www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 12 Dec,2013 Page No. 3534-3537

A Trust System for Broadcast Communications in SCADA

Manoj B C[1],

[1] Department of Computer Science
SCT College of Engineering
manoj9444@gmail.com

Abstract: ***Modern industrial facilities have command and control systems. These industrial command and control systems are commonly called supervisory control and data acquisition (SCADA). In the past, SCADA system has the closed operating environment, so this system was designed without security functionality. These days, as a demand for connecting the SCADA system to the open network increases, the study of SCADA system security is an issue. A key-management scheme is essential for secure SCADA communications. In this paper, ASKMA+TS which is a more efficient scheme that decreases the computational cost for multicast communication is introduced. ASKMA+TS reduce the number of keys to be stored in a remote terminal unit and provide multicast and broadcast communications. The last session discusses the use of a communications network security device, called a trust system, to enhance supervisory control and data-acquisition (SCADA) security. The major goal of the trust system is to increase security with minimal impact on existing utility communication systems.***

.

Keywords: *Computer Networks, SCADA (supervisory control and data-acquisition), Key Management, and KDC (key distribution Center).*

1. Introduction

MODERN industrial facilities, such as oil refineries, chemical factories, electric power generation plants, and manufacturing facilities have command and control systems. These industrial command and control systems are commonly called supervisory control and data acquisition (SCADA). In the past, the SCADA system has the closed operating environment, so this system was designed without security functionality. These days, as a demand for connecting the SCADA system to the open network increases, the SCADA system has been exposed to a wide range of network security problems. If the SCADA system is damaged from the attacks, this system can have a widespread negative effect to society. To prevent the attacks, many researchers have been studying the security of SCADA system. Many researchers have proposed key-management schemes for SCADA. A key establishment for SCADA systems (SKE) [2] and the SCADA key-management architecture (SKMA) [3] were proposed. Recently, ASKMA (advanced SKMA) [1] was proposed. While SKE [2] and SKMA [3] do not meet the security requirements, ASKMA [1] satisfies the security needs. It supports message broadcasting and secure communications. Although the overall performance of ASKMA [1] has many advantages compared to previous studies, it can be less efficient during the multicast communication process. Therefore, we divide the key structure into two classes, applying the Iolus framework [10] and construct each class as a logical key hierarchy (LKH) structure [9]. Through this key structure, ASKMA+TS which is a more efficient key-management scheme supporting efficient multicast communication by considering the number of keys to be stored in a remote terminal unit (RTU). Trust System is a communication security device, with firewall and intrusion detection capabilities, designed for use with time-critical network systems [3]. A trust system can perform at or near the real-time requirements that the supervisory control and data acquisition (SCADA) network requires even with the overhead of TCP/IP and UDP/IP communications, Internet Protocol Security (IPSec) encryption, firewall rules, format check, and access control functions. The goal is to both enhance security in traditional systems and to facilitate information sharing between regional utilities. The original trust system only had an active mode router-based implementation. Here introduce tunnel/gateway mode trust system to greatly add to the range of situations where security can be added to existing SCADA systems. The new trust system implementations allow firewall and intrusion detection security to be embedded through tunneled connections when SCADA traffic must pass through the Internet or other unsecured networks.

2. System Structure

Most SCADA systems have a hierarchical structure. The communication type of SCADA systems is a master-slave structure. Fig. 1 shows the simplified architecture of a SCADA system. A SCADA system consists of three types of communication equipment: 1) human–machine interface (HMI); 2) master terminal unit (MTU); and 3) the remote terminal unit (RTU). The explanation for each device is as

follows.

• HMI is an interface for the SCADA system operator. The HMI usually supports a graphic interface [3].

• MTU provides supervisory control of RTUs. This device is a root node of the SCADA system architecture. The MTUs have reasonable computational resources as a desktop computer [1].

• RTU is a device composed of sensors that are used for data acquisition, a component that carries out communications and a component responsible for executing instructions coming from the MTU.

The RTU has limited memory and processing power [1]. SCADA system network topology is static. The communication paths between nodes are known in advance, because there are few network changes. Communication occurs between HMI and MTU, MTU and SUB-MTU, two SUB-MTUs, MTU and RTU, SUB-MTU and RTU, and two RTUs. The HMI-MTU communication can be provided by the web service easily due to the use of transmission control protocol/Internet protocol (TCP/IP)-based protocols. Moreover, HMI-MTU communication has fewer resource limitations than the other communication.

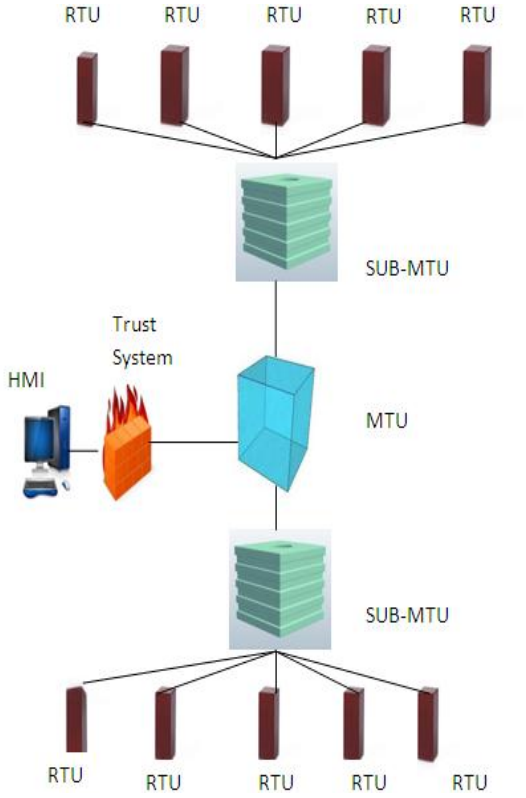

Fig: 1 SCADA System Architecture

3. Proposed Key Management Protocol (ASKMA++)

3.1 Joint protocol

Fig 2 shows where a new SUB-MTU joining at q=8 and h=3.

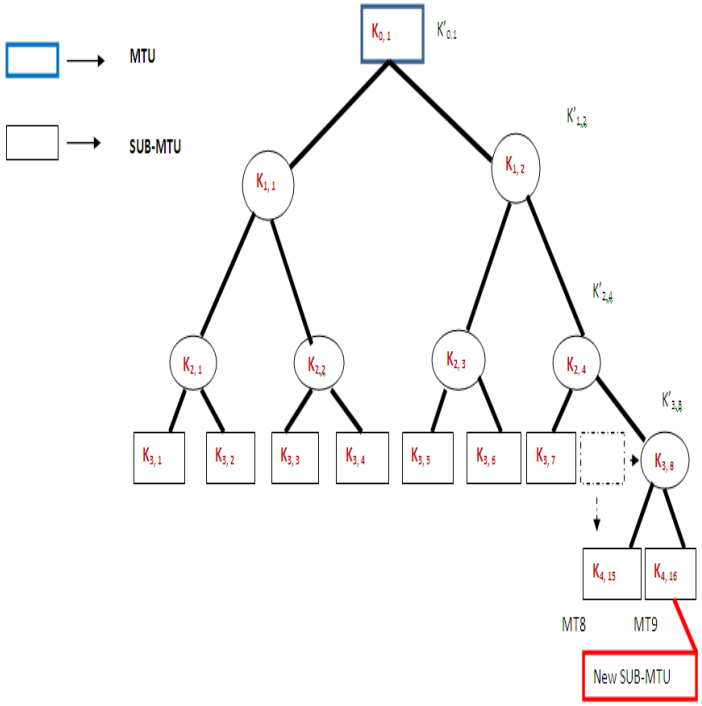

Fig:2 Joint Protocol

1) MT_8: MT_8 change a key $K_{3,8}$ into a key $K_{4,15}$.
2) KDC: KDC generates a MT_9's key $K_{4,16}$ by running a key generating algorithm K gen (1^b).
3) KDC: The KDC updates all $K_{i,j}$ with $K'_{i,j}=H(K_{i+1,2j-1}, K_{i+1,2j})$.
4) KDC: SUB-MTUs in $GM_{K1,1}$: KDC computes $E_{K1,1}(K'_{0,1})$ and then send to these SUB-MTUs.
5) KDC: SUB-MTUs in $GM_{K2,3}$: KDC computes $E_{K2,3}(K'_{0,1}, K'_{1,2})$ and then send to these SUB-MTUs
6) KDC: SUB-MTUs in $GM_{K3,7}$: KDC computes $E_{K3,7}(K'_{0,1}, K'_{1,2}, K'_{2,4})$ and then send to these SUB-MTUs.
7) KDC: SUB-MTUs in $GM_{K4,15}$: KDC computes $E_{K4,15}(K'_{0,1}, K'_{1,2}, K'_{2,4}, K'_{3,8})$ and then send to these SUB-MTUs.
8) MT9: KDC Computes $E_{K4,16}(K'_{0,1}, K'_{1,2}, K'_{2,4}, K'_{3,8})$ and then send to these SUB-MTUs

3.2 Leave protocol

1) KDC: The leaving SUB-MTU MT_8 is deleted from the MT set key structure. Then MT_7 will be the parent.
2) MT7: MT changes a key K_{37} into a key K_{24}.
3) KDC: The KDC updates all Ki, j with K'i, j=H ($K_{i+1,2j-1}$, $K_{i+1,2j}$).
4) KDC: SUB-MTUs in $GM_{K1,1}$: KDC computes $E_{K1,1}(K'_{0,1})$ and then send to these SUB-MTUs.
5) KDC: SUB-MTUs in $GM_{K2,3}$: KDC computes $E_{K2,3}(K'_{0,1}, K'_{1,2})$ and then send to these SUB-MTUs.
6) MT7: KDC computes $E_{K2,4}(K'_{0,1}, K'_{1,2})$ and then sends to these SUB-MTUs.

Fig 3 shows where a new SUB-MTU leaving

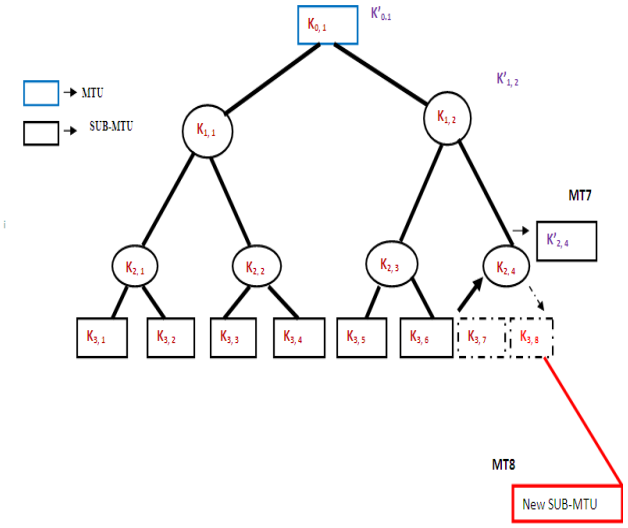

Fig: 3 Leave Protocol

3.3 Data Encryption

SCADA supports both unicast and multicast communication. In this scheme encryption key should be refreshed regularly. For that, encrypted keys are replaced with new keys in each session. Therefore, our mechanism uses a time-variant parameter (TVP) that is a combination of time stamp and sequence number. The MTU encrypts the message by using a random key & random key is encrypted with a session key shared between MTU & SUB-MTU. When SUB-MTU receives the encrypted messages & the encrypted random key, the SUB-MTU decrypts the random key & re-encrypt with a session key that is shared with the receivers. When the receiver receives the encrypted message and the encrypted random key, the receiver decrypts the random key & multicast the random key to its subgroup. Therefore, only the members of the subgroup are able to decrypt the messages with the random key.

3.4 Trust System

A trust system is a communication security device, with firewall & intrusion detection capabilities, designed for use with time- critical network systems.

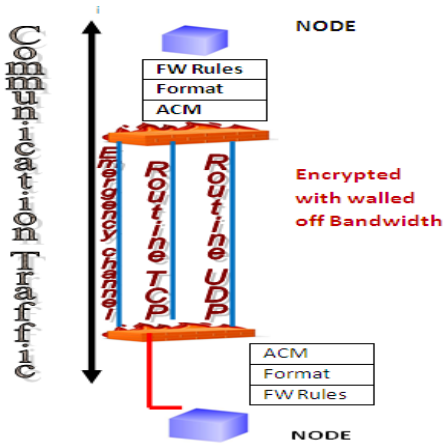

Fig: 4 Trust System in tunnel mode

The new trust system implementation allows firewall & intrusion detection security to be embedded through tunnelled connections when SCADA traffic must pass through the internet or other unsecured networks. The trust system may be implemented in tunnel mode as depicted in fig: 4. In tunnel mode the trust system routers provide firewall and other security features for the nodes behind them. They also create an encryption gateway between themselves to protect communications between trust systems. The advantage of tunnel implementation is that traffic can be protected & encrypted when travelling outside of a utility's network. The disadvantage is that tunnelling between trust systems. path for the transmission due to congestion is provided.

4. Comparison

5. TABLE I
SECURITY COMPARISON WITH EXISTING SYSTEMS & PROPOSAL

Security Requirements	SKE	SKMA	ASKMA	ASKMA+	ASKMA+TS
Broadcasting	Impossible	Impossible	possible	possible	possible
Multicasting	Impossible	Impossible	possible	possible	possible
Key Freshness	possible	possible	possible	possible	possible

In the SCADA system, multicast communication from an MTU to multiple RTUs is needed for efficient communication. Existing key-management schemes do not support multicasting or can be less efficient during the multicast communication. In our scheme, multicast communication is achieved by using Advanced key management technique and a trust system.

5. Conclusions

SCADA system is a significantly important system used in national infrastructure such as electric grids, water supplies, and pipelines. However, SCADA systems have security vulnerabilities. Any faults or damage to the SCADA system can affect society severely. Thus, the study of the SCADA system security is essential. Recently, in AKMA [1], the authors proposed advanced key-management architecture for secure SCADA communications. They redefined security requirements for a SCADA system, analyzed the previous key-management protocols, and proposed a new key-management scheme suitable for secure SCADA communications. While SKE and SKMA do not meet the security requirements, AKMA satisfies the security needs, in that it supports message broadcasting and secure communications. Although the overall performance of ASKMA has many advantages compared to previous studies, it can be less efficient during the multicast communication process. Therefore ASKMA+TS that is more efficient and secure compared to existing schemes were proposed. ASKMA+TS provide multicast and broadcast communication for efficient and stable operation of SCADA systems.

References

[1] D. Choi, H. Kim, D. Won, and S. Kim, "Advanced key management architecture for secure SCADA communications," *IEEE Trans. PowerDel.*, vol. 24, no. 3, pp. 1154–1163, Jul. 2009

[2] C. Beaver, D. Gallup, W. Neumann, and M. Torgerson, Key Management for SCADA. 2002. [Online]. Available:http://www.sandia.org/scada/documnets/013252.pdf Travel, P. 2007 Modeling and Simulation Design. AK Peters Ltd

[3] Sannella, M. J. 1994 Constraint Satisfaction and Debugging for Interactive User Interfaces. Doctoral Thesis. UMI Order Number: UMI Order No. GAX95-09398., University of Washington.

[4] M. Balenson, D. A. McGrew, and A. T. Sherman, "Key management for large dynamic groups: One-way function trees and amortized initialization," in *IETF Internet Draft*, 2000.

[5] Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan, Technical Report 12–1 Draft 5 revision 3 Amer. Gas Assoc., 2005. [Online]. Available: http://www.gtiservice.org/security.

[6] C. K.Wong, H. Gouda, and S. S. Lam, "Secure group communications using key graphs," in Proc. ACMSIGCOMM Conf. Applications, Technologies, Architectures, and Protocols for Computer Communication,1998, pp. 68–79.

[7] S., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", Work in Progress.

[8] R.E Securing SCADA Systems by Ronald L. Krutz. (Wiley Publishing, inc).

[9] Doc V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," in *Computer. Security*, Mar. 2006, vol. 25, pp. 498–506.

[10] K. C. Chan and S. H. Chan, "Key management approaches to offer data confidentiality for secure multicast," *IEEE Netw. Commun. Lett.* vol.17, no. 5, pp. 30–39, Sep./Oct. 2003.

[11] S. Mittra, "Iolus: A framework for Baratz, Doc V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," in *Computer. Security*, Mar. 2006, vol. 25, pp. 498–506.
.

Author Profile

Manoj B.C received the B.E and M.E. degrees in Computer Science Engineering from C.S.I Institute of Technology & Noorul Islam College of Engineering in 2003 and 2006, respectively. Currently, he is doing research in Anna University Chennai, in the field of network security.