Security Protocols Against Cyber Attacks in the Distribution Automation System

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

***Abstract*—As a communication technology plays an integral part in a power system, security issues become major concerns. This paper deals with the security problems in the distribution automation system (DAS) which has an inherent vulnerability to cyber attacks due to its high dependency on the communication and geographically widely spread terminal devices. We analyze the types of cyber threats in many applications of the distribution system and formulate security goals. Then we propose an efficient security protocol to achieve these goals. The protocol avoids complex computation of any encryption algorithm, considering resource-constraint network nodes. We also propose a secure key distribution protocol. Finally, we demonstrate the feasibility of the proposed security protocol by experiments.**

***Index Terms*—Cyber security, distribution automation system, power system security.**

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. 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 yet been invested on cyber security in the power system networks including the supervisory control and data acquisition (SCADA) system and the distribution automation system. In most SCADA systems, the approach for security relies on the physical security where equipments are located in highly protected sites and only authorized operators can access them.

Recent cyber breaches awakened the concerns about cyber security in the SCADA systems [1]. Since the incidents, security issues drew attention in various levels, and several government—level reports have been published [2], [3]. The major reason why the SCADA security is getting attention is that the SCADA system is no longer a closed network where only privileged and authorized persons can have rights to access. Recent advances in business model require the SCADA network to be connected with corporate networks. This means that the SCADA system is subject to be under the same potential cyber attacks as other corporate networks are. Moreover, the communication architecture is more relying on the open standard communication protocols. The use of the open communication protocols renders the SCADA system more vulnerable to cyber attacks.

The international standard organization recognized the importance of network security. Since 1997, the International Electro technical 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], [5]. With regard to the distribution system, IEC TC57 WG15 plans to publish its work on the security standards for the communication protocols, IEC 60870-5 and its derivative DNP [6]. And the equivalent work has been carried out in the DNP User Group, producing the secure DNP 3.0 specification [7].

In the past few years, the security issues in the SCADA system have been analyzed and some efforts have been carried out for developing security mechanisms [8]–[10]. The works have been focused on mostly key management schemes for cryptographic algorithm as well as transition issues for adapting security mechanisms and intrusion detection schemes [11]–[14].

As for the cyber attacks, the distribution system is more vulnerable in many ways. The terminal devices in the SCADA system are mostly located in restricted local area networks, while FRTUs in the distribution system are located at remote and unmanned sites in most cases, and are spread in wider area networks. As communication between the DAS server and FRTUs becomes more critical, security measures should be implemented to protect the normal control operations from any cyber threats. Recently, agent-based service-restoration algorithms in the DAS network have been proposed, and those algorithms are dependent on the security and reliability of the network [15], [16].

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 analyze the cryptographic algorithms and devise an efficient security pro-

Manuscript received November 05, 2008. First published October 30, 2009; current version published December 23, 2009. This work was supported by the 2nd Brain Korea 21 Project and the ERC program of MOST/KOSEF (Next-Generation Power Technology Center, NPTC). Paper no. TPWRD-00810–2008.

I. H. Lim, S. Hong, M. S. Choi, S. J. Lee, and T. W. Kim are with NPTC Myongji University, Yongin 449-728, Korea (e-mail: sojoo2jan@mju.ac.kr; swhong@mju.ac.kr; mschoi@mju.ac.kr; sjlee@mju.ac.kr; twkim@mju.ac.kr).

S. W. Lee and B. N. Ha are with the Korea Electric Power Research Institute, Korea (swlee@kepri.re.ke, bnha@kepri.re.kr).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TPWRD.2009.2021083

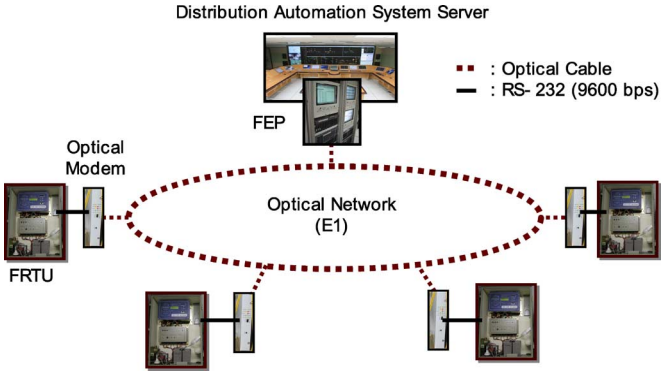

Fig. 1. DAS network architecture based on optical ring in KOREA.

tocol that can be adapted to achieve these security goals, considering the constraints imposed on the distribution system.

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 III, we consider the efficient ways of adapting the current cryptographic algorithms. In Section IV, we propose the security protocols to achieve the security goals. In Section V, we show some experiments to validate the proposed protocols.

II. Security Requirements in the Distribution Automation System

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 distribution system covers an area of as wide as 20 km. The distribution communication network in Korea is currently constructed using various transmission media and technology [17].

Fig. 1 shows the current fiber-based communication network on which the distribution system in Korea is based. As shown in this figure, the DAS server and FRTUs are connected to optical ring via modems with a speed of E1 (2 Mbps). 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.

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 a symmetric key encryption method 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

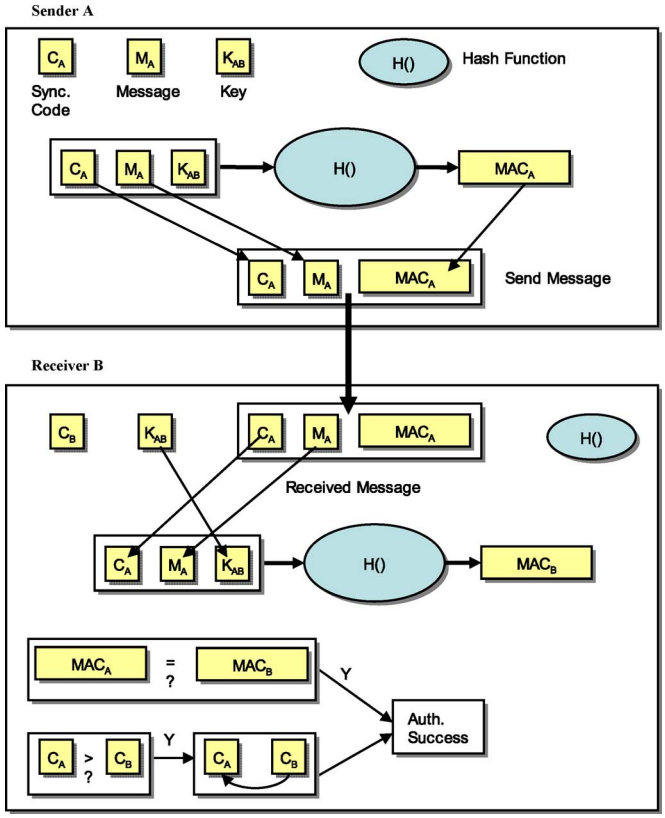

Fig. 2. Procedure for message authentication and integrity.

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 [17]. In this communication mode, traffic between the FRTUs will be more vulnerable to various kinds of cyber attacks.

B. Cyber Threats in the DAS Network

One of the typical network-related attacks to the server is the denial-of-service (DOS) attack. 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 cared 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 in remote sites.

The contents of messages that are exchanged between the server and FRTUs can be leaked to outsiders. Eavesdropping

is a typical 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 applications, messages can deliver highly sensitive information such as secret keys which should be known to only the concerned parties. 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 these false messages to the FTRUs. The modified messages can control automatic switches in the system maliciously, eventually causing power outages.

The second one is to create bogus messages and inject them in the communication channel. Attackers can disguise themselves as the server 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 system.

1) Message Confidentiality: As mentioned in Section II-B, message leakage is not so critical as message modification. In some applications, however, the message contents should be secured not to be read by illegitimate nodes. The typical application is the secret key distribution where the secret key should be delivered in secure ways. For this purpose, the message should be encrypted by a symmetric or asymmetric key which only intended parties share with.

2) Message Authentication: Receivers need to verify that messages are sent from claimed senders. Adversaries 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 system.

3) Message Integrity: Receivers need to make sure that the messages they receive are not altered on the way by adversaries.

4) Message Freshness: It is required that messages be fresh, which means that the message is recent, and old messages are not replayed by any adversary. There are two types of freshness. Weak freshness keeps ordering of the messages but not delay information, while strong freshness not only provides full ordering of the messages but also allow for delay estimation. Weak freshness is required for the application where preventing message replay attack is of main concern, but strong freshness is needed for the application such as time synchronization within network.

5) Availability: Services in the distribution network should be always available to all nodes. Servers especially 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 the security measures 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 by authorized 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 I shows the correlation between the security threats we considered in Section II-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.
- Receivers should be able to verify that messages they receive are not replayed by any attacker.
- Critical contents of messages such as secret keys should be secured in transit.

III. Considering Crytographic Algorithms

A. Notation

We use the following notation to explain the cryptographic algorithm and security protocol in this paper.

A, B, S	Communicating nodes; S denotes a server.
K_{AB}	A session authentication key between A and B.
AK_{SA}	A master authentication key between S and A.
EK_{SA}	A master encryption key between S and A.
$\{X\}_K$	Encryption of message X using key K.

TABLE I
CORRELATION OF SECURITY THREATS AND PROPERTIES

Properties	Cyber threats	Importance
Message confidentiality	eavesdropping	low(except key exchange)
	traffic analysis	Low
Message integrity	message modification	High
	false message injection	High
Message freshness	message replay	High
Availability	denial-of-service	Middle
	malicious codes	Middle
Source authentication	masquerade	High
	unauthorized access	middle

H	A hash function.
$\mathrm{M_A}$	Message sent by A.
$\langle \mathrm{M_A} \vert \mathrm{M_B} \rangle$	Concatenation of messages $\mathrm{M_A}$ and $\mathrm{M_B}$.
$\mathrm{N_A}$	A nonce generated by A.
C	A sync code used for verifying message freshness.

B. 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 between a sender and a receiver. The other is the asymmetric key algorithm which uses two keys, a public key and a private key. 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 impose the excessive overhead for computing encryption and decryption every time they exchange messages. For this reason, it is desirable to use the symmetric key algorithms when encryption is necessary as in the key distribution.

C. Methods for Message Authentication and Integrity

For message authenticity, a sender generates an authentication tag which is much shorter than the original message and appends it to each message for transmission. A receiver can verify that the message is not altered and the source is authentic by checking the authentication tag. The appended authentication tag is called the message authentication code (MAC). When A sends a message to B, A generates MAC by applying a function to the message and the secrete key between A and B; $\mathrm{MAC} = \mathrm{F}(\mathrm{M}, \mathrm{K_{AB}})$.

The one-way hash function can be used to generate MAC. A hash function, H takes a variable-size message M as input and calculate a fixed-size message digest (MD) as output; $\mathrm{MD} = \mathrm{H}(\mathrm{M})$.

The encryption algorithms can be used to generate MAC from MD. In some applications such as electronic transaction, the asymmetric key algorithm is used to generate MAC, which is known as the digital signature. In this case, if a message is encrypted by A's private key, then B can verify that the A really sent this message by decrypting the message with the A's public key.

The symmetric encryption algorithm is also applied to MD in order to generate the authentication code; $\mathrm{MAC} = \mathrm{E_K}(\mathrm{MD})$, where K is a symmetric key. Then A sends the concatenated message of M and MAC.

These approaches have an advantage in that they do not need to encrypt the whole message, consequently reducing the computation cost.

However, there is an alternative way to obtaining MAC without involving any encryption algorithm. In this case, A and B share a secret key $\mathrm{K_{AB}}$ which is appended to the original message when a hash function is applied; $\mathrm{MAC} = \mathrm{H}(\mathrm{M}|\mathrm{K_{AB}})$. A sends the concatenated message of M and MAC excluding $\mathrm{K_{AB}}$. B computes MAC by applying the same hash function to the concatenated message of M and $\mathrm{K_{AB}}$. When B calculates the same MAC as it receives, it is assured that the message must have been sent by the claimed sender A, but also the message has not been altered in transit.

HMAC is a comprehensive message authentication mechanism without encryption [18]. HMAC can be used in combination with any iterative cryptographic hash function such as MD5 and SHA-1.

The message authentication without encryption is preferable in the application we are focusing on in the DAS networks. The applications we consider in the distribution network are done in the two-way communication between a server and FRTUs based on the multi-access network, either the optical ring or wireless network. Thus, the same message is broadcasted to a number of FRTUs. It is cheaper and more reliable to have each node responsible for message authenticity, and being involved in less computation whenever it receives messages. These points are also noted in [19]. This message authentication method is widely used in the similar application such as exchange of routing information between routers [20].

IV. APPLYING SECURITY PROTOCOLS

A. Trust Requirement

The devices that implement the security protocols cannot be trusted since they are often deployed at remote unattended sites. The communication infrastructure that we are considering is not secure intrinsically.

Because the DAS server is the base node which communicates with the other nodes in the network, compromising the server will cause the whole network to be out of service. Generally the DAS server is deployed in the protected location. We assume that the server is a trusted base, and all FRTUs trust the server at the initial setup. At the creating time the server is given

two master keys. One key is the master encryption key used for encrypting the session key. The other is the master authentication key used to verify the origin of the message.

Each FRTU is also given two same master keys which are shared with the server at the creation time, and the session keys are distributed from the server whenever necessary. And we assume that each node keep the master keys without any harm.

B. Protocol for Message Authentication and Integrity

The message authentication code (MAC) is used to verify the authenticity of the sender and the integrity of the message. In order to avoid computational overhead of any encryption technique, ether symmetric or asymmetric, we choose Keyed-Hashing for Message Authentication (HMAC) as an authentication algorithm.

First, the sender A concatenates the Sync Code C, the original message $\mathrm{M_A}$, and the session key, $\mathrm{K_{AB}}$, then computes MAC by applying a one-way hash function, H, to the concatenated message. The detailed procedures are explained in [18]. Next, the sender replaces the session key by the MAC and finally delivers the message. The procedure is as follows:

$$MAC = H\left(C|M_A|K_{AB}\right)$$
$$A \rightarrow B :< C|M_A|MAC).$$

The node B applies the same hash function to obtain new MAC on the message it received with the shared session key. If these two MACs are the same, B can trust that the message was sent by the claimed sender A, and also the message was not modified on the way.

The session key can be of any length. But it is recommended that the key length should not be less than L bytes which is the byte-length of the hash function output, since it would decrease the security strength. Keys longer than L bytes are acceptable but the extra length would not provide significant increase of security [18]. In this protocol we use $\mathrm{L} = 16$ as a default secrete key length since the default keyed hash function is MD5 [21].

The Sync Code is used to verify the weak freshness of the message. Since the Sync Code is a 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.

C. Message Format

The message format and example packet whose message is "ABCD" used in this protocol is shown in Fig. 3. The Authentication Type (Auth Type) field specifies the type of the hash function used for generating the authentication data from the original message. The MD5 is used for the default hash function. The message is also used for distribution of the session key which should be shared between the sender and receiver. When the message is used for key distribution, the Auth Type value has 0×01.

The next unsigned 8-bit field is the Key Identifier (Key ID) which identifies the secret key used to create the authentication

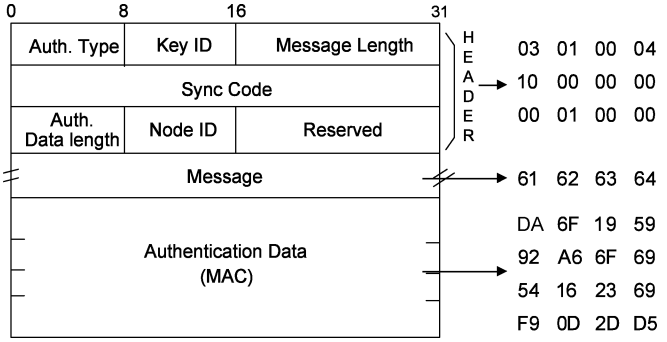

Fig. 3. Message format.

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.

The next field specifies the length of the authentication data, namely MAC. 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 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.

D. Key Distribution

The public key algorithm is generally used as a convenient way in establishing a secure channel for distributing the secrete key between two network nodes [13]. 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 node A use a session authentication key $\mathrm{K_{SA}}$ to set up a secure channel between them, and this key is refreshed on a regular base or on request. When the node A wants a new session key, it sends a nonce and its ID to the server with the message authentication code (MAC) computed from the message concatenated with the nonce, the ID, and the master authentication key between S and A. A nonce is a random bit string which is generated by A. MAC ensures that the server receives the legitimate request from the claimed node.

Then the server replies a fresh session key which is encrypted by the master encryption key. When replying, the server also sends the message authentication code which is concatenated with the nonce and the node ID and the encrypted new secret key. The message contains the Key ID value assigned to this session key. Because the nonce is generated by A and unknown to others except the server, it can verify that the session key is not changed on the way and is sent by the server on its own request.

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

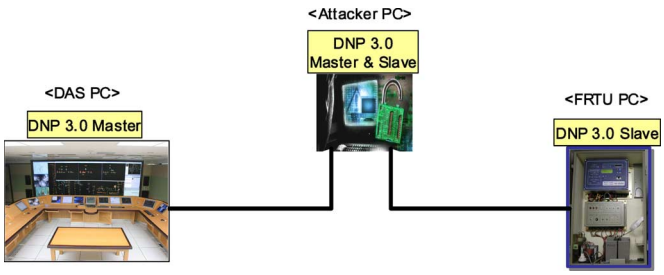

Fig. 4. Experiment configuration.

The protocol which is used to distribute the session key is shown below. The ISO/IEC 11770-2 server-less key establishment protocol can be applied for the same purpose [22]. The difference is that the proposed protocol is based on MAC for authentication and integrity, while the ISO/IEC protocol is using the encryption techniques. This protocol is designed for 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

$$\mathrm{A} \rightarrow \mathrm{S} : \langle N_A, A, H\left(N_A|A|AK_{SA}\right)\rangle$$
$$\mathrm{S} \rightarrow \mathrm{A} : \langle \{K_{SA}\}_{EK_{SA}}, H\left(N_A|A|\{K_{SA}\}_{EK_{SA}}|AK_{SA}\right)\rangle .$$

V. Case Study

A. Functionality Test

We demonstrate the functionality of the proposed protocols by experiment. The test configuration consists of three PCs each of which simulates a DAS server, a FRTU, and an attacker respectively as in Fig. 4. The keyed MD5 is used for the MAC algorithm, and the master keys are installed manually at the creation time. The following four cases have been tested.

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) The FRTU PC requests the secrete key to the DAS PC and obtains the key.
4) Using the secret key, the DAS PC sends commands to FRTU PC.
5) The attacker PC intercepts command messages from the DAS PC, and alters the contents and sends the modified message to the FRTU PC.
6) The attacker PC uses the same keyed MD5 to generate MAC without knowing the secret key. Then the attacker PC sends a message with the MAC to the FRTU PC.
7) The DAS PC sends three 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 II 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.

TABLE II
Results of Experiment

step	security	DAS	Attacker	FRTU
1	not adopted	send command	bypass	operation
2		-	send command	operation
3	adopted	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

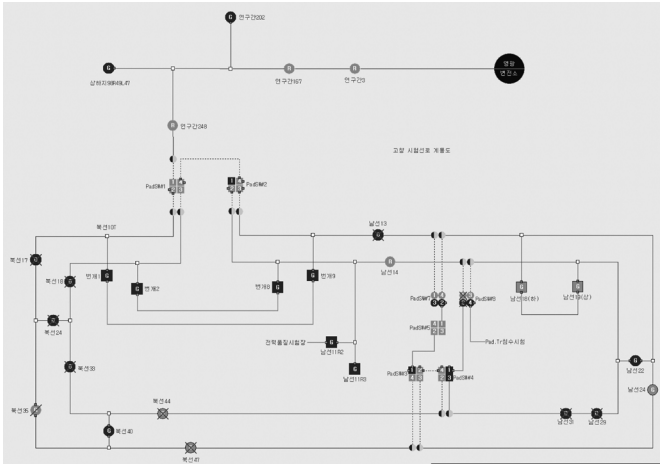

Fig. 5. Single-line diagram of distribution network testbed in Gochang.

B. Field Test

Korea Electric Power Corporation (KPECO) has a test site for DAS in Gochang City which has been used for various experiments of DAS software and equipments. Recently an agent-based service restoration mechanism developed by the Next-Generation Power Technology Center (NPTC) of Myongji University has also been tested, which depends on heavy communication among FRTUs and switch agents

The proposed security protocols have been applied to this system and the effects on the existing system performance as well as their validity have been carefully monitored and the results are reported.

The single line diagram of the Gochang testbed system is shown in Fig. 5.

Fig. 6 shows an example of switch open and close actions during the restoration process in case of a fault on the section between switch 2 and switch 3. The security protocols were applied to the communication between the switch agents as indicated by solid and dotted arrows. This experiment is focused on

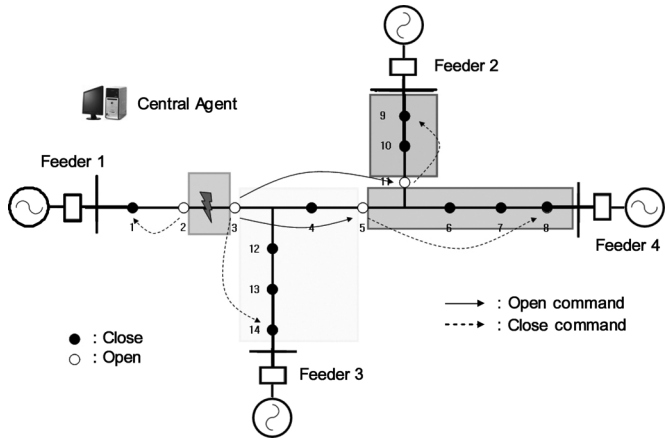

Fig. 6. Multiagent-based service restoration.

the effects of the security protocols on the performance of the overall system operation and turned out to not cause any noticeable operation speed reduction. Compared to the total time of service restoration which is about 40 s, the time delay caused by the added security overhead is considered negligible. Furthermore those cyber attacks in Table II of the previous test case in Section V-A have also been tested and no unsuccessful operation or any faulty operation due to the attacks has been monitored, showing the highly secure and reliable performance.

In the near future, the proposed security protocols are expected to be applied the Intelligent Distribution Management System (IDMS) of KEPCO in Korea.

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 of application types in the system.

In this paper, we identified the most critical security goals in the distribution automation system and proposed 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.

We propose a simple but efficient secret key distribution protocol which uses the symmetric key algorithm. Effectiveness of the proposed security protocols has been shown by various tests not only on the lab-scale test system but also on the KEPCO testbed system. The proposed protocols impose a negligible computation burden on FRTU, resulting in less time overhead on the DAS operation than the one when the encryption algorithms are used.

With more careful field tests, the proposed security protocols are expected to be applied to the KEPCO DAS system in the future.

References

[1] J. Slay and M. Miller, *Lessons Learned From the Maroochy Water Breach*. Boston, MA: IFIP Springer, 2007, vol. 253, pp. 73–82.
[2] IT Security Advisory Group, SCADA Security: Advice for CEOs Dept. Commun. Inform. Technol. and the Arts. Canberra, Australia, 2005.
[3] President's Information Technology Advisory Committee, Cyber Security: A Crisis of Prioritization Report to the President, Nat. Coord. Office Inform. Technol. Res. and Develop.. Arlington, VA, 2005.
[4] F. Cleveland, IEC TC57 Security Standards for the Power System's Information Infrastructure—Beyond Simple Encryption IEC TC57 WG15 Security Standards ver5, Oct. 2005.
[5] IEC Technical Committee 57, Data and Communications Security, Part 1: Communication Network and System Security-Introduction to Security Issues IEC TS 62351-1, May 2007.
[6] IEC technical committee 57, Data and Communications Security, Part 5: Security for IEC 60870-5 and derivatives IEC 62351-5 Second Committee Draft, Dec. 2005.
[7] DNP User Group [Online]. Available: http://www.dnp.org
[8] V. M. Igure, S. A. Laugher, and R. D. Williams, "Security issues in SCADA networks," *Comput. & Secur.*, vol. 25, pp. 498–506, 2006.
[9] M. Hentea, "Improving security for SCADA control systems," *Interdisc. J. Inform., Knowl., and Manag.*, vol. 3, 2008.
[10] S. C. Patel and Y. Yu, "Analysis of SCADA Security models," *Int. Manag. Rev.*, vol. 3, no. 2, 2007.
[11] S. Hong and S.-J. Lee, "Challenges and pespectives in security measures for the SCADA system," in *Proc. 5th Myongji-Tsinghua University Joint Seminar on Prototection & Automation*, 2008.
[12] L. Pietre-Cambacedes and P. Sitbon, "Cryptographic key management for SCADA systems—Issues and perspectives," in *Proc. Int. Conf. Information Security and Assurance*, 2008.
[13] C. Beaver, D. Gallup, W. Neuman, and M. Torgerson, Key Management for SCADA SANDIA, Tech. Rep. SAND2001-3252, 2002.
[14] R. Dawson, C. Boyd, E. Dawson, and J. M. G. Nieto, "SKMA-A key management architecture for SCADA systems," in *Proc. Australasian Workshops on Grid Computing and E-Research*, 2006.
[15] I. H. Lim, Y. I. Kim, H. T. Lim, M. S. Choi, S. Hong, S. J. Lee, S. I. Lim, S. W. Lee, and B. N. Ha, "Distributed restoration system applying multi-agent in distribution automation system," in *Proc. IEEE PES General Meeting*, 2008.
[16] F. Yu, T.-W. Kim, I.-H. Lim, M.-S. Choi, S.-J. Lee, S.-I. Lim, S.-W. Lee, and B.-N. Ha, "An intelligent fault detection and service restoration scheme for ungrounded distribution systems," *J. Elect. Eng. & Technol.*, vol. 3, no. 3, 2008.
[17] S. Hong, I. H. Lim, M. S. Choi, S. J. Lee, C. H. Shin, S. W. Lee, and B. N. Ha, "Evolution of communication networks for distribution automation system in Korea," in *Proc. Advanced Power System Automation and Protection*, Apr. 2007.
[18] H. Krawcryk, M. Bellare, and R. Canetti, HMAC: Keyed-hashing for message authentication RFC 2104, IETF, Feb. 1997.
[19] D. Davies and W. Price, *Security for Computer Networks*. New York: Wiley, 1989.
[20] F. Baker and R. Atkinson, RIP-2 MD5 Authentication RFC 2082, IETF, Jan. 1997.
[21] R. Rivest, The MD5 Message-Digest Algorithms RFC 1321, IETF, Apr. 1992.
[22] *Information Technology—Security Techniques—Key Management—Part 2: Mechanisms Using Symmetric Techniques*, ISO/IEC 11770-2, 1996.

Il Hyung Lim (S'05) was born in Seoul, Korea, in 1979. He received the B.E. and M.S. degrees in electrical engineering in 2007 from Myongji University, Yongin, Korea, where he is currently pursuing the Ph.D. degree.

His research interests are power system control and protective relaying, including artificial intelligence application.

Sugwon Hong (M'09) was born in Incheon, Korea, on January 7, 1957. He received the B.S. degree in physics from Seoul National University, Seoul, Korea, in 1979, and the M.S. and Ph.D. degrees in computer science from North Carolina State University, Raleigh, in 1988 and 1992, respectively.

He has previously worked with Korea Institute of Science and Technology (KIST), Korea Energy Economics Institute (KEEI), SK Energy Ltd., and the Electronic and Telecommunication Research Institute (ETRI). He has been a Professor in the Department of Computer Software, Myongji University, Yongin, Korea, since 1995. His major research fields are network protocol and architecture and network security.

Myeon-Song Choi (M'96) was born in Chungju, Korea, in 1967. He received the B.E., M.S., and Ph.D. degrees in electrical engineering from Seoul National University, Seoul, Korea, in 1989, 1991, and 1996, respectively.

He was a Visiting Scholar at the University of Pennsylvania State in 1995. Currently, he is an Associate Professor at Myongji University, Yongin, Korea. His major research fields are power system control and protection, including artificial intelligence applications.

Seung-Jae Lee (M'88) was born in Seoul, Korea, in 1955. He received the B.E. and M.S. degrees in electrical engineering from Seoul National University, Seoul, Korea, in 1979 and 1981, respectively, and the Ph.D. degree in electrical engineering from the University of Washington, Seattle, in 1988.

Currently, he is a Professor with Myongji University, Yongin, Korea, and a Director at Next-Generation Power Technology Center (NPTC). His major research fields are protective relaying, distribution automation, and AI applications to power systems.

Tae-Wan Kim (M'09) received the B.S., M.S., and Ph.D. degrees in computer science and engineering from Konkuk University, Seoul, Korea in 1994, 1996, and 2008, respectively.

He was with the Electro-Mechanical Research Institute in Hyundai Heavy Industries for seven years. Currently, he is a Research Professor at Myongji University, Yongin, Korea. His major research fields are industrial communication, real-time systems, and compilers.

Sung-Woo Lee received the Ph.D. degree in electrical engineering from Kunkook University, Seoul, Korea, in 1999.

He joined the Korea Electric Power Research Institute (KEPRI) Representative Research Center of Korea Electric Power Corporation (KEPCO) in 1992. As a Researcher in the Power Generation Laboratory, he contributed to developing distributed control systems for power plant for more than 14 years, with a specialty in nuclear instrumentation. He joined the Distribution Laboratory of the KEPRI in 2006, where he performs research projects related to distribution automation and distribution IT systems.

Bok-Nam Ha was born in Daejeon, Korea, in 1958. He received M.S.E.E and Ph.D. degrees from the Chungnam National University, Korea.

He has been with the Korea Electric Power Research Institute (KEPRI) of Korea Electric Power Corporation (KEPCO) since 1978. Since 1990, he has been a Deputy Researcher and the Leader of Distribution IT Group, which works to develop intelligent distribution automation systems. His research interests are the application programs of distribution automation and its field applications.