IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 18 November 2022, accepted 9 December 2022, date of publication 13 December 2022,
date of current version 16 February 2023.

Digital Object Identifier 10.1109/ACCESS.2022.3228905

RESEARCH ARTICLE

Achieving Light-Weighted Secure Scheme for Communication in a Smart Grid

AIJUAN WANG[1,2,3], JUNYANG LI[3], AND HAI NAN[3]
[1]School of Computer Science and Engineering, Chongqing Three Gorges University, Wanzhou, Chongqing 404000, China
[2]Chongqing Innovation Center, Beijing Institute of Technology, Yubei, Chongqing 401120, China
[3]College of Computer Science and Engineering, Chongqing University of Technology, Chongqing 400054, China

Corresponding author: Hai Nan (cqu.nn@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 62103070, in part by the China Postdoctoral Science Foundation under Grant 2022M720451, and in part by the Science and Technology Research Program of Chongqing Municipal Education Commission under Grant KJQN201901133 and Grant KJQN202001120.

ABSTRACT There are many security risks in the communication between the various nodes of the smart grid. Among these security risks, data leakage is a common one, which occurs in communicating between any two smart meters. In the existing studies, the data leakage is tackled by proposing various security strategies. In this paper, we propose a novel security communication scheme to ensure the security of transmission data between two smart meters against external malicious attacks. Specifically, an authentication scheme based on chaos theory is proposed for verifying the identity trustworthiness of smart meters. In the authentication phase, we use a chaos algorithm and a hash function to compute a shared session key that is used for authentication of both communicating parties, as well as for encryption of private information. Our proposed scheme implements a one-time session approach, i.e., each round of communication keys are unrelated to each other. In relevant validation experiments, we verify that the chaotic algorithm is sufficiently time efficient and compare the computational efficiency with other literature in terms of communication expenses, and the results prove that the proposed scheme is of lightweight nature. Finally we use the Proverif formal verification tool the BAN logic to verify the security as well as the feasibility of the proposed scheme.

INDEX TERMS Smart grid, privacy protection, chaos theory, session keys, one at a time.

I. INTRODUCTION

The smart grid, known as the grid of the future, has an additional information transmission network, which together with the electricity transmission network, forms a distributed and automated energy transmission network. Smart grid is a new type of grid that combines power engineering, monitoring, information and communication technologies to improve efficiency of the grid's operation. Under global pressure from resources and the environment, smart grid is focusing on flexibility, cleanliness, security and economy.

Generally, the smart grid consists of four main components, that is, Advanced Metering System (AMI), Advanced Distribution Operation (ADO), Advanced Transmission Operation (ATO) and Advanced Asset Management (AAM). In general, AMI implementation is the first step towards a smart grid. Its main function is to authorize users to connect systems and loads in order to support the grid, and the global delivery of power requires control and feedback of AMIs. These AMIs includes smart meters and detection sensors installed in customers' homes. The communication bridge in the smart grid between the network (operator) and reality (consumer) is the smart meter of AMIs. Smart appliances are able to communicate with smart meters in real time to achieve demand response control. Distributed detection sensors are responsible for collecting electricity usage data from individual smart appliances. In addition, they respond the energy usage and customer demand to the energy providers via home gateways, domain gateways, data collectors and substations (control centers). However, not all communication channels are secure during the operation of an AMI system, and a data breach can have a number of serious consequences.

Cyber security issues have always been a hot topic of research in the smart grid. Its communication networks have

The associate editor coordinating the review of this manuscript and approving it for publication was Luca Bedogni.

being exposed to various kinds of malicious attacks. For example, 2016 saw a massive network outage in the US, where attackers use a massive botnet to launch a mega DDos attack on the Internet Service Provider DNS infrastructure, rendering a large number of websites inaccessible. In 2018, in Kiev and western Ukraine, hackers disconnected power control systems and substations via a virus, and then they cut off the power company's communications with the outside world, which affects the lives of 1.4 million people to varying degrees. With the development of the smart grid, its structure has changed dramatically. Collecting, storing, transmission and processing of data have a very different way from before, which results in the greater risk of data leakage. Once data access rights are not set properly, or business logic design causes system flaws, which both may lead to privacy leaks of users' personal information. Researchers in [1] have shown that attackers are able to analyze a range of questions about user privacy through the obtained users' data. For example, What time do you go to bed? When do you get home? Are there any children in the house? Are there any physical illnesses, etc. [2]. Such fine-grained data may also be used as information in legal proceedings to refute or prove certain claims [3]. If the smart meter data is compromised, the privacy of the user's information will be immeasurably compromised. Hence, it motivates us to explore a secure authentication mechanism to ensure that the node's identity is trusted. Only when the authentication is passed, can the user's private information be transmitted properly and securely, which protects the user's privacy.

This paper presents a chaos theory-based message authentication scheme to ensure secure data interaction with smart meters in smart grids. Chaos is a behavior controlled by the laws of non-linear dynamics. It is mainly characterized by sensitivity to initial values and system parameters, and it has a very complex fractal structure and unpredictability of motion. In 1990, Matthews [4] firstly applied discrete chaotic dynamical systems to encryption algorithms, and proposed a one-dimensional chaotic mapping. Nowadays chaos theory is commonly used to encrypt images [5], [6], [7], [8], [9], and this technique is gradually maturing. It is pseudo-random and sensitive to the initial value, which makes it suitable for key generation. If one of the input parameters changes slightly, the generated value will be very different from the real value. In our scheme, we define three parameters that determine the value of the chaotic mapping, and only by mastering them can we participate in the whole call process.

The contributions of this paper includes threefold as follows:

- We propose a novel communication scheme to ensure the security of transmission data between two smart meters against external malicious attacks, which includes the identity credibility authentication and the message transmission. Correspondingly, the whole communication process is divided into the authentication phase and the message transmission phase.
- A chaos theory-based authentication scheme is proposed for the authentication phase, which ensures the identity credibility of smart meters. Only when the authentication is passed, can the one-time session key be generated to guarantee data transmission security.
- We expand the theoretical analysis on our scheme, including the security analysis and the performance analysis. The security analysis shows that it effectively resists replay attacks, man-in-the-middle attacks, and simulation attacks, etc. The performance analysis shows that it is lightweight and can be widely used.

The remainder of this paper is structured as follows. Related works are presented Section II. Section III presents our communication framework of the smart grid. In Section IV, we describe the threat model and design goals in the smart grid. Specific secure scheme based on chaos theory is given in Section V. We perform a security analysis of our scheme in Section VI. Section VII shows simulation of the experiments and its results. The last section is the conclusion.

II. RELATED WORK

The development of the smart grid has become a trend of the future development of the power grid. Smart grid can reduce waste of resources for the purpose of environmental protection, and it integrates individually generated renewable energy. In the smart grid, AMI establishes a two-way communication channel between the utility and consumers'smart meters, and the Wireless Mesh Network (WMN) ensures normal communication according to IEEE 802.15.4 or IEEE 802.11s standards. Being the same as existing IP-based communication networks, smart grid is also subject to the same security threats such as replay attacks, DOS attacks, traffic analysis and so on [10], [11].

Not every node in the network is trusted, and a strong authentication scheme is essential for communication frameworks of the smart grid [12], [13], [14], [15]. In [16] and [17], a PUF (Physical Unclonable Function) technique was proposed as an original language to counter physical attacks, but recent research [18] demonstrated that this technique is vulnerable to modeling attacks.

On the other hand, another method is proposed by adding noise to the data for the purpose of obfuscating data. A lightweight scheme is used in [19], where only a set of data is sent during transmission, and by a simple calculation such as addition and hashing, it can ensure that users' billing and power distribution are computed accurately. Adding noise method is a kind of the homomorphic encryptions. Homomorphic encryption, as one common method, is an operation that directly performs the data without needing a key. But this operation requires smart meters to have more computational overhead. In [20], [21], and [22], Shamir-based secret sharing scheme is investigated, which invokes dedicated data aggregators to collect electricity consumption data. And aggregating the data through a defined number of aggregators thus ensures the secure data transmission. However, this scheme

requires the installation of aggregators at different locations which will increase the construction overhead.With the gradual development in the field of cryptographic algorithms, the Elliptic Curve Cryptosystem (ECC) based protocol [23] is the most popular nowadays and it was proposed to address the weakness of RSA and the large key space required by Elgamal authentication schemes. References [24], [25], [26], [27] used ECC to design communication schemes for smart grids, the security in these schemes is high enough, but the point multiplication operation of ECC is very time consuming, especially in devices with limited computational resources like smart meters, which consume a lot of time to communicate.

In [10], Fouda et al. proposed a hierarchical communication model for smart grids and designed a lightweight communication scheme for smart grids based on the Diffie-Hellman key exchange protocol, which adopts hash-based message authentication codes in the message transmission phase to ensure secure message interaction, but the scheme uses RSA, a computationally intensive asymmetric Li et al. [28] followed the model proposed by Mostafa et al. and pointed out the shortcomings of their proposed scheme and improved it, reducing the communication overhead while ensuring the communication security by using the heterogeneous method and multiple hashes.

Most of the above studies improve and innovate on the basis of old algorithms, but few studies have gone to try to use algorithms from other fields, while chaos theory [29] possesses properties such as pseudo-randomness, ergodicity and sensitivity to initial values, which are very similar to those needed for the original language of cryptography, and the computation time of the one-dimensional logistic chaotic mapping is similar to that of the modal power operation after simulation analysis The computation time of the one-dimensional logistic chaos mapping is similar to that of the modal power operation after simulation. And most of the current research on chaos theory uses it as image encryption, optimization, trend prediction, etc [30], [31], [32]. So we try to propose a secure communication scheme for smart grid based on chaos theory, our scheme adopts the hierarchical communication model for smart grid proposed in literature [10], and takes into account the limited memory and computational power of smart meters, and finally our communication scheme is proved to be of light weight by simulation.

III. COMMUNICATION SYSTEM MODEL

In this paper, we consider the smart grid communication model shown in Fig. 1, a similar communication model structure has been proposed in [33], where the authors use fiber optic technology to establish communication between the control center and the building feeders, which is too costly. Therefore, in our model, WiMax technology is used instead of fiber optics. In this architecture, there are separately the electricity transmission network and the communication data transmission. First of all, from the distribution network, the power station generates electricity, and the nearby substation transmits it to the distribution substations (*DS*) in different areas through high-voltage transmission lines (*TS*). Then, *DS* converts high-voltage power into medium-voltage power, and then they are sent to the residential buildings. Finally, the feeders in the buildings convert it into low-voltage power that can be used by smart appliances.

From the communication point of view, the control centers (*CCs*) of the distribution substations are interconnected in such mesh networks (also known as Mesh networks) by using fiber optic technology. The lower-level networks include neighborhood area networks (*NANs*), building area networks (*BANs*), and home area networks (*HANs*). Each *DS* contains a *NAN*, which contains multiple *BAN* And each *BAN* contains multiple *HAN*. As shown in Figure 1, for communication between *NAN* and *BAN*, we use WiMax or other wireless communication technology to achieve, which is because wireless technology covers a larger area. And for the communication between smart appliances and smart meters (*SM*) inside the building area, ZigBee technology is usually used. Smart meters installed in the network have two main roles: one is to monitor power usage, and another is to act as a communication gateway.

In this paper, *NANGW*, *BANGW* and *HANGW* are the smart meters, and they are installed on *NANs*, *BANs* and *HANs* respectively, from which consumers can see their own power usage to decide the switching status of some smart appliances. It is worth mentioning that IP-based communication protocols are the most suitable for smart grid networks according to the existing standards, and it can be easily connected to *HANs*, *BANs*, *CCs* and substations. This means that each smart appliance has its own IP address. Therefore, the attacks defense for today's IP-based communication networks is also applicable to smart grid communication networks.

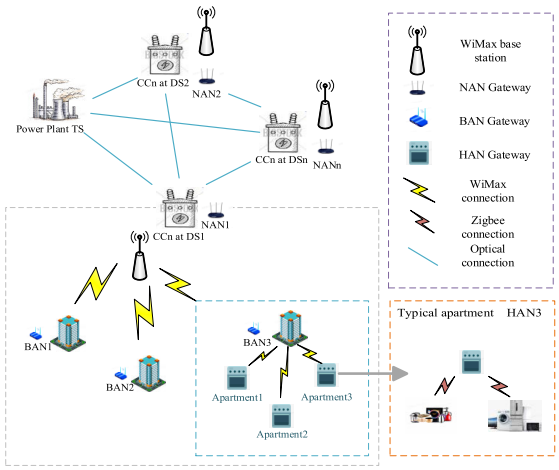


FIGURE 1. The smart grid communication model.

IV. DESIGN GOALS AND THREATS TYPES

In this subsection, we introduce that our proposed security scheme should achieve three design goals (the performances

of the proposed scheme), and we consider the following four various kinds of attacks.

A. DESIGN GOALS OF THE SECURITY SCHEME

This paper aims to enable secure end-to-end communication in the smart grid, and a strong security authentication scheme needs to be proposed to meet following requirements.

1) COMMUNICATION SECURITY

The scheme needs to detect the attackers sending dangerous messages, and be able to ensure the secure communication in the above threats.

2) LIGHTWEIGHT AND FAST COMMUNICATION

The limited resources of smart devices are the challenge issue, and a fast verification property is urgently needed. They can be achieved by reducing the size of the transmission packets and by reducing the verifying time from smart meters for the packets.

3) MAINTAIN FORWARD SECRECY

This scheme needs to ensure that the used keys do not reveal keys information that will be used in the future. So we need to ensure that there is no causal relationship between the keys before and after the different communication periods.

B. TYPES OF SECURITY THREATS

First, we assume that both the *HAN* and *BAN* gateways are physically indestructible and cannot tamper with internal information. Then, the following types of cyber-attacks are considered in our proposed communication framework.

1) REPLAY ATTACK

The attacker intercepts the *HAN* message by some means and resends this to the *BAN* gateway.

2) SNIFFING

As with traditional communication networks, an attacker steals data packets of communication networks.

3) SPOOFING

An attacker could impersonate a smart meter to send a fake message to the *BANGW*, which could lead to some serious consequences if unmonitored.

4) MAN-IN-THE-MIDDLE ATTACK

The attacker will impersonate and communicate between two communication subjects.

5) COMMUNICATION ANALYSIS

The attacker may intercept the communication message and modify it, which will lead to some wrong billing.

V. PROPOSED SCHEME

To achieve the above goals, this subsection describes detailedly our proposed secure authentication schemes.

TABLE 1. The notations and their semantic meanings.

Notations	Meaning
$HANGW_i$	The smart meter gateway on area network i
$BANGW_j$	The smart meter gateway on building network j
i, j	ID's of $HANGW_i$ and $BANGW_j$
t_i	Time stamp of $HANGW_i$
t_j	Time stamp of $BANGW_j$
X_0	Initial value of $HANGW_i$
X_0'	Initial value of $BANGW_j$
X_p,X_q	The value calculated from the chaotic mapping
K_{pq}	One-time session key
$Message_i$	On-demand information for smart appliances and appliance power requirements for $HANGW_s$
T_i	Time stamp of the final $HANGW$

The whole communication part can be divided into two phases: the authentication phase and the message transmission phase. Before these two phases, there is an additionally initialization phase. The whole communication process is similar to the three handshakes of TCP which describes the client and the server perform mutual authentication. In our scheme, it is mutual authentication and message transmission between two smart meters. Table 1 lists the symbols used in the scheme and their meanings.

A. INITIALIZATION

In each smart meter registration phase, the system assigns an ID number and μ, where μ can be updated as the system is updated. We assume that each meter has the same μ with $\mu \in [3.5699456, 4]$. It is worth mentioning that the use of chaotic mapping ensures that the generated values are unique as well as unpredictable. If μ, the initial value or iterations n change, the final value will be significantly different. For the mutual authentication of $HANGW_n$ and $BANGW_n$, we use a key exchange based on chaos theory to establish the protocol.

B. AUTHENTICATION

A set G with many large random numbers is assumed for the authentication phase. The authentication scheme is shown in Fig. 2, where we only consider two entities, i.e., $HANGW_i$ and $BANGW_j$, to participate in this communication. The scheme is explained in detail in three steps as follows.

- Step1: $HANGW_i$ chooses a random number $p \in G$ as the number of iterations, and chooses a initial value X_0, then calculates a unique X_p by logistic mapping $X_{n+1} = \mu X_n(1 - X_n)$ with iterations p times. The unique X_p is used to generate a one-time session key in the communication phase. $HANGW_i$ computes $A = hash(\mu||t_i) \oplus (X_p||i)$ and $B = hash(t_i||\mu||X_p||i)$ using the hash function and the iso-or operation, A, B and the timestamp t_i are then packaged and sent to $BANGW_j$. The format of the packet is: $M_1 = \{A, B, t_i\}$.
- Step2: After $BANGW_j$ receives the packet M_1, it first verifies the freshness t_i of the packet, then calculates the value of X_p and the ID number of the $HANGW_i$ using the hash function and the iso-or operation, and

then brings the obtained data and the value of μ into the hash function to verify the accuracy of the packet. Then, same as Step1, $BANGW_j$ selects a random number $q \in G$ and calculates the unique X_q by logistic mapping, at this time the $BANGW_j$ has the unique X_p of $HANGW_i$ and its own unique X_q, which can be used to calculate the session key after waiting for the completion of the authentication phase.Then $BANGW_j$ obtains the current timestamp t_j and calculates $A' = hash(\mu||t_j) \oplus (X_q||j)$ as well as $B' = hash(t_j||X_p||X_q||i||j)$. Then A', B' and timestamp t_j are packaged and sent to $HANGW_i$. The format of the packet is: $M_2 = \{A', B', t_j\}$.

- Step3: After receiving the response packet M_2 from $BANGW_j$, $HANGW_i$ first verifies the freshness of timestamp t_j, then calculates the value of X_q and the ID number of $BANGW_j$ using the hash function and the iso- or operation, then brings timestamp t_j, X_p, X_q, i, j into the hash function to determine whether the calculated is equal to B', if it is not equal then terminate the communication, if it is equal then enter the message transmission phase. $HANGW_i$ calculates the one-time session key as follows:$K_{pq} = Hash(X_p|X_q)$. Similarly, the $BANGW_j$ computes the session key by the same algorithm.

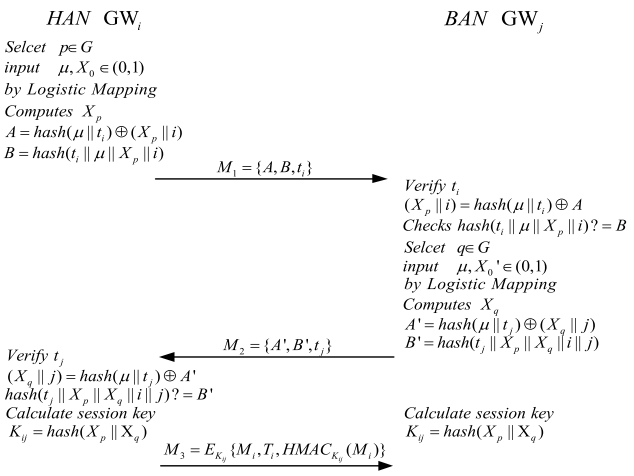


FIGURE 2. The authentication scheme.

In the Step 1-Step 3 of the above authentication process, those data packets packetized and sent by the smart meters contain very less data, and data packet is very small, where the transmission of the data packet can be completed in a short time. Moreover, the small data packet still completes the whole authentication process and achieve the authentication purposes. That is, the authentication needs take less time. Hence, our scheme is with the lightweight data.

In our security communication scheme, the identify authentication is fast due to the small data packet. Fast identity authentication will quickly determine whether smart meters enter the following communication phase, so it enables the whole communication to be completed quickly. Therefore, our scheme achieves the fast communication.

C. MESSAGE TRANSMISSION

We use $Message_i$ to represent messages, which contains the power requirements of the smart device for a certain time period, and the $HANGW_i$ needs to transmit it securely to the $BANGW_j$. After authentication, the one-time session key K_{pq} ensures that subsequent communication can be carried out properly. After $HANGW_i$ packages the packet containing $Message_i$ and T_i, the whole packet is encrypted using a symmetric encryption algorithm, and the key for encryption and decryption is K_{pq}. The encrypted packet is then sent to the $BANGW_j$. Here T_i is a timestamp added to prevent possible replay attacks. The packet form is as follows: $M_3 = \{Message_i|T_i\}_{K_{pq}}$.

Since K_{pq} is shared between $HANGW_i$ and $BANGW_j$, $BANGW_j$ uses K_{pq} to decrypt the packet and then verify the authenticity and integrity of the message. Only can the authenticated message be provided to the $NANGW$. If the values generated by the communication parties through the one-dimensional logistic mapping do not match, the final generated session keys are also different. Then, the packets in the final message transmission phase will not be decrypted by the session key.

VI. DESIGN GOALS ACHIEVEMENT ANALYSIS AND SECURITY ANALYSES

In this section, based on our proposed security scheme, the design goals about the performance of the proposed scheme is achieved, and security analysis for resisting the various kinds of attacks are given. In the following, we give the corresponding analysis, respectively. And it is shown that the security requirements can be guaranteed by our proposed security scheme.

TABLE 2. The BAN symbol and its meaning.

Notations	Meaning
A, B	Subjects involved in communication.
X, Y	Message Statements.
K	Encryption keys.
(X, Y)	X and Y connection.
$A\| \equiv X$	A thinks X is true.
$A \lhd X$	A has ever received a message containing X.
$A \sim X$	A has ever sent a message containing X.
$A \Rightarrow X$	A has control over X.
$\#X$	The X is fresh.
$A \overset{K}{\leftrightarrow} B$	The shared key K between A and B.
$\{X\}_K$	Results with K-encryption X.
$\langle X\rangle_Y$	Combination of X and Y.

A. DESIGN GOALS ACHIEVEMENT ANALYSIS

1) FORMAL ANALYSIS OF COMMUNICATION SECURITY

In the proposed scheme, the information we transmit in the authentication phase is the data encrypted by the hash function as well as the heterogeneous or operation, while the messages transmitted in the privacy information transmission

phase use the symmetric encryption algorithm to encrypt the data, and even if the attacker obtains these ciphertext data, he cannot infer the corresponding plaintext information without the corresponding decryption key. To prove the security of the scheme, we use BAN logic for formal analysis of the scheme, table 1 shows the basic notation and meaning regarding BAN logic, and the next few basic rules needed for the proof are given below:

- R_1: Message meaning rules: $\frac{A|\equiv A \overset{K}{\leftrightarrow} B, A \lhd \{X\}_K}{A|\equiv B|\sim X}$.
- R_2: Jurisdictional rules: $\frac{A|\equiv B \Rightarrow X, A|\equiv B|\equiv X}{A|\equiv X}$.
- R_3: Freshness-conjuncatenation rule: $\frac{A|\equiv \#(X)}{A|\equiv \#(X,Y)}$.
- R_4: Nonce-verification rules: $\frac{A|\equiv \#(X), A|\equiv B|\sim X}{A|\equiv B|\equiv X}$.
- R_5: Receiving message rules: $\frac{A \lhd (X,Y)}{A \lhd X}, \frac{A \lhd \langle X \rangle_K}{A \lhd X}, \frac{A|\equiv A \overset{K}{\leftrightarrow} B, A \lhd \langle X \rangle_K}{A \lhd X}$.
- R_6: Belief rules: $\frac{A|\equiv (X), A|\equiv (Y)}{A|\equiv (X,Y)}$.
- R_7: Session key rules: $\frac{A|\equiv \#(X), A|\equiv B|\equiv X}{A|\equiv A \overset{K}{\leftrightarrow} B}$.

In order to verify the security of the proposed protocol under BAN logic, the above rules must be used to satisfy the subsequent objectives(SM_i and SM_j denote two communication subjects):

- G_1: $SM_i| \equiv SM_i \overset{K_{ij}}{\leftrightarrow} SM_j$.
- G_2: $SM_j| \equiv SM_j \overset{K_{ij}}{\leftrightarrow} SM_i$.
- G_3: $SM_i| \equiv SM_j| \equiv SM_j \overset{K_{ij}}{\leftrightarrow} SM_i$.
- G_4: $SM_j| \equiv SM_i| \equiv SM_j \overset{K_{ij}}{\leftrightarrow} SM_i$.

The idealized conversion of the proposed protocol is as follows:

- M_1: $SM_i \rightarrow SM_j : A, B, t_i : \{i \overset{X_p}{\leftrightarrow} j, t_i\}$.
- M_2: $SM_j \rightarrow SM_i : A', B', t_j : \{j \overset{X_q}{\leftrightarrow} i, t_j\}$.

The following assumptions about the initial state of the program were used to evaluate the proposed program:

- H_1: $SM_i| \equiv \#(t_i)$.
- H_2: $SM_j| \equiv \#(t_j)$.
- H_3: $SM_i| \equiv SM_j \Rightarrow X_q$.
- H_4: $SM_j| \equiv SM_i \Rightarrow X_p$.
- H_5: $SM_i| \equiv SM_i \overset{\mu}{\leftrightarrow} SM_j$.
- H_6: $SM_j| \equiv SM_j \overset{\mu}{\leftrightarrow} SM_i$.

The formal proof procedure of the proposed protocol using BAN logic is as follows:

(1). According to the message M_1 we get,
$SM_i \rightarrow SM_j : \{i \overset{X_p}{\leftrightarrow} j, t_i\}$.

(2). From R_5 and H_6 we have,
$S_1 : SM_j \lhd \{A, B, t_i\} : \{\langle \mu, t_i \rangle_{(X_p,i)}, (\mu, X_p, i, t_i), t_i\}$.

(3). From S_1, R_1 and H_6, we have,
$S_2 : SM_j| \equiv SM_i| \sim \left\{ SM_i \overset{X_p}{\leftrightarrow} SM_j, t_i \right\}$.

(4). Using S_2, H_1 and R_4, we have,
$S_3 : SM_j| \equiv SM_i| \equiv \left\{ SM_i \overset{X_p}{\leftrightarrow} SM_j, t_i \right\}$.

(5). Using S_3, H_4 and R_2, we have,
$S_4 : SM_j| \equiv \left\{ SM_i \overset{X_p}{\leftrightarrow} SM_j, t_i \right\}$.

(6). Since $K_{ij} = hash(X_p||X_q)$, from S_4, H_1 and R_7, we get G_2,
$S_5 : SM_j| \equiv SM_i \overset{K_{ij}}{\leftrightarrow} SM_j$.

(7). Using S_5, H_4 and R_7, we get G_4,
$S_6 : SM_j| \equiv SM_i| \equiv SM_i \overset{K_{ij}}{\leftrightarrow} SM_j$.

Next, we consider the idealized form of M_2.

(8). According to the message M_2 we get,
$SM_j \rightarrow SM_i : \{j \overset{X_q}{\leftrightarrow} i, t_i\}$.

(9). From R_5 and H_5, we have,
$S_7 : SM_i \lhd \{A', B', t_j\} : \{\langle \mu, t_j \rangle_{(X_q,j)}, (\mu, X_q, j, t_j), t_j\}$.

(10). From R_5, S_7 and H_5, we have,
$S_8 : SM_i| \equiv SM_j| \sim \left\{ SM_i \overset{X_q}{\leftrightarrow} SM_j, t_j \right\}$.

(11). Using S_8, H_2 and R_4, we have,
$S_9 : SM_i| \equiv SM_j| \equiv \left\{ SM_i \overset{X_q}{\leftrightarrow} SM_j, t_j \right\}$.

(12). Using S_9, H_3 and R_2, we have,
$S_{10} : SM_i| \equiv \left\{ SM_i \overset{X_q}{\leftrightarrow} SM_j, t_j \right\}$.

(13). Since $K_{ij} = hash(X_q||X_p)$, from S_{10}, H_2 and R_7, we get G_1,
$S_{11} : SM_i| \equiv SM_i \overset{K_{ij}}{\leftrightarrow} SM_j$.

(14). Using S_{11}, H_3 and R_7, we get G_4,
$S_{12} : SM_i| \equiv SM_j| \equiv SM_i \overset{K_{ij}}{\leftrightarrow} SM_j$.

In steps (6), (7), (13) and (14), we achieve a logical proof of BAN for G_1, G_2, G_3 and G_4, respectively, proving that our scheme is capable of providing mutual authentication.

2) LIGHTWEIGHT AND FAST COMMUNICATION

In the proposed scheme, we only use hash functions, heteroskedastic operations, and one-dimensional logistic mappings from chaos theory in the authentication phase, which have the advantage of being computationally small and fast. Also, the authentication packets are sent with only two values calculated by the hash function and a timestamp, which minimizes the communication cost.

3) FORWARD CONFIDENTIALITY

In the session, each *HANGW* and *BANGW* generates its own random numbers p and q, and each time the X_p and X_q obtained by the algorithm are different from the previous ones. If a participant's key is leaked to an attacker, then the previous session keys are also secure. Thus, the scheme can guarantee forward secrecy.

B. INFORMAL SECURITY ANALYSIS

1) REPLAY ATTACK

During the authentication phase, each authentication message is given a temporary timestamp. In this scheme, when validating a packet, the freshness of the timestamp in the packet is verified first. If the message is intercepted and

replayed, the old t_i or t_j will not pass verification and then the communication will be aborted.

2) SNIFFING

The attacker can exist with the public channel to get the information we send, but all the information is in the form of ciphertext, either the value of μ or the symmetric key K_{ij}, which is not available to the attacker, then it is impossible to decrypt to get the plaintext information.

3) SPOOFING

In our proposed scheme, the identity of both communicating parties is authenticated before the user's electricity information is sent. If an attacker can masquerade as a smart meter to communicate with a normal user, he needs to have the knowledge of computing authentication information and to have the most critical shared key μ.

4) MAN-IN-THE-MIDDLE ATTACK

The timestamps used in the scenario are not only resistant to replay attacks, but also to man-in-the-middle attacks. If one of the parties delays sending the message, the timestamp is not guaranteed to be fresh and the session will be aborted. Also, in a session, the packets need a unique private key to be decrypted. So this scheme can resist man-in-the-middle attacks.

5) COMMUNICATION ANALYSIS

The attacker disguises as $HANGW_i$ and normal $BANGW_j$ to communicate, firstly the attacker needs to know the form of packet composition and secondly the way of X_p calculation. If there is no correct value of X_p, then finally $Hash(X_p|X_q)$ cannot calculate the correct K_{pq}. so this attack can be avoided.

VII. SIMULATION EXAMPLE

A. EFFECTIVENESS OF THE PROPOSED SCHEME

ProVerif is a formal verification tool that is widely used to verify the security and validity of key agreements; ProVerif has a "QUERY" function that determines whether a protocol is secure and functioning by the results returned by this query. We will detailed describe the ProVerif code that we use later. As shown below, in the simulation we consider two participants, Alice and Bob, with their ID numbers, private keys, shared key x, and an insecure communication channel ch defined in the code preparation phase, which are global variables that are private, meaning that an attacker cannot access them through the public channel.

```
free ch:channel.
free Kij:bitstring[private].
free IDi:bitstring[private].
free IDj:bitstring[private].
free r:bitstring[private].
free s:bitstring[private].
free x:bitstring[private].
```

Next, we define the functions to be used, such as chaos theory, hash, symmetric encryption, iso-or and hash-based message authentication code etc., rewrite the rules for encryption/decryption, and explain the iso-or operation.

```
fun chaos(bitstring,bitstring,bitstring):bitstring.
fun h(bitstring):bitstring.(*hash function*)
fun senc(bitstring,bitstring):bitstring.
      (*symmetric encryption*)
fun con(bitstring,bitstring):bitstring.
      (*string concatenation*)
fun xor(bitstring,bitstring):bitstring.(*exclusive-OR*)
fun HMAC(bitstring,bitstring):bitstring.
reduc forall m:bitstring,n:bitstring;sdec(senc(m,n),n)
      = m.(*symmetric decryption*)
equation forall m:bitstring,n:bitstring;xor(xor(m,n),n)=m.
```

Then the events are defined, as well as the queries for the events. The first query in the figure indicates that Alice needs to ensure that the event HANStart(id) occurs before the event HANAuth(id), and the second query indicates that Bob needs to ensure that the event BANStart(id) occurs before the event BANAuth(id). The query results can be divided into three types: 1) the query is true, which means that this scheme will not be attacked. 2) the query is false, which means that there is a possibility that this scheme will be attacked and the process of being attacked is also listed in the results. 3) the query is not provable, which means that the scheme cannot be proven to work properly or not.

```
event HANStart(bitstring).
event HANAuth(bitstring).
event BANStart(bitstring).
event BANAuth(bitstring).
query id:bitstring;inj-event(HANAuth(id))==>inj-event(HANStart(id)).
query id:bitstring;inj-event(BANAuth(id))==>inj-event(BANStart(id)).

(************************Alice*******************************)
let HAN=
event HANStart(IDi);
new X0:bitstring;
let A=chaos(X0,x,r) in
new ti:bitstring;
let B= xor(h(con(x,ti)),con(A,IDi)) in
let C=h(con(con(con(x,ti),IDi),A)) in
let M1=(B,C,ti) in
out(ch,M1);

in(ch,(bB:bitstring,bC:bitstring,btj:bitstring));
let (bIDj:bitstring , bA:bitstring)=xor(bB,h(con(x,btj))) in
if bC=h(con(con(con(con(bA,A),btj),IDi),bIDj)) then
let Kij=h(con(bA,A)) in
new messagei:bitstring;
new Ti:bitstring;
let Mi = senc(con(con(messagei,Ti),HMAC(Kij,messagei)),Kij) in
out(ch,Mi);
event BANAuth(IDj)
else 0.
```

On the Alice and Bob side, we follow the design logic of our proposed scheme to write the code. In which the packetized sent as well as received authentication information needs to pass through the insecure channel *ch*.

```
(************************Bob*******************************)
let BAN=
in(ch,(aB:bitstring,aC:bitstring,ati:bitstring));
let (aA:bitstring,aIDi:bitstring)=xor(aB,h(con(x,ati))) in
if (aC=h(con(con(con(x,ati),aA),aIDi))) then
new tj:bitstring;
new X0':bitstring;
let A'=chaos(X0',x,s) in
let B'=xor(h(con(x,tj)),con(A',IDj)) in
let C'=h(con(con(con(con(A',aA),tj),aIDi),IDj)) in
let M2=(B',C',tj) in
out(ch,M2);
event BANStart(IDj);
in(ch,aMi:bitstring);
let Kij'=h(con(aA,A')) in
let (amessagei:bitstring,aTi:bitstring,aHMAC:bitstring)=sdec(Kij',aMi) in
if (aHMAC=HMAC(Kij',amessagei)) then
event HANAuth(IDi)
else 0.
```

Finally we define a query: ''query attacker(Kij)'', which is used to determine if an attacker is able to crack the final communication password Kij. process execution code: ''process((!HAN)|(!BAN))'', is used to simulate the concurrent execution of several Alice as well as Bob processes.

The following figure shows the results of the code run, which shows that the final three queries are all true, indicating that the attacker cannot obtain the value of Kij, and that our solution works properly and can resist various common network attacks, which also proves the feasibility and security of the solution.

```
Verification summary:

Query inj-event(HANAuth(id)) ==> inj-event(HANStart(id)) is true.

Query inj-event(BANAuth(id)) ==> inj-event(BANStart(id)) is true.

Query not attacker(Kij[]) is true.
```

B. PERFORMANCE ANALYSIS BASED ON COMPARATIVE EXPERIMENT SIMULATION

(1). We simulated various algorithms running Python version 3.8 under 64-bit Windows 10 operating system, processor Intel(R) Core(TM) i5-6300HQ CPU @ 2.30GHz, running memory of 8GB, PyCharm Community Edition 2018.2.2, simulating various algorithms for nearly hundred times and then take the average running time, as shown in Table 3. We use T_h, T_{RSA}, T_{AES}, T_c, T_b, T_a, $T_m$and $T_{M-\exp}$ to denote the single hash function operation, RSA encryption and decryption operation, AES encryption and decryption operation, chaotic mapping, bilinear pairing operation, pointwise addition operation of elliptic curve, pointwise multiplication operation of elliptic curve, and modulo power operation, respectively.

TABLE 3. Simulation time.

Operations	Simulation(ms)
MD5	0.00050499999
RSA	2.615799989
AES-128	0.83099998
Chaos	0.05436669999
Bilinear Pairing	3.0041
ECC addtion	0.004834
ECC multiplication	0.126663
Modular exponentiation	0.019647999

TABLE 4. Comparison of communication time efficiency.

Scheme	Total(ms)
[10]	$2T_{RSA} + 4T_h + 1T_{AES} + 4T_{M-\exp} \approx 5.39531197556$
[24]	$4T_m + 14T_h + 5T_{M-\exp} + T_b \approx 6.653186999861$
[25]	$7T_m + 6T_a + 8T_h \approx 0.91968499992$
[28]	$8T_{M-\exp} + 8T_h + 1T_{AES} \approx 0.24432399712$
Our scheme	$2T_c + 12T_h + 1T_{AES} \approx 0.19789339786$

TABLE 5. Comparison of communication cost.

Scheme	our	[10]	[24]	[25]	[28]
Communication cost(bits)	704	1040	1920	2112	1600

The final results are shown in Table 4. The scheme in [10] uses RSA encryption and decryption twice, while the scheme in [24] uses the bilinear pairing technique in elliptic curves, and the computational complexity of both operations is higher, so the time consumed is longer. The scheme in [25] uses the dot product as well as the dot add operation in elliptic curves, and the scheme in [28] uses the modulo power operation, which has a relatively lower computational complexity than the dot product operation in elliptic curves, so it consumes relatively less time, while our scheme uses two chaotic iterative operations, 12 hash functions, and one AES encryption and decryption, and since the computational complexity of the anisotropic operation time is small enough, so we ignore it. It can be seen from the figure that our proposed scheme outperforms other schemes in the literature.

(2). The comparison of communication cost is shown in Table 5. In our simulation experiments, the user's ID is 64 bits, the output of the hash function is 160 bits, the ECC operation is 320 bits, and the timestamp is 32 bits. In the bilinear pairing, the elements of both G1 and G2 groups are 1024 bits, and the output of the modulo power operation is 256 bits. It is obvious that our scheme is much lower in terms of communication cost than other schemes.

(3). In terms of the space complexity of the scheme, it is worth mentioning that the chaotic mapping algorithm used in our proposed scheme is designed to obtain the final value, and the previous iteration value is released after the next iteration value is computed during the iterative process, so the storage space

temporarily occupied during the iterative operation does not increase due to the increase in the number of iterations.

VIII. CONCLUSION

IP-based communication technology is still the preferred choice for smart grid, but this technology is more vulnerable to security threats. In communication networks, not every subject is trusted, and once one of them has an abnormal node, then the others may suffer from privacy leakage. To solve this problem, this paper proposes an authentication scheme based on chaos theory, which generates unique values to reach a call protocol through a one-dimensional logistic chaos mapping. A security analysis of the proposed scheme is performed to address several possible security threats. The analysis shows that the scheme satisfies the five security requirements of providing mutual authentication, forward secrecy, resistance to replay attacks, resistance to man-in-the-middle attacks, and resistance to simulation attacks. Finally, the efficiency and security of the scheme are verified by experimental simulations. In summary, the scheme can achieve the protection of electricity consumption data during the communication process while appropriately reducing the burden of smart meter operation.

Future work can extend the chaotic mapping to two, three, or higher dimensions to enhance security, so the research direction proposed by this scheme still has great potential.

REFERENCES

[1] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, no. 1, pp. 81–85, Jan./Feb. 2010.

[2] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in *Proc. 2nd ACM Workshop Embedded Sens. Syst. Energy-Efficiency Building*, Nov. 2010, pp. 61–66.

[3] C. Rottondi, G. Verticale, and C. Krauss, "Distributed privacy-preserving aggregation of metering data in smart grids," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1342–1354, Jul. 2013.

[4] R. Matthews, "On the derivation of a chaotic encryption algorithm," *Cryptologia*, vol. 13, pp. 29–42, Jan. 1989.

[5] L. Chua, "Memristor, Hodgkin–Huxley, and edge of chaos," in *Handbook of Memristor Networks*. Bristol, U.K.: IOP Publishing, 2019, pp. 287–313.

[6] P. Junsangsri and F. Lombardi, "Design of a hybrid memory cell using memristance and ambipolarity," *IEEE Trans. Nanotechnol.*, vol. 12, no. 1, pp. 71–80, Jan. 2013.

[7] F. Xiang, C. Zhao, J. Wang, and Z. Zhang, "One-way hash function based on cascade chaos," *Open Cybern. Systemics J.*, vol. 9, no. 1, pp. 573–580, Jun. 2015.

[8] A. Kadir, M. Aili, and M. Sattar, "Color image encryption scheme using coupled hyper chaotic system with multiple impulse injections," *Optik*, vol. 129, pp. 231–238, Jan. 2017.

[9] T. Zhang, Y. Zhou, and C. P. Chen, "A new combined chaotic system for image encryption," in *Proc. IEEE Int. Conf. Comput. Sci. Autom. Eng. (CSAE)*, vol. 2, May 2012, pp. 331–335.

[10] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, Dec. 2011.

[11] V. Delgado-Gomes, J. F. Martins, C. Lima, and P. N. Borza, "Smart grid security issues," in *Proc. 9th Int. Conf. Compat. Power Electron. (CPE)*, 2015, pp. 534–538.

[12] X. Xiang and J. Cao, "An efficient authenticated key agreement scheme supporting privacy-preservation for smart grid communication," *Electr. Power Syst. Res.*, vol. 203, Feb. 2022, Art. no. 107630.

[13] A. Muzumdar, C. Modi, and C. Vyjayanthi, "Designing a blockchain-enabled privacy-preserving energy theft detection system for smart grid neighborhood area network," *Electr. Power Syst. Res.*, vol. 207, Jun. 2022, Art. no. 107884.

[14] K. Li, R. Shi, M. Wu, Y. Li, and X. Zhang, "A novel privacy-preserving multi-level aggregate signcryption and query scheme for smart grid via mobile fog computing," *J. Inf. Secur. Appl.*, vol. 67, Jun. 2022, Art. no. 103214.

[15] W. Zhang, S. Liu, and Z. Xia, "A distributed privacy-preserving data aggregation scheme for smart grid with fine-grained access control," *J. Inf. Secur. Appl.*, vol. 66, May 2022, Art. no. 103118.

[16] M. Nabeel, S. Kerr, X. Ding, and E. Bertino, "Authentication and key management for advanced metering infrastructures utilizing physically unclonable functions," in *Proc. IEEE 3rd Int. Conf. Smart Grid Commun. (SmartGridComm)*, Nov. 2012, pp. 324–329.

[17] P. Gope and B. Sikdar, "Privacy-aware authenticated key agreement scheme for secure smart grid communication," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3953–3962, Jul. 2018.

[18] P. Gope and B. Sikdar, "A privacy-aware reconfigurable authenticated key exchange scheme for secure communication in smart grids," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5335–5348, Nov. 2021.

[19] A. Guan and D. J. Guan, "An efficient and privacy protection communication scheme for smart grid," *IEEE Access*, vol. 8, pp. 179047–179054, 2020.

[20] C. Rottondi, G. Verticale, and C. Krauss, "Privacy-preserving smart metering with multiple data consumers," *Comput. Netw.*, vol. 57, no. 7, pp. 1699–1713, May 2013.

[21] J.-H. Hoepman, "Privacy friendly aggregation of smart meter readings, even when meters crash," in *Proc. 2nd Workshop Cyber-Phys. Secur. Resilience Smart Grids*, 2017, pp. 3–7.

[22] G. S. Wagh, S. Gupta, and S. Mishra, "A distributed privacy preserving framework for the smart grid," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2020, pp. 1–5.

[23] S. A. Chaudhry, H. Naqvi, M. Sher, M. S. Farash, and M. U. Hassan, "An improved and provably secure privacy preserving authentication protocol for SIP," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 1, pp. 1–15, Jan. 2017.

[24] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication," *Future Generat. Comput. Syst.*, vol. 81, pp. 557–565, Apr. 2018.

[25] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1900–1910, May 2016.

[26] D. He, H. Wang, M. K. Khan, and L. Wang, "Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography," *IET Commun.*, vol. 10, no. 14, pp. 1795–1802, Sep. 2016.

[27] K. Wu, R. Cheng, W. Cui, and W. Li, "A lightweight SM2-based security authentication scheme for smart grids," *Alexandria Eng. J.*, vol. 60, no. 1, pp. 435–446, Feb. 2021.

[28] X. Li, F. Wu, S. Kumari, L. Xu, A. K. Sangaiah, and K.-K.-R. Choo, "A provably secure and anonymous message authentication scheme for smart grids," *J. Parallel Distrib. Comput.*, vol. 132, pp. 242–249, Oct. 2019.

[29] L. Kocarev, "Chaos-based cryptography: A brief overview," *IEEE Circuits Syst. Mag.*, vol. 1, no. 3, pp. 6–21, 2001.

[30] I. Yasser, A. T. Khalil, M. A. Mohamed, A. S. Samra, and F. Khalifa, "A robust chaos-based technique for medical image encryption," *IEEE Access*, vol. 10, pp. 244–257, 2022.

[31] Y. Duan, N. Chen, L. Chang, Y. Ni, S. V. N. S. Kumar, and P. Zhang, "CAPSO: Chaos adaptive particle swarm optimization algorithm," *IEEE Access*, vol. 10, pp. 29393–29405, 2022.

[32] N. Darapaneni, S. Lahiri, K. Thakral, A. Ravatale, D. Bharadwaj, and A. R. Paduri, "COVID predictions and responsible weather parameters for infections in U.S.," in *Proc. 2nd Int. Conf. Secure Cyber Comput. Commun. (ICSCCC)*, May 2021, pp. 17–22.

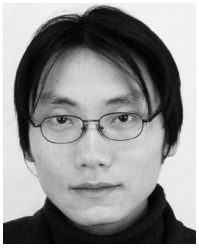
[33] K. Mahmood, S. A. Chaudhry, H. Naqvi, T. Shon, and H. F. Ahmad, "A lightweight message authentication scheme for smart grid communications in power sector," *Comput. Elect. Eng.*, vol. 52, pp. 114–124, May 2016.

AIJUAN WANG received the B.S. degree from Qufu Normal University, Shandong, China, in 2014, and the Ph.D. degree in computational intelligence and information processing from Southwest University, Chongqing, China, in 2019.

She was a Visiting Ph.D. Student with the University of Rhode Island, USA, from 2017 to 2018. She is currently an Associate Professor at the Chongqing University of Technology, China. Her research interests include nonlinear dynamical systems, optimal control, event-triggered control, consensus and privacy-preserving of multi-agent systems, optimization algorithm, economic dispatch of smart grid, and quantum neural networks.

JUNYANG LI received the bachelor's degree from Chengdu Neusoft University, in 2020. He is currently pursuing the master's degree with the Chongqing University of Technology.

His research interest includes smart grid communication security.



HAI NAN received the Ph.D. degree from the College of Computer Science, Chongqing University, in 2016. He is currently a Lecturer at the College of Computer Science and Engineering, Chongqing University of Technology. He has presided over one Chongqing Research Program of Basic Research and Frontier, one Science and Technology Research Program of Chongqing Municipal Education Commission, and two projects funded by the Basic Scientific Research Business Fees of Central Universities. In 2017, he was established the VR Innovation Laboratory of the College where he served as the Director. His research interests include digital image watermarking, artificial intelligence on games, and virtual reality technology.

He has won the first prize of the Fourth Natural Science Academic Award of Henan (ranked fourth). He led the team to win more than ten domestic top industry awards, including the Best Game Creativity Award of Tencent Next Idea Youth Game Developer Championship, the Best Audio-visual Performance Award of Indie Camp Game Creation Challenge, and the Champion of Chinese Undergraduate Computer Design Contest.