the status of audit-data generation on various target systems and on the audit-data generation component itself for its initiation and termination.

The resolver component depends on the statistical and rulebased components for their respective analysis which, in turn, depend on the audit data collection component for audit-data records. The audit-data collection component obtains audit data from the various audit-data generation components. We will focus on statistical component.

2.1. Description of statistical component

The statistical component observes behavior on a monitored computer system and adaptively learns what is normal for individual subjects: users, groups, remote hosts and the overall system. Observed behavior is flagged as a potential intrusion if it deviates significantly from expected behavior. The NIDES statistical component maintains a statistical subject knowledge base consisting of profiles. A profile is a description of a subject's normal behavior with respect to a set of intrusion-detection measures.

Profiles are designed to require a minimum amount of storage for historical data and yet record sufficient information that can readily be decoded and interpreted during anomaly detection. Rather than storing all historical audit data, the profiles keep only statistics such as frequencies, means and covariances.

The statistical knowledge base is updated daily, using the most recent day's observed behavior of the subjects. Before the new audit data are incorporated into the profiles, the frequency tables in each profile are aged by multiplying them by an exponential decay factor. Although this factor can be set by the security officer, we believe that a value that reduces the contribution of knowledge by a factor of 2 for every 30 day is appropriate. This is the long-term profile half-life. This method of aging has the effect of creating a moving time window for the profile data, so that the expected behavior is influenced most strongly by the most recently observed behavior. Thus, NIDES adaptively learns subjects' behavior patterns; as subjects alter their behavior, their corresponding profiles change.

2.1.1. Score value

For each audit record generated by a user, NIDES generates a single test statistic value that calls the NIDES score value that summarizes the degree of abnormality in the user's behavior in the near past. The score value is denoted T^2.

Large values for T^2 are indicative of

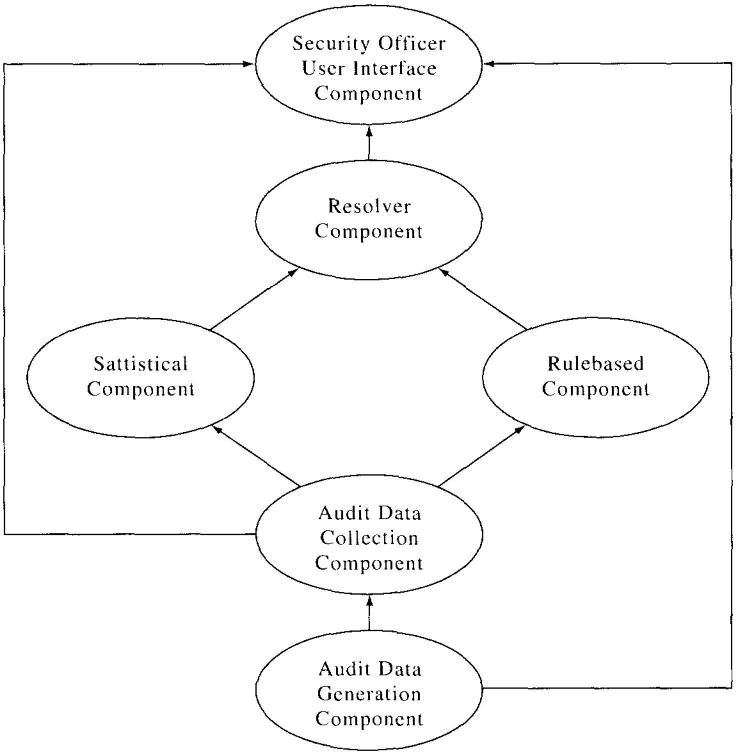

Security Officer User Interface Component
Resolver Component
Sattistical Component
Rulebased Component
Audit Data Collection Component
Audit Data Generation Component

Figure 1. The graph of the core component in NIDES

abnormal behavior, and values closed to zero are indicative of normal behavior. The T^2 statistic summary judgment of the abnormality of many measures taken in aggregate. Suppose that there are n such constituent measures, and let us denote these individual measures by S_i, $1 \leq i \leq n$. Each S_i is a measure of the degree of abnormality of behavior with regard to a specific feature such as CPU usage or file accesses. T^2 statistic has been set equal to the sum of the squares of the S_i:

$$T^2=(S_1^2+S_2^2+S_3^2+.........+S_n^2)/n \tag{1}$$

because the T^2 statistic is an average of the n squares of the S_i. If there is additional useful information contained in the correlations among the S_i, then L^2 statistic is defined as follow:

$$L^2=\frac{2}{n(n-1)}\sum_{i=l}^{n}\sum_{j>l} h(S_i, S_j, C_{ij}) \tag{2}$$

where, $h(S_i, S_j, C_{ij})$ is a well-behaved function of S_i, S_j, and their correlation C_{ij} that takes large values when S_i and S_j are not behaving in accordance with their historical correlations. C_{ij} can be a function value of S_i and S_j. Instantly, C_{ij} is a normal interaction value between S_i and S_j. It is evaluated by historical data.

2.1.2. Classification of individual measure

There are four classes of individual measure in NIDES statistical system.

- Intensity measures: These three measures track the number of audit records that occur in different time intervals, on the order of 1 minute to 1 hour. These measures can detect bursts of activity of prolonged activity that is abnormal, primarily based on the volume of audit data generated.
- Audit record distribution measure
    - Categorical measures
    - Counting measures

Because we will focus on intensity measure, will only use a fuzzy set in it.

2.1.3. Algorithm for computing intensity measure

For each S measure from a corresponding statistic, we will call Q. In fact, each S measure is a 'normalizing' transformation of the Q statistic so that the degree of abnormality for different types of features such as CPU usage and the names of files accessed can be added on a comparable basis. Two different methods for transforming the Q statistics into S values are used.

For the intensity measures, the value of Q corresponding to the current audit record represents the number of audit records that have arrived in the recent past. In addition to knowing the current value for Q, NIDES maintains a historical profile of all previous values for Q. Thus, the current value of Q can be compared to this historical profile to determine whether the current value is anomalous.

The transformation of Q to S for the intensity measures requires knowledge of the historical distribution of Q. For example, we might find the following historical information for the intensity measures Q with a half-life 1 minute:

- 3% of the Q value are in the interval 0 to 20 audit records
- 11% of the Q value are in the interval 21 to 30 audit records
- 21% of the Q value are in the interval 31 to 40 audit records
- 39% of the Q value are in the interval 41 to 60 audit records
- 12% of the Q value are in the interval 61 to 90 audit records
- 10% of the Q value are in the interval 91 to 150 audit records
- 4% of the Q value are in the interval 151 to 240 audit records

The S statistic would be a large positive value whenever the Q statistic was in the interval 0 to 20. The S statistic would be close to zero whenever Q was in the interval 41 to 60. The selection of appropriate intervals for categorizing Q is important to the functioning of the algorithm. NIDES is currently using 32 intervals for each Q measure, with interval spacing being either linear or geometric.

The algorithm for converting individual Q value to S for the intensity measures is as follows;

1) Let P_m denote the relative frequency with which Q belongs to the m-th interval. In

our example, the first interval is 0 to 20 and the corresponding P value(say P_0) equals 3% There are 32 values for P_m, with $0 \leq m \leq 31$. In the above example, $P_0=3\%$, $P_1=11\%$, ...

2) For the m-th interval, let $TPROB_m$ define the sum of P_m and all other P values that are smaller than or equal to P_m in magnitude. It is defined as follow :

$$TPROB_m = \sum_{p \leq p_m} p. \qquad (3)$$

For above example, $TPROB_4=12\%+11\%+10\%+4\%+3\%=40\%$

3) For the m-th interval, let s_m, be the value such that the probability that a normally distributed variable with mean 0 and variance 1 is larger than s_m in absolute value equals $TPROB_m$. The value of s_m satisfies the equation,

$$P(|N(0,\ 1)| \geq s_m) = TPROB_m$$
$$\Leftrightarrow s_m = (\Phi^{-1}(1-(\ TPROB_m/2)) \qquad (4)$$

where $N(0,\ 1)$ is the standard normal distribution, Φ is the cumulative distribution function of a $N(0,\ 1)$ variable. For example, if $TPROB_m$ is 5%, then we set s_m equal to 1.96, and if $TPROB_m$ is equal to 100%, then we set s_m, equal to 0. We do not allow s_m to be larger than 4.0.

$$\text{(i.e., } \Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{\frac{-y^2}{2}} dy)$$

4) Suppose that after processing an audit record we find that the Q value is in the m-th interval. Then S is set equal to s_m, the s value corresponding to $TPROB_m$.

2.1.4. Frequency distribution for Q and Q statistic for intensity measure

It is necessary that the historical frequency distribution for Q is required for Q to be transformed into S. Also, when a user is first audited, that user has no history. Consequently, we must choose some convenient value to begin the Q statistic history. For example, we might initially let each Q measure be zero, or some value close to the mean value for other similar users. Each Q statistic for intensities is updated each time a new audit record is generated.

2.2. Necessity of justifying for intensity measure

In the case of using intensity measure, If Q statistics are distributed uniformly for each interval, (i.e., variance of Q statistics is large value), it is reasonable to using $TPROB$ in above algorithm. Unless a variance of Q statistics is large value (i.e. in the case that Q statistics are gathered around one point), then it is necessary to justify $TPROB$. For example, in the interval of 20 to 40, suppose that Q statistic is distributed around 23 point, if Q statistic of new audit record number is 39, it is unreasonable that this statistic is in the interval of 20 to 40. It had better assign next interval, or it is reasonable to making appropriately weighted value for P_m. Thus, we will introduce algorithm for interval filtering using fuzzy set in the next section[10].

3. Interval filtering using fuzzy set

In the above section 2.1.3, we discussed converting algorithm. For that algorithm, it is possible to apply rule as follows; (Note that variance of Q statistics is small in each interval)

1) For each interval, let C_m is the mean of Q statistic.($0 \le m \le 31$)

2) For each interval, we can define fuzzy sets, F_m={a set of real number close to C_m} and, define a membership function as follows:

$$u_m(x) = \frac{1}{1+(x-C_m)^2} \tag{5}$$

where, $0 \le m \le 31$ and x is Q_m^{new}. Let Q_m^{new} denote a Q statistic of new audit record number in m-th interval. P_m has a weighted value as distance from C_m in m-th interval, or has a value of next(or previous) interval. This function is generally used to represent fuzzy set[10]. So it can be justified by variance of Q statistics.

3) For value of m is maximum, If $u_m(Q_m^{new})$ is greater than 0, then let FP_m is a fuzzy weighted value of P_m, and define as follow :

$$FP_m = u_m(Q_m^{new}) \times P_m. \tag{6}$$

We evaluate value of $TPROB_m$ as follow:

$$TPROB_m = FP_m + \sum_{p<p_m} p. \tag{7}$$

If value of p is minimum, then evaluate $TPROB_m$ as follow:

$$TPROB_m = FP_m. \tag{8}$$

If $u_m(Q_m^{new})$ is equal to 0, evaluate possibility value of Q_m^{new} for C_{m-1}. If its possibility value is equal to 0, then $u_m(Q_m^{new})$ is set to value of minimum grade(denoted $u_m^{min}(Q_m^{new})$) in m-th interval and evaluate FP_m as follow:

$$FP_m = u_m^{min}(Q_m^{new}) \times P_m. \tag{9}$$

Else, in other words, if a possibility value of Q_m^{new} is greater than 0 in the previous interval, evaluate FP_m as follow:

$$FP_m = u_{m-1}(Q_m^{new}) \times P_{m-1}. \tag{10}$$

4) For m is minimum value, If $u_m(Q_m^{new})$ is greater than 0, then let FP_m is a fuzzy weighted value of P_m, and define as follow:

$$FP_m = u_m(Q_m^{new}) \times P_m. \tag{11}$$

Note that we use 0.8 for α-cut value. We evaluate value of $TPROB_m$ as follow:

$$TPROB_m = FP_m + \sum_{p<p_m} p. \tag{12}$$

If value of P is minimum, then evaluate $TPROB_m$ as follow:

$$TPROB_m = FP_m. \tag{13}$$

If $u_m(Q_m^{new})$ is equal to 0, evaluate possibility value of Q_m^{new} for C_{m+1}. If its possibility value is equal to 0, then $u_m(Q_m^{new})$ is set to value of minimum grade(denoted ummin ($u_m(Q_m^{new})$)) in m-th interval and evaluate FP_m as follow:

$$FP_m = u_m^{min}(Q_m^{new}) \times P_m. \tag{14}$$

Else, in other words, if a possibility value of Q_m^{new} is greater than 0 in the next interval, evaluate FP_m as follow:

$$FP_m = u_{m+1}(Q_m^{new}) \times P_{m+1}. \tag{15}$$

5) Otherwise, we set to 0.8 for α-cut value. If a possibility value of Q_m^{new} is greater than 0, as the same way of third step, evaluate value of $TPROB_m$ as follow:

$$TPROB_m=FP_m+\sum_{p<p_m} p. \qquad (16)$$

However, in the case of a possibility value of Q_m^{new} is equal to 0, if Q_m^{new} is less than C_m and $u_{m-1}(Q_m^{new})$ is greater than 0, P_m is set to 0. Hence,

$$TPROB_m=\sum_{p\leq p_{m-1}} P. \qquad (17)$$

If Q_m^{new} is greater than C_m and $u_{m+1}(Q_m^{new})$ is grater than 0, P_m is set to 0. Hence,

$$TPROB_m=\sum_{p\leq p_{m-1}} P. \qquad (18)$$

Otherwise, both $u_m(Q_m^{new})$ and $u_{m+1}(Q_m^{new})$ are equal to 0.

$$FP_m=u_m^{min}(Q_m^{new})\times P_m. \qquad (19)$$

$$TPROB_m=FP_m\times \sum_{p<p_m} P. \qquad (20)$$

4. Experimental result

We verified the interval filtering model using fuzzy set. We suppose the historical distribution of Q as Table 1, and assume that the number of input audit record is random. The input audit record is uniformly distributed. The result of simulation is described in Figure 2. As we shown the Figure 2., the abnormality degree using fuzzy set filtering algorithm is smaller than the abnormality of NIDES's algorithm in 121 to 145 interval. It means that the false-positive rate is reduced. This false-positive rate is rate that normal user is regarded to abnormal user. We know that most normal user has 121 audit record to 145 audit record. If the number of audit record for new user is in 121 to 145, it is generally regarded to normal user. Hence, abnormality of the new user had been to reduce. Also, in the case of small distribution probability, the abnormality degree using set filtering algorithm is larger than the abnormality of NIDES's algorithm. It means that the true-positive is increased. The true-positive means rate that abnormal user is regarded to normal user. We know that most abnormal user has 26 audit record to 40 audit record. If the number of audit record for the new user is in 26 to 145 interval, it is can be regarded to abnormal user. So, abnormality of the new user had been to increase.

Hence, using this way, we find a method of tuning intensity measure of NIDES. For verifying, we used SUN sparc workstation with C.

Table 1. Historical distribution

audit record number	probability
0 - 10	0.03
11 - 25	0.02
26 - 40	0.01
41 - 70	0.13
71 - 90	0.19
91 - 120	0.15
121 - 145	0.26
146 - 168	0.11
169 - 180	0.06
181 - 200	0.04

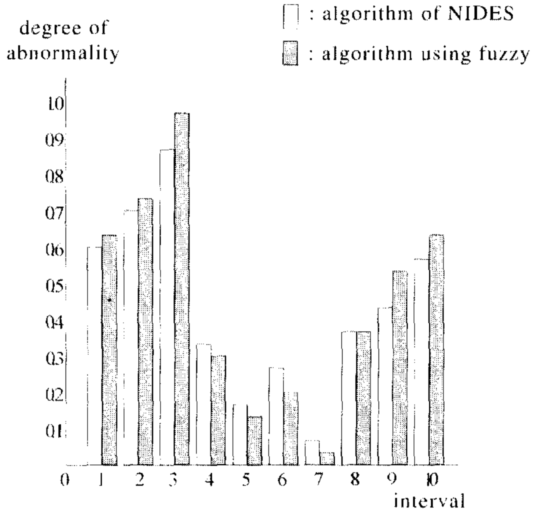


Figure 2. The degree of abnormality

5. Conclusions

We have described the method of statistical approach that interconnected fuzzy set. If NIDES has only a rule-based component, it is difficult that can be detected in case that the abnormal user follows the rule well. Hence, statistical component plays role of detecting abnormal user that follows rule on real time. But, when NIDES have used statistical approach, it had some necessity of justifying intensity measure for statistical component. So, this paper proposed a method of justifying intensity measure of NIDES to improve detecting rate. Using fuzzy set technique will allow us effectively to justify intensity measure of NIDES. Also, this method will also allow us to have the intuitive explanation of detecting intruder, since which is generic feature of fuzzy theory.

In future work, we plan to apply fuzzy set for all measure and will apply fuzzy set for NIDES's core component. In the case of statistical approach, we will research with fuzzy theory and in the case of rule based approach, we will research with hybrid intelligent system. In addition, we will develop the efficient audit trail tool on UNIX. We believe that the importance of intrusion detection system will continue to increase more and more.

References

[1] William Stalling, Network and Internetwork Security. New Jersey: Prentice-Hall, 1995. pp. 207-263.

[2] Aurobindo Sundaram, "An introduction to intrusion detection," Crossroads ACM, pp. 3-7, Apr. 1996.

[3] Dorothy E. Denning, "An intrusion detection model," IEEE Trans. S. E., Feb. 1987.

[4] K. Ilgun, "USTAT: A real-time intrusion detection system for UNIX," in Proc. of IEEE Computer Society Symposium in

Security and Privacy, pp. 16-28, 1993.

[5] Henry S. Teng, Kaihu Chen, and Stephen C. Lu, "Security audit trail analysis using inductively generated predictive rules," in Proc. of the 11th National Conference on Artificial Intelligence Applications, pp. 24-29, IEEE, IEEE Service Center, Piscataway, NJ, Mar. 1990.

[6] Teresa F. Lunt, "A survey of intrusion detection techniques," Computers and Security, pp. 405-418, Dec. 1993.

[7] H. Debra, et al, "A neural network component for an intrusion system," in Proc. of IEEE Computer Society Symposium Research in Security and Privacy, pp. 240-250, 1992.

[8] Tomas D. Garvey and Teresa F. Lunt, "Model-based intrusion detection," in Proc. of the 14th National Computer Security Conference, Washington DC., Oct. 1991.

[9] Teresa F, Lunt and Debra Anderson, Detecting Unusual Program Behavior Using the NIDES Statistical Component. SRI, Dec. 1993.

[10] George J. Klir and Tina A. Folger, Fuzzy sets, uncertainty, and information. New York: Prentice-Hall, 1992. pp. 10-14.

[11] Lotfi Zadeh, The Fuzzy Systems Handbook. New York: Academy Press, 1994. pp. 21-40.

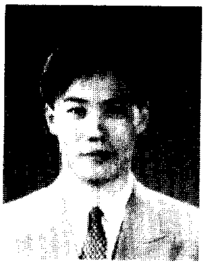
[12] J. R. Winkler, "A UNIX prototype for intrusion and anomaly detection in secure networks," in Proc. of 13th NCSC, Oct. 1990.

[13] Peter J. Denning, Computers under Attack. NY: Addison-Wesely, 1990.

□ 著者紹介

김 영 수

1986년 한남대학교 전자계산공학과(학사)
1990년 한남대학교 수학과(석사)
1986년 ~ 현재 한국전자통신연구원 선임연구원



황 우

1995년 한남대학교 수학과(학사)
1997년 한남대학교 전자계산공학과(석사)
1997년 ~ 현재 예인정보(주) 연구원

김 성 옥

연세대학교 수학과(학사)
University of Minnesota 전자계산학과(석사)
연세대학교 수학과(박사)
한남대학교 컴퓨터공학과 교수