A Secure SCADA System using MiniSec Sensor Network

Kousik Maity[1], Purnendu Chakraborty[2], Bidisha Goswami[2], Arup Paul[2], Arumoy Saha[3]

[1] Dept. of E.C.E., Bengal Institute of Technology, WBUT , Kolkata W. B., India
[2]Dept. of E.C.E., Future Institute of Engg. & Management, WBUT, Kolkata, W. B., India
[3] Dept. of I.T, Bengal Institute of Technology, WBUT , Kolkata W. B., India

Abstract- SCADA refers to a large-scale, distributed measurement(and control) system. SCADA is not a specific technology, but a type of application. SCADA stands for Supervisory Control and Data Acquisition — any application that gets data about a system in order to control that system is a SCADA application. A SCADA application has two elements:

1. The process/system/machinery we want to monitor a control — this can be a power plant, a watersystem, a network, a system of traffic lights, or anything else.

2. A network of intelligent devices that interfaces with the first system through sensors and control outputs.

Now modern SCADA system network are associated with large area through LAN/WAN. So automatically the secure security system of SCADA is necessary and for that in this paper we have propose a complete secure SCADA system base on the MiniSec, a secure network layer protocol for wireless sensor networks.By simulation we have shown that it will perform more securely then other SCADA system.

Index Terms- SCADA, RTU, MiniSec Network, TinySec Network, ZigBee Network

I. INTRODUCTION

SCADA systems are used to automate complex industrial processes where human controls impractical — systems where there are more control factors, and more fast-moving control factors, than human beings can comfortably manage.

Around the world, SCADA systems control:

• **Electric power generation, transmission and distribution:** SCADA is used around the world to control all kinds of industrial processes — SCADA can help us increase efficiency,lower costs and increase the profitability of your operations.tems to detect current flow and line voltage, to monitor the operation of circuit breakers, and totake sections of the power grid online or offline.

• **Water and sewage:** State and municipal water utilities use SCADA to monitor and regulate waterflow, reservoir levels, pipe pressure and other factors.

• **Buildings, facilities and environments:** Facility managers use SCADA to control HVAC, refrigeration units, lighting and entry systems.

• **Manufacturing:** SCADA systems manage parts inventories for just-in-time manufacturing, regulate industrial automation and robots, and monitor process and quality control.

• **Mass transit:** Transit authorities use SCADA to regulate electricity to subways, trams and trolley buses; to automate traffic signals for rail systems; to track and locate trains and buses; and to control railroad crossing gates.

• **Traffic signals:** SCADA regulates traffic lights, controls traffic flow and detects out-of-order signals.

Components of the SCADA system:

A SCADA system performs four functions:

1. Data acquisition
2. Networked data communication
3. Data presentation
4. Control

These functions are performed by four kinds of SCADA components:

1. **Sensors** (either digital or analog) and **control relays** that directly interface with the managed system.

2. **Remote telemetry units (RTUs).** These are small computerized units deployed in the field at specific sites and locations. RTUs serve as local collection points for gathering reports from sensors and delivering commands to control relays.

3. **SCADA master units.** These are larger computer consoles that serve as the central processor for the SCADA system. Master units provide a human interface to the system and automatically regulate the managed system in response to sensor inputs.

4. The **communications network** that connects the SCADA master unit to the RTUs in the field.

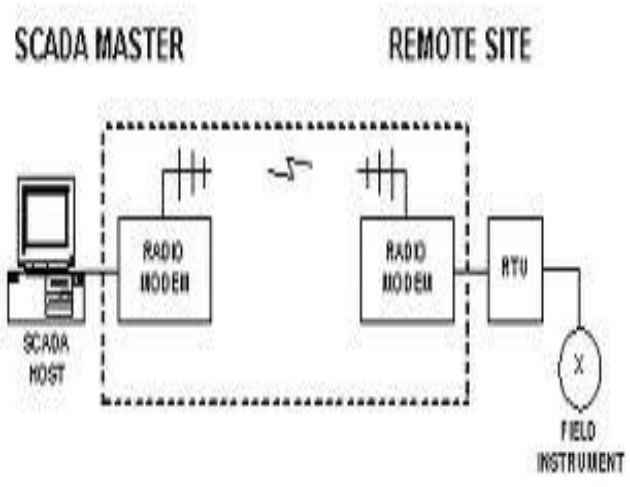

Fig: SCADA System

II. RELATED WORK

In this section, we describe recent works related to this paper. [9] offered an overview of technologies related to SCADA systems. Security issues regarding SCADA systems were discussed in [10, 2, 1]. In [10], Miller discussed the importance of the availability of process control systems within critical infrastructure systems and tried to call attention to the security aspects of these systems. In [1], Igure etal. did a survey on the research challenges of the security of modern SCADA systems. In [5], Goeke et al. examined the weakness of SCADA systems and proposed corresponding solutions. In [11], the U.S. Department of Energy proposed 21 suggestions to prevent attacks from the communication networks.In [12], Cheung et al. proposed a method to detect attacks towards SCADA systems using model-based intrusion detection. None of these studies considered the use of security patterns.

Security patterns.

Security patterns were first proposed as a research paper by Yoder et al. in [14]. [13] reviewed most of the existing security patterns and provided system designers with guidelines for using security patterns to build secure systems. More information regarding the concepts of security patterns and the principles of building secure systems using security patterns were illustrated in [6, 15]. None of the proposed patterns apply specifically to SCADA systems.

Attacks Against SCADA Systems

In today's corporate environment, internal networks are used for all corporate communications, including SCADA. SCADA systems are therefore vulnerable to many of the same threats as any TCP/IP-based system. SCADA Administrators and Industrial Systems Analysts are often deceived into thinking that since their industrial networks are on separate systems from the corporate network, they are safe form outside attacks. PLCs and RTUs are usually polled by other 3rd party vendor-specific networks and protocols like RS-232, RS-485, MODBUS4, and DNP, and are usually done over phone lines, leased private frame relay circuits, satellite systems, licensed and spread spectrum radios, and other token-ring bus topology systems. This often gives the SCADA System Administrators a false sense of security since they assume that these end devices are protected by these non-corporate network connections. Security in an industrial network can be compromised in many places along the system and is most easily compromised at the SCADA host or control room level. SCADA computers logging data out to some back-office database repositories must be on the same physical network as the back-end database systems, or have a path to access these database systems. This means that there is a path back to the SCADA systems and eventually the end devices through their corporate network. Once the corporate network is compromised, then any IP-based device or computer system can be accessed. These connections are open 24x7 to allow full-time logging, which provides an opportunity to attack the SCADA host system with any of the following attacks:

• Use a Denial of Service (DoS) attack to crash the SCADA server leading to shutdown condition (System Downtime and Loss of Operations)

• Delete system files on the SCADA server (System Downtime and Loss of
Operations)

• Plant a Trojan and take complete control of system (Gain complete control of system and be able to issue any commands available to Operators)

• Log keystrokes from Operators and obtain usernames and passwords (Preparation for future take down)

• Log any company-sensitive operational data for personal or competition usage (Loss of Corporate Competitive Advantage)

• Change data points or deceive Operators into thinking control process is out of control and must be shut down (Downtime and Loss of Corporate Data)

• Modify any logged data in remote database system (Loss of Corporate Data)

• Use SCADA Server as a launching point to defame and compromise other system components within corporate network. (IP Spoofing).

So the SCADA Security Problem are-
1.SCADA Network Vulnerabilities Unveiled
2. Internet Connection = Cyber Attacks Now Possible
3. Common Operating System Vulnerabilities Exposed
4. Legacy and Newer Equipment Incompatibilities
5. Online Protocol Libraries & System Documentation
6. Electrical Power Utility Deregulation
7. Competitive Industry
8. Security & Network Upgrades = Higher Costs
9. Physical Threats
10. Insider Threats
11.Terrorist Threats (Heightened After 9-11 Attacks)
12. Nation State Level Threats

III. PROPOSE WORK

So to solve those above problem of SCADA we need a network which can provide more security and as we know for Secure sensor network communication protocols need to provide three basic properties: data secrecy, authentication, and replay protection. Secure sensor network link layer protocols such as Tiny-Sec and ZigBee enjoy significant attention in this type of operation.

However, TinySec achieves low energy consumption by reducing the level of security provided. In contrast, ZigBee enjoys high security, but suffers from high energy consumption. MiniSec is a secure network layer that obtains the best of both worlds: low energy consumption and high security. MiniSec has two operating modes, one tailored for single-source communication, and another tailored for multi-source broadcast communication.The latter does not require per-sender state for replay protection and thus scales to large networks.

DREAW BACK OF PRIVIOUS SENSOR NETWORK

Considerable attention had been paid to developing secure sensor network communication protocols. Unfortunately, existing technologies, such as TinySec and ZigBee, are unable to achieve low_This research was supported in part by CyLab at Carnegie Mellon under grant DAAD19-02-1-0389 from the

Army Research Of_ce,and grants CNS-0347807 and CCF-0424422 from the National Science Foundation, and by a gift from Bosch. Virgil Gligor's work was supported by the US Army Research Laboratory under the Cooperative Agreement DAAD19-01-2-0011 for the Collaborative Technology. MiniSec, a secure network layer protocol for wireless sensor networks. simultaneously providing the three important properties of secure communication: secrecy, authentication, and message replay protection.TinySec, a popular secure link layer protocol, achieves low energy consumption and memory usage. Unfortunately, it also sacrices on the level of security. For example, it employs a single network-wide key, such that every node in the network can masquerade as any other node. Second, TinySec does not attempt to protect against replay attacks. ZigBee provides a higher level of security than TinySec since it is not restricted to a network-wide key. By keeping a per-message counter as the Initialization Vector (IV), ZigBee protects against message replay attacks. However, ZigBee is an expensive protocol. First, ZigBee sends the entire 8-byte IV with each packet, resulting in high communication overhead and high energy consumption by the radio. Also, ZigBee requires per-sender state, which consumes a large amount of memory as the number of participants increases

ADVANTAGE OF THE NETWORK

MiniSec, a secure network layer protocol for wireless sensor networks. We achieve the best of both worlds: lower energy consumption than TinySec, and a high level of security like ZigBee. We accomplish this by leveraging three techniques. First, we employ a block cipher mode of operation that provides both secrecy and authenticity in only one pass over the message data. Second, we send only a few bits of the IV,while retaining the security of a full-length IV per packet. In contrast, previous approaches require two passes over the plaintext (one for encryption and one for authentication) and transmission of the full-length IV.

Desired Properties

We now present the desired properties of a secure sensor network communication architecture.

Data Authentication.

Data authentication empowers legitimate nodes to verify whether a message indeed originated from another legitimate node (i.e., a node with which it shares a secret key) and was unchanged during transmission. As a result, illegitimate nodes should not be able to participate in the network, either by injecting their own messages or by modifying legitimate messages. Data authentication is one of the basic building blocks of a secure system. For example, nodes need to verify commands from the base station, and a base station needs to authenticate whether the data readings indeed originate from valid nodes. Typically, data authentication is achieved by the sender computing a message-authentication code (MAC) over the payload and appending that to the message. Upon reception, the packet is considered to be valid if the receiver recomputes the MAC and it matches with the received MAC. ZigBee, TinySec and SNEP provide data authentication by using the CBC-MAC function, using Skipjack or RC5 as the block cipher.

Data Secrecy.

Data secrecy, another basic requirement of any secure communication system, prevents unauthorized parties from discovering the plaintext. It is typically accomplished by setting up an encrypted communication channel. Encryption schemes or modes can be evaluated based on different criteria. A strong level of security is the notion of *semantic security* [3, 9]. The Handbook of Applied Cryptography de_nes semantic security such that .a passive adversary with polynomially bounded computational resources can learn nothing about the plaintext from the cipher text. Semantic security implies that an eavesdropper cannot gain any information about the plaintext, even after observing many encryptions of the same plaintext.

In secure communication protocols, data secrecy is provided by a cryptographic encryption scheme. To guarantee semantic security, we typically require a probabilistic encryption scheme and an unique initialization vector (or IV) for each encryption to add variation to the ciphertext. TinySec uses CBC-encryption, while SNEP and ZigBee employ counter-mode encryption. MiniSec provides both authentication and secrecy using OCB-encryption with a non-repeating counter.

Replay Protection.

A replay attack is when attackers record entire packets and replay them at a later time. TinySec is not resilient to such an attack, while SNEP provides protection using a counter. MiniSec provides replay protection in the unicast and broadcast setting, respectively.

Freshness.

Since sensor nodes often stream time-varying measurements, providing guarantee of message freshness is an important property. There are two types of freshness: strong freshness and weak freshness. MiniSec provides a mechanism to guarantee weak freshness, where a receiver can determine a partial ordering over received messages without a local reference time point. Note that both ZigBee and SNEP provide weak freshness, while TinySec does not provide any form of freshness.

Low Energy Overhead.

Energy is an extremely scarce resource in sensor nodes. Thus, it is of paramount importance for the security protocol to retain a low energy overhead.On the Telos platform, sending a single byte is equivalent to executing about 4720 instructions. Thus, to reduce energy consumption, it is imperative to minimize communication overhead. Although public key cryptography had enjoyed major advancement recently, it is still 3.4 orders of magnitude more expensive than symmetric cryptography in typical sensor nodes. Because it requires less energy consumed by the processor, security protocols that only employ symmetric cryptography are preferred in sensor network applications.

Resilient to Lost Messages.

The relatively high occurrence of dropped packets in wireless sensor networks requires a design that can tolerate high message loss rates.

IV. SIMULATION RESULTS

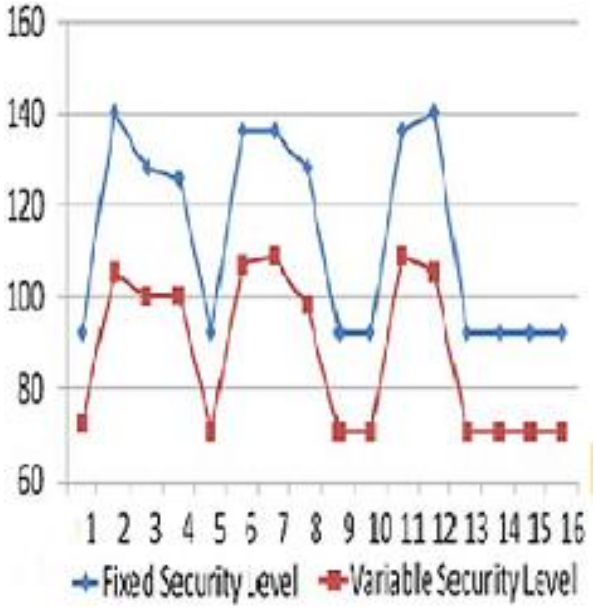

Fig:- 2

In the above figure a comparison is done between using fixed security level and variable security level over SCADA network. The figure state that using the Minisec sensor protocol network the variable security level is greaduely decreasing so the network is becoming more secure.

V. CONCLUSION

So using the Minisec secure sensor network protocol the total entire system of the SCADA become more trustable and efficiency.As the MiniSec network protocol has low energy consumption and high security so it is more cost effective.

REFERENCES

[1] D. Goeke and H. Nguyen. SCADA system security. http://islab.oregonstate.edu/koc/ ece478/05Report/Goeke-Nguyen.pdf, 2005.

[2] V. M. Igure, S. A. Laughter, and R. D. Williams. Security issues in SCADA networks. Journal of the Computers & Security, 25(7):498–506, 2006.

[3] A. Risley, J. Roberts, and P. Ladow. Electronic security of real-time protection and SCADA communications. In Proc.of the 5th Annual Western Power Delivery Automation Conference, 1-3 April 2003.

[4] E. Byres and J. Lowe. The myths and facts behind cyber security risks for industrial control systems. In Proc. of VDE Congress, Berlin, Germany, 2004.

[5] E. B. Fernandez, M. VanHilst, M. M. L. Petrie, and S. Huang. Defining security requirements through misuse actions. Advanced Software Engineering: Expanding the Frontiers of Software Technology, 219:123–137, 2006.

[6] E. B. Fernandez and R. Pan. A pattern language for security models. In Proc. of the 8th Annual Conference on the PatternLanguages of Programs (PLoP 2001), Urbana, Illinois, USA,11-15 September 2001.

[7] T. Priebe, E. B. Fernandez, J. I. Mehlau, and G. Pernul. Apattern system for access control. In Proc. of the 18th. Annual IFIP WG 11.3 Working Conference on Data and ApplicationsSecurity, 2004.

[8] A. Braga, C. Rubira, and R. Dahab. Pattern Languages of Program Design 4, chapter 16, Tropyc: A pattern language for cryptographic object-oriented software. Addison Wesley Publishing Company, 1999. Also in Proc. of PLoP, 1998.

[9] S. A. Boyer. Supervisory Control and Data Acquisition. ISA– The Instrumentation, Systems and Automation, 1999.

[10] A. Miller. Trends in process control systems security. IEEE Security and Privacy, 3(5):57–60, 2005.

[11] U.S. Department Of Energy. 21 steps to improve cyber security of SCADA networks.http://www.oe.netl.doe.gov/docs/

[12] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner,and A. Valdes. Using model-based intrusion detection for SCADA networks. In Proc. of the SCADA Security Scientific Symposium, Miami Beach, FL, USA, January 2007.

[13] M. Schumacher, E. B. Fernandez, D. Hybertson, F. Buschmann, and P. Sommerlad. Security Patterns: Integrating Security and Systems Engineering. John Wiley &Sons, Inc., 2006.

[14] J. Yoder and J. Barcalow. Architectural patterns for enabling application security. In Proc. of PLoP, 1997. Also Chapter15 in Pattern Languages of Program Design, vol. 4 (N.Harrison, B. Foote, and H. Rohnert, Eds.), Addison-Wesley,2000.

[15] E. B. Fernandez. Security patterns. In Proc. of International Symposium on System and Information Security, 2006.

AUTHORS

First Author – Kousik Maity, currently pursuing B.Tech in Electronics & Communication Engineering at Bengal Institute of Technology under West Bengal University of Technology. His research interest includes robotics & wireless Communication.

Second Author – Purnendu Chakraboty, currently pursuing B.Tech in Electronics & Communication Engineering at Future Institute of Engineering & Management under West Bengal University of Technology. His research interest includes robotics & wireless Communication.

Third Author - Bidisha Goswami, currently pursuing B.Tech in Electronics & Communication Engineering at Future Institute of Engineering & Management under West Bengal University of Technology. Her research interest includes robotics & wireless Communication.

Fourth Author – Arup Paul, currently pursuing B.Tech in Electronics & Communication Engineering at Future Institute of Engineering & Management under West Bengal University of Technology. His research interest includes wireless Communication.

Fifth Author – Arumoy Saha, currently pursuing B.Tech in Information Technology at Bengal Institute of Technology under West Bengal University of Technology. His research interest includes wireless Communication & satellite communication.