International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Secured Elliptic Curve Cryptography Authentication Scheme for Advanced Metering Infrastructure Communication

Otisitswe Kebotogetse*[1], Ravi Samikannu[2], Abid Yahya[3]

Submitted: 27/01/2024 **Revised**: 05/03/2024 **Accepted**: 13/03/2024

Abstract*:* Advanced Metering Infrastructure (AMI) has been a key element in upgrading the Smart Grid. The smart meter as one of the components of the AMI system allows the system to take measurements in the real-time resulting in a more efficient energy use and also good load balancing. Securing the smart meter's cyber-security is vital as a compromise will lead to serious problems affecting millions of users. This paper proposes an Elliptic Curve Authentication Scheme (ECCAS) method that is light-weight and utilizes bilinear map method to form an ideal elliptic curve. Furthermore, it improves the concealed-based method designed in NS2 environment and the proposed method to show the light-weight characteristic. Results show that total consumed energy by the nodes has been reduced by 6%, throughput increased by 4% and packets dropped reduced by 2%. All these results show a slight difference in computational costs to prove that the proposed method is light-weight and can safely be used in AMI subsystem.

Keywords: *Advanced Metering Infrastructure, Elliptic Curve Authentication Scheme, Elliptic Curve Cryptography, Smart Grid, Smart Meter*

1. Introduction

Communication technology and advanced digital information in the power grids have enhanced their efficiency. Through these enhancements, the original power grid is now known as the Smart Grid [1]. Using recent technologies, electricity is difficult to store in large quantities, unlike water or gas. Power production has to be balanced with the demand side for easy storage, which is done by the power grids [2]. The components of the smart grid, such as Phasor Measurement Unit (PMU) and AMI help to perform the roles of the smart grid. Smart meters are deployed to ensure smart load balancing, thus making sure that production meets demand not having to deal with large storage of electricity. Smart meters are part of the AMI. They provide a two-way communication between the utility provider and consumers [3]. The role of the smart meters enables monitoring of power consumption, load forecasting and control. The benefits include cost savings and reducing emissions of carbon-dioxide into the atmosphere [4]. While it is visible that the smart grid benefits electricity production and distribution, there are some privacy concerns related to it. Security in the smart grid is vital [5], and smart meters, one of the essential elements, must be protected. Some of the attacks associated with the components of the smart grid are the Denial of Service (DoS) attack[6], the impersonation attack, Man In the Middle (MITM) attack and the replay attack [7]. The reasons for Intruders range from trying to steal electricity, tempering with customer billing information or even taking over the grid control based on political grounds. The proposed method in the paper improves the scheme of CBSS in [8]. The scheme is improved by proposing an ECCAS lightweight scheme, utilising bilinear map for curve formation. The schemes are simulated in NS2 environment and comparison of their performance is made based on networking parameters. Results show that the ECCAS scheme gives better performance than CBSS. The rest of the paper is structured as follows: Section 2 explains the ECC method and compares different methods from the past. Section 3 describes the methodology of the proposed scheme. Section 4 shows how the scheme is developed on the software. Section 5 presents the results and discussion, it shows the improved computational times of ECCAS. Section 6 gives the conclusion of the paper.

2. Elliptic Curve Cryptography

The Elliptic Curve Cryptography (ECC) method is an example of an asymmetric algorithm that encodes and decodes using various keys [9]. The method was invented in 1985 by [10]. ECC method consumes less energy, making it ideal to use devices that work with the energy conservation characteristic. One of the main advantage of the method is that it works with small key lengths, resulting in faster encoding and decoding processes. The disadvantage is that ECC method induces size of ciphered text, making the method more complex. However, the method still provides less complexity when compared to other security algorithms like Advanced Encryption Standard (AES) [11].

The core feature of the ECC method is its different computational problems like the ECDLP (Elliptic Curve Discrete Logarithm Problem)[12]. No polynomial time algorithms are needed in the ECC to find computational problems.

[1] *Botswana International University of Science & Technology, Botswana ORCID ID : 0000-0002-9653-5223*
[2] *Botswana International University of Science & Technology, Botswana ORCID ID : 0000-0002-6945-6562*
[3] *Botswana International University of Science & Technology, Botswana ORCID ID : 0000-0003-3741-8315*
** Corresponding Author Email: ko19100017@studentmail.biust.ac.bw*

Table 1. Data management and Security solutions analysis

Author	Description	Strength	Weakness
[11]	A secure routing protocol based on trust management for WSN (2020)	This plan improves data delivery and conserves electricity.	Route request answers cause increased overheads in the system.
[12]	A flexible energy management system that makes use of smart meters (2020)	The process reduces billing information for clients while saving electricity.	The method compromises the security of AMI.
[13]	A Scalable Data Aggregation Method working on the Smart Grid using Elliptic Curves (2020)	The Scheme is scalable, allowing adding or removing a meter from the system without going through a long process. A meter can convey numerous pieces of data at once.	The method bombards the meter with many computations during the multiple data-sending process.
[14]	A smart grid with Internet of Things integration that uses formal, yet lightweight, certificate-based encryption with proxy re-encryption (CBSRE) (2020)	The method uses a hyper-elliptic curve crypto-system. This uses 80 bits key size to reduce computational and communicational costs.	The method is not secure enough to be adopted by AMI communication.
[15]	Internet of Things-based smart energy management system (2021)	With the possibility to cut costs associated with consumption, the technique controls consumer consumption.	Data security is not considered in this method.
[16]	The Smart Grid: A Very Lightweight Mutual Authentication Scheme for Two-Way Communications (2021)	For each data transmission in the smart grid, the approach offers two-way communication and a secure one-time pad key. The plan increases computational and storage efficiency.	The method can be easily cracked as it has a simple encryption method.
[17]	KNN Classification Algorithm for Smart Grid with Privacy Preserving (2022)	The approach offers privacy and is adaptable to other Internet of Things (IoT) smart devices.	Denial of service assaults is a problem with the method, especially while reestablishing an internet connection.
[18]	Smart Grid's Anonymous and Efficient Message Authentication Scheme (2019)	The approach offers authentication and fixes Li's authentication scheme's flaws.	The method ignores communication costs.
[6]	Advanced Metering Infrastructure Security Using a Concealed Basis (2022)	The Scheme showed a reduction in the amount of energy the nodes use during communication and authenticates the communication in AMI.	The security considered is only for AMI communication. The method can be easily cracked as it has a simple encryption method.
Proposed Security Scheme	A Secure Elliptic Curve, Cryptography Authentication method, designed for AMI	The Scheme improved the security of the CBSS on the AMI network. It also showed a reduction in energy consumption by the nodes.	The method has more computations than the CBSS method, hence increased encryption and decryption times.

3. Methodology

The The Elliptical Curve Cryptography and fully hashing method are used to improve the CBSS [8]. The authentication server is located between the sensor and the user to act as credential authority. The initialization procedure comes first, during which the generator chooses the curve parameters. Curve points, prime numbers, curve factors, and defined prime pitch are some of these parameters. The security process is then launched after creating the bilinear map. In the following order, rotation groups (m), (n) and (o) are generated together with prime numbers. Prime numbers are the numbers that are divisible by one and themselves here.

$$choose\ m\ \ from\ 0-\ 998 \tag{1}$$

$$choose\ n\ \ from\ 0-\ 999 \tag{2}$$

$$choose\ o\ \ from\ 0-\ 1000 \tag{3}$$

$$If(m \neq n \text{ and } n\ \neq\ o \text{ and } m \neq\ o) \tag{4}$$

$If e(n, m+o) = e(m+o, n) and\ e(m+o, n)$ (5)

The purpose of rotation groups is to control the magnitude of the calculated numbers. Then, the values of **G (m), G (n),** and **G (o)** are updated. The numbers in the group are then either **a** or **b**, and **p** is then chosen and stored to the final group. The generators a and b are used to construct the map e after the prior processes have been completed. The values for the e map function are obtained from the computations of **(f-g)(f+g).** The prime number is determined, as can be seen below, with **i** being used as the number 2 as well since its value is smaller than **a**. Just like the groups, the members of **i** will be updated constantly. Prime occurs everytime if **a mod i** is equal to **1**. After selecting the prime numbers, they are stored to the table J_P . The random numbers R in the equation 6 below are selected from a range 0 to J_P

$$\boldsymbol{R = OS2IP(SHA1(J_P(R)))} \quad (6)$$

For the network to be more secure, multiple calculations and the generation of random numbers require the J (P) values. The one-way hash code, H (1)code, is also produced with the aid of the numbers. At the beginning of the network simulation, the meters, B (S), and G (W) establish a connection with the Credential Authority (CA), after which authentication occurs. Before delivering data, the network's sensors first send a control message. The interactions are handled after the meter authorization has been confirmed. Every time the meter makes contact, the key transmission and authentication processes are requested. The sensors transmit data about the sensed meter to the CA. A unique key U_{Key} and common key P_{Key} are generated if the server recognizes the meter. The inputs I_P such as (P_N, P_T, P_F, x,y) determine the curve points. After selecting , key U_{Key} and the key P_{Key} are generated. . The values of the curve's constants are **x** and the prime pitches are denoted by P_F , while the elliptic curve's point is denoted by P_T . These values are employed to produce the prime pitches and the elliptic curve point produce the pseudo-arbitrary numerical values and multi-factor calculations.

$$X = (S_{ID}, R) \quad (7)$$

$$U_{Key} = (D_P, X) \quad (8)$$

$$P_{Key} = (R, U_{Key}) \quad (9)$$

Later, the public key for the meter, P_{Key} , is produced in reference to the curve P_T . The basic parameter of the elliptic curve, D_P , is employed.

The meter channel receives the generated key K pair. The process is done repeatedly for all the devices.

$$K = (U_{Key}, M) \rightarrow M_{ID} \quad (10)$$

The credential authority checks for uniqueness and re-creates the identity M_{ID} if it is not unique. Devices' mutual recognition is created when the sharing of key between the C_{RA} and the sensor is done. Public key and private key are used for the data transmission.

When M and G_W are mutually recognized, the prime number R is chosen from the resulting curve.To determine the time-cast T_C , R and other parameters are multiplied by the generator point. The present time, C_T , is the same as this.

$$C_T = T_C \quad (11)$$

$$G_K = (R, S_P, T_{SM})(G_{WR}, G_P) \quad (12)$$

G_K is the name of the private key for the gateway. M creates a random number. This is called R→M_R. It is deduced from the J_P numbers and computed as N. Taking $N\ as\ (I_P M_R)$.

$$G_{Wr} = OS2IP(SHA1(N)) \quad (13)$$

$$G_{WR} = I_P G_{Wr} \quad (14)$$

$$G_P = P_{Key}(M_R) \quad (15)$$

$$S_P = P_{Key}(G_P) \quad (16)$$

The gateway public key is called G_P. The random number associated with the gateway is called G_{WR} . The two hash values f and g are calculated as shown by equations 17 and 18. S_P represents the public key of the smart meter.

$$f = H_1(R, S_P, G_{WR}, G_P, T_{CS}, T_{GW},) \quad (17)$$

$$g = H_1(G_{WR}, R, S_P, G_P, T_{GW}, T_{CS}) \quad (18)$$

The nearby gateway of the sensor verifies the number formed by the bilinear map in the group, along with the time the sensor transmitted the message and time T_{CS}, each time a connection is made in the network. The number is chosen at random from new new $G_{WR} \in S_P$, and the elliptic curve point multiplication method is used to determine the matching R. Upon completion of this process, time T_{GW} is denoted and is known as gateway time. Then compute $(R + f^2)$ % v and $S_{GW}(G_{WR} + g\ G_P)$, they are, respectively, the new meter and additional value for I_{GW} . The reverse authentication code(I_{GW} , T_C, G_{WR}) is the secondary hash value H_2 of S_P .

$$S_{GW} = (g + G_{WR}) f \% \text{ v} \quad (19)$$

$$I_{GW} = S_{GW}(R + f S_P) \quad (20)$$

R and T_C are delivered to the end device once the process of validation has been established. The tool validates T_C and R. After successful verification, the device multiplies the generator point by the number it randomly selects from the P_N curve, G_{WR} .

Time T_{GW} is projected as the current time-stamp. For (f_{SM} , G_{WR}), S_P and G_{WR} are identified for all end devices. When using R, G_{WR} , S_P , G_P , T_{CS} , and T_{GW} as inputs, f and g are calculated by single-way hash function.

S_{GW} , $G_{WR} + gf_{GW}$ is calculated as percentage of v, where v is equal to the point of curve. S_{GW} and I_{GW} are the common parameters of the two end devices. H_2 (I_{GW} , T_C , f_{GW} G_{WR}) is the final validation code. The other end device receives the value for verification of correctness of the system security. The ownership of T_{GW} and G_{WR} is confirmed here by this device. Upon successful verification, reverse transmission parameters are calculated. These parameters are taken from the hash function of f and g inputs R, G_{WR} , S_P , G_P , T_{CS} and T_{GW} .

S_{GW} and I_{GW} are measured as follows, $R + ff_{SM}$ %v and S_{MR} ($G_{WR} + gS_P$)) respectively. The reverse validation code of the following I_{GW} , T_{CS} , G_{WR} is computed from the secondary hash value of G_P .

A comparison of the secure validation code and the reverse authentication code is made. The connection is hold until all devices are verified if a match is found. After a verification is successful the shared key function is provided, with I_{SM}, T_{CS} , and T_{GW} for the session's key generating entries.

The second level hashed value computes the authentication meter that has been secured such as H_2 (I_{SM}, T_{CS} , $f_{SM}R$) and to complete the agreed validation process, the generated value is transferred. At the receiver, the authentication meter that is secured is re- generated as a second level hashed value of the H_2 (I_{GW}, T_{GW} , RS_P).

The secondary hash value I_{SM} is calculated, then H_2 , T_{CS} , $f_{SM}R$, and also the hash are made available to finish the process of mutual secure validation. The device then re-generates the code of validation after receiving the data.

When the code generated is the same as the one received, then the transmitted device is said to be successfully checked. Shared keys are generated as inputs with I_{GW}, T_{SM}, and T_{GW} entries by the use of the key derivative function. The processes of encryption and decryption are executed by the shared key when data transmission occurs.

Algorithm 1: Elliptic Curve Cryptography Authentication Scheme (ECCAS)

The algorithm described in the document is a cryptographic protocol based on Elliptic Curve Cryptography (ECC). The protocol involves several steps: initialization, security process, map construction, random number generation, authentication, key generation, mutual recognition, forwarder selection and algorithm flow, verification, mutual validation, and shared key function. Here is a more mathematical representation of the protocol:

1. **Initialization**:
    - Let E be an elliptic curve over a finite p, where p is a prime number.
    - Let G be a generator point on E.
    - Let n be the order of G, and n is a large prime number.
2. **Security Process**:
    - Generate a cyclic group Zn of order n.
    - Select a random integer a from Zn.
3. **Map Construction**:
    - Construct a bilinear map $e: E \times E \rightarrow Fp$ such that for all points P,Q ,R on E and all integers a,b , we have

$$e(aP + bQ, R) = e(P, R)^a \cdot e(Q, R)^b$$

4. **Random Number Generation**:
    - Generate a random number R from Zn.
5. **Authentication Process**:
    - Let CA be the credential authority.
    - Let S be a sensor that sends a message M to CA.
    - If CA authenticates S, it generates a unique key $U(K)$ and a common key $P(K)$.
6. **Key Generation**:
    - Generate the public key for the meter, $P(K) = aG$, where a is the private key.
    - Send the key pair $P(K)$, to the meter channel.
7. **Mutual Recognition**:
    - Share keys between the credential authority CA and the sensor S for data transmission.
8. **Forwarder Selection and Algorithm Flow**:
    - Choose a prime number R from Zn.
    - Determine the time-cast $T(C)$.
    - Calculate two hash values f and g using a one-way hash function.
9. **Verification**:
    - Verify the random number in the group and the bilinear map formed, along with the time the sensor transmitted the message.
    - Choose a random number from new $G(WR) \in S(P)$, and use the elliptic curve point multiplication method to determine the matching R.

10. **Mutual Validation Process**:

    - Compute the reverse authentication code and the secure validation code and compare these two codes. If they match, the connection is held until all devices are verified.

11. **Shared Key Function**:

    - After successful verification, provide the shared key function, which uses the $I(SM)$, $T(CS)$, and $T(GW)$ entries for the session's key-generating entries. Encryption and decryption processes are then executed by the shared key when data transmission occurs.

This is a high-level mathematical representation of the protocol. Each step would involve more detailed mathematical operations and computations. The protocol uses advanced cryptographic techniques to ensure secure and authenticated data transmission. The validation and verification steps ensure that only authenticated devices can communicate, enhancing the network's security.

The work is an addition to the work done in [8]. This work makes an addition to improve the security of advanced metering infrastructure by adding the ECCAS method to the already developed two methods AMI Data Communication Scheme (ADCS) and Concealed Based Security Scheme (CBSS). Most of the development work was done in [8], published in IEEE Access journal.

4. Prototype Development

The proposed scheme and other comparison methods were simulated using Network Simulator-2 (NS 2), a simulation tool for modelling networks [21]. The software resembles real life structure network components like routers, servers e.t.c [21]. NS 2 supports Object Oriented Tool Command Language (OCTL) and C++ language [22].
The selected scenario in the environment of NS2 given in Table 2 resulted in the figures 1-3. The area of the network is 500m by 500m and the simulation time for each cycle is 200 seconds. The Advanced Metering Infrastructure environment is to be resembled. The paper shows the performance results of three different security methods in AMI. The graphs in figures 1-3 analyse the results from the simulations, and certain parameters were considered. The Advanced On Demand Vector (AODV) routing protocol is employed, and the antenna is the Omni Antenna, which is widely used in the NS 2 environment. Compared to other routing protocols, this routing system has demonstrated the ability to carry data more quickly.

Table 2: Parameters of Simulation of the 3 different security schemes

Parameters	**Values**
Simulation Time	200 (s)
Size of field	500 by 500 (m^2)
Channel	Wireless
Antenna	Omni Antenna
MAC type	Mac/802.11
Routing Protocol	Advanced On Demand Vector (AODV)
Number of Nodes	Variable

Four network environments were considered:

- Scenario 1: 101 nodes for each method.
- Scenario 2: 150 nodes for each method.
- Scenario 3: 200 nodes for each method.
- Scenario 4: 250 nodes for each method.

The measured parameters are total energy consumed, number of packets dropped and the throughput. The parameters here are measured to compare the three methods of ADCS, CBSS and ECCAS in AMI communication.
The number of dropped packets: Dropped packets are data packets sent during data transmission but do not reach the destination location, the receiver nodes here. The transmitter sends the packets but they are dropped in the network and not reaching the destination nodes [23]. The major contribution to dropping of packets is associated with network congestion. Packet drop also affects the throughput in the network. This signals a bad communication network. It is expressed by:

Total number of packets transmitted by all sending nodes - the total number of packets received by all receiving nodes = the number of dropped packets (21)

Total energy consumed: The total energy consumed combines three types of energy. The energy of transmitting (E_T), energy used during computation (E_C), and energy used during reception (E_R) [24]. Energy is seen to be consumed more during E_T and E_R. E_C energy is less [25]. Total energy consumed can be expressed by:

Total energy consumed = $E_T + E_C + E_R$ (22)

Throughput: This is the total number of data packets transmitted from the sender to receiver in a unit time. It is measured using bytes/second. This parameter is badly affected by topology change, low energy, low bandwidth and bad node communication. Throughput can be expressed by:

Throughput = Size of file / Time for transmission (23)

5. Results and Discussion

A Figure 1 demonstrates that as the number of nodes grows, the total number of packets dropped rises until a large number of nodes are in the network area. The number of packets dropped started to drop from 200 nodes for every method and this is indicated by the software giving an error during simulation of more than 200 nodes. The ECCAS scheme provides better packet dropping than other methods during the transmission of data. As security is increased in the network less packets are being lost. The packet dropping of the 3 methods shows a huge difference between 150 to 200 nodes. After the 200 nodes they all go down as the area can no longer take extra nodes. From the simulation results at 200 nodes, ADCS dropped 39% of packets, CBSS dropped 37% of packets and ECCAS dropped 35% of packets. The three techniques' different levels of security are

to blame for this. The ADCS approach is more impacted by the attacks than are the other two systems. Since the ADCS lacks an authentication procedure, it is inescapably open to network attacks.

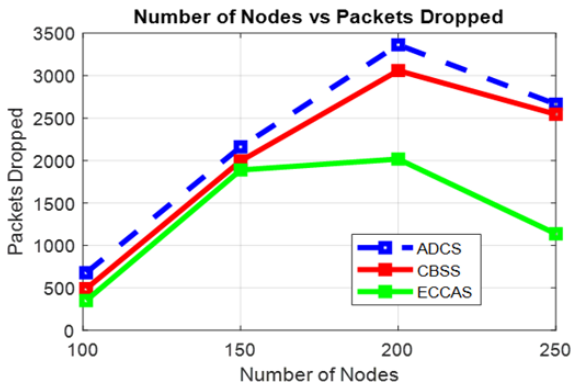

Fig 1: Varying number of nodes on: the total number of dropped packets at transmission process

Figure 2 demonstrates that energy usage is higher for low security approaches and lower for methods that increase network security. At 150 nodes, the simulation of ADCS revealed a 31% energy consumption, the simulation of CBSS revealed a 27% energy consumption, and the simulation of ECCAS revealed a 21% energy consumption. In all three approaches, the network is exposed to certain attacks, such as replay attacks, during transmission. This is one of the causes of increased energy use for less secure techniques like ADCS. There is evidence that making the system more secure reduces the quantity of bogus data traffic in the AMI network, which reduces the consumption of energy by sensing nodes [26].

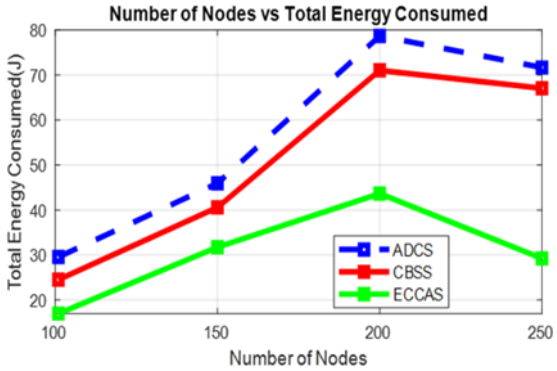

Fig 2: Varying number of nodes on: Total Energy Consumed at transmission process

Figure 3 shows throughput in ECCAS giving better results than that of the two other methods CBSS and ADCS. The difference in the throughput in terms of percentage between ECCAS and CBSS is around 4% and ECCAS and ADCS is around 9%. Reliability between communication nodes is one of the impact factors on throughput, resulting on the difference. Network congestion can also be one of the contributing factors, when the congestion is seen to be more, bandwidth is affected, and this leads to throughput being reduced. Low energy also badly impacts throughput. When energy is consumed more, less remains, making the network's throughput low.

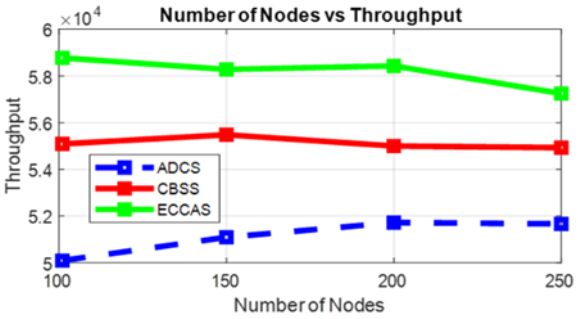

Fig 3: Impact of a varying number of nodes on throughput at transmission process

6. Conclusion

This paper has developed a secure elliptic curve cryptography authentication scheme for AMI. The proposed plan enhances the security of the previous work of AMI communication using a concealed-based approach. Comparing the proposed scheme and other methods shows an improvement in throughput, packets dropped, and energy consumed by the nodes during transmission. Throughput has been improved by 4% from CBSS method. Packets dropped have been improved by 2%, and total energy consumed improved by 6%. The ECCAS method proved to be a better security method for AMI communication providing lightweight characteristics compared to CBSS and ADCS methods. The introduction of this method to the designed AMI network was to give the network a more secure communication environment better than that in the CBSS method. The method provides security with consideration of the low computational ability characteristic of smart meters. This is a very important aspect usually ignored by most of the previous works that provide security to the AMI and the smart grid. The proposed method can be improved by introducing attacks to the system and testing the impact of attacks on the network against other security methods.

Declarations

Data Availability: The data will be provided based on the request from the readers.

Declaration of Competing Interest: The authors have no conflict of interest to declare.

Funding: The research received funding from the Botswana International University of Science and Technology (BIUST) Postgraduate Research Grant under Project Code: S00172**.**

References

[1] G. Rahman, M. F. Bin, R. Chowdhury, A. Al Mamun, R. Hasan, and S. Mahfuz, "Summary of Smart Grid : Benefits and Issues," *Int. J. Sci. Eng. Res.*, vol. 4, no. 3, pp. 1–7, 2013, [Online]. Available: http://www.ijser.org.

[2] Archana, R. Shankar, and S. Singh, "Development of smart grid for the power sector in India," *Clean.*

Energy Syst., vol. 2, p. 100011, 2022, doi: https://doi.org/10.1016/j.cles.2022.100011.

[3] P. Rai, A. Mishra, and A. Lal, "Smart Grid and IEC 61850," in *2021 International Conference on Intelligent Technologies (CONIT)*, 2021, pp. 1–6, doi: 10.1109/CONIT51480.2021.9498555.

[4] F. Syed and A. Ullah, "Estimation of economic benefits associated with the reduction in the CO2 emission due to COVID-19," *Environ. Challenges*, vol. 3, p. 100069, 2021, doi: https://doi.org/10.1016/j.envc.2021.100069.

[5] M. Z. Gunduz and R. Das, "Analysis of cyber-attacks on smart grid applications," *2018 Int. Conf. Artif. Intell. Data Process. IDAP 2018*, no. March, pp. 1–5, 2019, doi: 10.1109/IDAP.2018.8620728.

[6] O. Kebotogetse, R. Samikannu, and A. Yahya, "A Concealed Based Approach for Secure Transmission in Advanced Metering Infrastructure," *IEEE Access*, vol. 10, pp. 84809–84817, 2022, doi: 10.1109/ACCESS.2022.3195240.

[7] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow, "Elliptic Curve Cryptography in Practice."

[8] O. G. Abood and S. K. Guirguis, "A Survey on Cryptography Algorithms," *Int. J. Sci. Res. Publ.*, vol. 8, no. 7, 2018, doi: 10.29322/ijsrp.8.7.2018.p7978.

[9] M. Faheem, S. Jamel, A. Hassan, Z. A., N. Shafinaz, and M. Mat, "A Survey on the Cryptographic Encryption Algorithms," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 11, 2017, doi: 10.14569/ijacsa.2017.081141.

[10] S. D. Galbraith and P. Gaudry, "Recent progress on the elliptic curve discrete logarithm problem," *Des. Codes Cryptogr.*, vol. 78, no. 1, pp. 51–72, 2016, doi: 10.1007/s10623-015-0146-7.

[11] W. Fang, W. Zhang, W. Chen, Y. Liu, and C. Tang, "TMSRS: trust management-based secure routing scheme in industrial wireless sensor network with fog computing," *Wirel. Networks*, vol. 26, no. 5, pp. 3169–3182, 2020, doi: 10.1007/s11276-019-02129-w.

[12] N. T. Mbungu, R. C. Bansal, R. M. Naidoo, and M. Bettayeb, "A dynamic energy management system using smart metering," *Appl. Energy*, vol. 280, no. October, p. 115990, 2020, doi: 10.1016/j.apenergy.2020.115990.

[13] Y. Chen, J. F. Martinez-Ortega, P. Castillejo, and L. Lopez, "An Elliptic Curve-Based Scalable Data Aggregation Scheme for Smart Grid," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2066–2077, 2020, doi: 10.1109/JSYST.2019.2954080.

[14] S. Hussain *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, doi: 10.1109/ACCESS.2020.2994988.

[15] M. U. Saleem, M. R. Usman, and M. Shakir, "Design , Implementation , and Deployment of an IoT Based Smart Energy Management System," pp. 59649–59664, 2021, doi: 10.1109/ACCESS.2021.3070960.

[16] S. Aghapour, M. Kaveh, M. R. Mosavi, and D. Martin, "An Ultra-Lightweight Mutual Authentication Scheme for Smart Grid Two-Way Communications," *IEEE Access*, vol. 9, pp. 74562–74573, 2021, doi: 10.1109/ACCESS.2021.3080835.

[17] Z. Song, Y. Ren, and G. He, "Privacy-Preserving KNN Classification Algorithm for Smart Grid," vol. 2022, 2022.

[18] L. Wu, J. Wang, S. Zeadally, and D. He, "Anonymous and Efficient Message Authentication Scheme for Smart Grid," vol. 2019, 2019.

[19] T. Issariyakul and E. Hossain, *Introduction to Network Simulator NS2*. 2009.

[20] V. Odelu, A. K. Das, S. Kumari, X. Huang, and M. Wazid, "Provably secure authenticated key agreement scheme for distributed mobile cloud computing services," *Futur. Gener. Comput. Syst.*, vol. 68, no. C, pp. 74–88, 2017, doi: 10.1016/j.future.2016.09.009.

[21] M. F. Khan, E. A. Felemban, S. Qaisar, and S. Ali, "Performance analysis on packet delivery ratio and end-to-end delay of different network topologies in wireless sensor networks (WSNs)," *Proc. - IEEE 9th Int. Conf. Mob. Ad-Hoc Sens. Networks, MSN 2013*, pp. 324–329, 2013, doi: 10.1109/MSN.2013.74.

[22] A. Saravanaselvan and B. Paramasivan, "Implementation of an Efficient Light Weight Security Algorithm for Energy-Constrained Wireless Sensor Nodes," *Circuits Syst.*, vol. 07, no. 09, pp. 2234–2241, 2016, doi: 10.4236/cs.2016.79194.

[23] M. A. Hamid and C. S. Hong, "Energy conserving security mechanisms for wireless sensor networks," *Ann. des Telecommun. Telecommun.*, vol. 64, no. 11–12, pp. 723–734, 2009, doi: 10.1007/s12243-009-0088-z.

[24] S. Randhawa and S. Jain, "An intelligent PSO-based energy efficient load balancing multipath technique in wireless sensor networks," *Turkish J. Electr. Eng. Comput. Sci.*, vol. 25, no. 4, pp. 3113–3131, 2017, doi: 10.3906/elk-1606-206.