Engineering Science and Technology, an International Journal xxx (2016) xxx–xxx

HOSTED BY

ELSEVIER

Contents lists available at ScienceDirect

Engineering Science and Technology, an International Journal

journal homepage: www.elsevier.com/locate/jestch

Review

# Key management issue in SCADA networks: A review

Abdalhossein Rezai [a,*], Parviz Keshavarzi [b], Zahra Moravej [b]

[a] Academic Center for Education, Culture and Research (ACECR), Isfahan University of Technology (IUT) branch, Isfahan, Iran
[b] Electrical and Computer Engineering Faculty, Semnan University, Semnan, Iran

ARTICLE INFO

*Article history:*
Received 28 April 2016
Revised 12 August 2016
Accepted 15 August 2016
Available online xxxx

*Keywords:*
Critical infrastructure security
Key management scheme
Network security
Power system security
SCADA network

ABSTRACT

Supervisory Control And Data Acquisition (SCADA) networks have a vital role in Critical Infrastructures (CIs) such as public transports, power generation systems, gas, water and oil industries, so that there are concerns on security issues in these networks. The utilized Remote Terminal Units (RTUs) and Intelligence Electronic Devices (IEDs) in these networks have resource limitations, which make security applications a challenging issue. Efficient key management schemes are required besides lightweight ciphers for securing the SCADA communications. Many key management schemes have been developed to address the tradeoff between SCADA constrain and security, but which scheme is the most effective is still debatable. This paper presents a review of the existing key management schemes in SCADA networks, which provides directions for further researches in this field.


**Contents**

1. Introduction . . . 00
2. SCADA network architecture . . . 00
3. Security threats in SCADA networks . . . 00
3.1. Loss of availability . . . 00
3.2. Loss of integrity . . . 00
3.3. Loss of confidentiality . . . 00
4. Existing key management schemes/architectures . . . 00
4.1. Literatures review . . . 00
4.1.1. Centralized key distribution architecture . . . 00
4.1.2. Decentralized key distribution architectures (point-to-point architectures) . . . 00
4.2. Performance evaluation . . . 00
4.3. Open research issues . . . 00
5. Conclusion . . . 00
References . . . 00

## 1. Introduction

Supervisory Control And Data Acquisition (SCADA) networks play a vital role in modern Critical Infrastructures (CIs) such as power generation systems, water plants, public transports, gas, and oil industries [59,6,23,25,24,5]. Conventional SCADA networks have been initially designed to maximize functionality in closed operating environments. As a result, a little attention has been paid to the security [29,46,8,28,30,42,51,37,31].

In today's competitive markets, it is essential for infrastructures and industries to connect to the open access networks such as Internet [5,51,31,61,15,55,10]. Thus, modern SCADA networks have been exposed to a wide range of network security problems [46,37,55]. Therefore the security of modern SCADA networks is a challenging issue [5,51,31,61,55,52].

Due to many specific characteristics of SCADA networks such as resource limitations in Remote Terminal Units (RTUs) and

* Corresponding author.
*E-mail addresses:* rezaie@acecr.ac.ir (A. Rezai), pkeshavarzi@semnan.ac.ir (P. Keshavarzi), z.moravej@ieee.org (Z. Moravej).
Peer review under responsibility of Karabuk University.

http://dx.doi.org/10.1016/j.jestch.2016.08.011
2215-0986/

**Table 1**
Acronyms in SCADA networks.

| Acronym | Definition |
|---|---|
| ASKMA | Advance SCADA Key Management Architecture |
| BITW | Bump-In-The-Wire |
| C2S | Controller-to-Subordinate |
| CA | Certificate Authority |
| CI | Critical Infrastructure |
| CKD | Centralized Key Distribution |
| DCS | Distributed Control Systems |
| ECC | Elliptic Curve Cryptography |
| GK | General Key |
| GSK | General Seed Key |
| HECC | Hyper Elliptic Curve Cryptosystem |
| HMI | Human Machine Interface |
| IDS | Intrusion Detection System |
| IED | Intelligence Electronic Device |
| IT | Information Technology |
| KDC | Key Distribution Centre |
| LAN | Local Area Network |
| LEN | LENgth of data |
| LiSH | Limited Self-Healing |
| LKH | Logical Key Hierarchy |
| LTK | Long Term Key |
| MAC | Message Authentication Code |
| MSU | Master Station Unit |
| MTU | Master Terminal Unit |
| PKC | Public Key Cryptography |
| PKI | Public Key Infrastructure |
| RI | Random Integer |
| RTU | Remote Terminal Unit |
| SCADA | Supervisory Control And Data Acquisition |
| SKE | SCADA Key Establishment |
| SKMA | SCADA Key Management Architecture |
| SSU | Slave Station Unit |
| TS | Time Stamp |

Intelligence Electronic Devices (IEDs), it is impossible to use general IT techniques for securing SCADA networks [38,14,48]. This issue has been extensively investigated by researchers and professional organizations and several reports and standards have been developed for securing the SCADA communications [9,47,8,1,2,32,4]. In other words, the SCADA communications are vulnerable, which make it prone to several threats. Key management schemes are essential for the secure SCADA communications. However, the utilized key management scheme for a secure application should incorporate authenticity, confidentiality, integrity, scalability, and flexibility [25,51,60].

There are several reviews in literatures related to SCADA networks security [23,25,46,31,39]. Although these review articles are suitable, but there isn't any review article related to key management scheme/architecture in SCADA networks in detail.

Motivated by these facts, this paper presents some of the fundamental aspects of the security in SCADA networks. The focus will be on key management schemes/architectures. Some open research issues related to key management scheme/architecture in SCADA networks are also highlighted. Table 1 summarizes the acronyms used through this paper.

The remaining of this paper is organized as follows: Section 2 briefly describes the SCADA network architecture. Section 3 presents security threats in the SCADA networks. Section 4 provides a literature review of articles related to key management scheme/architecture in SCADA networks. Some important open research issues are also presented in this section. Finally, Section 5 concludes this paper.

## 2. SCADA network architecture

SCADA networks are especial computer-based networks and devices which are designed to monitor and control infrastructures and industries [46,51,38]. In the SCADA networks, data acquisition systems, data transmission systems and Human Machine Interface (HMI) software are integrated for providing the centralized monitoring and control system for processing outputs and inputs. SCADA networks are also utilized for collecting field information, transferring it to a central computer facility, and displaying the information for users graphically or textually. As a result, it allows the users to real time monitor or control an entire network from a remote location. The control of any system, task, or operation can be performed by user commands or automatically [57,36,51]. Fig. 1 shows a simplified SCADA network architecture.

SCADA networks typically consist of software and hardware. Commonly used hardware includes (1) Master Station Unit (MSU) or Master Terminal Unit (MTU), which is placed at a control center, (2) sub-MSUs, (3) geographically distributed field sites consisting of RTUs and IEDs, which monitors sensors and controls actuators, and (4) communication links and equipment [51,52,37,39,19,50]. However, in some SCADA networks, sub-MSUs may not be used. In these cases, the MSU directly connected to each slave station unit, RTU or IED, using communication links [46,51,37,50]. In these cases, slave station units provide a direct interface to control and monitor equipment and sensors. Slave station units may be directly polled and controlled by the MSU or MTU. Moreover, slave station units, in these cases, have local

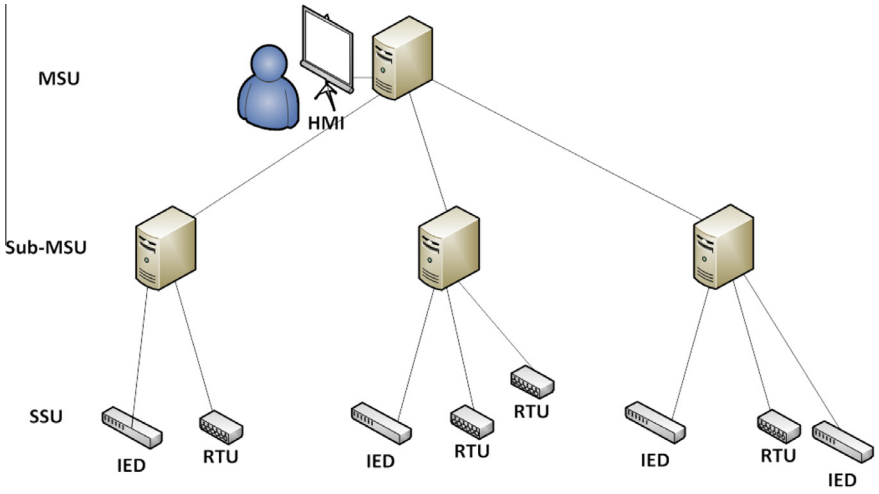


**Fig. 1.** A simplified SCADA network architecture.

Please cite this article in press as: A. Rezai et al., Key management issue in SCADA networks: A review, Eng. Sci. Tech., Int. J. (2016), http://dx.doi.org/10.1016/j.jestch.2016.08.011

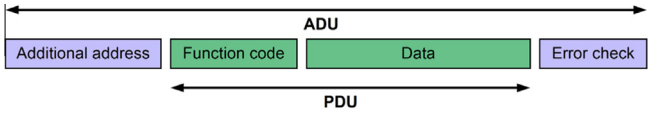


**Fig. 2.** General MODBUS frame [45].

programming, which allows for the slave station units to act without direct instructions from the MSU or MTU [57,36,51].

The MSU or MTU stores and processes the outputs and inputs information of slave station units, RTUs or IEDs, while the slave station units control the local process. The communication links transfer the information. In addition, the software is programmed to indicate the SCADA network what and when should be monitored, what response should be initiated when parameters go outside acceptable values, and what parameter ranges are acceptable [57,36,51].

It should be noted that control networks and systems are very similar in operation, but they have some key differences aspects. One of the key differences is that control systems such as Distributed Control Systems (DCS) are typically located within a more confined factory or plant-centric area in comparison with geographically dispersed SCADA field sites. DCS communications are usually performed by using Local Area Network (LAN) technologies, which are usually high speed and more reliable in comparison with the long-distance communication systems utilized by SCADA networks and systems [57]. In other words, SCADA networks and systems are specifically designed to handle long-distance communication challenges such as data loss and delays posed by the utilized various communication media. Other control networks and systems commonly employ greater degrees of closed loop control than SCADA networks and systems [57]. It is because the control of industrial processes is usually more complicated than the supervisory control of distribution processes [57].

Based on the AGA-12 standard, there are about 200 SCADA protocols. More popular SCADA protocols are MODBUS, DNP3, and IEC 60870-5-101. Note that none of these protocols contain security format [25,26,21]. Fig. 2 shows general MODBUS frame [45].

Shahzad et al. [54] described in detail the SCADA/MODBUS challenges and issues that are commonly used in transmission.

It should be noted that the trend in the modern SCADA networks is leading away from serial communication model towards IP-based open standards [38]. Moreover, wireless communication plays an important role in the modern SCADA networks [6,38,53,34]. Unfortunately, both trends are mainly used for enhancing the efficiency at the expense of the increasing vulnerability of SCADA communications [38].

## 3. Security threats in SCADA networks

Threats in the SCADA networks can be classified into three important types: (1) loss of availability, (2) loss of integrity, and (3) loss of confidentiality [47,17,40,20,16].

### 3.1. Loss of availability

A loss of availability means a disruption of reliable and timely access to systems or data. This can delay or disturb the identification and isolation of faults, and the restoration of power in abnormal conditions, such as power outage. Moreover, it can reduce the efficiency of the power supply chain. Since inefficient security solutions can disrupt time-critical processes and operations in the SCADA networks, the security solution should be efficient to preserve availability [40].

### 3.2. Loss of integrity

This type of threat means unauthorized modification or destruction of information. The loss of integrity can cause serious damages to infrastructures. To protect against insider threat, digital signature and source authentication schemes should be utilized. On the other hand, Message Authentication Codes (MACs) should be utilized to protect against outsider threats [40].

### 3.3. Loss of confidentiality

A loss of confidentiality means unauthorized divulgence of information via eavesdropping. An example of eavesdropping is to violate consumer privacy by eavesdropping on the energy consumption sent from RTUs or IEDs to user. A common method to protect against eavesdropping is encrypting SCADA communications using a secure key [40].

Note that efficient security solutions against these threats require efficient key management schemes [23,51,40,56].

## 4. Existing key management schemes/architectures

During the last decade, several papers related to the key management scheme/architecture in SCADA networks have been published, which can be classified into two important categories: (1) centralized key distribution architecture such as [52,17,20,12,18,33,35,36], and (2) decentralized key distribution architectures or point-to-point architectures such as [51,37,50,22,58].

In the centralized key distribution architecture, the secret key for secure communication is generated by the trusted Key Distribution Centre (KDC), and then distributed between two nodes, which will be communicated with each other [52,17,20,12,18,33].

In the decentralized key distribution architecture, there is no KDC. These architectures are established based on the pre-shared master keys. These keys allow the establishment of session keys [51,37,50].

It should be noted that some key management schemes have been developed, which utilized public key based technique to secure SCADA communications [51,37,50,17,12]. A Public Key Infrastructure (PKI) is defined as a set of securing services, including policies, processes, hardware, and software that use Public Key Cryptography (PKC) to create, manage, distribute, and revoke digital certificates [6,17,56]. In the PKI, two keys are utilized: (1) public key, and (2) private key. While only each node knows its private key, all other nodes can utilize the public key. In addition in PKI, documents issued and signed by a third party, which is named Certificate Authority (CA). The commonly certificate in PKI is X.509 certificate [52,51,17].

Although, the public key based techniques are time-consuming and power-consuming techniques, investigations show that the public key techniques such as Elliptic Curve Cryptography (ECC) are suitable for using in hybrid key management scheme to secure SCADA communication, when there are enough resources [51,17,56]. The public key based technique can be used in both centralized key distribution architectures and the decentralized key distribution architectures as described in next sections. The aim of this section is to provide a brief overview of some of these schemes/architectures, and some important open research issues.

### 4.1. Literatures review

#### 4.1.1. Centralized key distribution architecture

Beaver et al. [12] proposed a SCADA Key Establishment (SKE). The basic SKE communication strategy is a Controller-to-Subordinate (C2S) communication. For example, the MSU-RTU

Please cite this article in press as: A. Rezai et al., Key management issue in SCADA networks: A review, Eng. Sci. Tech., Int. J. (2016), http://dx.doi.org/10.1016/j.jestch.2016.08.011

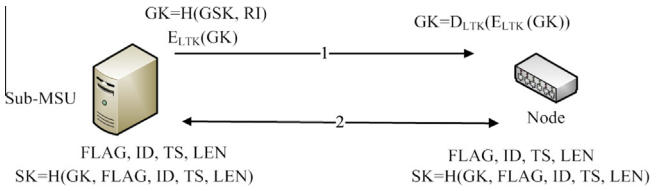


**Fig. 3.** The session key generation process in the SKE [18].

and sub-MSU-RTU communications in the SCADA networks are C2S communication. The SKE utilizes the symmetric cryptosystem for securing the C2S communications. The session key generation process in this scheme contains three types of key: (1) Long Term Key (LTK), (2) General Seed Key (GSK), and (3) General Key (GK). The session key generation process in this scheme is illustrated in Fig. 3 [12,18].

In Fig. 3, two nodes in communications share the LTK that is manually distributed. For example, the sub-MSU randomly generates a 128 bit Random Integer (RI), and after that it generates a GK by hashing the RI and GSK. The GK is encrypted before transmission using the LTK of each RTU or IED. On the other hand, the receiver derives a session key from GK, FLAG, ID, TimeStamp (TS), and LENgth of data (LEN) [12,18].

The SKE also uses the PKC for securing communication between MSU and sub-MSUs. In SKE, the KDC assigns each sub-MSU public/private key pair. After two sub-MSUs communicate in a secure manner, they should give identical secure keys, which play the same role as the GK in symmetric cryptosystems [20,12,18].

Dawson et al. [20] only utilized symmetric cryptosystem for securing SCADA communication. Their SCADA Key Management Architecture (SKMA) utilizes the following set of keys [20,18].

- Long term node-KDC key: This key is manually shared between a node and the KDC.
- Long term node-node key: This key is shared between nodes, which communicate with each other.
- Session key: This key is utilized for the message encryption.

Fig. 4 shows the key establishment protocol in the SKMA between KDC, node A, and node B.

This key establishment protocol is based on ISO 11770-2 mechanism 9 [20,18,33]. In SKMA, a session key is computed using a

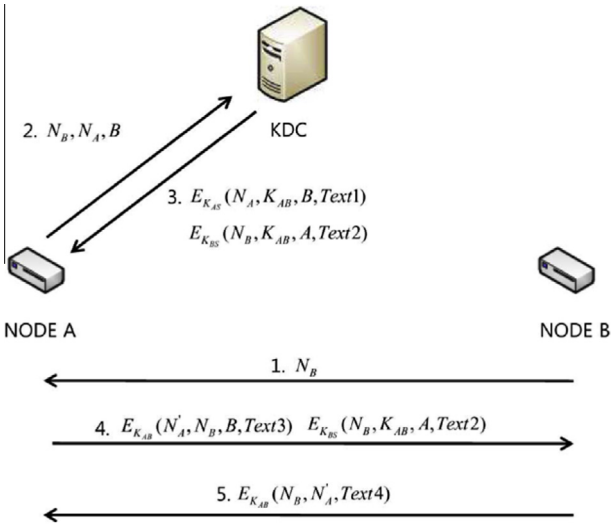


**Fig. 4.** Key establishment protocol in SKMA [20,18].

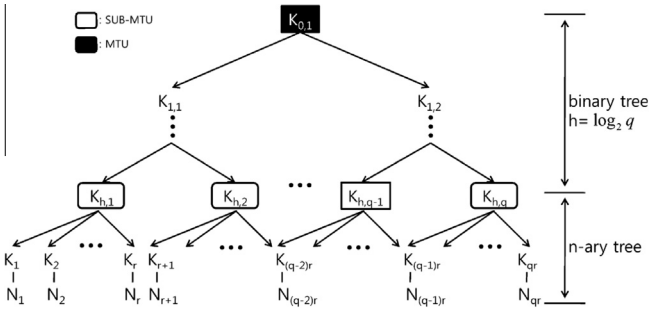


**Fig. 5.** The key management architecture in Choi et al. [18].

pseudorandom function, and encrypted using the node-node key and a timestamp [20].

Choi et al. [18] utilized a Logical Key Hierarchy (LKH) to provide the broadcast communication. Fig. 5 shows this key management architecture, which is named Advance SCADA Key Management Architecture (ASKMA).

In the ASKMA, the nodes, RTUs, IEDs, sub-MSU, and MSU, are arranged into two tree structures: n-ary tree and binary tree. All RTUs and IEDs are located at leaves of this n-ary tree. The sub-MSUs and MSU are located at levels $h = \log_2^q$ and 0 of binary tree, respectively.

The efficiency of the ASKMA [18] is enhanced in ASKMA+ [19] by providing the multicast communication. In SKMA+, a key structure is divided into two classes, each class as a LKH structure. These two classes are connected using Iolus framework [44]. Using Iolus framework, the multicast and broadcast communications for multiple RTUs and IEDs are provided.

To address the availability issue in SCADA communications, Choi et al. [17] proposed hybrid key management architecture. Fig. 6 shows this key management architecture.

In this key management architecture, the Centralized Key Distribution (CKD) protocol is applied between MSU and sub-MSU. The LKH protocol is also applied between sub-MSU and RTUs or IEDs. The Iolus framework is utilized to connect these two parts.

Rezai et al. [52] developed an advance Hybrid Key Management Architecture for the SCADA network (HSKMA), which increased the performance and security of Choi et al. [17] key management architecture. The HSKMA uses Elliptic Curve Cryptography (ECC) [43,41,3,49] for communication between MSU and sub-MSUs and symmetric cryptography between sub-MSUs and its RTUs or IEDs. This key management architecture supports the three SCADA communications: unicast, multicast and broadcast. This architecture is shown in Fig. 7.

Jiang et al. [35] proposed a Limited Self-Healing (LiSH) key distribution, which provides collusion-resistant and revocation capability for SCADA group communication. Although their scheme, LiSH, provides all security requirements, it cannot revoke compromised users dynamically. Moreover, it has less efficient during the multicast communication.

To address the dynamic revocation mechanism, Jiang et al. [36] proposed LiSH+ scheme. The rekeying procedure of the Jiang et al. [36] scheme with dynamic revocation mechanism is shown in Fig. 8.

#### *4.1.2. Decentralized key distribution architectures (point-to-point architectures)*

Kang et al. [37] investigated the key management scheme in the radial SCADA networks. They supposed that communications in these networks were only made between the MSU and each RTU or IED. Fig. 9 shows this key management scheme.

Initiator of SCADA communication in the key management scheme in [37] is the MSU that asks RTUs or IEDs to provide and

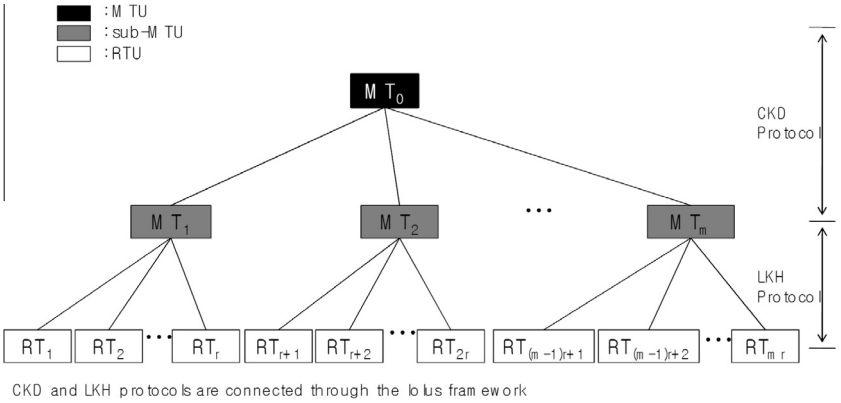


**Fig. 6.** The key management architecture in [17].

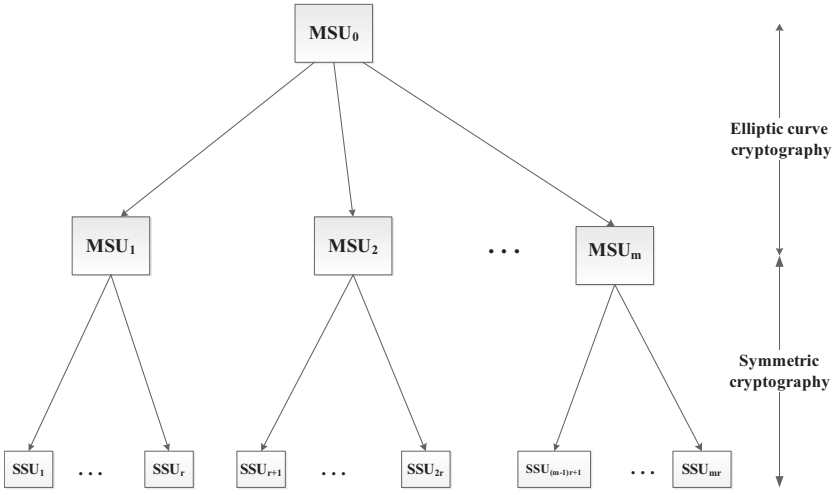


**Fig. 7.** The key management architecture in Rezai et al. [52]. $MSU_0$: Master Station Unit. $MSU_i$ ($i \in [1, m]$): sub-$MSU_i$, m: number of sub-MSU. r: number of slave station unit (RTUs or IEDs) in each sub-MSU.

send a new session key using communication link 1 in Fig. 9. The slave station unit, RTU or IED, choses a new session key, and then encrypts this session key using the master key, which is pre-shared with the MSU. The slave station unit sends this encrypted session key to the MSU using communication link 2. Finally, the MSU confirms this process using communication link 3 [37,50].

Rezai et al. [50] enhanced the performance of the radial SCADA networks by reducing the network traffic of Kang et al. [37] scheme. Fig. 10 shows this key management scheme.

In this key management scheme, the security devises on the MSU generate a new session key based on a timestamp. After that the MSU encrypts the session key using the master key, which is pre-shared by slave station unit, and sends it to the slave station unit using link 1 in Fig. 10. Finally, slave station unit sends the confirm message to the MSU using link 2 in Fig. 10. On sharing the session key, the MSU and slave station devices begin to communicate using this new session key.

They [51] also enhanced the performance of their previous works [50] using the hybrid key management scheme for these networks. In this key management scheme, the ECC is utilized to refresh the master key, and the symmetric cryptosystem is utilized to encryption, decryption, and session key update. Fig. 11 shows the session key update in this key management scheme.

Ebrahimi et al. [22] enhanced the performance of Rezai et al. [51] using Hyper Elliptic Curve Cryptosystem (HECC) to refresh the master key. Fig. 12 shows this key management scheme.

In this key management scheme, the MSU sends a request message to slave station unit, then slave station unit send an acceptable message to MSU, after receiving request message. Finally, MSU and slave station unit communicate with each other after authentication.

Tawde et al. [58] proposed a key management scheme that satisfies SCADA requirements of providing availability and quick response to real-time SCADA traffic. They installed two Bump-In-The-Wire (BITW) devices between MSU and slave station unit. Fig. 13 shows this key management scheme.

In this scheme, encryption and authentication are provided using symmetric key that should be secretly shared between MSU and slave station. The CDAC's sec-KeyD is utilized to provide the key distribution and key management scheme. The sec-KeyD protocol is also utilized to automatically revoke section key periodically.

### 4.2. Performance evaluation

To give an overview about the performance of each scheme/architecture, the performance of the most relevant and recent schemes, based on authors' opinion, are summarized in Tables 2–4.

Total delay time in Table 2 denotes the sum of the message encryption/decryption time, group key setup time, certificate verification time, and data transmission time. In this table, the run times are based on the Crypto++ 5.6.0 benchmarks [51,17,11].

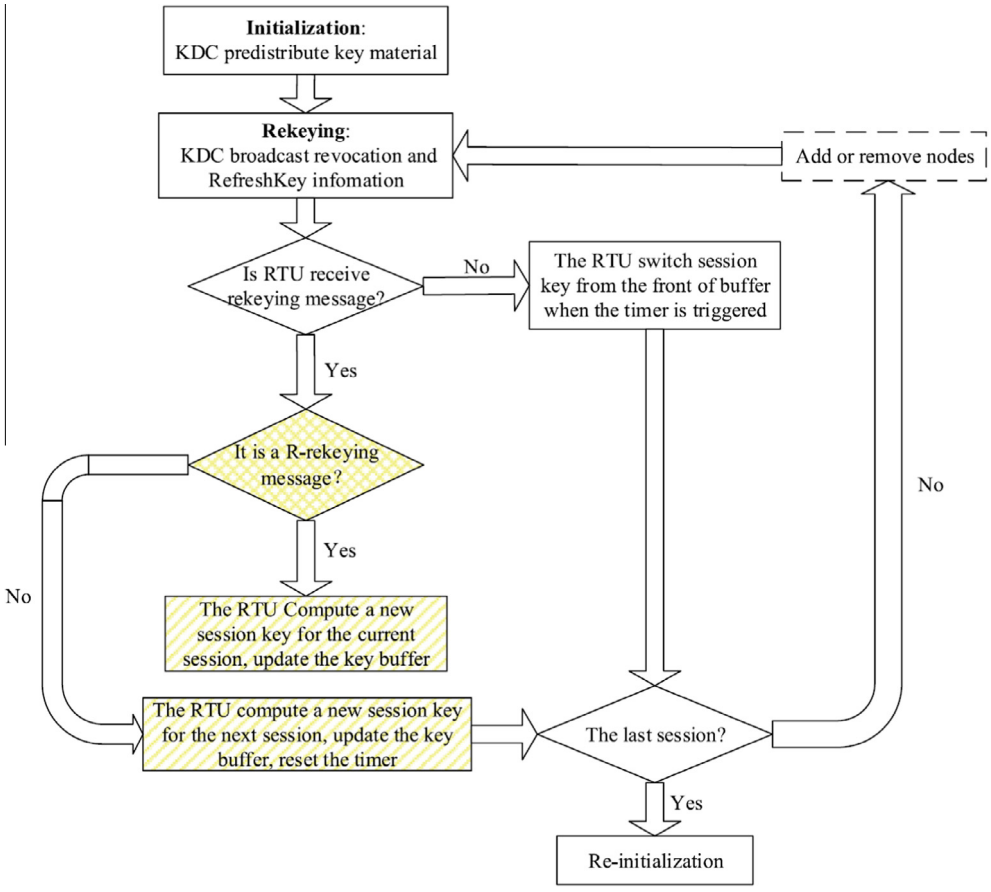


**Fig. 8.** The rekeying procedure of the Jiang et al. [36] scheme with dynamic revocation mechanism.

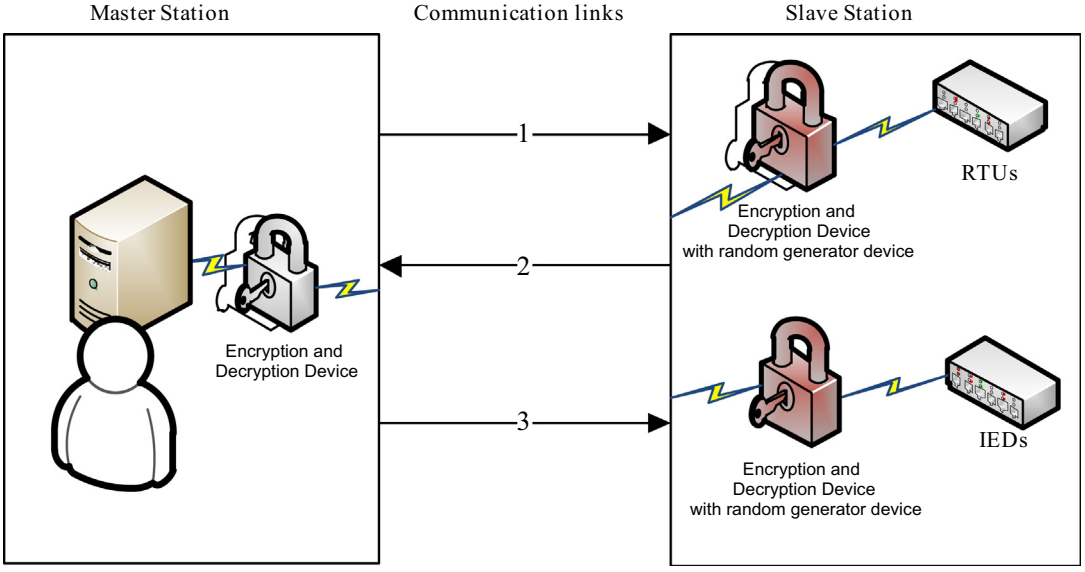


**Fig. 9.** The key management architecture in [37].

X.509.v3 is utilized for the certificate format [51,17,62]. Moreover, SCADA communication links operate at speeds such as 300 to 19,200 baud rates [51,17,7]. The default baud rates in the MODBUS implementation are 9600 and 19,200 [51,17]. The delay time at 9600 baud rate should be less than 0.54 s [51,17,13]. The highlighted box in Table 2 shows the total delay times that are less than 0.54 s. For example in [17], the message size in the SCADA networks is less than 1000, so message encryption time is 18 μs. The utilized symmetric key size is 128 bits. As a result, key encryption/decryption time is 3.4 μs. In addition, group key setup phase requires one exponentiation and one verification operation, so the group key setup time is 150 μs. Therefore, the total delay time,

Please cite this article in press as: A. Rezai et al., Key management issue in SCADA networks: A review, Eng. Sci. Tech., Int. J. (2016), http://dx.doi.org/10.1016/j.jestch.2016.08.011

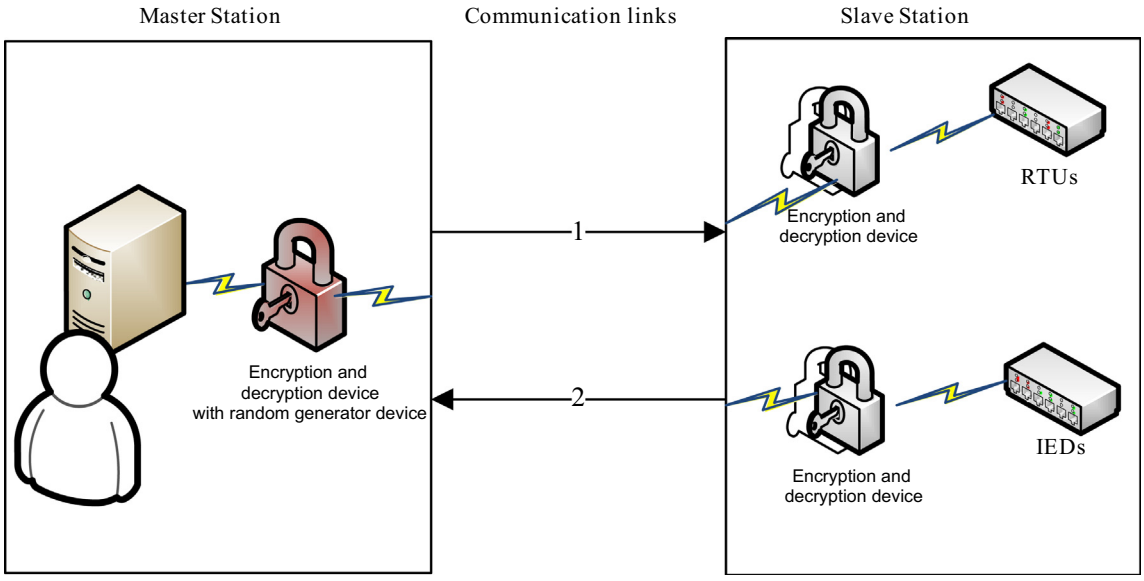


**Fig. 10.** The key management architecture in [50].

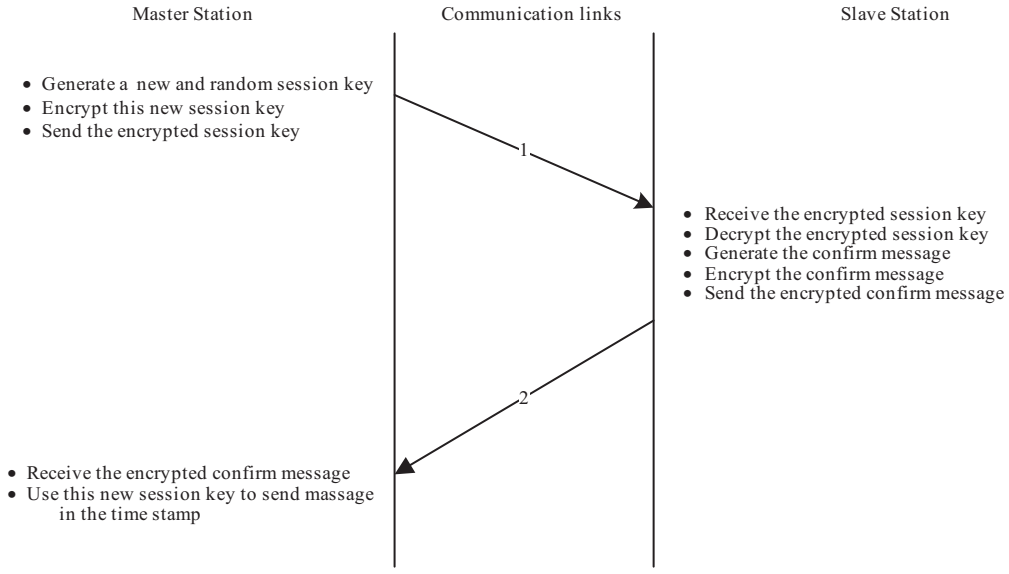


**Fig. 11.** The session key update scheme in the key management scheme in [51].

which is sum of these values and transmission time, in [17] is 0.453505 s. for 9600 baud rate.

Another important parameter in the performance evaluation of SCADA networks is storage cost (the number of required keys, which should be stored). As RTUs and IEDs are remote from MSU, they are physically insecure. As a result, they need to periodically update the security keys. One the other hand, if the RTU or IED has many keys and this RTU or IED is compromised, other RTUs and IEDs, which have those keys become vulnerable. So, the update process is required. Since the communication and computation costs of this process increase the number of vulnerable RTUs, IEDs, and keys, SCADA networks need to reduce the number of stored keys on each RTU or IED for security and efficiency. Table 3 summarizes the storage cost in the various key management architectures, where r denotes the maximum number of RTUs or IEDs per sub-MSU, and m denotes the number of sub-MSU.

In addition, security analysis is an important parameter in the performance evaluation of the SCADA networks. Note that to share the group key only with legitimate numbers, several requirements such as group key secrecy, forward secrecy, and backward secrecy should be met. The group key secrecy guarantees that it is computationally infeasible for adversaries to discover any group key. The forward (backward) secrecy guarantees that passive adversaries who know a contiguous subset of old group keys (a subset of group keys) cannot discover subsequent (preceding) group keys. Table 4 shows the security analysis for key management schemes/architectures presented in Section 4.1 based on security analysis in [42,19,40,18,27].

Based on our investigations which are shown in Tables 2–4, each scheme has advantages and disadvantages. For example, Kang et al. [37] key management scheme has a minimum delay time at the expense of some vulnerability. Choi et al. [17] key management

Please cite this article in press as: A. Rezai et al., Key management issue in SCADA networks: A review, Eng. Sci. Tech., Int. J. (2016), http://dx.doi.org/10.1016/j.jestch.2016.08.011

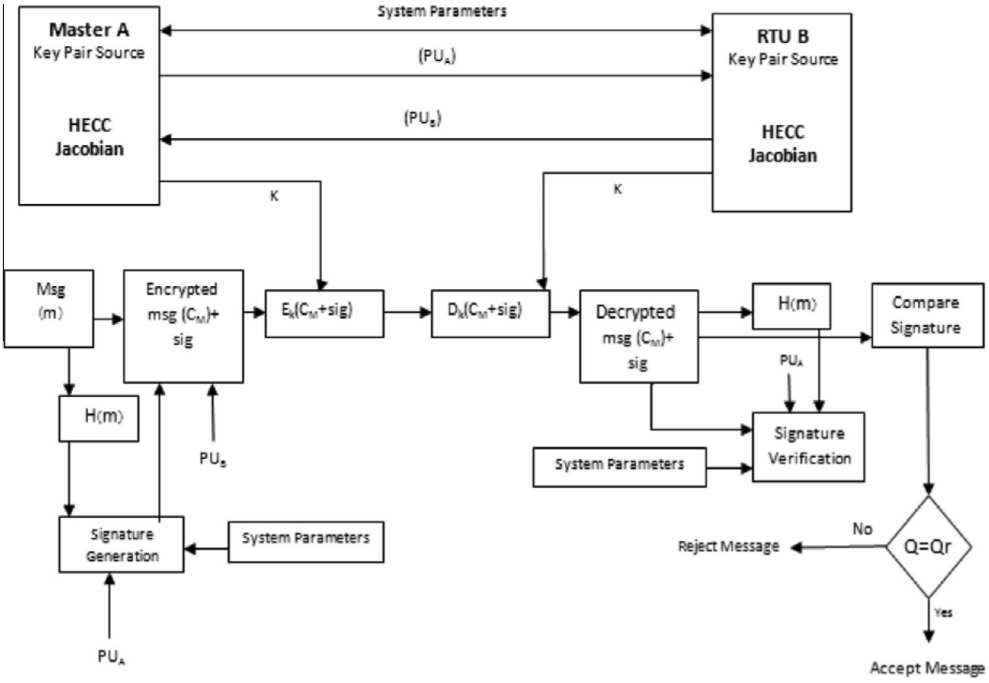


**Fig. 12.** Ebrahimi et al. [22] key management scheme.

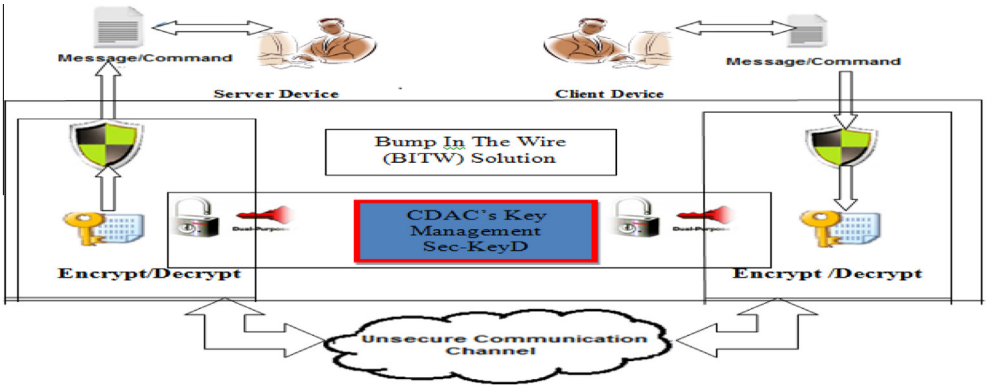


**Fig. 13.** Tawde et al. [58] key management scheme.

**Table 2**
The comparative table for total delay time.

| Ref. | Baud rate | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 115200 | 38400 | 19200 | 9600 | 4800 | 2400 | 1200 | 600 | 300 | 110 |
| Choi et al. [18] | 0.020039 | 0.060039 | 0.120039 | 0.240039 | 0.480039 | 0.960039 | 1.960039 | 3.84003 | 7.680039 | 20.94549 |
| Choi et al. [19] | 0.020039 | 0.060039 | 0.120039 | 0.240039 | 0.480039 | 0.960039 | 1.960039 | 3.84003 | 7.680039 | 20.94549 |
| Choi et al. [17] | 0.037949 | 0.113505 | 0.226838 | 0.453505 | 0.906838 | 1.813505 | 3.626838 | 7.25350 | 14.50684 | 39.56381 |
| Kang et al. [37] | 0.004673 | 0.01384 | 0.02759 | 0.05509 | 0.11009 | 0.22009 | 0.44009 | 0.88009 | 1.76009 | 4.80009 |
| Rezai et al. [51] | 0.020013 | 0.048516 | 0.091270 | 0.176778 | 0.347793 | 0.689825 | 1.373887 | 2.74201 | 5.478262 | 14.93076 |
| Rezai et al. [52] | 0.030663 | 0.080507 | 0.155272 | 0.304804 | 0.603866 | 1.201996 | 2.398241 | 4.79074 | 9.575741 | 26.10574 |

scheme provides security issues at the expense of maximum delay time in comparison with other schemes and all schemes/architectures in Tables 2 and 3 can support the MODBUS implementation.

### 4.3. Open research issues

As described in the previous sections, the SCADA networks have specific limitations, and requirements that introduce new security concerns. Availability, integrity, and confidentiality are important security aspects. To circumvent threats against these security aspects, an efficient key management scheme is required. In SCADA

**Table 3**
The comparative table for the storage cost.

| Ref. | Device | | |
|---|---|---|---|
| | $MSU_0$ | $MSU_i$ | Each RTU or IED |
| Beaver et al. [12] | $mr$ | $r+1$ | 1 |
| Dawson et al. [20] | $mr$ | $r+1$ | 1 |
| Choi et al. [18] | $2m+mr$ | $r+\log_2^m$ | $2+\log_2^r$ |
| Choi et al. [19] | $m$ | $1+r+\log_2^m$ | $1+\log_2^r$ |
| Kang et al. [37] | $r+1$ | – | 2 |
| Rezai et al. [51] | $r+1$ | – | 2 |
| Choi et al. [17] | $m+2$ | $2r+1$ | $1+\log_2^r$ |
| Rezai et al. [52] | $m+2$ | $2r+1$ | $1+\log_2^r$ |

**Table 4**
The security comparison between key management architectures.

| Ref. | Security requirement | | | | | | |
|---|---|---|---|---|---|---|---|
| | Broadcasting | Multicasting | Group key security | Forward security | Backward security | Key freshness | Availability |
| Beaver et al. [12] | Impossible | Impossible | – | – | – | Possible | – |
| Dawson et al. [20] | Impossible | Impossible | – | – | – | Possible | – |
| Choi et al. [18] | Possible | Possible | Provide | Provide | Provide | Possible | Impossible |
| Choi et al. [19] | Possible | Possible | Provide | Provide | Provide | Possible | Impossible |
| Kang et al. [37] | Impossible | Impossible | – | – | – | Possible | – |
| Rezai et al. [51] | Impossible | Impossible | – | – | – | Possible | – |
| Choi et al. [17] | Possible | Possible | Provide | Provide | Provide | Possible | Possible |
| Jiang et al. [35] | Possible | Possible | Provide | Provide | Provide | Possible | Possible |
| Jiang et al. [36] | Possible | Possible | Provide | Provide | Provide | Possible | Possible |
| Ebrahimi et al. [22] | Possible | Possible | – | – | – | Possible | – |
| Tawde et al. [58] | Impossible | Impossible | – | – | – | Possible | – |
| Rezai et al. [52] | Possible | Possible | Provide | Provide | Provide | Possible | Possible |

networks, neither asymmetric key management alone, nor symmetric key management alone is sufficient. Asymmetric key management alone is not suitable due to some RTUs and IEDs lack of ability to utilize PKC. Symmetric key management alone cannot provide suitable security [51,56]. As a result, development of efficient hybrid asymmetric and symmetric key management schemes/architectures is in the focal point of major researches in this area.

In addition to the research efforts investigated in this paper, there are some other issues, which still require extensive research efforts such as public key infrastructures, cryptographic authority and certificate management in the SCADA key management scheme, finding vulnerabilities of SCADA networks, distributed security mechanism, which meet the resource limitations of SCADA networks, application of cloud security in SCADA networks, lightweight cryptographic algorithms and protocols and even some new hardware specifically designed for SCADA networks, Intrusion Detection Systems (IDSs), access control, protocol vulnerability assessment, and firewalls.

## 5. Conclusion

In today's competitive markets, it is essential to connect SCADA systems to the open access networks such as Internet. So, the security of the SCADA networks is a challenging issue. Key management is essential for the SCADA communication security. Motivated by these facts, in this paper, we've investigated important security threats in SCADA networks, and then the ongoing works on SCADA key management scheme are classified based on their properties. To complement the review of key management schemes in the SCADA networks, we then reviewed existing efforts [52,51,37,19,17,50,20,12,18,22,58,35,36] and highlighted some open research issues. Based on our investigation, development of efficient hybrid asymmetric and symmetric key management schemes/architectures is in the focal point of major research in this area.

## References

[1] AGA, Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan, American Gas Association Rep., 2006. AGA-12_ part_1.
[2] AGA, Cryptographic Protection of SCADA Communications; Part 2: Retrofit Link Encryption for Asynchronous Serial Communications, American Gas Association Rep., 2006. AGA-12_Part_2.
[3] H.R. Ahmadi, A. Afzali-kusha, A low-power and low-energy flexible GF(p) elliptic-curve cryptography processor, J. Zhejiang Univ. Sci. C 11 (9) (2010) 724–736.
[4] C. Alcaraz, J. Lopez, A security analysis for wireless sensor mesh networks in highly critical systems, IEEE Trans. Syst. Man. Cybernetics-Part C: Appl. Rev. 40 (4) (2010) 419–428.
[5] C. Alcaraz, R. Roman, P. Najera, J. Lopez, Security of industrial sensor network-based remote substations in the context of the Internet of Things, Ad Hoc Netw. 11 (3) (2013) 1091–1104.
[6] E. Ancillotti, R. Bruno, M. Conti, The role of communication systems in smart grids: architectures, technical solutions and research challenges, Comput. Commun. 36 (17) (2013) 1665–1697.
[7] K. Andrew, A. John, M. Joe, Low-latency cryptographic protection for SCADA communications, Proc. 2nd Appl. Crypto. Netw. Secur., LNCS., vol. 3089, 2004, pp. 263–277.
[8] API 1164, Pipeline SCADA Security, American Petroleum Institute, API standard, Washington, DC, 2004.
[9] ANSI, Security Technologies for Industrial Automation and Control Systems, International Society of Automation, ANSI/ISA Rep., Research Triangle Park, NC, 2007. TR99.00.01-2007.
[10] M.H. Assaf, R. Mootoo, S.R. Das, E.M. Petriu, V. Groza, S.N. Biswas, Designing home security and monitoring system based on field programmable gate array, IETE Tech. Rev. 31 (2) (2014) 168–176.
[11] E. Barker, D. Johnson, M. Smid, Recommendation for Pair-wise Key Establishment Schemes Using Discrete Logarithm Cryptography, NIST Standard, 2007. SP 800-56A.
[12] C. Beaver, D. Gallup, W. Neumann, M. Torgerson, Key Management for SCADA, SAND Report SAND2001-3252., 2002.
[13] C.L. Bowen, T.K. Buennemeyer, R.W. Thomas, Next generation SCADA security: Best practices and client puzzles, Proc. 6th Annual IEEE SMC Inf. Assur. Workshop (IAW), 2005, pp. 426–427.
[14] E.J. Byres, D. Lissimore, N. Kube, Who Turned Out the Lights? Security Testing for SCADA and Control Systems, in: Presented at the CanSecWest, Vancouver, British Columbia, 2006.
[15] C.L. Chen, C.C. Chen, D.K. Li, P.Y. Chen, A verifiable and secret buyer-seller watermarking protocol, IETE Tech. Rev. 32 (2) (2015) 104–113.
[16] J. Chen, N. Liu, W. Liu, H. Luo, A key management scheme for secure communications of advanced metering infrastructure, in: D. Zheng (Ed.), Appl. Inf. Commun., Springer, Berlin Heidelberg, 2011, pp. 430–438.
[17] D. Choi, H. Jeong, D. Won, S. Kim, Hybrid key management architecture for robust SCADA systems, J. Inf. Sci. Eng. 29 (2) (2013) 281–298.
[18] D. Choi, H. Kim, D. Won, S. Kim, Advanced key management architecture for secure SCADA communications, IEEE Trans. Power Del. 24 (3) (2009) 1154–1163.
[19] D. Choi, S. Lee, D. Won, S. Kim, Efficient secure group communications for SCADA, IEEE Trans. Power Del. 25 (2) (2010) 714–722.
[20] R. Dawson, C. Boyd, E. Dawson, J. Nieto, SKMA, A key management architecture for SCADA systems, in: Proc. Australasian Workshops on Grid Computing and E-research, 2006, pp. 183–192. Darlinghurst, Australia.
[21] Z. Drias, A. Serhrouchni, O. Vogel, Analysis of cyber security for industrial control systems, Proc. IEEE Int. Conf. Cyber Sec. Smart Cities, Indus, Control. Syst. Commun., Shanghai, 2015, pp. 1–8.
[22] A. Ebrahimi, F. Koropi, H. Naji, Increasing the security of SCADA systems using key management and hyper elliptic curve cryptography, Proc. 9th Symp. Adv. Sci. Tech., Mashhad, 2014, pp. 17–24.
[23] I.N. Fovino, SCADA system cyber security, in: K. Markantonakis, K. Mayers (Eds.), Secure Smart Embedded Devices, Platforms and Applications, Springer, New York, 2014, pp. 451–471.
[24] I.N. Fovino, A. Coletta, A. Carcano, M. Masera, Critical state-based filtering system for securing SCADA network protocols, IEEE Trans. Ind. Electron. 25 (10) (2012) 3943–3950.
[25] J. Gao, J. Liu, B. Rajan, R. Nori, B. Fu, Y. Xiao, W. Liang, C.L. Philip Chen, SCADA communication and security issues, Secur. Commun. Netw. 7 (1) (2014) 175–194.
[26] D.J. Gaushell, W.R. Block, SCADA communication techniques and standards, IEEE Comput. Appl. Power 6 (3) (2002) 45–50.
[27] H.R. Hassen, H. Bettahar, A. Bouadbdallah, Y. Challal, An efficient key management scheme for content access control for linear hierarchies, Comput. Netw. 56 (8) (2012) 2107–2118.
[28] M. Hentea, Improving security for SCADA control systems, Int. J. Inf. Knowledge Manag. 3 (2008) 73–86.
[29] J.L. Hieb, J. Schreiver, J.H. Graham, A security-hardened appliance for implementing authentication and access control in SCADA infrastructures with legacy field device, Int. J. Crit. Infr. Prot. 6 (1) (2013) 12–24.

Please cite this article in press as: A. Rezai et al., Key management issue in SCADA networks: A review, Eng. Sci. Tech., Int. J. (2016), http://dx.doi.org/10.1016/j.jestch.2016.08.011

[30] J. Hull, H. Khurana, T. Markham, K. Staggs, Staying in control: cyber security and the modern electric grid, IEEE Pow. Energy Mag. 10 (1) (2012) 41–44.
[31] V.M. Igure, S.A. Laughter, R.D. Williams, Security issues in SCADA networks, Comput. Secur. 25 (7) (2006) 498–506.
[32] ISA, Integrating Electronic Security into the Manufacturing and Control Systems Environment, ISA Standard, 2007. ANSI/ISA-TR99.00.02-2004.
[33] ISO, Information Technology-Security Techniques-Key Management-Part 2: Mechanisms Using Symmetric Techniques, ISO Standard, 2008. ISO/IEC11770-2.
[34] P. Jokar, N. Arianpoo, V. Leung, A survey on security issues in smart grids, Secur. Commun. Netw. 9 (3) (2016) 262–273.
[35] R. Jiang, R. Lu, C. Lai, J. Luo, X. Shen, Robust group key management with revocation and collusion resistance for SCADA in smart grid, in: Proc. IEEE globe Commun. Conf., Atlanta, GA, 2013, pp. 802–807.
[36] R. Jiang, R. Lu, J. Luo, C. Lai, X. Shen, Efficient self-healing group key management with dynamic revocation and collusion resistance for SCADA in smart grid, Secur. Commun. Netw. 8 (6) (2015) 1026–1039.
[37] D. Kang, J. Lee, B. Kim, D. Hur, Proposal strategies of key management for data encryption in SCADA network of electric power systems, Int. J. Electr. Power Energy Syst. 33 (9) (2011) 1521–1526.
[38] A. Khelil, D. Germanus, N. Suri, Protection of SCADA communication channel, in: J. Lopeze et al. (Eds.), Critical Inf. Infrast. Protection, Springer, Berlin Heidelberg, 2012, pp. 177–196.
[39] H. Kim, Security and vulnerability of SCADA systems over IP-based wireless sensor networks, Int. J. Distr. Sensor Netw. 2012 (2012) 1–10.
[40] J.Y. Kim, H.K. Choi, An efficient and versatile key management protocol for secure smart grid communications, in: Proc. IEEE Wireless Commun. Netw. Conf., Shanghai, 2012, pp. 1823–1828.
[41] N. Koblitz, Elliptic curve cryptosystem, Math. Comput. 48 (1987) 203–209.
[42] N. Liu, J. Chen, L. Zhu, J. Zhang, Y. He, A key management scheme for secure communications of advanced metering infrastructure in smart grid, IEEE Trans. Ind. Electron. 60 (10) (2013) 4746–4756.
[43] V. Miller, Use of elliptic curves in cryptography, Proc. Adv. Crypto. (CRYPTO), 1985, pp. 417–428.
[44] S. Mittra, Iolus: a framework for scalable secure multicasting, Proc. ACM SIGCOMM '97 Conf. Appl. Tech., Architec., Protocols Comput. Commun., New York, NY, USA, 1997, pp. 277–288.
[45] MODBUS, 2008. MODBUS application protocol specification V1.1b, Modbus-IDA, 2008, available from: <http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf>.
[46] A. Nicholson, S. Webber, S. Dyer, T. Patel, H. Janicke, SCADA security in the light of cyber warfare, Comput. Secur. 31 (4) (2012) 418–436.
[47] NIST, System Protection Profile-Industrial Control Systems v1.0, NIST Standard, 2004. SPP-ICSv1.0, 2004.
[48] P. Ralston, J. Graham, J. Hieb, Cyber security risk assessment for SCADA and DCS networks, ISA Trans. 46 (4) (2007) 583–594.
[49] A. Rezai, P. Keshavarzi, CCS representation: a new non-adjacent form and its application in ECC, J. Basic Appl. Sci. Res. 2 (5) (2012) 4577–4586.
[50] A. Rezai, P. Keshavarzi, Z. Moravej, A new key management scheme for SCADA network, Proc. 2nd int. Symp. Comput. Sci. Eng., Aydin, Turkey, 2011, pp. 383–388.
[51] A. Rezai, P. Keshavarzi, Z. Moravej, Secure SCADA communication by using a modified key management scheme, ISA Trans. 52 (4) (2013) 517–524.
[52] A. Rezai, P. Keshavarzi, Z. Moravej, Advance Hybrid Key Management Architecture for SCADA Network Security, 2016. Secur. Commun. Netw. http://dx.doi.org/10.1002/sec.1612.
[53] P. Serrano, A. Oliva, P. Patras, V. Mancuso, A. Banchs, Greening wireless communications: status and future directions, Comput. Commun. 35 (14) (2012) 1651–1661.
[54] A. Shahzad, M. Lee, Y. Lee, S. Kim, N. Xiong, J. Choi, Y. Cho, Real time MODBUS transmissions and cryptography security designs and enhancements of protocol sensitive information, Symmetry 7 (3) (2015) 1176–1210.
[55] J. Zhang, S. Wang, Efficient key management scheme for SCADA system, in: Y. M. Huang, H.C. Chao, D.J. Deng, J.J. Park (Eds.), Adv. Tech. Embedded and Multimedia for Human-centric Computing, Springer, Netherlands, 2014, pp. 619–625.
[56] M. Sleeper, Key management for secure power SCADA, Dartmouth Comput. Sci. Tech. Report TR (2008) 2008–2628.
[57] K. Stouffer, J. Falco, K. Kent, Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, NIST Spec. Publ. (2006) 800–882.
[58] R. Tawde, A. Nivangune, M. Sankhe, Cyber security in smart grid SCADA automation system, Proc. 2nd IEEE Int. Conf. Inf. Emb. Commun. Syst., Coimbatore, 2015, pp. 1–5.
[59] J. Townsend, M.A. Badar, J. Szekerces, Updating temperature monitoring on reciprocating compressor connecting rods to improve reliability, Eng. Sci. Technol. Int. J. 19 (1) (2016) 566–573.
[60] C.K. Wong, M. Gouda, S. Lam, Secure group communications using key graphs, IEEE/ACM Trans. Netw. 8 (1) (2000) 16–30.
[61] L. Xiao, I. Yen, F. Bastani, Scalable authentication and key management in SCADA, in: Proc. IEEE Int. Conf. Parallel Distributed Syst., Shanghai, 2010, pp. 172–179.
[62] Y. Yangtao, L. Quan, L. Fen, A Design of Certificate Authority Based on Elliptic Curve Cryptography, Proc. IEEE 9th int. symp. Distributed Comput. Appl. Business Eng. Sci. (DCABES 2010), Hong Kong, 2010, pp. 454–457.

Please cite this article in press as: A. Rezai et al., Key management issue in SCADA networks: A review, Eng. Sci. Tech., Int. J. (2016), http://dx.doi.org/10.1016/j.jestch.2016.08.011