An Industrial Control System Situation Awareness Method based on Weighting Algorithm

Hui Shi [a], Xiangyun Tu [b], Zhenhua Wang [c]
China aerospace science and technology research institute Beijing, China
[a] shiyunyin1017@gmail.com, [b] tuxiangyunbj@163.com, [c] 603109545@qq.com

Abstract. This article introduces a brand-new posture perception approach towards the industrial control system to improve the capability of its related network security monitoring. Took full account of the combination issue of multi-source heterogeneous information to accurately reflect the network security situation by extracting its characteristic information that aims to industrial control environment features. Leveraged factor weighting algorithm to extract the intrusion information flow and detect the correlation so that can achieve the prediction and perception of security situation. the final simulation result showed that the calculation approach has higher effective & real-time applied value with lower complexity.

Keywords: network security, situation awareness, industrial control, weighted algorithm.

1. Introduction

With the acceleration of industrialization process, more and more computer and network communication technologies are applied to industrial and manufacturing system [1]. The application of industrial Ethernet can not only reduce cost, but also realize system integration, facilitate information sharing and management. Because of the operation of industrial Ethernet control system, the data communication between field equipment, field monitor, database server, Web server and remote monitoring host is indispensable. In each of the data communication link can there be invaded by unauthorized users. In particular, the data communication between the remote monitoring host through the Internet and the field control system will face the severe test of network security [2-3].

2. Analysis of Industrial Network Security Situation

It is well known that a complete industrial control system can be divided into three levels, namely information management, process monitoring layer and field equipment layer from top to bottom [4].

Industrial Ethernet has become the consensus of the industry with its advantages such as low cost, high bandwidth, easy connection, easy management and so on. Industrial Ethernet has many advantages and also brings many safety problems to industrial control network. Some of these problems are caused by the defects of industrial Ethernet itself (such as the limitations of the CSMA/CD mechanism itself), and some are caused by malicious attacks [4].

Generally speaking, the type of attack in industrial system can be divided into three categories according to the industrial network deployment level:

2.1 Monitor Network Attacks

For example, tamper with data group and destroy its integrity.

2.2 System Attacks

By injecting illegal command damage field devices, or in violation of the bus protocol data packet format definition, such as tamper with the some of the parameters, make its beyond the scope and form attack.

2.3 Process Attacks

Command is in conformity with the protocol specification, but has violated the production logic process of industrial control system, the system is in a state of dangerous (such as the reaction kettle feeding valve and a discharge valve cannot open at the same time) [5-6].

Generally speaking, the security measures for industrial control network system mainly include traditional active defense solutions. However, traditional methods can not perform well in the case of high real time and the limited resources.

Therefore, in recent years, industrial network traffic anomaly detection is a research focus in this field.The traditional intrusion detection method has the problem of large granularity and incompatible protocol type in the process of traffic filtering and monitoring. Moreover, due to the particularity of industrial environment, traditional methods cannot protect the middleman or insider attacks[7]. Therefore, it is necessary to develop an intrusion detection technology based on industrial control system, which takes into account industrial control protocol and industrial control environment,instead of using traditional intrusion detection techniques directly.

3. An Industrial Control System Situation Awareness Method based on Weighted Algorithm

In this paper, an industrial control system intrusion detection method based on weighted algorithm is proposed. In order to realize the network situation awareness, the proposed algorithm is designed by means of signal processing [8]. Because the network security situation data is a set of wide and stable Gaussian linear time signal model. In the industrial control system environment [9], the characteristic distribution of virus invasion information flow on the m terminal is:

$$\begin{aligned} &x(k)=[x_1(k),x_2(k),...,x_m(k)] \\ &i=1,2,...,m \end{aligned} \tag{1}$$

k represents the attribute value of network security posture distribution, $x_i(k)$ represents the attribute value of network security posture distribution. Assuming that the $(x_1,x_2,...x_n)$ dimensional random distribution variable is n, its eigenstate distribution function is:

$$\begin{cases} v_s=\left\| X_s-\sum_{i=1}^{n}\omega_i X_i \right\| \\ \omega_i=\dfrac{\dfrac{1}{\dfrac{v_s}{\sum_{j=1}^{n}v_j}+\lambda}}{\sum_{j=1}^{n}\dfrac{v_s}{\sum_{j=1}^{n}v_j}+\lambda} \end{cases} \\ s=1,...,n \tag{2}$$

Which v_s represents the variation behavior of the network data acquisition data during the invasion., the deviations of x_i and r_t indicate the difference between the output data of the system under attack and the output data when the attack is not received.

We assume that the state model of the intrusion model when an attacker attacks an industrial network is: $V=\{V_1,V_2,...,V_n\}$ and the conditional transfer probability of network threat security situation is expressed as [10]:

$$L = C - m\sum_{s=1}^{n}\log(\sigma_s) - \sum_{s=1}^{n}\sum_{t=1}^{m}\frac{(x_{st} - r_t)^2}{2\sigma_s^2} \tag{3}$$

Which C stands for constant, σ_s represents the random state vector, $a_{i,j}$ represents the probability of distribution, then we get the discrete signal of the attack model x, the signal sampling sequence length is N. The steady-state probability is:

$$\sigma_s^2 = \frac{1}{m}\sum_{i=1}^{m}(x_{st} - r_t)^2 \tag{4}$$

Here we take the average trust weight, and set the weight attribute according to the empirical value [11]:

$$\phi(\omega_1, \omega_2, ..., \omega_n) = E\left\{\exp\left[j(\omega_1 x_1 + \omega_2 x_2 + ...\omega_n x_n)\right]\right\} \tag{5}$$

The characteristic amplitude and frequency of the attacker can be expressed as:

$$m_k = E[x_k] = \int_{-\infty}^{+\infty} x_k f(x)dx \tag{6}$$

$$\mu_k = E[(x-\eta)^k] = \int_{-\infty}^{+\infty}(x-\eta)^k f(x)dx \tag{7}$$

At the same time, we construct an intrusion immune control model, which is distributed in s domain and z domain. In the time domain, we reconstruct the intrusion characteristics of the attacker, and we get the iterative function according to the nonlinear characteristics:

$$\theta_1(k+1) = \theta_1(k) - \mu\,\mathrm{Re}[y(k)\varphi^*(k)] \tag{8}$$

Which $\theta_1(k)$ represents the initial state vector after the system is attacked, when the attacker's attack dimension is M, the proposed model is intercepted in the form of $\theta_0, \theta_1, ..., \theta_p$, thus forming an intrusion detection model in the industrial network environment.

It is well known that in the process of industrial control network security situation, there are many complex observation indexes of mutual conflict and uncertainty [12]. Some indicators play an important role in the situation awareness, while some indicators have little effect on it, and there may be redundancy between indicators [13].

Therefore, it is necessary to select some representative indicators and eliminate the redundancy so as to obtain the factors for network security situation awareness. Here we introduce the concept of "mutual information" in information theory, which is used to represent the interrelationship between information. Mutual information is suitable for measuring the interdependence between two random variables. When two random variables depend on each other, the value of "mutual information" is large; conversely, the value of "mutual information" is small. Therefore, the "mutual information" value can be used to select the observation indexes and eliminate the redundant indicators.

We define the mutual information of two event X and Y as: $I(X,Y) = H(X) + H(Y) - H(X,Y)$, which $H(X,Y)$ means joint entropy:

$$
\begin{aligned}
& I(X,Y) \\
& = H(X) - H(X \mid Y) \\
& = H(X) + H(Y) - H(X,Y) \\
& = \sum_x p(x) lb \frac{1}{p(x)} + \sum_x p(y) lb \frac{1}{p(y)} + \sum_{x,y} p(x,y) lb \frac{1}{p(x,y)} \\
& = \sum_{x,y} p(x,y) lb \frac{p(x,y)}{p(x)p(y)}
\end{aligned} \tag{9}
$$

Which $p(x)$ represents the probability of x, $p(x,y)$ represents the joint probability of event x and y.We can discretize the continuous observations into five equal values, and the values are "2, 1, 0, -1, -2". Monitoring a number of data for a period of time to approximate their probability of occurrence, and to compute the mutual information of two random variables in $I(X,Y)$. If their mutual information value is greater than a specified threshold, they are considered to be highly correlated and redundant.

In accordance with the above methods, we get the “CPU utilization, memory usage, average survival time of key device in the network, the network traffic rate, network data flow amount, network packets in different size distribution, network number for key equipment, network MTBF” as the factors constitute the basis of industrial control system running; we get the “number of network vulnerabilities and levels, system configuration, protection software is installed, key equipment, number of holes and grades, subnet’s safety equipment, each key equipment in the subnet open port number” as the factors of industrial control system vulnerability; we get the “alarm number, DDoS, worm attacks, number of trojans and common virus, network bandwidth utilization, network data flow, the net inflow of growth” as the factors to constitute the threat of industrial control system.

4. Using the Template

In order to verify the rationality and correctness of the network security situation awareness method proposed in this paper, this chapter carries out the MATLAB simulation experiment. The experimental data came from: part of the data is real-time data monitored on each component of the industrial control system, and the other part comes from the observation data in the Snort intrusion detection system. At the same time, the data of all kinds of malicious network traffic are injected into normal flow to obtain the abnormal data needed in the experiment.

In this paper, "Blade IDS Informer" is adopted to set the speed of attack type, frequency and attack, and we use "Solar Winds Engineers Tool" to do network test as shown in Fig. 1:

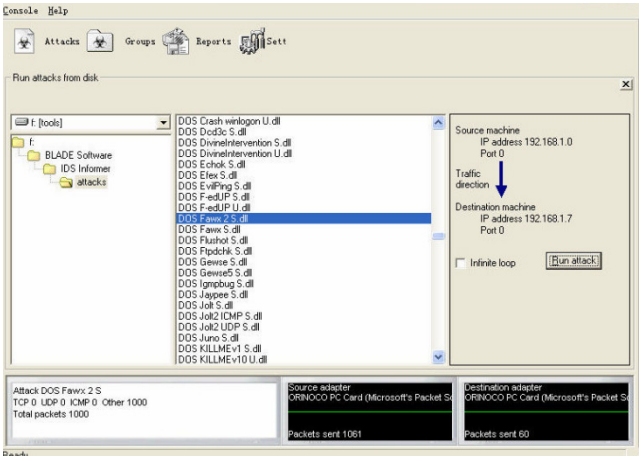

Fig.1 sends the test attack package

Set the sampling time for 5 seconds and collect 2000 samples dynamically as the historical data of the dispersion, taking the factor: "CPU utilization, memory, attack frequency" as an example. As shown in Fig. 2 and Fig. 3, it is a sampling data of a master system which had installed common antivirus software, then the above abnormal data is injected into the experimental data.

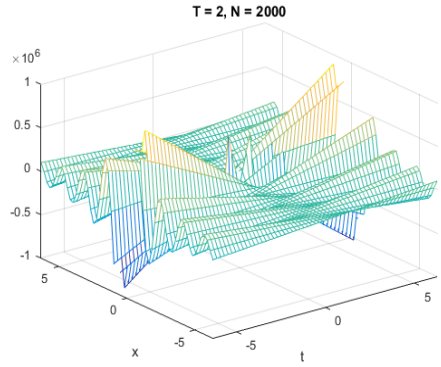

Fig.2 Sampling data of three factors (CPU utilization)

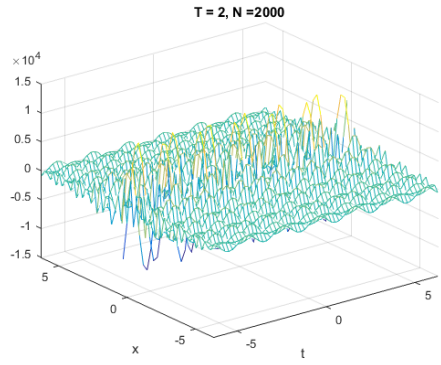

Fig.3 Sampling data of three factors (memory)

After the fusion of multiple weighted function data, the network security situation perception diagram shown in Fig. 4 is drawn, which reflects the security situation in this time period as shown in the Fig.4:

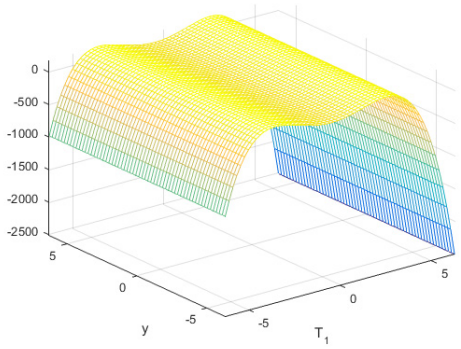

Fig.4 Security situation during attack test period

5. Conclusion

The research of situation awareness technology of industrial control system is a rapidly developing field, although some results have been achieved, but with the escalation of the attack, new challenges have emerged. Currently common intrusion detection techniques are still limited in industrial networks. For example, some process attacks cannot be effectively detected, and in the future, variant attacks can be more deceptive.This paper makes an in-depth study on attack process and attack

detection technology because of the problems of traditional industrial control system intrusion detection technology. An intrusion detection model is established, and we have selected the model factors that accord with the industrial production condition,then according to the actual circumstance of industrial network weighted algorithm is proposed based on the factor of industrial control system method of situation awareness. After experimental verification, the proposed method can effectively identify the different types of attacks, achieve the purpose of situation awareness, this method is a small amount of calculation, high accuracy and has great application value.

Acknowledgments

The authors acknowledge generous support from my team for laboratory space, materials, and training, all of which were integral to the completion of this project. I shall extend my thanks to Dr. Zhen Hua Wang for all his kindness and help.

References

[1]. BASS T. Multi-sensor data fusion for next generation distributed intrusion detection systems//Proceedings of the 1999 IRIS National Symposium on Sensor and Data Fusion. Baltimore: Johns Hopkins University Press, 1999:24-27.

[2]. DIGIOIA G, FOGLIETTA C, OLIVA G, et al. Aware online inter dependency modelling via evidence theory[J]. International Journal of Critical Infrastructures, 2013, 9(1/2):74-92.

[3]. LIU X, WANG H, YU H, et al. Quantitative awareness of network security situation based on fusion[J]. Journal of Jilin University: Engineering and Technology Edition, 2013, 43(6):1650-1657.

[4]. HUANGC, TSENG T, FAN Y, et al. Alternative rule induction methods based on incremental object using rough set theory[J]. Applied Soft Computing, 2013, 13(1):372-389.

[5]. BAZANJG, BAZAN-SOCHA S, BUREGWA-CZUMA S, et al Classifiers based on data sets and domain knowledge: a rough set approach[J]. Intelligent Systems Reference Library, 2013, 43(2):93-136.

[6]. LIU B, GAO L. Method of disease diagnosing based on SVM and rough set[J]. Advanced Materials Research, 2013(605/606/607): 887-890.

[7]. WANG H, GONG Z. Algorithm based on entropy for finding critical traffic matrices [J]. Journal of Software, 2009, 20(5):1377-1383.

[8]. ZHUO Y, ZHANG Q, GONG Z. Research and implementation of network transmission situation awareness[C]//Proceedings of the 2009 WRI World Congress on Computer Science and Information Engineering. Piscataway: IEEE, 2009:210-214.

[9]. WEI Y, LIAN Y, FENG D, et al. A network security situational awareness model based on information fusion[J]. Journal of Computer Research and Development, 2009, 46(3):353.

[10]. CHEN X, ZHENG Q, GUAN X, et al. Quantitative hierarchical threat evaluation model for network security [J]. Journal of Software, 2006, 17(4):885-897.

[11]. WANG C, FANG L, WANG D, et al. Network security situation awareness system based on knowledge discovery [J]. Computer Science, 2012, 39(7):11-24.

[12]. XIE L, WANG Y, YU J. Network security situation awareness based on neural networks[J]. Journal of Tsinghua University: Science and Technology, 2013, 53(12):1750-1760.

[13]. LIU Y, FENG D, LIAN Y, et al. Network situation prediction method based on spatial-time dimension analysis[J]. Journal of Computer Research and Development, 2014, 51(8):1681-1694.