Applying Security Algorithms against Cyber Attacks in the Distribution Automation System

I. H. Lim, *Student Member, IEEE,* S. Hong, M. S. Choi, *Member, IEEE,* S. J. Lee, *Fellow, IEEE,*
S. W. Lee, and B. N. Ha, *Member, IEEE*

***Abstract*--As the communication technology weighs heavily in the power system, so the security issues becomes major concerns. So far most security research has focused on the SCADA system. In this paper we consider the security problems in the network environment of the distribution automation system (DAS) which is much different from the SCADA system. First we analyze the types of cyber threats in many applications of the distribution system, and formulate the security goals. Then we propose the efficient security algorithms to achieve these goals. The algorithm avoids complex computation of any encryption algorithm, considering the resource-constraint network nodes. We also propose the efficient secret key distribution algorithm without resort to the public key encryption. Finally we demonstrate the feasibility of the proposed security protocol by experiment.**

***Index Terms*--distribution automation, distribution network security, cyber attack, security algorithm, key distribution, Message Authentication Code**

I. Introduction

The distribution automation system (DAS) provides capabilities for a central server to collect operation data such as voltage and current, to monitor and control feeder remote terminal units (FRTU) which are dispersed in the remote areas, and to detect and restore faults automatically [1]. As information exchange between the DAS server and field equipments becomes more critical for the system operation, communication technology plays an integral part of the distribution system.

Despite the importance of the communication technology, little effort has been invested for cyber security in the distribution system. In most cases, the approach for security relies on the physical security where equipments are located in the highly protected sites and only authorized operators can access them.

However, this approach is no longer valid as communication is becoming increasingly prevalent and especially communication architecture is more relying on the open standard communication protocols. The use of the open communication protocols renders the distribution system more vulnerable to cyber attacks in many applications.

Recently cyber threats waken major countries' concerns in the control system including the power system [2]. Most efforts in the power industry focus on the SCADA systems [2, 3].

The international standard organization also recognized the importance of network security. Since 1997, the International Electrotechnical Commission (IEC) Technical Council (TC) 57 has undertaken the development of standards that increase the informational security assurance aspects of the protocols specified within TC57 [4].

IEC TC57 WG15 will publish its work on the security standards for the communication protocols: IEC 60870-5, its derivative DNP, IEC 60970-6 (ICCP), and IEC 61850 [5-9]. Among these standards, security in the distribution system is directly related to the standards, IEC 60870-5 and DNP. Some Researches on the network security in the distribution system is motivated by the increasing threats when DNP3.0 is employed over TCP/IP network protocols because the similar attacks in the Internet might succeed in the DNP3.0 [10].

In this paper we consider possible cyber attacks in the applications based on the current distribution communication architecture, and then derive the security goals. Next we show how the security algorithms can be adapted to achieve these security goals. We intend to adapt the most efficient ways of secure message exchange, taking the resource-constrained FRTUs into account.

In the following section we explain the communication architecture we make reference to, and analyze the cyber threats and formulate the security goals. In section 3, we consider the efficient ways of adapting the current up-to-date security algorithms. In section 4, we propose the security protocols to achieve the security goals. In section 5, we show some experiments to validate the protocols.

II. Security requirements in the distribution automation network

A. DAS communication architecture

Two integral components of the distribution automation system are the DAS server and the FRTUs. A single local distribution system in Korea consists of approximately 100 to 500 FRTUs depending on the geographic size. A local

This work was supported by the ERC program of MOST/KOSEF (Next-generation Power Technology Center) and the development program of Intelligent Distribution Management System of Ministry of Commerce, Industry and Energy.

Il Hyung Lim, Sug Won Hong, Myeon-Song Choi, , Seung-Jae Lee are with the Next-generation Power Technology Center, Department of Electrical Engineering and Computer Software Engineering, Myongji University, Yongin 449-728, Korea (e-mail: sojoo2jan@mju.ac.kr, swhong@mju.ac.kr, mschoi@mju.ac.kr, sjlee@mju.ac.kr).

Sung Woo Lee, Bok Nam Ha are with the KEPRI, Daejeon Korea (e-mail : swlee@kepri.re.kr, bnha@kepri.re.kr).

978-1-4244-1904-3/08/$25.00 ©2008 IEEE

distribution system covers an area of as wide as 20km. The distribution communication network in Korea is currently constructed using various transmission media and technology [11].

Figure 1 shows the current fiber-based communication network. As shown in this figure, the DAS server and FRTUs are connected to optical ring via modems with a speed of E1 (2Mbps). A DAS server is connected to a modem through Ethernet while FRTUs are connected through serial ports. The DAS server and each FRTU exchange DNP 3.0 messages on a one-to-one basis.

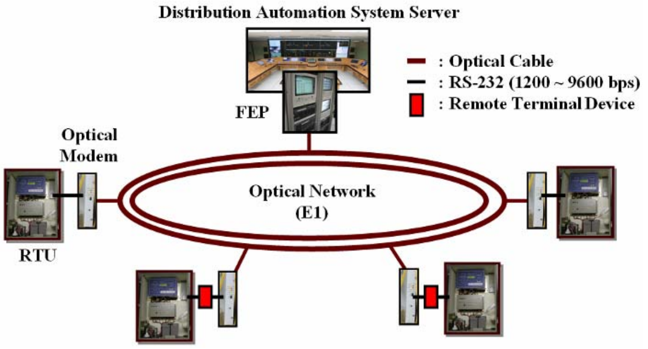

Fig 1. DAS network architecture based on optical ring in KOREA

Normally the DAS server is deployed in a protected area, while FRTUs are placed in untrusted sites as an unmanned system. The communication between the server and FRTUs are not secure since traffic is exposed to the outside of the system, and unwanted traffic can be injected and replayed.

Wireless communication is also used in some areas. This kind of communication is basically insecure. Because of its broadcast property, traffic is more vulnerable to malicious access of outsiders. For this reason, Korea Electric Power Co.(KEPCO) uses the symmetric key encryption methods such as DES for wireless communication.

In the current communication architecture each FRTU cannot exchange information directly each other. Instead the DAS server, acting as a switching hub, delivers data between the FRTUs. But, in order to improve performance and provide enhanced services in the distribution system, a decentralized communication architecture will emerge to offer capability that each FRTU can exchange information directly without any intervention of the DAS server. In this communication mode, traffic between the FRTUs will be more vulnerable to various kinds of cyber attacks.

In the following section we focus on the network vulnerability and analyze possible cyber threats based on the current communication architecture. Then we derive security goals we intend to achieve in most applications.

B. *Cyber threats in the DAS network*

One of the typical network-related attacks to the server is denial-of-service (DOS) attacks. The DOS attack renders the services of the server unusable to the FRTUs. Generally the DOS attack is possible by generating excessive load to the server and consequently exhausting its computing resources. In some cases by taking over legitimate nodes, attackers can swamp the server with unwanted messages. As passive attacks to servers, attackers use malicious codes such as virus and worms to cause malfunctions or halt their functions partially.

Servers can be recovered by rebooting or some other methods when they cannot function properly. Normally these recovery actions can be taken in a short time since servers are always taken care of by authorized operators. In this sense, the damage on servers would have little impact on the functions of FRTUs and it is unlikely to cause any severe damage such as power outage to the system. Compared to servers, attacks to FRTUs will make more dangerous effects since they are directly responsible for operations in the field, and are installed mostly unattended as an unmanned system.

The contents of messages that are exchanged between the server and FRTUs can be leaked to outsiders. Eavesdropping is an active attack of this kind. Attackers can also collect traffic and guess indirectly inside information of the system by analyzing traffic pattern.

Messages exchanged between the server and FRTUs contain operating data such as voltage and current, and control commands. Even though information about operation data or commands is exposed to outsiders, this information leakage would not lead critical damage directly to the system operation unless FRTUs are forced to function improperly.

In some application, messages can deliver highly sensitive information such as secret key which should be known to only two communication nodes. In this case we need to protect the message contents from eavesdropping.

The most dangerous attacks in the distribution system are to cause FRTUs to fail to work properly. There are three distinctive attacks to lead FRTUs to malfunctions.

The first one is to alter the contents of the messages exchanged between the server and FRTUs and then to deliver this false messages to the FTRUs. The modified or bogus messages can control automatic switches in the system maliciously, eventually causing power outages.

The second one is to create false messages and inject them in the communication channel. Attackers can disguise themselves as the servers or they can intercept the communication session. Either way, attackers can deliver illegal commands to the FRTUs.

The third one is the replay attack. All messages contain time-varying information which reflects current system status and actions required. Attackers can catch some messages and deliver the messages afterwards. This replay attacks can also make FRTUs to lead malfunctions.

C. *Requirements for the DAS network security*

First we consider security properties required by the distribution network.

1) *Message confidentiality*

As mentioned in section 2.B, message leakage is not so critical as message modification. In some applications, however, the message contents should be secured not to be read to illegitimate nodes. The typical application is the secret key distribution where secret keys should be delivered in secure ways. For this purpose the message should be encrypted with a symmetric key which only intended receivers have.

2) *Message authentication*

Receivers need to verify that messages are sent from claimed senders. Attackers can inject malicious messages to the FRTUs, consequently causing malfunctions. To authenticate the owner of messages is one of the most important security requirements in many applications in the distribution network.

3) *Message integrity*

Receivers need to make sure that the messages they receive are not altered on the way by attackers.

4) *Availability*

Services in the distribution network should be always available to all nodes. Especially servers should function properly all the time as they are originally intended. The denial-of-service attack is a typical threat to impair the availability of servers.

A single measure cannot solve all security threats. At the same time the approach which makes all components and their resources be secured is unrealistic since this approach makes security measures we have to take too costly. It is desirable to decide the priorities of what need to be secured taking into consideration the application types and their characteristics in the whole system..

In many applications, to hide the message contents by encryption is not so critical. One exception is when the server distributes secret keys to the FRTUs. Message authentication and integrity is far more important than message confidentiality in the applications we consider in the distribution network.

Servers are located in physically protected areas. Since they are always attended to by operators, when they are compromised, they can be recovered in a short time. Moreover it is highly improbable that the damage of servers leads to severe malfunctions of the whole distribution system. On the contrary the FRTUs are placed mostly in remote unmanned sites. Attacks to the FRTUs could cause malfunctions of field equipments, consequently devastating major distribution network services. In this sense to protect the functions of the FRTUs is far more important than to keep servers available.

Table 1 shows the correlation between the security threats we considered in section 2.B and the security properties, and the degree of importance considering the characteristics of the applications in the distribution network. Based on this security analysis, we formulate the following security goals, and then consider security protocols to achieve these security goals.

•Receivers should be able to verify that messages they receive are from claimed senders.

•Receivers should be able to verify that messages they receive are not compromised in transit.

•Critical contents of messages such as secret keys should be secured in transit.

TABLE 1. CORRELATION OF SECURITY tHREATS AND PROPERTIES

cyber threats	properties	importance
eavesdropping	confidentiality	●
traffic analysis		●
message modification	message integrity	●●●
false message injection		●●●
message replay		●●●
denial-of-service	availability	●●
malicious codes		●●
masquerade	authentication	●●●
unauthorized access		●●

III. SECURITY ALGORITHMS CONSIDERATION

A. *Encryption algorithms*

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]. 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.

B. *Message authentication code*

In many applications, the asymmetric key algorithm is used for message authentication. In this case, if a message is encrypted by a sender's private key, then a receiver can verify that the sender really sent this message by decrypting the message with the sender's public key.

But encrypting the whole message requires a lot of computation. To reduce the computation cost, a sender can append a short-length authentication data which is derived from the original message. This authentication data, which is

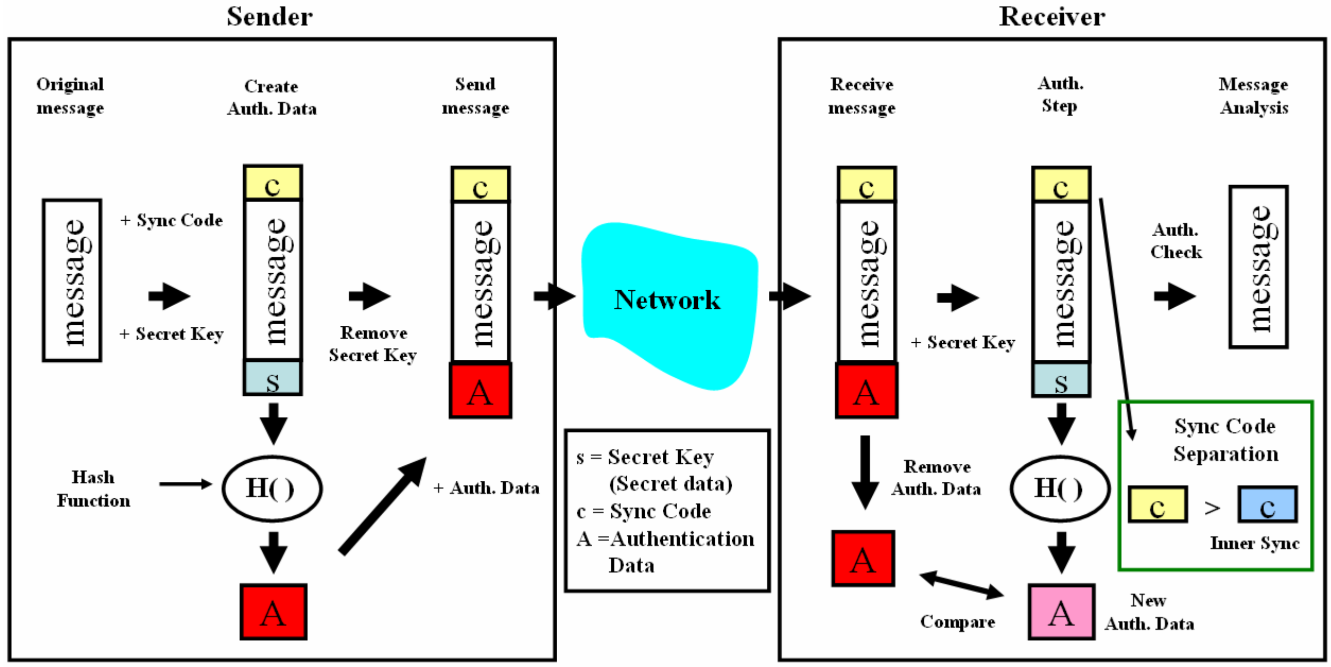

Fig 2. Message processing procedures at the sender and receiver

called the message authentication code (MAC), is obtained by applying a hash function to the original message and encrypting this short message. The encryption can be done either symmetric or asymmetric key algorithms.

However, there is a way of obtaining MAC without encryption. In this case, a sender and a receiver share a secret data which is appended to the original message when computing MAC of the message to be delivered. When the message has a correct MAC, the receiver knows that it must have been sent by the claimed sender, but also the message has not been altered in transit [15-16].

The applications we consider in the distribution network are done in the two-way communication between a server and a FRTU. Thus we can apply easily this mechanism to obtain MAC without encryption, subsequently reducing computation cost.

IV. Security protocols

A. Protocol for message authentication and integrity

In this paper we are using the message authentication code (MAC) to verify the authenticity of the sender and the integrity of the message. In many applications, MAC is computed using asymmetric encryption algorithm. As mentioned in section 3.A, however, encryption algorithms require a lot of computation overhead. For this reason it is desirable to avoid any encryption technique, ether symmetric or asymmetric when we obtain the MAC, i.e., the authentication data.

Figure 2 shows the procedure for the message authentication used in this paper. First, a sender adds a secret data (secrete key) and the Sync Code to the original message, and then computes MAC by applying a hash function to the message. The secret key is the same data which is shared with the receiver, and the Sync Code is non-decreasing number. Next, the sender replaces the secret key with the MAC, and finally delivers the message.

The receiver replaces the MAC with the secret key which was used to compute MAC by the sender, and then applies the same hash function to obtain new MAC on the message it received. If these two MAC are the same, the receiver can trust that the message was sent by the claimed sender, and also the message was not modified on the way.

The Sync Code is used to verify the freshness of the message. Since the Sync Code is non-decreasing number, the value of a new message should be bigger than the one of an old message. Comparing these two values reveals whether the message was resent or not, thus ensuring that no attackers replay old messages.

B. Message format

The message format used in this protocol is shown in figure 3. The Authentication Type field specifies the type of the message digest algorithm, i.e. the hash function used for generating the authentication data from the original message. The keyed MD5 is used for the default message digest algorithm [15]. The message is also used for distribution of the secret key as explained in the next section, when the value has 0x01.

The next unsigned 8-bit filed is the Key Identifier (Key ID) field which identifies the secret key used to create the authentication data. In implementation of supporting more than one secret key, the Key ID indicates the secret key in use for this message.

The next Sync Code field is an unsigned 32-bit long. This field contains non-decreasing number. The value used in the

Sync Code is arbitrary. One suggestion is to use a simple message counter, and the other suggestion is to use the time of the message's creation.

The next field specifies the length of the authentication data. When MD5 is used, this is 16 bytes long.

The next field is the node ID, which identifies the FRTU which sends this message. The node ID is used for the case when the FRTUs exchange messages directly each other on a peer-to-peer basis.

The authentication data (MAC) field follows the original message field. This field is 16 bytes long. If the message digest algorithm in use generates the authentication data more than 16 bytes long, the data will be truncated up to 16 bytes.

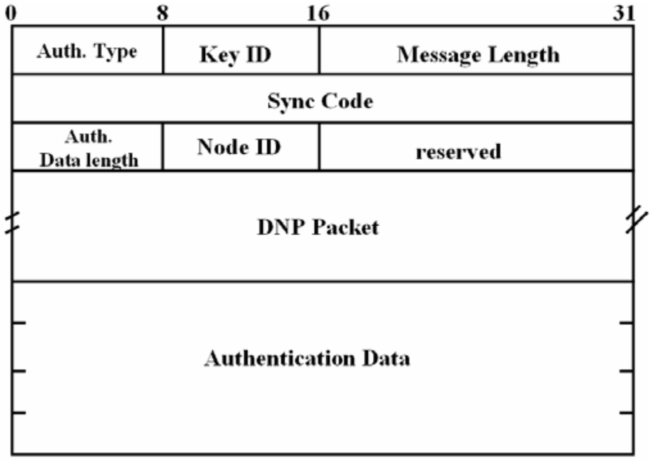

Fig 3.Message format

C. Key distribution

Generally the DAS server is deployed in the protected location. The server acts as a central hub for all communication with the FRTUs. We assume that the DAS server is a trusted base, and all FRTUs trust the DAS server at the initial setup. At the creating time each FRTU is given a master key which is shared with a server, and any following secret data (secrete keys) are distributed using this master key.

The public key algorithm is generally used as a convenient way in establishing a secure channel between two network nodes [16]. However, the public key cryptography places computationally heavy burden on the resource-constrained FRTUs. Thus in this paper we use the symmetric key algorithm using the DAS server as a trusted base node for distributing the secret key.

.A server (S) and a FRTU (A) use a secret key to set up a secure channel between them, and the secret key is refreshed after timeout. When a FRTU wants a fresh secret key, it sends a nounce and a message to the server with the message authentication code computed from the message concatenated with the nounce and the master key between the server and the FRTU. Because the MAC ensures that the server receives the legitimate request from the claimed FRTU, it can protect the server from the denial-of-service attacks.

Then the server replies a fresh secret key which is encrypted by the master key. At replying, the server also sends the message authentication code obtained from the message which is concatenated with the nounce and the encrypted secret key. The message contains the Key ID value assigned to this secret key. Because the nounce is generated by the FRTU itself and unknown to others except the server, it can verify that the secret key is not changed on the way.

The FRTU uses different nounces each time that it requests a new secret key. The use of different nounces also guarantees the freshness of the secrete key, preventing from any replay attack.

The protocol which is used to distribute the secret key is shown below. This protocol explains the case of establishing a secure channel between a server and a FRTU. But this protocol can be easily expanded to the case of the setup of a secure channel between FRTUs.

$$A \rightarrow S : N_A, M_A, MAC(N_A \mid M_A \mid MK_{SA})$$
$$S \rightarrow A : \{SK_{SA}\}_{MK_{SA}}, MAC(N_A \mid M_A \mid \{SK_{SA}\}_{MK_{SA}})$$

where

N_A	: a nonce generated by node A
M_A	: a message sent by node A
SK_{SA}	: a secrete key between S and A
MK_{SA}	: master key between S and A
$\{M\}_S$	: encrypted message by symmetric key s
$x \mid y \mid z$	: concatenation of x, y, and z

V. Case study

We demonstrate the feasibility of implementing the proposed protocols by experiment. The test configuration consists of 3 PCs each of which simulates a DAS server, a FRTU, and an attacker respectively as in figure 4. The keyed MD5 is used for the message digest algorithm, and the master key is installed manually at the creation time. The test is done in the following steps.

1) The DAS PC sends commands to FRTU PC, and ensures that the FRTU PC operates correctly without applying the security protocols.

2) The attacker PC also sends the same commands to FRTU PC and make sure that the FRTU PC also operates in the same way.

3) Using the secret key, the DAS PC sends commands to FRTU PC.

4) The attacker PC intercepts command messages from the DAS PC, and alters the contents and sends the altered messages to the FRTU PC.

5) The attacker PC uses the same keyed MD5 to generate MAC without knowing the secret key. Then attacker PC sends messages with the MAC to the FRTU PC.

6) The DAS PC sends 3 consecutive command messages to the FRTU PC. During the delivery, the attacker PC intercepts

the messages, and resends them in the same order after a certain period of time.

The results of the experiment are shown in table 3 step by step. Step 1 and 2 show that attackers can access the distribution system in the same way as any legitimate node does.

Step 3 and 4 verify that the protocols guarantee the message integrity. Step 5 shows that the protocols protect the system from any attacks against the message authentication. Step 6 proves that the system is immune to the message replay attacks.

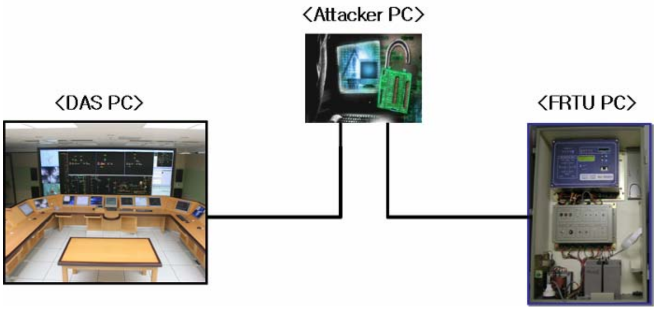

Fig 4. Experiment configuration

TABLE 3. THE RESULT OF EXPERIMENT

step	securi ty	DAS	Attacker	FRTU
1	X	send command	bypass	operation
2		–	send command	operation
3	O	send command	bypass	auth. success operation
4		send command	modify the command and resend	auth. fail no operation
5		–	apply MD5 and send the message	auth. fail no operation
6		send 3 messages	store the 3 messages	auth. success operation
		–	resend the 3 stored messages	auth. fail no operation

VI. CONCLUSION

A single measure cannot solve all security threats. The desirable approach for solving security problems is to decide the priorities of what need to be secured taking into consideration the application types in the system.

In this paper we isolate the most critical security goals in the distribution network and propose efficient ways of achieving these goals. The message authentication and integrity is far more important than any other security requirements in the distribution system applications.

For the message authentication and integrity, we avoid any encryption algorithm, either symmetric or asymmetric, and rely on the message authentication code using the secrete data which is shared with two communication nodes. We also propose the secret data distribution protocol which uses the symmetric key algorithm, avoiding the public key encryption.

Finally we demonstrate that the security protocols work by experimenting in the various cases and can be adapted to the real system. The proposed protocols impose much less computation burden on FRTU compared to when we use the encryption algorithms, especially like RSA.

VII. REFERENCES

[1] I. H. Lim, S. Hong M. S. Choi, S. J. Lee, and B. N. Ha, “ A distributed communication architecture based on the peer-to-peer model for enhancing distribution automation system services” , Tran. of KIEE, Vol. 56:3, pp. 443-450, 2007.

[2] DOE Office of Electricity Delivery and Energy Reliability, "A Summary of Control System Security Standards Activities in the Energy Sector", October 2005

[3] A. Creery and E. J. Byres, "Industrial cybersecurity for power system and SCADA networks", Industry Application Magazine, IEEE, Vol. 13:4, July-Aug. 2007.

[4] F. Cleveland, "IEC TC57 Security Standards for the Power System's Information Infrastructure - Beyond Simple Encryption", IEC TC57 WG15 Security Standards ver5, October 2005.

[5] IEC technical committee 57, “ Part 1: Communication network and system security - Introduction to security issues” , IEC 52351-1, May 2007.

[6] IEC technical committee 57, “ Part 3: Communication network and system security - Communication network and system security - Profiles including TCP/IP” , IEC 62351-3, June 2007.

[7] IEC technical committee 57, “ Part 4: Communication network and system security - Profiles including MMS” , IEC 62351-4, June 2007.

[8] IEC technical committee 57, “ Part 6: Data and communication security - Security for IEC 61850” , June 2007.

[9] IEC technical committee 57, “ Part 5: Communication network and system security - Security for IEC 60870-5 and derivatives” , IEC 62351-5, February 2008.

[10] T. Mander, F. Nabhani, L. Wang, and R. Cheung, “Data Object Based Security for DNP3 Over TCP/IP for Increased Utility Commercial Aspects Security”, Power Engineering Society General Meeting IEEE, June 2007.

[11] S. Hong, and et. al., "Evolution of communication networks for distribution automation system in Korea", Advanced Power System Automation and Protection, April 2007

[12] R. Rivest and A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", Communications of the ACM, February 1978.

[13] D. Davies and W. Price, Security for Computer Networks, New York,: Wiley, 1989.

[14] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[15] R. Rivest, "The MD5 Message-Digest Algorithms", RFC 1321, April 1992..

[16] D. Harkins and D. Carrel, "The Internet Key Exchange(IKE)", RFC 2409, November 1998.