Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **3**, May **2016**

One Communication Key Udate with Whitelist Attribute in SCADA System

Nong Si

Beijing Laboratory of Advanced Information Networks, Beijing, 100124
College of Electronic Information and Control Engineering
Beijing University of Technology
100 Ping Le Yuan, Beijing 100124, China
nongsi@ieee.org

Ke-Bin Jia*

Beijing Laboratory of Advanced Information Networks, Beijing, 100124
College of Electronic Information and Control Engineering
Beijing University of Technology
100 Ping Le Yuan, Beijing 100124, China
*Corresponding author
kebinj@bjut.edu.cn

Received March, 2016; revised March, 2016

Abstract. *The Supervisory Control and Data Acquisition (SCADA) networks provide high efficiency in various industries which became one primary and specific industrial control systems. The data encryption method is usually applied to current SCADA system to improve security. This paper proposes a new cryptographic key management scheme for SCADA networks with whitelist attribute. It is able to mitigate varied cyber-attack threats. The session key update and master key update protocol in this scheme reduces from three or two communications to one communication. From the evaluation result, the traffic and energy consumption of the session key update phase and master key update phase drop considerably, while the QoS increases in proposed scheme.*

Keywords: Industrial system security, Key management, SCADA network

1. **Introduction.** Todays advanced industrial facilities are giant and distributed complexes, such as electric power plants, oil pumping control systems, waste water treatment plants and manufacturing facilities. The traditional point to point remote control system has been substituted by an integrating system consisted with continuing monitor and controller to remote sensors connecting with internal common communication bus. The Supervisory Control and Data Acquisition (SCADA) networks which provide high efficiency in various industries became one primary and specific industrial control system [1, 2].

The traditional SCADA is only a closed network for internal using. Thus, seldom regulations and security algorithms were implemented in such system. The vulnerability of SCADA system is increasing by many SCADA systems turned to openly connect to internet due to requirement for information sharing or operation performing [3]. Therefore, the data encryption method was usually applied to current SCADA system. And key distribution is a critical issue for data encryption.

The communication in SCADA network is mainly running between a master station and Remote Terminal Units (RTUs) or Intelligence Electronic Devices (IEDs). RTUs and IEDs continue to overlap in functionality and capability [4]. The method of sharing keys can be categorized into two ways: centralized key distribution and decentralized key distribution. This paper mainly focuses on the decentralized key distribution method, where the master station often works as a key distributor.

Many researches were performed to increase the security architecture in key management. Researchers at Sandia, Beaver et al. [5] presented a paper on key establishment for SCADA (SKE) which discussed a key management solution using symmetric and public key cryptography techniques. Dawson et al. [6] proposed a key management architecture (SKMA) using a Key Distribution Center (KDC) for authentication and access control. Choi et al. proposed Advance SKMA (ASKMA) [3] and ASKMA+ [7] which improved SKMA proposal. Kang et al. [8] proposed a key management scheme for SCADA networks secure communication, which proposed a symmetric encryption method with low requirement of key exchange frequency and energy consumption. Most of above proposals were using three communications in key update procedure. Rezai et al. [9] present a key management scheme using only two communications to finish key update. In this scheme the communication links are decreased from 3 links to 2 links compared to Kang et al.s key management scheme. The energy consumption, the speed and network traffic, the security of the master key, the SI and QoS, the required hardware and computational cost in RTUs and IEDs in the session key update phase are improved in comparison with Kang et al.s key management scheme.

This paper proposed a new cryptographic key management scheme for SCADA networks which improved the proposal in [9]. The proposed scheme decreases the key update phase between master station and RTU or IED from two communications to one communication. In this paper, the detailed protocols are discussed and several main performance evaluations have conducted, which proved some important indices like Energy Consumption, Traffic and Quality of Service (QoS) have been improved. .

The rest of this paper is organized as follows: Section 2 describes briefly background of SCADA networks. In Section 3, the Rezai et al.s key management scheme is discussed. Section 4 presents the proposed key management scheme for SCADA networks. Section 5 evaluates the proposed key management scheme by comparing with others work. Finally, conclusion is given in Section 6.

2. **SCADA networks background.** The industrial control network is most typically made up of several distinct and remote areas for using at critical infrastructures like water, gas, oil, electricity and SCADA is one specific piece of an industrial network. A typical SCADA network consists of master station, Communication Links and Slave Stations. Master station is the controlling asset or host involved in an industrial protocol communication session. And the master station is typically responsible for timing, synchronization, and command and control aspects of an industrial network protocol. The slave stations contain RTUs and IEDs. A RTU is a device combining remote communication capabilities with programmable logic for the control of processes in remote locations. An IED is an electronic component that has a microprocessor and is able to communicate using fieldbus or other industrial protocols.

To keep the data transfers of SCADA networks are secure from unwanted attacks, several cryptography methods are evaluated and performed. The symmetric encryption algorithm, a typical and applied encryption algorithm, is often set up at the communication link ends between master station and each slave stations. A visual administration section is installed to monitor no abnormal activities and errors are happening and to

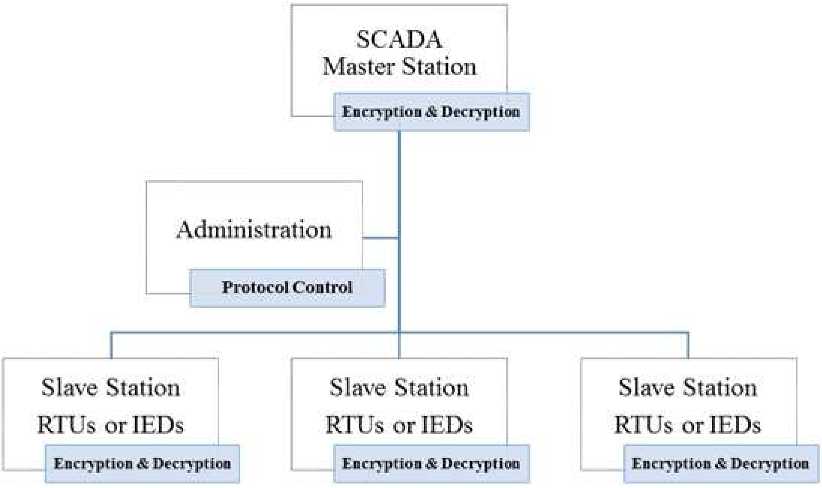

Figure 1. Typical SCADA network structure

guarantee the proper protocols are performed as described in Fig 1. This symmetric encryption algorithm uses an identical encryption and decryption key during the both calculate directions; it also has another name as single-key algorithm. Therefore, the key management scheme becomes crucial to ensure the whole cryptography processes are safe and becomes a foundation and bottom of the SCADA security architecture.

3. **Rezai et al.'s key management scheme.** Recently Rezai et al. presented a scheme for key management. In this key management, it contained three phases: initial condition phase, session key update phase and master key update phase. In the session key update, the steps were decreased from three communications to two communications compared to Kang et al.'s key management scheme. The session key generation devices were also displaced from slave side (RTUs and IEDs) to master station side. In the session key master station generated session key and sent it to slave side. And confirm message was used for slave station to inform the master station the complement. In the master key update phase, the ECDH protocol was exploited.

4. **The proposed key management scheme.** The SCADA networks are vulnerable due to its several constrains such as Resource Constrained RTU, High Resiliency, Low Bandwidth and Low Latency Communications, Long Node Life, Real Time, RTUs Physically Insecure and etc. Therefore, we propose a new and automatic key management scheme aiming to improve these conditions for a decentralized key distribution. In this scheme, at a configurable certain interval, the session key and master key will be created by RTU or IED and master station. The key update information will transmitted with data message together, which can reduce the traffic of communication links. There is no requirement for transmitting confirmation messages during key update, because the counterpart will verify the key by itself. And confirm it by using the new key in next communication. In order to make SCADA cyber systems more secure, the messages from RTU and IED to master station are added with whitelist secure attribute IDs, The master station uses a whitelist checker to classify the incoming messages by scanning the whitelist secure IDs. If the checking results shows the attribute ID is valid. The messages will be passed to the next procedure, and regarded as legitimate massages. If not, the message will be dropped as fishing messages.

The proposed key management contains three phases: initial condition phase, session key update phase and master key update phase.

4.1. **Initial condition phase.** Protocol 1 System initialization

(1) Clock synchronization at all devices with master station.
(2) Set Initial Master Key (mk) table in the master station.
(3) Broadcast and set the Initial Master Key with paired RTU or IED in secure way.
(4) Set session key refresh interval and new session key update algorithm.

4.2. **Key update phase.** Protocol 2 Session Key Update: From RTU and IED to master station

(1) Generate data message from sensors (m).
(2) Locate current Session Key ID (I_{sk}).
(3) Calculate Session Key (K_{sk}) from Session Key ID (I_{sk}).

$$K_{sk} = f(I_{sk}) \tag{1}$$

(4) Encrypt the data message by session key.

$$c_1 = E_{sk}(m) \tag{2}$$

(5) Encrypt the Session Key ID by master key.

$$c_2 = E_{mk}(I_{sk}) \tag{3}$$

(6) Combine encrypted message(c) and encrypted Session Key ID. (c= c_1+c_2).

$$c = c_1 + c_2 \tag{4}$$

(7) Add whitelist attribute to message(c).

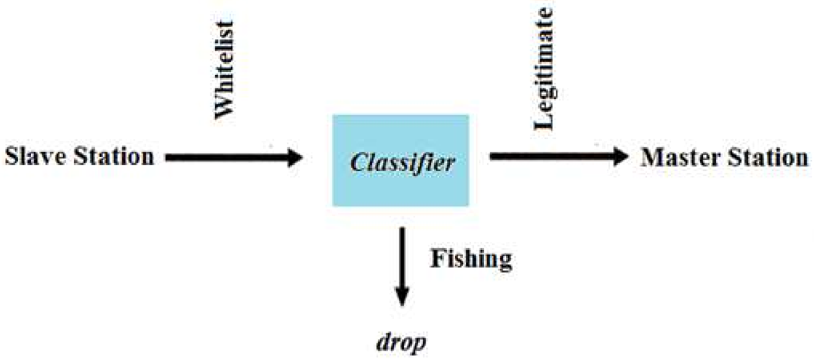

FIGURE 2. Proposed whitelist classifier procedure

Protocol 3 Session Key Update: master station to RTU and IED
(1) Receive the encrypted message (c).
(2) Checking the message (c) with its whitelist attribute.
(3) Divide c into c_1 and c_2
(4) Decrypt Session Key ID with the master key from c_2.

$$I_{sk} = D_{mk}(c_2) \tag{5}$$

(5) Calculate the desired Session Key by K_{sk}

$$K_{sk} = f(I_{sk}) \tag{6}$$

(6) Decrypt data message with the Session Key.

$$m = D_{sk}(c_1) \tag{7}$$

(7) If the decryption result is ok, use the new session key to send message.

The master station and the RTU or IED begin to communicate with each other by the new session key. Fig.2 shows a complete procedure of whitelist classifier. Fig. 3 shows a complete procedure of session key update with whitelist attributes

4.3. **Master key update phase.** Protocol 4 Master Key Update: master station to RTU and IED

(1) Calculate New Master Key (K$_{nmk}$).
(2) Encrypt this New Master Key by session key.

$$c_2 = E_{sk}(K_{nmk}) \tag{8}$$

(3) Encrypt the Master Key Update Code by Current Master Key (K$_{cmk}$).

$$c_4 = E_{cmk}(C_{mku}) \tag{9}$$

(4) Combine encrypted New Master Key and Master Key Update Code. (c= c3+ c4).

$$c = c_3 + c_4 \tag{10}$$

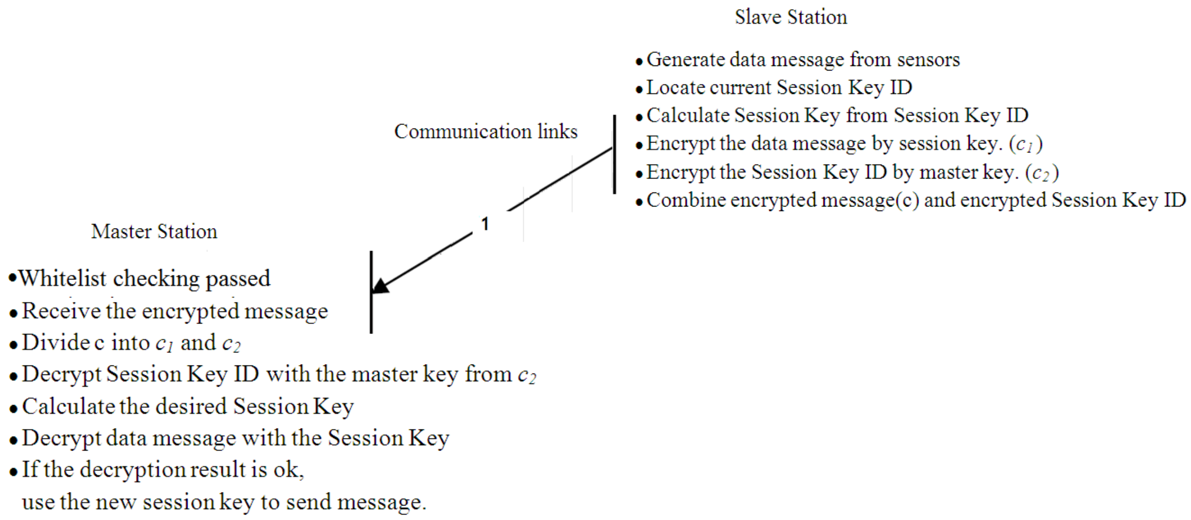
Slave Station
• Generate data message from sensors
• Locate current Session Key ID
• Calculate Session Key from Session Key ID
• Encrypt the data message by session key. (c_1)
• Encrypt the Session Key ID by master key. (c_2)
• Combine encrypted message(c) and encrypted Session Key ID
Communication links
1
Master Station
•Whitelist checking passed
• Receive the encrypted message
• Divide c into c_1 and c_2
• Decrypt Session Key ID with the master key from c_2
• Calculate the desired Session Key
• Decrypt data message with the Session Key
• If the decryption result is ok,
use the new session key to send message.

FIGURE 3. Proposed session key update protocol with whitelist attribute

Protocol 5 Master Key Update: From RTU and IED to master station
(1) Receive the encrypted message (c).
(2) Divide c into c$_3$ and c$_4$
(3) Decrypt Master Key Update Code with the master key from c$_4$.

$$C_{mku} = D_{mk}(c_4)) \tag{11}$$

(4) Verify the Master Key Update Code.
(5) If verify is success, Decrypt New Master Key with the Session Key.

$$I_{sk} = D_{mk}(c_2) \tag{12}$$

(6) If the decryption is success, use the New Master Key to send new session key.

5. **Evaluation.** The proposed key management scheme is analyzed under this environment Crypto++ 5.6.0 benchmarks with ECC X.509.v3 selected [10], [11]. Run time of AES-128/CBC: 9 s.

A comparison between the proposed key management scheme and the key management scheme in [8], [9] is summarized as in Table 1. The Number of required communication in the session key update phase has dropped from 2 to 1, which has decreased 50% communication quantity for key updating.

Table 1. Comparison between proposed key management scheme and other key management scheme

Parameter	The proposed scheme	Scheme in [8]	Scheme in [9]
Initiator of the key update phases	RTUs or IEDs station	Master station	Master station
Generator of the session key	Master station and RTUs or IEDs station	Master station	RTUs or IEDs station
Number of required communication in the session key update phase	1	2	3
Number of the stored key in each RTU or IED	2	2	2
Number of the stored key in master station for n RTUs or IEDs	n+1	n+1	n+1

5.1. **Energy consumption evaluation.** From previous studies [12], [13] [14] [15]and [16]the energy consumption the transmitting and receiving between master station and RTU or IED can be estimated by computing n bits over a distance d as follows equations:

$$E_T = n(E_elec + E_amp) \tag{13}$$

$$E_R = nE_elec \tag{14}$$

$$WhereE_amp = {}_fd^2whend = 50m \tag{15}$$

The typical values for E$_{elec}$, $_f$, $_m$ and d$_0$ are 50 nJ/bits for a 1 Mbps transceiver, 10 pJ/bit/m2, 0.0013 pJ/bit/m^4 and 86.2 m [12], [13] and [14]. The d=50m is assumed and the consumption of energy for key update session is computed and summarized in table 2. The proposed scheme has reduced at least 40% energy consumption, from 16J or 22.4J in previous schemes to 9.6J [3], [7], [8] , [9] and [10].

5.2. **Traffic evaluation.** The proposed key management scheme only needs one communication to finish session key update and master key update, which has reduced the traffic between master station and RTU or IED in a great number. And furthermore, the message has combined the key update message with the sensor data message together, which can also make the traffic less than other proposal. From table 1, the length of

Table 2. Comparison between proposed key management scheme and other key management scheme

Reference	This paper		[9]		[8]		[3], [7] and [10]	
	# of bits	Energy consumption (μJ)	# of bits	Energy consumption (μJ)	# of bits	Energy consumption (μJ)	# of bits	Energy consumption (μJ)
Link 1	128	9.6	128	6.4	128	6.4	128	9.6
Link 2	-	-	128	9.6	128	9.6	128	6.4
Link 3	-	-	-	-	128	6.4	-	-
Total	128	9.6	256	16	384	22.4	256	16

communication bits is 50% less than proposal in [9], from 256 bits to 128 bits in each update.

5.3. **QoS evaluation.** The evaluation and prediction of QoS for SCADA system has several different proposals. We use the common method in article [8] and [9].

The QoS of SCADA is defined as follows:

$$QoS = PI + SI = 1 - \frac{(k/t_d)}{T} + e^{(-\lambda t_d)} \tag{16}$$

$$PI = \frac{T - (k/(t_d))}{T} = 1 - \frac{(k/t_d)}{T} \tag{17}$$

$$SI = e^{-t_d} \tag{18}$$

where PI and SI show the performance index and security index respectively. The PI is determined based on the communication delay time of the session key update phase. The PI and SI are computed based on Eq.(17) and (18). T and t$_d$ denote the communication period and key distribution period respectively in SCADA networks and k is a constant. $\lambda > 0$ is Poisson process rate.

The communication period and key distribution period t$_d$ has decreased considerably, near 50%, in the proposed scheme. So the SI increases exponentially while PI decreases linearly. So the QoS is still improved. Because the decreasing range of t$_d$ is larger, so the QoS is better than other proposals.

6. **Conclusions.** In modern industries the security of SCADA networks is a crucial part for the whole fundamental infrastructures. This paper presents a new scheme for key management with whitelist attribute. From the evaluation result, the traffic and energy consumption of the session key update phase and master key update phase has dropped, while the QoS increases.In this scheme, the computational cost in the master station and RTU or IED are increased, which will be compensated by the increasing hardware calculation speed of processors in RTU or IED. In developing this protocol, the following areas of future related work have been identified: decrease the scheme computational consummation, hardware implement, and security weakness evaluation.

REFERENCES

[1] K. Curtis, *A DNP3 protocol primer*, Technical report, DNP Users Group, 2005.

[2] B. Cai, Y. Liu, Z. Liu, F. Wang, X. Tian, Y.Zhang, Development of an automatic subsea blowout preventer stack control system using PLC based SCADA, *ISA Transactions*, vol.51, pp.198–207, 2012.

[3] D. Choi, H. Kim , D. Won, S. Kim, Advanced key management architecture for SCADA communications. *IEEE Transactions on Power Delivery*, vol.24, no.3, pp.1154C-1163, 2009.

[4] E, Knapp, *Industrial Network Security*, Syngress, pp.7-20,2011.

[5] C. Beaver, D.Gallup, W. Neumann, M. Torgerson, *Key management for SCADA*, Technical report, Sandia, 2002.

[6] Dawson R, Boyd C, Dawson E, Nieto J. SKMA, a key management architecture for SCADA systems, *Proceedings of the fourth Australasian information security workshop*, pp.138C192, 2006.

[7] D. Choi, S. Lee, D. Won, S. Kim, Efficient secure group communications for SCADA, *IEEE Transactions on Power Delivery*, vol.25, no.2, pp.714-722, 2010.

[8] D. Kang, J. Lee, B. Kim, D. Hur, Proposal strategies of key management for data encryption in SCADA network of electric power systems, *International Journal of Electrical Power & Energy Systems*, vol.39, no.9, pp.1521-1526, 2011.

[9] A. Rezai, P. Keshavarzi, Z. Moravej, Secure SCADA communication by using a modified key management scheme, *ISA Transactions*, vol.52, pp.517C524, 2013.

[10] D. Choi, H. Jeong, D. Won, S. Kim, Hybrid key management architecture for robust SCADA systems, *Journal of Information Science and Engineering*, vol.29, no.2, pp.281C298, 2013.

[11] Information on *http://www.cryptopp.com/benchmarks.html*

[12] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, An application-specific protocol architecture for wireless micro sensor networks, *IEEE Transactions on Wireless Communications*, vol.1, no.4, pp.660C670, 2002.

[13] A. Ahmad, H. Shi, Y. Shang, A survey on network protocols for wireless sensor networks, *ITR03 Proceedings of the international conference on information technology: research and education*, pp.301C5, 2003.

[14] H. Alzaid, D. Park, J. J. H. Gonzalez,E. Foo, Mitigating sandwich attacks against a secure key management scheme in wireless sensor networks for PCS/SCADA, *Proceedings of the 24th international conference on Advanced Information Networking and Applications*, pp.859C865, 2010.

[15] M. Nutzinger, Real-time Attacks on Audio Steganography, *Journal of Information Hiding and Multimedia Signal Processing*, vol.3, no.1, 2012.

[16] Y. Liu, C. Chang, C. Sun, A Secure and Efficient Scheme for Digital Gift Certificates, *Journal of Information Hiding and Multimedia Signal Processing*, vol 6, no.3, 2015.