Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.029725
Article

Smart Grid Communication Under Elliptic Curve Cryptography

B. Prabakaran[1,*], T. R. Sumithira[2] and V. Nagaraj[3]

[1]Mahendra Engineering College, Salem, 637503, Tamilnadu, India
[2]Government College of Engineering, Salem, 636011, Tamilnadu, India
[3]Knowledge Institute of Technology, Salem, 637504, Tamilnadu, India
*Corresponding Author: B. Prabakaran. Email: prabakaranb1469@gmail.com
Received: 10 March 2022; Accepted: 22 June 2022

Abstract: Smart Grids (SGs) are introduced as a solution for standard power distribution. The significant capabilities of smart grids help to monitor consumer behaviors and power systems. However, the delay-sensitive network faces numerous challenges in which security and privacy gain more attention. Threats to transmitted messages, control over smart grid information and user privacy are the major concerns in smart grid security. Providing secure communication between the service provider and the user is the only possible solution for these security issues. So, this research work presents an efficient mutual authentication and key agreement protocol for smart grid communication using elliptic curve cryptography which is robust against security threats. A trust authority module is introduced in the security model apart from the user and service provider for authentication. The proposed approach performance is verified based on different security features, communication costs, and computation costs. The comparative analysis of experimental results demonstrates that the proposed authentication model attains better performance than existing state of art of techniques.

Keywords: Smart grid; elliptic curve cryptography; key management; mutual authentication

1 Introduction

Smart Grid is considered as the next-generation power system and the development of the smart grid has gained more attention due to ever-increasing electricity demand, electrical power systems complexity and the requirement for reliable and efficient power sources. Unlike conventional grids, a bi-directional flow is possible in smart grids to transfer electricity and information. The demand requirements of a consumer can be satisfied through a smart grid. Reliable and secure data communication, system monitoring and supervisory control strategies of the smart grid reduce the consumer energy cost and consumption and increases the overall system efficiency. Smart grid monitoring ability simplifies the manual interventions in network management. From production to distribution of energy to consumers can be effectively monitored through smart grids. As per statistics, by 2040 the electricity demand will increase more than 40% keeping the present situation as a baseline. The global energy utilization will increase by 49% and

the total energy generation will increase by 72% compared to energy demand in the year 2014 [1]. Smart plays a major role to balance demand and generation through its smart features.

Fig. 1 the existing legacy power grid systems provide a limited unidirectional flow of energy and information. Legacy grid communication is widely adapted for data acquisition from sensors located in the distribution and transmission points. It uses limited control signals for transmission and fault detection [2]. Supervisory Control and Data Acquisition Systems (SCADA) perform the data acquisition. However, due to limited sensors and control signals, legacy power grids provide limited services to consumers [3]. On the contrary smart grid can handle a large number of sensors and actuators. The components can be deployed at any level from user homes to power plants [4]. Sensors are not only used for data acquisition and can be used for information exchange also. In order to handle such large sensor data, smart grids must have a reliable secure communication infrastructure. A high data rate requires wide bandwidth and that must be satisfied by the communication infrastructure [5]. Also, the infrastructure must be adaptive to changes [6]. A simple illustration for smart grid communication is depicted in Fig. 1.

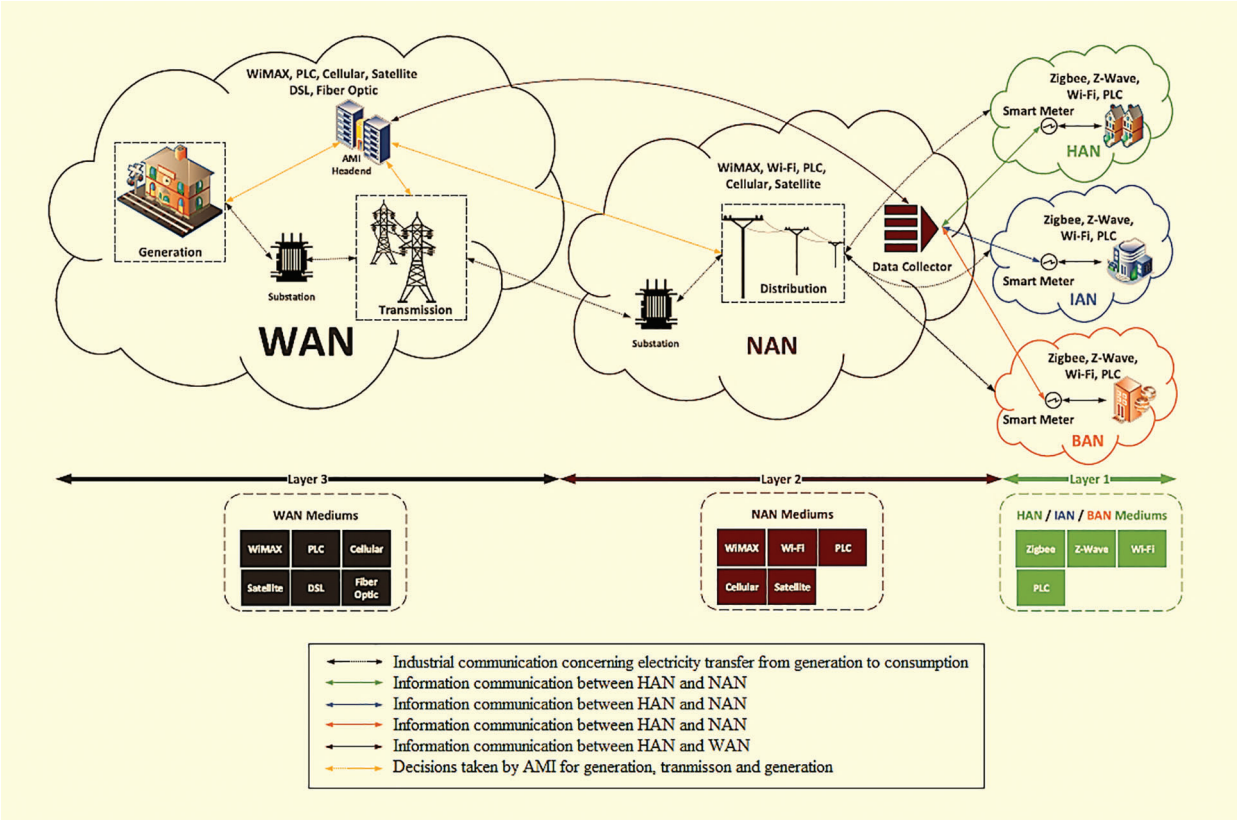

Figure 1: Smart grid communication

Smart grid communication infrastructure comprises three networks such as Wide Area Network (WAN), Neighborhood Area Network (NAN) and Home Area Network (HAN) [7]. Small region communication typically for offices or homes can be operated with HAN. The transmission rate of HAN is 100 bps. Devices in the home that consumes electrical energy and smart meter are generally connected to HAN. Using Ethernet or ZigBee technology HAN can be implemented for efficient energy management [8]. Neighborhood Area Network is employed where connection requires for urban buildings. One NAN can able to connect multiple HANs. In the smart grid, the energy consumption data of individuals can be

obtained from NAN by connecting HANs. The data collected in NAN are stored in data centers and it is analyzed to obtain energy generation and demand patterns [9]. The transmission rate of NAN is a maximum of 2 Kbps and it can be deployed through cellular and Wireless Fidelity (Wi-Fi) technologies. To extend the range of communication WAN is deployed that can connect several NANs and the operating range is usually tens of kilometers [10]. Based on WAN, all the smart grid communication modules such as energy generation, control center, transmission and distribution are performed. It has the maximum transmission rate in Gbps and it can be implemented using Worldwide Interoperability for Microwave Access (WiMAX), Ethernet, 3G or Long-Term Evolution (LTE), microwave communications [11].

In order to control smart grid components, data acquisition and analysis are important and they can be obtained through efficient communication systems. Thousands of smart meters and control devices deployed in smart grid generated huge data continuously and it needs to be transferred bidirectionally [12]. Processing such huge data through a communication system is vulnerable to attacks [13,14]. Smart grid data transmission is divided into three categories as

1) Transmission of smart meter data to the local data center and operator center.
2) Transmission of data from smart devices to operator center.
3) Transmission of control signals from operator center to smart devices.

Intercepting the first category of data transmission, the intruder can modify the billing system and it will lead to economic loss for the generation company [15]. Intercepting the second category of data transmission, intruders modify the parameters of smart devices such as transformers, switches, generators, Flexible AC Transmission (FACT) devices and turbines to make wrong decisions. Intercepting the third category of data transmission, an intruder will replace the signal which leads to severe equipment damage, loss of control, etc., Securing the data transmission in smart grid communication to prevent unauthorized access requires an efficient encryption mechanism at the software level [16]. This research work is aimed to develop a secure communication infrastructure for the smart grid so that efficient monitoring and controlling of smart data is achieved to improve operational efficiency.

2 Literature Works

The authentication model reported improves the security features of advanced metering infrastructure in smart grids using a certificate and Intrusion Detection (ID) based mechanism. Data integrity attacks, replay attacks, and impersonation attacks are eliminated using the authentication model. The performance of this two-stage authentication is much better than complex certificate-based authentication schemes. The Key generating center in the system performs complex computations thereby it reduces the computational complexities of individual terminals. Customer data privacy support through software guard extensions (SGX) enabled smart grid system reported in eliminates the requirement of complex cryptography mechanisms. Advanced encryption standard algorithm is incorporated with SGX to ensure data privacy and provides high-speed data communication for smart grids.

A certificate less signcryption for smart grid system access control reported in [17] used proxy re-encryption to improve the data confidentiality, non-repudiation and integrity. To ensure the benefits of certificate-based signcryption, the Internet of things (IoT) enabled smart grid system with certificate-based signcryption and proxy re-encryption model [18] is reported in that improves the confidentiality, unforgeability and forward secrecy in the smart grid communication. The reported signcryption process reduces the computation cost and communication cost and makes it appropriate for the system which needs more resources.

A demand response management system (DRMAS) for the smart grid [19] is proposed in to prevent modifications in the smart grid communication channel. Elliptic curve cryptography-based certificate is

used to secure the demand responses and obtain a better tradeoff between overall performance and security features. A similar Elliptic curve cryptography-based secure key arrangement model for smart grid is reported to authenticate [20] the communication between the smart meter and service provider. An automatic protocol verifier is also used to assess the security features of the system [21]. However, the system requires a separate module to identify anonymities which is considered as a major limitation.

To detect data integrity attacks in smart grid load frequency control a model-based detection system is reported [22] in that uses statistical methodologies with public key encryption to verify the messages in the power system communication. authors have designed a resilient controller that identifies three different types of attacks on data integrity and identifies even a small modification in the data. Secure transmission of big data in smart grid communication reported presents a lightweight [23] quantum cryptography model for guaranteed security. The traditional communication model is improved by introducing a quantum key generation and distribution protocol that ensures data safety in the power system.

The impact of security attacks on smart grid communication is analyzed [24] through a semi-supervised deep learning model. To identify false data injection attacks General Adversarial Network (GAN) is combined with an autoencoder. High detection accuracy and robustness against attacks are the major merits of the research model. However, it requires a clustering method to group the operation model which increases the computation cost of the system. To detect malicious data injection attacks a priority-based protection mechanism is reported in [25]. The enhanced protection mechanism performs better than existing priority-based protection strategies and reduces the further possibilities of attacks. From the analysis, it is observed that efficient authentication and encryption schemes can improve system performance and enhance grid communication security. However, the performance of the existing certificate-based authentication system can be further increased. In the case of Intrusion Detection (ID), based on authentication approaches the security of data is uncertain. So, it is essential to develop a model that provides data security and authentication to enhance the efficiency of the smart grid system. Based on this observation, a hybrid authentication and encryption scheme are presented in the following section.

3 Preliminaries

The essential preliminaries for the proposed work are discussed before preceding the working of the secure smart grid communication model.

3.1 Network Model

The proposed system model for smart grid communication is depicted in Fig. 2. It mainly consists of three components such as user u_i, service provider (SP) and trust authority (TA). The trust authority is responsible for providing essential parameters and security keys for the users. So that user can encrypt the data and store it in the server. Users can access data service from the server using the key obtained from the trust authority.

- u_i is an active user in the smart grid which holds the smart meter and other devices to receive the key from the trust authority (TA) in the registration process. The user then exchanges the essential parameters with the service provider (SP) and initiates secure communication using the session key obtained from (TA).
- Trust authority (TA) is an entity that registers the user u_i, and Service Provider (SP) and provides the necessary credentials. The user and service provider will authenticate each other using a public network with the support of a trusted authority.
- Similarly, service provider (SP) also need to register with Trusted Authority (TA) to obtain credentials to authenticate the user u_i. If the u_i and (SP) authenticate each other mutually through Trust authority (TA) then they will establish a shared session key for further communication Fig. 2.

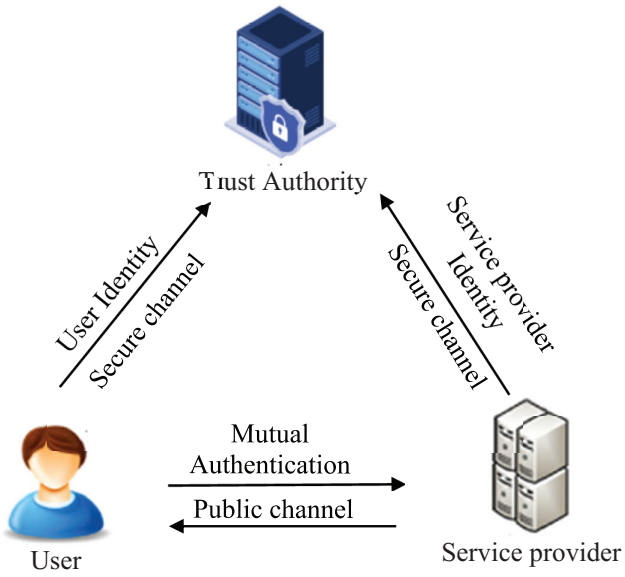

Figure 2: Proposed work system model

3.2 Security Requirements

The security requirement of the proposed system model is defined to ensure guaranteed security in smart grid communication. The definitions are observed based on the common network communication functionalities and requirements. Tab. 1 gives a summary of requirements and their description. Based on seven categories the security requirements of the proposed system are framed and it is described in detail . All the given requirements are essential and the proposed system must satisfy all in order to be a better and more efficient smart grid communication model.

Table 1: Security requirements

S. no	Requirement	Description
1	Mutual authentication	Mutual authentication should be introduced for the user, service provider and trust authority to access the information
2	Session key agreement	The session should be used for subsequent communication once mutual authentication is performed
3	Untraceability	Relevant details must be hidden from an attacker.
4	Anonymity	Only trusted party identities can be revealed
5	Availability	Access to services at any time and secure against DoS attacks
6	Robustness	The system should resist various attacks such as Replay Attacks, Man-in-the-Middle attacks, Server Impersonation attacks, Smart Meter Anonymity, Information attacks, Private Key Leakage, Privileged Insider attacks.
7	Execution overhead	The system must exhibit low computation and communication costs

3.3 Elliptic Curve Cryptography (ECC)

In the proposed smart grid communication, elliptic curve cryptography is used. The performance of elliptic curve cryptography is much better than Rivest–Shamir–Adleman (RSA), Digital Signature Algorithm (DSA), and other cryptography algorithms. The basic definition for elliptic curve cryptography is presented here, however, we have included few modifications in the cryptography scheme that is discussed in Section 4. The traditional elliptic curve cryptography is defined based on a non-singular elliptic curve $E_q(m,\ l)$ over a finite field z_q and it is mathematically expressed as

$$v^2 mod\ q = (n^3 + mn + l)\ mod\ q \tag{1}$$

where q represents a large prime number, $m,\ l$ are the elements of the finite field. The condition to attain nonsingular elliptic is $4m^3 + 27l^2\ mod\ q \neq 0$. The commutative group is expressed as

$$c_g = \{(n,\ v): n,\ v \in z_q\ and\ (n,\ v) \in E_q(m,\ l\})\ \cup\{o\} \tag{2}$$

The above expressed group is obtained from the points $E_q(m,\ l)$ and the term $\mathcal{O}$ represents the point at infinity. The points denoted by (1) must satisfy the condition $q + 1 - 2\sqrt{q} \leq E_q \leq q + 1 + 2\sqrt{q}$. The operation of elliptic curve cryptography is summarized as follows.

- If $q = (n_1,\ v_1)$ and $p = (n_2,\ v_2)$ are the two points obtained from Eq. (1), the scalar addition of q and p is obtained as $s = (n_3,\ v_3)$, if q and p are not equal. Where $n_3 = (\alpha^2 - n_1 - n_2)(mod\ q)$ and $v_3 = (\alpha(n_1 - n_3) - v_1)(mod\ q)$. The term α is given as

$$\alpha = \begin{cases} \dfrac{l_2 - l_1}{n_2 - n_1}(mod\ q), & if\ p \neq q \\ \dfrac{3n_1^2 + m}{2v_1}\ (mod\ q), & if\ p = q \end{cases} \tag{3}$$

- The point q on Eq. (1) should be added x times for scalar point multiplication and it is given as

$$xq = q + q + q + \ldots + q(xtimes) \tag{4}$$

- For doubling operation, the point q is added with same q to obtain new point and it is expressed as

$$p = 2q = q + q \tag{5}$$

- For point subtraction operation, the points $q = (n_1,\ v_1)$ and $p = (n_2,\ v_2)$ are equal to $\mathcal{O}$ as $q + p = \mathcal{O}$. This indicates that $n_1 = n_2$ and $v_2 = -v_1$.
- The order of point q is defined as smallest positive integer i and it is given as $iq = \mathcal{O}$.

Based on the above operations, elliptical curve cryptography characteristics are observed.

In the hardness function description, two factors are considered such as negligible function, computational Diffie-Hellman assumption. If the function r is the security parameter, then the negligible function $\varepsilon(r)$ is given as $\varepsilon(r) \leq \frac{1}{r^h}\ if\ \forall\ h > 0,\ \ \exists r_0$. So that $\forall\ h > r_0$. For computational Diffie-Hellman assumption, for a given tuple $(q,\ \ xq,\ \ yq)$ where $x,\ y \in z_q$ and $q \in E_q(m,\ l)$. However, it is intractable to compute xyq based on that the adversary function $\mathcal{A}$ is given as

$Adv_{\mathcal{A}}^{CDH} = Prob[\mathcal{A}(q,\ xq,\ yq)] = xyq : q \in E_q(m,\ l),\ x,\ y \in z_q]$. The success probability of time bounded probabilistic polynomial and adversary are related and it is given as $Adv_{\mathcal{A}}^{DH} \leq \varepsilon$.

3.4 Threat Model

The threat model for the proposed work is extracted from the security assumptions given in [26]. The threat model assumes that adversary function can able to track the messages, and it can modify the

information in the messages, stored keys, session states, credentials and insertion of malicious contents or deletion of existing contents can be performed by adversary function. Also, the endpoint entities are also considered as non-trustworthy. To obtain the maximum capability of proposed system, other than existing security assumptions few more assumptions are considered as follows.

- The adversary is considered as polynomial time-bounded adversary $\mathcal{A}$ and the participants $(u_i,\ TA,\ SP)$ interacts each other about the queries that helps to perform attack. The adversary attack may be an outsider attack or any other attack as listed in Tab. 1.
- If the adversary $\mathcal{A}$ is an insider and maintains trust authority is allowed to access the stored data present with service provider to extract secret information.
- All the communication takes place in public channel is controlled by adversary $\mathcal{A}$. So that blocking, removing, injecting or modifying the messages can be possible.
- The adversary $\mathcal{A}$ function has no capability to alter the messages in the secure channel.
- The secret value of user can be obtained by adversary $\mathcal{A}$ through reverse engineering process or directly obtain from Trust authority (TA) and Service Provider (SP). However, simultaneous operations are not allowed.

4 Proposed Secure Smart Grid Communication Model

The proposed secure smart grid communication model includes secure authentication and key agreement scheme and it comprises of four tasks such as user registration, service provider registration, authentication, and dynamic update. Initially to set up the environment, trust authority selects the private key and system public parameters. The process of selecting trust for that large prime number is selected. As per Eq. (1) the condition is given as $q \geq 2^j$. A base point is selected with order q as $q \in E_q(m,\ l)$, similarly, a hash function is considered as $h: \{0,\ 1\}^* \rightarrow \{0,\ 1\}^j$. A private key is selected $s_{pr} \in z_q$ and published as system parameters $\{E_q(m,\ l),\ q,\ p,\ h(.)\}$.

4.1 Service Provider Registration

The service provider registration phase registers the system to trust authority and receives the secret parameters which are required for further authentication. Each system registration ID are obtained along with its pseudo-identity and it will be stored in the trust authority database to verify the service provider. The steps followed in the service provider registration is summarized as follows.

- SP chooses an identity ID_x and it is transmitted to Trust Authority (TA) through a secure channel.
- The uniqueness of ID_x is verified by Trust Authority (TA) by comparing with the existing identities in the database. If it matches then TA requests SP to select new ID_x. Otherwise, TA selects a uniform random number $a_x \in z_q$ and generates PID_x and k_x as Fig. 3

$$PID_x = h(a_x||ID_x) \tag{6}$$

$$k_x = h(ID_x\|s\|a_x) \tag{7}$$

The details $ID_x,\ PID_x,\ k_x$ are stored in the Trust Authority (TA) database and $ID_x,\ PID_x,\ k_x$, h(.) are send to Service Provider (SP) through a secure channel. Fig. 3 depicts the service provider registration process in detail.

4.2 User Registration

The user registration phase registers the user to trust authority and receives the secret parameters which are required to prove the identity to Service Provider (SP). For each user, a registration ID is obtained along

with its pseudo identity so that the user can have access to the data from the database. Fig. 4 depicts the service provider registration process in detail.

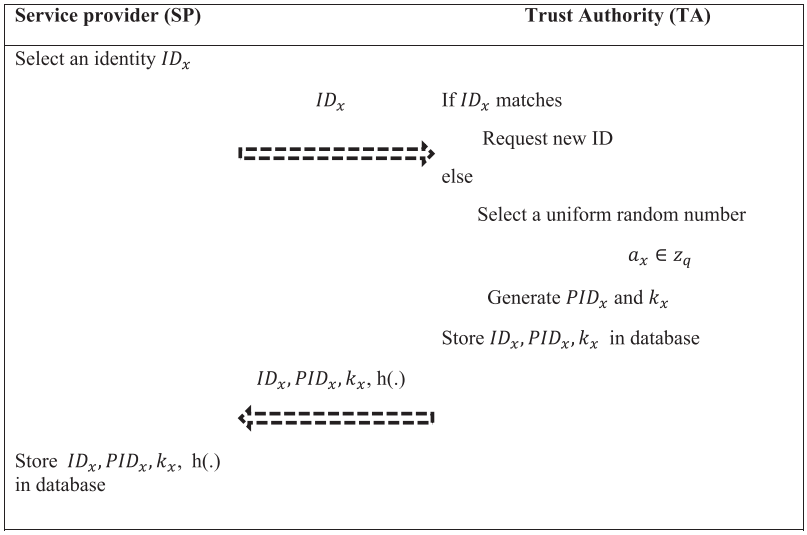

Figure 3: Service provider registration process

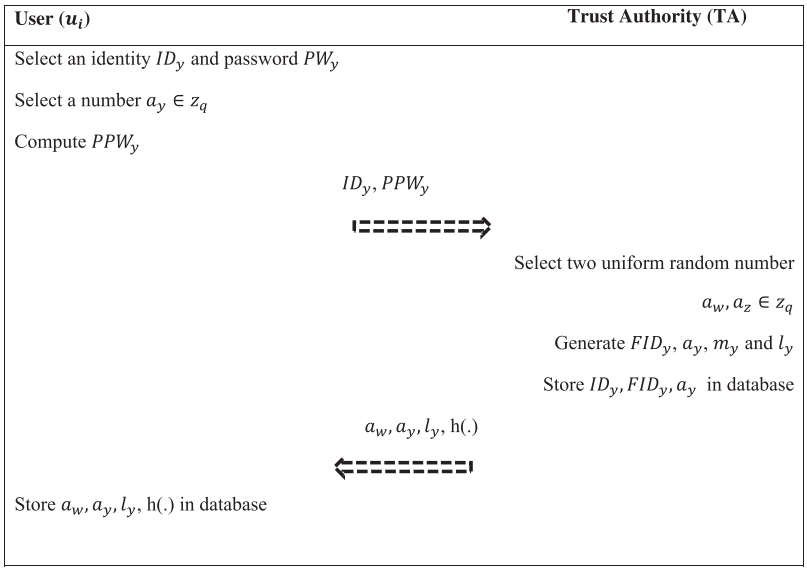

Figure 4: User registration process

The steps followed in the user registration are summarized as follows.

- User u_i chooses an identity ID_y and password PW_y it is transmitted to trust authority (TA) through a secure channel. The uniqueness of ID_y is verified by TA by comparing with the existing identities in the database. If it matches then TA requests u_i to select new ID_y. Otherwise, it generates PPW_y as

$$PPW_y = h(h(ID_y||a_y) \oplus h(PW_y||a_y) \tag{8}$$

The details ID_y, PPW_y are send to SP securely.

- SP receives ID_y, PPW_y and selects two uniform random numbers a_w, $a_z \in z_q$ and generates FID_y, a_y, m_y, *and* l_y as

$$FID_y = h(ID_y||a_w) \tag{9}$$

$$a_y = h(FID_y\|s\|a_z) \tag{10}$$

$$m_y = h(FID_y\|PPW_y\|a_w||a_y) \tag{11}$$

$$l_y = h(m_y||FID_y) \tag{12}$$

The details are stored in SP database and sends a_w, a_y, l_y, h(.) to user u_i through secure channel.

- The details a_w, a_y, l_y, h(.) received from SP are stored in u_i storage.

4.3 Login and Authentication

In login and authentication process, the user and service provider mutually authenticate each other with the support of trust authority and then establishes a common session key. So that user will securely transmit the data which is encrypted using the session key. The process is summarized as follows.

- User u_i enters the identity ID_y and password PW_y and calculates the following

$$PPW_y^* = h(h(PW_y||a_y) \oplus h(ID_y||a_y)) \tag{13}$$

$$FID_y^* = h(ID_y||a_w) \tag{14}$$

$$m_y^* = h(FID_y^*\|PPW_y^*\|a_w||a_y) \tag{15}$$

$$l_y^* = h(m_y^*||FID_y^*) \tag{16}$$

The user database checks whether $l_y^* = l_y$ and if so, the next step is executed otherwise, the login request is aborted.

- A timestamp (T_1) is selected by u_i along with a random number $a_t \in z_q$, then u_i generates m_{1_i}

$$m_{1_i} = h(T_1||FID_y||a_y) \tag{17}$$

The details T_1, a_tq, m_{1_i}, FID_y, PID_x to SP through a public channel.

- At time (T_2) the messages T_1, a_tq, m_{1_i}, FID_y, PID_x are received by SP and check the message freshness based on verifying the time durations $|T_2 - T_1| \leq \Delta T$. If it is correct SP receives the tuple ID_y, FID_y, a_y from database and generate A'_{1_i} as

$$m'_{1_i} = h(T_1||FID_y||a_y) \tag{18}$$

Then it checks $m'_{1_i} = m_{1_i}$ if so, then user u_i gets authenticated and SP computes k_{xy} and m_{3_i}, other wide process get terminated.

$$k_{xy} = k_x \oplus k_y \tag{19}$$

$$m_{3_i} = h(T_1||FID_y||a_y) \tag{20}$$

Further the values $m'_{3_i} = m_{3_i}$ is checked to authenticate TA. Now CP selects a uniform random number $a_o \in z_q$ and generates the session key and authentication function as

$$sk_y = h(ID_y||a_o z_x p||a_y||FID_x) \tag{21}$$

$$Aut_y = h(sk_y||FID_x||T_3||a_y) \tag{22}$$

The final details $a_o p,\ T_3,\ Aut_y$ are transferred to u_i through the public network.

- User u_i receives the details $a_o p,\ T_3,\ Aut_y$ and checks the freshness of arrival $|T_4 - T_3| \leq \Delta T$. The session key is calculated as $sk_x = h(ID_y||a_o z_x p||a_y||FID_x)$ and authentication as $Aut_x = h(sk_x||FID_x||T_3||a_y)$. The user terminal checks $Aut_x = Aut_y$, if so, it authenticates the SP, else the process will be terminated Fig. 5.

Fig. 5 depicts the Login and Authentication process in detail

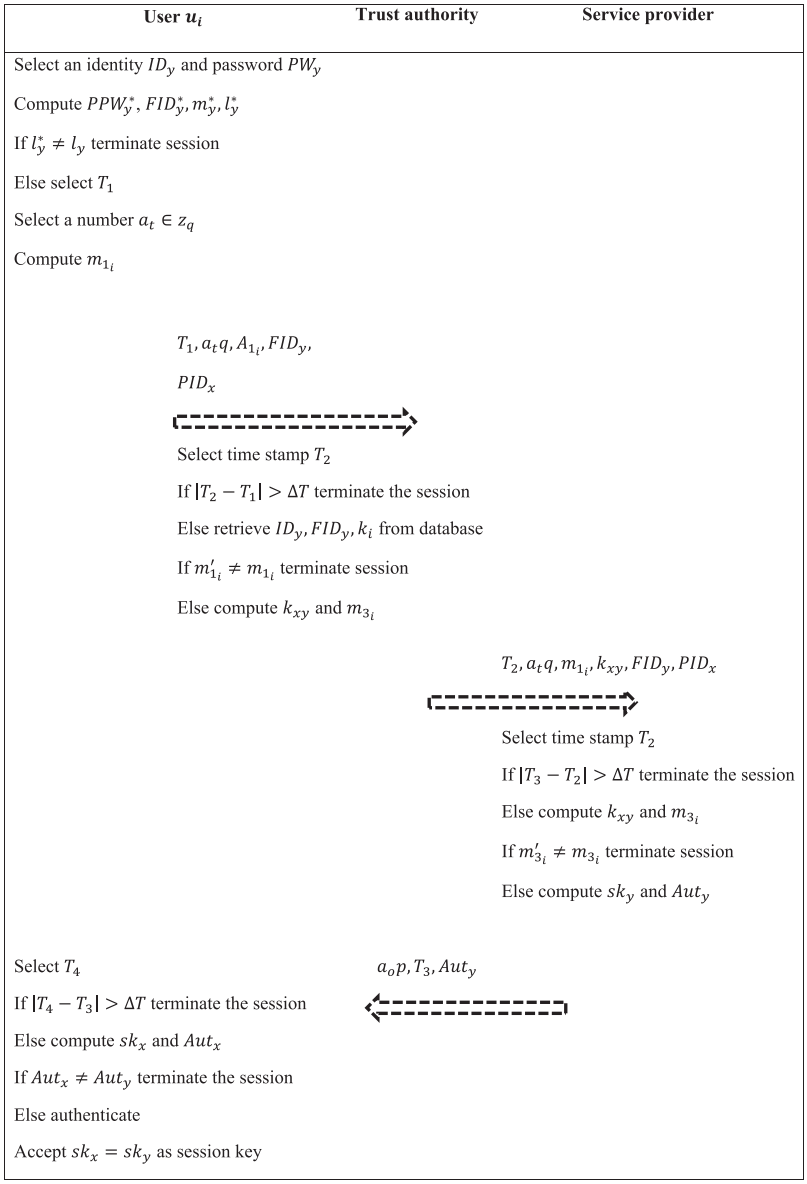

Figure 5: Login and authentication process

4.4 Dynamic Update

The dynamic update discusses the necessity of adaptability of changes in the communication module. Due to physical damage or accidental damages, the system must update itself and reconfigures to reach the nearby location. The steps followed in the dynamic update process are given as follows.

- A new unregistered user selects an identity ID_x^{new} and transmit the details to the trust authority across the secure channel.
- The uniqueness of ID_x is verified by TA by comparing with the existing identities in the database. If it matches then TA requests SP to select new ID_x. Otherwise, TA selects a uniform random number $a_x^{new} \in z_q$ and generates PID_x and k_x as

$$PID_x^{new} = h(a_x^{new}||ID_x^{new}) \tag{23}$$

$$k_x^{new} = h(ID_x^{new}\|s\|a_x^{new}) \tag{24}$$

- The details ID_x^{new}, PID_x^{new}, k_x^{new} are stored in the TA database and ID_x^{new}, PID_x^{new}, k_x^{new}, h(.) are send to SP through a secure channel. Fig. 6 depicts the service provider registration process in detail.

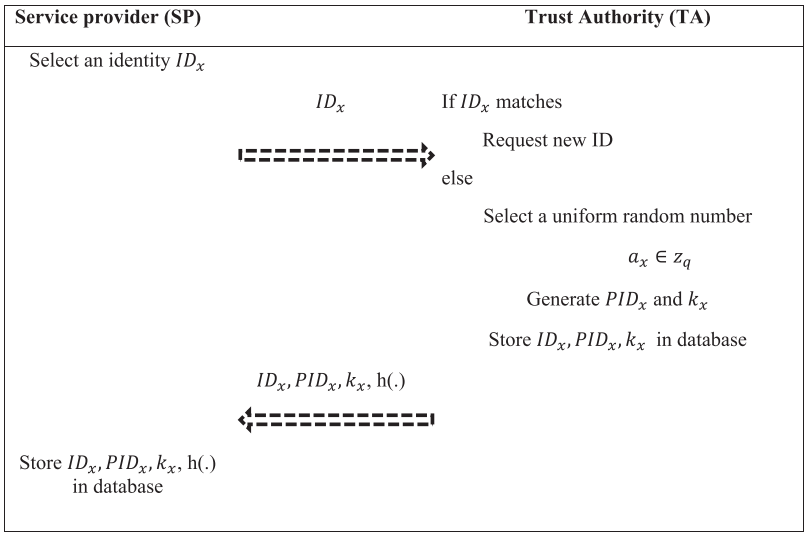

Figure 6: Dynamic update process

5 Result and Discussion

The proposed model performance is evaluated by cross verifying the features of the authentication process. This informal security analysis checks whether the system satisfies the security attributes and functionalities. For this, the parameters like Mutual authentication, Session Key Agreement, Untraceability, Anonymity, Availability, Robustness are considered.

- Mutual authentication: In the proposed approach, the trust authority authenticates the message T_1, a_tq, m_{1_i}, FID_y, PID_x received from the user u_i through the condition $m'_{1_i} = m_{1_i}$. Similarly, the service provider also authenticates the message a_op, T_3, Aut_y through the condition $m'_{3_i} = m_{3_i}$. The user also computes Aut_y and verifies whether the received Aut_y is equal to Aut_x. From this, it is clear that mutual authentication is obtained in the proposed model.
- Session Key Agreement: In the proposed work a session key $sk_y = h(ID_y||a_oz_xp||a_y||FID_x)$ is used. The session key is common for user and service provider

- Untraceability: The authentication step in the proposed work specifically selects the timestamps, uniformly selected random numbers for each section which prevents the adversary to obtain the relationship between the user and service provider.
- Anonymity: In the proposed work, to preserve the user anonymity, user and service provider identities are kept safe from an adversary $\mathcal{A}$. Since the communication model uses encrypted text on the public channel while requesting access. Also, the utilization occurrence of identities is used in the registration phase only after pseudo identities are used for further communication. This depicts that the proposed communication model maintains the anonymity of the adversary.
- Availability: In order to prevent access to the authorized user, adversary $\mathcal{A}$ send flooding messages which may increase the computation overhead to the system. This leads to denial of service to the user. In the proposed communication model, before accepting the communication request, the user authentication request is verified using a scalar multipoint elliptical curve multiplication operation. Also, to ensure the freshness of the messages timestamps are used in the proposed work that avoids processing of old messages. In the authentication process, a random number is used that prevents the adversary $\mathcal{A}$ to submit repetitive messages.
- Robustness: The proposed communication model is robust to attacks such as Impersonation Attack, Known Session Key Attack, Replay Attack, Man-in-the-Middle Attack, Insider Attack, capture attacks. The utilization of session key, authentication key and its verification based on trust authority make the system robust against attacks.

The proposed model has been simulated in a Java environment and the JDK version is 1.8. Java cryptography library function is used in the experimentation. The system processor is an Intel i5 processor 3.5 GHz frequency and 16 GB RAM. Based on the NIST standard a 256-bit key length is considered for the experimentation. Security functionality features, computation cost and communication cost are compared with related works. From the results it is observed that proposed work attains better performance for all three parameters. Tab. 2 depicts the security feature comparison of the proposed work and existing works. 10 features are considered for analysis and it is observed that for all the ten features the proposed model responds and performs well than existing works.

Table 2: Security features comparison

Security features	Odelu et al. [27]	Abbasinezhad et al. [28]	Braeken et al. [29]	Khan et al. [30]	Proposed
Replay attack	✓	✓	✓	✓	✓
Anonymity	✓	✓	✓	✓	✓
Message authentication	✓	✓	✓	✓	✓
Impersonation attack	✓	✗	✓	✗	✓
Session key agreement	✓	✓	✗	✓	✓
Session key security	✓	✓	✗	✓	✓
Insider attack	✓	✗	✗	✓	✓
Man-in-the-middle attack	✓	✓	✓	✓	✓
Key freshness	✓	✓	✓	✓	✓
DoS attack	✗	✗	✓	✗	✓

The computation cost of the proposed model and existing models are compared and depicted in Fig. 7. It is observed that the proposed model attains minimum computation cost compared to existing methods. The simple authentication procedure followed in the proposed approach consumes minimum computation cost whereas the complex procedures in the existing works take more time for authentication which increases the computation cost.

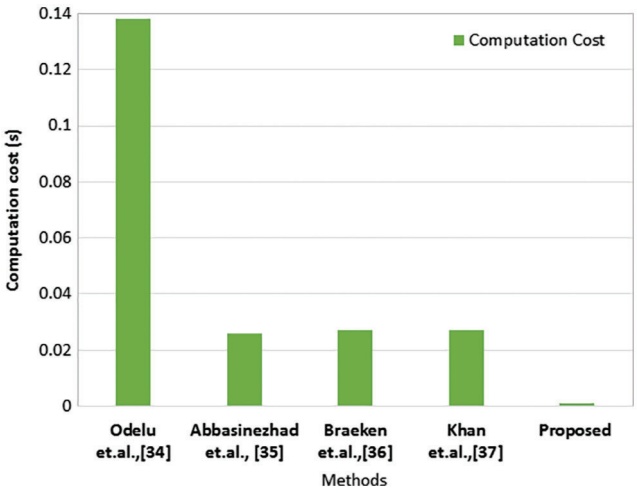

Figure 7: Comparison of computational cost

The communication cost for the proposed approach and existing approaches are compared and depicted in Fig. 8. Three messages are forwarded in the communication model to measure the communication cost in bits. It is observed from the analysis, existing methods exhibits more communication cost compared to proposed communication model. Due to the increased communication cost the overall performance also degrades in the existing works. However, in the proposed work due to minimum communication cost and computation cost the overall performance and efficiency of the system increases which makes the application suitable for dynamic environments.

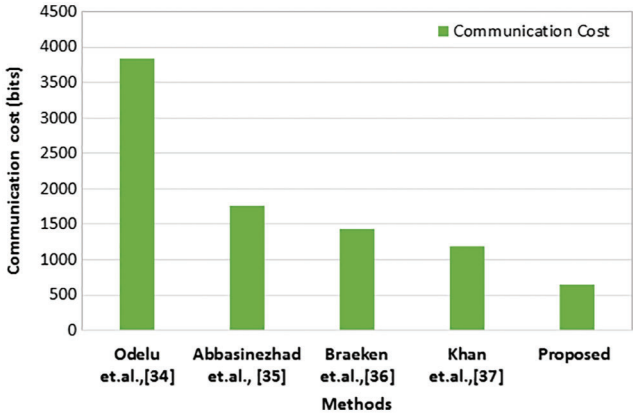

Figure 8: Comparison of communication cost

6 Conclusion

This research work presents an authentication and key agreement protocol for smart grid secure communication. The fast-mutual authentication and key agreement between user and service provider along with trust authority ensure that high security is provided for smart grid communication. The security features like Replay attack, Anonymity, Message authentication, Impersonation attack, Session key agreement, Session key security, Insider attack, Man-in-the-middle attack, Key freshness, Denial of Service (DoS) attack are analyzed and compared with existing works. Through simulation analysis, the communication cost and computation cost of the proposed model are evaluated. Results demonstrate that the proposed model attains better performance in all aspects and improves the overall efficiency of the system. In the future, the proposed model will be extended by introducing artificial intelligence to increase its feasibility and practicability.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Y. Fard, M. Hosseinzadehtaher, M. B. Shadmand and S. K. Mazumder, "Cyberattack resilient control for power electronics dominated grid with minimal communication," in *2021 IEEE 12th Int. Symp. on Power Electronics for Distributed Generation Systems (PEDG)*, Chicago-USA, pp. 1–6, 2021.

[2] M. Ghorbanian, S. H. Dolatabadi, M. Masjedi and P. Siano, "Communication in smart grids: A comprehensive review on the existing and future communication and information infrastructures," *Ieee Systems Journal*, vol. 13, no. 4, pp. 4001–4014, 2019.

[3] U. Zafar, S. Bayhan and A. Sanfilippo, "Home energy management system concepts, configurations and technologies for the smart grid," *Ieee Access*, vol. 8, pp. 119271–119286, 2020.

[4] Q. Zhou, M. Shahidehpour, A. Paaso, S. Bahramirad, A. Alabdulwahab *et al.,* "Distributed control and communication strategies in networked microgrids," *Ieee Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2586–2633, 2020.

[5] M. Ghorbanian, S. H. Dolatabadi and P. Siano, "Big data issues in smart grids: A survey," *Ieee Systems Journal*, vol. 13, no. 4, pp. 4158–4168, 2019.

[6] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems," *Ieee Access*, vol. 7, pp. 46595–46620, 2019.

[7] M. H. Shawon, S. M. Muyeen, A. Ghosh, S. M. Islam and M. S. Baptista, "Multi-agent systems in ict enabled smart grid: A status update on technology framework and applications," *Ieee Access*, vol. 7, pp. 97959–97973, 2019.

[8] Y. Saleem, N. Crespi, M. H. Rehmani and R. Copeland, "Internet of things-aided smart grid: Technologies, architectures, applications, prototypes, and future research directions," *Ieee Access*, vol. 7, pp. 62962–63003, 2019.

[9] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *Ieee Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.

[10] C. Peng, H. Sun, M. Yang and Y. Wang, "A survey on security communication and control for smart grids under malicious cyber attacks," *Ieee Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1554–1569, 2018.

[11] M. Biagi, S. Greco and L. Lampe, "Geo-routing algorithms and protocols for power line communications in smart grids," *Ieee Transactions on Smart Grid*, vol. 9, no. 2, pp. 1472–1481, 2018.

[12] J. The and C. Lai, "Reliability impacts of the dynamic thermal rating system on smart grids considering wireless communications," *Ieee Access*, vol. 7, pp. 41625–41635, 2019.

[13] A. Ghosal and M. Conti, "Key management systems for smart grid advanced metering infrastructure: A survey," *Ieee Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2831–2848, 2019.

[14] S. Hsieh and C. Lai, "A novel scheme for improving the reliability in smart grid neighborhood area networks," *Ieee Access*, vol. 7, pp. 129942–129954, 2019.

[15] J. Ni, K. Zhang, X. Lin and X. Shen, "Balancing security and efficiency for smart metering against misbehaving collectors," *Ieee Transactions on Smart Grid*, vol. 10, no. 2, pp. 1225–1236, 2019.

[16] S. Khan, R. Khan and A. H. Al-Bayatti, "Secure communication architecture for Dynamic energy management in smart grid," *IEEE Power and Energy Technology Systems Journal*, vol. 6, no. 1, pp. 47–58, 2019.

[17] E. Ahene, Z. Qin, A. K. Adusei and F. Li, "Efficient signcryption with proxy Re-encryption and its application in smart grid," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9722–9737, 2019.

[18] S. Hussain, I. Ullah, H. Khattak, M. Adnan, S. Kumari *et al.*, "A lightweight and formally secure certificate based signcryption with proxy Re-encryption (CBSRE) for internet of things enabled smart grid," *IEEE Access*, vol. 8, pp. 93230–93248, 2020.

[19] S. A. Chaudhry, H. Alhakami, A. Baz and F. Al-Turjman, "Securing demand response management: A certificate-based access control in smart grid edge computing infrastructure," *IEEE Access*, vol. 8, pp. 101235–101243, 2020.

[20] F. Wu, L. Xu, X. Li, S. Kumari, M. Karuppiah *et al.*, "A lightweight and provably secure Key agreement system for a smart grid with elliptic curve cryptography," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2830–2838, 2019.

[21] D. Abbasinezhad-Mood, A. Ostad-Sharif, M. Nikooghadam and S. M. Mazinani, "A secure and efficient Key establishment scheme for communications of smart meters and service providers in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1495–1502, 2020.

[22] H. Yang, S. Liu and C. Fang, "Model-based secure load frequency control of smart grids against data integrity attack," *IEEE Access*, vol. 8, pp. 159672–159682, 2020.

[23] Y. Li, P. Zhang and R. Huang, "Lightweight quantum encryption for secure transmission of power data in smart grid," *IEEE Access*, vol. 7, pp. 36285–36293, 2019.

[24] Y. Zhang, J. Wang and B. Chen, "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 623–634, 2021.

[25] K. Khanna, B. K. Panigrahi and A. Joshi, "Priority-based protection against the malicious data injection attacks on state estimation," *IEEE Systems Journal*, vol. 14, no. 2, pp. 1945–1952, 2020.

[26] J. L. Tsai and N. -W. Lo "Secure anonymous key distribution scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 906–914, 2016.

[27] 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, 2018.

[28] A. Abbasinezhad-Mood and M. Nikooghadam, "An anonymous ECC-based selfcertified key distribution scheme for the smart grid," *IEEE Trans. Ind. Electron*, vol. 65, no. 10, pp. 7996–8004, 2018.

[29] Braeken, P. Kumar and A. Martin, "Efficient and provably secure key agreement for modern smart metering communications," *Energies*, vol. 11, no. 10, pp. 1–12, 2018.

[30] 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 Energy System*, vol. 121, pp. 1–16, 2020.