A Proposed Method for Increase Security in SCADA Systems

M. R. poushideh and J. Haddadnia

***Abstract*—SCADA (Supervisory Control and Data Acquisition) refers to the combination of telemetry and data acquisition [1]. Modern public infrastructure systems use SCADA systems for daily operation. This includes water treatment systems; electric power transmission, distribution, and generation; petroleum storage and refineries; chemical production and processing; railroads and mass transit; and manufacturing. The SCADA system provides monitoring, data analysis, and control of the equipment used to manage most public infrastructure systems. Little attention was given to security considerations in the initial design and deployment of these systems, which has caused an urgent need to upgrade existing systems to withstand unauthorized intrusions potentially leading to terrorist attacks. The security of these systems is critical for the operation of our society. Security of these services should have high priority. This paper identifies threats faced by SCADA and investigates effective methods to enhance its security by analyzing DNP3 protocols, which has become a de facto industry standard protocol for implementing the SCADA communications. Finally we will summarize our results and try to recommend methods to overcome the vulnerabilities on these systems.**

***Index Terms*—Supervisory control and data acquisition, SCADA networks, communication protocol security, internet-based SCADA, TCP/IP.**

I. Introduction

SCADA systems are used in industrial and civil engineering applications to control and monitor distributed systems from a central location. SCADA is a system operation with coded signals over communication channels so as to provide control of Remote Terminal Unit (RTU) equipment [1]. Fig. 1 shows a general SCADA system. Recently Intelligent Electronic Device (IED) which is control unit having communication function with master station is replacing the role of RTU. In the beginning stage, power system used its own private network, but it has been opened and connected to external networks, finally to the internet, because of saving the cost of building networks and reinforcing the new functions of power system like automation, intelligence, etc. The SCADA technology was initially designed to maximize functionality and performance with little attention to security. This weakness in security makes the SCADA systems vulnerable to manipulation of operational data that could result in serious disruption to public health and safety.

Common protocols include Modbus and DNP3. Although originally designed to run on low-bandwidth proprietary networks, many protocols have included extensions to operate over TCP/IP. However, the Internet has opened SCADA, and the systems they support, to new vulnerabilities. Private network is still used on some countries, but the network partly started to be connected to internet network for monitoring and maintenance problem of many stations. Connection to the internet brings the improvement on economics in a positive aspect but also the escalation of vulnerability on system from cyber-attacks. As cyber-attacks increase on general communication networks, SCADA network has been also exposed to cyber security problems.

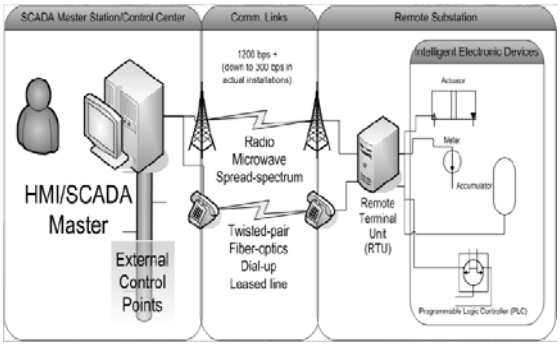

Fig. 1. General SCADA system

II. SCADA Network and Communication

A. Protocols

SCADA networks have become popular since the 1960's to control electrical and other infrastructure systems. Central SCADA communicates using TCP/IP protocol. It is possible for different systems provided by various vendors to communicate each other and to be integrated into one entire system. DNP is also telecommunication standard with ICCP, which defines communication between master stations, RTUs and other intelligent electronic devices (IEDs).

Since the early 1990's SCADA systems perform more operations automatically. Use of "smart" RTUs or PLCs (programmable logic controllers), which are capable of autonomously executing simple logic processes without involving the master computer, is increasing [2]. Current generation digital IEDs and microprocessor relays have the ability to transmit varying degrees of functional and real-time information. A single IED can provide a number of applications and could be configured for different system parameters. The Fig. 2 illustrates today's SCADA architecture:

Manuscript received October 14, 2012; revised November 25, 2012. This work was supported by Tarbiat Moallem University of Sabzevar, Iran.

The authors are with Tarbiat Moallem University of Sabzevar, Electrical and Computer Engineering Faculty, Sabzevar, Iran (e-mail:m.poshideh@gmail.com, haddadnia@sttu.ac.ir).

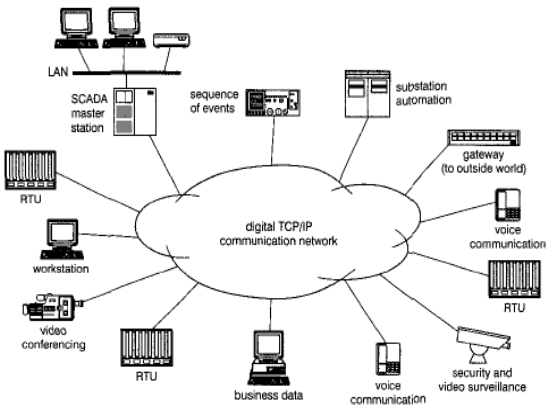

Fig. 2. Modern SCADA architecture

B. DNP3 Protocol

The SCADA protocols provide transmission specifications to interconnect substation computers, RTUs, IEDs, and the master station. The most common protocols used are: IEC (International Electro technical Commission) 60870-5-101, Distributed Network Protocol version 3.0 (DNP3) and Modbus. The IEC and DNP3 protocols provide more functionality than Modbus and are used for higher data volumes. Both protocols provide similar application functionality. They were primarily designed for point-to-point or multi-drop serial link architectures, but can work over radio, LAN, etc. IEC protocols dominate the market in Europe whereas DNP is a major market player in North America [5]. DNP3 protocols are also widely used in Australia and China.DNP3 is an open and public protocol standard that is now owned and maintained by the DNP User Group and DNP Technical Committee [6]. The protocol enables the Master Station to request data from Substations using pre-defined commands and Substations to respond by transmitting the requested data. DNP3 is based on the early work of the IEC, that resulted in the IEC 60870-5 protocol for SCADA communication. Both protocols use a simplified 3 layer version of the OSI 7 Layer model called Enhanced Performance Architecture (EPA) (Fig. 3).

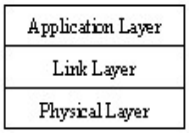

Fig. 3. Enhanced performance architecture

DNP3 and IEC 60870-5 are both part of the IEEE Standard 1379. DNP3 was not designed with security mechanisms in mind. The protocol itself lacks any form of authentication or encryption. It is made worse when industrial stations have started to connect to the Internet as this will allow conventional TCP/IP-based attacks to be launched. DNP3's functionality contributes to the protocol's widespread use in substation local area networks using TCP/IP Ethernet. More and more vendors use TCP/IP (the protocols used to communicate over the Internet) to transport DNP3 messages in lieu of the traditional media mentioned above (dedicated and dial-up telephone lines, multi-dropped telephone line, fiber optic cable, licensed/unlicensed radio, corporate frame relay networks, standard or CDPD cellular systems). Link layer frames are embedded into TCP/IP packets for transmission. This approach has enabled DNP3 to take advantage of Internet technology and permitted collecting data economically and controlling widely separated devices [6]. By using any web browser, SCADA users can get the latest data from a variety of widely-separated remote field devices instantaneously and conveniently. The benefits of using the Internet technology to carry SCADA communications come at the cost of compromised security since the data over the Internet can be an easy target for an attack. To make the situation more challenging, DNP3, as most other SCADA protocols, has no built-in security feature such as message authentication [7], which assures that a party to some computerized transaction is not an impostor. This protocol does not provide effective authentication or encryption mechanisms. Although utilities have increased the use of DNP3 protocol in recent years, many owners and operators do not yet have the technology, capabilities, and/or resources needed to secure their systems.

III. Security Overview

Fig. 4 illustrates how the modern SCADA networks are integrated with corporate networks and the Internet. The figure also shows that the field data (obtained using RTUs and IEDs) is transmitted over a wide range of communication lines and can even be accessed via a web browser to SCADA users. Communication between such integrated system elements often uses Ethernet and Internet technology. Network enabled devices, routers, switches, and Window-based operating systems are now quite common in SCADA systems, bringing with them the vulnerabilities that are experienced in desktop computers and corporate networks [3].SCADA networks are part of our nation's critical infrastructure and require protection from a variety of threats. When initially designed, SCADA equipment was designed for maximal functionality. As a result many security risks were exposed to maximize the communication efficiency. This makes many SCADA networks potentially vulnerable to attack. The security of a SCADA network can be improved in a number of ways such as installing firewalls, securing devices that make the network, implementing access control, network enhancements, and so forth. We identify SCADA communication protocol such as DNP3 as the most essential and appropriate place to enhance the security and propose various methods to secure the protocols. There is a common misconception the belief that the SCADA system resides on a separate standalone network. Most SCADA systems were originally built on separate standalone networks, but were eventually bridged as a result of changes in information management practices. The need for real-time data became desirable on the corporate network. In addition to this misconception certain network mediums present their own set of security risks. Sniffing, Denial of Service (DOS) and spoofing attacks are all serious threats. There are several steps that can be taken to minimize the threat and impact of such vulnerabilities and attacks. Proper access controls should be implemented to verify the identity of the user. If passwords are used they should be changed frequently. Biometric devices are also helpful. The operating system must also be hardened. Any unnecessary software and

services should be removed. Apply all stable patches to the system. Communication protocols must be configured for maximal security. In certain instances external access to the SCADA network may be necessary. Vendors may need access, or connections to the corporate network may be necessary. Every one of these connections presents a serious threat. It is extremely important that all external access points be identified. Determine what specific access is needed. Identify the methods used to connect.

Studies have been conducted to statistically analyze the effectiveness of the security measures or the potential threats. For example, in order to apply security safeguards to prevent an attack, as the first step, organizations depend on a methodology such as the one suggested by Farahmand et al. [4] that guide managers and assist them to assess and understand the vulnerabilities of the business operations and control measures. Convenient access to Internet resources and online search capabilities provide a systematic footprint for hackers to identify an organization's security posture. There are increasingly sophisticated intrusion tools that include [8]:

War dialing: It can be executed in the scripts to the surrounding numbers to detect potential connection once the main phone number prefix is determined.

Scanning: It scans the destination IP addresses to determine the service ports on the machine that are either running or in listening state for connection to potential access points.

Traffic sniffing: The network analyzer is used to capture the packets traversing within a network.

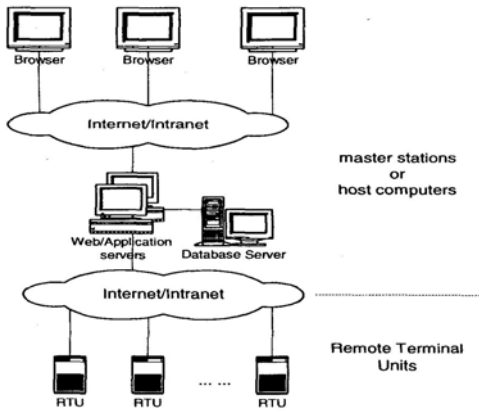

Fig. 4. Architecture of a web-based SCADA system [9].

Password cracking: A program that repeatedly tries to guess a password in order to gain (unauthorized) access to a network.

IV. Proposed Method

There are no new solutions that are unique to SCADA systems per se. Most of the security solutions to potential vulnerabilities in SCADA systems are already known to the Internet security world. Due to the nature of the assets being protected, the computing resources used have to be able to withstand most of the known vulnerabilities. We will explore this through the basic elements of security.

Encryption algorithms: Encryption is the process of systematically altering data to make it unreadable to unauthorized users. Message encryption can hide message contents from outsiders. There are two kinds of encryption algorithms. One is the symmetric key algorithm which uses the same encryption key which is shared with a sender and a receiver together. The other is the asymmetric key algorithm which uses two keys, a public key and a private key [12]. Symmetric encryption is called symmetric because the decryption process is exactly the reverse of the encryption process. Asymmetric encryption is called asymmetric because the key used to encrypt the data is different from the key used to decrypt the data. The encryption algorithms are used for not only message confidentiality, but message authentication and integrity. The asymmetric key algorithm requires far more computation than the symmetric key algorithm. Considering that the FRTUs in the distribution network have very limited computing power, it is recommended not to permit the excessive overhead for computing encryption and decryption every time they exchange messages. For this reason it is desirable to avoid the asymmetric key algorithm when encryption is necessary as in the key distribution.

Authentication with Digital Signatures: All employees with access to SCADA control terminals should be authorized to do so, and their authorization needs to be current. Strong authentication should be used. Simple password protection may not be sufficient. At least a two-factor authentication system should be used. Access to IEDs should require the use of strong authentication or smart card access. A digital signature is a block of encrypted data included with a message. The block of encrypted data is sometimes called an authenticator. A digital signature typically uses the public key encryption process in reverse. The digital certificate process is designed to serve a community of users. As you might guess, the security of the process depends on the safe distribution of any keys necessary for communicating with the certificate server. This might seem like simply transferring the problem.

V. Conclusion

SCADA networks are diverse systems. The integration of legacy hardware with new technologies leads to a vast array of technologies and protocols being used. The integration of these technologies is typically oriented towards functionality with little thought for security. The correct Cyber security problems of SCADA network of critical infrastructures such as electric power, gas and oil are very important against cyber-attack and terrorism. Recently, researching efforts to solve the problem are accelerating and bringing the improvement. We focused on two public methods that combine with uses protocol to increase security with no change on instinct properties of protocol: Encryption and Digital Signatures.

References

[1] G. Clarke, D. Reynders, and E. Wright, "Practical Modern SCADA Protocols," *Newnes*, 2004

[2] Fact Index, SCADA Systems. [Online]. Available: http://www.fact-index.com/s/sc/scada.html

[3] Sandia National Laboratories. [Online]. Available: http://www.sandia.gov/scada/history.htm
[4] F. Farahmand, S. B. Navathe, P. H. Enslow, and G. P. Sharp, "Managing vulnerabilities of information systems to security incidents," in *Proc. of 5th international conference on Electronic commerce*, Pittsburgh, Pennsylvania, September 2003, pp. 348 – 354.
[5] J. Makhija and L. R. Subramanyan. Comparison of protocols used in remote monitoring: DNP 3.0, IEC 870-5-101 and Modbus. [Online]. Available: http://www.ee.iitb.ac.in/~esgroup/es_mtech03_sem/sem03_paper_03307905.pdf
[6] DNP3 Organization's Website. DNP3 Technical Document. A DNP3 Protocol Primer. [Online]. Available: http://dnp.org/files/dnp3_primer.pdf
[7] M. Bishop, *Computer Security*, Addison-Wesley, 2003.
[8] S. M. Clure, J. Scambray, and G. Kurtz, *Hacking Exposed: Network Security Secrets and Solutions*, 4th ed. Emeryville, CA: McGraw-Hill/ Osborne, 2003.
[9] D. Li, Y. Serizawa, and M. Kiuchi, *Concept Design for a web-based Supervisory Control And Data-Acquisition (SCADA) System*
[10] K. H. Mak and B. Holland, "Migrating electrical power network SCADA systems to TCPAP and Ethernet networking," *power engineering journal*, December 2002.

Javad Haddadnia received his B.S. and M.S. degrees in electrical and electronic engineering with the first rank from Amirkabir University of Technology, Tehran, Iran, in 1993 and 1995, respectively. He received his Ph.D. degree in electrical engineering from Amirkabir University of Technology, Tehran, Iran in 2002. He joined Tarbiat Moallem University of Sabzevar in Iran. His research interests include network security, neural network, digital image processing, computer vision, and face detection and recognition. He has published several papers in these areas. He has served as a Visiting Research Scholar at the University of Windsor, Canada during 2001 and 2002. He is a member of SPIE, CIPPR, and IEICE.

Mohammad Reza Pooshideh received the B.Sc. degree in Electrical engineering from Shahid Rajaie University of Tehran of Iran in 2006 and the M.Sc. degree in Electronic engineering with honors from Tarbiat Moallem University of Sabzevar, Iran in 2010, respectively. His research interests include network security, signal processing and image and video processing and their applications**.**