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

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

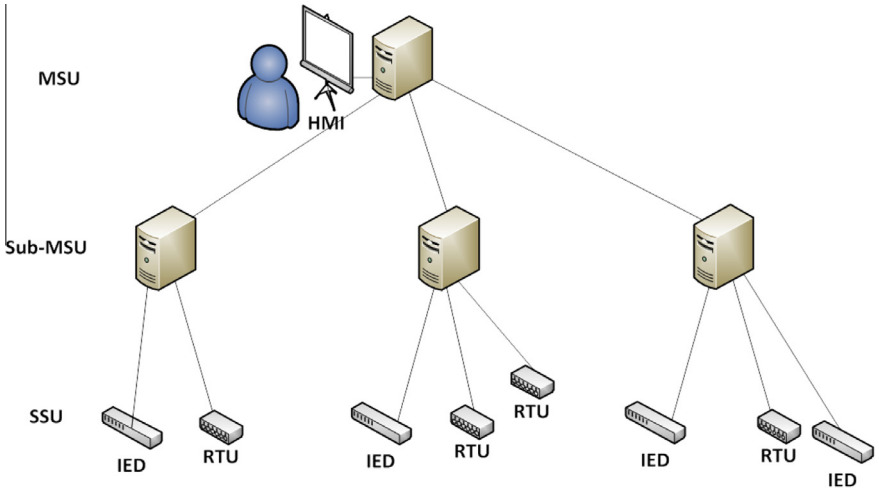


**Fig. 1.** A simplified SCADA network architecture.

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