A Security Mechanism for Remote Monitoring System Security using Smartphone

Sungjae Yu Chau Ngoc Tu Souhwan Jung
School of Electronic Engineering
Soongsil University
SEOUL, KOREA
{ysj77777, chaungoctu, souhwanj}@ssu.ac.kr

***Abstract*—This paper proposes a security mechanism for remote monitoring system through a combination between user's password and random number by using SMS service over 3G networks. By using random number and phone number, this mechanism is not only able to provide robust security from replay attack and dictionary attack but also provide an efficiency user authentication method. Based on above idea, we have designed and developed secure remote control system. Developed remote monitoring system is for applying more security into monitor procedure inside factory using mobile node. This approach provides more enhanced security than existing mechanisms that only use ID/PW as an authentication method.**

Keywords-component; Remote monitoring system; Smartphone; Security event; Security alarm

I. INTRODUCTION

In recent years, wired/wireless M2M network research has been actively applying to support process automation system in industrial facilities. Wired networks are generally in the plant control system and management system, and are applied to the industrial plant backbone. Wireless is applied in harsh industrial environment which is difficult to connect by the cable installation. By using wireless network, the automation system can support mobility devices, so plant administrator can easily manages the process inside the industrial. Unit domain network's devices can be managed by system in the plant network as well as external networks. Plant administrator can use a mobile device in the external networks to control and monitoring in plant devices. In addition, administrator can communicate with devices in the other unit domains.

For this reason, SCADA (Supervisory Control And Data Acquisition) system must connect to the internet, and the security solution for protecting control system is required.[5][9] Through the internet, the infrastructure of electricity, gas, water, heating, railways, and roads can be connected. Although importance infrastructure has been distinguished using intranet, attacker still able to access, control and steal information via the network. Because of that, a solution to defend again security threats, and research about technology of controlling system or devices in the factory using mobile device (smart phone, tablet pc, etc...) are in need.

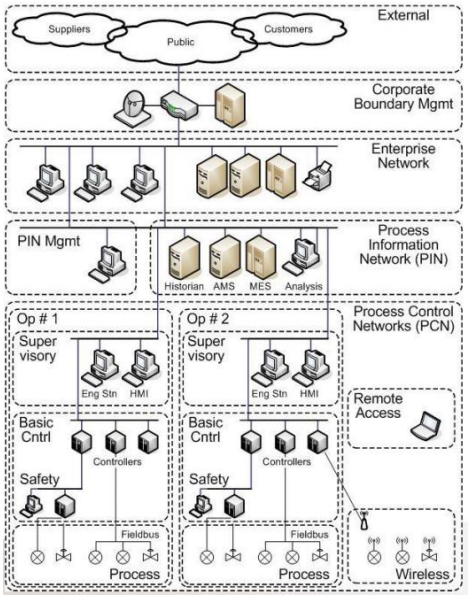

Figure 1. Network architecture in Industrial environment (ANSI/ISA99 std)

Proposed system is designed for monitoring and controlling the industry environment securely using mobile device. The paper is organized as follows. In section Ⅱ, we introduce the existing security scheme in the industrial environment. In section Ⅲ, proposed scheme and the system are given. In section Ⅳ, we introduce the design of remote control system. And the security strength of system is evaluated in section Ⅴ.

II. RELATED WORK

A. Security standards of SCADA

In the last 10 years, there are many security incidents in the plant resulted in significant loss of financial and life. We distributed incidents based on recent cases occurred in the control network security as follows:

- Poor Network Segmentation; Most of the control network is connected to the intranet and there are no distinguish within Sub-systems. As a result, if problem occurs, it quickly propagates through control network.

- Soft Target; Unable to implement security update periodically because of fully operating PCs connected to the control network.
- Multiple Network Entry Point; Most of the cyber-attack on the network is through the Secondary Point approach (For example USB keys, Maintain port for connection, Laptops, etc.), these points can be easily configured to allow access through the control system.

As previously mentioned, the cause of security incidents occurred in industrial facilities commonly relate to the connection of external network. Since earlier a closed-SCADA system has been turned into an open-SCADA system, because of security incidents described above, the importance and necessity of security was a significant incidence. As a result, SCADA security standard that defines the security protocol also occurred. Organizations that develop standard can be distributed to government-funded research institutions, product manufacturers that develop De-facto standard, non-profit organizations in the automation standards and such as ISA (International Society of Automation).

- FERC/NERC CIP; General manager of the U.S. Energy FERC (Federal Energy Regulatory Commission) due to cyber security threats, in order to prevent the occurrence of pre-NERC (North American Electric Reliability Corporation) to others U.S. power system, presented the eight reliability CIP (Critical Infrastructure Protection) standards.[8]
- ANSI/ISA99; In ISA, the control system (DCS, PLC, SCADA, network equipment) which maintains and assets the security of sensitive information during the system /network configuration were presented that allow you to prevent the loss of network / system design criteria.[7]
- IEC 62443; IEC (International Electro technical Commission) standards in the industry for a variety of networks are presented. Among them, the IEC 62443 'Security for industrial process measurement and control - Network and system' for the equipment security used for the purpose to define standards in the control network has been released.[9]

Double Defined from the ISA 'ANSI/ISA99 Security Standards for Improved Security and Reliability' aim at the separation of the business network and control network (Firewall), as well as through a simple security mechanism within the control system to control the distribution of functional level or degree of risk assets Layer broken down by management to emphasize the concept of Zones and Conduits.

The existing system of control equipment connected to SCADA network for PLC (Programmable Logic Controller) communication (which facilitates the tracking of traffic) is used to limit the Port (502/tcp) to prevent the attacker's approach. In this way, it's useful to install one Firewall between b network and control network, but outside there is a risk that could cause by the attacker who can operate Filtering thought Port traffic of entire SCADA equipment.

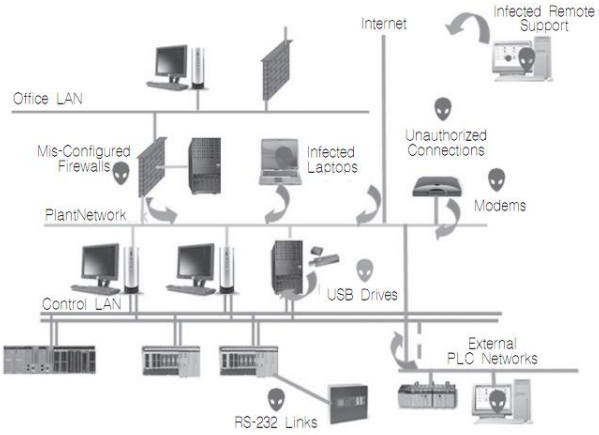

Figure 2. Risk factors in plant system

In addition, industrial facilities that must be used in real-time for controlling equipment and the security patches for control system that may not be able to manage have made the blind spot. In existing system, there is only a SCADA control network in Intranet, and Firewall is setup between SCADA control network and Internet. This formation has a problem, if attacker creates a hole in firewall, all network system will be broken-down, but if the concept of "Zones & Conduits" proposed by ISA99 is applied to security system, it will increase the security structure.[7] However these standards are vulnerable because they don't have security scheme to prevent attacker from connecting through external network and until now there is no mobile device authentication of external network in these standards.

B. Security Management Integration

Earlier secure communication in industrial facilities is designed to support security mechanisms in only intrusion detection system (firewall) level, but recently, from the aspect culminated in specializations have included IDS (Intrusion detection), Virtual Private Network(VPN), system security, authentication, virus, data backups. Each of the security technologies that have the confidentiality, integrity, availability, and access control features such as the mutual interaction is needed. In the industrial environment, there are many security problems in systems because security policies in the past mainframe environment cannot properly applied to the client/server computing environment. "Like this, is too difficult to keep security conduct professional and subdivided functions according to the development trend."

Figure 3. Zone & Conduits presented by ANSI/ISA99

Identify applicable sponsor/s here. *(sponsors)*

Currently, these administrative and functional issues are being studied with an effort to complete the integrated security management (Enterprise Security Management: ESM). To create a security monitoring system, we must integrate security solution of various vendors and this means we must develop proper ESM. ESM consists of IDS (Intrusion Detection System), IPS (Intrusion Prevention System), VPN, etc ESM is not only system manager but also a security manager. As the security manager aspect, ESM integrates Firewall, VPN, Virus Scanning, Content filtering, URL monitoring and filtering, intrusion detection. To cover not only from authentication, monitoring authorization, and access control but also to network manager, we research ESM for-all "one tools (One tool to cover everything).

ESM means enterprise solution that can manage products from the different vendors as well as same vendors and provides security solution like IPS, IDS, VPN, authentication/encryption/decryption products, Virus Scanning products, and Backup solution through central management module. ESM can also provide the enterprise security policies with heterogeneous security solution and interoperability. ESM makes security policies and according to these security policies, it provides monitoring and event alarm for quick action. ESM can be divided into:

- First, it is a system and policy management. ESM used to administrate aspects of the personality, rather than the side of a secure system. Security or management policies in accordance with the user and access permission management are focused. In this case, there are eTrust of CA and Unisys Corporation.
- Second, ESM focus on the vulnerability and risk analysis for security management. ESM monitors and analyzes vulnerability of network and system as well as risk factors. In this case, there are provider-1 of Checkpoint, and Symantec Corporation.

Security protocol standards made by vendors are OPSEC (OPerations SECurity), IAP (Intrusion Alert Protocol), many vendors made central management module using OPSEC and try to make other's standards but these standards are not international standards yet. In recently time, ESM provides agents for detecting intrusion and monitoring states of network devices in control areas. Using agents, administrator can monitor all of the systems through central control center. But there is no authentication of mobile devices and users through external network using remote monitoring system.

III. PROPSED SCHEME

A. Environment

In this paper, proposed Remote monitoring system offers without modification of the existing SCADA system. This system is developed for monitoring and controlling industrial facilities securely. Security administrator manages systems in internal/external of plant using this remote monitoring system. Through the wireless M2M network of process automation system and homes being developed for this system, Figure 4 illustrates a hierarchical structure which is applied to the network.

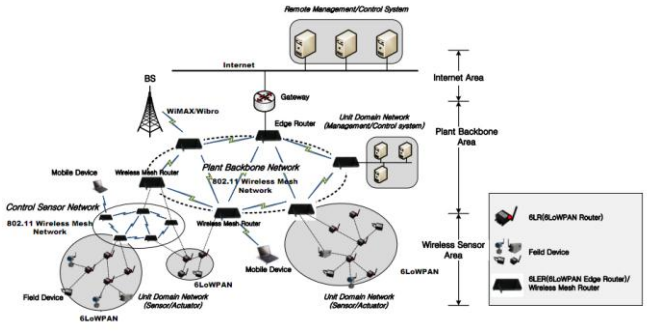

Figure 4. IISA100.11a Hierarchical structure according to the industrial network

In Figure 4, in plant intranet and external networks are protected by the Firewall, ISA99 and ISA100.11a standards mentioned above are implemented. With information of sensors, processes, devices and security log records, administrator can analyze this information through HMI and central monitoring system.[1] By applying security protocol to this system using this method, administrator can confirm information through smart phone of external network. The system also provides CCTV security to capture a video when there is motion detection and alarm to the administrator. The report can be sent to administrator's smart phone using through 3G network.

B. Procedure of the system

In this paper, proposed Remote system provides access control through authentication of user and mobile device. User who wants to connect to the system must input ID and Password for authentication and his/her smart phone can share encryption/decryption key with systems of plant using "Random Number" which sent by systems through 3 network. According to ISA99 standard, connecting from device in external network to internal system of plant is limited except area of PIN (Process Information Network). In this paper, proposed system will be divided into three stages.

1) Event Detection

In this system, the certificated equipment (visual equipment, sensors, etc..) inside the Industrial Facilities is used to identify the attacker's movements. If unauthorized access occurs, sensor device and video camera send information of log and video to PIN using PLC. PIN distinguishes security threats using context information (time, access information, location etc.) PIN sends event information to Administrator's smart phone using SMS service.

2) Security Protocol

After smart phone receives SMS with system identification for distinguishes event log, smart phone turns on application automatically. SMS content consists of random number and system ID. After application turned on, user can input ID/Password and connects to system. Smart phone can make encryption/decryption key ($K_{symmetric}$) using "Random Number" and user password, using Hash function.

$$K_{symmetric} = H(random\ number, PW) \quad (1)$$

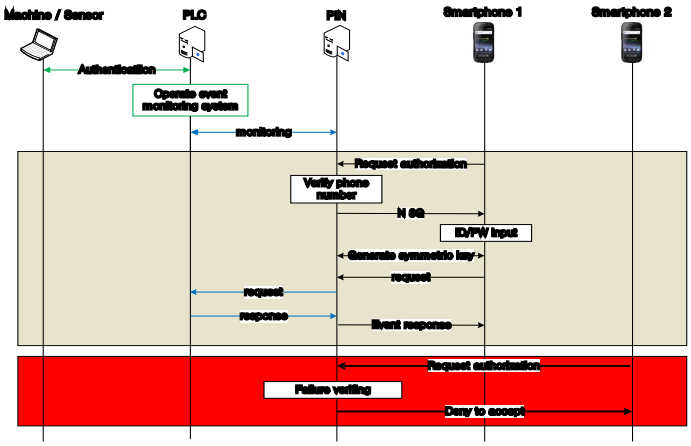

Figure 5. Security protocol of proposed remote monitoring system

The smartphone can communicate with PIN using this key. Because "Random Number" is changed for every attacker can't implement replay attack. "Random Number" is sent to authorized smart phone by phone number of user through 3G network, existing authentication scheme based on ID/Password vulnerable to replay attack or dictionary attack, but for attacking this system, attacker must steal both phone physically and user password.

3) Event Monitoring

Authenticated user who uses authorized smart phone can access information of log in DB through "Random N and password and user can save information (For example: Intrusion types, and intrusion in their logs the time, place, CCTV images are recorded which stored in DB) in smart phone and monitor log event. The record log and video information are encrypted using $K_{symmetric}$ made by security protocol.

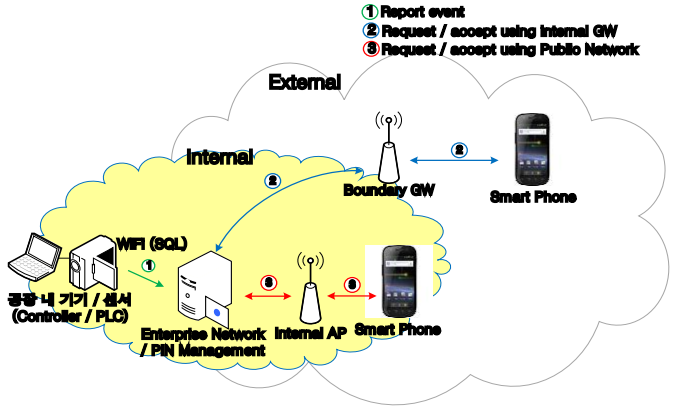

Figure 6. Procedure of proposed system

IV. Remote Control System Design

A. Goal of Design

In this paper, remote control/monitoring system is designed so that when security problem occurs, system stores information of log and videos into DB of central management system and user can confirm it securely through smart phone. There is one gateway for connecting PIN and smart phone of external network can connect to system through only this gateway and this type of system uses based on the concept "Zone & Conduit "of ISA99 standard. System architecture of M2M network is designed according to ISA100.11a standard and information of sensor/process of M2M network is sent to smart phone. All procedures of this system are automatic except the process of user's ID/Password input.

B. Environment Configuration

The environment of this system is configured M2M network in industrial plant. Developed M2M network is consisted of sensor, actuators, control/monitoring systems and Gateway. Figure 8 illustrates the developed M2M network 6 sensor devices made topology of wireless mesh network and sensing data is sent to monitoring system (For example: HMI or PIN). The monitoring system can monitor states of devices or information of process as well as security threats through VTC (Virtual Topology Controller) tool and CoAP (Constrained Application Protocol) browser. Monitoring system can transfer particular information to Mobile Device when strange situation occurs and user can verify through mobile device.

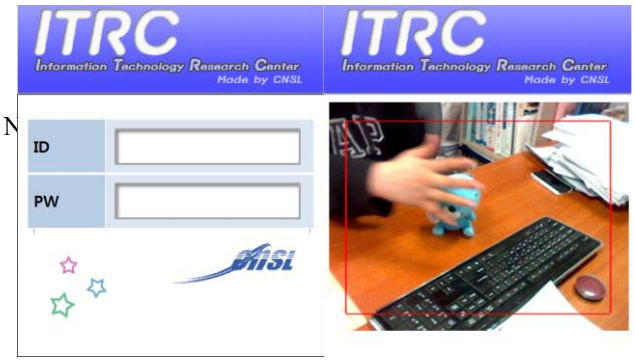

Figure 7. Remote monitoring system application UI of smart phone

C. System

The environment of developed remote control system consists of 2 computers, wireless router and smartphone. The PC1 acting PLC is installed WINDOWS XP. The MFC program in the PC1 analyzes the video of camcorder and save video of camcorder. The MFC program using VFW (Video For Windows) extracts parameters of video by comparing with current video parameters and average parameters. Parameters are average value of outline and color in image. The average of parameters in recent video have more weight If the program finds erratic movements, PC1 send video data and log information to PC2. The Data sent PC1 is stored in DB of PC2 (PIN). The PC2 acting PIN is installed APM (Apache, PHP, MySQL). The MFC program in PC2 sends SMS to smartphone of external network when system confirms security threats. The wireless router is the role of internal/external BS (Base

Station). The PC2 send SMS to smartphone by confirming phone number of user through wireless router. SMS service consists of random number and system ID. The smartphone based android turn on the application when PIN's SMS is arrived. User who wants to connect to system can input ID/PW. The smartphone application can make key consisted of random number and user PW. The smartphone can communicate with PIN using this key securely. After input ID/PW, User can connect UI of PIN system based Web. The UI is served by APM of PIN and User can confirm log information and video data of MySQL DB through UI.

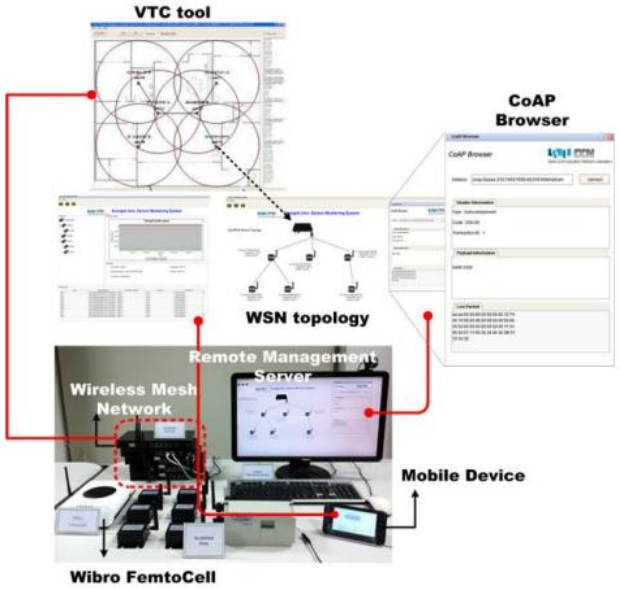

Figure 8. Implementation and test environment

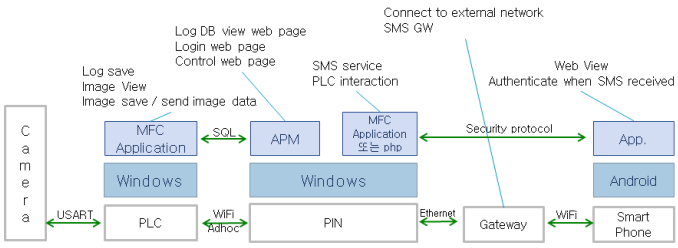

Figure 9. Structure of proposed remote monitoring system

V. CONCLUSION

Network system for process automation, machine control and monitoring in industrial environments is requiring remote control / monitoring system to help plant managers who want to keep things fast and convenient. But all connected systems to internet in the factory can be vulnerable to external attacks due to the open of infrastructure. It can cause significant financial damage to enterprise and loss of life.

The proposed security mechanism provides robust authentication by combining between users and their equipment for monitoring system remotely in a secure way. SMS is sent by system to user smartphone through phone number. As soon as receiving SMS, smartphone turn on application for connecting system automatically. User who wants to connect to system must input ID/PW for authentication and smartphone that was registered as user's device shares symmetric key with system. Shared key is made of user PW and random number and transferred through 3G network. Because system uses random number, attacker can't attempt to replay attack or dictionary attack. For attacking system, attacker must steal both random numbers that sent from system through 3G network and user's password.

This approach provides more enhanced security than existing systems that only use ID/PW as an authentication method. By using this method, plant administrator can secure monitor information and report about security threats in factory securely. Under Zone & Conduits concept of ISA99 standard the external access to the system, limited to area of PIN in this remote system,

ACKNOWLEDGMENT

This research was supported by the MKE (The Ministry of Knowledge Economy), Korea, under the Convergence-ITRC (Convergence Information Technology Research Center) support program (NIPA-2011 C6150-1101-0004) supervised by the NIPA (National IT Industry Promotion Agency)

REFERENCES

[1] ISA100.11a-2009, International Society of Automation, Wireless Systems for Industrial Automation : Process Control and Related Applications, 2009.

[2] Gray, Basu,"Turbine control system upgrade for Bruce Nuclear plant units 1 and 2", IEEE International Conference on Electro/Information Technology, September, 2009.

[3] A. Nakrachi, C. Chera, C. Dimon, Air-stram and Temperature Plant Remote Control," IMACS Multiconference on "Computational Engineering in Systems Applications"(CESA), October 4-6, 2006.

[4] Critical Infrastructure Protection : Challenges and Efforts to Secure Control Systems, GAO-04-354, GAO, 2004.

[5] Perspectives on the future of control system security, Jeff Dagle, PE, SANS process control & SCADA security summit 2006, march, 2006.

[6] SPP-ICS(system protection profile- Industrial control system), NIST, 2004.

[7] ANSI/ISA-TR99.00.01-2007, Security Technologies for Manufacturing and Control Systems, ISA, 2007.

[8] FERC/NERC CIP-002-3, Cyber Security –Critical Cyber Asset Identification, December, 2009.

[9] BS IEC 62443, Industrial Communication Network and System Security, Establishing an industrial automation and control system security program, June, 2011.

[10] Willig, Matheus, Wolisz, Wireless Technology in Industrial Netwoks. Proceedings of the IEEE, 2005.

[11] Draft-Sp800-82 guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Controal Systems Security, NIST, September, 2006.