A Novel Anonymous Authentication and Key Agreement Scheme for Smart Grid

Hamza Hammami[1], Mohammad S. Obaidat[2,3,4,*] and Sadok Ben Yahia[5,6]

[1] *University of Tunis El Manar, Faculty of Sciences of Tunis, LIPAH-LR11ES14, 2092 Tunis, Tunisia*

[2] *College of Computing & Informatics, University of Sharjah, U.A.E.*

[3] *King Abdullah II School of Information Technology, Universality of Jordan, Jordan*

[4] *University of Science and Technology Beijing, China*

[5] *University of Tunis El Manar, Faculty of Sciences of Tunis, LIPAH-LR11ES14, 2092 Tunis, Tunisia*

[6] *Tallinn University of Technology, Department of Software Science, Akadeemia tee 15a, Tallinn 12618, Estonia*

Keywords: Smart Grid, Consumption, Attacks, Security, Costs.

Abstract: The smart grid is a new technology that is revolutionizing the services and uses of the electric power sector. It is a solution that integrates the new information and the communication technology into its operation in order to modernize the electrical system and optimize the transport of electrical energy from production points to distribution ones. Indeed, the smart grid represents a future solution mainly based on two participants: the distribution and calculation center and the smart meter installed at the end customer. This smart meter sends the information carrying the energy consumption data of its customer to the distribution and calculation center. The latter processes the received consumption data and returns the result of its calculation to the end customer in the form of an invoice containing the amount of its consumption. This communication can be susceptible to several types of attacks due to its sending in a network, which is not always secure. These types of attacks can modify data and can subsequently generate a falsified consumption invoice. Our work therefore focuses on this issue. It particularly concerns the development of a solution that has the capacity to stem attacks targeting the smart grid with a lower computation and communication costs than its competitors.

1 INTRODUCTION

The smart grid represents an electrical network that has used the new information and the communication technology to modernize this network and make it intelligent (Raza et al. 2019). This is a recent technology that responds to the current trend in the field of electrical energy (Bagdadee et al. 2019). This technology takes the form of the power distribution server and the smart meter. The latter represents the first brick that plays an important role in the transformation of the conventional electrical network into an intelligent electrical network (the smart grid) (Wang et al. 2018). It consists of transmitting the communication data from the end customer to the energy distribution server and receiving the invoice for its counted electricity consumption by the energy distribution server (Nguyen et al. 2019).

We cannot deny that the smart grid solution offers a wide range of advantages to its customers by enabling them to follow its consumption in real time, not to request the reading of its meter, to subscribe an offer adapted to its consumption and to better control its electricity consumption (Avancini et al. 2019). However, this advanced technology has highlighted a fundamental security problem due to the migration of data exchanged between the energy distribution server and its smart meter through a network which is not always secure, hence making these data vulnerable to multiple types of attacks that can cause real damage (Romdhane et al. 2019). This security problem is therefore a major obstacle to the expansion of this solution, which highlights the implementation of solutions to contain these types of attacks in order to ensure the security of the smart grid technology (Romdhane et al. 2019). Our proposed solution can face attacks targeting connection parameters and consumption data exchanged between the energy distribution server and its smart meter and can respond

[*] Fellow of IEEE

Hammami, H., Obaidat, M. and Ben Yahia, S.
A Novel Anonymous Authentication and Key Agreement Scheme for Smart Grid.
DOI: 10.5220/0009824203570362
In *Proceedings of the 17th International Joint Conference on e-Business and Telecommunications (ICETE 2020) - SECRYPT*, pages 357-362
ISBN: 978-989-758-446-6

comprehensively and efficiently to all security needs with lower communication and calculation costs.

The paper is organized as follows: In section 2, we describe the work that has appeared recently to ensure the security of the smart grid technology. Then, in section 3, we detail our solution with its different steps. After that, in section 4, we analyze the performance and reliability of the solution we have proposed with other competing solutions. Finally, this paper ends with a general conclusion and some perspectives.

2 RELATED WORK

The problem of the security of the smart grid technology has prompted several researchers to take an interest in this delicate subject. For this, several approaches have been devoted to the search for solutions to face this problem. For example, in (Garg et al. 2019), the authors suggested an authentication scheme, which took advantage of the opportunities offered by elliptic curve cryptography, the one-way hash functions and the benefits provided by the Menezes-Qu-Vanstone key exchange solution. Indeed, this authentication scheme designated a lightweight solution ensuring the security and anonymity of communications in the smart grid with lower communication and calculation costs. However, this solution was vulnerable to the insider attack and the password guessing attacks.

In addition, the authors in (P. Kumar et al. 2019) put forward an authentication solution with a key agreement based on hybrid cryptography. This solution provided bidirectional authentication between a remote smart meter and the server in order to obtain a session key agreement to ensure the security of the data communications exchanged. In addition, it checked anonymity and the dynamic session key. However, it did not provide security against the insider attack and the password guessing attacks.

Moreover, the authors in (Tsai et al. 2015) used an identity-based signature scheme, as well as another identity-based encryption scheme, in order to achieve a new anonymous key distribution scheme ensuring the technology security of the smart grid. In the suggested solution, a smart meter could anonymously access the services offered by service providers using a private key and without the use of a trusted anchor during authentication. However, this solution did not verify perfect forward secrecy and did not provide security against the man-in-the-middle and session-key-discloser attacks.

Furthermore, the authors in (Odelu et al. 2016) proposed a security scheme ensuring secure authentication in the smart grid. The authentication scheme reinforced the security of the solution propounded in (Tsai et al. 2015), but this authentication scheme was vulnerable to the man-in-the-middle attacks.

Besides, the authors in (He et al. 2016) suggested an anonymous authentication scheme ensuring the security of the smart grid. This proposed scheme took advantage of the opportunities offered by elliptical curves to provide the anonymity of the smart meter and authentication between the power distribution server and its smart meters without the help of any trusted anchor. However, this solution did not verify anonymity and did not provide security against insider and password guessing attacks.

3 PROPOSED SOLUTION

In our work, and in order to offer a more satisfactory level of security in the intelligent electrical network, more particularly in the security of all communications exchanged between the smart meter and the data center, we have developed a solution of strong and light authentication allowing mixing several authentication parameters, in order to properly authenticate a smart meter with its energy distribution server, to protect and verify that the energy consumption data sent by the smart meter are correct and come from a legitimate smart meter. In fact, in our authentication solution we take advantage of the opportunities offered by cryptography based on elliptic curves in combination with light cryptographic functions, *i.e.* hash functions and concatenation functions, to use them in the account of our security solution. Indeed, our authentication solution is presented in three phases: *(i)* setup, *(ii)* identification and *(iii)* authentication and key agreement.

3.1 Setup Phase

During this first step, the energy distribution server performs a process of generating a set of parameters. These parameters enable the other stages to execute safely. The details of this generation process are as follow:

- At the start, the energy distribution server randomly generates two large prime integers a and b. Subsequently, it calculates $z = (a - 1)(b - 1)$ and $r = a \cdot b$. Then, it randomly generates two integers x and y so that $PGCD(x, z) = 1$ and $(y \cdot x) \bmod z = 1$.
- After completing the generation, the energy distribution server chooses a hash function $h_1(.)$: {

$0, 1 \}^* \rightarrow \{0, 1\}^k$ where *k* denotes the size of the hashed chain and subsequently publishes its public key *(x, r)* and keeps its private key *y* secret.

3.2 Identification Phase

Once the setup step is complete, the energy distribution server publishes its parameters. In this step, any smart meter can easily register with its server. Just enter its login *(pseudo)* and its password *(passwd)*. Subsequently, it arbitrarily generates a number λ and calculates $\beta = h_1(passwd \parallel \lambda)$. After completing this calculation, it sends $<pseudo\ ;\ \beta >$ to the power distribution server.

As soon as the energy distribution server receives $<pseudo\ ;\ \beta >$, it will perform the following calculation: $E= h_1(pseudo \parallel y)$; $K= h_1(E \parallel \beta \parallel pseudo)$; $N= E \oplus h_1(\beta \parallel pseudo)$. Once it has completed the calculation, the energy distribution server saves these results and then sends $<N\ ;\ K>$ to the smart meter.

3.3 Authentication and Key Agreement Phase

In this phase, the smart meter provides its login *(pseudo')* and its password *(passwd')*. Subsequently, it calculates $\beta' = h_1(passwd' \parallel \lambda)$ and extracts $E' = N \oplus h_1(\beta' \parallel pseudo')$. Then it calculates $K' = h_1(E' \parallel \beta' \parallel pseudo')$. As soon as it completes the calculation, it checks result *K'* found with previously recorded *K*. If the two results are equal, this means that *pseudo'= pseudo* and *passwd' = passwd*. Thereafter, it performs the following calculations $\mu = h_1(E' \parallel h_1(\beta \parallel pseudo') \parallel S \parallel \varepsilon\ )$; $\nu = (pseudo' \parallel \mu \parallel \varepsilon)^x \ mod\ r$. We note here that *S* is a current timestamp and ε denotes an arbitrarily generated number. As soon as the smart meter completes the calculation, it sends $< N\ ;\ S\ ;\ \nu >$ to the power distribution server.

Upon the receipt of $< N\ ;\ S\ ;\ \nu >$ by the energy distribution server, this latter will first check the time stamp $(S - S^*) <= \Delta T$, where ΔT represents the maximum transmission delay and S^* is the timestamp during which the connection message is received by the power distribution server. If the timestamp is verified to be correct, the energy distribution server will perform the following calculations: $v^y\ mod\ r$ in order to get $(pseudo' \parallel \mu' \parallel \varepsilon'\ )$; $E^* = h_1(pseudo' \parallel y)$ and then extract $h_1(passwd' \parallel pseudo') = N \oplus E^*$. Therefore, it calculates $\mu^* = h_1(E^* \parallel h_1(\beta' \parallel pseudo') \parallel S \parallel \varepsilon)$. Once the distribution server finishes the calculation, it then checks whether $\mu^* = \mu'$. If it is not, the power distribution server rejects the session. Otherwise, this means that it is a legitimate smart meter. In this case, the energy distribution server will perform the following calculation: $U= h_1(E' \parallel D)$; $W= D \oplus \varepsilon'$. After completing the calculation, the energy distribution server sends $<U\ ;W\ ;S''>$ to the smart meter. We note here that *S"* denotes a timestamp and *D* represents an arbitrarily generated number.

As soon as the smart meter receives $<U\ ;W\ ;S''>$, it will first check the timestamp $(S''\text{-}\ S^*)<= \Delta T$. If the timestamp is verified to be correct, in this case the smart meter will calculate $D' = \varepsilon \oplus W$; $U' = h_1(D' \parallel E^*)$ and will then check whether $U = U'$. If so, this means that the authentication step is completed successfully. In this case, the smart meter and the energy distribution server agree on a shared *Key Agreement* = $h_1(\varepsilon \parallel E' \parallel D') = h_1(\varepsilon' \parallel E^* \parallel D)$. This key is intended for encryption and decryption of all data exchanged between the smart meter and the energy distribution server.

4 PERFORMANCE ANALYSIS

In this section, we analyze the security of our solution while showing its performance and robustness during resistance against various attacks targeting the smart grid. Then, we present the reliability and efficiency of our solution compared to the solutions presented in the literature in terms of cost of communication and computation.

4.1 Security Analysis

In this subsection, we analyze attacks targeting the smart grid, and try to show the advantages and reliability of our solution concerning the fight against these types of attacks.

4.1.1 Replay Attack

This is an attack in which a malicious participant intercepts and then replays a valid data transmission over a network (Das et al. 2019). Due to the validity of the original data, which generally comes from an authorized participant, network security solutions treat this type of attack as if it were a legitimate data transmission. We remedy this type of attacks in our solution by using randomly generated numbers (ε, D) and time stamps $(S, S\ ^*, S'')$,which are different for each communication. In this case, our solution will detect any replay of a data transmission, so a malicious participant has no way to execute this type of attacks.

4.1.2 Perfect Forward Secrecy

This is a key agreement property which ensures that session keys cannot be compromised if the private key of the power distribution server is compromised. In our security scheme, we generate a unique session key *Key Agreement* = $h_1(\varepsilon \parallel E' \parallel D') = h_1(\varepsilon' \parallel E^* \parallel D)$ for each communication session between the smart meter and the energy distribution server. Here, the compromise of a single session key will only affect the data exchanged during the session encrypted by the key in question.

4.1.3 Ensuring Smart Meter Anonymity

This is a property that allows a smart meter to prove its identity without revealing any sensitive data that can identify it (McDonald et al. 2019). We verify this property in our scheme by protecting the login *(pseudo)* of the smart meter with an irreversible hash function $h_1(.)$ and encapsulating it in the following parameters: $E = h_1(pseudo \parallel y)$; $N = E \oplus h1(\beta \parallel pseudo)$ and $K = h_1(E \parallel \beta \parallel pseudo)$. In this way, a malicious participant has no way of having y and β in order to obtain information about the login *(pseudo)* of the smart meter.

4.1.4 Insider Attack

This is a malicious attack that perpetrates on a network by a participant with authorized access to the system (Gusrialdi et al. 2019). In our solution, we fight against this type of attacks through the calculation of $\beta = h_1(passwd \parallel \lambda)$. We note here that we apply the hash function $h_1()$ on the concatenation of the smart meter password *(passwd)* with a randomly generated number λ. In this case, a malicious participant has no way to calculate the reciprocal function $h_1()^{-1}$ to successfully apply this type of attacks.

4.1.5 Man in the Middle

This is an attack by which a malicious participant gains access to communications between the smart meter and the power distribution server, without either of these parties being aware of it (Fritz et al. 2019). We contain this type of attack in our security scheme by using randomly generated numbers ε and D and by the secret key y of the energy distribution server. In this case a malicious participant will not be able to generate whatsoever falsified communications when sending $< \nu = (pseudo' \parallel \mu \parallel \varepsilon)^x \bmod r$; $N = E \oplus h_1(\beta \parallel pseudo); S >$ to the energy distribution server during the identification phase or when sending $< U = h_1(E' \parallel D)$; $W = D \oplus \varepsilon' >$ during the authentication phase.

4.1.6 Password Guessing Attack

In this type of attacks a malicious participant seeks to find a way to recover the password *(passwd)* of the smart meter when sending parameters $< N ; S ; \nu >$ and $< U ; W ; S" >$ during the identification and authentication phases. In our scheme, we fight against this type of attacks by using the following parameters: $\beta = h_1(passwd \parallel \lambda)$; $E = h_1(pseudo \parallel y)$; $K = h_1(E \parallel \beta \parallel pseudo)$. In this case, a malicious participant has no way to find *(passwd)* because he should have both $(\lambda ; pseudo ; y)$ to be able to calculate the hash function h_1.

4.1.7 Session Key Discloser Attack

In our scheme, we remedy this type of attacks by using *Key Agreement* = $h_1(\varepsilon \parallel E' \parallel D') = h_1(\varepsilon' \parallel E^* \parallel D)$ generated to ensure the security of all exchanged communications between the smart meter and the power distribution server. We note that this key agreement is variable for each session; thanks to the arbitrarily generated numbers. This key agreement is therefore robust because it is generated from *(pseudo)* where it is transmitted encrypted in the network $\nu = (pseudo \parallel \mu \parallel \varepsilon)^x \bmod r$. Thus, a malicious participant has no way to find the key agreement because he must have both the decryption key y, the *pseudo* of the smart meter as well as the randomly generated numbers.

Table 1 illustrates the security analysis of our approach with other approaches presented in the literature.

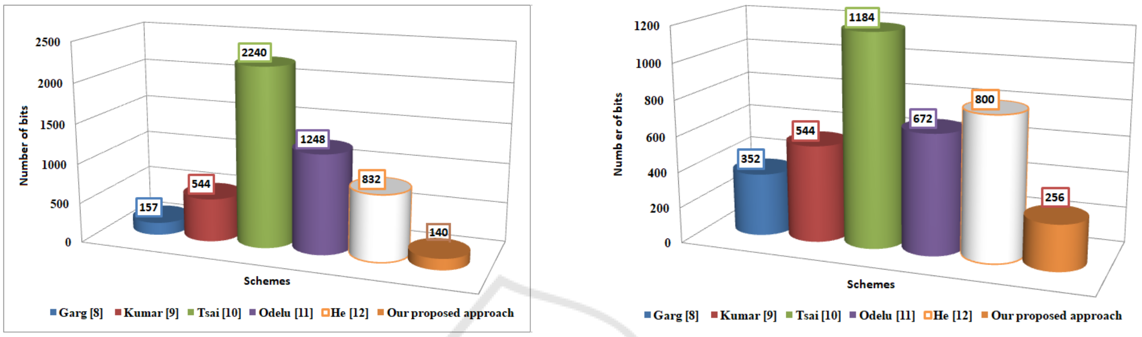
4.2 Performance Evaluation of Our Proposed Scheme

In this last sub-section, we carry out various experiments in order to illustrate the performance and effectiveness of our solution compared to other approaches in the same context as ours in terms of communication and computation costs. In what follows, we describe the details of the experiments that we perform as well as their results.

After completing our experiments, we obtain the following two figures Figure 1.a and Figure 1.b. These latter present the number of bits used by our scheme and the other schemes presented in the literature while sending and receiving data. From these two figures, we can say that our approach surpasses all its competing approaches in terms of cost and number of bits used during communications (sent / received).

Table 1: Security analysis.

Security Properties	**[8]**	**[9]**	**[10]**	**[11]**	**[12]**	**Ours**
Secure against replay attack	✓	✓	✓	✓	✓	✓
Ensures perfect forward secrecy	✓	✓	×	✓	✓	✓
Ensures anonymity of smart meter	✓	✓	✓	✓	×	✓
Secure against insider attack	×	×	✓	✓	×	✓
Secure against man-in-the-middle attack	✓	✓	×	×	✓	✓
Secure against password guessing attack	×	×	✓	✓	×	✓
Secure against session key discloser attack	✓	✓	×	✓	✓	✓



(a) The number of bits used during communications sent

(b) The number of bits used during communications received

Figure 1: The number of bits used during communications (sent / received) between the smart meter and the power distribution server.

Table 2 shows the calculation cost used by our solution compared with the other competing solutions presented in the literature. We note that in Table 2, *(Tm)* indicates the execution time used to ensure the multiplication operations, *(Ted)* denotes the execution time used to ensure encryption and decryption steps, *(Th)* designates the execution time used for the hash function, *(Tbp)* represents the execution time used for the bilinear pairing funtion, *(Tadd)* denotes the execution time used to ensure the the addition operations and *(Texp)* indicates the execution time used to ensure the exponentiation operations. This table clearly demonstrates that our security scheme is better than its competitors in terms of cost of calculation.

Table 2: Total computational cost of our solution compared to the solutions presented in the literature.

Schemes	**Total Computational Cost**
[8]	4Tm + 8Th
[9]	6Tm+ 4Ted + 4Tmac + 9Th
[10]	7Tm + 2Tadd + 2Tbp + 2Texp + 10Th
[11]	5Tm + 6Tadd + 2Tbp + 2Texp +12Th
[12]	10Tm + 3Tadd + 11Th
Ours	2Texp + 8Th

In this last section, we can conclude that our proposed security scheme outperforms all of its competitors in terms of communication and computation costs and can be easily checked against all the different attacks targeting the smart grid.

5 CONCLUSION

In this paper, we have devised an approach with the capacity to ensure the security of the smart grid technology against any attack aimed at their deployment. In fact, by the presentation of the different experimental results, we can say that the solution we have proposed surpasses all its competing solutions in terms of fight against the different attack scenarios presented previously and in terms of computation and communication costs. This is due to the fact that our solution has resorted to the use of light cryptographic functions in order to ensure a strong security of all the data exchanged between the energy distribution server and the smart meter with a lower cost.

REFERENCES

Raza, N., Akbar, M. Q., Soofi, A. A., & Akbar, S. (2019). Study of smart grid communication network architectures and technologies. Journal of Computer and Communications, 7(3), 19-29.

Bagdadee, A. H., & Zhang, L. (2019). Smart Grid: A Brief Assessment of the Smart Grid Technologies for Modern Power System. Journal of Engineering Technology, 8(1), 122-142.

Wang, Y., Chen, Q., Hong, T., & Kang, C. (2018). Review of smart meter data analytics: Applications, methodologies, and challenges. IEEE Transactions on Smart Grid, 10(3), 3125-3148.

Nguyen, D. H., Tran, H. N., Narikiyo, T., & Kawanishi, M. (2019). A distributed optimization method for optimal energy management in smart grid. In Energy Efficiency in Smart Grids. IntechOpen.

Avancini, D. B., Rodrigues, J. J., Martins, S. G., Rabêlo, R. A., Al-Muhtadi, J., & Solic, P. (2019). Energy meters evolution in smart grids: A review. Journal of cleaner production, 217, 702-715.

Romdhane, R. B., Hammami, H., Hamdi, M., & Kim, T. H. (2019, June). A novel approach for privacy-preserving data aggregation in smart grid. In 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC) (pp. 1060-1066). IEEE.

Romdhane, R. B., Hammami, H., Hamdi, M., & Kim, T. H. (2019, June). At the cross roads of lattice-based and homomorphic encryption to secure data aggregation in smart grid. In 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC) (pp. 1067-1072). IEEE.

Garg, S., Kaur, K., Kaddoum, G., Rodrigues, J. J., & Guizani, M. (2019). Secure and Lightweight Authentication Scheme for Smart Metering Infrastructure in Smart Grid. IEEE Transactions on Industrial Informatics.

P. Kumar, A. Gurtov, M. Sain, A. Martin, and P. H. Ha, “Lightweight Authentication and Key Agreement for Smart Metering in Smart Energy Networks,” IEEE Transactions on Smart Grid, vol. 10, no. 4, pp. 4349–4359, 2019.

Tsai, J. L., & Lo, N. W. (2015). Secure anonymous key distribution scheme for smart grid. IEEE transactions on smart grid, 7(2), 906-914.

Odelu, V., Das, A. K., Wazid, M., & Conti, M. (2016). Provably secure authenticated key agreement scheme for smart grid. IEEE Transactions on Smart Grid, 9(3), 1900-1910.

He, D., Wang, H., Khan, M. K., & Wang, L. (2016). Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography. IET Communications, 10(14), 1795-1802.

Das, A. K., & Zeadally, S. (2019). Data Security in the Smart Grid Environment. In Pathways to a Smarter Power System (pp. 371-395). Academic Press.

McDonald, N., Hill, B. M., Greenstadt, R., & Forte, A. (2019, May). Privacy, anonymity, and perceived risk in open collaboration: A study of service providers. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (pp. 1-12).

Gusrialdi, A., & Qu, Z. (2019). Smart grid security: Attacks and defenses. In Smart grid control (pp. 199-223). Springer, Cham.

Fritz, J. J., Sagisi, J., James, J., St Leger, A., King, K., & Duncan, K. (2019). Simulation of Man in the Middle Attack On Smart Grid Testbed. Proceeding of 2019 IEEE SoutheastCon.