National Conference on New Technologies in Electrical and Computer Engineering
17 January 2018 - Iran, Isfahan

High-Performance Key Management Scheme for Secure SCADA Communication

Abdalhossein Rezai
ACECR Institute of Higher Education, Isfahan Branch, Isfahan, 84175-443, Iran
rezaie@acecr.ac.ir

Parviz Keshavarzi
Electrical and Computer Engineering Faculty, Semnan University
Semnan, 3513119111- Iran
pkeshavarzi@semnan.ac.ir

Zahra Moravej
Electrical and Computer Engineering Faculty, Semnan University
Semnan, 3513119111- Iran
zmoravej@semnan.ac.ir

Abstract—**SCADA networks have important role in modern industries and infrastructures. Thus, secure SCADA communication is important for industries and infrastructures. Key management scheme is essential for secure SCADA communication. This paper presents and evaluates new and high-performance key management scheme by using CCS scalar multiplication and compact SD modular multiplication for encryption and decryption. The results demonstrate that the proposed CCS compact SD key management scheme provides an improvement in terms of the number of required multiplication steps compared to other key management schemes.**

Keywords- SCADA; security; key management; compact SD; modular multiplication

I. INTRODUCTION

Supervisory Control And Data Acquisition (SCADA) networks have important role in modern industries and infrastructures such as power generation systems, gas and oil [1, 2, 3, 4]. On the other hand, it is necessary for modern industries and infrastructures to utilize the open access networks such as Internet for today's comparative markets [1, 2, 3, 4]. As a result, the security plays an important role in today's SCADA networks [1, 2, 3, 4]. Key management schemes play important role in secure communication [2, 5, 6].

Recently several key management schemes have been proposed to increase the security of SCADA networks [1-4, 7-13]. A good review on key management schemes is presented in [1]. Among them, Rezai et al. [3] key management scheme is an efficient key management scheme for radial SCADA networks. They reduce the network traffic by reducing the communication links. However, this key management scheme is suitable, but the performance of this key management scheme can be improved.

In this paper, the performance of Rezai et al. [3] key management is improved by increasing the performance of data encryption and decryption required in key management scheme. Our analysis show that the proposed scheme provide an improvement in key management scheme in terms of the required multiplication steps.

The rest of this paper is organized as follows. Background of the SCADA networks is described in section II. Section III presents the developed key management scheme. Section IV compares the developed key management scheme to other key management schemes. Conclusion is given in section V.

II. BACKGROUND

SCADA networks are computer-based networks that utilize to control modern infrastructures and industries [3, 4]. Figure 1 illustrates the simplified SCADA network [3].

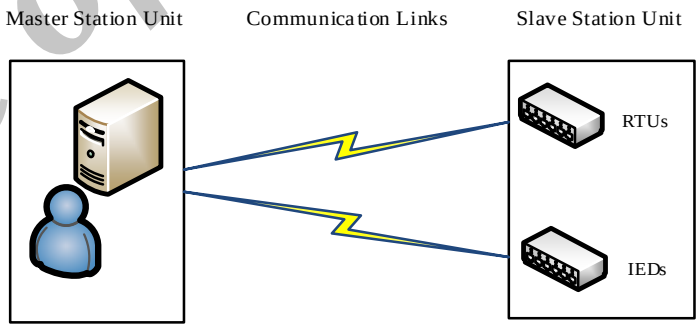

Figure 1. The simplified SCADA network [3]

As it is shown in this figure, SCADA networks composed of three sections. Master Station Units (MSU), Communication Links (CLs), and Slave Station Unit (SSU). It should be noted that the SSU has resource limitation and the CL has security issue. As a result, low complexity cryptography system is required for secure SCADA communication. For secure SCADA communication, the security devices should be installed on inlet or outlet of MSU and SSUs. Figure 2 illustrates a secure SCADA network [1, 3, 4].

Archive of SID

www.SID.ir

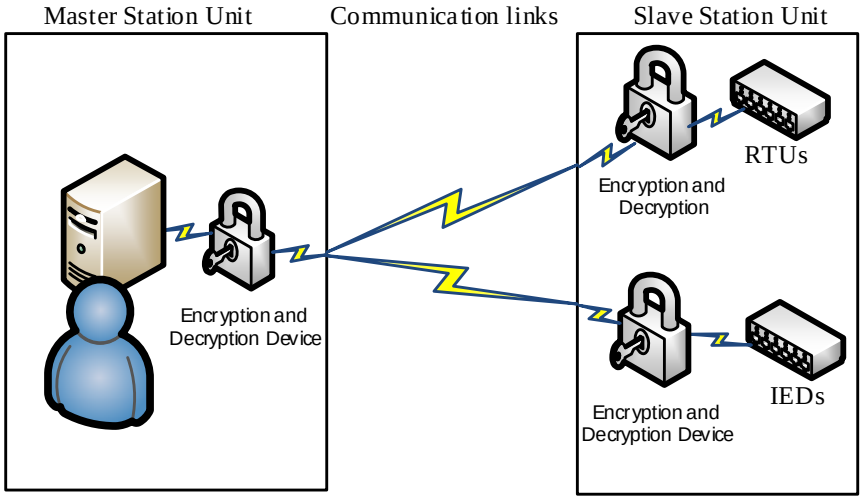

Figure 2. A secure SCADA network [3]

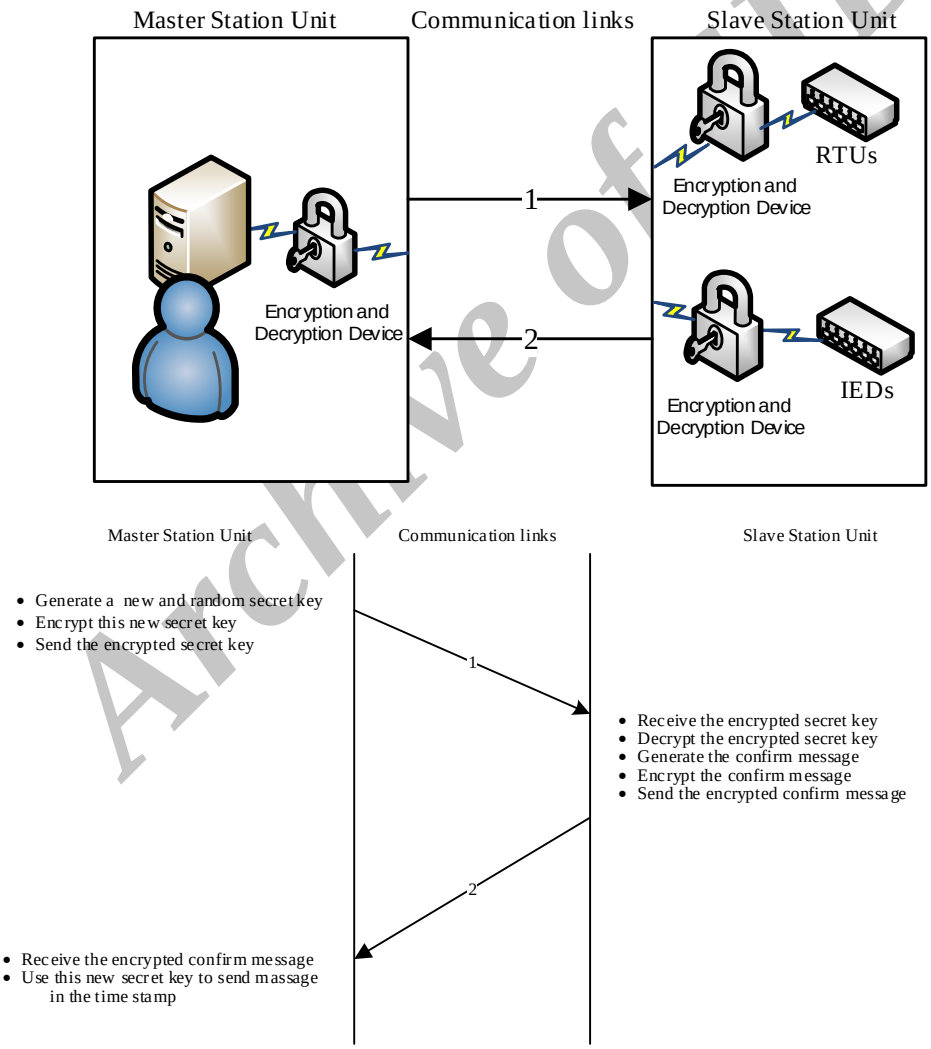

Figure 3. Key management scheme in [3]

Archive of SID

www.SID.ir

III. THE PROPOSED KEY MANGEMENT SCHEME

Key management scheme is essential for secure SCADA communication. There are several key management schemes for secure SCADA communication [1-4, 7-13]. One of the recent key management scheme is Rezai et al. [3] key management scheme. Figure 3 illustrates this key management scheme.

As it is shown in this figure, the master station is initiator in communication in this key management scheme. New secure key is generated in MSU side based on a refresh time. Moreover, the MSU and SSU tasks are shown in this figure. Most important task in this key management scheme is encryption and decryption. Moreover, the key management in [3], utilized Elliptic Curve Cryptosystem (ECC) for encryption and decryption. The main operation in ECCs is scalar multiplication. Figure 4 illustrates the three-level model for elliptic curve scalar multiplication [14, 15].

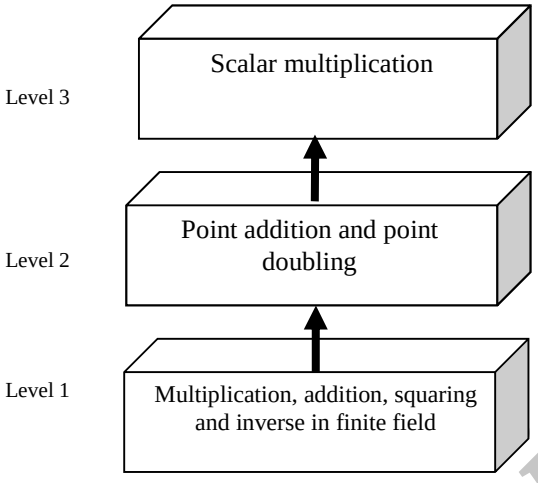

Figure 4. The three-level model for scalar multiplication [14]

As it is shown in this figure, the scalar multiplication is performed using point operations, point addition and point doubling. The basic operation for performing point operation is finite field multiplication or modular multiplication [14, 15]. This key management scheme utilized binary method for scalar multiplication and Montgomery modular multiplication for finite field multiplication [1, 3].

On the other hand, we recently developed the compact SD modular multiplication [16-18], and the CCS scalar multiplication [14] that are efficient modular multiplication, and scalar multiplication, respectively.

In addition, the delay in data processing in SCADA can cause serious concerns. Thus, the speed of SCADA networks has an important issue.

In this section we propose to utilize the CCS scalar multiplication to perform the scalar multiplication, and utilize compact SD modular multiplication to perform finite field multiplication as structural units.

IV. RESULTS AND COMPARISON

The required point addition and point doubling in ECC are 16 and 8 finite field multiplications in projective coordinate. The number of required multiplication steps in modular multiplication is calculated as follows:

$$S=(A_1\times A_2+B_1\times B_2)\times C \quad (1)$$

Where S, A_1, A_2, B_1, B_2, and C denote the number of required multiplication steps, point addition/subtraction operation, finite field operation in each point addition/subtraction operation, point doubling operation, finite field operation in each point doubling operation, and loop iterations in scalar multiplication, respectively.

Table 1 shows the number of required point addition/subtraction in encryption and decryption in GF(p=256).

Table 1: The number of required point addition/subtraction in encryption and decryption in GF(p=256)

Scalar multiplication method	Operation		
	encryption	decryption	summation
Binary	256	128	384
CCS	42	22	64

It should be noted that the authors in [16] show that the number of required multiplication steps is reduced to n/3 for n-bit modulus in compact SD modular multiplication compared to Montgomery modular multiplication.

Table 2 summarized the number of required multiplication steps for two scalar multiplications (binary and CCS method), where using Montgomery modular multiplication and compact SD modular multiplication for finite field multiplication based on table 1.

Table 2: The number of required multiplication steps for two scalar multiplications

Scalar multiplication method	Finite field multiplication	
	Montgomery	Compact SD
Binary	3145728	1048576
CCS	1835008	611670

Based on our results, the number of required multiplication steps in the proposed CCS compact SD key management are reduced by about 66%, 41%, and 80% compared to CCS Montgomery kay management schem, Binary compact SD key management scheme, and binary Montgomery key management scheme, respectively.

Archive of SID

www.SID.ir

V. CONCLUSION

SCADA networks have important role in modern infrastructures and industries. Security issue plays an important role in this network. Key management scheme is essential to secure communication in SCADA networks. This paper presented and evaluated high-performance key management scheme by using CCS scalar multiplication and compact SD modular multiplication. The evaluation results show that the developed key management scheme provides an improvement in comparison with other key management schemes in terms of the number of required multiplication steps.

REFERENCES

[1] A. Rezai, P. Keshavarzi, and Z. Moravej, "Key management issue in SCADA networks: a review," Engineering science and technology, an international journal, vol. 20 , pp. 354–363, 2017.

[2] A. Rezai, P. Keshavarzi, and Z. Moravej, "Advance hybrid key management architecture for SCADA network security," Security and communication networks, vol. 9, pp. 4358–4368, 2016.

[3] A. Rezai, P. Keshavarzi, and Z. Moravej, "Secure SCADA communication by using a modified key management scheme," ISA transactions, vol. 52, pp. 517-524, 2013.

[4] A. Rezai, P. Keshavarzi, and Z. Moravej, "A New Key Management Scheme for SCADA Network," In proc. 2nd International Symposium on Computing in Science & Engineering (ISCSE 2011), pp. 373-378, 2011.

[5] R. Khalilian, A. Rezai, and F. Mesrinejad, "Secure Wireless Body Area Network (WBAN) communication method using new random key management scheme," International journal of security and its applications, vol. 10, pp. 13-22, 2016.

[6] R. Khalilian, A. Rezai, and E. Abedini, "An efficient method to improve WBAN security," Advanced science and technology letters, vol. 64, pp. 43-46, 2014.

[7] D. Choi, H. Jeong, D. Won, and S. Kim, "Hybrid key management architecture for robust SCADA systems," Journal of information science and engineering, vol.29, pp. 281–298, 2013.

[8] R. Dawson, C. Boyd, E. Dawson, and J. Nieto, SKMA, "A key management architecture for SCADA systems," In: Proc. Australasian Workshops on Grid Computing and E-research, pp. 183–192, 2006.

[9] C. Beaver, D. Gallup, W. Neumann, and M. Torgerson, "Key Management for SCADA," SAND Report SAND2001-3252., 2002.

[10] D. Choi, H. Kim, D. Won, and S. Kim, "Advanced key management architecture for secure SCADA communications," IEEE transactions on power delevery, vol. 24, pp. 1154–1163, 2009.

[11] R. Jiang, R. Lu, C. Lai, J. Luo, and X. Shen, "Robust group key management with revocation and collusion resistance for SCADA in smart grid," In: Proc. IEEE globe Commun. Conf., pp. 802–807, 2013.

[12] R. Jiang, R. Lu, J. Luo, C. Lai, and X. Shen, "Efficient self-healing group key management with dynamic revocation and collusion resistance for SCADA in smart grid," Security and communication networks, vol. 8, pp. 1026–1039, 2015.

[13] D. Kang, J. Lee, B. Kim, and 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. 33, pp. 1521–1526, 2011.

[14] A. Rezai, and P. Keshavarzi, "A New Finite Field Multiplication Algorithm to Improve Elliptic Curve Cryptosystem Implementations," Journal of information systems and telecommunication, vol. 1, pp. 119-129, 2013.

[15] A. Rezai, and P. Keshavarzi, "High-performance implementation approach of elliptic curve cryptosystem for wireless network applications," In proc. The International Conference on Consumer Electronics, Communications and Networks (CECNet 2011), pp. 1323-1327, 2011.

[16] A. Rezai, and P. Keshavarzi, "Compact SD: A new encoding algorithm and its application in multiplication," International journal of computer mathematics, vol. 94, pp.554-569, 2017.

[17] A. Rezai, and P. Keshavarzi, "High-performance scalable architecture for modular multiplication using a new digit-serial computation," Microelectronics journal, vol. 55, pp. 169–178, 2016.

[18] A. Rezai, and P. Keshavarzi, "High-throughput modular multiplication and exponentiation algorithms using multibit-scan–multibit-shift technique," IEEE transactions on Very Large Scale Integration (VLSI) systems, vol. 23, pp. 1710 – 1719, 2015.

Archive of SID

www.SID.ir