Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2014, Article ID 208424, 8 pages
http://dx.doi.org/10.1155/2014/208424

Research Article

Enhanced ID-Based Authentication Scheme Using OTP in Smart Grid AMI Environment

Sang-Soo Yeo,[1] Dae-il Park,[1] and Young-Ae Jung[2]

[1] *Division of Computer Engineering, Mokwon University, Daejeon 302-729, Republic of Korea*
[2] *Division of Information Technology Education, Sun Moon University, Asan 336-708, Republic of Korea*

Correspondence should be addressed to Young-Ae Jung; dr.youngae.jung@gmail.com

Received 20 November 2013; Accepted 21 January 2014; Published 7 April 2014

Academic Editor: Jongsung Kim

This paper presents the vulnerabilities analyses of KL scheme which is an ID-based authentication scheme for AMI network attached SCADA in smart grid and proposes a security-enhanced authentication scheme which satisfies forward secrecy as well as security requirements introduced in KL scheme and also other existing schemes. The proposed scheme uses MDMS which is the supervising system located in an electrical company as a time-synchronizing server in order to synchronize smart devices at home and conducts authentication between smart meter and smart devices using a new secret value generated by an OTP generator every session. The proposed scheme has forward secrecy, so it increases overall security, but its communication and computation overhead reduce its performance slightly, comparing the existing schemes. Nonetheless, hardware specification and communication bandwidth of smart devices will have better conditions continuously, so the proposed scheme would be a good choice for secure AMI environment.

1. Introduction

Smart grid is a convergence technology adding information technology to a conventional electrical power grid to bilaterally exchange and use real-time information electricity generated in a power plant with users through the core infrastructure of AMI (advanced metering infrastructure) [1–3]. Consumers can utilize AMI to monitor power use in real time and save household and company energy cost, contributing to an appropriate level of energy production, lower production cost, and higher confidence on sustainable energy supply [1–3]. Also, more new and renewable energy is used to help overcome global environmental problems [4]. With such a widespread smart grid environment, smart grid security has also become significant [3, 5].

The existing power grid operated in a closed net, effectively distancing itself from people having malicious intentions [6, 7]. However, smart grid puts the grid device in the customer domain, making its power net vulnerable to malicious attacks both online and offline. Malicious attacks can be made by penetrating into an upper-level power grid system through smart grid devices or by taking over a user's device to send false information or infringing private information by using a user's power consumption pattern and so forth [8–10].

To prevent such malicious attacks, devices installed in the users' domain and power suppliers' own system should securely communicate. To this end, more researches are necessary to find a way for supplier systems to authenticate user-domain devices and allow only valid users to transmit data [3, 5–11].

This paper proposes a novel scheme for improving security aspects of KL scheme [12] in order to provide forward secrecy. We, in this paper, investigate the previous research results first, then make suggestions on how to provide forward secrecy where the existing schemes did not pay attention. To guarantee forward secrecy, we propose the time synchronization scheme OTP to let undisclosed values change. The proposed scheme herein satisfies every security requirement of the KL scheme and adds hash calculation and communication frequency for forward secrecy.

The proposed scheme added a function of time synchronization server to the meter data management system (MDMS) to resolve the problem of having a separate set of time synchronization server but it requires one more round of communication for time synchronization to make the total

communication frequency of four. Based on the analysis of the proposed time synchronized OTP scheme, we show the best time and the best conditions for using that scheme.

This paper is structured as follows. Sections 2 and 3 introduce AMI components and previous security schemes with their weak points or problems. Section 4 proposes a security protocol to increase the security aspects of the existing schemes. Section 5 presents a comparison of security and performance between the existing schemes and the proposed one. Section 6 finishes by drawing a conclusion.

2. Related Work

In this section, we look at the components of AMI as described in previous researches and analyze those authentication schemes.

2.1. AMI Components. AMI components, as in Figure 1, are identified centering on the MDMS as the upper system in a power company; Smart Meter, communication system connecting a power company and household's smart meter; household devices, and so forth. For smart meter's authentication of devices, we adopted the power line communication (PLC), a power line communication, and ZigBee through home area network (HAN). The neighborhood area network (NAN) is used for communication between smart meter and MDMS for data transmission.

2.2. KL Scheme. The KL scheme proposed by Kim and Lee in [12] encodes N, an undisclosed value created by the device, and saves it in the device itself and smart meter to create information necessary for authentication based on the security of the N value. Then it performs authentication and verification, as describe in Figure 2. The device creates an authentication key to make possible the inference of a random number of R included in an undisclosed individual N value transmitted in the registration stage during the smart meter authentication process. Then it sends the value to smart meter to proceed with authentication and identify device through ID identifiers. P value is not shown during communication so that N value can hardly be inferred. By combining existing information and data sent from the device for mutual authentication, the proposed scheme generates V' value based on the smart meter-generated P' for successful mutual authentication.

Nonrepudiation is possible in authentication and data exchange between smart meter and MDMS as private keys are sent only to specifically intended MDMSs by using smart meter $\mathrm{MAC}_{\mathrm{Addr}}$ and hash-calculated private keys to encode data. And the MDMSs receiving the data send their ID's to smart meter to identify MDMS when transmitting power, ensuring power information is sent to a right MDMS.

3. Vulnerabilities of KL Scheme

The KL scheme deals with device-smart meter-MDMS authentication and data transmission to help resolve problems such as, for instance, an external device accesses smart meter to increase power use in an AMI network environment or raise charges. Also as regular communication is made between smart meter and MDMS, we suggested a scheme that requires less calculation and less communication frequency for faster data processing when multiple smart meters send data to MDMS to authenticate smart meters securely and send data effectively. But the undisclosed value of N is fixed, which is used for device-smart meter authentication and data transmission, and each session needs it for operation. Therefore, if a disclosed key or N value is inferred and exposed, those values already used for session performance to complete transmission could be assessed by malicious attackers, risking forward secrecy.

Forward secrecy refers to a situation where a malicious attacker who happened to make a successful attack to know current communication information should not be able to trace previous secret information only with that disclosed information.

The undisclosed value of KF scheme, N is secured as devices and smart meters exchanged in the registration status. But if any malicious attackers get to know N value or symmetric key at any given point, they can infer the undisclosed value of N after getting communication information from successful attacks on the authentication stage communication. Thus, past information records are easily captured by malicious attackers in the system.

4. Security-Enhanced ID-Based Authentication

In this section, we propose a security scheme using IDs for authentication as described in the KL scheme yet in a further improved version with better forward secrecy protection than previous design protocols. The proposed scheme herein is an encryption to calculate through OTP function an undisclosed value and the present time based on the time synchronized by the time synchronization to allow the undisclosed value to change.

The proposed ID-based authentication scheme is an advanced version that guarantees to meet all of the security requirements while guaranteeing forward secrecy at the same time.

4.1. Terms. Codes and terms used for the protocol herein are defined as follows:

M: Meter data

ks: Session keys shared by each entity

$\mathrm{MAC}_{\mathrm{Addr}}$: MAC address of smart meter

ID_*: Name of $*$

T_*: Transmission hour value of $*$

R_*: Random number created by $*$

PW_*: Passwords entered by $*$ in synchronization

$B_*[]$: Encryption by using $*$'s key

$h()$: One-way hash function

OTP(): OTP function

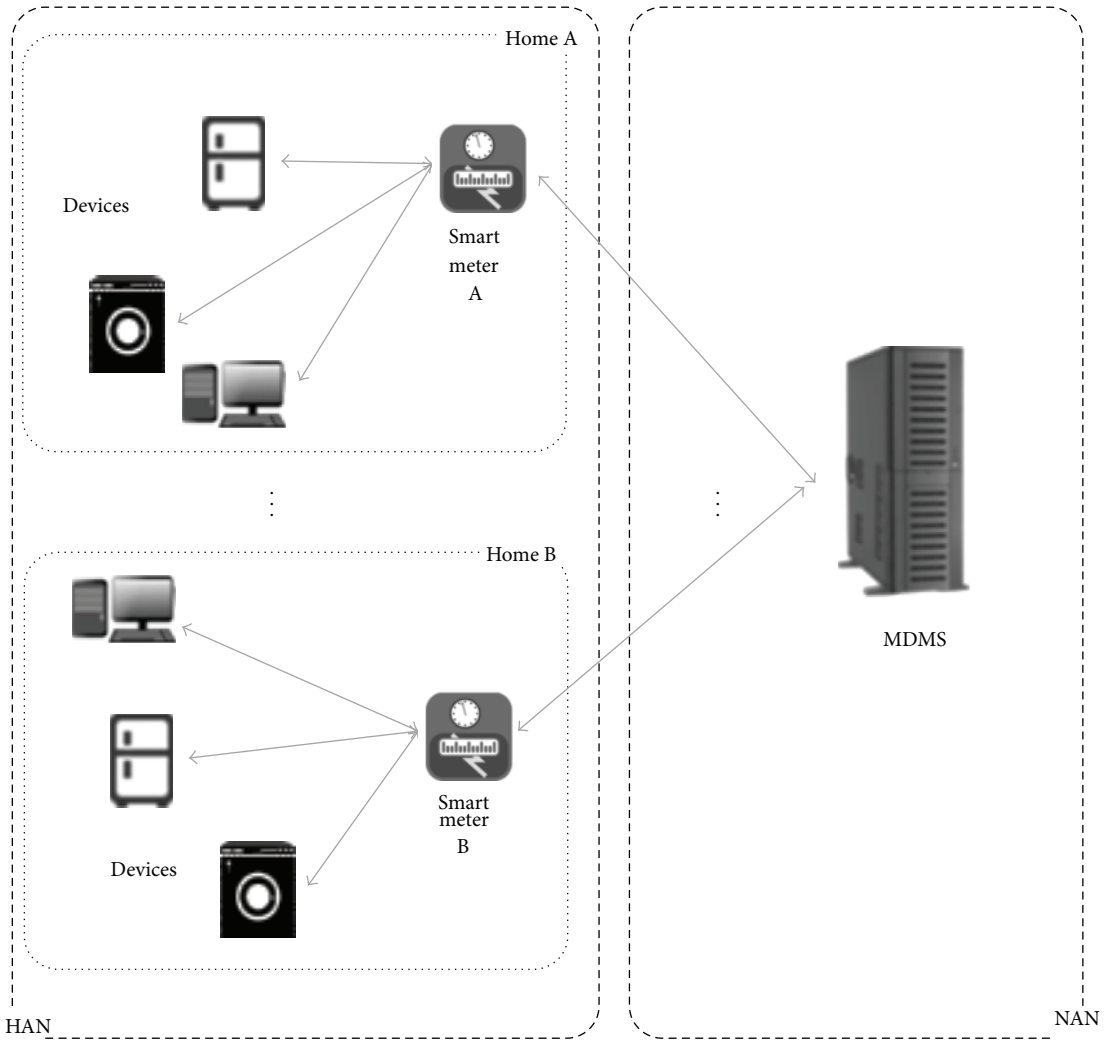

Figure 1: General structure of AMI.

T_{MDMS}: MDMS global time synchronization value

T_{SYN}: Smart meter global time synchronization value

K_{SMP}: Private key of smart meter

‖: Bit combination.

4.2. The Proposed Scheme. An authentication scheme is suggested to help resolve forward secrecy problems by using MDMS, of the KL scheme components, as a global time synchronization server to activate the time synchronization OTP scheme. The suggested scheme requests a time synchronization value of T_{MDMS} to the time synchronization server MDMS in the smart meter registration phase to perform smart meter's time synchronization. Smart meters with completed synchronization send T_{SYN} to devices for smart meter time synchronization at any registration request by a device to synchronize time between smart meter and devices. After synchronization, the device calculates the present time Time of the synchronized time and the undisclosed value of N_{seed} through OTP function to encryption. The time synchronization OTP scheme is performed in line with the order as follows.

Phase 1: Smart Meter Registration and Time Synchronization. MDMS used for registration and time synchronization stages functions as a global time synchronization server. Smart meter, during registration, sends a request of the time synchronization value of request T_{MDMS} to MDMS. The receiving MDMS generates T_{MDMS} value based on the global time of request receipt from smart meter and sent it back to smart meter. Smart meter, then, synchronizes time with MDMS versus T_{MDMS}. Smart meter registration and time synchronization procedures are as follows in Figure 3.

(1) Smart meter A produces N_A by calculating its own private key K_{SMP}'s hash-calculated value $h(K_{SMP})$ with smart meter's MAC_{Addr}. Then the produced value N_A is bit combined with T_{SM}, MAC_{Addr} and

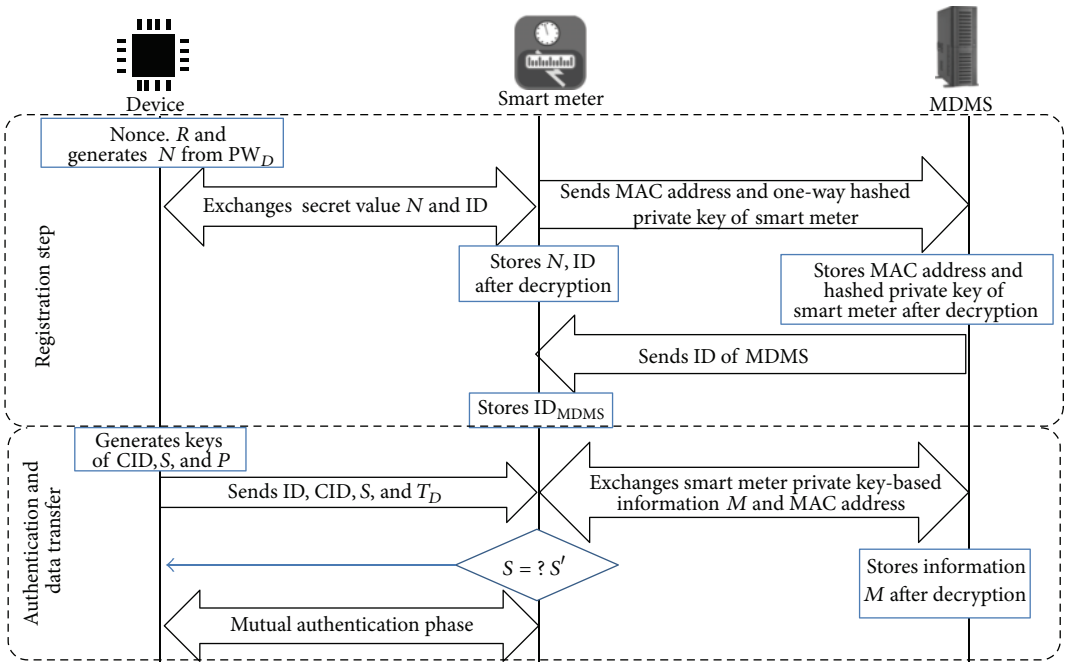

Figure 2: Initial setup and authentication phase of KL scheme.

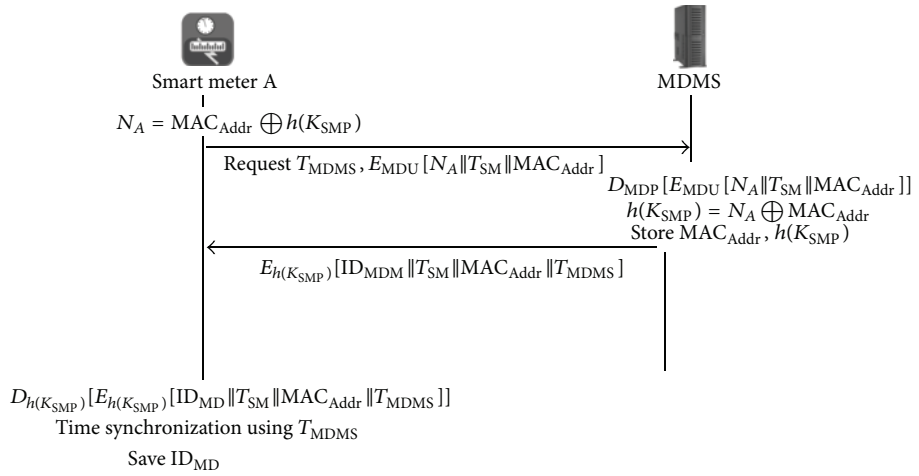

Figure 3: Smart meter registration and synchronization phase between smart meter and MDMS.

encrypted by using disclosed MDMS key and information, in addition the request for time synchronization request T_{MDMS} is sent to MDMS. Consider

$$\begin{aligned} &\mathrm{SM} : N_A = \mathrm{MAC}_{\mathrm{Addr}} \oplus h\left(K_{\mathrm{SMP}}\right) \\ &\mathrm{SM} \longrightarrow \mathrm{MD} : \text{request } T_{\mathrm{MDMS}}, \\ &E_{\mathrm{MDUU}}\left[N_A \parallel T_{\mathrm{SM}} \parallel \mathrm{MAC}_{\mathrm{Addr}}\right]. \end{aligned} \tag{1}$$

(2) MDMS produces the time synchronization value of $\mathrm{T}_{\mathrm{MDMS}}$ based on request T_{MDMS} and decodes the transmitted data which was encrypted with an MDMS disclosed key by using a private key. Based on the decoded value of N_A and $\mathrm{MAC}_{\mathrm{Addr}}$, it draws out smart meter's hash-calculated private key $h(K_{\mathrm{SMP}})$. In the authentication phase, it saves $\mathrm{MAC}_{\mathrm{Addr}}$ and $h(K_{\mathrm{SMP}})$in MDMS to make a proper search of $h(K_{\mathrm{SMP}})$ by using identifier $\mathrm{MAC}_{\mathrm{Addr}}$. Consider

$$\begin{aligned} &\mathrm{MD} : \left[E_{\mathrm{MDU}}\left[N_A \parallel T_{\mathrm{SM}} \parallel \mathrm{MAC}_{\mathrm{Addr}}\right]\right] \\ &h\left(K_{\mathrm{SMP}}\right) = N_A \oplus \mathrm{MAC}_{\mathrm{Addr}} \\ &\text{Store } h\left(K_{\mathrm{SMP}}\right), \mathrm{MAC}_{\mathrm{Addr}}. \end{aligned} \tag{2}$$

(3) After saving a private key of smart meter, MDMS performs bit combination between MDMS ID of $\mathrm{ID}_{\mathrm{MD}}$, T_{SM}, and $\mathrm{MAC}_{\mathrm{Addr}}$ transmitted from smart meter and T_{MDMS}, the time synchronization value.

Then with the extracted hash-calculated private key of smart meter $h(K_{\mathrm{SMP}})$, it encodes the value and sends to smart meter. Consider

$$\mathrm{MD} \longrightarrow \mathrm{SM}: E_{h(K_{\mathrm{SMP}})}\left[\mathrm{ID}_{\mathrm{MD}} \parallel T_{\mathrm{SM}} \parallel \mathrm{MAC}_{\mathrm{Addr}} \parallel T_{\mathrm{MDMS}}\right]. \tag{3}$$

(4) Smart meter decodes the received value by using hash-calculated private key $h(K_{\mathrm{SMP}})$ and carries out time synchronization through the time synchronization value of T_{MDMS}. After time synchronization, MDMS' ID of $\mathrm{ID}_{\mathrm{MD}}$ is saved in smart meter to complete smart meter-MDMS registration. Consider

$$\mathrm{SM}: D_{h(k_{\mathrm{SMP}})}\left[E_{h(k_{\mathrm{SMP}})}\left[\mathrm{ID}_{\mathrm{MD}} \parallel T_{\mathrm{SM}} \parallel T_{\mathrm{MDMS}}\right]\right]. \tag{4}$$

Time synchronization to T_{MDMS}
Store $\mathrm{ID}_{\mathrm{MD}}$.

Phase 2: Device Registration and Time Synchronization. Devices encrypt and send undisclosed values with a symmetric key in the smart meter registration phase and send it. And at the same time, they request a synchronization value. Smart meter uses a symmetric key to decode the undisclosed value and save device ID to identify the undisclosed value and device. Smart meter produces the time synchronization value of T_{SYN} and produces T_{res} through undisclosed value N_{seed} from devices and device identifier ID_D. The produced T_{res} is encrypted with a symmetric key and sent to a device. The device decodes the received value T_{res} and extracts T_{SYN} and saves the value then completes the time synchronization and registration phase. The registration and time synchronization procedures are shown in Figure 4.

(1) Devices, to generate undisclosed value of N_{seed}, conduct hash calculation of the password PW_D entered initially to start the device and device ID, ID_D; then they calculate final values with the random number R_D value created by the device. Consider

$$N_{\mathrm{seed}} = R_D \oplus h\left(\mathrm{ID}_D \oplus \mathrm{PW}_D\right). \tag{5}$$

(2) Devices use a mutually-shared symmetric key for encryption of N_{seed} to securely send the undisclosed value to smart meter. By bit combining the encrypted value with device identifier ID_D, they request the time synchronization value while sending it to smart meter. Consider

$$D \longrightarrow \mathrm{SM}: \text{request } T_{\mathrm{SYN}}, E_{\mathrm{ks}}\left[N_{\mathrm{seed}}\right] \parallel \mathrm{ID}_D. \tag{6}$$

(3) Smart meter extracts ID_D value from the value it received and deciphers the encrypted undisclosed value N_{seed} and saves ID_D and N_{seed} in smart meter. Consider

$$\begin{aligned} &\mathrm{SM}: D_{\mathrm{ks}}\left[E_{\mathrm{ks}}\left[N_{\mathrm{seed}}\right]\right]. \\ &\mathrm{SM}: \text{Store } N_{\mathrm{seed}}, \mathrm{ID}_D. \end{aligned} \tag{7}$$

(4) Smart meter, in order for a device to decode the time synchronization value, performs hash calculation by using device ID, ID_D, and N_{seed}, then calculates them with the time synchronization value T_{SYN} to produce T_{res}. The generated value T_{res} is encoded with a shared symmetric key and sent to a device from smart meter. Consider

$$\begin{aligned} &\mathrm{SM}: T_{\mathrm{res}} = T_{\mathrm{SYN}} \oplus h\left(\mathrm{ID}_D \oplus N_{\mathrm{seed}}\right) \\ &\mathrm{SM} \longrightarrow D: \text{respones } E_{\mathrm{ks}}\left[T_{\mathrm{res}}\right]. \end{aligned} \tag{8}$$

(5) The device uses the symmetric key to decipher the received value and extracts from T_{res} the time synchronization value T_{SYN} to perform time synchronization between smart meter and the device. Here, based on the time synchronization value of T_{SYN}, the present time value generating every fixed period is Time. Consider

$$\begin{aligned} &D: D_{\mathrm{ks}}\left[E_{\mathrm{ks}}\left[T_{\mathrm{res}}\right]\right] \\ &T_{\mathrm{SYN}} = T_{\mathrm{res}} \oplus h\left(\mathrm{ID}_D \oplus N_{\mathrm{seed}}\right). \end{aligned} \tag{9}$$

Time synchronization to $D: T_{\mathrm{SYN}}$.

Phase 3: Authentication. In the device registration and time synchronization stage, devices and smart meters completing undisclosed value transmission and time synchronization store undisclosed value N_{seed} and ID_D to identify devices. Devices and smart meters are time synchronized by T_{SYN} to generate the value of present time Time that has a certain cycle and create final value N_{OTP} through $\mathrm{OTP}(N_{\mathrm{seed}}, \mathrm{Time})$.

Using the generated value N_{OTP}, devices produce CID, P, S and then send ID, CID, S, and T_D to smart meter. Smart meter calculates the value N_{OTP} by itself and also calculates the value P which is not transmitted through the communication. And then smart meter performs authentication using N_{OTP}, P, and S. If the authentication succeeds, they produce value V' based on value P'. Mutual authentication between device and smart meter remains secure by not exchanging value P through communication.

Even though N_{OTP} value is noticed by inferring, Time values change each session; thus the produced value of N_{OTP} varies from session to session to satisfy forward secrecy. Authentication steps are shown in Figure 5.

(1) Devices use N_{seed} and the present time value Time of synchronized devices, which are synchronized every session based on Time through OTP function to produce N_{OTP} value and calculate CID, P, S by using the time stamp value of T_D that changes secret number N_{OTP} each session along with the random number R_D generated in the registration stage, the

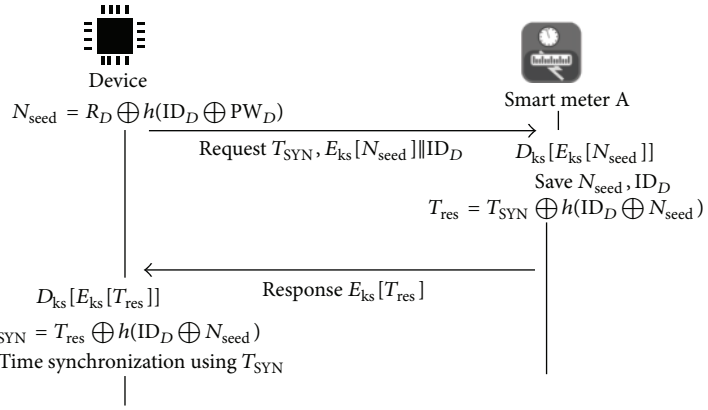

Figure 4: Device registration and synchronization phase between device and smart meter.

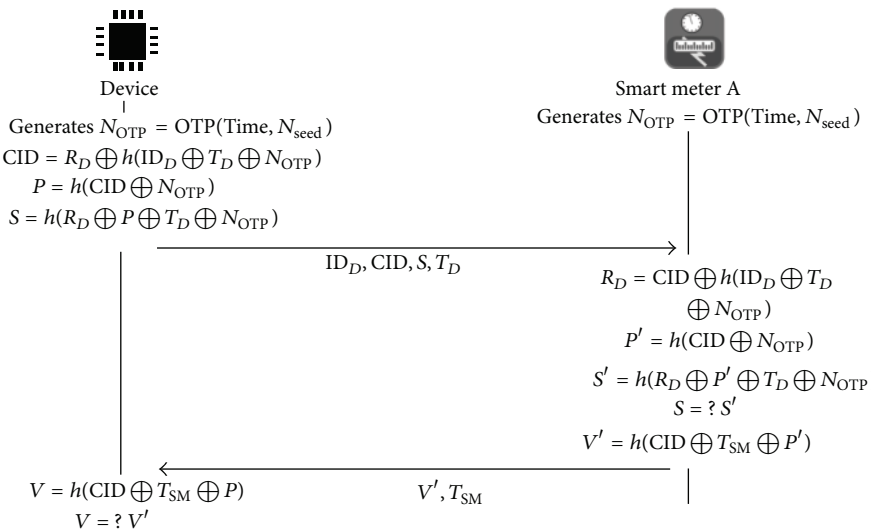

Figure 5: Authentication phase.

undisclosed value N_{OTP}, and the device ID value. Consider

$$\begin{aligned} N_{OTP} &= OTP(N_{seed}, Time) \\ D: CID &= R_D \oplus h(ID_D \oplus T_D \oplus N_{OTP}) \\ P &= h(CID \oplus N_{OTP}) \\ S &= h(R \oplus P \oplus T_D \oplus N_{OTP}). \end{aligned} \tag{10}$$

(2) Devices send ID_D, CID, S, and T_D to smart meter excluding P value of the generated values. Smart meter, just as devices, generates N_{OTP} value. Consider

$$\begin{aligned} D &\longrightarrow SM: ID, CID, S, T_D \\ SM: N_{OTP} &\text{ Create.} \end{aligned} \tag{11}$$

(3) Smart meter performs hash calculation of N_{OTP} and the values generated by CID and smart meter of the received values to produce P' and extracts random value R_D based on CID to get the value of S', necessary for authentication. Consider

$$\begin{aligned} SM: R &= CID \oplus T_D \oplus N_{OTP} \\ P' &= h(CID \oplus N_{OTP}) \\ S' &= h(R \oplus P' \oplus T_D \oplus N_{OTP}). \end{aligned} \tag{12}$$

(4) After comparing S received from smart meter and the produced value S', the authentication process is completed. If authentication succeeds, the value of V' is produced to be used for mutual authentication through ID, P' value, and smart meter's time stamp value T_{SM}. It is sent to devices, including the smart meter's time stamp T_{SM}. Consider

$$SM: S' = ?S$$

$$\mathrm{SM} : V' = h\left(\mathrm{CID} \oplus T_{\mathrm{SM}} \oplus P'\right).$$
$$\mathrm{SM} \longrightarrow D : V', T_{\mathrm{SM}}. \tag{13}$$

(5) Devices produce V value based on the received T_{SM} and compare with the received value V' to perform mutual authentication. Consider

$$D : V = h\left(\mathrm{CID} \oplus T_{\mathrm{SM}} \oplus P\right)$$
$$D : V =? V'. \tag{14}$$

5. Security and Performance

KL's device authentication scheme shares N value after encryption in the registration stage and conducts authentication while hiding the secrecy of the N value. In this scheme, the main data of N is not shared in the process of communication to keep its secrecy and as secret key K_A is hash calculated, its integrity is secured. By adding time stamp to generated CID, P, and S values, the scheme allows change for every session in preparation for possible reuse attack. Devices and smart meter include a mutual authentication process to verify they are in communication with the right counterpart. But, in this case, if a symmetric key that encodes the undisclosed value or undisclosed value N is exposed by inference, even previously-used data, not just the current information, could be exposed too, implying the risk of forward secrecy vulnerability. Also, we found a missing part in the calculation amount estimation process so we recalculated the calculation load of Hash scheme. Deciphering process was also not included in the calculation load estimation, so it was reassessed and presented in Table 1.

The proposed scheme is designed for reducing the disclosure possibility of constant N value, a key factor for forward secrecy, throughout the authentication process; the value of N_{seed} is encoded upon registration and sent to smart meter. Even though the initial N_{seed} value is exposed, further exposure of other N_i values would be extremely difficult by design to guarantee forward secrecy.

The proposed scheme utilizes MDMS as a time synchronization server to receive time synchronization value from MDMS in the initial smart meter registration stage and performs smart meter synchronization. Smart meters completing time synchronization encode smart meter time synchronization value based on device ID and undisclosed value used for devices to request registration to smart meter; then it sends it to devices. Devices encrypt the time synchronization values and synchronize time. Devices put the present time Time based on the synchronized hour and the undisclosed value of N_{seed} to OTP function to produce N_{OTP} for authentication. Even if N_{seed} value is exposed, further information is necessary including the value of N_{seed} used for device-smart meter authentication and the present time Time based on the synchronized hour to get the initial authentication data. And N_{OTP} value can't be guessed because it is calculated using Time value that varies every session, and the time synchronization value of N_{SYN} is not exchanged in communication to complicate inference attempts.

Table 1: Security and performance comparison.

	KL scheme	Proposed scheme
Confidentiality	◯	◯
Integrity	◯	◯
Mutual authentication	◯	◯
Forward secrecy		
Disclosure on communication channel	×	◯
Disclosure on devices	×	×
Calculation amount		
Device		
Registration step	1H + 2E	3H + 4E
Authentication step	8H	10H
Authentication		
Registration step	2H + 2E + 2U	2H + 2E + 2U
Authentication step	2H + 4E1	2H + 4E
Communication number		
Device		
Registration step	1	2
Authentication step	2	2
Smart meter		
Registration step	2	2
Authentication step	1	1
Synchronization problem	—	Yes, but not critical

◯: fully supported; ×: not supported; H: hashing; E: symmetric encryption; U: asymmetric encryption.

6. Conclusion

KL scheme which is designed to protect the AMI-network environment supports mutual authentication by using the undisclosed value transmitted during the initial registration from devices to smart meter while accelerating calculation speed. However, in this scheme, if any undisclosed value is exposed at any given time, malicious attackers can use their accumulated data and the undisclosed value to even get the data used before the time of exposure, troubling forward secrecy. Therefore, in this paper, to resolve forward secrecy problem, we used MDMS as a time synchronization server so that the smart meter receives the time synchronization value from MDMS during the initial registration and exchanges the time synchronization values in the device registration phase to calculate the present time based on the synchronized time in devices and smart meter and the undisclosed value through OTP function for synchronization.

The proposed scheme in this paper is a simpler way to time synchronize but as initially undisclosed values do not change and the time value with cycles based on the synchronized time is used for authentication, undisclosed

values are easily exposed if devices and smart meter are physically attacked. Considering this, we believe it would be more effective to apply the scheme in a closed environment, for instance, where structures are relatively secure against physical attacks and devices or smart meter synchronization and management are conducted altogether.

Conflict of Interests

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

Acknowledgments

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] D. Bailey and E. Wright, *Practical SCADA for Industry*, Newnes, New South Wales, Australia, 2003.

[2] US National Institute of Standards and Technology, "NIST smart grid framework 1.0 document," NIST Special Publication 1108, U.S. National Institute of Standards and Technology, Gaithersburg, Md, USA, 2009.

[3] J.-D. Choi and J.-T. Seo, "Separate networks and an authentication framework in AMI for secure smart grid," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 22, no. 3, pp. 525–536, 2012.

[4] 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, 12 pages, 2009.

[5] J.-W. Jeon, S.-H. Lim, and O.-Y. Yi, "A wireless network structure and AKA(authentication and key agreement) protocol of advanced metering infrastructure on the smart grid based on binary CDMA," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 20, no. 5, pp. 111–124, 2010.

[6] Y. Wang, "sSCADA: securing SCADA infrastructure communications," *International Journal of Communication Networks and Distributed Systems*, vol. 6, no. 1, pp. 59–78, 2011.

[7] G. H. Lee, J. T. Seo, and C. W. Lee, "Smart grid and cyber security," *The Journal of the Korean Institute of Communication Sciences*, vol. 27, no. 4, pp. 23–30, 2010.

[8] N. Wan, H. Jo, K. Cho, and D. H. Lee, "Study on smart grid security," *Review of Korea Institute of Information Security & Cryptology*, vol. 20, no. 5, pp. 20–30, 2010.

[9] M. Abrams and J. Weiss, "Malicious control system cyber security attack case study -Maroochy water services, Australia," Report, NIST Computer Security Division, Gaithersburg, Md, USA, 2008.

[10] R. J. Robles, M.-K. Choi, E.-S. Cho, S.-S. Kim, G.-C. Park, and J. Lee, "Vulnerabilities in SCADA and critical infrastructure systems," *Review of Korea Institute of Information Security & Cryptology*, vol. 1, no. 1, pp. 99–104, 2012.

[11] M. J. Kim, M. Y. Yoon, H. Jung, and H. Y. Yeom, "Standardization trend for smart grid security," *Review of Korea Institute of Information Security & Cryptology*, vol. 22, no. 2, pp. 15–22, 2012.

[12] H. G. Kim and I. Y. Lee, "A study on ID-based authentication scheme in AMI smart grid environment," *The KIPS Transactions C*, vol. 18, no. 6, pp. 397–404, 2011.