applied sciences

MDPI

Article

A Lightweight Scheme to Authenticate and Secure the Communication in Smart Grids

Israa T. Aziz [1,2], Hai Jin [1,*], Ihsan H. Abdulqadder [1], Zaid Alaa Hussien [3], Zaid Ameen Abduljabbar [4] and Firas M. F. Flaih [5]

1 Cluster and Grid Computing Laboratory, Services Computing Technology and System Laboratory, School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China; israa_aziz@hust.edu.cn (I.T.A.); ihsan@hust.edu.cn (I.H.A.)
2 College of Sciences, University of Mosul, Mosul 41002, Iraq
3 Southern Technical University, Basrah 61001, Iraq; zaidpc2005@gmail.com
4 College of Education for Pure Sciences, University of Basrah, Basrah 61001, Iraq; alsulamizaid@gmail.com
5 General Directorate of the North Distribution Electricity, Ministry of Electricity, Baghdad 10013, Iraq; firas_flaih@hust.edu.cn
* Correspondence: hjin@hust.edu.cn; Tel.: +86-27-8754-3529

Received: 31 July 2018; Accepted: 26 August 2018; Published: 1 September 2018

Abstract: Self-reconfiguration in electrical power grids is a significant tool for their planning and operation during both normal and abnormal conditions. The increasing in employment of Intelligent Electronic Devices (IEDs), as well as the rapid growth of the new communication technologies have increased the application of Feeder Automation (FA) in Distribution Networks (DNs). In a Smart Grid (SG), automation equipment, such as a Smart Breaker (SB), is used. Using either a wired or a wireless network or even a combination of both, communication between the Control Center (CC) and SBs can be made. Nowadays, wireless technology is widely used in the communication of DNs. This may cause several security vulnerabilities in the power system, such as remote attacks, with the goal of cutting off the electrical power provided to significant consumers. Therefore, to preserve the cybersecurity of the system, there is a need for a secure scheme. The available literature investments proposed a heavyweight level in security schemes, while the overhead was not considered. To overcome this drawback, this paper presents an efficient lightweight authentication mechanism with the necessary steps to ensure real-time automatic reconfiguration during a fault. As a first stage, authentication will be made between CC and SB, SB then sends the information about its status. To ensure the integrity of the authentication exchange, a hash function is used, while the symmetric algorithm is used to ensure privacy. The applicability of the suggested scheme has been proved by conducting security performance and analysis. The proposed scheme will be injected on ABB medium voltage breaker with the REF 542*plus* controller. Therefore, the probable benefit of the suggested scheme is the contribution to provide more flexibility for electrical utilities in terms of reducing the overall computational overhead and withstanding to various types of attacks, while also opening new prospects in FA of SGs.

Keywords: smart grid; control center; smart breaker; authentication scheme; distribution networks; Feeder Automation

1. Introduction

A topic that is currently being frequently discussed is how the electrical power networks will be designed in the future. Nowadays, many application fields have rapidly grown in their technological evolution, including power systems. With the benefits of IEDs and communication networks, the FA system in DNs can easily be applicable. Therefore, the electrical distribution grid recently witnessed

a transition from the old-style electrical grid to the new style of grid that is called the SG [1]. By implementing intelligent monitoring and control from a distance to power the equipment, an SG will become a promising platform for increasing the efficiency and the quality of service [2]. The primary purpose of the SG is to combine valuable data from the electrical grid to permit the CC to evaluate the present status of the electrical grid [3]. The objective of SGs is to create a new power grid that runs economically and smartly [4]. In an SG environment, feeder handling can be implemented via automatic reconfiguration to improve the voltage profile, power quality and to reduce the branch power loss [5,6]. The ability to self-heal, in case of a fault, is one of the required features for a SG, which brings significant economic benefits [7]. The effect of a prolonged outage in the electric DN to an area would be greater than the economic loss. To achieve a fast power restoration, the power utilities have been using smart remote-controlled breakers in distribution networks to ensure continuous power supply. Guaranteeing the continuity of provided power is one of the primary functions of a power system [8]. SG systems with remote and fast switching breakers make network reconfigurations possible and thus, they reduce the breakout period when an outage occurs [9,10]. The SB can offer new functions such as a real-time remote switch by the CC. The remote signal can be sent by the CC to the SB to connect or disconnect a power line. These breakers have a high impact [11] and become economically sustainable due to a lot of automation equipment and to new communication technologies. The general purpose of computing and communication in power system resources is to improve the system efficiency [12,13]. In the SG, the SB device lies far from CC and uses two-way communications at normal and fault conditions. Therefore, the maneuvers for self-reconfiguration must be passed in a secure way or through a secure process. The data can be sent to the CC and to the SB over wireless or wired networks. Wireless technologies are extensively used for local communication subsystems in the SG [14]. The wireless communication technology may produce new and important challenges for the security of existing network [15]. For instance, a faked fault data can be invented and forwarded to CC or SB. Therefore, without suitable security, the SG cannot perform well as an energy management system [16,17].

In this paper, a secure authentication scheme using a new fast technique for a SB in the SG has been introduced. The proposed scheme consists of two scenarios for authentication between the SB and the CC. The first permits a CC to authenticate with the SB, while the second is similar to the first and allows the SBs to authenticate with its CC. Where, the CC or SB will be Sending End (SE), while the SB or CC will be Receiving End (RE). This scheme permits authentication between the SE and the RE. The SE creates a random number, which is then hidden in the breaker ID, to encrypt the result using the hidden parameter. Afterwards, the SE creates the hash value for the proposed authentication and authorization. At last, the RE receives an authentication signal that contains the hash value from the SE. After receiving the authentication message, firstly, the RE re-decrypts the information to get the random number and then it generates a new parameter called the obtained hash value. The obtained hash is compared with the hash that was previously sent from the SE; if both are equal, then the calculated random number was right. Then, the RE creates a random number and conceals it within the breaker ID and then it encrypts the final result. Secondly, the RE generates an additional hash value that contains the received random parameter and another random parameter and then forwards the authentication message to the SE; this message includes the hash value and the encrypted result. As soon as the authentication message is received, the SE decrypts the information and gets a random value. The SE utilizes a hash value to check if the obtained random value was right.

Numerous investigations have been undertaken in the field of SG security, particularly on mutual authentication. In this section, the key security problem of authentication is presented. The authors in Reference [18] suggested a scheme that offers mutual authentication between smart meters at various locations. The calculated time and communication size of the proposed scheme is high owing to the use of Rivest, Shamir, and Adleman (RSA). In Reference [19], the authors proposed an effective privacy-preserving scheme; holomorphic encryption was employed by the suggested scheme to realize Privacy-Preserving Demand Aggregation (PPDR) and a better response. The authors in

Reference [20] presented several types of schemes and protocols; they proposed a mutual authentication scheme for a Smart Meter (SM) to solve the challenges in SGs. In Reference [21], a scheme to address mutual authentication and to prevent several types of attacks between SG utility networks and SMs was presented. Also, the authors proposed a new protocol for key management to secure data among the utility server and the SMs. The Wide Area Measurement Systems (WAMS) offer a time-synchronized assessment of the situations for electrical power networks over a large geographical area. The WAMS Key management (WAKE) scheme was proposed for securing communications in WAMS [22]. The proposed authentication scheme employed a symmetric key to secure real-time data in the transmission lines. To the best of our knowledge, it is the first study to propose an authentication scheme between CC and SBs in SG. Therefore, the related works are very limited and almost nonexistent.

There is an excessive variability of methods for performing authentication. Unfortunately, much of the available literature investigated SG security, while all the above-mentioned works [18–26] lack high computation and long communication sizes and use a complex scheme such as the Public-Key Infrastructure (PKI). Signature generation as well as signature verification are needed for the PKI. Therefore, these actions cause high computation and communication overhead. An excessive amount of authentication steps is sometimes needed to secure communications, which causes additional computation and communication costs. In this paper, all the previous challenges were addressed by proposing a lightweight authentication scheme for securing the communication between the CC and SBs in an SG.

Generally, this paper contributes to providing SE authentication with RE and to the creation of a secure channel between the CC and the SBs. The proposed scheme will use the symmetric system to ensure the integrity of various interactions with the cryptographic hash function. The benefits of the suggested lightweight scheme offer the authentication with low communication and computation costs; thus, the power consumption will be low. Where, the most articles in wireless security such as [27] focus on the energy cost. The scheme offers the identity of SE detection and ends with the Session Key Agreement (SKA) among SE and RE. The suggested scheme also offers SG Mutual Authentication (SGMA) and with a suitable level of security against multiple attacks. The experiments and measurements adopted in: first, theoretical method then, the simulations platform was done using MATLAB R2014a software. Finally, we recommended to apply the proposed scheme (by the help of ABB switchgear companies) on ABB eVD4 SB and REF542*plus* controller. This work successfully manages the above proposition and is organized as follows.

The discussion of the related works is presented in Section 1. Section 2 deals with the SB in the SG. The network architecture is presented in Section 3, which clarifies the network model and the main goals of this work. Section 4 illustrates the proposed authentication mechanism with all notations and all phases. Section 5 offers the main results and the system performance. The proposed scheme's security analysis for this paper is presented in Section 6 and involves all the necessary safety needs between the CC and the SB. Finally, Section 7 concludes this work.

2. Smart Breaker in Smart Grid

In a smart electrical distribution network, all probable fault locations [6] which can occur in the network were listed in the CC and the SB was designed for online monitoring. The observed electrical network can use the data from the Supervisory Control and Data Acquisition (SCADA) or WAMS. Then, the automatic breakers will isolate the faulty line (during fault occurrence) till the network reconfiguration. The SB sends data about its status to CC, while the CC send commands to the remote switches to connect or disconnect (on or off) [28]. The reconfiguration allows to handover the demand on other lines that have lower loads [29]. The action of the SBs is an automatically process from the CC, which permits the SG to implement the strategies for the continuous process. The CC has fault analysis and application software, where the CC generates an automatic breaker action, while in some situations, directly sends a movement action to the SBs [30]. SG communication mostly uses wireless

infrastructure to send the breakers actions. Using wireless technology in parts of SGs causes a delay in the sensitive data and in various types of attacks [18]. Therefore, there is a necessary need to find a secure path or secure scheme.

The smart breaker which will be used is ABB eVD4, the hardware minimum requirements for "*Initialization Phase*" are: Pentium III, 800 MHz; 128 MB of RAM; 40 MB of available disk space. The software requirements are: Operating system Microsoft Windows 98/2000/XP; PCM600 Version 2.3 Production Build; Microsoft .NET Framework 2.0; and eVD4-RBX615 Connectivity Package. The eVD4 classified as Intelligent Electronic Device (IED) and use the international standard for substation communication and modeling IEC 61850 with GOOSE messaging and Modbus. The controller of the SB will be REF542*plus*, the block diagram of this controller shown in Figure 1. The ability of REF542*plus* is extremely powerful in terms of automation.

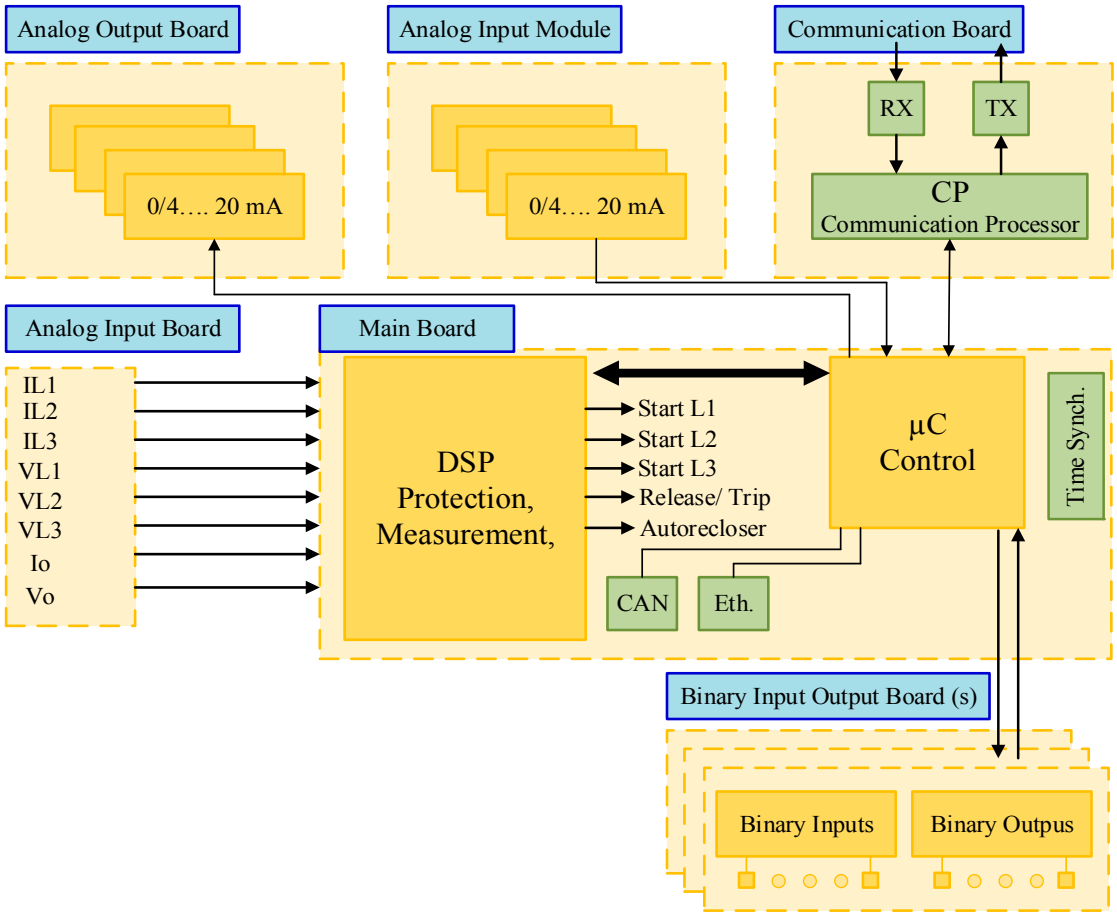

Figure 1. The block diagram of REF 542*plus*.

3. Network Architecture

3.1. Network Model

The suggested manner is applied to the medium scale system of the standard IEEE 33-bus, which is exceedingly utilized as a network model which is shown in . The network includes 33 buses and 37 branches ranging from *s1* to *s37*. It includes 32 branches with normally closed SB pairs, as shown in Figure 2 with solid black lines, and 5 branches with normally opened SB pairs that are shown with the hidden black line. The pairs of breakers shown as red circles denote the beginning and ending of each branch.

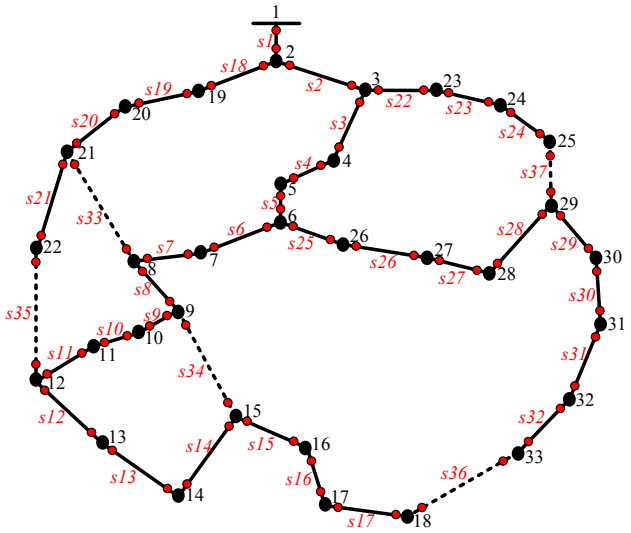

Figure 2. The single-line diagram of IEEE 33-bus network.

The network architecture of the proposed approach between the CC and the SBs under a fault via wireless network of the SG is shown in Figure 3. The real physical fault in DN may occur in any branch due to several causes such as: Lightning, tree contact, birds, squirrels, and vandalism. The fault type may be Line to Ground (LG), Line to Line (LL), Line to Line to Ground (LLG) or Line to Line to Line (LLL). The most fault type is LG which constitutes 80% from the total number of faults. The protection system will manage the fault by physical response to open the SB. The SB is designed to send the information (data) about its status and several measurements such voltage, current, frequency, time and date. The CC is designed to send actions (commands) to open or close the SBs. The wireless communication is widely used where the cyber-attack may be taken place to made a faked fault or disconnect the electricity on a pivotal area.

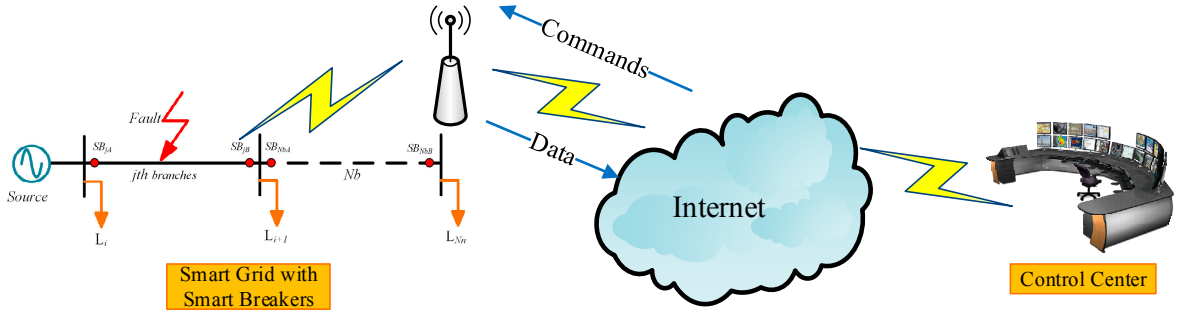

Figure 3. Network Architecture.

where, L_i represents the load at the node i, SB_j represents the smart breaker of the jth branches.

3.2. Design Goals

The SB can disconnect the power line in case of a fault in its line, in which case, the SB tries to communicate with the CC to hand over the load to another line as fast as possible. The goals of this design are as follows:

- Secure the communication channel between the CC and the SBs to avoid cyber-attacks.
- Reduce the overhead of the network in terms of computation and communication costs.
- Anonymous IDs for the SBs and the CC to avoid receiving a fabricated faked fault.
- Prevent different types of attacks.

4. The Proposed Authentication Mechanism

This section presents the proposed scheme, which involves two scenarios to secure the communication between the SBs and the CC. In the first scenario, an SB will be SE, and the CC will be RE. While in the second scenario, the CC will be SE and the SBs will be REs. The notations used in this study (first scenario) are given in Table 1. While, the notations of the second scenario are similar to the first one.

Table 1. The notation used.

Symbol	Definition
$IDsb_j$	Identification of the *j*th *SB*
$IDsbw_j$	ID_j shadow of the *SB*
IDcc	Identification of *CC*
$Msbw_j$	Mask of ID shadow for the *SB*
p_j	Secure Parameter of the *j*th *SB*
p_c	Secure Parameter *CC*
α_j, β_j	Random values from the *SB*, *CC*
Hsb_j	Hash function of the *SB*
$OHsb_j$	Hash function obtained from $IDsbw_j$
$IDcrw_j$	Replay of the control ID shadow
$Mcrw_j$	Mask of the replay of the control ID shadow
Hcrj	Hash value of $IDcrw_j$
$OHcr_j$	Hash value obtained from $IDcrw_j$
$\oplus$	XOR function
$\|\|$	Concatenation function
h	Hash function

The suggested scheme offers SGMA, authorization and information privacy between the SB and the CC. The proposed scheme is involved in the following phases.

- *Initialization Phase*: the SBs in this phase are recorded in the CC with unique identity numbers.
- *Authentication Phase*: from the SB to the CC to authenticate each other.
- *Key Session Phase*: is the mutual key creation, which is utilized as a session key and forwards data from the SB and the CC.

4.1. Initialization Phase

This is like a registration process among the SBs and the CC; it is very important to run the proposed scheme. The SBs are connected to the CC, where the CC is assumed to be a trusted entity. The applied suites cypher, such as a type of hash function, and the cryptography procedure are defined. In addition, an off-line supplier defined the SB identity $IDsb_j$ and the corresponding parameters p_j and p_c for each recorded SB as shown in Figure 4.

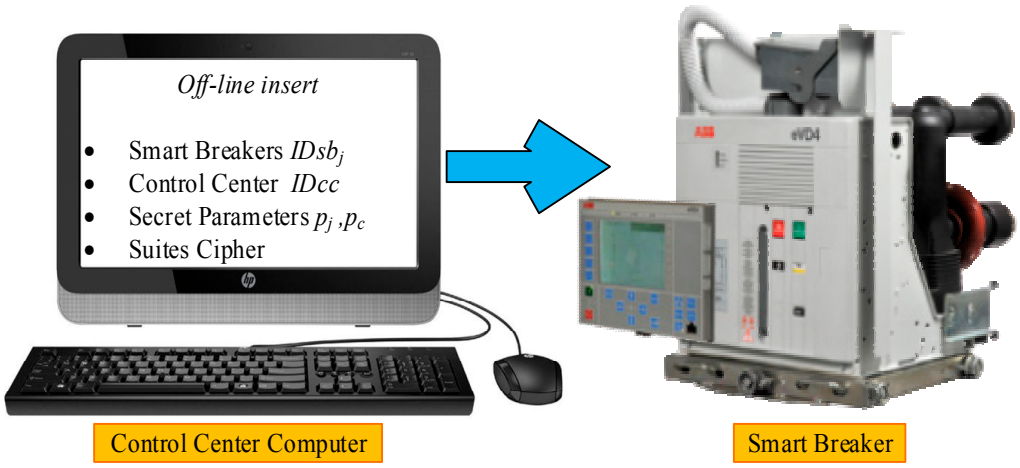

Figure 4. Initialization phase.

4.2. Authentication Phase

In traditional power distribution networks, when a fault occurs in any medium voltage power line, a portion of the load will be unsupplied. Therefore, in the SG, to use the property of self-healing, the SB will disconnect automatically and start to inform the CC about its existing status. This needs particular authentication steps between the SB and the CC. Each remote SB that requires communication with the CC must implement and pass the authentication steps. The suggested authentication scheme can be seen in Figure 5. After confirming the sureness of the information from the SB, the CC will send actions to other SBs. This action, which is achieved through the software, is already saved in the CC and has the ability to deal with fault issues automatically. The CC will make its decisions for specific SBs to handover the network branches to maximize the service within acceptable power losses and the voltage profile. Therefore, the CC will send actions to SBs.

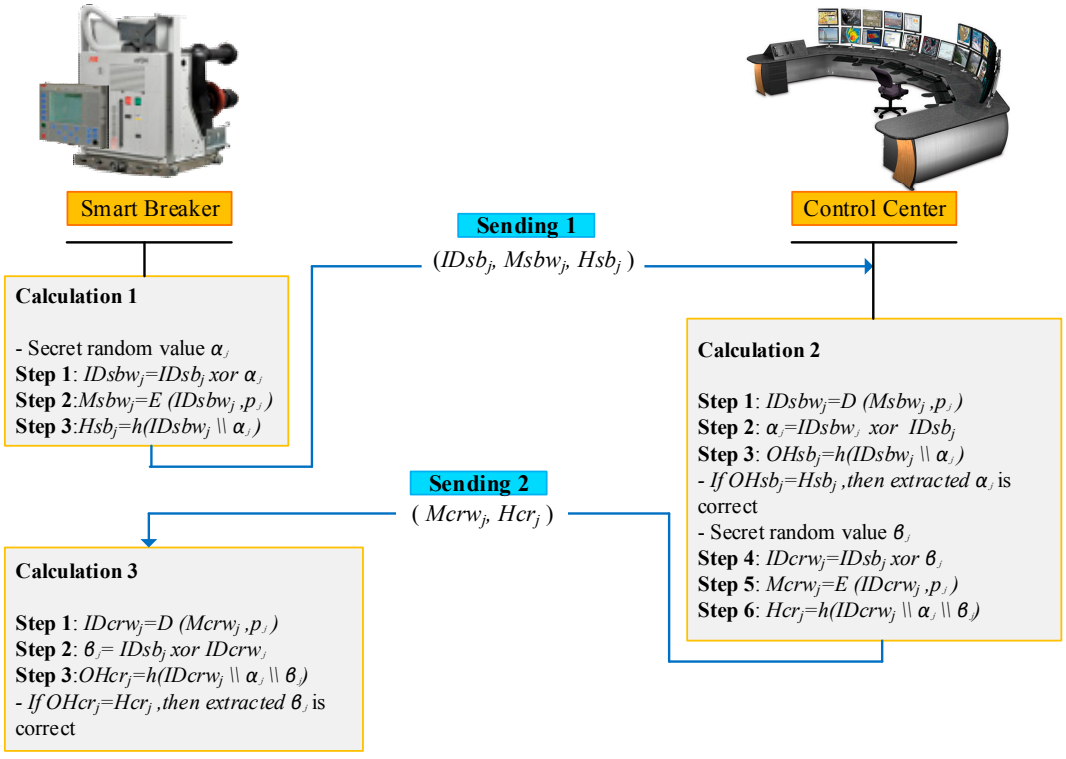

Figure 5. Authentication Scheme SB to CC.

The steps of the authentication phase in this scenario are outlined in the steps below.

Calculation 1

Step 1 the SB generates an unknown random number $\alpha_j \leftarrow$ Z* then it computes *IDsbwj*:

$$IDsbw_j = IDsb_j \oplus \alpha_j$$

Step 2 the SB computes *Msbwj* by coding the *IDsbwj* via the unknown parameter p_j as the secure key:

$$Msbw_j = E(IDsbw_j, p_j)$$

Step 3 the SB computes the hash function *IDsbwj* and concatenates it with α_j:

$$Hsb_j = h\ (IDsbw_j \parallel \alpha_j)$$

Sending 1, the SB forwards a message authentication to the CC, the message includes (Hsb_j; $Msbw_j$; $IDsb_j$).

Calculation 2

Step 1 after receiving the message authentication, the CC decrypts $Msbw_j$ to get *IDsbwj*:

$$IDsbw_j = D(Msbw_j, p_j)$$

Step 2 the CC extracts α_j from $IDsbw_j$:

$$\alpha_j = IDsbw_j \oplus IDsb_j$$

Step 3 to confirm the value of α_j, the CC calculates the $OHsb_j$ of the *IDsbwj* and concatenates it with α_j:

$$OHsb_j = h\ (IDsbw_j \parallel \alpha_j)$$

If $OHsb_j$ = *Hsbj*, then the resulting value of α_j is right. Else,
Failure Sending 1, the CC forwards a message of failure to the SB.

Step 4 the CC creates a random number $\beta_j \leftarrow Z^*$ and then calculates the replay control ID shadow $IDcrw_j$:

$$IDcrw_j = IDsb_j \oplus \beta_j$$

Step 5 the CC computes $Mcrw_j$ by encrypting $IDcrw_j$ using p_j as the unknown key:

$$Mcrw_j = E(IDcrw_j, p_j)$$

Step 6 the CC calculates the hash value of $IDcrw_j$ and concatenates it with α_j and β_j:

$$Hcr_j = h\ (IDcrw_j \parallel \alpha_j \parallel \beta_j)$$

Sending 2, the CC forwards a message of authentication to the SB, which involves (*Hcrj;* $Mcrw_j$).

Calculation 3

Step 1 after getting the message of authentication from the CC, the SB decrypts $Mcrw_j$ to obtain $IDcrw_j$:

$$IDcrw_j = D(Mcrw_j, p_j)$$

Step 2 the SB extracts β_j from $IDcrw_j$ through:

$$\beta_j = IDsb_j \oplus IDcrw_j$$

Step 3 to confirm the value of β_j, the SB calculates the hash value of $IDcrw_j$ and concatenates it with α_j and β_j:

$$OHcr_j = h\left(IDcrw_j \parallel \alpha_j \parallel \beta_j\right)$$

If $OHcr_j$ = $Hcrj$, then the resulting value of β_j is corrected. Else,
Failure Sending 2, the SB sends a message of failure to the CC.

4.3. Key Session Phase

As soon as the authentication phase is successfully passed, a mutual symmetric key K_j is generated to give the channel of communication its security. K_j can be computed as:

$$K_j = h\left(\alpha_j \parallel \beta_j \parallel IDsb_j\right)$$

The key K_j is used in data privacy of the existing session. After the ending of this session, the value of the secret parameters α_j and β_j are deleted from the system. The key session from the SB to the CC is shown in Figure 6.

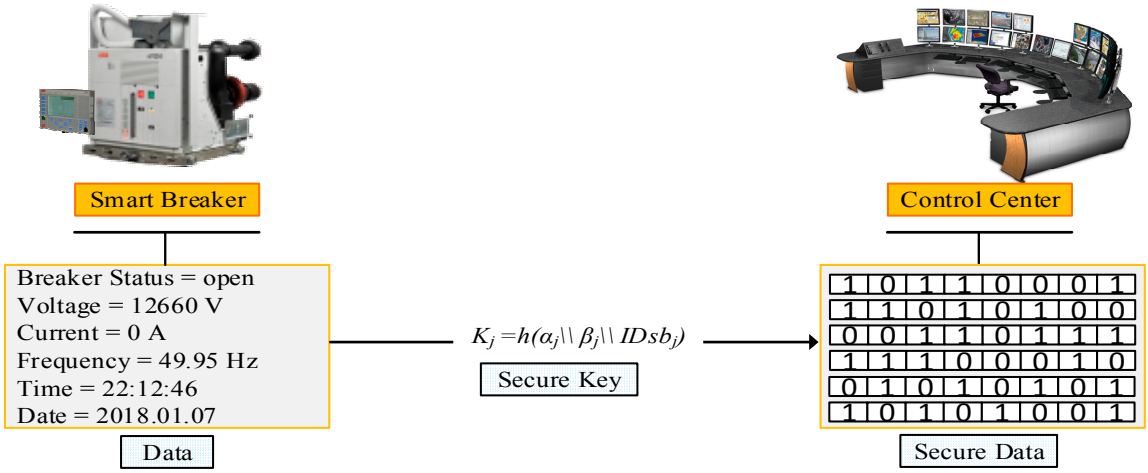

Figure 6. Key Session from the SB to the CC.

5. Results and System Performance

In this section, a comparison in the performance of the proposed scheme with References [18,31,32] is discussed. The initialization phase will only be implemented one time. Therefore, the required comparison will be in the authentication phase of performance. Where, the standard costs regarding to authentication which are computational and communication cost as shown in Tables 2 and 3, are considered. Such these costs are well known and common in most authentication researches.

The experiments are conducted on a 2.5 GHz Intel i3-M380 processor, with a Windows 7 operating system of 64-bits, and 4 GB RAM (Lenovo PC HK limited, Hong Kong, China). Where, MATLAB R2014a is used to implement our experiments. While, Java class is used to implement the cryptosystem.

In Table 2, a comparison is made among References [18,31,32] with the proposed scheme in terms of their computational costs. The total computational cost of our proposed scheme for the authentication phase is 14.1 milliseconds, which is deemed the lowest. The other mentioned papers have respective computational costs of 23.13, 34.65 and 34.65 milliseconds. In addition, another comparison of the communication costs, as shown in Table 3, is the total communication cost, which is

510 bits for the proposed scheme and 800, 1040 and 1040 bits for the other schemes respectively. In our proposed scheme, three considerations are involved with the key requirements of authentication phase (*Hsbj; Msbwj; IDsbj*). The full length of the communication requirement is $3 \times 128 = 354$ bits. In the upcoming requirement, two considerations are elated, which are $2 \times 128 = 256$ bits. Thus, we proved that the suggested scheme is the best and overcomes the others, that is References [18,31,32] in terms of computational cost and communication costs.

Table 2. The comparison in computational cost (msec).

Scheme	SE to RE	RE to SE	Total
Proposed	8.10	6.40	14.10
[31]	-	-	23.13
[18]	-	-	34.65
[32]	-	-	34.65

Table 3. The comparison in communication cost (bit).

Scheme	Sending 1	Sending 2	Sending 3	Total
Proposed	354	256	-	510
[31]	464	336	-	800
[18]	384	512	144	1040
[32]	384	512	144	1040

6. Security Analysis

This part primarily offers a discussion of the proposed scheme, which can meet all of the necessary safety needs between the SB and the CC. The subsequent condition is identical to the initial one.

As mentioned earlier, the components of data security include data integrity, privacy and confidentiality. Considering the broadcast nature of wireless and internet communications, the SG data may be interfered with and substituted by the adversary; such a system is considered quite risky in the event of a system outage. Therefore, the present model decrypts the data by utilizing a one-time session key. This unique random key is generated after the authentication stage and is altered periodically. This method of data encryption (one-time key-based) may meet all three data security properties, whereby any data alteration or adversary's replay attempt may simply be identified using a tag that is highly resistant to falsification.

6.1. Preventing the Replay Attack

The process of conducting a replay attack requires the attacker to tap into the authentication message that is normally transferred to the CC from the SB. After the SB-CC interchange, the attacker's attempts to have the same message replayed surpasses the system's verification process. In the present authentication procedure, it is only practical to transfer the secret parameter in the authentication message to the CC from the SB only once. Therefore, in case the attacker attempts to have the same request message intercepted or resent, the CC is then able to easily identify it by using the ID shadow's hash function of the SB's Hsb_j. In the same method, if an attacker tries to copy an authentication message and resends it to the SS, then this action can be easily detected by the CC. For this approach, the suggested unidentified authentication protocol may hold against the replay attacks.

6.2. Resistance to Forgery Attacks

Interception and modification of existing legal data for the SB to pass the CC's authentication procedure may be targeted by the attacker as well. In such a situation, the attacker is expected to build a useable authentication message using a useable secret parameter to meet the SGMA. Therefore, to achieve this, it is important for the attacker to get rid of the ID shadow's function of the SB and to

understand the unknown parameter (p_j). The attacker finds it quite hard to determine this parameter (secret parameter p_j) as its insertion into the SB is done in its offline mode, while the α_j value is random and is utilized only one time. Contrary to this, the attacker may disguise attempts as the CC to acquire the benefits. If this happens to be the case, then the attacker is required to create a valid message of authentication and to equally understand the random value (α_j; β_j) and the secret parameter p_j. In doing this, the proposed scheme will be able to offer resistance against forgery attacks.

6.3. Sustaining Mutual Authentication

In the present proposal, the SB is authenticated by the CC via having the random value α_j and the ID shadow's hash function of the SS verified in the message of authentication, where a genuine SB creates a valid message of authentication. Nonetheless, a random value of α_j is considered in the authentication of the SS by the CC, where this value is computed from $IDsbw_j$ ($\alpha_j = IDsbw_j \oplus IDsb_j$). The resulting hash is $OHsb_j = h$ ($IDsbw_j$ || α_j) and is expected to correspond to the ID shadow's hash function of the SB in the message of authentication $OHsb_j = Hsb_j$. On the other hand, the CC's legitimacy can be authenticated by the SB using the random values of β_j and α_j, as well as the hash value $Hcc_j = h$ ($IDccw_c$ || α_j || β_j), which are expected to correspond to the resulting hash value of $OHcc_j$. By doing this, the proposed scheme suits the mutual authentication property.

6.4. Supporting Anonymity Authentication

For the proposed design, both the random values (α_j; β_j) and the secure number p_j may offer solution issues like intractability and anonymity, nonetheless, the idea that the secure number p is integrated into the SB while being in offline status. For this study, this concept is considered during the ID shadow's encryption and decryption. The ID shadow is used in hiding the one-time random value (α_j; β_j), whereby a secret parameter p_j is considered for encrypting it. Authentication is achieved as a courtesy of this random value; therefore, the scheme in the present study promotes anonymous authentication. Nonetheless, while executing the process of anonymous authentication in the present study, the parameters in the authentication message are not allowed to be sent at one time. For the purposes of acquiring PAE (Privacy Against Eavesdroppers), it is imperative to employ an effective approach such as the proposed scheme.

7. Conclusions

The SG is likely to be the most reasonable key for forthcoming energy problems. With proper security, the SG can play a vital role in solving these energy management issues. The security and privacy of communication between the SB and the CC are important to prevent partial system outages that may lead to large-scale blackouts, damage of the electrical equipment or serious consequences in the power grid. Pursuing higher security by sacrificing communication and computation costs is unfair to the utility. The main contributions of this paper are highlighted as follows: Firstly, the authentication between the CC and the SBs in SG is introduced in this paper, which is presently missing in the literature of this field. Second, in the field of performance, a lightweight authentication scheme for SG communication using the crypto hash function with masked identity, as well as symmetric cryptography for various exchanges, is proposed. Third, upon its comparison with other schemes, the proposed scheme is the best regarding the computation and communication costs. For future work, the proposed scheme can be injected to the REF542*plus* controller using manufacturing software such as CAN Open digital fieldbus, which can be applied by the help of ABB switchgear companies. Thus, the suggested scheme can be appropriate for real-time SG applications. Therefore, the importance of this article is that the proposed scheme can provide a suitable industry-security level with low computation and communication costs.

Author Contributions: The work was leaded by Hai Jin. The modeling process with the security analysis has been performed and discussed by I.H.A., Z.A.H., Z.A.A., and F.M.F.F. Simulation and analysis of the results have been performed by I.T.A.

Funding: This work is supported by the National Basic Research Program of China (973 Program) under grant No.2014CB340600.

Acknowledgments: The authors would like to thank the staff of the School of Computer Science & Technology/Huazhong University of Science & Technology, Wuhan, China and the people who assisted in this work.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Arafat, Y.; Tjernberg, L.B.; Gustafsson, P.-A. Remote switching of multiple smart meters and steps to check the effect on the grid's power quality. In Proceedings of the 2014 IEEE PES T&D Conference and Exposition, Chicago, IL, USA, 14–17 April 2014; pp. 1–5.
2. Baki, A. Continuous monitoring of smart grid devices through multi protocol label switching. *IEEE Trans. Smart Grid* **2014**, *5*, 1210–1215. [CrossRef]
3. Liu, H.; Chen, Y.; Chuah, M.C.; Yang, J.; Poor, V. Enabling Self-healing Smart Grid Through Jamming Resilient Local Controller Switching. *IEEE Trans. Dependable Secur. Comput.* **2015**, *14*, 377–391. [CrossRef]
4. Torres, S.P.; Castro, C.A. Practical heuristic approach to solve the Optimal Transmission Switching problem for Smart Grids. In Proceedings of the 2014 IEEE PES Transmission & Distribution Conference and Exposition-Latin America (PES T&D-LA), Medellin, Colombia, 10–13 September 2014; pp. 1–6.
5. Pfitscher, L.L.; Bernardon, D.P.; Canha, L.N.; Montagner, V.F.; Comasseto, L.; Ramos, M.S. Studies on parallelism of feeders for automatic reconfiguration of distribution networks. In Proceedings of the 2012 47th International Universities Power Engineering Conference (UPEC), London, UK, 4–7 September 2012; pp. 1–5.
6. Aziz, I.T.; Jin, H.; Abdulqadder, I.H.; Imran, R.M.; Flaih, F.M. Enhanced PSO for network reconfiguration under different fault locations in smart grids. In Proceedings of the 2017 International Conference on Smart Technologies for Smart Nation (SmartTechCon), Bangalore, India, 17–19 August 2017; pp. 1250–1254.
7. Bernardon, D.; Garcia, V.; Sperandio, M.; Russi, J.; Daza, E.; Comassetto, L. Smart Grid concepts applied to distribution networks operation. In Proceedings of the 2010 45th International Universities Power Engineering Conference (UPEC), Cardiff, UK, 31 August–3 September 2010; pp. 1–6.
8. Boteza, A.; Tirnovan, R.; Boiciuc, I.; Stefanescu, S.; Rafiroiu, D. Automatic transfer switch using IEC 61850 protocol in smart grids. In Proceedings of the 2014 International Conference and Exposition on Electrical and Power Engineering (EPE), Iasi, Romania, 16–18 October 2014; pp. 1071–1076.
9. Siirto, O.K.; Safdarian, A.; Lehtonen, M.; Fotuhi-Firuzabad, M. Optimal distribution network automation considering earth fault events. *IEEE Trans. Smart Grid* **2015**, *6*, 1010–1018. [CrossRef]
10. Farhangi, H. The path of the smart grid. *IEEE Power Energy Mag.* **2010**, *8*, 18–28. [CrossRef]
11. Zhang, P.; Li, F.; Bhatt, N. Next-generation monitoring, analysis, and control for the future smart control center. *IEEE Trans. Smart Grid* **2010**, *1*, 186–192. [CrossRef]
12. Alizadeh, M.; Li, X.; Wang, Z.; Scaglione, A.; Melton, R. Demand-side management in the smart grid: Information processing for the power switch. *IEEE Signal Process. Mag.* **2012**, *29*, 55–67. [CrossRef]
13. Hur, J.B.; Koo, D.Y.; Shin, Y.J. Privacy-Preserving Smart Metering with Authentication in a Smart Grid. *Appl. Sci.* **2015**, *5*, 1503–1527. [CrossRef]
14. De Araújo, P.R.C.; Filho, R.H.; Rodrigues, J.J.P.C.; Oliveira, J.P.C.M.; Braga, S.A. Infrastructure for Integration of Legacy Electrical Equipment into a Smart-Grid Using Wireless Sensor Networks. *Sensors* **2018**, *18*, 1312. [CrossRef] [PubMed]
15. Karbouj, H.; Maity, S. On using TCBR against cyber switching attacks on smart grids. In Proceedings of the 2016 IEEE Innovative Smart Grid Technologies-Asia (ISGT-Asia), Melbourne, Australia, 28 November–1 December 2016; pp. 665–669.
16. Doh, I.; Lim, J.; Chae, K. Secure Authentication for Structured Smart Grid System. In Proceedings of the 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Blumenau, Brazil, 8–10 July 2015; pp. 200–204.

17. Koo, D.; Shin, Y.; Hur, J. Privacy-Preserving Aggregation and Authentication of Multi-Source Smart Meters in a Smart Grid System. *Appl. Sci.* **2017**, *7*, 1007. [CrossRef]
18. Fouda, M.M.; Fadlullah, Z.M.; Kato, N.; Lu, R.; Shen, X.S. A lightweight message authentication scheme for smart grid communications. *IEEE Trans. Smart Grid* **2011**, *2*, 675–685. [CrossRef]
19. Li, H.; Lin, X.; Yang, H.; Liang, X.; Lu, R.; Shen, X. EPPDR: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 2053–2064. [CrossRef]
20. Nicanfar, H.; Jokar, P.; Beznosov, K.; Leung, V.C. Efficient authentication and key management mechanisms for smart grid communications. *IEEE Syst. J.* **2014**, *8*, 629–640. [CrossRef]
21. Nicanfar, H.; Jokar, P.; Leung, V.C. Smart grid authentication and key management for unicast and multicast communications. In Proceedings of the 2011 IEEE PES Innovative Smart Grid Technologies Asia (ISGT), Perth, Australia, 13–16 November 2011; pp. 1–8.
22. Law, Y.W.; Palaniswami, M.; Kounga, G.; Lo, A. WAKE: Key management scheme for wide-area measurement systems in smart grid. *IEEE Commun. Mag.* **2013**, *51*, 34–41. [CrossRef]
23. Fouda, M.M.; Fadlullah, Z.M.; Kato, N.; Lu, R.; Shen, X. Towards a light-weight message authentication mechanism tailored for smart grid communications. In Proceedings of the 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Shanghai, China, 10–15 April 2011; pp. 1018–1023.
24. Li, H.; Lu, R.; Zhou, L.; Yang, B.; Shen, X. An efficient merkle-tree-based authentication scheme for smart grid. *IEEE Syst. J.* **2014**, *8*, 655–663. [CrossRef]
25. Lu, R.; Lin, X.; Shi, Z.; Shen, X. EATH: An efficient aggregate authentication protocol for smart grid communications. In Proceedings of the 2013 IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, China, 7–10 April 2013; pp. 1819–1824.
26. Wen, M.; Lei, J.; Bi, Z.; Li, J. EAPA: An efficient authentication protocol against pollution attack for smart grid. *Peer-to-Peer Netw. Appl.* **2015**, *8*, 1082. [CrossRef]
27. Singelée, D.; Seys, S.; Batina, L.; Verbauwhede, I. The communication and computation cost of wireless security. In Proceedings of the Fourth ACM Conference on Wireless Network Security, Hamburg, Germany, 14–17 June 2011; pp. 1–4.
28. Uribe-Pérez, N.; Angulo, I.; de la Vega, D.; Arzuaga, T.; Fernández, I.; Arrinda, A. Smart Grid Applications for a Practical Implementation of IP over Narrowband Power Line Communications. *Energies* **2017**, *10*, 1782. [CrossRef]
29. Badran, O.; Mekhilef, S.; Mokhlis, H.; Dahalan, W. Optimal reconfiguration of distribution system connected with distributed generations: A review of different methodologies. *Renew. Sustain. Energy Rev.* **2017**, *73*, 854–867. [CrossRef]
30. Huang, X.; Yuan, Q.; Li, C.; Yuan, Q.; Dong, L. Research on the network reconfiguration after distribution network fault. In Proceedings of the 2014 China International Conference on Electricity Distribution (CICED), Shenzhen, China, 23–26 September 2014; pp. 1–7.
31. Mahmood, K.; Chaudhry, S.A.; Naqvi, H.; Shon, T.; Ahmad, H.F. A lightweight message authentication scheme for Smart Grid communications in power sector. *Comput. Electr. Eng.* **2016**, *52*, 114–124. [CrossRef]
32. Sule, R.; Katti, R.S.; Kavasseri, R.G. A variable length fast message authentication code for secure communication in smart grids. In Proceedings of the 2012 IEEE Power and Energy Society General Meeting, San Diego, CA, USA, 22–26 July 2012; pp. 1–6.