Advances and Applications in Mathematical Sciences
Volume 21, Issue 7, May 2022, Pages 4011-4021

CRYPTANALYSIS AND SUGGESTED IMPROVEMENT OF LIGHT WEIGHT MUTUAL AUTHENTICATION STRATEGY FOR INTERNET OF ELECTRIC THINGS

SAMIULLA ITOO[1], VINOD KUMAR*, AKBER ALI KHAN[1], MUSHEER AHMAD[1] and GAJRAJ SINGH[3]

Department of Applied Sciences and Humanities
Jamia Millia Islamia, New Delhi, India-110025
E-mail: samiullaitoo93@gmail.com
mahmad@jmi.ac.in
cs.akberkhan@gmail.com

Department of Mathematics PGDAV College
University of Delhi, New Delhi, India-110065

Discipline of Statistics, School of Sciences
Indira Gandhi National Open University
New Delhi, India-110068
E-mail: gajrajsingh@ignou.ac.in

Abstract

Authentication protocols for smart devices in the Internet of Things (IoT) requires secure data transmission, data confidentiality, and resource consumption restrictions to prevent smart grid system vulnerabilities. "An elliptic curve cryptography-based authentication protocols for Internet of Electric Things (IoET)" has been proposed by Zhao et al. We examine their protocol and identify security flaws such as an insider attack, a stolen device attack, failure to protect the session key, a lack of login phase, user anonymity, lack of password and clock synchronization problem. Thus, Zhao et al. protocol is unsuitable in a smart grid context. Further, we suggest a possible improvement for Zhao et al. protocol.

2020 Mathematics Subject Classification: Primary 05A15; Secondary 11B68, 34A05.

Keywords: ECC, Authentication, Cryptanalysis, Smart card, IoET.

*Corresponding author; E-mail: vinod.iitkgp13@gmail.com

Received November 13, 2021; Accepted December 14, 2021

1. Introduction

Modern smart grid technology demands electrical grids that are extremely efficient, secured, and trustworthy, capable of data gathering, data interaction, sensor systems, intelligent forecasting, and smart control [1]. Internet of things is a technology that combines smart sensors, automation, smart computers, the internet, and other contemporary devices [2]. To establish the Internet of Electric Things (IoET), smart grid technology is used in the production, distribution, processing, transmission, and consumption of electric power. IoET is often recognized as the forefront of innovation of smart grid (SG) technology since it significantly increases electric grid monitoring, transmission and intelligent processing capabilities [3]. If an attacker can trace data from IoET or shut down the server's communication, the electric networks operation could be affected [4]. In March 2019, a cyber-attack on the "Guri Hydropower Station and power grid control center of Venezuelas National Electric Power Company" disrupted all network communications [5]. An electricity blackout hit Ukraine in 2015, affecting roughly 700,000 households for several hours [6]. For secure communication, the RSA algorithm and TLS are recommended. In end-to-end application models, TLS can be applied. Massive Smart Terminal Gadgets (STGs), mostly including several forms of smart terminals, are featured in the IOET. To meet the power grids criteria for STG security, the communication network structures operational reliability must be improved. Mutual authentication and key agreements methods for devices with increased security and lower computation consumption are necessary to establish for secure IoET and smart electric grids.

1.1 Related Works. In 2011, Wang and Zhou [7] proposed "a key management strategy for the smart grid environment based on the enhanced elliptic curve cryptography algorithm". To make key management simple, the protocol adopted a composite cryptographic system that included symmetric and asymmetric key encryption. Srinivas et al. [8] presented a cloud-based user authentication technique that uses the internet of things to allow wireless devices and user terminals to conduct mutual authentication and establish keys. They stated that the protocol outperforms against the existing protocols in terms of communication and computational resource consumption, and security. In the year 2020, Wang et al. [9] proposed an

ECC-based technique for wireless network communication for session key agreement in portable sensor health monitoring devices. The protocol has a high computational performance and is resistant to well-known attacks. However, there is a lot of improvement in terms of privacy protection and processing performance. Khan et al. [10] suggested a "lightweight key agreement framework for smart grids based on ECC" that have pre distributed keys. In this architecture, each connected device keeps a list of communication devices, containing device IDs and public keys. Further, Zhao et al. [5] suggested "A lightweight authentication protocol for smart grid networks" suggested by Zhao et al. We analyzed the Zhao et al. protocol, which is found to be vulnerable to a variety of security threats.

1.2 Motivation and Contribution. Smart meters that are properly authenticated could address privacy concerns for SG communications. However, such a system would have to assess that are communicably secure. Thus, any authentication system for smart grid communication should be designed in such a way that security risks are prioritized above SG restricted resources, such as minimal storage and processing cost. Therefore, SG communication requires the deployment of a secure authentication system to minimize design flaws and security threats. "A lightweight authentication protocol for smart grid networks" suggested by Zhao et al. We analyzed the Zhao et al. protocol, which is found to be vulnerable to a variety of security threats such as: lack of password information, stolen device attack, guessing identity attack, session key disclosure attack, denial of service (DoS) attacks, fails to maintain mutual authentication, user anonymity, clock synchronization problem, insider attack, lack of login phase.

1.3 Paper organization. The rest of this paper is organized as follows: The preliminary materials used in this paper are discussed in Section 2. In section 3, review of baseline protocol is given. In section 4, design flaws of baseline protocol are given. Suggested improvement for baseline protocol is given in section 5. Finally, we draw a conclusion and future direction.

2. Preliminaries

We define the important mathematical definition and some notations, which are helpful for analyzing and describing, Zhao et al. framework.

Let q be a positive integer, and $E_q(c, d)$ represent an elliptic curve over a finite field F_q. An equation for an elliptic curve over a prime finite field is defined as.

$$y^2 = x^3 + cx + d \bmod q \text{ where } c, d \in F_q$$

and

$$4c^3 + 27d^2 \bmod q \neq 0$$

Where the parameters c and d determine the specific curve.

ECC is a finite group $G(F_q)$ based public key encryption technique constitute of (x, y) and ∞ points on the elliptic curve $E_q(c, d)$ [11].

Addition on ECC If R and S are two points in $G(F_q)$ and $R \neq -S$, then $R + S = N \in G(F_q)$ and N is also a point in elliptic curve. The algebraic calculation is defined as [12]:

Let $R = (x_r, y_r)$, $S = (x_s, y_s)$ then $N = (x_n, y_n)$

where $x_n = (\lambda^2 - x_r - x_q) \bmod q$ and $y_n = (\lambda(x_r, x_s) - y_r)$

$$\lambda = \begin{cases} \dfrac{(y_r - y_s)}{(x_r - x_s)} \bmod q, & \text{if } R \neq S \\ \dfrac{3(x_r^2 + c)}{2y_r} \bmod q, & \text{if } R = S \end{cases}$$

Scaler multiplication every point on elliptic curve is non-singular, so the scaler multiplication based on addition rule define as $n \cdot R$ in $G(F)$ as:

$$R + R + \ldots + R = n \cdot R \text{ where } n \in F_q, R \in G(F)$$

Notation table. The important notation that are used in this paper are shown in Table 1.

3. Review of Baseline Protocol

In this section, we first review the baseline protocol of Zhao et al. [5] and then performs its cryptanalysis.

Table 1. Symbol and their Meaning.

Symbol	Meaning	Symbol	Meaning
ECC	Elliptic curve cryptography	SK_{ij}	Key between i and j
$\mathcal{A}$	Attacker	$E_q(c, d)$	Elliptic curve over finite prime field F_q
G	Additive group	$CAAS$	Cloud assisted server
q	Prime number	SGW	Smart gateway
STD	Smart Terminal Device	$h(\cdot)$	Hash function
$dec(C)SK$	Decryption C with secret key SK	Δt_i	Time span
$enc(M)SK$	Encrypt M with SK	$\|$	Concatenation operation
(q_i, Q_i)	key pairs of device i	p_i and P_i	Identification code of SGW and STD

3.1 Registration phase. SGW and STD are communicating to CAAS via a secure network during registration. The procedure for registering of SGW or STD are discussed below:

Step 1. In the prime field F_q, an SGW or STD selects an integer q_i at random.

Calculates $Q_i = q_i \cdot G$ and $K_{i,s} = q_i \cdot Q_i = q_i \cdot q_s \cdot G$, then utilized to generate Q_i, $K_{i,s} \in E(F_q)$.

Step 2. ID_i, Q_i are sent to CAAS by SGW or STD.

Step 3. CAAS calculates $K_{i,s} = q_s \cdot Q_i$ and encrypts the data ID_i, Q_i, $K_{i,s}$ before storing it in the database.

Table 2. Authorizing SGW to access STD in Zhao et al. protocol.

SGW	*CAAS*
	Select $r_g \in Z_q^*$
	Computes $p_g = r_g \cdot Q_s$
	Computes $p_d = r_g \cdot Q_d$
	Computes $SK_{k,g} = h(q_s, Q_g) = h(K_{g,s})$
	Computes $V_{s,d} = h(t_s \| P_g \| Q_d \cdot q_s \| ID_d)$
	Computes $M_{s,g} = \{V_{s,d} \| P_d \| P_g \| t_s \| ID_d \| ID_g\}$
	Encrypts enc $(M_{s,g})SK_{s,g} = C_{r,g}$
	Sends $(C_{s,g})$
	$\Leftarrow$ = ...

3.2. Authorized access phase. The STDs status data or control data is received in real time by CAAS to allows an SGW to access the STD, as demonstrated in Table 2, bellow:

3.3 Authentication phase.

SGW	*STD*
Decrypts $Dec(C'_{s,g})SK_{s,g} = M'_{s,g}$	
Gets t'_s, ID'_g	
Checks $\| t_g - t'_s \| \leq \Delta t$	
Verifies $ID'_g = ID_g$	
Calculates $SK_{g,d} = (q_g \cdot P_d) = (q_g \cdot r_g \cdot q_d \cdot G)$	
Selects $x \in Z_q^*$	
Computes $V_{g,d} = h(x \| t_s \| ID_g \| ID_d)$	

Encrypts $C_{g,d} = enc(V_{g,d})SK_{g,d}$

Sends $M_1 = \{C_{g,d}, P_g, t_s, V_{s,d}\}$

..... $= \Rightarrow$

Checks $| t_g - t'_s | \leq \Delta t$

Verifies $V'_{s,d} = h(t'_s) \| ID_d \| K_{d,s} \| P'_g$

Calculates
$SK_{d,g} = (q_d, P'_g) = (q_d, r_g, q_s, G)$

Decrypts $dec(C'_{g,d})SK_{d,g} = V'_{g,d}$

Gets ID'_d, t'_s, x and ID'_g from $V'_{g,d}$

Checks $ID'_d = ID_d$ and $t'_s = t_s$

Computes $y = getV_{g,d}(x) + 1$

Computes $V_{g,d} = h(x \| t_s \| ID_g \| ID_d)$

Encrypts $C_{d,g} = enc(V_{d,g})SK_{d,g}$

Sends $\{C_{d,g}\}$

$\Leftarrow$ .....

Decrypts $dec(C'_{d,g})SK_{g,d} = V'_{d,g}$

Gets y', t'_s, …

Verifies $| t_g - t''_s | \leq \Delta t$

Checks $ID'_g = ID_g$, $y' = x + 1$

4. Cryptanalysis of Baseline Protocol

In this section, we discuss some possible drawback of Zhao et al. protocol below:

4.1 Insider attack. A malicious adversary $(\mathcal{A})$ can register and authorize the terminal devices in the authentication phase of Zhao et al. protocol as follows:

Step 1. An adversary select his ID_i and send it to the cloud server CAAS

Step 2. After getting ID_i, CAAS begin to computes, select r_g where $R_g = r_g$.Gcomputes: $P_g = r_g \cdot Q_g$, $P_d = r_g \cdot Q_d$, $SK_{s,g} = h(q_s, Q_s) = h(K_{g,s})$ and $V_{s,d} = h(t_s \| ID_g \| q_s \cdot Q_d \| P_g)$, $M_{s,g} = \{ID_g \| ID_d \| t_s \| P_g \| P_d \| V_{s,d}\}$ and sends $SK_{s,g}$, $M_{s,g}$ to STD or SGW. Any adversary guesses the identity as $ID_{\mathcal{A}} = ID$.

Step 3. In step 1 of authentication phase the $\mathcal{A}$ selects x a random integer and p_d. Further $\mathcal{A}$ computes $V_{g,d}$, $C_{g,d}$ and sends $M_1 = \{t_s, P_g, V_{s,d}, C_{g,d}\}$.

Step 4. STD checks the $| t_g - t_s | \leq \Delta t$, if possible, then verifies $SK_{d,g} = (q_d \cdot P'_g) = (q_d \cdot r_g \cdot q_g \cdot G)$ and $V_{g,d}$, ID_d. Hence $\mathcal{A}$ successfully break this phase.

4.2 Guessing identity attack. In registration phase of Zhao et al. protocol, a malicious adversely attempt following steps to obtain the identity of terminal devices.

Step 1. The attacker guessing as $ID_{\mathcal{A}} = ID_i$, where $i = 1, 2, 3, \ldots, n$.

Step 2. If $ID_{\mathcal{A}} = ID_i$ any $\mathcal{A}$ guesses the identity of STD, else $\mathcal{A}$ does not guess the identity of STD.

Step 3. As $\mathcal{A}$ guess identity, after that $\mathcal{A}$ sends $ID_{\mathcal{A}}$ to cloud server CAAS.

Step 4. CAAS began to computing as, select r_g where $R_g = r_g$. Gcomputes: $P_g = r_g \cdot Q_g$, $P_d = r_g \cdot Q_d$, $SK_{s,g} = h(q_s, Q_s) = h(K_{g,s})$ and $V_{s,d} = h(t_s \| ID_g \| q_s \cdot Q_d \| P_g)$, $M_{s,g} = \{ID_g \| ID_d \| t_s \| P_g \| P_d \| V_{s,d}\}$. After that CAAS sends $SK_{s,g}$, $M_{s,g}$ to attacker $\mathcal{A}$.

Hence, $\mathcal{A}$ obtains the information from the authentication phase. Therefore, Zhao et al. fails to verify the said attack in the authentication phase.

4.3 Stolen device attack. Any attacker can stole the parameter P_g, $SK_{s,g}$ and $V_{s,d}$ from the authorized phase and use these parameters in authentication phase with the help of insider attack. So, an attacker successful to implying stolen device attack. Hence, Zhao et al. fails to verify the stolen device attack.

4.4 Session key disclosure attack. In the Zhao et al. protocol, the STD and SGW in the authentication phase not encrypts their Session key. As a result of this, a man in the middle (an attacker) with help of insider attack can get the session key. Hence, Zhao et al. fails to protect the session keys.

4.5 Fails to maintain mutual authentication. In the Zhao et al. protocol STD selects random integer value q_g, and also the gateway SGW selects random integer value q_d. Since $SK_{s,d} = (q_g \cdot P_d)$ and $K_{d,g} = (q_d \cdot P'_g)$, if $q_g \neq q_d$ then $SK_{g,d} \neq SK_{d,g}$. Hence, Zhao et al fails to maintain the mutual authentication.

4.6 User anonymity. In the Zhao et al. protocol, no anonymous identity was utilised. The attacker will be able to trace all information of authenticated users. As a result, the Zhao et al. protocol fails to provide user anonymity.

4.7 Lack of login phase. The login and verification phases were not used by Zhao et al. This system for logging in and verifying an authentic user has a design problem in it. As a result, Zhao et al. protocol lacks the login phase approach.

4.8 Lack of password information. Zhao et al. does not utilise a password during the registration and authentication process. As a result, using an identity guessing attack, any adversary can easily access the authentication phase. Thus, the absence of password use, the Zhao et al. framework fails to protect the information.

4.9 Denial of Service (DoS) attacks. In the Zoe et al. protocol there is no login and password phase. So, an adversary $\mathcal{A}$ easily can enter into the system and tries to send different ID_s.

In this way, the $\mathcal{A}$ sending a large number of requests to SGW. The SGW

fails to verify them. That will lead to denial of the services. Hence, the Zhao et al. fails to resists the DoS attack.

4.10 Clock synchronization problem. To prevent replay attacks, the Zhao et al. protocol uses a random number and a time stamp. However, in network systems such as WAN and LAN communication, time stamps cause a difficulty known as time synchronisation. It means that the Zhao et al. protocol fails to verify the probabilistic replay attack.

5. Suggestion to Improvement for Zhao et al. Scheme

The followings improvement needs in Zhao et al. scheme are as follows:

Step 1. In Zhao et al. protocol, they should utilize the login step in the authentication phase.

Step 2. In registration and authentication phase, SGW or STD need to adopt a biometric or password-based technique.

Step 3. In the Zhao et al. protocol, the password update phase is required.

Step 4. Using the light weight authentication protocol is SG environment that will help to reduce the communication and computation cost.

6. Conclusion and Future Direction

We have reviewed the Zhao et al. scheme in this paper, which is failed to protect the session key, susceptible to insider attacks, guessing identity attacks, user anonymity, stolen device attacks, ensure mutual authentication, lacks a login phase, lack password information, and has a clock synchronisation problem. Thus, in a smart grid environment, Zhao et al. scheme is insecure. Therefore, Zhao et al. scheme is unsuitable for network system in terms of internet of electric things. Further, we have suggested a possible solution of Zhao et al. scheme. In the future, we will try to develop an IoET based authentication protocol which addresses the improvement of Zhao et al. protocol in real-world smart grid infrastructure.

References

[1] K. Mahmood, X. Li, S. A. Chaudhry, H. Naqvi, S. Kumari, A. K. Sangaiah and J. J. Rodrigues, Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure, Future Generation Computer Systems 88 (2018), 491-500.

[2] A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, G. Schreier and R. Istepanian, Luigiatzori, antonioiera, giacomomorabito, the internet of things: A survey, Computer Networks 54(15) (2010), 2787-2805.

[3] H. Lee, R. Sriramdas, P. Kumar, M. Sanghadasa, M. G. Kang and S. Priya, maximizingpower generation from ambient stray magnetic fields around smart infrastructures enabling self-powered wireless devices, Energy and Environmental Science 13(5) (2020), 1462-1472.

[4] N. Komninos, E. Philippou and A. Pitsillides, Survey in smart grid and smart homesecurity: Issues, challenges and countermeasures, IEEE Communications Surveys and Tutorials 16(4) (2014), 1933-1954.

[5] B. Zhao, S. Zeng, H. Feng, Z. Chen, Z. Wang, J. Yang and J. Zhao, Lightweight mutual authentication strategy for internet of electric things, Sustainable Energy Technologies and Assessments 45 (2021), 101-130.

[6] E. J. Oughton, D. Ralph, R. Pant, E. Leverett, J. Copic, S. Thacker, R. Dada, S. Ruffle, M. Tuveson and J. W. Hall, Stochastic counterfactual risk analysis for the vulnerability assessment of cyber-physical attacks on electricity distribution infrastructure networks, Risk Analysis 39(9) (2019), 2012-2031.

[7] D. Wu, C. Zhou, Fault-tolerant and scalable key management for smart grid, IEEE Transactions on Smart Grid 2(2) (2011), 375-381.

[8] J. Srinivas, A. K. Das, N. Kumar and J. J. P. C. Rodrigues, Cloud centric authentication for wearable healthcare monitoring system, IEEE Transactions on Dependable and Secure Computing 17(5) (2020), 942-956. doi:10.1109/TDSC.2018.2828306

[9] Z. Wang, L. Gong, J. Yang and X. Zhang, Cloud-assisted elliptic curve password authenticated key exchange protocol for wearable healthcare monitoring system, Concurrency and Computation: Practice and Experience (2020) e5734.

[10] A. A. Khan, V. Kumar, M. Ahmad, S. Rana and D. Mishra, Palk: Password-based anonymous lightweight key agreement framework for smart grid, International Journal of Electrical Power and Energy Systems 121 (2020), 106-121.

[11] A. Kumari, V. Kumar, M. Y. Abbasi and M. Alam, The cryptanalysis of a secure authentication scheme based on elliptic curve cryptography for IOT and cloud servers, In 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN) IEEE 12 (2018), 321-325.

[12] A. A. Khan, V. Kumar, M. Ahmad, B. B. Gupta, A. El-Latif and A. Ahmed, A secure and efficient key agreement framework for critical energy infrastructure using mobile device, Telecommunication Systems 78(4) 539-557.