A secure SHA-MECC based privacy preserving data aggregation system with fault tolerance for smart grids

Mrs.Shyma S, Assistant Professor, BMCE, Sasthamcotta

Mrs.Sujatha S, Assistant Professor, BMCE, Sasthamcotta

Abstract: The smart grid (SG) concept has turned as a convergence of conventional power system engineering with the information and communication technology. To attain a clean, secure, resilient, and efficient system, a '2'-way communication technology and computational intelligence on an integrated style athwart electricity distribution, generation, transmission, along with consumption is used by the SG. Centred on the incessantly collected information as of the consumers, the power generation and pricing of SG are made. Thus, security acts as an important facet of it. This paper, to enhance the security, proposed a secure SHA-MECC centred privacy-preserving Data Aggregation (DA) system with fault tolerance for SG. The proposed work encompasses '3' phases i) system initialization, ii) DA, and iii) secure report reading and response. In the 1st phase, the parameters are initialized for further processing and the Residential user (RU) data using SHA-MECC is encrypted. Followed by which, the data is aggregated. Next, the final phase is implemented wherein the data is decrypted. Lastly, the proposed work's performance with that of the existent system is compared. The proposed system provides more security than the existent systems.

Key words: *Secure Hashing Algorithm-Modified Elliptic Curve Cryptography (SHA-MECC), Smart Meters (SMs), Control Center (CC), Trusted Certificate Authority (TCA), and Residential user (RU).*

1. INTRODUCTION

A concept that is closely associated with grid monitoring is Grid synchronization, which is an adaptive process [1]. Synchronization is the diminution of the variation in voltage, frequency in addition to phase angle amid the equivalent phases of the generator's output as well as grid supply [2]. The synchronization will be the primary thing required by any closed control system which can well be single or '3'-phase inverter that is linked to the grid. To produce the reference signal aimed at modulation, the synchronization method is used. There are

numerous synchronization techniques to produce the reference signal of the '3'-phase inverter linked with the grid [3–6], for instance, PLL [7].

Aimed at a single-phase supply, the linear Phase Locked Loop (PLL) is chiefly employed to detect phase. In terms of balanced '3'-phase supply, Synchronous References Frame (SRF) PLL is employed. But, the PLL does not detect phase aimed at unbalanced supply [8]. Thus, to handle unbalanced grid states, Decoupled-Double-SRF (DDSRF) PLL was employed [9], which is capable of detecting the positive sequence phase angle for this. DDSRF-PLL centred upon synthesis circuit was employed in [10] that is frequency-adaptive and could well be simply implemented.

Synchronization failure produces voltage deviation, transients in addition to redundant oscillations inside the network that cause disturbances in power system stability as well as lessens the general effectiveness. The generator might be disconnected as of taking load; in addition, the system gets stricken by means of unbalanced parameters [11]. Consequently, it is vital to generate synchronization, which is why there are disparate sorts of techniques to do so [12]. The connecting generator as well as the grid has to encompass the voltage magnitude, phase sequence, frequency, and phase angle intended for the synchronization process [13]. Disparate countries have disparate grid specifications for the generator synchronization with the main power stream [13].

Here, Section 2 offers surveys of the associated works regarding the proposed work. In sections 3, a concise discussion about the proposed methodology is presented; section 4 analyzes the Investigational outcome and section 5 conveys the conclusion of this paper.

2. RELATED WORK

Lanchao Liu *et al.* [14] recommended a technique called false data detection centred upon the parting of nominal power grid states in addition to anomalies. The nuclear standard minimization along with low-rank matrix factorization was designed to resolve the issues that occur in the electric power grid. This exhibited that the techniques were capable of identifying correct power system operation states; in addition, detect the malevolent attacks, even in the situation where the gathered measurement was partial. Numerical simulation outcomes of the synthetic in addition to real-data authenticated the mechanism's effectiveness.

Mohamed Amine Ferrag [15] exhibited an effective Privacy-Preserving (PP) energy expenditure system having updating certificates, termed EPEC, for safe SG communications. It encompassed '4' phases i) Gateways (GW) initialization, ii) party registration, iii) PP energy consumption, iv) updating certificates. With respects to transmission delay performance, an extensive performance evaluation was done to display the EPEC effectiveness. This evaluation included '3' sorts of curves i.e. the Barretos–Naehrig curve, the Kachisas–Schaefer–Scott curve, and the Barretos–Lynn–Scott curve.

Le Chen *et al.* [16] suggested a MuDA, which is a multi-functional DA scheme aimed at PP-SG communications. By means of MuDA, the SG control center (CC) was computed diverse statistical functions of data in a PP mean to offer diversiform services. In addition, MuDA handled the differential attack that most safe DA schemes suffer from. The approach elucidated via 'meticulous security as well as utility analyses' that MuDA preserved data privacy along with a tolerable noise rate. Wide-ranging performance evaluations were done. These exemplified the effectiveness of MuDA scheme to a renowned aggregation scheme with respect to communication overhead (CO).

Hongwei Li *et al.* [17] presented a competent scheme that employed homomorphic encryption for attaining PP demand aggregation as well as efficient response. Security examination implied that it attained PP of electricity requirement, forward privacy of session keys, as well as the evolution of private keys. It had enhanced efficiency regarding computation as well as CO with reference to an existent scheme that as well attained forward secrecy, and adaptively controls the key evolution for balancing the trade-off amid the communication effectiveness along with security level.

Lajos Török *et al.* [18] exhibited an adaptive PLL-centred grid-fault tolerant control. The corrected line voltage was synchronized with the inductor current. Trailing the phase angle of the corrected line voltage gave the likelihood to envisage the subsequent sampling value. The re-compensation error was brought about by means of the delays of sampling as well as modulation. The solution offered noise immunity aimed at the present controller to the line voltage conflict.

3. PROPOSED METHODOLOGY

A propitious approach that could solve the carbon emission along with the energy crisis issues is the SG. For the optimal use of energy, the power consumption data are gathered in

SG. Practically still, the security issue is present there during communication. This paper proposed a secure SG communication system based on the Secure Hashing Algorithm – Modified Elliptic Curve Cryptography (SHA-MECC) algorithm. The proposed work mainly comprises '3' parts: i) system initialization, ii) DA, and iii) secure report reading and response. The proposed methodology's block diagram is exhibited in Figure 1,

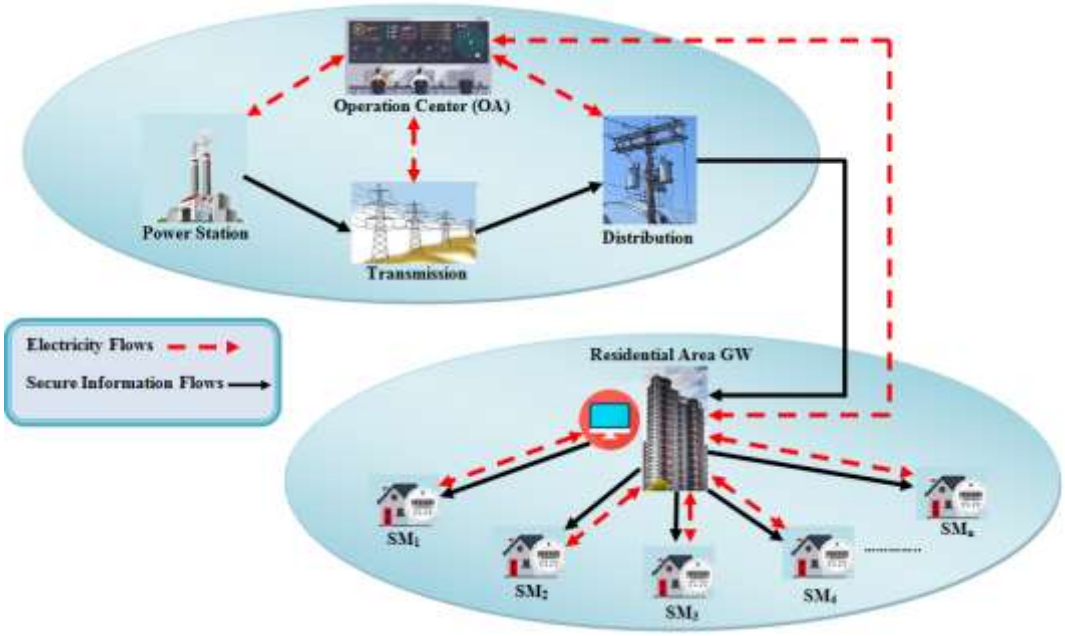

Figure 1: Structure for the proposed system

3.1 System Initialization

Here, the system is initialized, where the Trusted Certificate Authority (TCA) and CC plays an important role. In order to prudently equipoise the consumption between peak and off-peak periods, the CC contrives a better power generation plan. A certificate authority is basically an authentication server in grid. For the entire system, a sensible bootstrap would be the trusted Operation Authority (OA). The TCA and CC generate the associated parameters aimed at the operations so as to initialize the system. In this phase, the private key (pr_y), public key (pu_y), secret key (se_y) and the hash value of the public key $H((pu_y))$ are generated by the OA. Precedently to initialization, the CC sends a data collection request to the RU. The data collection of the RU is expressed as follows,

$$Ru_s = \{Ru_1, Ru_2, Ru_3, ..., Ru_n\} \quad (1)$$

Where, Ru_s denotes the residential users set and the Ru_n signifies the n-number of RU and the collected data from the RU is denoted as D_r. Then, the SM of the grid, by utilizing the SHA-MECC, encrypts the current electricity usage data and transmits the encrypted packet to the local-GW in RU. SMs stand as the vital components in SG that are deployed at the consumer's side to periodically record the energy consumption. Collecting the electricity usage data might contrive to the divulgence of user privacy-sensitive information that will lead to the user's privacy breach. The attackers could envisage the user's activities just by tapping the communication messages that take place between SMs and CC i.e., the individual's electricity demand. Thus, the RU data is encrypted in order to protect their privacy. The encryption using SHA-MECC is explained as follows,

The mechanism that is utilized for key generation acts as the main strength that the encryption technique depends-on in the cryptographic procedure. In the proposed methodology, three keys are generated, which are expressed in the below equations. The SHA 512 algorithm generates the hashed public along with the private key to get hash codes and these hash codes are utilized in the encryption as well as decryption process.

$$pu_y = pr_y * p_c \tag{2}$$

Here, p_c represents the Point on the Curve.

Secret Key:

Now, the se_y is created by summing the pu_y, pr_y and p_c , which is shown in the below equation,

$$se_y = pu_y + pr_y + p_c \tag{3}$$

Encryption (E_c):

After generating se_y, the values that are acquired from the RU are encrypted. The encrypted data encompasses '2' cipher texts, which are being mathematically depicted as given below.

$$C_1 = \left(\left(K := 1,2,.....(n-1)\right) * p_c\right) + se_y \tag{4}$$

$$C_2 = \left(D_r + \left((K := 1,2,.....(n-1)) * H(pu_y)\right)\right) + se_y \quad (5)$$

Here, C_1 and C_2 represents the '2' cipher texts, K is the random number generated in (1 to $n-1$) interval, D_r is the original data from the RU, $H\left(pu_y\right)$ represents the Hash value of Public key.

SHA 512 Algorithm:

Several computational procedures are performed here, which are visually exhibited in Figure 2. In order to form a multiple of 1024 bits, the message bits are being padded with the additional bits, which is then split into tiny parts of 1024 bits. The 1st block is connected to the initializing vector and the hash code is generated. The subsequent blocks are connected to the formerly generated hash codes. The SHA 512 algorithm's operation is exhibited in Figure 2,

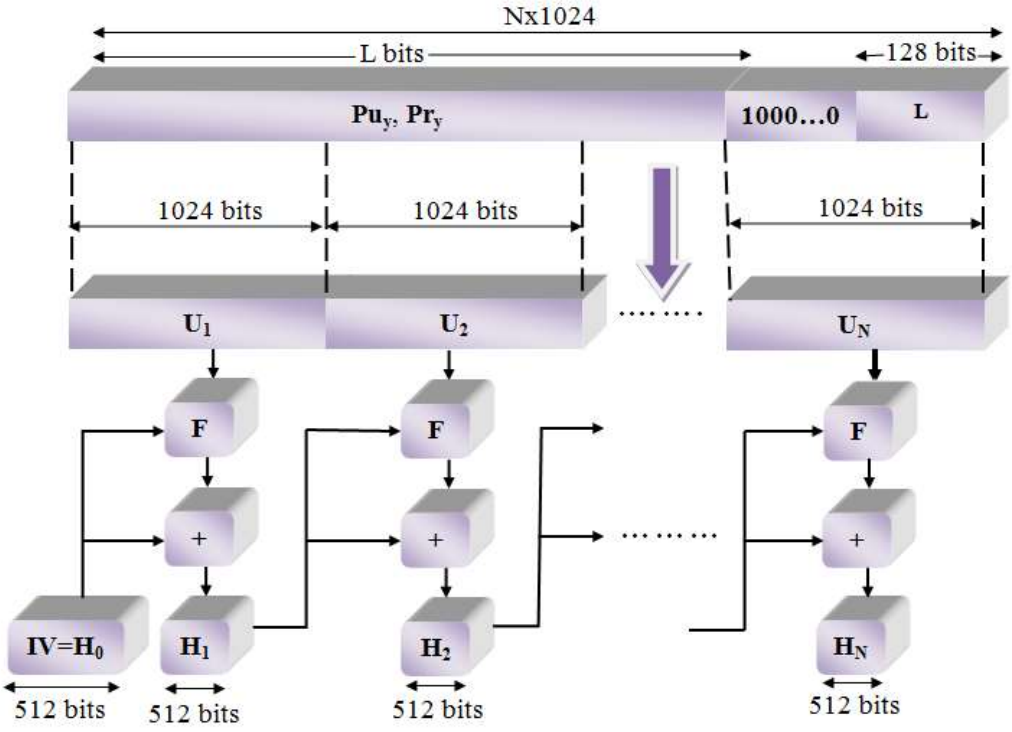

Figure 2: Illustration of the SHA 512 Algorithm

The proposed SHA-MECC's Pseudocode is portrayed in Figure 3,

Input: Residual user (Ru) data D_r

Output: Encrypted data E_c

Begin

Generate Public Key (pu_y), Private Key (pr_y), Secret Key (se_y)

for

//Encryption

$$C_1 := ((K := 1,2,3,.....n-1) * p_c) + se_y$$

$$C_2 := (D_r + (K := (1,2,3,.....n-1) * H(pu_y))) + se_y$$

//Decryption

$$D_r := ((((C_2 - H(pr_y)) * C_1) - se_y)$$

End

Figure 3: Pseudo code for the proposed SHA-MECC

3.2 Data aggregation

After encryption, the data of the RU are aggregated. For every η minutes, the real-time electricity usage data (almost) of the RU is gathered for getting a more precise power consumption style. For the authentication verification, the local-GW fixed the threshold value. The RU reports arrive at the GW, and it verifies the authentication. The GW aggregates the legitimate usage data, check if the flexible threshold can be met. And if it does, then GW forwards the encrypted aggregation data to the CC or else it stops the aggregation, and resends data requests to users. The checking condition of the aggregation is expressed as follows,

$$Ru_s \rightarrow GW_s : \{E_c \| T_h\} \tag{6}$$

Where, GW_s represents the gateway of the RU set, E_c denotes the encrypted data and T_h denotes the threshold value.

3.4 Secure report reading

Subsequent to receiving the data packets as of GW, CC authenticates the packet source and verifies the validity of the data. This is done to double-check its claims of coming as of the GW ($C(GW)$) as well as the data integrity. The checking condition is expressed as,

$$S_r \rightarrow E_c \| C(GW) \tag{7}$$

After verification, the CC decrypts the ciphertext and recovers the aggregated usage data of the Residential Area. Then, it can obtain the power consumption style centred on the almost real-time aggregation data without exposing the individual user data, and consequently, make the generation schedule as well as dynamic pricing accordingly. The decryption process is expressed as,

Decryption:

Here, se_y is added to two cipher texts.

$$D_r = \left(\left(\left(C_2 - H\left(pr_y\right)\right) * C_1\right) - se_y\right) \tag{8}$$

Where D_r signifies the original message. In the decryption process, the se_y is subtracted from the normal decryption equation.

4. RESULT AND DISCUSSION

In this section, the proposed privacy-preserving DA system centred on SHA-MECC performance is analyzed. The proposed work is employed in the MATLAB/Simulink. The proposed system's performance is compared with the existing Elliptic Curve Cryptography (ECC) based DA in the SG communication system with respect to computational cost and CO. The comparison is displayed in Figure 4,

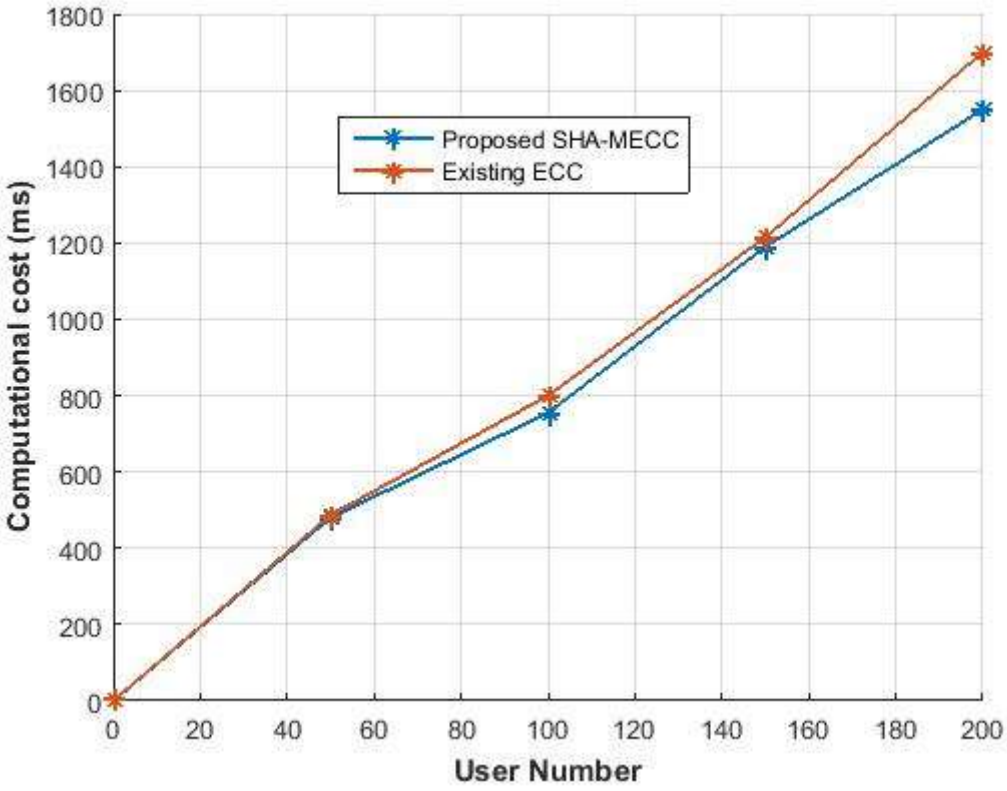

Figure 4: Compared the performance of the proposed SHA-MECC with the existing ECC in terms of computational cost

Figure 4 demonstrates the proposed SHA-MECC based secure DA's performance on grid communication with that of the existing ECC base DA concerning the computational cost. Here, the computational cost is measured in ms, and it varies based on the number of users that ranges from 0 to 200. The proposed SHA-MECC has less computational cost compared to the existing ECC. Hence, it proved that the proposed system has a better performance when weighted against the existing method.

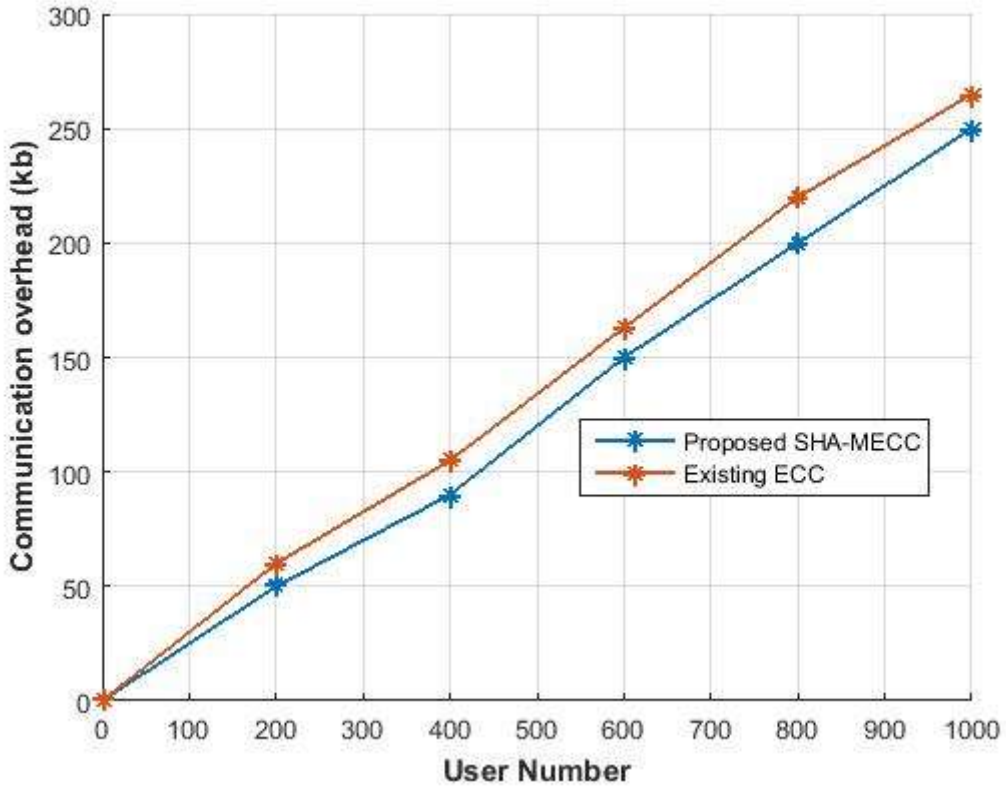

Figure 5: Compared the performance of the proposed SHA-MECC with the existing ECC in terms of CO (different users)

Figure 5 compared the proposed SHA-MECC performance with that of the existent ECC base DA concerning the CO. Here, the CO is gauged in kb and the CO varies based on the number of users that ranges as of 0 to 1000. The proposed SHA-MECC has less CO than the existing ECC. Thus, it concluded that the proposed system shows enhanced performance than the existing methodology.

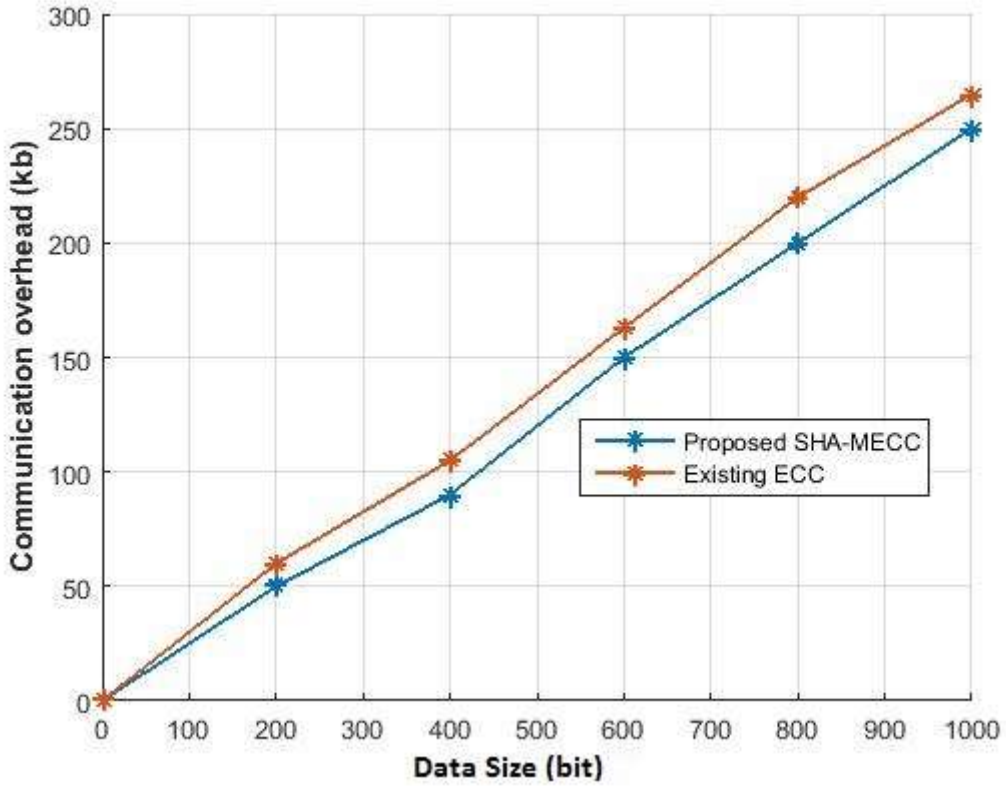

Figure 6: Compared the performance of the proposed SHA-MECC with the existing ECC in terms of CO (different data size)

Figure 6 exhibits the performance of the proposed SHA-MECC with the existing ECC base DA concerning CO. Here, CO performance varies based on different data size that ranges from 0 to 2000. The proposed SHA-MECC has low CO than the existing ECC. Figure 6 observation exhibits that the proposed system gives better security than the existing methodology.

5. CONCLUSION

For the upcoming-generation smart technologies, the SG is viewed as the most imperative trend. The conventional power grid is taken and being integrated with a real-time (almost) communication system and intelligent control system in the SG. The security acts as an vital aspect for grid communications. This paper proposed a secure SHA-MECC based privacy-preserving DA system with fault tolerance for SG. The proposed methodology consists of three phases, i) system initialization, ii) DA, and iii) secure report reading and response. Compared to the preceding schemes, the SHA-MECC system provides better performance. It as well provides security analysis to demonstrate the level of security achieved in this

scheme. Finally, by comparing the computational cost as well as the CO with existing schemes, the proposed work establishes the efficiency of this scheme.

REFERENCES

1. Yonggang Li, Jianwen Li, Yaxiong Lei, and Wei Sun, "Grid synchronization technology for distributed power generation system", In IEEE Conference and Expo Transportation Electrification Asia-Pacific (ITEC Asia-Pacific), pp. 1-6, 2014.
2. Naga Sarvani, B., Vineela Thulasi B., Rahul K., K. Satish Kumar, and V D Sekhara Varma, "Detection of power grid synchronization failure on sensing frequency and voltage beyond acceptable range and load protection", 2017.
3. Valentin Oleschuk, Gabriele Grandi, and Padmanaban Sanjeevikumar, "Simulation of processes in dual three-phase system on the base of four inverters with synchronized modulation", Advances in Power Electronics, 2011.
4. Wei Chen, Yifei Wu, Renhui Du, Qingwei Chen, and Xiaobei Wu, "Speed tracking and synchronization of a dual-motor system via second order sliding mode control", Mathematical Problems in Engineering, 2013.
5. Remya Krishna, Deepak E. Soman, Sasi K. Kottayil, and Mats Leijon, "Synchronous current compensator for a self-balanced three-level neutral point clamped inverter", Advances in Power Electronics, 2014.
6. Sifeu Takougang Kingni, Gaetan Fautso Kuiate, Romanic Kengne, Robert Tchitnga, and Paul Woafo, "Analysis of a no equilibrium linear resistive-capacitive-inductance shunted junction model, dynamics, synchronization, and application to digital cryptography in its fractional-order form", Complexity 2017.
7. Ricardo Bressan Pinheiro, and José Roberto C. Piqueira, "Designing all-pole filters for high-frequency phase-locked loops", Mathematical Problems in Engineering 2014.
8. Godha, R., Ch VSS Sailaja, and KV Ramana Murthy, "Improved grid synchronization algorithm for DG system using and UH PLL under grid disturbances", vol. 3, no. 12, pp.69, 2014.
9. Khaled Syfullah Fuad, and Eklas Hossain, "Performance of grid-voltage synchronization algorithms based on frequency-and phase-locked loop during severe

grid fault conditions", In 3rd International Conference on Electrical Engineering and Information Communication Technology (ICEEICT), pp. 1-6, 2016.

10. Fang Xiong, Wang Yue, Li Ming, Wang Ke, and Lei Wanjun, "A novel PLL for grid synchronization of power electronic converters in unbalanced and variable-frequency environment", In The 2nd International Symposium on Power Electronics for Distributed Generation Systems, pp. 466-471, 2010.
11. Ruturaj V. Shinde, Bharadwaj P.D, "A review on generator grid synchronization needs effects, parameters and various methods", International Journal for Research in Applied Science & Engineering Technology (IJRASET), vol. 4, no. IV, 2016.
12. Muhammad Waqas Khan, Muhammad Saleem, Ashfaq Ahmad and 4Ahmad Ayaz, "Synchronization of photo-voltaic system with a grid", IOSR Journal of Electrical and Electronics Engineering, vol. 7, no. 4,pp. 01-05, 2013.
13. Mishal Mahmood, Mariam Azam, Khair-un-Nisa Fatima, Muhammad Sarwar, Muhammad Abubakar, and Babar Hussain, "Design and implementation of an automatic synchronizing and protection relay through power-hardware-in-the-loop (phil) simulation", 2019.
14. Lanchao Liu, Mohammad Esmalifalak, Qifeng Ding, Valentine A. Emesih, and Zhu Han, "Detecting false data injection attacks on power grid by sparse optimization", IEEE Transactions on Smart Grid, vol. 5, no. 2, pp. 612-621, 2014.
15. Mohamed Amine Ferrag, "EPEC: an efficient privacy-preserving energy consumption scheme for smart grid communications", Telecommunication Systems, vol. 66, no. 4, pp. 671-688, 2017.
16. Le Chen, Rongxing Lu, Zhenfu Cao, Khalid AlHarbi, and Xiaodong Lin, "MuDA: Multifunctional data aggregation in privacy-preserving smart grid communications", Peer-to-peer networking and applications, vol. 8, no. 5, pp. 777-792, 2015.
17. Hongwei Li, Xiaodong Lin, Haomiao Yang, Xiaohui Liang, Rongxing Lu, and Xuemin Shen, "EPPDR: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 8, pp. 2053-2064, 2013.

18. Lajos Török, Laszlo Mathe, and Stig Munk-Nielsen, “Robust control of boost PFC converter using adaptive PLL for line synchronization”, In IECON 39th Annual Conference of the IEEE Industrial Electronics Society, pp. 7098-7102, 2013.