Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2014, Article ID 280978, 10 pages
http://dx.doi.org/10.1155/2014/280978

Research Article

Authentication Method for Privacy Protection in Smart Grid Environment

Do-Eun Cho,[1] Sang-Soo Yeo,[2] and Si-Jung Kim[3]

[1] *Innovation Center for Engineering Education, Mokwon University, Daejeon 302-729, Republic of Korea*
[2] *Division of Convergence Computer & Media, Mokwon University, Daejeon 302-729, Republic of Korea*
[3] *College of General Education, Hannam University, Daejeon 306-791, Republic of Korea*

Correspondence should be addressed to Si-Jung Kim; sjkim6183@gmail.com

Received 15 December 2013; Accepted 8 March 2014; Published 8 July 2014

Academic Editor: Jongsung Kim

Recently, the interest in green energy is increasing as a means to resolve problems including the exhaustion of the energy source and, effective management of energy through the convergence of various fields. Therefore, the projects of smart grid which is called intelligent electrical grid for the accomplishment of low carbon green growth are being carried out in a rush. However, as the IT is centered upon the electrical grid, the shortage of IT also appears in smart grid and the complexity of convergence is aggravating the problem. Also, various personal information and payment information within the smart grid are gradually becoming big data and target for external invasion and attack; thus, there is increase in concerns for this matter. The purpose of this study is to analyze the security vulnerabilities and security requirement within smart grid and the authentication and access control method for privacy protection within home network. Therefore, we propose a secure access authentication and remote control method for user's home device within home network environment, and we present their security analysis. The proposed access authentication method blocks the unauthorized external access and enables secure remote access to home network and its devices with a secure message authentication protocol.

1. Introduction

The smart grid with which studies are being actively conducted based on recent convergence technology is also called intelligent electrical grid and great attention is paid to it as the technology for the accomplishment of low carbon green growth. Smart grid is a power infrastructure system of the next generation linked to smart demand management and new renewable energy by applying IT to the existing electrical grid and exchanging real-time information both ways between supplier and consumer. Combining IT technologies to the existing electrical grid systems can enable power supplier and consumer to obtain useful information from each other on real-times basis, and this can maximize the energy efficiency of the whole electrical grid systems. Particularly, two-way information exchange infrastructure between power suppliers and consumers called AMI (advanced metering infrastructure) can be considered as the core of smart grid [1–3].

As of now, the government is planning to supply AMI to over 50% of total consumers nationwide until 2016. The supply of AMI has already been completed for the high voltage consumer of KEPCO (Korea Electric Power Corporation). For the diversity in rate plan, more selection for consumer, and the creation of new service to result from the application of AMI, the replacement from mechanic watt-hour meter to smart meter is essential. With the replacement, the base for optimization in energy use can be arranged through real-time confirmation on one's own electricity use and rate and the control by automated remote device [4].

When the interworking between the AMI system currently under study with power supplier as its sponsor and the home network is completed, there are advantages that additional installation cost can be reduced. Also telecommunication infrastructure of broadband internet which is already supplied to millions of households can be used in smart grid environment. Home network refers to the connection of information appliances within home via network and

control of information appliance regardless of the location of user with connection via external internet network.

However, home network possesses security vulnerability that the legacy mediums and protocols possess since various wired and wireless mediums and protocols coexist within it. Also, there is a problem that previously used network based cyber-attack technology via internet can be applied to the home network.

Therefore, in secure smart grid environment, there is a necessity for reliable security framework and technologies for the combination of various devices with new concept and wired and wireless telecommunication terminal. Particularly, in smart grid environment, the detailed personal information would be collected, stored, processed, and sometimes illegally disclosed, so the needs of privacy protection framework consisting of securing devices, detecting unauthorized invasion of privacy, adopting efficient home device access control mechanism, and others are greatly increasing [5–8].

AMI of smart grid should protect various services against external attackers through various security solutions including secure access control mechanism same as other contemporary communication networks. Particularly, study on privacy information protection during the accesses to, from, and in home network is an important research aspect for building secure smart grid environment [9–14].

Therefore, the purpose of this study is to propose authentication method for privacy information protection of home device in smart grid environment.

Initial version of this study was presented and discussed in MUSIC 2012 and this study is expanded and is more concrete version. The composition of this study is as follows. The telecommunication network of smart grid, security vulnerability, and security requirement will be examined in Section 2 and authentication method for secure privacy protection in home device will be proposed in Section 3. Security of the proposed method will be analyzed in Section 4 and conclusions will be made in Section 5.

2. Related Work

2.1. Smart Grid. Smart grid includes various infrastructures including the various monitoring and control facilities installed to not only electricity generation, electricity transmission, and electricity supply facilities but also smart devices such as smart meter, software, and hardware.

Main technology of smart grid includes IT technology, smart device including smart meter, distributed system technology for energy management, reliability of energy quality based technology, energy production, storage, and transmission technology, entire system monitoring technology, and core system that is security technology that guarantees the stability of system.

Also, there is main telecommunication infrastructure called AMI with two-way telecommunication as its base for more reliable smart grid. Telecommunication infrastructure of AMI can be composed by suing wired telecommunication technology such as Ethernet and PLC (power line communication) and wireless telecommunication technology such as ZigBee, Wi-Fi, and 3GPP.

It is composed as hierarchical structure in which several smart meters in AMI telecommunication environment access a DCU (data aggregate unit) that plays the role of gateway and several DCU also access AMI server of the power supplier through WAN.

Since AMI is a point of contact for internal and external telecommunication networks of power consumer, it can be the target of firmware, worm, virus, and malicious code circulation, meter bot, DDoS (distributed denial of service) attack, and others [15, 16].

AMI telecommunication network for interworking between power system and control systems that composes smart grid is as Figure 1.

2.2. Security Threats and Vulnerabilities of Smart Grid. Smart grid environment is vulnerable to cyber-attack different from the existing electrical grid. First of all, as smart grid environment requires two-way data transmission, adequate power supply and system operation are automatically performed through collection of various data. Therefore, in case wrong information or forged and falsified data is provided in some node, the reliability of smart grid cannot be secured and it could lead to cyber threat. Also, smart devices such as smart meter, home gateway, sensors, and others that can become a point of contact for information exchange at the terminal of consumer can be utilized as the route of cyber-attack. Moreover, information appliances of home network are relatively low in computing capacity; thus it is difficult to install powerful security function and there is high possibility that it could be used or targeted for cyber-attack [17, 18].

Although various home networking technologies can be used, home network does not possess correspondence technology to resolve the security vulnerability of medium on its own. Also, in case of middleware, there is lack of security infrastructure that can satisfy all security functions required by each middleware and flexibly provide security function in integrated middleware environment in which all middlewares are combined together. Therefore, it has security vulnerability toward cyber-attack such as hacking, malicious code, worm, virus, DDoS attack, and wiretapping of telecommunication network. In order to correspond to such cyber-attack, the security of home gateway is necessary by priority as it is the door that connects the public network outside the house and home network within the house and the security for wired and wireless network technology which is access route of home network environment is also necessary [19–22].

When looking into AMI based security threat elements in smart grid environment, it can be divided into the access to each device and user based information security in user environment. The elements of security threat in AMI are described in Figure 2, and also explained in detail as follows.

(i) Firmware Manipulation. It is a threat element entailing the disclosure of device's password and consequent disclosure of all information through firmware manipulation in unprotected devices such as smart meter.

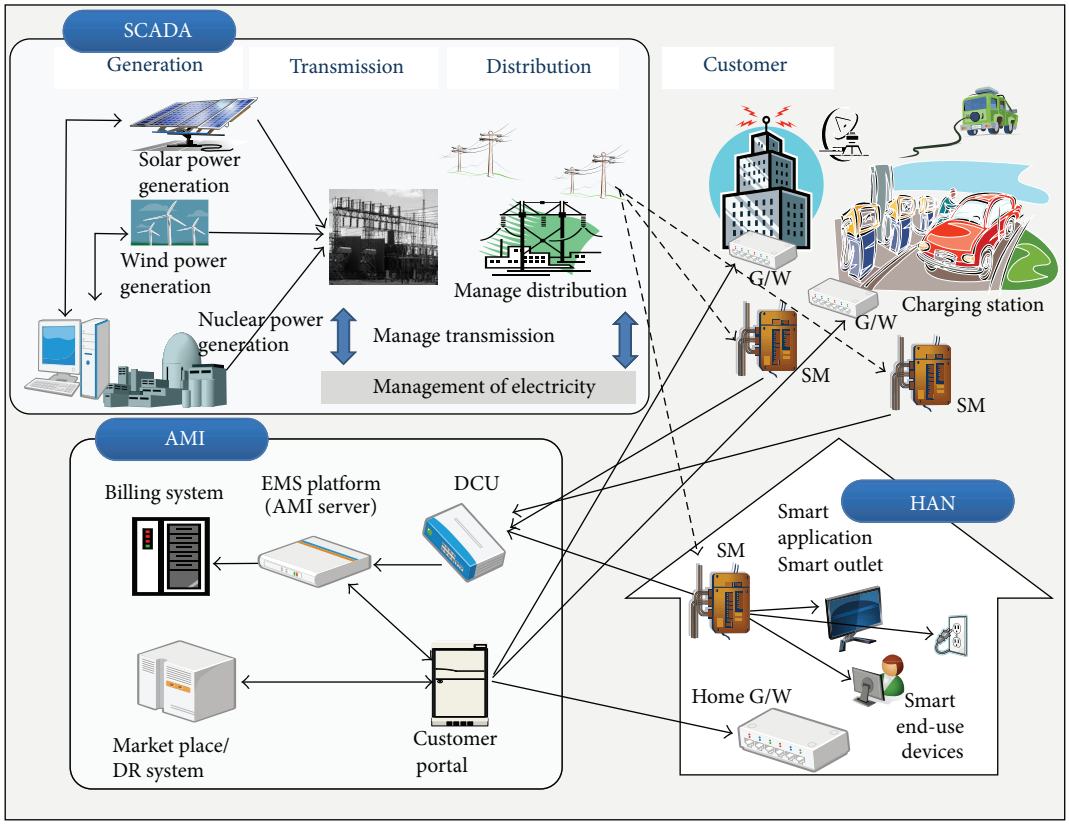

Figure 1: Communication structure of smart grid.

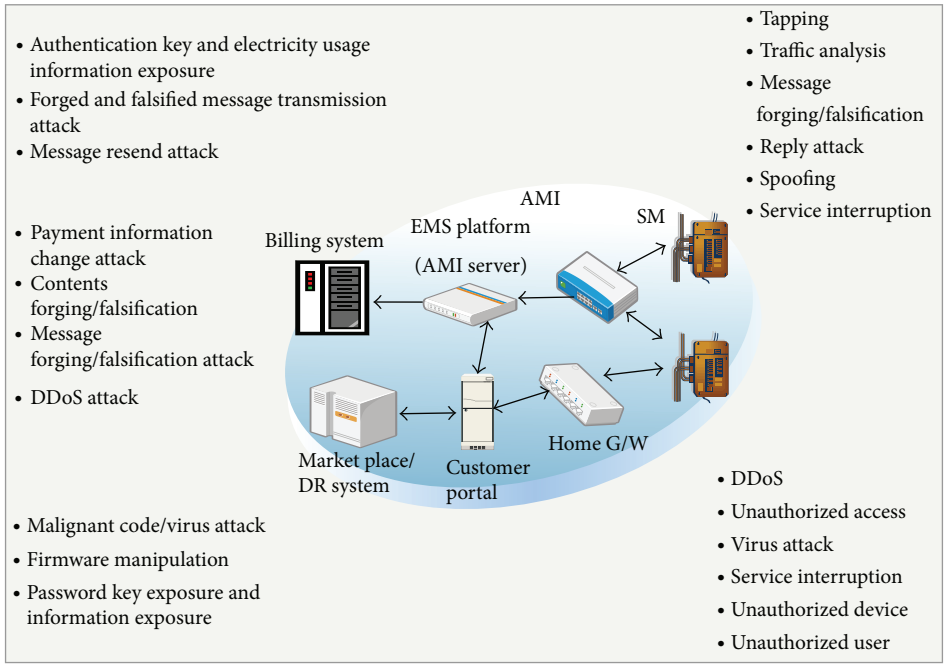

Figure 2: Security threats in AMI network.

(ii) DDoS Attack. It is a threat element entailing the service denial attack using the traffic increase and distributed denial of service attack targeting the smart meter during the provision of various services by taking advantage of the fact that field device of embedded device based AMI provides service via CPU.

(iii) Malicious Code and Virus Attack. It is a threat element entailing the attack by implementation of malicious code and virus code to smart devices including smart meter which takes advantage of the vulnerability of device within AMI in which it is difficult to install vaccine against virus due to the limitation in capacity.

(iv) User Information Change and Disclosure Attack. It is payment information change attack through forging and falsification of payment information, electricity bill, user information, and others of each user in user environment and it is a threat element to not only electrical grid but also e-commerce.

(v) Authentication Key and User Information. It is a threat element entailing the disclosure of authentication key created during the communication between each device within AMI and encrypted communication and the disclosure of electricity usage information of user followed by the abovementioned disclosure.

(vi) Message Resend. It is a threat element entailing the forging and falsification of messages as information transmitted and received within AMI including electricity usage information, power demand information, network status information, electricity bill information, and user information uses continuous two-way telecommunication.

2.3. Security Requirements of Smart Grid. The security requirements of smart grid basically include the goals of general network security, confidentiality, integrity, and availability. Moreover, in order to mitigate to security threats that can be expected in smart grid environment, several security requirements should be considered additionally.

(i) Confidentiality. The confidentiality for the data transmitted through network and data stored to system and device needs to be secured. In case of data collected from local and remote smart device in smart grid environment, important information including privacy information such as the amount of use and rate related information is transmitted through network; thus, the protection of important information is required by using mechanism such as encryption so that unauthorized user cannot have an access.

(ii) Data Integrity. It should be guaranteed that unauthorized user did not change the data during the process such as the creation, transmission, and storage of data. In regard to the smart grid environment, an attack which forges and falsifies the message transmitted between the server and smart device is possible using man-in-the-middle attack. Therefore, in order to correspond to such security threat, a solution that can secure the integrity of data transmitted between mediums is necessary.

(iii) Device Integrity. Devices such as smart meter in smart grid environment are generally placed in the location where they are not monitored, but they are devices that process important data for the service provision. Such devices are mostly implemented at platform with open interface for the reasons such as cost reduction and convenience in implementation. When the device integrity is not secured, network can be contaminated or availability of device can be damaged by inserting malicious software to device or changing the role of device. Therefore, verification on the integrity of device is additionally required.

(iv) Availability. Availability should be secured for all networks and services. DDoS attack which is an attack method against the availability is a method that harms the availability and productivity of system and it reduces service provision ability to system resource and information. Therefore, adequate security mechanism for smart grid environment that can secure the availability is required so that information access capacity of subject or devices would not be harmed.

(v) Access Control. In case of accessing to another system and device, it should grant minimum authority to authorized member only. In case administrator or users attempt to access device installed to remote place in smart grid environment, access control and authentication mechanism to fight inadequate access, application, and user's action that surpass the approved authority are necessary.

(vi) Nonrepudiation. Nonrepudiation service should be provided in case payment and DR related information is being exchanged. A mechanism that prevents the fact repudiation in smart grid environment by verifying the fact after the message transmission and reception or completion of telecommunication or process is necessary.

(vii) Key Management. Encryption key used for the information protection needs to go through key creation, key distribution, key storage, and key revocation accordingly with secure and adequate procedures; thus, secure and verified key management should be provided.

The security policy on various privacy or sensitive information created from AMI and HAN (home-area network) should be conducted by applying such security requirement for smart grid. The privacy information created in smart grid is as Table 1.

3. Proposed Access Authentication Method for Home Device

In this study, authentication method and access control method for privacy protection are proposed so that remote user can securely access HAN and perform the work in home network based smart grid environment.

The privacy subgroup within CSWG (cyber security working group) of NIST divides the privacy largely into 4 categories that are privacy of personal information, privacy of person, privacy of personal behavioral, and privacy of personal communications [1]. Among them, privacy of personal information refers to the rights to control and access

Table 1: Personal information of smart grid.

Type	Description
Name	A proper name registered to the account
Address	A location information of service area
Account number	Unique identification number related to account
Meter IP	Internet protocol address used by meter
HAN	Electronic devices currently in use from house connected to network
Current rate	Rate information imposed to the account
Billing history	All data and rate information of metering devices
Service provider	Information of supplier that supplies user account
Distributed resource	Existence of power generation or storage device, operation status, and usage pattern

the personal information which enables the identification of certain individual and others. Privacy of person is a right to control the integrity of user's body and it includes the matters that are physically necessary. Privacy of personal behavior includes the right to maintain the fact of certain individual behavior as confidential to others. Then, privacy of personal communications refers to the right for communication without censorship such as unjust monitoring. For the privacy within smart grid, all of the above 4 aspects should be considered. In order to achieve this, authentication method that can control the service access of remote user and encryption process for important data is necessary. This study provides the privacy within smart grid through secure access service through authentication process performed for user who accesses the system.

3.1. System Structure of AMI. AMI within smart grid plays an important role in connecting smart device and electrical grid and it receives and transmits the important information such as electricity consumption and user consumption pattern information generated within home network. Figure 3 illustrates the whole structure of home network based AMI that is composed of home server, authentication server, and MDMS (meter data management system). Home server can effectively exchange energy management information with MDMS through web service. MDMS provides meter data management, electricity monitoring service, and others. Meter data is integrated to home server and it is transmitted to web service based MDMS.

Home server which is added of service module for electricity management to the existing home gateway provides multimedia service, data and network device sharing service, and home appliances control services within household. Data of home server is applied to DB access control module; thus access is controlled according to the access level of user. This provides not only system and service access control for each user but also access control differentiated based on service access environment of user. Figure 3 illustrates the overall structure of the proposed home network authentication system.

3.2. Remote User Access Authentication Module. User can monitor and control the standby power of devices in home network by using remote control function through home network based AMI while one is out of home. The proposed user authentication method enables authorized remote user to securely control the device.

In the proposed user authentication method, it is assumed that the device always exists in the range where telecommunication with authentication server is available, the device, home server, and authentication server are secure from physical attack such as side channel attack, and home server and authentication server exchange messages through secure channel. The notation of key used in communication is as shown in Notation section.

3.2.1. Preliminary Phase. The authentication server creates the ID of device and shared secret key (K_i) and securely stores them in the memory of device during the device registration process. Also, the authentication server saves the device's ID and its shared secret key to its own database. Then, a remote user who wants access to the device registers his own ID and password to authentication server in advance. At the moment, the password of user is used in key creation for the encryption of ticket (master key) for device access.

3.2.2. Mutual Authentication and Key Exchange Phase. Remote user A transmits his ID, ID of device to access, and time stamp to the authentication server and demands the creation of token necessary to receive approval for device access. Remote user A who received token transmits it to device for the mutual authentication with device and creation of session key. Detailed process is as follows.

① Remote user A sends his ID ($\mathrm{ID_A}$), ID ($\mathrm{ID_B}$) of device B to access, and time stamp ($\mathrm{TS_1}$) to the authentication server in order to receive token necessary for access to device B.

② The authentication server checks ID and password of remote user A and creates secret key K_A from time stamp ($\mathrm{TS_1}$) and password of A with the use of hash function. The authentication server uses one-time secret key through one-way hash function:

$$K_A = h(\mathrm{TS_1} \oplus \mathrm{password}). \quad (1)$$

③ The authentication server creates a session key ($K_{A,B}$) for remote user A and device B and then creates token as the following with the use of secret key (K_B) shared with device:

$$\mathrm{Token} = E(K_B, \mathrm{ID_A} \parallel R_S \parallel K_{A,B} \parallel \mathrm{Lifetime} \parallel \mathrm{TS_2}). \quad (2)$$

The information in token includes Lifetime which informs of the expiration date of token, time stamp $\mathrm{TS_2}$, and random value R_S created from the server;

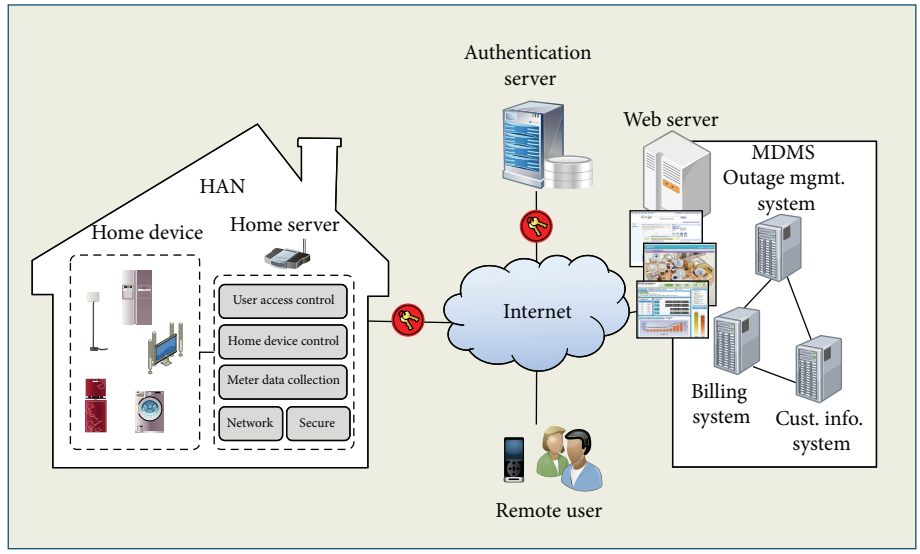

Figure 3: Structure of the proposed authentication system.

thus it can prevent nonrepudiation attack. Also, it includes the session key $K_{A,B}$ and the identifier of remote user, ID_A.

④ In order to securely transmit token to remote user, the authentication server sends encrypted token, session key, and random value R_S with the use of secret key induced from TS_1 and password of remote user A. At the moment, token is encrypted with the secret key of user; thus person other than user A cannot grasp the contents even when the packet is acquired.

⑤ Remote user creates secret key (K_A) using his password and time stamp and acquires token, session key, and random value by decrypting the message received from the authentication server.

⑥ Remote user creates time stamp TS_3 and creates message authentication code for integrity test of message to be transmitted to device B:

$$\mathrm{MAC}\left(K_{A,B}, \mathrm{Token} \parallel \mathrm{TS}_3\right). \tag{3}$$

⑦ Remote user A transmits ID of device B, token, TS_3, and MAC to the home server.

⑧ Home server identifies the device to access through ID of message received from the remote user and transmits the message to the device.

⑨ Device B which received the message decrypts the token through secret key (K_B) shared with the authentication server and acquires the session key ($K_{A,B}$).

⑩ Device B verifies MAC through acquired session key and approves the remote user.

⑪ Device B calculates the random value (R_{S+1}) with the use of session key acquired for mutual authentication.

⑫ Device B sends ID_A of remote user and $E(K_{A,B}, R_{S+1})$ to the home server.

⑬ Home server transmits the message ID_A and $E(K_{A,B}, R_{S+1})$ received from the device to the remote user.

⑭ Remote user A authenticates the device by decrypting the received message with the use of session key ($K_{A,B}$), creates secure channel with the use of shared session key, and performs the secret communication.

3.2.3. Shared Secret Key Update Phase. The secret key K_S shared between the authentication server and registered device which is used for the encryption and decryption of ticket for remote user needs to be updated regularly. In order to update secret key K_B shared with device B, the authentication server transmits newly created shared secret key K_B' created as follows by encrypting with previous shared secret key:

$$\begin{aligned}&\text{Share Secret Key Update Information}\\ &= E\left(K_B, \mathrm{ID}_S \parallel \mathrm{ID}_B \parallel K_B' \parallel \mathrm{TS}_1\right).\end{aligned} \tag{4}$$

Remote user demands token necessary to receive access approval of home device to the authentication server. The authentication server checks the information of remote user and transmits token to remote user. The remote user who received the token transmits it to the home device for the mutual authentication with device and creation of session key. Mutual authentication between remote user and home device and process of session key creation are as Figure 4.

3.3. Authentication Module for Home Device Access Control. When the user authentication process is accomplished, access to each device is accomplished through home server as Figure 5. When remote user accesses the home device, home server verifies the access authority of user for the home device and goes through the authentication process for service and data access. Through authentication process for each user,

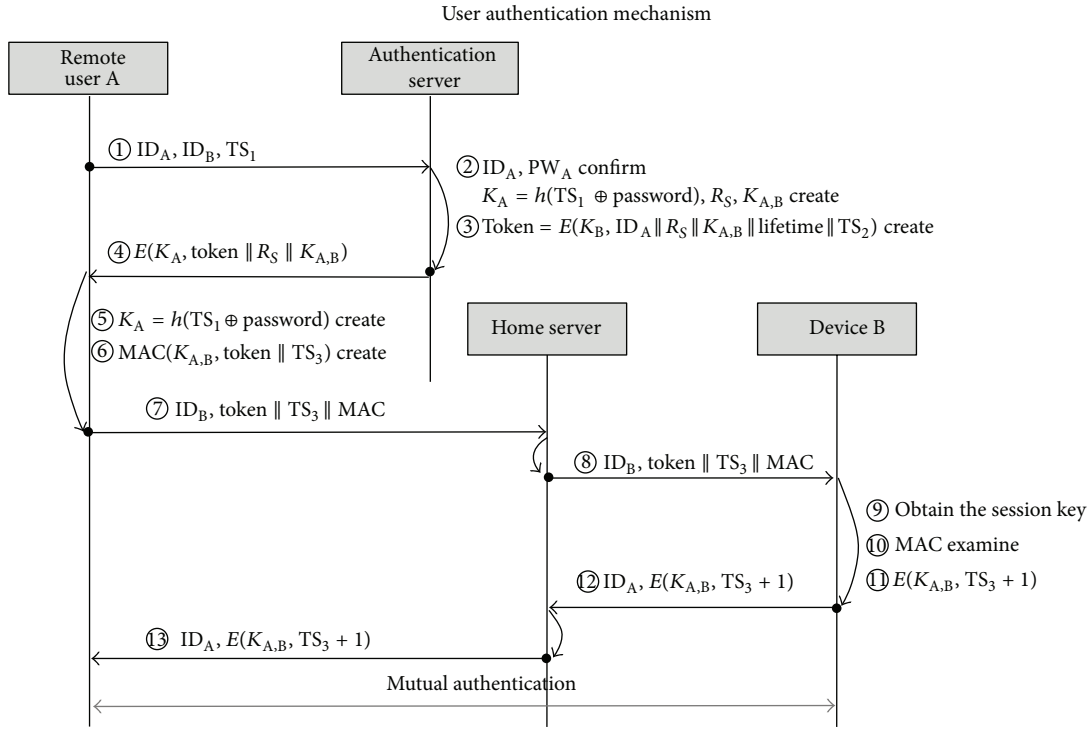

Figure 4: Access control module flow chart mutual authentication between user and home device and session key creation process.

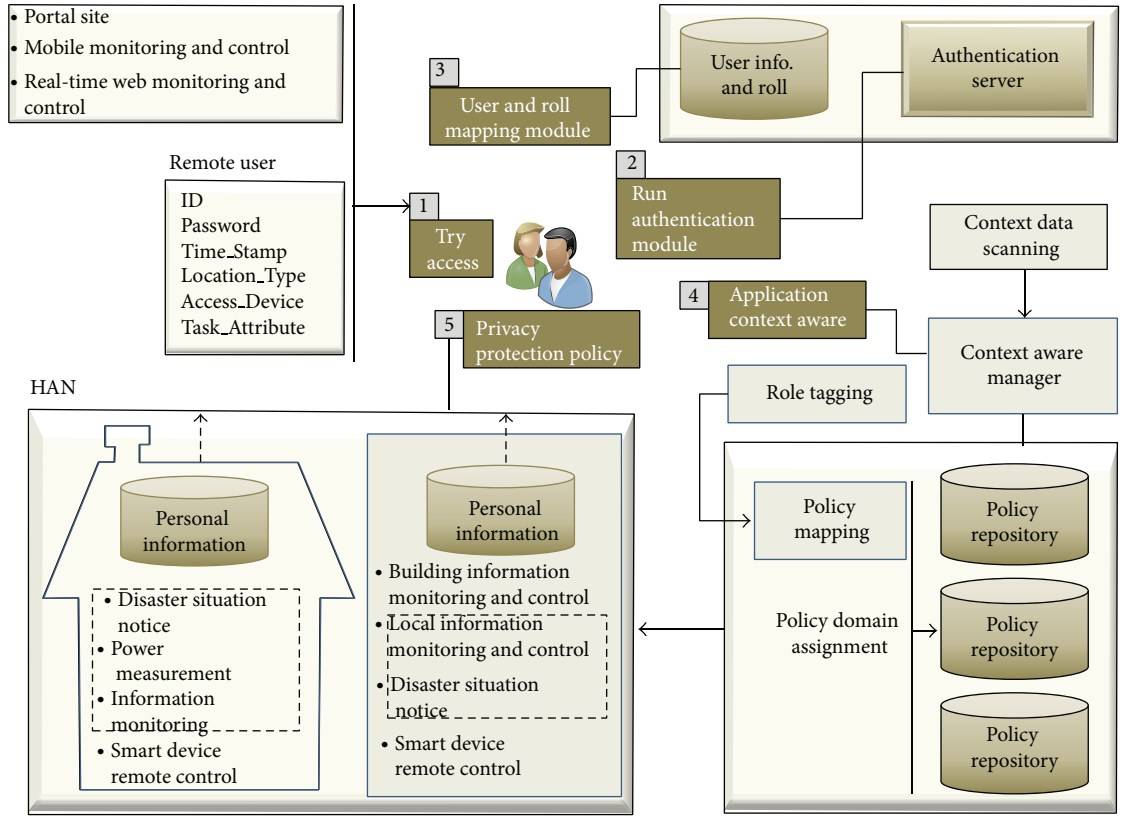

Figure 5: Access control module flow chart.

access to home device is controlled. Access to personal information created within home is controlled through access control of home device. The proposed access control module differentiated the access authority between users inside and outside the home and between administrator and general user. Therefore, it was made so that only administrator level can exercise certain authority such as registration of home device, smart meter, and user device. This becomes easy access control method when user generally attempts to gain access from outside with the use of mobile device. Personal information created within smart grid is regularly encrypted and stored to home network DB for the management and access to it is authorized through the management of access control module in the authentication server. In order to achieve this, a different range of data access is applied to each user according to the service type and access level of each user when the service is requested.

4. Security Analyses

The security from not only data misuse and abuse, immoral use, malicious internal user, technical problem related to sharing, data loss or spill, and account or service hijacking but also unknown threat profile is required for various privacy information created in smart grid environment.

For the privacy protection of user in smart grid, managerial and technical countermeasure such as internal management plan for privacy information, forging/falsification prevention of access control and authorized access record, and encryption process for personal information of user and electricity consumption information needs to be set.

In HAN telecommunication field, there is security vulnerability for information spill by the wiretapping of telecommunication data between AMI and home appliances. Technical countermeasure such as the encryption of HAN telecommunication data and entity authentication needs to be set and it is necessary to apply the encryption algorithm and key management mechanism supported in telecommunication protocol. The authentication method proposed in Section 3 controls the access to service through access authentication method of remote user within HAN; thus, confidentiality of important personal information within home network is secured.

As a plan for privacy information management, users within home network should be granted different service authority according to the role. Therefore, security policy and access control method regarding the grant of service authority based on role of users should be defined.

The most vulnerable aspect of ID/password based authentication protocol used by the existing home network lies in the dictionary attack of the attacker. Therefore, in order to prevent this, attacker should not be able to acquire any information on password with passive attack such as wiretapping, while proper user authentication protocol is being executed. The proposed method creates one time key by using password and time stamp of previously registered user and random number for the authentication of remote user. Therefore, the access cannot be gained even with the acquisition of password registered by the user.

Also, in case of impersonation attack, authorized MAC value has been used in authentication process; thus, the session value for each registered device is required. In this aspect, access of unauthorized user is restricted.

For checking the overall security of the proposed scheme, the various security analyses against major attacks including replay attack, impersonation attack, entity mutual authentication, access control, and man-in-the-middle attack have been described as follows.

(i) Replay Attack. The proposed method creates one-time secret key through one-way hash function using time stamp and password. Therefore, the attacker cannot execute replay attack and use intercepted ID. Due to such reasons, even when the attacker attempts to reuse it by using the session, the access is denied accordingly with the application of value of time stamp.

(ii) Impersonation Attack. When unauthorized user remotely attempts the home device spoofing, the attacker needs authorized MAC value. At the moment, in order to create authorized MAC value, the session value of registered device is necessary. In order to acquire the session value at the moment, the secret key of device granted from the authentication server needs to be entered. Therefore, access by unauthorized user is impossible.

(iii) Mutual Authentication. The authentication process for mutual authentication between remote user and home device is performed by examining the justification of device to access using MAC value, random value, session value, and registered device ID; thus, it is secure from unauthorized piracy, access, and invasion of unauthorized user.

(iv) Access Control. Access level is applied accordingly with the context aware data only for the authorized members when accessing DB system and device within home network; thus, it minimizes the access to personal information and device by differentiating the level of access for the same service. When administrator or users attempt to access device located in remote place in smart grid environment, access control and authentication mechanism to defend the inadequate access and application and user's behavior that exceeds the approved authority will be applied.

(v) Man-in-the-Middle Attack. In case of attack in which the attacker intercepts the data transmitted from the telecommunication channel and disguises as the receiver for the sender and as the sender for the receiver, the behavior of middle attacker including the data forging and modification of message is blocked with the creation of proper key value applied during the creation of session. As the secret key of device granted from the authentication server needs to be input in order to acquire the session value during the creation of each session, the access is blocked for the spoofing.

With the analyses on security evaluation as above, the access of unauthorized external user to the home device was blocked and it enabled the secure remote access of authorized user in home network based smart grid environment. Also, it enabled various services such as remote confirmation on

the amount of electricity use in home network and control of home devices. In aspect of power supplier, it can provide the information check on electricity consumption of user, monitoring on irregular use, and illegal invasion detection service and this would maximize the energy use efficiency of the consumer who uses the home network.

5. Conclusions

Smart grid security confronts more difficulties compared to basic network security. This is due to the fact that it requires the power security, IT security, and telecommunication system security. Also, it requires reliability, defense on cyber-physical attack, and privacy protection, in addition to confidentiality, integrity, and availability security. Smart grid is intelligent electrical grid of the next generation that optimizes the energy efficiency by applying IT technology to the existing electrical grid so that supplier and consumer can exchange real-time information both ways. However, in such smart grid environment, there is a high possibility of various security threats including data disclosure and data piracy that exist in the two-way communication using smart devices such as smart meter and AMI.

Particularly, it is necessary to conduct studies on service access authentication process of user in regard to various attacks on privacy within smart grid. Living information, personal information, and payment information are gradually becoming the big data and there is increase in concern for the security of data. Secure authentication method for the protection of user's privacy in home network based environment within smart grid was proposed in this study. The proposed authentication method protects security against replay attack, impersonation attack, entity mutual authentication, and others by performing the authentication process for user who accesses personal information created and transmitted from home network and AMI.

The access control authentication method in this study blocks unauthorized access from the outside and enables secure remote control of access to personal information in home network by creating one-time key using random value and password and performing message authentication using this key.

In the authentication process, it was implemented so that time stamp value and one-time key cannot be reused regardless of key value spill once the session has been created with them.

Such service in smart grid environment provides not only consulting information of energy consumption reduction such as electricity use history management and usage pattern analysis of users but also additional function in which user can directly participate to reduce the amount of energy use.

More light security system compared to the proposed security module should be implemented and studies on more diverse forms of use should be conducted in the future.

Notation

ID_A, ID_B: ID of user A and device B
K_A: Encryption key of user A
TS_i: Time stamp
R_S: Random value created from authentication server
$K_{A,B}$: Session key of user A and device B
$E(K, M)$: Encryption of message M using symmetric key K
$MAC(K, M)$: Message authentication code of message M that uses symmetric key K
$A \parallel B$: A and B are concatenated.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2011-0014394).

References

[1] E. W. Gunther, A. Snyder, G. Gilchrist, and D. R. Highfill, "Smart Grid Standards Assessment and Recommendations for Adoption and Development (Draft v0. 82)," Enernex for California Energy Commission, 2009.

[2] U.S. Department of Commerce, "NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1. 0 (Draft)," 2009.

[3] S.-S. Yeo, D.-J. Kang, and J. H. Park, "Intelligent decision-making system with green pervasive computing for renewable energy business in electricity markets on smart grid," *Eurasip Journal on Wireless Communications and Networking*, vol. 2009, Article ID 247483, 2009.

[4] K. Geun-Young and K. Young-Myoung, "Implemen-tation of Telco Home Network-based AMI," *Journal of the Korean Institute of Information Scientists and Engineers*, vol. 27, no. 11, pp. 93–97, 2009.

[5] D.-S. Wang and J.-P. Li, "A novel mutual authentication scheme based on fingerprint biometric and nonce using smart cards," *International Journal of Security and Its Applications*, vol. 5, no. 4, pp. 1–12, 2011.

[6] H. Jin-Bum and H. Jong-Wook, "A security model for home networks with authority delegation," in *Proceedings of the International Conference on Computational Science and Its Applications (ICCSA '4)*, pp. 360–369, 2006.

[7] S. Sun, Z. Yan, and J. Zambreno, "Demonstrable differential power analysis attacks on real-world FPGA-based embedded systems," *Integrated Computer-Aided Engineering*, vol. 16, no. 2, pp. 119–130, 2009.

[8] D.-E. Cho, B.-S. Koh, and S.-S. Yeo, "Secure D-CAS system for digital contents downloading services," *Journal of Supercomputing*, vol. 64, no. 26, pp. 477–491, 2011.

[9] T. A. L. Pham, N. Le-Thanh, and P. Sander, "Decomposition-based reasoning for large knowledge bases in description logics," *Integrated Computer-Aided Engineering*, vol. 15, no. 1, pp. 53–70, 2008.

[10] X. Tao, Y. Li, and R. Nayak, "A knowledge retrieval model using ontology mining and user profiling," *Integrated Computer-Aided Engineering*, vol. 15, no. 4, pp. 313–329, 2008.

[11] Q. Chen, S. Zhang, and Y.-P. P. Chen, "Rule-based dependency models for security protocol analysis," *Integrated Computer-Aided Engineering*, vol. 15, no. 4, pp. 369–380, 2008.

[12] H. Ko, G. Marreiros, H. Morais, Z. Vale, and C. Ramos, "Intelligent supervisory control system for home devices using a cyber physical approach," *Integrated Computer-Aided Engineering*, vol. 19, no. 1, pp. 67–79, 2012.

[13] S.-C. Kim, S.-S. Yeo, and S. K. Kim, "A hybrid user authentication protocol for mobile IPTV service," *Multimedia Tools and Applications*, pp. 1–14, 2011.

[14] A. Sánchez, E. O. Nunes, and A. Conci, "Using adaptive background subtraction into a multi-level model for traffic surveillance," *Integrated Computer-Aided Engineering*, vol. 19, no. 3, pp. 239–256, 2012.

[15] L. Tan and S. Xu, "A model-checking-based approach to risk analysis in supply chain consolidations," *Integrated Computer-Aided Engineering*, vol. 16, no. 3, pp. 243–257, 2009.

[16] https://sites.google.com/a/itrconline.net/itrc/projectinfo/2012semina.

[17] J. Kim, H. Jeon, and J. Lee, "Network management framework and lifetime evaluation method for wireless sensor networks," *Integrated Computer-Aided Engineering*, vol. 19, no. 2, pp. 165–178, 2012.

[18] D.-E. Cho and S.-J. Kim, "Study on safe remote control method of home device under environment of smart grid," *Lecture Notes in Electrical Engineering*, vol. 179, no. 2, pp. 281–286, 2012.

[19] Z. Banković, J. M. Moya, Á. Araujo, D. Fraga, J. C. Vallejo, and J.-M. de Goyeneche, "Distributed intrusion detection system for wireless sensor networks based on a reputation system coupled with kernel self-organizing maps," *Integrated Computer-Aided Engineering*, vol. 17, no. 2, pp. 87–102, 2010.

[20] D.-E. Cho, H.-J. Shin, and S.-J. Kim, "The personal information protection technique in smart grid environment," *Information B*, vol. 16, no. 3, pp. 2179–2184, 2013.

[21] NIST, "Smart Grid Cyber Security Strategy and Requirements," DRAFT NISTIR, 7628, 2010.

[22] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security and Privacy*, vol. 7, no. 3, pp. 75–77, 2009.