A Security Mechanism for Automation Control in PLC-based Networks

[1]Joon Heo, [1]Choong Seon Hong, [2]Seong Ho Ju, [2]Yong Hun Lim, [2]Bum Suk Lee, [2]Duck Hwa Hyun
[1]Department of Computer Engineering, Kyung Hee University
1 Seochun, Giheung, Youngin, Gyeonggi, Korea, 449-701
[2]KEPRI KEPCO, Korea
[1]{heojoon, cshong}@khu.ac.kr, [2]{shju1052, adsac, leebs, hyundh}@kepri.re.kr

***Abstract*—In power line networks, the metering and control data can be modified by malicious attacker. We can expect that an attacker may be able to eavesdrop the transmission data, and may be able to send modified data to device for control system. This aspect is especially important if data should be used for billing or other power control purpose. In this paper, we propose a security provider using the encryption, key generation and authentication algorithm for automation system in PLC-based network. To prove the necessity and the efficiency of the proposed security mechanism, we have organized the automation metering system.**

***Keywords*—Security, Power Line Communication, Metering, Modbus**

I. INTRODUCTION

Power Line Communications is known for many years as Power Line Carrier. It uses the low bandwidth analog and digital information to communicate over the residential, commercial, and high voltage power lines for AMR (Automatic Metering Reading), home automation, and protective relay. The fast development of new communication services and the deregulation of the telecommunication market offer both electricity and telecom sectors a new significant business potential. The main idea of PLC is to use the electrical grid for the communication because it is an existing infrastructure and it covers a wider area than any other traditional communication networks. The topology of the power line network and the convenience of its power sockets as potential access points make it a good candidate for automation metering system[3][10].

The aim of the UPLC(Ubiquitous Power Line Communication) project (part of Korea Electric Power Corporation projects) is to design and develop a communication system, to provide metering and automation control service from the electric power company down to the home of the customers, using the exiting power-line infrastructure. The intended implementation will allow energy resource companies to remotely and autonomously control and monitor the use of various energy resources, while simultaneously allowing the infrastructure to be used for various services offered by the energy resource company. The developed system should allow various energy resource companies such electricity, gas or district heating companies to remotely monitor and control their energy resources via the same shared (public) distribution network. It is obvious that it is (economically) infeasible to replace existing infrastructure (e.g., meters). Hence, compatibility between existing technologies and the newly developed UPLC infrastructure must be accounted for. Due to the large geographic coverage of power-line networks and the public installation and operation, it is impossible to keep the network under exclusive control and surveillance, especially if equipment like meters are installed on private property. For these reasons the network and every link therein, must be assumed to be insecure, and not suitable for the transmission of sensitive data [2][9].

Similar problems were faced with the creation and development of the Internet. However the means, by which these problems were solved for the Internet, were found to be unsuitable for implementation within the PLC system. On the IP-based Private Networks the use of standard (Internet) technologies such as SSH tunneling is reasonable. These measures also have the advantage that they are already provided by most Application Servers. For the PLC network the situation is different especially due to the very small packets (typical 32 or 64 bytes) and high error rate (up to 20%) and limited bandwidth. Common Internet measures are not directly applicable; security services have to be adapted to the peculiarities of the PLC network to offer efficient usage [2][9].

Until now, researches on security method in PLC-based network mainly focused on data encryption [1] and using the secret key [10]. In this paper, we propose a new Security Provider for metering and automation control in PLC-based network. When a meter send the raw data to gathering device, the security provider encrypt the data and generate message authentication code using the secret key.

This paper is organized as follows. Section 2 includes system architecture of UPLC project. And we will explain the attack possibility of current architecture in section 3. Section 4 describes the proposed key generation, encryption and authentication module of security provider. Section 5 introduces public key based agreement mechanism for UPLC system. Implementation results of proposed mechanism are presented in section 6. Finally, we give some concluding remarks and future works.

II. System Architecture of UPLC Project

The UPLC system[9] is comprised of various components, namely meter such as electricity, water and gas, Power Conservation Monitoring (PCM) and Intelligent PLC Gateway (IPG), Integrated Regional Manager (IRM). According to the structure of the distribution network, the PLC-based network is also organized hierarchically (as shown in Figure 1). Application servers are either metering servers or automation servers. They are attached to the UPLC infrastructure via a private IP-based network or high-voltage power line network, which is connected to the power line communication system at the IRM. IPG are used to interconnect IRM and PCM. Finally meter and automation control device are connected to the PCM by standard protocol such as Modbus[5] and IEC 62056-61[15]. Data transmission is usually organized in a request-response or broadcast request scheme.

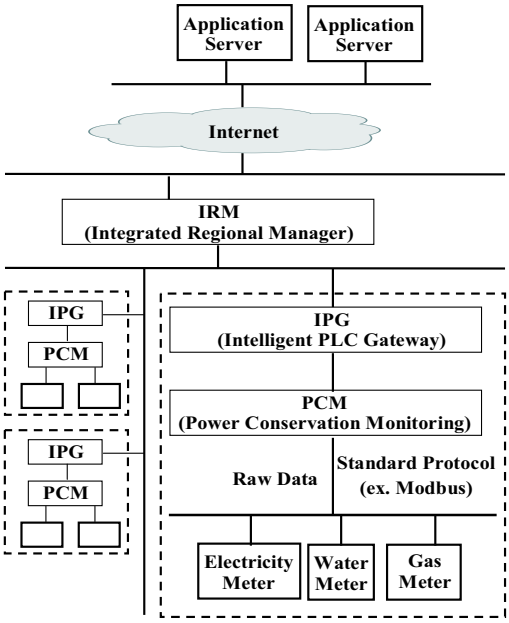

Fig. 1. UPLC system architecture

III. Possibility of Attack

The security concept of UPLC system must cope with two completely different networks and environments: an IP-based network with computationally powerful nodes like IPG, IRM and Application Servers and the field level with low bandwidth power line communication as well as meters or PCM device with low computational resources. Application Servers, IRMs and IPGs usually act as one entity differently privileged users are handled internally. Hence, it seems feasible to implement access control and integrity services on the basis of well-known servers. Configuration is in general static and the network interconnect is assumed to be stable. Additionally, these measures are already supported by existing operating systems commonly employed on Application Servers. The situation at the PLC network is a little bit different since performance considerations rule out the direct usage of standard IP security procedures[12][13]. According to figure 2 possible attacks on the services might be by eavesdropping and modification of data at the power line network or at the nodes. Theses devices are either directly integrated into the nodes or external components that use standardized protocols like Modbus or IEC 62056-61 to communicate. Up to now UPLC system only external device will be used. It is important to mention that the standard protocols used within UPLC do not support security measures. Figure 2 shows the security problem between meters and PCM in UPLC system. Until now, any security mechanism has not been developing for this section. Therefore the meters will send the raw data to PCM as plaintext type. Without difficulty attacker can eavesdrop and modify this data. This aspect is especially important if data should be used for billing or other power control purpose.

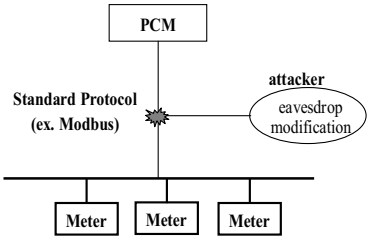

Fig. 2. Weakness between meters and PCM

IV. Proposed Security Provider

As shown in Figure 3, proposed security provider is composed of three modules, namely key generation module, encryption module and authentication module. The objective of this system is to provide security functions for PLC-based network. We describe each of these in the following subsections.

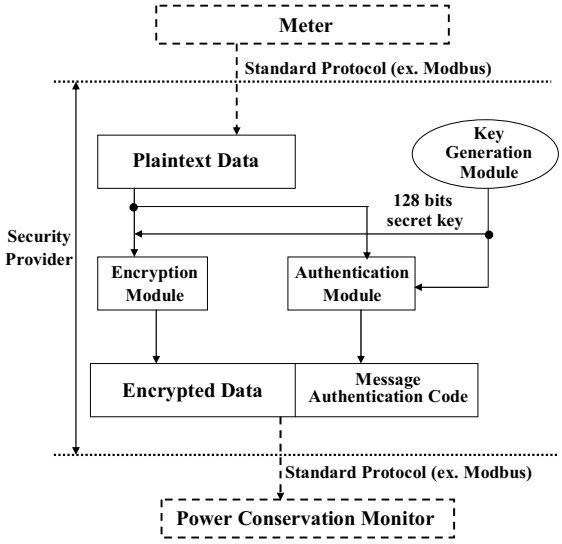

Fig. 3. Overall architecture for proposed Security Provider

A. Key Generation Module

A key generation module uses Diffie-Hellman algorithm [4] to generate secret key between meter and PCM. Let q be a prime number and α a primitive element of the prime number q. Then the powers of α generate all the distinct integers from 1 to q-1 in some order. Suppose the meter(m) chooses a random integer X_m and the PCM(p) a random integer X_p. Then the meter(m) picks a random number X_m from the integer set $\{1,2,\ldots,q\text{-}1\}$. The meter($m$) keeps X_m secret, but sends

$$Y_m \equiv \alpha^{Xm} (\text{mod } q)$$

to the PCM(p). Similarly, the PCM(p) choose a random integer X_p and sends

$$Y_p \equiv \alpha^{Xp} (\text{mod } q)$$

to the meter(m). Both meter(m) and PCM(p) can now compute;

$$K_{mp} \equiv \alpha^{XmXp} (\text{mod } q)$$

And use K_{mp} as their common key. The meter (m) computes K_{mp} by raising Y_p to the power X_m:

$$K_{mp} \equiv Y_p{}^{Xm} (\text{mod } q)$$
$$\equiv (\alpha^{Xp})^{Xm} (\text{mod } q)$$
$$\equiv \alpha^{XpXm}$$
$$\equiv \alpha^{XmXp} (\text{mod } q)$$

And the PCM(p) compute K_{mp} in a similar fashion:

$$K_{mp} \equiv Y_m{}^{Xp} (\text{mod } q)$$
$$\equiv (\alpha^{Xm})^{Xp}$$
$$\equiv \alpha^{XmXp} (\text{mod } q)$$

Thus, both meter(m) and PCM(p) have exchanged a secret key. Since X_m and X_p are private, the only available factors are the public values q, α, Y_m and Y_p.

If an attacker is able to analyze the keys, they will be compromised and an attacker is able to communicate with an IPG and meters respectively. To further reduce danger of compromising the keys it is desirable to update frequently used keys. The system should support functions that allow a PCM to inform key generation module of security provider that it should change to a new secret key.

B. Encryption Module

Strictly packet oriented communication and high probability of packet loss introduce further restrictions to the security system. Stream ciphers would be a very efficient solution for small packets, but they easily become very efficient on highly disturbed communication links due to the increasing effort to resynchronize them. Re-synchronization and initialization cause too much overhead. Moreover stream cipher can't be used because of high error rate of transmission packet. Hence, symmetric block cipher algorithms like triple DES (Data Encryption Standard) [8] and AES (Advanced Encryption Standard) [6][11] will be used for the majority of operations due to their good performance[2].

In security provider, an encryption module use AES as encryption algorithm. If we use the Modbus as transmission protocol between meter and PCM, the encrypted frame format is like Figure 4.

Station ID	Function	Byte Count	Encrypted Data	Error Check	MAC
1 Byte	1 Byte	1 Byte	16 Byte	1 Byte	16 Byte

Fig. 4. Encrypted raw data (when using the Modbus protocol)

C. Authentication Module

An authentication module uses HMAC-MD5 algorithm [7] to generate message integrity code. In this algorithm, secret key from key generation module is used. HMAC is a secret-key authentication algorithm which provides both data integrity and data origin authentication for packets sent between two parties. Its definition requires a cryptographic has function H and secret key K. H denotes a hash function where the message is hashed by iterating a basic compression function on data block. Let b denote the block length of 512bits for all hash function MD5. h denotes the length of hash values. The secret key K can be of any length up to b=512bits. Figure 5 illustrates the overall operation of authentication module.

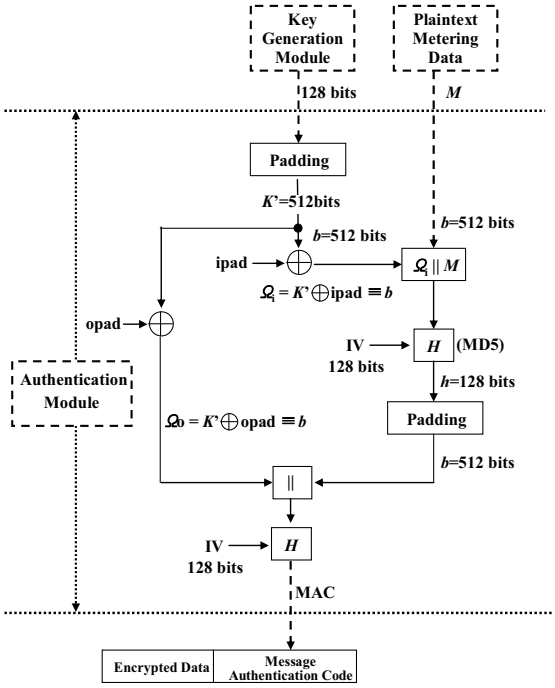

Fig. 5. The overall operation of authentication module

To compute HMAC over the message, the HMAC equation is expressed as follows [4]:

$$\text{MMAC} = H[(K \oplus \text{opad}) || H[(K \oplus \text{ipad}) || M]]$$

Where

ipad = 00110110(0x36) repeated 64 times (512bits)

opad = 01011100(0x5c) repeated 64 times (512bits)
ipad is inner padding, opad is outer padding

① Append zeros to the end of K to create a b-byte string (i.e. if K=128bits in length and b=512bits, then K will be appended with 384 zero bits)
② XOR(bitwise exclusive-OR) K' with ipad to produce the b-bit block computed in setp ①.
③ Append M to the b-byte string resulting from step ②.
④ Apply H to the stream generated in step ③.
⑤ XOR(bitwise exclusive-OR) K' with opad to produce the b-byte string computed in step ①.
⑥ Append the hash result H from step ④ to the b-byte string resulting from step ⑤.
⑦ Apply H to the stream generated in step ⑥ and output the result.

V. Public Key Based Secret Key Agreement

Additional security effort for UPLC system is an attempt to use the IRM for public key management of IPGs. A device with IRM capabilities is used to configure a system by provisioning initial trust parameters such as base point and elliptic curve coefficients to IPGs. Devices in the system use initial trust parameters to establish permanent public key and ephemeral public key, which are then used for secure communications of the actual payload. IPG need the capability to recognize an IRM before accepting initial trust parameters. Our proposed mechanism is based on the EC-MQV algorithm [14][16][17]. The IRM generates common parameters for Elliptic Curve algorithm and gives common parameters to IPG. Then IRM request IPG's public key when a new IPG requires initial registration with IRM. This paper assumes that only permitted IPG could receive the common parameter through initial registration process with IRM. Notations that are used in this mechanism:

- P: base point
- E: elliptic curve coefficients
- Q: permanent public key
- d: private key
- R: ephemeral public key
- k: ephemeral random data

A public key registration process is shown in Figure 6. All IPGs have registered their permanent public key (Q) to the IRM when join the system. The shared secret key agreement mechanism is shown in Figure 7; U is initiator IPG and V is responder IPG.

(a) When the U desire to generate the shared secret key with V, U requests the Q_V to the IRM.
(b) The IRM searches Q_U and Q_V in the public key management table.
(c) The IRM give Q_V and a flag (state=on) to U. A flag (state=on) means that U begins the request to V. And then the IRM give Q_U and a flag (state=off) to V.
(d) U generates ephemeral data (k_U) then generates R_U. And then U sends the R_U to V. Through the same procedure V sends the R_V to U.
(e) U and V calculate the shared secret key.

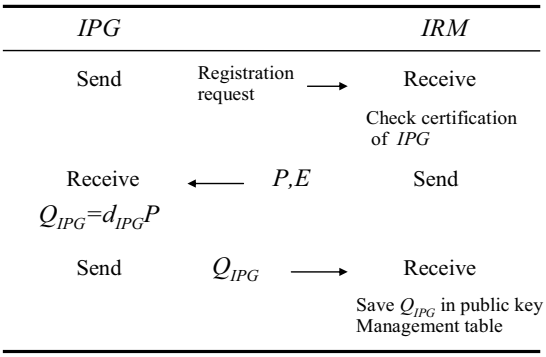

Fig. 6. Key generation and registration between IRM and IPG

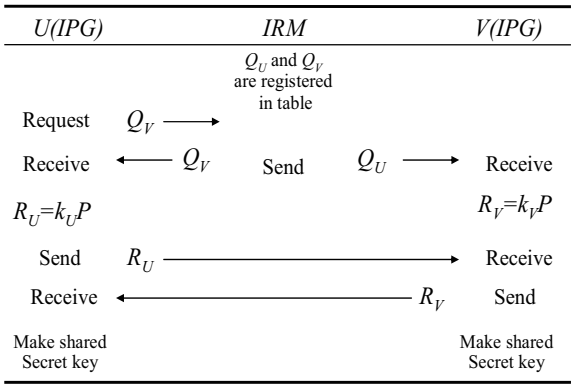

Fig. 7. Shared secret key agreement

In this mechanism, the initial IPG receives other side's permanent public key from the IRM. Only permitted IPG could register their public key to IRM; therefore all IPG which want shared secret key authenticate each other. And also, the shared secret is different every time the two sides communicate, because ephemeral public key has been introduced on each side; therefore IPGs can maintain high level security.

VI. Implementation

To prove the need for and the efficiency of the proposed mechanism, we have implemented a prototype of operation scenario, including a prototype of security provider, which we describe in this section.

As Figure 8 illustrates, the prototype consists of four devices, electricity meter which is metering voltage, converter which is converting from RS422 interface to RS232 interface, security provider which is implemented in laptop and power conservation monitoring which is using the PLC modem.

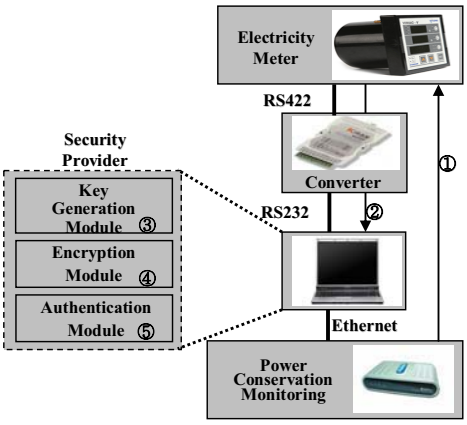

Fig. 8. Experiment environment

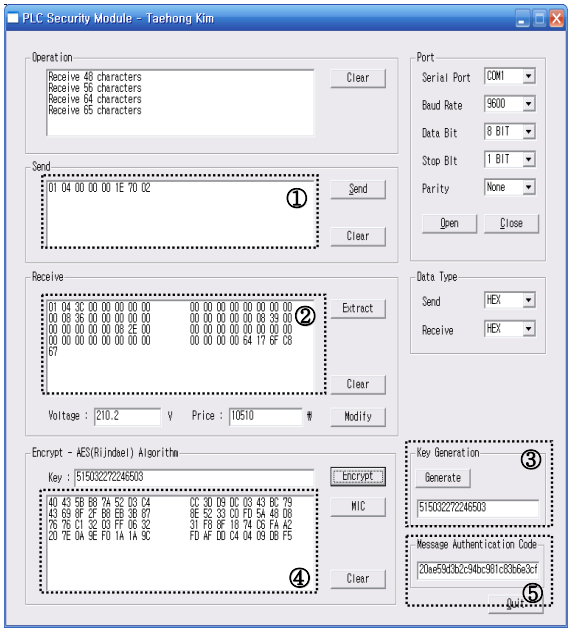

Fig. 9. Operation result of security provider

Figure 8 and Figure 9 explain the operation process of implementation environment. We used Modbus[5] as transmission protocol between meter and PCM.

① PCM requests the current voltage value to electricity meter using the Modbus protocol.

② Electricity meter sends the raw data (voltage value) to the security provider.

③ When initially connection between security provider and PCM is established, the 128bits secret key is shared between two devices by key generation module.

④ The raw data is encrypted by encryption module using the secret key from step ③.

⑤ Authentication module generates 128bits message authentication code of raw data.

VII. Conclusion and Future Works

We propose a Security Provider for metering and automation control system in PLC-based network. When a meter sends the raw data to gathering device (PCM), the security provider encrypt the data and generate message authentication code using the secret key. Also, we introduce a public key based agreement mechanism between IRM and IPGs. To prove the need for and the efficiency of the proposed mechanism, we have implemented a prototype of operation scenario, including a prototype of security provider. Our future work will focus on implementation at real UPLC system environment and considering other security factor for PLC-based network. Also, security is always a trade-off between security, cost and convenience. Therefore we should measure the performance and enhance the security function of proposed mechanism.

References

[1] Richard Newman, Sherman Gavette, Larry Yonge and Ross Anderson, "Protecting Domestic Power-line Communications," In Proceedings of Symposium On Usable of Privacy and Security (SOUPS), pp. 122-132, July 2006.

[2] Albert Treytl, Noel Roberts and Gerhard P. Hancke, "Security Architecture for Power-line Metering System," In proceedings of IEEE Factory Communication Systems 2004, pp. 393-396, September 2004.

[3] T.Tran-Anh, P. Auriol and T.Tran-Quoc, "Distribution network modeling for Power Line Communication applications," In proceedings of IEEE International Symposium on Power Line Communications and Its Applications 2005, pp. 361-365, April 2005.

[4] Man Young Rhee, "Internet Security Cryptographic principles, algorithms and protocols," WILEY, 2002.

[5] MODBUS Application Protocol Specification V1.1a, http://www.modbus.org

[6] FIPS Publication ZZZ, "Announcing the Advanced Encryption Standard (AES)," US DoC/NIST, 2001.

[7] Cheng, P. and R. Glenn, "Test Cases for HMAC-MD5 and HMAC-SHA-1," RFC2202, September 1997.

[8] FIPS Publication 46-3, "Data Encryption standard (DES)," US DoC/NIST, 1999.

[9] UPLC(Ubiquitous Power Line Communication) project part of Korea Electric Power Corporation projects, http://www.kepri.re.kr/uplc

[10] HomePlug Specification Version 1.0, http://www.homeplug.org

[11] Daemen, J. and V. Rinmen, "AES Proposal: Rijndael, AES Algorithm Submission," September 1999.

[12] Albert Treytl and Thilo Sauter, "Security Concept for a Wide-Area Low-Bandwidth Power-Line Communication System," In proceedings of IEEE International Symposium on Power Line Communications and Its Applications 2005, pp. 66-70, April 2005.

[13] Albert Treytl and Thomas Novak, "Practical Issues on Key Distribution in Power Line Networks," In proceedings of IEEE Emerging Technologies and Factory Automation 2005, vol. 2, pp.83-90, September 2005.

[14] Joon Heo and Choong Seon Hong, "Efficient and Authentication Key Agreement Mechanism in Low-Rate WPAN Environmnet," In proceedings of International Symposium on Wireless Pervasive Computing 2006, pp.1-5, January 2006.

[15] IEC 62056-61, "Data Exchange for Meter Reading, Tariff and Load Control- Part61," http://www.nssn.org

[16] ANSI X9.63-2001, "Public Key Cryptography for the Financial Services Industry - Key Agreement and Key Transport Using Elliptic Curve Cryptography," 2001.

[17] Michael Rosing, "Implementing Elliptic Curve Cryptography," MANNING, 1999.