Anomaly Detection Approach based on Function Code Traffic by Using CUSUM Algorithm

Ming Wan[a]*, Wenli Shang[b], Peng Zeng[c]

Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang, China

Key Laboratory of Networked Control System, Chinese Academy of Sciences, Shenyang, China

[a] wanming@sia.cn, [b] shangwl@sia.cn, [c]zp@sia.cn

Keywords: Anomaly detection; Modbus/TCP; Function code traffic; Cumulative sum;

Abstract. There is an increasing consensus that it is necessary to resolve the security issues in today's industrial control system. From this point, this paper proposes an anomaly detection approach based on function code traffic to detect abnormal Modbus/TCP communication behaviors efficiently. Furthermore, this approach analyzes the Modbus/TCP communication packets in depth, and obtains the function code in each packet. According to the function code traffic change, this approach uses the Cumulative Sum (CUSUM) algorithm for change point detection, and generates an alarm. Our simulation results show that, the proposed approach is very available and effective to provide the security for industrial control system. Besides, we also discuss some advantages and drawbacks when using this approach.

Introduction

Nowadays, industrial control system has become an important part in many critical infrastructures, for example power, water, oil, gas, transportation, et al. With the development of modern networking, computing and control technologies, the deep integration of industrialization and informationization has been regarded as the inevitable tendency by both academia and industry. Especially, the "Industry 4.0" revolution, defined by Germany, further emphasizes the essential role of the networking technology [1]. However, the incoming networking technology has broken the original closure in industrial control system, and has brought some security problems into industrial control system [2]. Although there are various kinds of security methods in regular IT system, the traditional security methods cannot be applied directly to networked control system [3].

There are two general approaches for improving the security in industrial control system. One is the communication control or access control approach, and its typical application is industrial firewall [4]. However, due to the manual rule setting and the real-time performance, this approach has been used to a limited extent. Secondly, the intrusion detection approach in industrial control system [5,6] is effective to identify network attacks, and it can give an alarm when suffering a great destruction. As a bypass approach to monitor the abnormal behaviors, intrusion detection technology has been attracting great interests of industry and researchers. Furthermore, intrusion detection can be into two categories: misuse detection and anomaly detection, and the proposed approach in this paper falls into the latter category.

Anomaly detection technology in industrial control system can be divided into three categories [7,8]: statistics-based approach, knowledge-based approach, and machine learning-based approach. By supervising the industrial communication behaviors, these three categories of approaches can detect attacks, alarm and carry out the defensive measures before suffering from kinds of attacks. In the statistics-based approaches, Reference [9] uses the sequential detection model to realize the aberrant communication behaviors in control system. References [10] and [11] use the CUSUM algorithm to implement the communication traffic statistics in industrial control system, and explore the abnormal change point. However, the above statistical analysis only aims at the common industrial communication traffic, and cannot analyze the communication packets in depth according to the industrial communication protocol specification. In this paper, we propose an anomaly

approach based on function code traffic. In accordance with the Modbus/TCP protocol specification, this approach analyzes the Modbus/TCP communication packets in depth, and utilizes the function code traffic to detect abnormal Modbus/TCP communication behaviors. According to the function code traffic change, this approach uses the Cumulative Sum (CUSUM) algorithm for change point detection, and generates an alarm.

Modbus/TCP and Vulnerability Analysis

Modbus/TCP, regarded as an application layer protocol, is an open industrial communication protocol, and uses a typical master-slave communication mode. Namely, one Modbus master sends a request message to one Modbus slave, and the Modbus slave responds this message in accordance with the protocol specification. The Modbus/TCP packet format is shown in Fig.1.

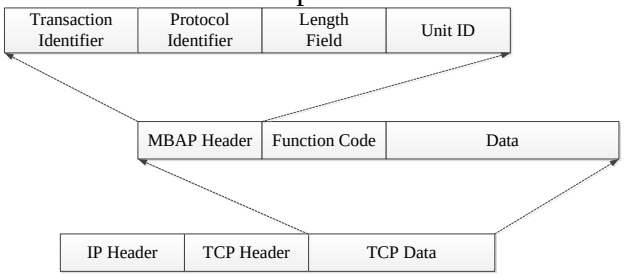


Fig.1 Modbus/TCP packet format

As shown in Fig. 1, the Modbus/TCP packet format mainly consists of three parts: MBAP (Modbus Application Protocol) header, Modbus function code and data. Wherein, MBAP header is a special header which is used to identify Modbus application data unit. Function code is a flag field to perform various operations, and is used to inform the slave to operate the corresponding function. The data domain can be regards as the parameters of function code, and indicates the specific data to perform one operation.

The vulnerabilities of this protocol are increasingly exposed in recent years [12,13], and can be concluded as follows: firstly, Modbus/TCP lacks the authentication, and any Modbus master can use an illegal IP address and one function code to establish a Modbus session; secondly, Modbus/TCP does not consider the authorization, and any Modbus master can perform any operation by using some invalid function codes; finally, Modbus/TCP is short of the integrity detection, and the communication data may be tampered. For example, the function code can be changed to another illegal function code by one attacker.

Anomaly Detection Approach based on Function Code Traffic

It is highly necessary to study on the anomaly detection approach in industrial control system. However, the industrial communication traffic is high-dimensional, and it hard to detect the abnormal communication behaviors. Therefore, we use the function code traffic to execute the anomaly detection, because the function code traffic is simple and single dimensional, and can indirectly reflect the industrial communication behaviors. In our approach, we first capture the industrial communication packets, and extract the Modbus/TCP communication packets. After that, we analyze these Modbus/TCP packets in depth, and get the function code in each packet. From this base, we perform a statistical analysis to form the function code traffic in each specified time interval. Finally, according to the function code traffic, we use the CUSUM algorithm to detect the change point. When one change point appears, the corresponding alarm will be generated. The CUSUM algorithm can be described as follows [14]:

Assume the time sequence x_1, x_2,…, x_{v-1} are independent identically distributed variables with the Gaussian distribution $N(0,1)$, and the time sequence x_v, x_{v+1},…, x_n are independent identically distributed variables with the Gaussian distribution $N(\delta,1)$, where v $(v<n)$ is an unknown change

point and the value x_i represents the number of function codes in the i_{th} time interval. Suppose there is no change point, namely $v=\infty$, the statistical value of the log-likelihood ratio is:

$$Z_n = \max_{1\le v<n} \sum_{i=v+1}^{n} (x_i - \frac{\delta}{2}) \tag{1}$$

Eq. (1) describes the most ordinary CUSUM statistical value. Suppose h ($h>0$) is a chosen threshold which may be determined empirically through experiments. If $Z_i \le h$, $i=1,2,...,n$, the former $n-1$ values are under normal conditions; if $Z_n > h$, anomaly happens and an alarm should be generated. Similarly, the foregoing judgment also can be understood that if an existing number r satisfies $\sum_{i=0}^{r} x_{n-i} - (r+1)\frac{\delta}{2} > h$, where $0 \le r \le n-1$, then the anomaly happens and an alarm should be generated.

The aforementioned equation illustrates the basic CUSUM algorithm. However, the prerequisite is that we have assumed that $\{x_n\}$ are independent Gaussian random variables. Of course, this is not true for network traffic measurements owning to seasonality, trends and time correlations [16]. Therefore, in order to remove such non-stationary behaviors, the work in [15] further improves the basic CUSUM algorithm, and Z_n can be calculated by:

$$\begin{cases} Z_n = [Z_{n-1} + \frac{\alpha\overline{\mu}_{n-1}}{\sigma^2}(x_n - \overline{\mu}_{n-1} - \frac{\alpha\overline{\mu}_{n-1}}{2})]^+ \\ Z_0 = 0 \end{cases} \tag{2}$$

where α is an amplitude percentage parameter, which intuitively corresponds to the most probable percentage of increase of the mean rate after a change has happened. σ^2 is the variance of σ. Meanwhile, the mean $\overline{\mu}_n$ can be calculated by using an exponentially weighted moving average (EWMA) of previous measurements:

$$\overline{\mu}_n = \beta\overline{\mu}_{n-1} + (1-\beta)x_n \tag{3}$$

where β is the EWMA factor. Thus, the conditions to generate an alarm can be summarized as follow:

$$f(Z_n) = \begin{cases} 1, & \text{if } Z_n > h; \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

In Eq. (4), 1 indicates that the anomaly in the detected sequence $\{x_n\}$ is identified and an alarm is generated. By contrast, 0 indicates that the detected sequence $\{x_n\}$ is normal.

However, a disadvantage or flaw exists in the CUSUM algorithm [17]. That is, when the anomaly or attack is over, CUSUM still continues generating the false alarms for a long time. Resulting from accumulation effect of the CUSUM algorithm, the increased amount to Z_n caused by the attack traffic is much greater than the decreasing amount provided by the normal traffic. In order to resolve this issue, our approach uses the following formula to revoke an alarm.

$$f(Z_n) = 0, \text{ if } Z_n \ge h \text{ and } x_i < \varphi\overline{\mu}_{2v-i} \tag{5}$$

where φ is an amplitude and $\varphi > 1$. Assume an anomalous behavior happens at time v, and x_i is the detected mapping request traffic in the i_{th} time interval, $i > v$. $\overline{\mu}_{2v-i}$ is the traffic mean of the former $2v-i$ time intervals, which can be calculated by Eq. (3). The main idea of Eq. (5) is that when the traffic x_i is less than the traffic mean $\overline{\mu}_{2v-i}$ and $Z_n \ge h$, the alarm will be revoked. In addition, in order to revoke an alarm more accurately, the condition $x_i < \varphi\overline{\mu}_{2v-i}$ can be improved as:

$$\sum_{j=0}^{k} 1_{\{x_{i+j} < \varphi \overline{\mu}_{2v-i-j}\}} \geq \theta \tag{6}$$

where θ is a positive integer and $k > \theta > 1$. Eq. (6) describes that when the number satisfies the condition $x_i < \varphi \overline{\mu}_{2v-i}$ is larger than θ, the alarm will be revoked. At the same time, after revoking the alarm, we also reset Z_n between 0 and h.

Performance Evaluations

In the simulation experiment, we build a small SCADA system, whose communication is based on Modbus/TCP. As shown in Fig. 2, the whole technological process can be simply depicted as follows: when the valve switches A and B are respectively turned on, materials A and B successively flow into the container through the valve switches A and B to produce material C. When material C in the container reaches the level upper point, the valve switches A and B are turned off, and then the valve switch C is turned on. When material C in the container exhausts and reaches the level lower point, the valve switch C is turned off. Besides, the above-described technological process is repeatedly performed every 5 minutes.

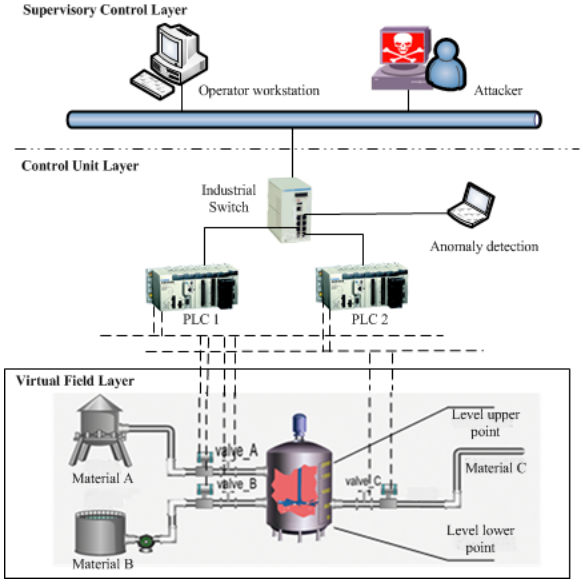
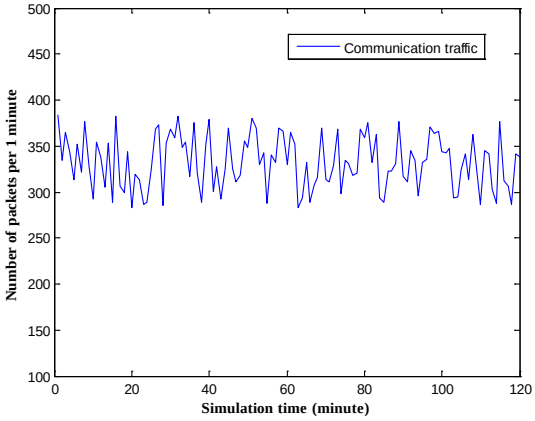
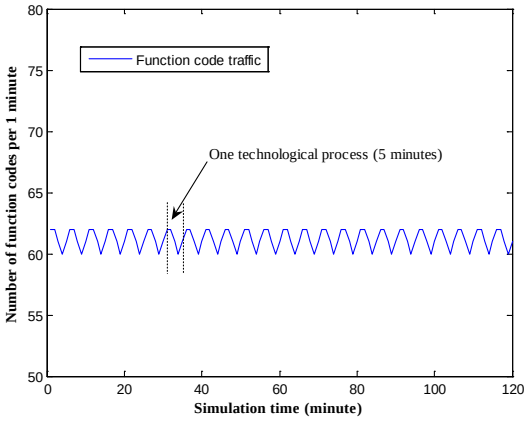


Fig.2 Simulation experiment topology

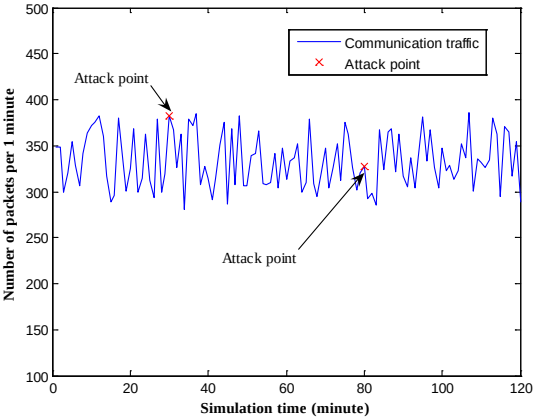
In order to detect the abnormal communication behaviors, we deploy a monitoring computer on industrial switch to capture the communication packets between the supervisory control layer and the control unit layer. Furthermore, we carry out two experiments: one is under normal condition, and the other is under abnormal condition. Under normal condition, we run the simulation for 120 minutes. Fig. 3(a) shows the communication traffic captured by the monitoring computer per 1 minute, and Fig. 3(b) shows the corresponding function code traffic. From these two figures we can see that, the communication traffic is complex and changed, but the function code traffic varies periodically and can reflect every technological process. Under abnormal condition, we perform two attacks at 30th minute and at 80th minute respectively. Here, the attacker sends 50 Modbus/TCP packets whose function code is to write a coil at 30th minute, and sends the same 30 packets at 80th minute. Besides, we apply our anomaly detection approach to the corresponding function code traffic. Fig. 4(a) plots the communication traffic after the attacks. From this figure we can conclude that the attack traffic is hidden into the normal communication traffic, and we cannot identify the attack behaviors only from the communication traffic. Similarly, Fig. 4(b) plots the alarm points in the function code traffic after the attacks. From this figure we find that the proposed approach can detect the abnormal behaviors and generate alarms when the attacks happen. To sum up the above arguments, our approach is available and effective to identify and diagnose some network anomalies in industrial control system. In other words, compared with the anomaly detection using the communication traffic, our approach is more advantage.

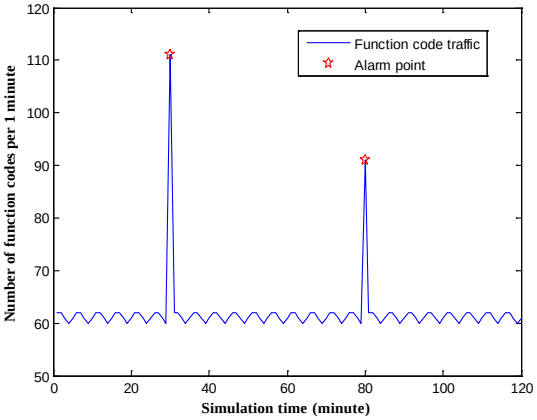




(a) Function code traffic per 1 minute (b) Communication traffic per 1 minute

Fig.3 Under normal condition





(a) Attack points in the communication traffic (b) Alarm points in the function code traffic

Fig.4 Under normal condition

Conclusion

This paper aims to propose an anomaly detection approach based on function code traffic, and the basic idea behind the proposed approach is very simple. That is, identifying and detecting the anomalous communication behaviors in industrial control system by judging the function code traffic anomaly. In this paper, we first analyze Modbus/TCP protocol and its vulnerabilities, and then we present the detailed design of our approach, including the CUSUM algorithm. At last, we evaluate our approach in detail by simulation experiment. We show that, our approach is very available and effective to provide the security for industrial control system. Besides, we also discuss some drawbacks of our approach for our future research.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (Grant No. 61501447) and Independent project of Key Laboratory of Networked Control System Chinese Academy of Sciences: Research on abnormal behavior modeling, online intrusion detection and self-learning method in industrial control network.

References

[1] H. Kagermann, W. Wahlster, J. Helbig, Recommendations for implementing the strategic initiative INDUSTRIE 4.0, Final Report, http://www.plattform-i40.de/finalreport2013, 2013.

[2] B. Genge, C. Siaterlis, I. N. Fovino, et al., A cyber-physical experimentation environment for the security analysis of networked industrial control systems, Computer and Electrical Engineering, 38(5) (2012) 1146-1161.
[3] C. Shao, L. G. Zhong, An information security solution scheme of industrial control system based on trusted computing, Information and Control, 44(5) (2015) 628-633.
[4] S. S. Zhang, W. L. Shang, M. Wan, et al., Security defense module of Modbus TCP communication based on region/enclave rules, Computer Engineering and Design, 35(11) (2014) 3701-3707.
[5] A. Carcano, A. Coletta, M. Guglielmi, et al., A multidimensional critical state analysis for detecting intrusions in SCADA systems, IEEE Transactions on Industrial Informatics, 7(2) (2011) 179-186.
[6] A. Anoop, M. S. Sreeja, New genetic algorithm based intrusion detection system for SCADA, International Journal of Electronics Communication and Computer Engineering, , 2(2) (2013) 171-175.
[7] S. M. Papa, V. S. S. Nair, A behavioral intrusion detection system for SCADA systems, Southern Methodist University, 2013.
[8] B. Zhu, S. Sastry, SCADA-specific intrusion detection/prevention systems: a survey and taxonomy, The 1st Workshop on Secure Control Systems (SCS), 2010.
[9] A. A. Cardenas, S. Amin, Z. S. Lin, Attacks against process control systems: risk assessment, detection, and response, The 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, 2011, pp.355-366.
[10] Y. G. Zhang, H. Zhao, L. N. Wang, A non-parametric CUSUM intrusion detection method based on industrial control model, Journal of Southeast University(Natual Science Edition), A01 (2012) 55-59.
[11] M. Wei, K. Kim, Intrusion detection scheme using traffic prediction for wireless industrial networks, Journal of Communications and Networks, 14(3) (2012) 310-318.
[12] N. Goldenberg, A. Wool, Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems, International Journal of Critical Infrastructure Protection, 6(2) (2013) 63-75.
[13] T. H. Kobayashi, A. B. Batista, A. M. Brito, et al., Using a packet manipulation tool for security analysis of industrial network protocols, IEEE Conference on Emerging Technologies and Factory Automation. Patras, 2007, pp.744-747.
[14] M. Wan, H. K. Zhang, T. Y. Wu, et al., Anomaly detection and response approach based on mapping requests, Security and Communication Networks, 7 (2014) 2277-2292.
[15] V. A. Siris, F. Papagalou, Application of anomaly detection algorithms for detecting SYN flooding attacks, 2004 IEEE Global Telecommunications Conference GLOBECOM'04, Dallas, 2004, pp.2050-2054.
[16] J. L. Hellerstein, F. Zhang, P. Shahabuddin, A statistical approach to predictive detection, International Journal of Computer and Telecommunications Networking, 35(1) (2001) 77-95.
[17] H. H. Takada, U. Hofmann, Application and analyses of cumulative sum to detect highly distributed denial of service attacks using different attack traffic patterns, http://www.ist-intermon.org/dissemination/newsletter7.pdf, 2004.