Data Security Transmission Mechanism in Industrial Networked Control Systems against Deception Attack

Zulan Deng¹, Lun Xie^{1*}, Yu Rong², Weize Li¹, Liangchen Jin¹

¹ School of Computer and Communication Engineering,
University of Science and Technology
Beijing, Beijing, China

² Beijing ChenJiGuoTai Science & Technology Co.,Ltd.

*Correspondence Author: Lun Xie,
xielun@ustb.edu.cn

Abstract

Industrial networked control systems (INCSs) are widely used in the modern critical infrastructures and the collapse of INCSs will cause serious economic losses. Due to the communication protocols used in INCSs mostly without security control, this paper proposes a data security transmission (DSTM) to protect the data transmitted in INCSs, which integrates DES, MD5 algorithms and a dynamic key mechanism synchronous with events. The former two algorithms are used to enforce the data confidentiality and check the data integrity and reliability. For the key's update in encryption, the dynamic key mechanism based on event synchronization is proposed to avoid transmitting the key through network. The results of simulation performed in the MATLAB/SIMULINK suggest that the DSTM can effectively solve the key management problem of encryption and secure the data transmission in INCSs.

Keywords: Industrial Networked Control Systems (INCSs), Data Security, Data Security Transmission Mechanism (DSTM), Dynamic Key Mechanism, Deception Attack

1. Introduction

Industrial networked control systems (INCSs) include supervisory control and data acquisition system (SCADA), the distributed control system (DCS), program logic control system (PLC) and other control systems. INCSs are widely used in critical infrastructures for automatic control, the real-time data acquisition and detection of process control. Once they are attacked, it will cause serious social economic losses. Nowadays, with the increasing complexes of connections, INCSs have been developed from a closed system into a more open network environment^[1], and they are very vulnerable to cyber attacks for the widely used communication protocols (such as Modbus and DNP3) without security control^{[2],[3]}. This paper aims at proposing a security mechanism to compensate for the protocol vulnerabilities and protect the data transmitted in INCSs.

There are three main security requirements of the data transmitted in INCSs: confidentiality, integrity and reliability^[4]. Data confidentiality is the protection of transmitted data from passive attacks^[5], such as eavesdropping on or monitoring of transmissions. Encryption is the most effective solution of enforcing data confidentiality. There are many encryption algorithms, such as DES, 3DES, RSA and AES, of which first one is considered in this paper. Because DES has a fast encryption speed, is easy to implement and difficult to crack^[6]. Gupta *et al.*^[7] used the DES and 3DES algorithms to protect the confidentiality of the data in the NCS. For active attacks in the NCS, Paper [8]

¹ Lun Xie is the corresponding author.

applied DES algorithm to secure the data from plant with the comprehensive comparison of several classic encryption algorithms.

Data integrity and reliability is the protection of transmitted data from active attacks, such as deception attacks and denial of service (DoS) attack. For data integrity and reliability, paper [9] used DES to encrypt the data transmission in NCS and MD5 to detect its integrity. Pang *et al.*[10] applied MD5 to compress the original data and get the digital abstract. The abstract was attached to the original data and the time-stamp followed it. Finally they encrypted the new primitive data with DES algorithm.

As shown above, encryption with DES algorithm can effectively protect data confidentiality. Data integrity and reliability were checked from the viewpoint of information security technology. Hash functions are effective for data integrity and reliability, which are considered in this paper.

Although encryption and hash function are effective for data security transmitted in INCSs, there is an important problem that is the key's distribution and management. DES is one of the symmetrical encryption algorithm, the keys used in the encryption and decryption are the same. Therefore, all operations will be in vain once key leakages.

To solve the key's distribution and management used in DES, Yang *et al.*[11] used 3DES to encrypt the original data and MD5 to compress the original data for digital abstract. Then they used RSA to encrypt the data and 3DES keys. Although this method effectively combines advantages and disadvantages of the symmetrical encryption algorithm and asymmetric encryption algorithm, but it will bring the following disadvantages: 1) The method doesn't consider about updating the key of RSA. 2) The transmitted data are encrypted twice, which additionally increasing the system's running time and decreases the transmission efficiency of network data, especially for the multiple-input multiple-output distributed systems.

To effectively solve the distribution and management of the key used in encryption, this paper proposes a dynamic key mechanism synchronous with events. This mechanism uses a counter to record the number of data transmission and as the mechanism's start switch. Based on this mechanism, a data security transmission mechanism (DSTM) of INCSs has been proposed. DSTM firstly uses DES to ensure the confidentiality of the data, and then uses MD5 to detect and verify the integrity and reliability of transmitted data, finally has a simple attacks compensate measures. As a result, this paper performs the system simulation with the Simulink tools in MATLAB and verifies the effectiveness of DSTM.

2. Data Security Transmission Mechanism

2.1 Implementation of the Security of Data

As introduced in section 1, the security of data consists mainly of confidentiality, integrity and reliability. Data confidentiality can be achieved by encryption algorithm, which can be classified into symmetric encryption algorithm and asymmetric encryption algorithm. Compared with the asymmetric encryption algorithm, the symmetric encryption algorithm is faster by two to three orders of magnitude and require much shorter keys to achieve the same level of security^[6]. Typical symmetric algorithms are DES, 3DES, and AES, of which the first one is used in this paper because it is the fastest one of them and enough to guarantee the data confidentiality.

DES is a symmetric encryption algorithm, using a key of 56 bits to operate 64 bits packet. The input of the algorithm is the 64 bits block of plain-text and the output is the 64 bits block of cipher text grouping. There are 16 rounds of consistent iterative operation between plain-text and cipher text. The 56 bits key is generated by ignoring every eighth bit in a given 64 bits key.

The data integrity and reliability can be secured by using the principle of the Hash

function. The Hash function can compress any length strings into a fixed length strings and the output of this process is the Hash value, also called a message digest, digital fingerprint. It has the following security features[12]:

(1) the unidirectional and irreversible

A string of arbitrary length can easily get its positive Hash values, but the contrary operation is difficult to take.

(2) Collision resistance

It's impossible to exist several different strings matching the same Hash value.

The most widely used hash functions are MD5 and Secure Hash Algorithm (SHA, e.g., SHA-1/256/384/512), and the former is used in this paper due to its low computation[6]. MD5 accepts the message input of arbitrary length and produces 128-bits fixed message digest.

2.2 Detection of Deception Attack

In the INCSs, there are three kinds of attacks that deception attacks, denial of service attack and the attack aiming at the field equipment^[13]. This paper focuses on deception attack. There are many ways to perform it, such as sniffing messages, fabricating fake messages, modifying the messages, recombining of the messages, replying the original messages and destroying messages.

According to the principle of deception attack, it mainly destroys the data integrity and reliability. As shown in Figure 1, a sender gets encrypted data through DES encryption and digital digest by MD5. The encrypted data and digital digest are sent to the receiver. In the receiver, MD5 is used again to the encrypted data for a new digital digest. If the new digital digest is equal to the incoming one, the data will be considered authentic. Otherwise, the data will be regarded to be modified in transmission and then discarded.

Figure 1. Detection of Deception Attack

2.3 Dynamic Key Mechanism Synchronous with Events

One of the important issues involved in the encryption operation is the key's distribution management.

To ensure the data confidentiality more effectively, the key used by DES should update constantly. When the DES key updates, the problem comes out that how we can manage the key safely and effectively. As introduced in section 1, many people used asymmetric encryption algorithm to solve the key's distribution and management of symmetric encryption. However, they didn't consider about the update of the key used in asymmetric encryption.

For the key's management problem of encryption, we propose a dynamic key mechanism synchronous with events. The mechanism uses a counter to track the number of data transmission in a network communication session. In network communication, we consider the number of sending data and receiving data as the standard of the event's classification.

Figure 2. The Relationship between the Events in Network Communication

In Figure 2, e_i ($i=1,2,3,4$) is the event defined in this paper; Cs and Cr is the result of send data and receive data respectively; t is used to countdown the maintain time of an event and t_0 is the maintain time of an event.

In event e_1 , $Cs = 0$, $Cr = 0$, $t = 0$. At this point, if there is data to send, e_1 is changed to e_2 . Or if there is data to receive, e_1 is changed to e_3 .

In event e_2 , $Cs = 1$, $Cr = 0$, $t = t_0$. At this point, t is gradually reduced. If there is data to receive before t is reduced to zero, e_2 is changed to e_4 . Or if there is no data to receive until t is reduced to zero, e_2 is changed back to e_1 .

In event e_3 , $Cs = 0$, $Cr = 1$, $t = t_0$. At this point, t is gradually reduced. If there is data to send before t is reduced to zero, e_3 is changed to e_4 . Or if there is no data to receive until t is reduced to zero, e_3 is changed back to e_1 .

In event e_4 , $Cs = 1$, $Cr = 1$, $t > 0$. At this point, dynamic key mechanism is triggered. e_4 is changed to e_1 after updating the encryption key.

In dynamic key mechanism, the initial value of seed of the dynamic key generation is zero. When dynamic key mechanism is triggered again, the value of seed pluses 1. The software implementation of dynamic key generation uses the random numbers produced functions in MATLAB in the simulation phase. Otherwise, a random pool can be used to generate special and unique key. In this way, the mexFunction implemented in C file is chosen. As shown in Figure 3, the happening of event e_4 results in the increasing of the value of seed used in dynamic key generation. The value is used to function `srand()` to initial the random number seed. Then the function `rand()` is used to pick randomly characters from random pool. Each eight random characters form one key of symmetric encryption. With the continuous transmission of data in the network communication, the value of counter updates constantly. Thus, the key updates constantly in the mechanism.

Figure 3. Dynamic Key Mechanism Synchronous with Events

2.4. Data Security Transmission Mechanism

To achieve the data security and the deception attack detection simultaneously, this paper presents a data security transmission mechanism (DSTM) shown in Figure 4. This mechanism is comprised of two parts: a safe sender unit and a safe receiver unit.

In safe sender unit, DSTM firstly uses the DES encryption algorithm to encrypt the original data ensuring the data confidentiality. Then DSTM uses a one-way operation Hash algorithm MD5 to compress encrypted data, which creates a fixed length digital digest. Finally, the transmitted data includes the encrypted data and the digital digest. The key of DES operation is generated by dynamic key mechanism introduced in section 2.3.

In safe receiver unit, DSTM separates the encrypted data and digital digest from the received data. It secures the data integrity and reliability with the one-way Hash function MD5 and creates a new digital digest. Then DSTM compares the new digital digest and the received digital digest. If they are consistent, it uses the key generated by the dynamic key mechanism to decode the encrypted data. If the new digital digest is not equal to the received one, DSTM will discard the received data and use the previous received data for the attack compensation.

Figure 4. The Structure of DSTM

3. Simulation and Result Analysis

The typical architecture of NCS is shown in Figure 5-a. NCS is composed of three parts: controller, actuator and sensor. In Figure 5-b, DSTM is deployed in NCS. The controller passes control variables $u(t)$ to the actuator through the network, and the actuator transmits it to the controlled process. The output signal of the controlled process is passed to the controller as the sensor variable $y(t)$ through network.

In MATLAB simulation environment, we use Simulink and Turetime tools to perform a simulation test for our proposed DSTM. As shown in Figure 6, the simulation structure contains 4 computer nodes and one network part. The network part uses the Truetime Network module, of which network type is chosen as CSMA/CD (Ethernet), and each computer node is composed of Truetime Kernel. The sensor node is triggered by time samples data periodically and transmits results to all controller nodes through network. These controller nodes calculate the control signal and send it to the actuator, which completes the action. This simulation also contains an attacker node, launching an attack with the trigger signal, i.e the value of clock.

Figure 5. The Architecture of NCS

Figure 6. The Structure of Simulation Test in MATLAB

3.1. The Controller and the Controlled Process

In this simulation, the control algorithm adopts the traditional PID control. In the industrial control application, PID controller is a kind of common feedback loop component. It compares the collected data and a reference value, and then the difference

is used to calculate the new input values, aiming at letting the system data to achieve or maintain at the reference value. The PID controller can adjust the input value according to the historical data and the difference rate, making the system more accurate and stable.

The PID controller (proportional-integral-differential controller) is composed of unit P, unit I and unit D integral differential^[14], as shown in Figure 7.

Figure 7. PID Controller

The unit P, integral unit I and unit D of PID controller are respectively corresponding to the current differential error, the past accumulated error and the future error. If we don't know the characteristics of the controlled system, generally PID controllers are the most suitable^[15].

$$u(t) = K_p e(t) + K_i \int_0^t e(\tau) d\tau + K_d \frac{de(t)}{dt} \quad (1)$$

$$e(t) = r(t) - y(t) \quad (2)$$

The calculation formula of PID controller is the formula (1). K_p, K_i, K_d respectively are the proportion coefficient, integral coefficient, differential coefficient. $u(t)$ is the control variable of controller output. $y(t)$ is the sensor variable from the sensor. $r(t)$ is the reference value given to the controller by system. The error $e(t)$ can be calculated according to the formula (2). By adjusting the three parameters of PID controller K_p, K_i, K_d , we can make the control system meet the design requirements.

$$P(k) = K * (\beta r(k) - y(k))$$

$$I(k+1) = I(k) + \frac{Kh}{T_i} (r(k) - y(k)) \quad (3)$$

$$D(k) = a_d D(k-1) + b_d (y(k-1) - y(k))$$

$$u(k) = P(k) + I(k) + D(k)$$

In our simulation, the control algorithm selects PD control, such as a formula (3). In the formula (3), $a_d = \frac{T_d}{Nh + T_d}$, $b_d = \frac{NKT_d}{Nh + T_d}$, $\beta = 0.5$, $T_i = 0.12$, $T_d = 0.049$, $N = 100$, $h = 0.006$, $K = 0.96$.

The controlled process in the simulation is a DC servo motor, whose transfer function is shown in the formula (4)^[16]. In the formula, $V(s)$ is the end input voltage of DC servo motor, $\Omega(s)$ is the rotating speed output of DC servo motor.

$$G(s) = \frac{\Omega(s)}{V(s)} = \frac{1000}{s(s+1)} \quad (4)$$

3.2 The Simulation Results

The reference value r in this simulation is a 0.25Hz, 1V square wave. When deception attack does not exist in the network, the simulation's tracking square wave is shown in Figure 8-a. From the graph, we can see that r spreads through the network and reaches the controlled process $G(s)$. The system's tracking waveform y can converge to the r although it will have a little fluctuation when r changes. Comparing figure 8-a and 8-b, the use of DSTM have no influence on the performance of INCSs.

(a) The Simulation Waveform of INCSs without DSTM

(b) The Simulation Waveform of INCSs with DSTM

Figure 8. The System's Tracking Square Wave of INCSs without Deception Attack

When the sensor's return value $\tilde{y}(t)$ received by the controller is not equal to the value $y(t)$ namely $\tilde{y}(t) \neq y(t)$, there exists deception attack in system^[11]. Similarly, when the control command $\tilde{u}(t)$ received by actuator is different with the control command $u(t)$ sent by controller, namely $\tilde{u}(t) \neq u(t)$, there is deception attack in system.

Taking the actuator input $\tilde{u}(t)$ which is the control command as an example, the mathematical model of deception attacks is shown in formula (5). In the formula, $\tilde{u}(t)$ is the actuator's input from the network at t moment, t is the clock value of this simulation and the trigger signal of deception attack. $a(t)$ is the value of attack, $u(t)$

is the legal control input.

$$\tilde{u}(t) = \begin{cases} a(t), & 3.9 < t < 4.5 \\ u(t), & \text{others} \end{cases} \quad (5)$$

In our simulation, we perform deception attack on the controller output value $u(t)$ in the interference node, sending fake control commands to actuator. Taking the clock value t as the trigger signal, when t is between 3.9 and 4.5, attacker sends fake control commands $a(t)$ between -5 to 10 to actuator. The waveform of control output $u(t)$ has a distortion when $3.9 < t < 4.5$, as shown in Figure 9.

(a) The Simulation Waveform of $u(t)$ without Deception Attack

(b) The Simulation Waveform of $u(t)$ with Deception Attack

Figure 9. The Effects of Deception Attacks on Control Output $u(t)$

Under deception attack, the simulation waveforms of INCSs are shown in Figure 10. In INCSs without DSTM, actuator is unable to identify whether the control command is legitimate, it will execute all received commands, causing the return value y of sensor deviating from the reference value r of system, as shown in Figure 10-a. DSTM uses the previous legal control command u as the attack compensation. Thus, in figure 10-b, we can see that the value of y doesn't change when t ranges from 3.9 to 4.5 and the system's tracking waveform y can converge to the r eventually in INCSs with DSTM.

(a) The Simulation of $y(t)$ in INCSs without DSTM

(b) The Simulation of $y(t)$ in INCSs with DSTM

Figure 10. The Tracking Waveform of Square Wave in INCSs Under Deception Attack

From the above simulation results, we can see that the use of DSTM can protect the security of transmitted data and has a little influence on the system's performance.

As shown in Figure 11-a, the network delay from controller to actuator is between 0 and 0.1094s and network delay from sensor to controller varies from 0 to 0.0938s. In Figure 11-b, network delay from controller to actuator changes from 0 to 0.500s while network delay from sensor to controller is from 0.0156 to 0.8438s in INCSs with DSTM. The increase of the network delay is in the acceptable range for our simulation, but may be unacceptable for some systems with high requirements of real-time. That is our future work to reduce the network delay caused by DSTM.

Figure 11. The Network Delay of INCSs

4. Conclusion

This paper proposes a dynamic key mechanism synchronous with events to solve the key manage problem of encryption. On this basis, a data security transmission mechanism (DSTM) is proposed to protect the transmitted data in INCSs. We use deception attack to validate the effectiveness of DSTM with simulink tools. Our simulation results suggest that DSTM can not only protect the transmitted data in INCSs, but also has a little influence on the system's performance. Even though, we have focused on the implementation of DSTM and the data security in INCSs, the attack compensation in this paper is too simple and the network delay increases too much. Moreover, this paper can be further extended by considering the following three issues: 1) special attack compensation for deception attack in INCSs; 2) the security mechanism's influence of the network delay in INCSs; 3) other attacks in INCSs, such as denial of service attack (DoS).

Acknowledgments

This work is supported by National Key Technologies R&D Program of China (No.2014BAF08B04) and National Natural Science Foundation of China (Normal Project No. 61170115), (Key Project No.61432004) and the Foundation of Beijing Engineering and Technology Center for Convergence Networks and Ubiquitous Services.

References

- [1] C. W. Ten, C. C. Liu, G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems", *Power Systems, IEEE Transactions on*, vol.23, no. 4, (2008), pp. 1836-1846.
- [2] G. Dondossola, J. Szanto, M. Masera, *et al.* "Effects of intentional threats to power substation control systems". *International journal of critical infrastructures*, vol.4, no. 1, (2008), pp. 129-143.
- [3] G. Hayes, K. El-Khatib. "Securing modbus transactions using hash-based message authentication codes

- and stream transmission control protocol". Communications and Information Technology (ICCIT), 2013 Third International Conference on. IEEE, **(2013)**, pp. 179-184.
- [4] Z. H. Pang, G. P. Liu, "Design and implementation of secure networked predictive control systems under deception attacks", *Control Systems Technology*, IEEE Transactions on, vol. 20, no. 5, **(2012)**, pp. 1334-1342.
- [5] A. Kahate, "Cryptography and network security". Tata McGraw-Hill Education, **(2013)**.
- [6] P Swaminathan , K Padmanabhan, S Ananthi , *et al.* "The Secure Field Bus (SecFB) protocol-network communication security for secure industrial process control". TENCON 2006. 2006 IEEE Region 10 Conference. IEEE, **(2006)**, pp. 1-4.
- [7] R A Gupta, M Y Chow, A K Agarwal, *et al.* "Information security with real-time operation: performance assessment for next generation wireless distributed networked-control-systems". Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE. IEEE, **(2007)**, pp. 420-425.
- [8] P. Zhonghua, L Guoping, Z Donghua, "Detection of deception attacks on the backward channel of networked control systems", *Control Conference (CCC)*, 2012 31st Chinese. IEEE, **(2012)**, pp. 5972-5977.
- [9] L. Guoping. "Secure networked control systems under data integrity attacks". *Control Conference (CCC)*, 2010 29th Chinese. IEEE, **(2010)**, pp. 5765-5771.
- [10] Z H Pang, G Zheng, G P Liu, *et al.* Secure transmission mechanism for networked control systems under deception attacks. *Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, 2011 IEEE International Conference on. IEEE, **(2011)**, pp. 27-32.
- [11] K H Yang, S J Niu. "Data Safe Transmission Mechanism Based on Integrated Encryption Algorithm". *Computational Intelligence and Software Engineering*, 2009. CiSE 2009. International Conference on. IEEE, **(2009)**, pp. 1-4.
- [12] H Qi, Z Qinqin, W Yongliang, *et al.* "Research and hardware implementation of MD5 algorithm based on Hash function". *Computer Engineering*, vol. 39, no. 3, **(2013)**, pp. 137-141.
- [13] A A Cardenas, S Amin, S Sastry. "Secure Control: Towards Survivable Cyber-Physical Systems". *IEEE International Conference on Distributed Computing Systems Workshops*. IEEE, **(2008)**, pp. 495 - 500.
- [14] Y Li, K H Ang, G C Y. Chong Patents, "software, and hardware for PID control: an overview and analysis of the current art". *Control Systems*, IEEE, vol. 26, no. 1, **(2006)**, pp. 42-54.
- [15] S. Bennett, "A history of control engineering", *IET*, **(1993)**, pp. 1930-1955.
- [16] Z Liying, X Lun, L Weize, *et al.* "A secure mechanism for networked control systems based on TrueTime". *International Conference on Cyberspace Technology. IET*, **(2013)**, pp. 44 - 49.