An Attack Detection Method of Industry Control System Based on Multi-dimension Abnormities

Zihua Fan[1, a], Chaowen Chang[1, b], Dongcun Pan[1, c]

[1]Information Engineering University, ZhengZhou, 450000, China

[a]email: fanzihua1993@163.com, [b]email:changchaowen@hnsl.gov.cn, [c]email:pandongcun@163.com

Keywords: Industrial Control System; multi-dimension abnormities; Redundant Relationship; Parallel Relationship

Abstract. The existing attack detection methods cannot extract attack of industrial control system(ICS) correctly. In the view of that, we analyze the characteristics of ICS and proposes an attack detection method of ICS based on multi-dimension abnormities. First of all, we divide hosts into multiple dimensions according to business behavior characteristics of ICS. The multi-dimension abnormities could be used by attack detection method as input. Secondly, we use a hierarchical progress to detect attack because of the different relationships of multi-dimension abnormities. For redundant relationship, we use attribute similar method to extract the abnormal events; For parallel relationship, we use the improved native bayesian to do attack aggregation. Finally, we do a simulation experiment and it shows that our attack detection method has good detection effect.

Introduction

Industry control system is a special type of computer network which is applied in enterprise infor mation system layer. There are a large number of industry control systems in key areas of our count ry and they have became the critical infrastructure, such as distribution automation system of power grid, electricity information collection system, etc.If ICS has been attacked,there will be a huge im pact and bring irreparable damage to the owner , such as the 2010 "Stuxnet" virus caused huge losse s on Iran's nuclear facilities.In recent years, the number of malicious attacks is rising quickly [1] , so the study of ICS security is imminent.

Existing research of ICS security is mainly on anomaly detection and safety assessment. Anomaly detection is the technology which could judge the security states of ICS by testing the abnormal data and user behavior patterns. Anomaly detection mainly included Expert system technology [2], Fuzzy mathematics technology [3] [4], Data mining technology[5] [6], etc. But we couldn’t obtain security status only through anomaly detection. First of all, not all of anomalies are the result of attack, such as misuse of users could cause the response of the anomaly detection. Secondly, there are a large number of abnormities and the administrator can't understand the security status of ICS exactly.

The research of safety assessment include the safety assessment rules and the safety assessment model. Many organizations have released many safety assessment rules such as NIST SP800-82 [7], ANSI/ISA - 99 [8]. The safety evaluation model is primarily concerned on qualitative and quantitative analysis methods. The traditional methods including factor analysis, time sequence model, regression model, the decision tree method, etc[9]. The existing assessment rules and models is based on the existing vulnerabilities of ICS. It is a continuous process to found the vulnerabilities, so the ability to find the attack which use unknown vulnerabilities is very poor.

Existing researches are mainly about anomaly detection and safety assessment. As we all know, the result from anomaly detection could not use by safety assessment and the input used by safety assessment is not effective enough. So there is lack of a middle level research between them. The middle level obtain the safety status or attacks form anomaly detection of ICS and provide it to safety assessment as input. According to the above problems, we put forward an attack detection

method of ICS based on multi-dimension abnormities. According to the characteristics of ICS business behaviors, the hosts are divided into multiple dimensions. The multi-dimension abnormities could be used by attack detection method as input. We use a hierarchical progress to detect attack because of the different relationships of multi-dimension abnormities. For redundant relationship, we use attribute similar method to extract the abnormal events; For parallel relationship, we use the improved native bayesian to do attack aggregation.

Definitions of ICS

ICS is a information system to realize the special missions and has the fixed work behaviors. The operations of ICS can be described by finite state model.Compared with other information systems, the main characteristic of ICS are as follows.

- Composition is clear. The components of ICS is embedded devices which OS is Linux, VXworks or cutting of Linux and VXworks. So we can clearly identify each component in ICS.
- Business process is clear. In ICS, the division of responsibilities and the working characteristics is clear, the business processes is relatively fixed and clear. So ICS can describe the normal working state clearly and find any abnormal working status in the business process easily.
- Communication methods is fixed. ICS using the relatively fixed communication mode and protocol, and ics is also relatively fixed internal communication between each other relations.

The clear business processes of ICS make the description of normal working states much easier. So the abnormal working status could be found easily. Although the attack itself is invisible, the abnormal working status caused by attacks is visible. We embarks from the internal business behaviors of ICS and divide the host into several dimensions according to the internal functions. For each dimension, a complete model of the normal behaviors will be established. Obviously, any operation which does not conform to the normal behavior model will produce abnormal working states of corresponding dimensions. According to the multi-dimension abnormities, the attacks in ICS could be found.

Through the analysis of the existing attack instances in ICS, the observable behaviors caused by the attacks mainly include as follows.

- Illegal flow of business data. It could damage the confidentiality of business data.
- Disorder of business execution. It could cause that the ICS cannot perform its normal business processes.
- Abnormal change of resource using. It could cause the resources occupation and make business execution slowly.
- Unexpected events of users. It leads to the abnormal status which caused by artificial factors.
- Error of network communication. It results in error, delay or halt in data transmission.

Therefore, the dimensions of host included business data dimension, business control dimension, resource use dimension, user activity dimension, network communication dimension. The definition of abnormal states is given below.

Definition 1 Abnormal Signal(AS)

Abnormal signal is a deviation from the normal behavior models. It is also called abnormal states above. It could be showed as AS=(ID, EN_ID, Dimension, Time, Priority, Degree). The fields are defined as follows.

- ID represented a unique identifier of abnormal signal.
- EN_ID is host ID. The abnormal signal is in this host.
- Dimension is the dimension which this abnormal signal belongs to.
- Time represents the time of this abnormal signal.
- Priority represents the attributes of this abnormal signal. We use a vector to store them.
- Degree represents the deviation degree from abnormal signal to normal behavior model. Each attribute in Priority has a deviation degree and we use a vector to store them, too.

By above knowledge, Dimension contains the business data Dimension, business control dimensions, resource use Dimension, user activity dimension and network communication

Dimension. Each dimension corresponds to the different functions, so the Priority have different properties. The Priority for each dimension attribute and deviation calculation method is giving as follows.

- Business data dimension reflect the flow of business data. Stealing business data by attackers will lead to the abnormal flow of data. Attribute vector of data flow dimension is (Name, L1, L2,..., Ln), the Name on behalf of the name of the business data, Li for the position of data flow , L1, L2,...,Ln represent the sequence of positions in data flow progress.
- Business control dimension reflects the order of business process execution. The tampering with the business instruction by attackers could lead to business process abnormities. Attribute vector of business control dimension is (Name, Cl1, Cl2,...,Cln herculean task), the Name for the business Name of the business control, Cli for a single business instruction, Cl1, Cl2,...,Cln for the business instructions sequence of business control.
- Resource use dimension reflects the host resource usage. The instantaneous increase or decrease in resource metrics is the most direct expression when the host is attacked. Attribute vector of resource use dimension is(CPU, ROM), CPU for the host CPU usage, ROM for host memory usage.
- User activity dimension reflects the operations of user are expected or not. The statistics of users will be abnormal when attackers disguise as a normal user and get into ICS. Attribute vector of user activity dimension is (Role, Type, Time), Role for the user's identity, Type for the operation type, Time for the time of the operation.
- Network communication dimension reflects the network communication between hosts is in accordance with the regulation or not. There will be network communication that never be seen or don’t accordance with the regulation. Attribute vector of network communication dimension is (Relate, Type, Time), Relate for the hosts that have communication, Type for the network communication protocol Type, Time for the time of communication.

There are two deviation calculation formulas. Formula(1) is mainly used by business data dimension and business control dimension, m is the number of nodes that can match in the sequence, n is the number of nodes that couldn’t match in the sequence. Formula(2) is mainly used by resource use dimension, user activity dimension and network communication dimension, p_n is the value of attribute in current situations, p_m is the value of attribute in models.

$$de_d = \frac{n}{m+n} \quad (1)$$

$$de_s = \frac{p_n - p_m}{p_n} \quad (2)$$

One step of attack often produce different dimensions of abnormal signals. So there are relationships between abnormal signals. We analyze the attack instance and divide those relationships into two types-- redundant relationship and parallel relationship. The definitions of these two relationship is below.

Definition 2 Redundant Relationship

A simple attack or a step of complex attacks may trigger the same dimension and produce abnormal signals for many times. These abnormal signals are redundant relationship for each other. Port scanning attack, for example, will scan multiple ports of a host for many times. So there will be many abnormal signals that have the same EN_ID and Dimension.

Definition 3 Parallel Relationship

A simple attack or a step of complex attacks may trigger multiple dimensions. These abnormal signals are parallel relationship for each other. Parallel relationship reflects the influence of the attack of different function. So the abnormal signals are independent of each other.

The Main Idea of Attack Detection Method

Any operation that does not conform business processes will produce abnormal signals. These

operations including attacks on ICS, misuse operation, emergency and so on. Therefore we can detect the attacks in ICS based on multi-dimension abnormities and proposes a hierarchical attack detection methods. According to the redundant relationship and parallel relationship the between abnormal signals, the attack detection can be divided into abnormal event extraction and attack aggregation. The attack detection process as shown in figure 1. Abnormal event extraction use attribute similarity to deal with redundancy abnormal signals in the same dimensions on the same host. Abnormal signals turn into abnormal event after abnormal event extraction. Attack aggregation use improved native bayesian method to deal with parallel abnormal signals in different dimensions. We can get the attacks form abnormal events in ICS after attack aggregation.

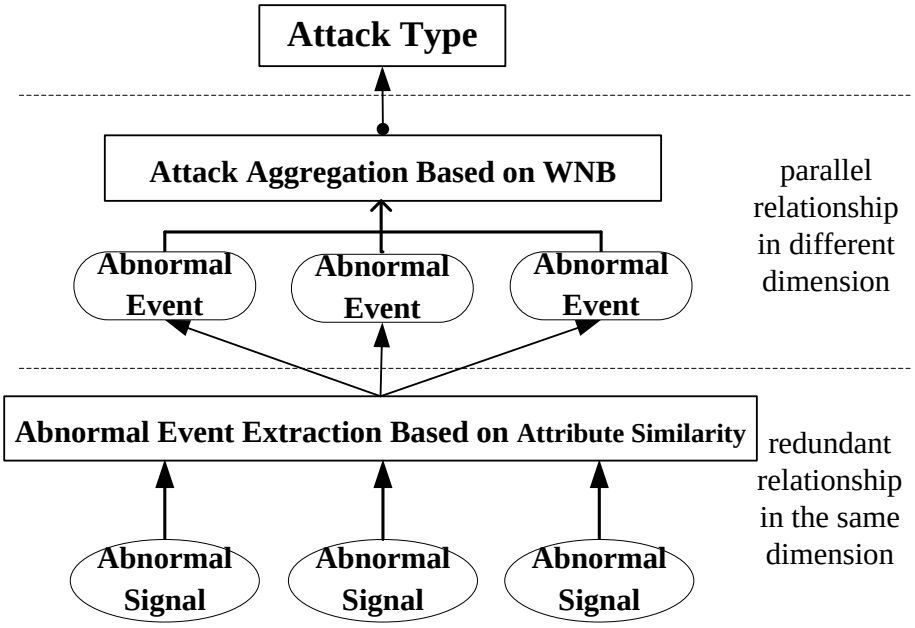

Fig.1. The attack detection process of ICS

Abnormal Event Extraction for Redundant Relationship Based on Attribute Similarity

The methods and successful rate of attackers make attackers repeatedly attack for one step and produce multiple abnormal signals in the same dimension. These abnormal signals are redundant relationship between each other and have the same meaning for attack detection. But these abnormal signals rise the number to deal with. The first thing we should do is to merge with redundant relationship of abnormal signals.

The properties of redundant abnormal signals are the same or similar because of the way they were produced. For example, constant properties such as EN_ID, Dimension must be the same. Variable properties such as Time, Degree must be similar. So redundant relationships could be determined according to the similarity between abnormal signal properties. We could reduce the number of abnormal signals by merge multiple redundant signals into a record. In this paper, these records called abnormal events. Abnormal event is defined as follows.

Definition 4 Anomaly Event(ANE)

Abnormal events is a record merged from redundant abnormal signals of the same dimension in the same host. It could showed as ANE=(ID, E_Tml_ID, E_Dimension, Start_Time, End_Time, E_Priority, Degree). The meaning of each field is showed as followed.

- ID is a unique identifier for the abnormal event.
- E_EN_ID is host ID. It is the same host between abnormal event and abnormal signals.
- E_Dimension is the dimension which this abnormal event belongs to.
- Start_Time represents the time of first signal in all abnormal signals.
- End_Time represents the time of last signal in all abnormal signals.
- E_Priority represents the attributes of this abnormal event. We use a vector to store them. The vectors are the same between abnormal event and abnormal signals.

Degree represents the deviation degree from abnormal event to normal behavior model. It could be calculated by the Degree of abnormal signals.

1. Calculation Method of Abnormal Signal Attribute Similarity

Because the redundant abnormal signals have similar attributes, abnormal events could be extracted from abnormal signals in the same dimension. The formula to calculate one attribute is be different with the others. But the results of all formulas are the interval [0, 1] for a value, the greater value means the more similar two abnormal signals attribute are. 0 represents a completely different, 1 represents exactly the same. The signal similarity could be calculated from the properties similarities. Two abnormal signals will be redundant if the signal similarity is big enough. Then we could merge all the redundant abnormal signals into abnormal event.

According to different types of abnormal signal properties, properties can be divided into three kinds, numerical type, enumeration type and sequence type. The attributes similarity calculation method is given as followed.

(1)Formula of numeric attribute similarity

Numeric attribute is a attribute that shows as a numeric value, including integer, decimal, percent, and so on. For example, the attributes of resource use dimension are CPU and ROM which use percentage to show the utilization. These attributes are typical numerical attributes. Numeric attribute similarity is calculated by the following formula.

$$Sim = \begin{cases} \dfrac{\lambda - |C_1 - C_2|}{\lambda} & |C_1 - C_2| \le \lambda \\ 0 & |C_1 - C_2| > \lambda \end{cases} \tag{3}$$

In the formula, C_1 and C_2 are the value of the same attribute in two abnormal signals. λ is similarity threshold which is depended on the type of attribute and set by the administrator,Sim is the result of attribute similarity. It is the interval [0, 1] for a value.

(2)Formula of enumeration attribute similarity

Enumeration attribute is a attribute that shows as an element of a collection of the name. For example, the attributes of user activity dimension is Role which uses names to behalf a user. It is the same user only when Role is the completely same. So Role is a typical enumeration attribute. For two abnormal signals, if they have the corresponding enumeration type attribute redundancy relationship is must have the same value. If the value is different, the two abnormal signals will not belong to the same abnormal event. Enumeration attribute similarity is calculated by the following formula.

$$Sim = \begin{cases} 1 & AN_1.att = AN_2.att \\ 0 & AN_1.att \neq AN_2.att \end{cases} \tag{4}$$

In formula, AN_1 and AN_2 represent two abnormal signals of the same dimension. Att on behalf of the abnormal signal of enumeration type attribute. Sim is the result of attribute similarity. Sim only have two values 0 and 1. It is 1 when names are the same. It is 0 when names are not the same.

(3)Formula of sequence attribute similarity

Sequence attribute is a attribute that shows as a sequence. For example, the control flow sequence of business control dimension is a typical sequence attribute. The calculation of sequence attribute similarity is depended on corresponding enumeration attributes of abnormal signal. It is meaningless to discuss the sequences similarity of two different names. Abnormal signals belong to the same abnormal event only when the name is the same. Sequence attribute similarity is calculated by the following formula.

$$Sim = \begin{cases} \dfrac{C_1 - C_2}{C_1} & AN_1.att = AN_2.att \\ 0 & else \end{cases} \tag{5}$$

In formula, AN_1 and AN_2 represent two abnormal signals of the same dimension. Sim is the result of attribute similarity. It is 0 when names are not the same. C_1 is the number of nodes in the sequence. C_2 is the number of nodes that can not match. Sim is a value of interval [0, 1].

2. Abnormal Event Extraction

According to the attribute similarity in section 4.2 and time threshold in section 4.3, we can determine that abnormal signals are redundant or not. ASi and ASj are two abnormal signals in the same dimension. The similarity between ASi and ASj can be calculated by the following formula.

$$Sim(i, j) = \frac{\sum_{k=1}^{m} w_k \times Sim_{ij}^{k}}{\sum_{k=1}^{m} w_k} \quad (6)$$

m is the number of abnormal signal properties. K is any attribute in properties. Simijk is the attribute similarity of K. Wk is the weights of K in all the attributes.

If ASi and ASj belong to the same event, they have characteristics as followed.

ASi. EN_ID = ASj. EN_ID and ASi. Dimension = ASj. Dimension;

The attribute similarity of abnormal signals is big enough.Sim(i,j)$\geqslant\lambda$, λ is the threshold of attribute similarity.

The abnormal signals that can meet the above conditions belong to the same abnormal event. So we can deal with the redundant abnormal signals by merging them into abnormal events.

Attack Aggregation for Parallel Relationship Based on Improved Native Bayesian

1.The Introduction of Native Bayesian

Naive Bayesian is a practical mathematical model for classification. It has the advantages of simple and efficiency. Naive Bayesian could be used in most cases and has perfect classification accuracy.

Before using Naive Bayesian, the attributes should be independent of each other and contribute to the result independent. Calculating the possibility of each classification, and then view the like for categorical data in classification of X. Because of the properties independent of each other, can be calculated for the possibility of classification data X in each category, the most likely class is the class which has the highest probability.

Due to the characteristics of independent, the conditional probability P (X|C_1) of categorical data X can be calculated by the following formula:

$$P(X \mid C_1) = P(X_1 \mid C_1) * P(X_2 \mid C_1) * P(X_3 \mid C_1) * \cdots * P(X_n \mid C_1) \quad (7)$$

According this, we could calculate P(C_1|X) by the following formula. In the formula, C_1 is a class and X is categorical data. P(C_1|X) means the probability of class C1 when we have data X.

$$P(Y = c_k \mid X = x) = \frac{P(X = x \mid Y = c_k)P(Y = c_k)}{\sum_k P(X = x \mid Y = c_k)P(Y = c_k)} = \frac{P(Y = c_k)\prod_j P(X^{(j)} = x_j \mid Y = c_k)}{\sum_k P(Y = c_k)\prod_j P(X^{(j)} = x_j \mid Y = c_k)} \quad (8)$$

2.The Attack Aggregation Based on Improved Native Bayesian

Although the vulnerabilities used by attackers are uncertain, the attack models are determined. Despite the vulnerabilities, the attacks of the same models influence the fixed dimensions and produce abnormal signals. At this point, although we don't know what vulnerabilities in ICS, we can obtain the attacks through multi-dimension abnormal signals. According to the abnormal events, we propose a improved Naive Bayesian method to detect attacks in ICS. We use Naive Bayesian because of the following advantages.

the determination of dimensions is based on the function of host. The attack influence of each dimension is independent. So the dimensions are independent among each other. This characteristic could meet the strict requirements of using Naive Bayesian.

Naive bayes method is simple in logic and the time complexity is low. We can meet the real-time or efficiency requirements of ICS.

The input of attack aggregation is a sequence of abnormal events G = (ANE_1, ANE_2,..., ANE_n). The output of attack aggregation is a attack SSF. According to the formula of Native Bayesian, each attack model can correspond a classify C_i. A grouping as staying with the X in the Naive Bayesian

classification data corresponding to each exception events is an attribute, property between independent each other. For each classification probability of C_i, it can be given with the expert knowledge. $P(X|C_i)$ can be obtained by history data.

In the traditional Naive Bayesian, each condition attributes contribute to the classification results equally. As shown in formula, there is no parameter can reflect important degree of each condition attribute. In ICS, the abnormal events with different deviation degree obviously have different impact on the classification results. According to the above problem, we join a deviation factor in the process of attack aggregation and put forward an improved Naive Bayesian method to detect attacks in ICS. The computation formula is as follows:

$$C_i(x) = P(C_i)\prod_{i=1}^{n} P(x_j \mid C_i)^{\alpha j} \tag{9}$$

The α_j is the weight of abnormal event x_j. Because the range of α_j and the deviation degree are [0, 1], we use the deviation degree of abnormal event to represent the weight of abnormal event. $C_i(X)$ is the attack model in the condition of the sequence of abnormal events. We can compute all the $C_i(X)$ for every attack model. In the condition of the sequence of abnormal events, It is attack model that has the highest value in all $C_i(X)$. Attack aggregation process description is as follows:

Input：G=(ANE_1, ANE_2, …, ANE_n)
Output：Attack Type
TrainParameter{
For each $c_i \in C$ //C is the classes set and ci is a class in set
Nc←CountEventsInClass(c_i) // Count the number of events in ci
prior[c_i][C]←Nc/N // N is the total number of all events
for each $t \in V$ // V is the events set of train data
Tct←CountEventsOfTerm(t) // Count the number of event t in ci
condprob[t][c_i][α_j] //Calculate P(t|c) with the weight
return V,prior,condprob}
ApplyMultiNomialNB(C,V,prior,condprob) {
for each $c_i \in C$
score[c_i][C]←prior[c_i][C]
for each $t \in G$
score[c_i][C] *= condprob[t][c][α_j]
SSF= max(score[c_i][C]) //SSF is the attack type to which G belongs
return SSF
}

Test Results

In order to test the attack detection method in our paper, we do an experiment with the data set LLDOS1.0 provided by DARPA. LLDOS1.0 is a data set contains a variety of attacks. These attacks form a a complete sequence. The sequence of LLDOS1.0 contains the following:(1) Detect activity hosts through the IPSweep;(2)Detect the hosts which have loopholes sadmind through scaning sadmind daemon service port ;(3)Get root of three hosts by invading the hosts through sadmind loopholes;(4)Install DDoS attacks software in these hosts;(5)Start attacks using the accused hosts.

For LLDOS1.0, we could regard alerts as abnormal signals. At first, we process the redundancy relationship and merge them into abnormal events through the attribute similarity. Then we process the parallel relationship and aggregate them into attack type. In the experiment, IP address of the external host is 202. 77. 162. 213; IP addresses of the three accused hosts are respectively 172. 16. 115. 20, 172. 16. 112. 50, 172. 16. 112. 10; IP addresses of the target hosts is 131. 84. 1.31. The results of experiment is attack types and it is shown in the table below.

Table.1 Record of Attack Type

	Target Address	Attack Type	Attack
Phrase1	172. 16. 112. 0/24	IP_SWEEP	ICMP_PING_SWEEP
Phrase1	172. 16. 113. 0/24	IP_SWEEP	ICMP_PING_SWEEP
Phrase1	172. 16. 114. 0/24	IP_SWEEP	ICMP_PING_SWEEP
Phrase1	172. 16. 115. 0/24	IP_SWEEP	ICMP_PING_SWEEP
Phrase2	172. 16. 112. 0/24	PORT_SCAN	SADMIND_PORT_REQUEST
Phrase2	172. 16. 113. 0/24	PORT_SCAN	SADMIND_PORT_REQUEST
Phrase2	172. 16. 114. 0/24	PORT_SCAN	SADMIND_PORT_REQUEST
Phrase2	172. 16. 115. 0/24	PORT_SCAN	SADMIND_PORT_REQUEST
Phrase2	172. 16. 112. 10	PORT_SCAN	SADMIND_PORT_CONNECT
Phrase2	172. 16. 112. 50	PORT_SCAN	SADMIND_PORT_CONNECT
Phrase2	172. 16. 115. 20	PORT_SCAN	SADMIND_PORT_CONNECT
Phrase3	172. 16. 112. 10	REMOTE_OVERFOLW_ATTEMP	SADMIND_OVERFLOW_ATTEMP
Phrase3	172. 16. 112. 50	REMOTE_OVERFOLW_ATTEMP	SADMIND_OVERFLOW_ATTEMP
Phrase3	172. 16. 115. 20	REMOTE_OVERFOLW_ATTEMP	SADMIND_OVERFLOW_ATTEMP
Phrase4	172. 16. 112. 10	REMOTE_LOGIN	RSH_LOGIN
Phrase4	172. 16. 112. 50	REMOTE_LOGIN	RSH_LOGIN
Phrase4	172. 16. 115. 20	REMOTE_LOGIN	RSH_LOGIN
Phrase5	131.84.1.31	DDOS	DDOS

In the table, Attack Type is the results aggregated from LLDOS1.0; Attack is the corresponding attacks in LLDOS1.0. Through the table above, it is shown that our method can identify attack type and make a perfect preparation for safety assessment of ICS.

Conclusion

The existing Security of ICS is based on vulnerabilities and could detect unknown attacks that use unknown vulnerabilities. Aiming at these shortcoming, we divide host into multiple dimensions according to the characteristics of ICS and detect attacks based on multi-dimensional abnormities. According to the relationships between abnormities, the detection process is divided into two phases -- abnormal event extraction and attack detection-- and using attribute similarity and improved Naive Bayesian method respectively. The Experiment results show that this method has good detection efficiency. In the next step, we will use the attack types which are the results of our method to evaluate the safety of ICS.

Acknowledgement

In this paper, the research was sponsored by the Nature Science Foundation of China (Project No. 61572517).

References

[1] Cheminod M, Durante L, Valenzano A. Review of Security Issues in Industrial Networks[J]. IEEE Transactions on Industrial Informatics,2013, 9(1): 277-293.

[2] Anderson D, Frivold T, Valdes A. Next-generation intrusion detection expert system (NIDES): A Summary. Technical Report SRI-CSL-95-07, Computer Science Laboratory, SRI International, May 1995.

[3] Dickerson J E, Dickerson J A. Fuzzy network profiling for intrusion detection [C].In

Proceedings of Fuzzy Information Processing Society, 2000.

[4] Dickerson J E, Juslin J, et al. Fuzzy intrusion detection [C]. Proceedings of IFSA World Congress and 20th NAFIPS International Conference, Vancouver, British Columbia, 2001:1506-1510.

[5]LIAN YI-feng, DAI Ying-Xia & Wang Hang. (2002). Anomaly Detection of User Behaviors Based on Profile Mining. CHINESE J.COMPUTERS, 25(3), 325-330.

[6]Xiao xiao. (2009). Research and Application of Intrusion Detection Systems Based on Data Mining.(Doctoral dissertation, Jiangnan University).

[7]Stouffer, K., Falco, J., & Scarfone, K. (2008). Guide to industrial controlsystems (ICS) security. NIST Special Publication, 800, 82.

[8]Wang, Y. (2012). sSCADA: Securing SCADA infrastructurecommunications.arXiv preprint arXiv:1207.5434.

[9]Saaty, T. L., & Vargas, L. G. (2012). Models, methods, concepts &applications of the analytic hierarchy process (Vol. 175). Springer.

[10]Kizza, J. M. (2013). Security Assessment, Analysis, and Assurance. InGuide to Computer Network Security (pp. 145-168). Springer London.