Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Security Protocols Against Cyber Attacks Using SMS Alert

P.Natarajan[1]
[1] P.G Scholar
Department of Computer Science & Engineering, Bharath University, Chennai, India.

D.Udhaya Kumara Pandiyan[2]
[2] Asst.Professor
Department of Computer Science & Engineering, Bharath University, Chennai, India.

Abstract— Cybercrime refers to any crime that involves a computer and a network, where the computers may or may not have played an instrumental part in the commission of a crime. Cybercrime refers, more precisely, to criminal exploitation of the Internet. Issues surrounding this type of crime has become high-profile. On the global level, both governments and non-state actors continue to grow in importance, with the ability to engage in such activities as espionage, financial theft, and other cross-border crimes sometimes referred to as cyber warfare. The international legal system is attempting to hold actors accountable for their actions, with the International Criminal Court among the few addressing this threat. When the system identifies some typed words as Threat words, it automatically sends a SMS to the admin or to the Police along with the IP address of that particular system and the entire sentence of up to 160 characters.

Keywords—

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 re- mote terminal units (FRTU) which are dispersed in the remote areas, and to detect and restore faults automatically. As infor- mation 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, se-curity issues drew attention in various levels, and several gov- ernment—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 priv- ileged and authorized persons can have rights to access. Re- cent 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 commu- nication architecture is more relying on the open standard com- munication protocols. The use of the open communication pro- tocols renders the SCADA system more vulnerable to cyber at- tacks.

The international standard organization recognized the im- portance 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 se- curity 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 car- ried 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 appli- cations based on the current distribution communication archi- tecture, and then derive the security goals. Next, we analyze the cryptographic algorithms and devise an efficient security pro- tocol that can be adapted to achieve these security goals, con- sidering the constraints imposed on the distribution system.

In the following section, we explain the communication ar- chitecture we make reference to, and analyze the cyber

threats and formulate the security goals. In Section III, we consider the

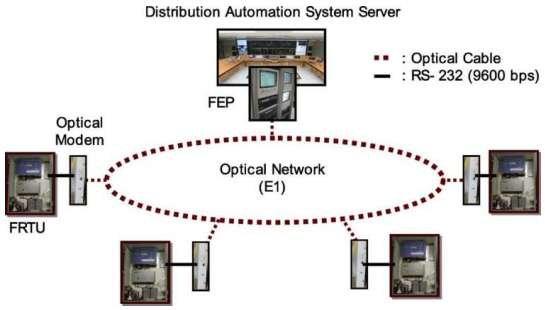


Fig. 1. DAS network architecture based on optical ring in KOREA.

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 val- idate 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 dis- tribution 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 broad- cast 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 commu- nication.

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

B.Cyber Treat in DAS Network :

One of the typical network-related attacks to the server is the denial-of-service (DOS) attack. The DOS attack renders the ser- vices 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 malfunc- tions or halt their functions partially.

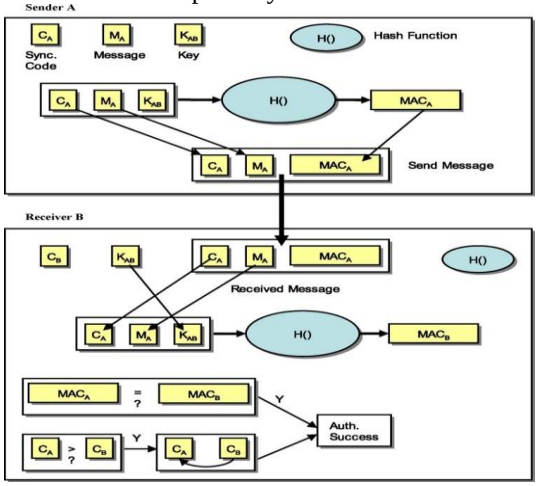


Fig. 2. Procedure for message authentication and integrity.

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 ana- lyzing traffic pattern. Messages exchanged between the server and FRTUs contain operating data such as voltage and current, and control com- mands. Even though information about operation data or com- mands 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 mes- sage 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 ex-changed 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 them- selves 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 de- liver the messages afterwards. This replay attacks can also make FRTUs to lead malfunctions.

B. Requirements for the DAS Network Security

First we consider security properties required by the distribu- tion 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 se- cured not to be read by illegitimate nodes. The typical applica- tion 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 in- tended 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 mal- functions. 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 fresh- ness. 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 func- tion properly all the time as they are originally intended. The de- nial-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 prior- ities 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 en- cryption is not so critical. One exception is when the server dis- tributes 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 com- promised, 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 ap- plications 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 re- ceive are from claimed senders.
- Receivers should be able to verify that messages they re- ceive are not compromised in transit.
- Receivers should be able to verify that messages they re- ceive 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.

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

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

B. Encryption Algorithms

Message encryption can hide message contents from out- siders. 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 dis- tribution.

C. Methods for Message Authentication and Integrity

For message authenticity, a sender generates an authentica- tion tag which is much shorter than the original message and ap- pends 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;

$F(M, K_{AB})$

IV.MDSS BASED ON DYNAMIC CHOICE OF ALTERNATIVES

Although DSSs have typically been associated with desktop systems and involve considerable processing, the development of new compact and mobile technologies provides new oppor- tunities to develop this kind of DSSs over M-Internet [12], [16], [17]. In this section, we describe the implemented GDM model that incorporates a tool for managing dynamic decision models in which the alternatives of the set of solution alternatives can change throughout the decision process and uses different formats to represent preferences. It allows us to develop GDM processes at any time and anywhere and to simulate with more accuracy level the real processes of human decision making, which are developed in dynamic environments such as the web, financial investment, and health. Finally, the prototype of the MDSS is presented.

A. Structure of the Implemented GDM Model

The structure of the proposed MDSS model is composed of the following five processes: 1) uniformization; 2) selection;

3) consensus; 4) dynamic choice process of alternatives; and 5)feedback .

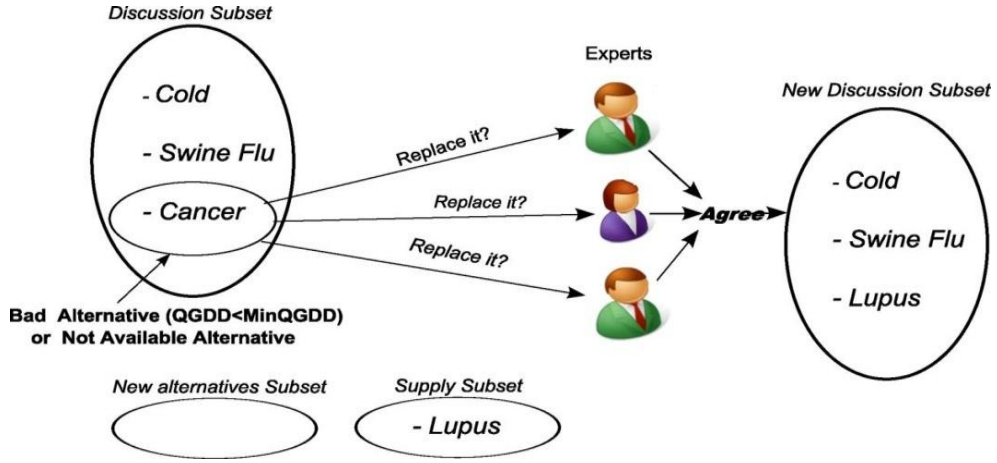
In such cases, due to different factors, the set of solution alternatives can vary throughout the decision process. One typical example of this situation is the medical diagnosis. This environment is dynamic in the sense that a patient can present new symptoms, or he can set better due to the medication, and thus, any change in state of the patient should be taken into account by the doctors.

Classical GDM models are defined within static frameworks. To make the decision-making process more realistic, we pro- vide a new tool to deal with dynamic alternatives in decision making. This way, we can solve dynamic decision problems in which, at every stage of the process, the discussion can be centered at different alternatives.

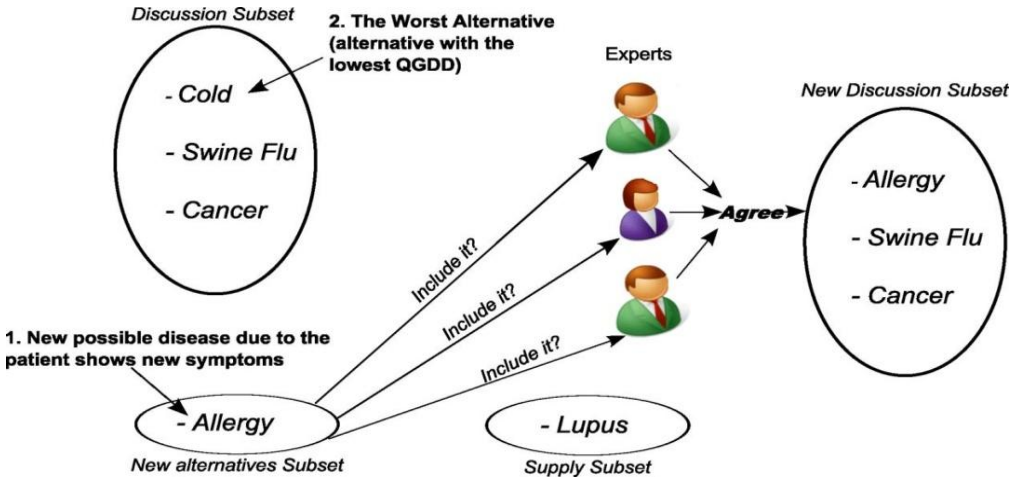
To do so, we define a method that allows us to remove and insert new alternatives into the discussion process. First, the system identifies the worst alternatives that might be removed and the new alternatives to include in the set. These new alternatives can be obtained from a set of new alternatives that appeared at a time or from the supply set of alternatives that includes all the alternatives that we had at the beginning of the process but were not included in the discussion sub- set because of limitations due to specific parameters of the problem.

Thus, the method has two different phases.

1) *Remove old bad alternatives*. The first phase manages situations in which alternatives of the discussion subset are not available at the moment due to dynamic external factors or because the experts have evaluated them poorly and they have a low dominance degree (*QGDD*). There- fore, the system checks the availability and the *QGDD* of each alternative in the current discussion subset. If an alternative is not available or has a *QGDD* lower than a threshold (*minQGDD*), the system looks for a new good alternative in the new alternatives subset. If this subset is empty, the system uses the supply subset of alternatives provided by the expert at the beginning of the decision process and that were not taken into account then because of the impossibility of comparing all the alternatives at the same time. Then, the system asks for the experts' opinions about the replacement and acts according to them (see Fig. 3).



Dynamic choice process of alternatives: Case 1.



2) *Insert new good alternatives.* The second case manages the opposite situation, i.e., when new alternatives have emerged. The system checks if new good alternatives have appeared in the new alternatives subset due to dy- namic external factors. If this is the case, the system has to identify the worst alternatives of the current discussion subset. To do this, the system again uses the dominance degree *QGDD* of all alternatives to choose the worst alternatives. Then, the system asks for the experts' opin- ions about the replacement and acts according to them.

V. APPLYING SECURITY PROTOCOLS

A. Trust Requirement

$$MAC = H\,(C|\mathrm{M_B}\rangle K_{AB})$$

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 communi- cates with the other nodes in the network, compromising the server will cause the whole network to be out of service. Gen- erally 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 Comparing these two values reveals whether the message was resent or not, thus ensuring that no attackers replay old messages.

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 authenti- cation 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 mes- sage. 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:

C. Message Format

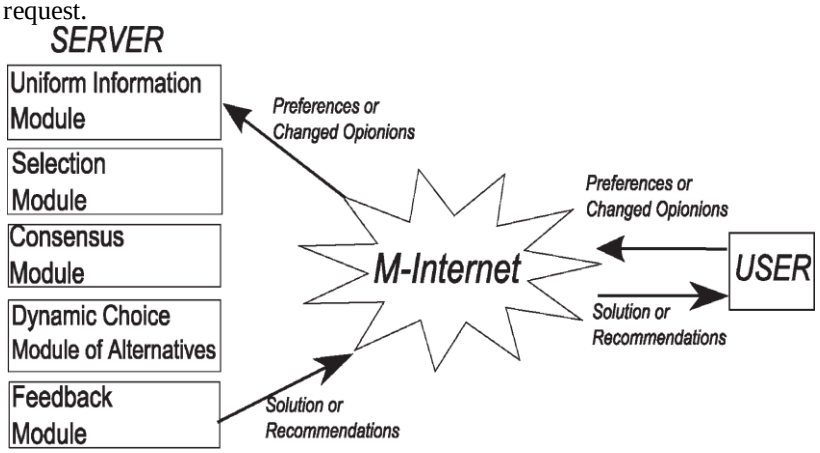
The message format and example packet whose message is "ABCD" used in this protocol is shown in Fig. 3. The Authen- tication Type (Auth Type) field specifies the type of the hash function used for generating the authentication data from the original message. The MD5 is used for the default hash func- tion. 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.

D. Key Distribution

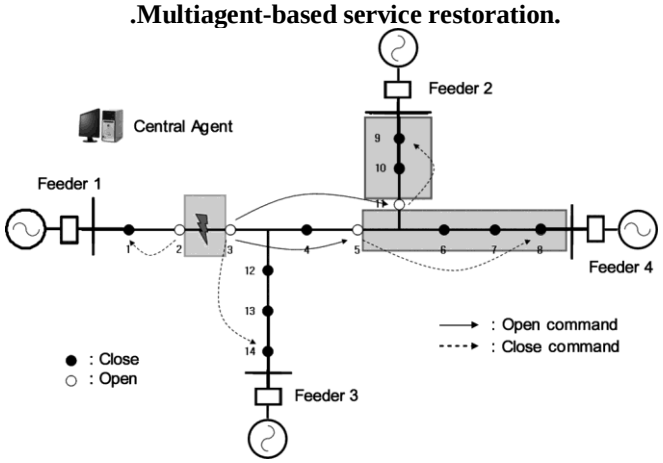
The public key algorithm is generally used as a convenient way in establishing a secure channel for distributing the secrete $\times$ key between two network nodes [13]. However, the public key cryptography places computationally heavy burden on the re- source-constrained FRTUs. Thus in this paper we use the sym- metric 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.



.Multiagent-based service restoration.



VI. Conclusion

The revolutionary changes email is bringing about in the workplace have been likened to those brought about by the introduction of the typewriter. Email has enabled the easy, reliable, rapid and inexpensive transmission of information to large numbers of people at the same time, and offers access to people and at times precluded by face-to-face communication. More information does not, however, mean better information and information overload is becoming a major email-related issue.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 intoconsiderationof application types in the system.In this paper, we identified the most critical security goals inthe distribution automation system and proposed efficient waysof achieving these goals. The message authentication and integrityis far more important than any other security requirementsin the distribution system applications.We propose a simple but efficient secret key distributionprotocol which uses the symmetric key algorithm. Effectivenessof the proposed security protocols has been shown byvarious tests not only on the lab-scale test system but also onthe KEPCO testbed system. The proposed protocols imposea negligible computation burden on FRTU, resulting in lesstime overhead on the DAS operation than the one when theencryption algorithms are used.With more careful field tests, the proposed security protocolsare 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 Se- curity: 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 Se- curity 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 Com- mittee 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," *Inter-disc. 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 mea- sures for the SCADA system," in *Proc. 5th Myongji-Tsinghua Univer- sity 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. In- formation Security and Assurance*, 2008.

[13] F. Burstein and C. Holsapple, *Handbook on Decision Support Systems*.New York: Springer-Verlag, 2008.

[14] S. French and M. Turoff, "Decision support systems," *Commun. ACM*, vol. 50, no. 3, pp. 39–40, Mar. 2007.

[15] J. Muntermann, "Mobile Notification and Decision Support for Private Investors," in *Event-Driven mobile Financial Information Services*. Wiesbaden, Germany: Deutscher Universitäts-Verlag, 2008.

[16] J. Schiller, *Mobile Communications*, 2nd ed. Reading, MA: Addison- Wesley, 2003.

