Identity-Based Mutual Device Authentication Schemes for PLC System

[1]Joon Heo, [1]Choong Seon Hong*, [2]Moon Seok Choi, [2]Seong Ho Ju, [2]Yong Hoon Lim
[1]Department of Computer Engineering, Kyung Hee University
1 Seocheon, Giheung, Youngin, Gyeonggi, Korea, 449-701
[2]KEPRI KEPCO, Korea
[1]{heojoon, cshong}@khu.ac.kr, [2]{cms96, shju1052, adsac}@kepri.re.kr

Abstract— **Power Line Communication (PLC) is a rapidly evolving technology, aiming to use electrical power lines for the transmission of data. With the expansion scale of PLC, the security issues in PLC system have been focused on as one of the challenging problems. Until now in several well-defined technical specifications, security mechanisms which are symmetric key based system have been defined and implemented; these symmetric key based security mechanism are uncomplicated ways to use in a small scale network. This paper presents public/private key distribution and device authentication schemes that adopt IBC (Identity-based Cryptography) concept in order to use public key based security scheme in large scale PLC system. By eliminating the needs of public key certificates, proposed scheme can reduce the complexity of deploying and managing authentication credentials.**

Keywords- **Device Authentication, Key Distribution, Power Line Communication, Identity-based Cryptography**

I. INTRODUCTION

Power Line Communication 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 give 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 [1]. Power line communications are similar, from the security viewpoint, with short-range radio communications such as wireless LANs, Bluetooth and UWB. There are three main differences that make the security design exercise different and instructive. First, while short-range radio is inherently range-limited, power line networks can become unmanageable. If all the devices in a large apartment block are allowed to assemble themselves into a single network, the performance drops significantly. Therefore power line networks may have to be partitioned into logical networks for performance reason. Second, power line networking is aimed at a very wide range of consumer electronic devices, from PCs and DSL routers down to devices such fire alarm sensors and loudspeakers. Not all of these have rich user interfaces: some may have no more than a reset button. Third, the physical layer provided by the modulation scheme in some standards can provide a certain amount of assurance even in the absence of cryptography. It has basically two modes: broadcast mode and normal mode. In the broadcast mode, the bit rate is low but if two stations transmit simultaneously, this is likely to be detected. Normal mode is point-to-point and uses a much higher bit rate. In order to achieve this, tone maps (bit loading choices per carrier) must be adaptively selected for each direction of communication on each virtual link. This makes wiretapping fairly difficult [2].

Until now in several well-defined technical specifications, security methods for power line communication have been defined. In Korea standard [3], the devices in same cell use the equivalent secret key for data encryption/decryption; class A for data network, uses 56 bits DES algorithm and class B for AV network, uses 3-DES or AES algorithm. In HomePlug specification [4], they have defined five modes for secure power line system namely security mode, insecure, user-confirm, secure and lock-down; also, they have defined various secret keys such as DAK, DPW and PPK. HomePlug specification uses AES-CBC or 1024 bits RSA algorithm for data encryption/decryption. In OPERA specification [5][6], they use DES algorithm as encryption method and Diffie-Hellman algorithm as secret key agreement; also, they have defined RADIUS server based authentication system. Although these specifications are well-defined and implemented, most of these use symmetric key based system; these symmetric key based authentication and encryption are uncomplicated ways to use in a small scale network such as home, office and factory which are typically composed of around 10-20 devices.

In this paper, we propose new mutual device authentication schemes including identity based public/private key distribution. This paper is organized as follows. Section 2 explains about security issues in large scale power line system. Identity-based cryptography (IBC) will be introduced in section 3. Section 4 describes the proposed key distribution and device authentication schemes. Security considerations of proposed scheme are presented in section 5. Finally, we give some concluding remarks.

* Dr. CS Hong is corresponding author.

II. Security Issues in Large Scale Power Line System

In current fixed and mobile communication system, most of applications use public key techniques and an underlying public key Infrastructure (PKI). Public key techniques are based on the use of asymmetric key pairs. Usually each user is in possession of just one key pair. One of the keys of the pair is made publicly available, while the other key of the pair is kept private. As one of the keys is available publicly there is no need for a secure out-of-band key exchange. However there is a need for an infrastructure to distribute the public key in a secured way. The management of certificates during their lifecycle in and administrative domain requires an infrastructure – the public key infrastructure (PKI). The core component of a PKI is the certification authority (CA). This authority is trusted by the end-entities in its administrative domain and is responsible for the status of the certificates it issues. Nowadays public key techniques and their supporting PKI are used in the fixed network by a number of security protocols to support the establishment of the session keys required by the protocol to provide confidentiality and integrity, as well as the parties involved in initiating the session. Public key techniques are also used to support the provision of secure execution environments by singing downloadable code. The killer application for public key techniques was the ability to provide end-to-end security between two unknown parties, first in closed environments and later on in the Internet [7].

With the rapid expansion of the PLC system, managing the security of the devices and their communication has become more challenging, especially in provisioning and managing device authentication credentials. Until now, most of security problems have been solved using the symmetric key based schemes. However, it takes huge management cost in a large scale power line system environment in which hundreds of thousands of devices will communicate with each other. When we apply public key based security scheme, certificate revocation is also a problem: in the absence of a dependable update scheme for many devices, revocation post-manufacture may be hard. Moreover, most of power line system has not useful CA (Certificate Authority).

III. Identity Based Cryptography

This paper adopts the IBC concept to apply public key based security scheme in large scale power line system. In 1984, Shamir brought up the concept of identity-based cryptography (IBC) to address the issue of credentials management [8]. In IBC, the entity's identification, e.g. its email or IP address, can be used as its public key. By eliminating the needs of public key certificates, IBC can reduce the complexity of deploying and managing authentication credentials. Shamir's concept of IBC does not provide a complete solution to realize it, and it took nearly two decades to find a breakthrough for his open problem. In 2001, Boneh and Franklin [9] announced the first full realization of IBC. Since then, active researches have solidly advanced the theoretical foundation for identity-base cryptography. Although IBC can be used for encryption, digital signature, and other security functions, this paper focuses on its application in authentication [10].

The need to make available authentic copies of entities' public keys is a major drawback to the use of public-key cryptography. The traditional approach for doing this is to use the public key infrastructures, in which a certification authority (CA) issues a certificate which binds a user's identity with his/her public key. With ID-based cryptosystems, this binding is not necessary as the identity of the entity would be his/her public key (If not directly, the public key is derived from the identity). In ID-based PKC, everyone's public keys are predetermined by information that uniquely identifies them, such as their email address. Original motivation for ID-based encryption was to simplify certificate management in systems. Each entity in the system sends his/her identity to a trusted third party called the Key Generation Center (KGC), to obtain the private key. The private key is computed using the private key of the KGC and the identity of the user. Key escrow is inherent in ID-based systems since the KGC knows all the private keys. For various reasons, this makes implementation of the technology much easier, and delivers some added information security benefits [11]. Figure 1 explains the original concept of IBC encryption.

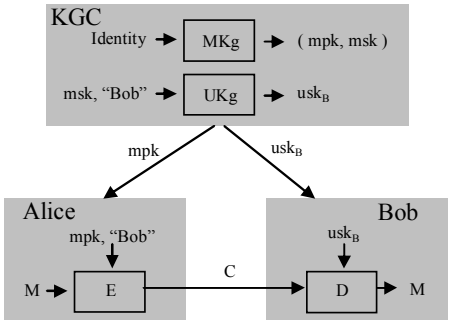

Fig. 1. Concept of IBC Encryption

IV. Proposed Authentication Schemes

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[12].

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 UPLC system is comprised of various components, namely Security Server, Integrated Regional Manager (IRM) and Master. Application servers comprise security server, metering server and automation server. 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. Master is used to interconnect IRM and devices in a cell [13].

According to the structure of the distribution network, the PLC-based network is also organized in hierarchical (as shown in Figure 2).

To apply proposed schemes in this system, we define the role of each device and assume security factors like below:

- Server (KGC) and IRM authenticated each other and have the secure channel.
- Master device has no user interface such as Password and user identification.
- Master device performs as Cell Header and can communicate with Master of other Cell. Each Cell has unique CID (Cell ID).
- Already IBC based public/private key pair has been applying at Server (KGC) and IRM.
- Server has the AML (Access MAC address List) whether new Master device legal or not.
- Inside of each cell can use existing symmetric based security scheme of well-defined specifications such as HomePlug, OPERA and Korea standard.

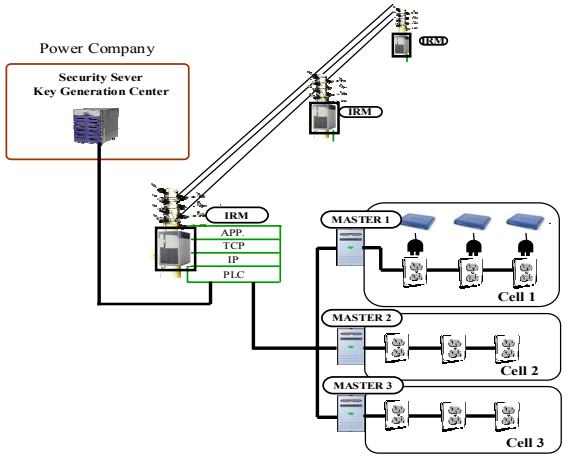

Fig. 2. Large Scale UPLC System

A. Bilinear paring

Let G_1 be an additive group generated by X with prime order f and G_2 be a multiplicative group with the same order f. Let $e : G_1 \times G_1 \rightarrow G_2$ be a pairing map satisfying the following properties:

(1) Bilinearity: $e(aX, bY) = e(X, Y)^{ab}$ for all $X, Y \in G_1$ and for all $a, b \in \mathbb{Z}$ where $\mathbb{Z}$ is integer set.

(2) Non-degeneracy: $e(X, X) \neq 1$.

(3) Computability: Given $X, Y \in G_1$, $e(X, Y)$ can be computed in polynomial time of f.

B. Parameters and Notations

We assume that f is large enough to make solving discrete logarithm problem in G_1 and G_2 infeasible. Let H_1 be a map from arbitrary bit string to the group G_1. We denote H_2 is a cryptographic hash function $H_2 : G_1 \rightarrow Z^*_f$.

The domain parameters are common variables to entities involved in schemes. We let $<f, G_1, G_2, H_1, H_2>$ be the domain parameters through the discussed schemes in this paper.

The key generation center KGC randomly chooses a secret key $k \in Z^*_f$ as a master key. We denote H_3 is a cryptographic hash function to generate temporary key. Only legal device support H_3. Notations that are used in this paper:

- A_{MAC} : MAC address of Device A
- $P(A)$: Private key of A
- $Q(A)$: Public key of A
- $TEK(AB)$: Temporary key between A and B
- N_A : Nonce value from A
- I : IRM
- M : Master
- S : Server (KGC)
- $\{W\}_K$: Encrypted W using the key K
- $[W]_K$: Signature W using the key K
- V_A : Verification value from A for authentication
- IV_A : IV value from A
- CID_A : Cell ID of Master A
- k: master key of KGC

C. Key Distribution

This section describes a key distribution when new Master device is connected to the IRM. The public/private key pair distribution is shown in Figure 3. In this scheme, we assume that already IBC based public/private key pair has been applying at Server (KGC) and IRM.

- Server (KGC): Public key = $Q(S)$, Private key = $P(S)$
- IRM: Public key = $Q(I)$, Private key = $P(I)$

(a) When new Master is connected to IRM, Master sends own MAC addresses M_{MAC} and generated random value IV_M to IRM.

(b) IRM sends own MAC addresses I_{MAC} and generated random value I_{VI} to Master.

(c) Master and IRM can generate $TEK(IM)$ with exchanged value using the cryptographic hash function H_3.

$$TEK(IM) = H_3 (M_{MAC}||I_{MAC}||IV_M||IV_I)$$

(d) IRM encrypts (M_{MAC}, CID_M) using the public key of Server $Q(S)$ and sends it to Server.

$$\{M_{MAC}, CID_M\}_{Q(S)}$$

(e) Server decrypts received $\{M_{MAC}, CID_M\}_{Q(S)}$ using the own private key $P(S)$. Then, Server checks the received M_{MAC} over AML (Access MAC address List) of the system. If exists, Server authenticates the new Master device and takes the next step.

(f) Server generates public key $Q(M)$ and private key $P(M)$ for new Master device using the received M_{MAC} and CID_M.

$$Q(M) = H_1 (M_{MAC}||CID_M)$$
$$P(M) = kQ(M)$$

(g) Server encrypts $Q(M)$, $P(M)$ using the public key of IRM $Q(I)$ and sends it to IRM.

$$\{Q(M), P(M)\}_{Q(I)}$$

(h) IRM decrypts received $\{Q(M), P(M)\}_{Q(I)}$ using the own private key *P(I)*. Then encrypts *Q(M)*, *P(M)* using the temporary key *TEK(IM)* between IRM and Master and sends it to Master.

$$\{Q(M), P(M)\}_{TEK(IM)}$$

(i) Master decrypts received $\{Q(M), P(M)\}_{TEK(IM)}$ using the *TEK(IM)* and possesses own public/private key.

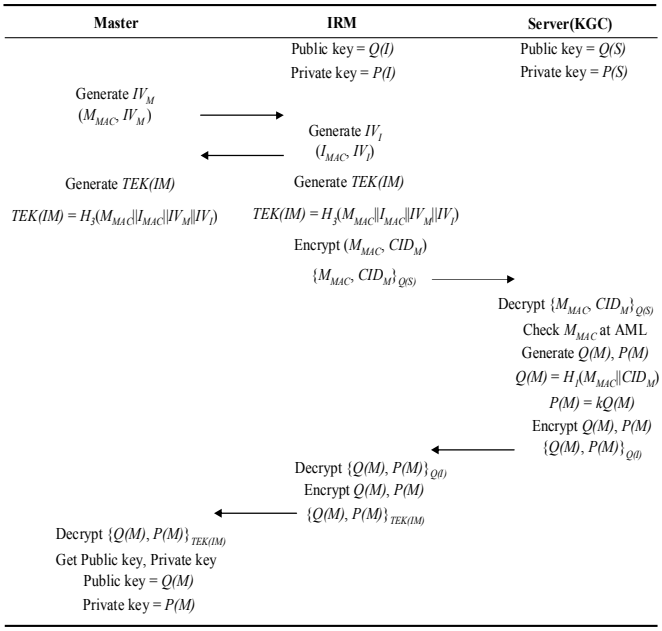

Fig. 3. Proposed Key Distribution Scheme

D. Device Authentication

The ID-based authentication scheme is described in the following Figure 4. The devices exchange challenge-response messages to verify that each peer has the valid public/private key. Diffie-Hellman algorithm [14] is used to generate the session key. After the authentication succeeds, Master 1 (M1) and Master 2 (M2) share a common session key g^{ab}.

(a) M1 generates a random nonce value N_{M1}, and sends it to M2.
(b) M2 generates random nonce value N_{M2}, and choose a random number y from the integer set (1, 2,…, p-1). M2 computes $V_{M2} = [\{N_{M1}, g^y \bmod p\}_{Q(M1)}]_{P(M2)}$ and sends (N_{M2}, V_{M2}) to M1 for identifying.
(c) M1 checks V_{M2} true or not, if true, authenticates the M2 and takes the next step, otherwise denies this communication. M1 chooses a random number x from integer set (1, 2,…, p-1).
(d) M1 computes $V_{M1} = [\{N_{M2}, g^x \bmod p\}_{Q(M2)}]_{P(M1)}$ and sends V_{M1} to M2 for identifying.
(e) M2 checks V_{M1} true or not, if true, authenticates the M1, otherwise denies this communication.
(f) M1 and M2 can generate session key g^{xy} for secure communication.

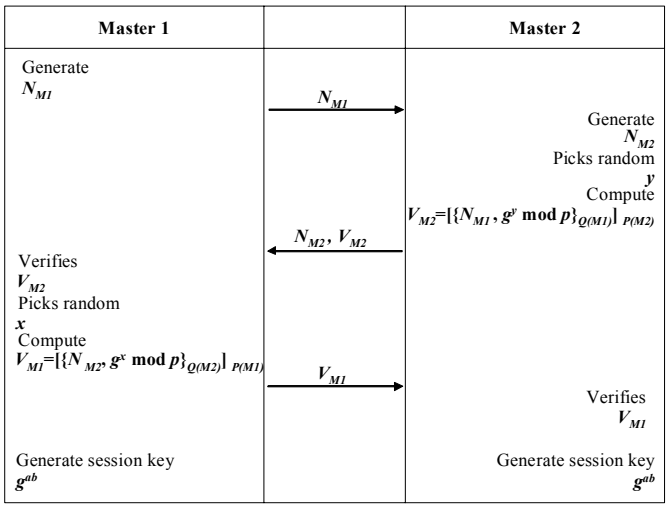

Fig. 4. Mutual Device Authentication Scheme

V. Security Consideration

Security of temporary key: The random *IV* exchange in temporary key generation is sent the clear, and so in theory a capable opponent who observes the exchange can derive the temporary key. If the attacker discover hash function H_3, this is harder than it seems. The *IV* exchange uses high bit rate communications, and it is hard for stations other than the participants to decode this, even given knowledge of the participants' tone maps. Because the analogue characteristics of power networks are generally such that the signal-to-noise ratio will in general be too poor at different locations (that is why tone maps have to be negotiated) [15].

Managing Overhead: Proposed schemes are based on public key security, therefore administrator and electric power company can reduce managing overhead. Also, proposed schemes adopts IBC concept; this makes implementation of the technology much easier.

Efficiency: Not all of devices have rich user interface; proposed schemes use MAC addresses and unique Cell ID for public/private key generation instead of user input.

Computation Overhead: Not all of devices have CPUs capable of public-key cryptography; proposed public key based scheme can be applied to out of Cell. Inside of each cell can use existing symmetric based security scheme. After authentication, authenticated Masters can use session key for mutual communication. Due to these reasons, the proposed public key based security scheme can reduce computation overhead.

Forward Security: Proposed device authentication scheme uses ephemeral Diffie-Hellman key exchange algorithm. Therefore devices of system can keep the forward security.

Mutual authentication: The Masters of the system can authenticate each other using the proposed scheme.

VI. Conclusion and Future Works

Currently some technical specifications about power line have defined security mechanism for secure communication

and implemented in devices, most of these use symmetric key based mechanism; these symmetric key based authentication and encryption are uncomplicated ways to use in a small scale network. It takes huge management cost in a large scale power line system environment in which hundreds of thousands of devices will communicate with each other. In this paper, we have proposed new mutual device authentication schemes including identity based public/private key distribution. This paper adopts the IBC concept to apply public key based security scheme in large scale power line network, because most of power line system has not useful Certificate Authority. Proposed schemes use MAC addresses and unique Cell ID for public/private key generation instead of user input. Not all of devices have CPUs capable of public-key cryptography; proposed public key based scheme can be applied to out of Cell. Our future work will focus on analysis of security and performance overhead of proposed scheme.

REFERENCES

[1] 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.

[2] 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.

[3] Korea Standard, "High Speed Power Line Communication MAC and PHY," KS X4600-1, 2006.

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

[5] Opera Alliance, "OPERA Specification: Technology," January 2006.

[6] Opera Alliance, "OPERA Specification: System," January 2006.

[7] J. Dankers, T. Garefalakis, R. Schafflhofer and T. Wright, "Public Key Infrastructure in mobile systems," ELECTRONICS & COMMUNICATION ENGINEERING JOURNAL, pp. 180-190, October 2002.

[8] A. Shamir, "Identity-based Cryptosystems and Signature Schemes," Proceedings of Crypto '84, Springer-Verlag, 1984, pp.47-53.

[9] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proceedings of Crypto '01, Springer-Verlag, 2001, pp.213-229.

[10] Khanh V. Nguyen, "Simplifying Peer-to-Peer Device Authentication Using Identity-Based Cryptography," In proceedings of IEEE ICNS 2006, pp. 43-47, July 2004.

[11] D. Nalla and K. C. Reddy, "Signcryption scheme for identity based cryptosystems," Cryptology ePrint Archive, Report2003/066, http://eprint.iacr.org/

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

[13] J. Heo, C. S. Hong, S. H. Ju, Y. H. Lim, B. S. Lee and D. H. Hyun, "A Security Mechanism for Automation Cotrol in PLC-based Network," In proceedings of IEEE ISPLC 2007, pp. 466-470, March 2007.

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

[15] Richard Newman, Larry Yonge, Sherman Gavette and Ross Anderson, "HomePlug AV Security Mechanisms," In proceedings of IEEE ISPLC 2007, pp. 366-371, March 2007.