

Research Article

A Novel Security Methodology for Smart Grids: A Case Study of Microcomputer-Based Encryption for PMU Devices

Metin Varan ¹, Akif Akgul ², Fatih Kurugollu ³, Ahmet Sansli ⁴, and Kim Smith³

¹Department of Electrical and Electronics Engineering, Faculty of Technology, Sakarya University of Applied Sciences, Serdivan 54050, Sakarya, Turkey

²Department of Computer Engineering, Faculty of Engineering, Hitit University, Corum 19030, Turkey

³Department of Electronics, Computing and Mathematics, Derby University, Derby, UK

⁴Department of Computer and Information Science Engineering, Sakarya University, Serdivan 54050, Sakarya, Turkey

Correspondence should be addressed to Akif Akgul; akifakgul@hitit.edu.tr

Received 12 July 2020; Revised 30 June 2021; Accepted 3 September 2021; Published 18 September 2021

Academic Editor: Ning Cai

Copyright © 2021 Metin Varan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Coordination of a power system with the phasor measurement devices (PMUs) in real time on the load and generation sides is carried out within the context of smart grid studies. Power systems equipped with information systems in a smart grid face with external security threats. Developing a smart grid which can resist against cyber threats is considered indispensable for the uninterrupted operation. In this study, a two-way secure communication methodology underpinned by a chaos-based encryption algorithm for PMU devices is proposed. The proposed system uses the IEEE-14 busbar system on which the optimum PMU placement has been installed. The proposed hyperchaotic system-based encryption method is applied as a new security methodology among PMU devices. The success of results is evaluated by the completeness of data exchange, durations, the complexity of encryption-decryption processes, and strength of cryptography using a microcomputer-based implementation. The results show that the proposed microcomputer-based encryption algorithms can be directly embedded as encryption hardware units into PMU and PDC devices which have very fast signal processing capabilities taking into considerations the acceptable delay time for power system protection and measuring applications and quality metering applications which is 2 ms and 10 ms, respectively. While proposed algorithms can be used in TCP or UDP over IP-based IEEE C37.118, IEC 61850, and IEC 61850-90-5 communication frameworks, they can also be embedded into electronic cards, smartcards, or smart tokens which are utilized for authentication among smart grid components.

1. Introduction

A smart grid is defined as the provision of conventional electric power grids with modern information technologies. For smart grids, the most fundamental goal can be explained as the achievement of economic and clean energy generation on a global scale [1, 2]. Conventional power grids are currently being equipped with intelligent devices and systems which, in general, are data-collecting devices, distribution controller units, data manager, electric market monitoring systems, remote terminal units, circuit breakers, human-machine interface equipment, network management tools and routers, network concentrators, phasor measuring

units, smart meters, and protection relays [3]. These devices function in risky decision-making operations such as energy cutoff, commissioning, and load shedding which play crucial roles in fulfilling the desired operations as well as monitoring and measuring activities in the grid. The installation of such devices makes power systems vulnerable to external cyber threats. If the two-way communication is blocked due to a cyberattack, there may be unforeseeable damages in the grid. Therefore, developing security tools which are resistant to cyber threats is indispensable. Having the grid resistant to cyber threats is a strategic precaution to prevent unforeseeable damages in the event that two-way communication is blocked.

The security concept in the smart grid should be regarded within a wide range as to the grids consisting of various types of communication systems such as GSM networks, fiber optic lines, WiMAX, RS-232 and RS-485, cable lines, radio frequency lines, and power system communication lines [4]. The development of high-security hardware and computing infrastructure to ensure that all these hardware and systems work reliably is a matter of working separately within smart grid operations.

By using various and these complex infrastructures, the synchrophasor technology is used to monitor and control the real-time power system condition by using synchrophasor measurements across large geographical areas in real time with very low latency. These measurements are driven by IEEE C37.118 and IEC 61850 synchrophasor communication frameworks whose security is crucial as any incorrect information can cause severe damage to physical equipment. However, nearly all these communication frameworks have no built-in security mechanism, and they have restricted communication to only the local network. Among these communication frameworks, we consider that IEC 61850 is a complete communication system that addresses modeling of power system components, abstracting of services, and communication protocols [5], but only IEC 61850-90-5 communication framework uses the built-in encryption algorithm and periodic refreshing of secret keys which can easily detect unauthorized modifications [6]. On the contrary, IEC 61850-90-5 communication framework has three times larger packet size due to metadata and carrying complete decoding information in each packet compared to IEEE C37.118.1 and IEEE C37.118.2 frameworks.

Today, various state-of-the-art methodologies have started to be used for enhancing the security level of power grids. One of the important applications in grid security is to connect each grid component under a software-defined network (SDN) in which its configuration is specified according to power system component vulnerabilities to cyberattacks [7]. The symmetrical and asymmetric encryption-based privacy and authentication methods are also currently used among PLC and RTU units in grid automation systems [8]. Another security application in the grid is based on the control of grid components, especially controlling the data package of PMUs, with regard to damaging data by external or internal attacks or malfunction reasons by using the Kalman filter method [9]. Protection against cyberattacks is also achieved by using secure VPN technology [10]. All these methods fulfil quite complex and tightly linked rules to meet the specified security goals. Doing all this requires high computational cost, high memory, and power consumption. This prevents the spread of these security systems and causes them to remain in a limited number of devices and regions. In this context, chaotic stream ciphers can be considered as an alternative for block ciphers with regard to both low complexity and low resource consumption [11].

The issues of chaos and chaotic systems are the most complex dynamic behavior known in nonlinear systems. They are a field of science that help explain nonlinear

systems. Chaos-based engineering applications have emerged and have resulted in significant improvements in control [12, 13], communication [14], artificial intelligence [15, 16], and genetic algorithm [17] areas in the recent years. They have also been used as a random number generator [18–20] in cyber security applications such as encryption [21–23] and data hiding [24].

In this work, a novel microcomputer with a hyperchaotic system encryption method is proposed to allow PMU devices to communicate with each other in a secure way in the smart grid. According to our best knowledge, this is the first use of microcomputer-based encryption in a smart grid environment. The proposed security methodology is based on a cryptographic engine ensuring a secure communication layer for PMU and phasor data concentrator (PDC) components. For this purpose, application server software, which communicates with IEEE C37.118.1 compliant PMU devices via the Wireshark platform in real time, is also developed. The results are evaluated by the completeness of data exchange, encryption-decryption durations, and strength of cryptography. The results show that very fast and complex encryption capabilities of the proposed microcomputer-based encryption method can be easily used for ensuring secure communication among smart grid components which have very narrow time intervals such as PMUs.

This paper is organized as follows: in Section 2, methodologies for modern power system analysis are introduced. In Section 3, a novel security methodology for smart grids is given. In Section 4, the nonlinear system used in the proposed method and its dynamical analysis are presented. Section 5 is devoted to random number generator design, and its statistical tests are presented in Section 6. The details of the PMU data encryption application and its security analysis are also provided in this section. Finally, the paper is concluded in Section 7.

2. Methodologies for Modern Power System Analysis

The coordination and reliability of the power system depend on establishing a harmony between power and information infrastructure to create a real-time two-way communication network in the generation, transmission, and distribution of electricity. Two-way communication technologies, control systems, and computer processing are key for smart grids. Advanced sensors, meters, programmable relays, and automated feeder switches are some of modern pieces of equipment used in smart grids. Healthy operation of the power system depends on measurements of operational data at substations continuously. Within this context, it can be said that PMUs are widely acknowledged as one of the most promising developments in the field of real-time monitoring of power systems. The ability of PMUs to calculate synchronized phasors for voltages and currents instantaneously and more accurately has encouraged their consistent proliferation in power system networks all over the world.

2.1. Phasor Calculations and Principles of Phasor Measurement Units

2.1.1. *Phasor Calculations.* Phasor calculations of a power bus within a pure sinusoidal signal are given as

$$x(t) = X_m \cos(\omega t + \varphi), \quad (1)$$

where ω and φ are the resemble frequency of the signal in radians per second and phase angle in radians, respectively, while X_m is the peak amplitude of the signal. Figure 1 represents all parts of a pure sinusoidal signal.

Phasor representation is only possible for a pure sinusoidal signal. In practice, a waveform is often corrupted with other signals of different frequencies. Extracting a single frequency component of the signal, Fourier transform is used. For sampled data extraction, discrete (DFT) or fast transform (FFT) is used [25]. A $x(t)$ sinusoid signal with frequency $k f_0$ representation into Fourier series is shown as follows:

$$\begin{aligned} x(t) &= a_k \cos(2\pi k f_0 t) + b_k \sin(2\pi k f_0 t) \\ &= \left\{ \sqrt{a_k^2 + b_k^2} \right\} \cos(2\pi k f_0 t + \varphi) \quad \text{where } \varphi \\ &= \arctan\left(\frac{-b_k}{a_k}\right). \end{aligned} \quad (2)$$

Here, the Fourier series coefficients a_k and b_k measure the amount of $\cos(2\pi k f_0 t)$ and $\sin(2\pi k f_0 t)$ present in the function $x(t)$. Phasor representation of the signal becomes as

$$X_k = \frac{1}{\sqrt{2}} \left\{ \sqrt{a_k^2 + b_k^2} \right\} e^{j\varphi}. \quad (3)$$

The complex form of equation (3) is constituted as follows:

$$X_k = \frac{1}{\sqrt{2}} (a_k - j b_k). \quad (4)$$

Using the relationship of the Fourier series coefficients with DFT, the phasor representation of the k^{th} harmonic component is given by

$$X_k = \frac{1}{\sqrt{2}} \frac{2}{N} \sum_{n=0}^{N-1} x(n\Delta T) e^{-j(2\pi k n/N)}, \quad (5)$$

$$X_k = \frac{\sqrt{2}}{N} \sum_{n=0}^{N-1} x(n\Delta T) \left\{ \cos\left(\frac{2\pi k n}{N}\right) - j \sin\left(\frac{2\pi k n}{N}\right) \right\}, \quad (6)$$

$$x(n\Delta T) = x_n \text{ and } \theta = \frac{2\pi}{N},$$

where N is the number of samples in the data window, n is the sample number, x_n is the input sample, and θ refers to the sample angle. Then, equation (6) becomes as follows:

$$X_k = \frac{\sqrt{2}}{N} \sum_{n=0}^{N-1} x_n \{ \cos(kn\theta) - j \sin(kn\theta) \}. \quad (7)$$

Sin and cosine parts of x_n are separated, respectively, as X_{kc} and X_{ks} in the form of

$$X_k = X_{kc} - j X_{ks},$$

$$X_{kc} = \frac{\sqrt{2}}{N} \sum_{n=0}^{N-1} x_n \cos(kn\theta), \quad (8)$$

$$X_{ks} = \frac{\sqrt{2}}{N} \sum_{n=0}^{N-1} x_n \sin(kn\theta).$$

Finally, X_k is used to represent the phasor in most of the phasor computations. In phasor calculation process, it is necessary to update the phasor estimation with newer data. This is the simplest way for continuous phasor calculation and known as the nonrecursive phasor update method.

$$X^{N+r} = \frac{\sqrt{2}}{N} \sum_{n=0}^{N-1} x_{(n+1)+r} \{ \cos(n\theta) - j \sin(n\theta) \}. \quad (9)$$

In equation (9), $r = -1, 1, 2, 3, \dots$; when $r = -1$, x_0 sample is present on the right-hand side, but when $r = 0$, there is no x_0 sample even if the total number of samples, i.e., N , remains the same.

As seen in Figure 2, phasor 1 is calculated with samples $n = 0, \dots, N-1$, while phasor 2 is calculated with samples $n = 1, 2, \dots, N$. θ is the angle between successive samples based on the period of the fundamental frequency. Here, n is the sample number, and N is the number of samples in the data window. The phasor calculations are performed fresh for each window without using any data from the earlier estimates; this algorithm is the simplest way and known as a “nonrecursive algorithm.”

$$X^{N+r} = X^{N+(r-1)} + \frac{\sqrt{2}}{N} \sum_{n=0}^{N-1} x_{N+r} - x_r \{ \cos n\theta - j \sin n\theta \}. \quad (10)$$

In equation (10), $r = 0, 1, 2, 3$; when r represents the present state, $(r-1)$ represents the past state. As seen in equation (10), recursive estimation current output, X^{N+r} , depends on the previous output, $X^{N+(r-1)}$, and the current input, x_{N+r} . Recursive phasor estimation is faster compared to nonrecursive phasor estimation as phasor calculation is not performed in each step. If the sine wave is not continuous, there is a small error in phasor updating. Then, in case of recursive phasor estimation, this small error is accumulated resulting in much larger error over time.

2.1.2. *Principles of Phasor Measurement Units.* PMUs which are equipped with global positioning system (GPS) receivers take highly precise measurements of voltages and currents within defined timestamps. Here, the GPS receivers coordinate the synchronization of several current and voltage

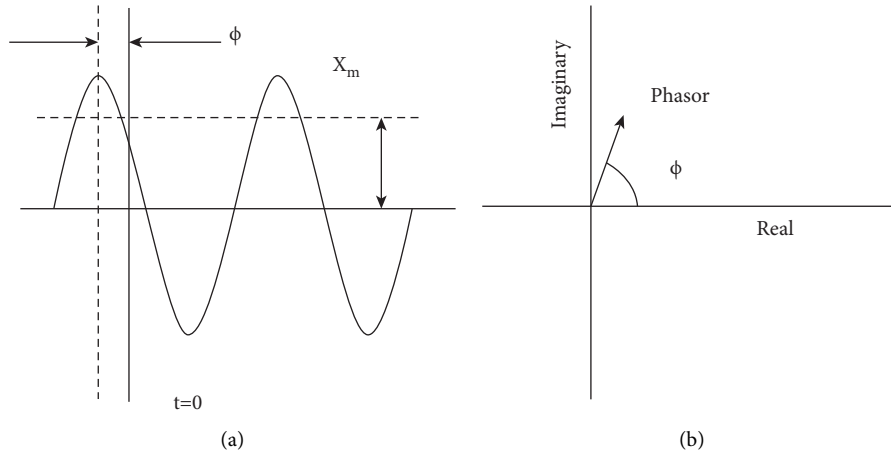


FIGURE 1: A sinusoid (a) and its representation as a phasor (b). The phase angle of the phasor is arbitrary as it depends on the choice of the axis $t = 0$.

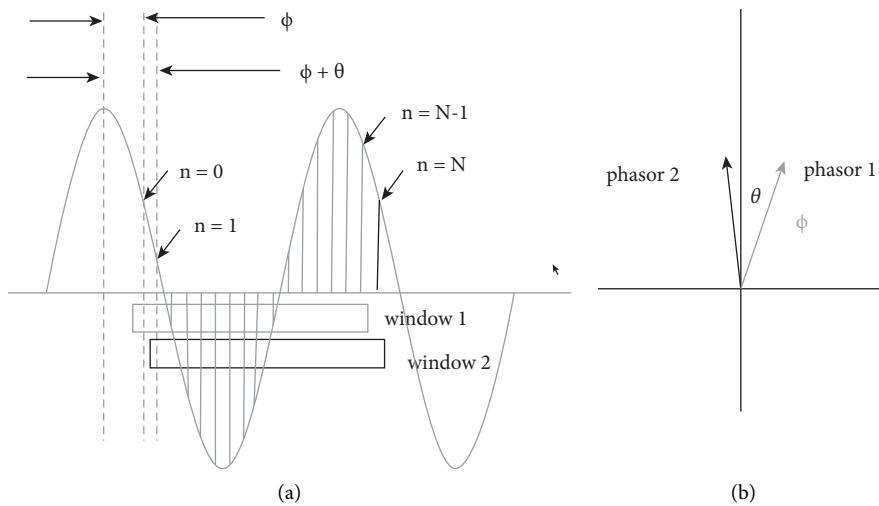


FIGURE 2: Nonrecursive update of phasor estimates with N sample windows.

measurements [26]. PMUs use recursive algorithm for calculating symmetrical components of voltage and current such as symmetrical component distance relay (SCDR) [27].

The GPS [28] is a system of 36 satellites to produce time signals at the Earth's surface. 24 satellites are used each time for generating time signals. A GPS receiver measures distance using the travel time of radio signals. One microsecond precision is a suitable range of measuring power frequency voltages and currents [27].

Since the introduction of PMUs to power systems, power system designers have been looking for using the ability of PMUs in order to observe the system in a better way. Today, gathering and merging information of PMUs are the best fault detection method in power transmission lines [28]. The processing data of PMUs are used to improve stability coordination [29], power system state estimation [30], remedial action schemes [31], and disturbance monitoring [32]. On the contrary, linearization mainly occurs when the state vector, as well as the PMU measurements, is expressed in rectangular coordinates.

2.1.3. IEEE-14 Bus Model and PMU Placement Algorithm.

It can be stated that the most important condition of increasing reliability and stability of a power system depends on establishing a continuous and accurate measurement system. Kirchhoff's current and voltage laws are based on the fundamental principle that electrical quantities are phasors. Similarly, it is possible to assume that the electrical signal is moving at the speed of light and that the instantaneous voltage and current value of the system are possible by combining all voltage and current phasor measurements taken with an accurate timer. PMU devices, which are customized as phasor measuring devices in power systems, can detect the voltage and current phasor information of the grid. The optimum placement of PMU devices should be considered due to the fact that a great economic cost is required for the installation of PMUs at every busbar in a power system [33, 34]. Instead of installing PMUs to every busbar of the power system, the busbars with high dynamics and intense variability of conditions are chosen for installation. In this context, firstly, the placement of PMU

devices on the IEEE-14 bus system has been established by the depth-first search method [35–38]. In this study, an IEEE-14 busbar system is used, and the optimum PMU placement is installed on the studied busbar system. Then, a microcomputer with a hyperchaotic system encryption method is proposed as a new security methodology among PMU devices.

The open-source PSAT power flow analysis tool is used for the placement of the secure communication-based PMUs in the most suitable number of the IEEE-14 busbar system. According to the depth-first search method, the number of PMU devices that are placed is 6, and the most suitable busbars for PMU placement are busbars 1, 4, 6, 8, 10, and 14, respectively. Figure 3 shows the placement of PMUs on the IEEE-14 busbar power system.

Thanks to the use of these devices, it is determined that 16 current phasors can be measured on the studied power system which consists of 14 busbars and 20 lines. The list of measurable phasor lines of the PMU-installed power system is given in Table 1, respectively.

Similarly, another kind of IEEE test system can be used for case studies. In such a test scenario, the most important difference would be to determine the number of PMUs that would allow full monitoring of the system and to define appropriate PMU and PDC data exchange procedures within the IEEE C37.118.1 protocol [39]. For example, in the case of IEEE-39, IEEE-118, and IEEE-300 were used as a test system, only a different data exchange scenario would be created over the placement of 14, 39, and 73 PMU devices, respectively, which would provide full monitoring of the studied test system using some optimal placement algorithms [40]. Figure 4 shows the structure of the data packet of an IEEE C37.118.1 compliant PMU device. The data packet structure includes the device ID, the GPS timestamp, the second fraction, user-defined flag commands to send the packet within the communication protocol standards, the phasor data, the rate of data, and a 16-bit CRC data integrity controller. The phasor data consist of frequency (f), voltage magnitude (m_V), voltage phase angle (δ_V), current magnitude (m_I), and current phase angle (δ_I) of the busbar.

3. A Novel Security Methodology for Smart Grids

Getting a correct phasor calculation in the studied IEEE-14 busbar system depends on appropriate placing of PMU devices with adequate numbers. A correct phasor calculation also depends on an effective and proper data communication of PMU devices with each other. In this study, instead of acquiring durations and package latencies for the completion of one full phasor calculation, we have, especially, focused on a stream-based communication which is used for revealing encryption success of data communication among one PMU to PDC devices. Here, the built-in PMU devices at the IEEE-14 busbar system communicate by using the IEEE C37.118.1 synchronous phasor communication protocol with TCP/IP support. The PDC unit which is responsible for collecting all PMUs' data in the grid uses the IEEE C37.118.1

protocol. In this study, the Wireshark platform is only responsible for interfacing data repository of PMU devices via a predetermined IP and socket address. A client-based application at PMU sides and server-based application software at the PDC side handle together the microcomputer-based hyperchaotic encryption processes of captured PMU data.

As seen in Figure 5, the Rasp3 unit operates as one of the PMU devices that encrypts the digital phasor packet data in harmony with the IEEE C37.118.1 protocol using the chaos encryption engine. While connecting remained PMU units on the IEEE-14 bus system except for Rasp3, the PDC server performs microcomputer-based encryption by gathering data using the Wireshark platform. The encryption and decryption processes are performed by the client and server using the proposed microcomputer-based cryptographic engine.

As seen in Figure 6, studied real-time data acquisition of PMU devices is acquired by the IEEE C37.118.1 compliant Wireshark platform. The application server manages both PMU and PDC sides with a chaotic cryptographic engine.

PDC server is responsible for determining appropriate initial conditions for the chaotic system and other parameters for secure communication. The communication is carried out with sessions in which 1 Mbit random numbers generated by the chaotic system are used in the stream cipher. To facilitate this secure communication, PDC, first, generates random numbers using the 5D hyperchaotic system and tests them against NIST-800-22 statistical tests for randomness. Then, it sends these parameters to the PMU as a part of cryptographic key. PMU uses the parameters to generate the same sequence using the same chaotic system. Then, PMU data are encrypted with a stream cipher by means of the tested random numbers.

4. The Used Nonlinear System and Its Dynamical Analysis

In this study, a 5D hyperchaotic Lorenz system is used [41–43]. The 5D hyperchaotic system and its dynamical analysis are given in this section. Equilibrium points, Lyapunov, and bifurcation analysis are examined for dynamical analysis. Also, phase portraits are shown in Section 5. The 5D hyperchaotic Lorenz system is set as follows:

$$\begin{aligned}\dot{x} &= -\sigma(x - y) + w, \\ \dot{y} &= rx - y - xz - w, \\ \dot{z} &= -\beta z + xy, \\ \dot{u} &= -xz + pw, \\ \dot{w} &= qy,\end{aligned}\tag{11}$$

where w is the fifth state variable and q is a positive real parameter. 5D system (11) has three positive, one negative, and one zero Lyapunov exponents.

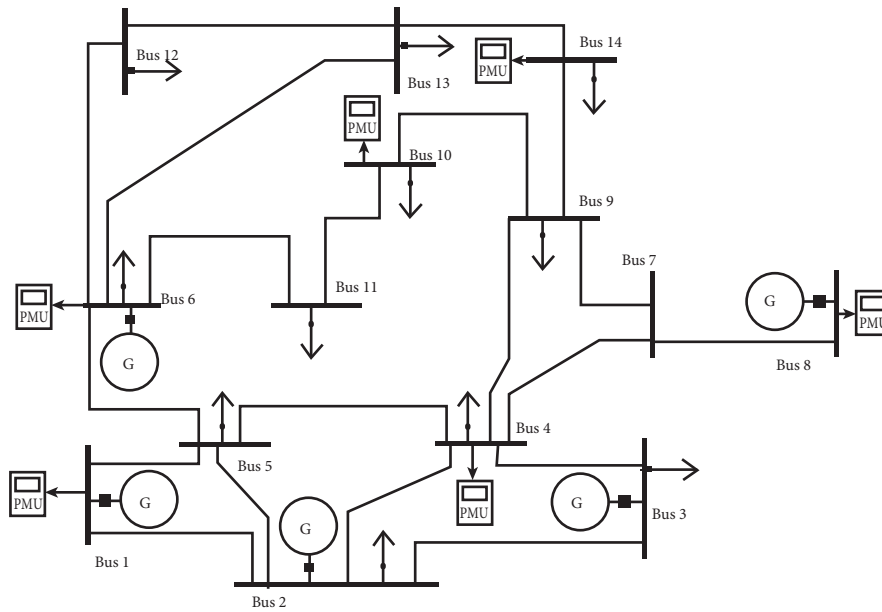


FIGURE 3: IEEE-14 busbar PMU built-in model with depth-first search algorithm.

TABLE 1: Measurable phasor lines of the PMU-installed IEEE-14 busbar system.

1-2 line	4-5 line	6-11 line	9-10 line
1-5 line	4-7 line	6-12 line	9-14 line
2-4 line	4-9 line	6-13 line	10-11 line
3-4 line	5-6 line	7-8 line	13-14 line

SYNC	FRAME	ID	SOC	FRACSEC	CMD	PHASORS	DATARATE	CRC
2 BYTE	2 BYTE	2 BYTE	4 BYTE	4 BYTE	2 BYTE	0-65518 BYTE	2 BYTE	2 BYTE

FIGURE 4: IEEE C37.118.1 compliant PMU package definition.

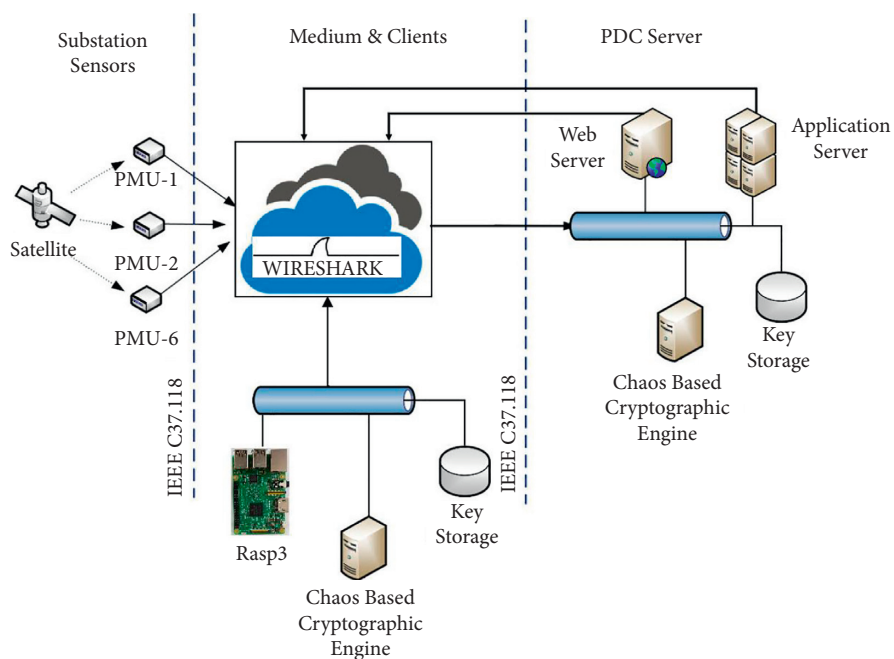


FIGURE 5: Overall PMU-based chaotic cryptography scheme.

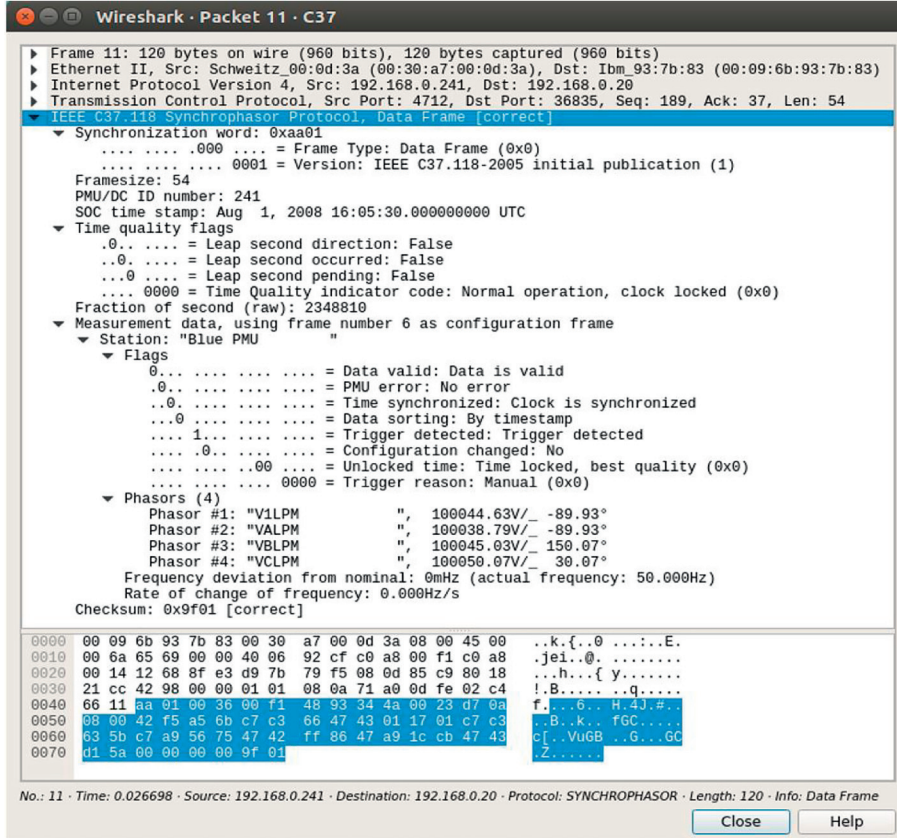


FIGURE 6: Studied IEEE C37.118.1 frames captured by Wireshark network protocol analyzer software.

The equilibria of five-dimensional hyperchaotic Lorenz system (11) can be found by assuming $\dot{x} = 0$, $\dot{y} = 0$, $\dot{z} = 0$, $\dot{u} = 0$, and $\dot{w} = 0$ and solving the following equation:

$$\begin{cases} -\sigma(x - y) + w = 0 \\ rx - y - xz - w = 0 \\ -\beta z + xy = 0 \\ -xz + pw = 0 \\ qy = 0. \end{cases} \quad (12)$$

Thus, this system has only zero equilibrium point: $E_0(0, 0, 0, 0, 0)$. The Jacobian matrix of the linearized system of the hyperchaotic system at the only equilibrium E_0 is

$$J = \begin{bmatrix} -\sigma & \sigma & 0 & 1 & 0 \\ r & -1 & 0 & 0 & -1 \\ 0 & 0 & -\beta & 0 & 0 \\ 0 & 0 & 0 & p & 0 \\ 0 & q & 0 & 0 & 0 \end{bmatrix}. \quad (13)$$

We study the dynamics around the original equilibrium point E_0 when the critical bifurcation values of parameters are taken as $p = 2$ and $q = 8$. So, the characteristic equation of the system becomes as follows:

$$(\lambda - p)\left(\lambda + \frac{8}{3}\right)(\lambda^3 + 11\lambda^2 + (q - 270)\lambda + 10q) = 0. \quad (14)$$

By using wolf algorithm [44], Lyapunov exponents of the 5D hyperchaotic system are calculated as 0.4580, 0.3371, 0.0415, 0.0000, and 12.5046.

For the values of $p > 0$ and $q < 2970$, the only equilibrium E_0 is an unstable saddle-node point due to the presence of eigenvalues with positive real parts.

The bifurcation diagrams are also inspected to identify the chaos in the simulations. The visualization of dynamic behaviors and solutions of the 5D hyperchaotic system are gathered by using MATLAB ODE45 solver, and the phase portraits of the hyperchaotic system are depicted in Figure 7 which shows the bifurcation diagrams in terms of p parameter varying between -7.5 and 2.5 values by keeping the other parameters fixed. The initial states of the 5D hyperchaotic Lorenz system are determined as $x(0) = 0$, $y(0) = -0.01$, $z(0) = 9$, $u(0) = 1$, and $w(0) = 0$. For a step size of 0.005 , the chaos appears in two regions where parameter p is less than -1.5 and it is greater than 1 .

In Figures 8(a) and 8(b), it is also revealed that the system falls into a hyperchaotic situation as it can be seen that it has distinct features in its Lyapunov exponents. In this context, bifurcation and Lyapunov exponent diagrams confirm each other.

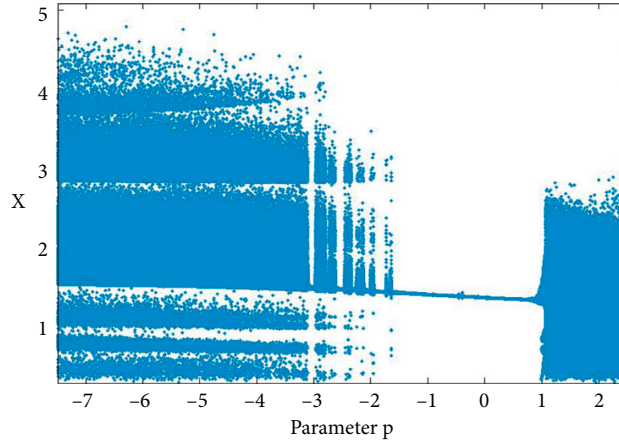


FIGURE 7: Bifurcation diagram for p parameter varying between -8 and 3 .

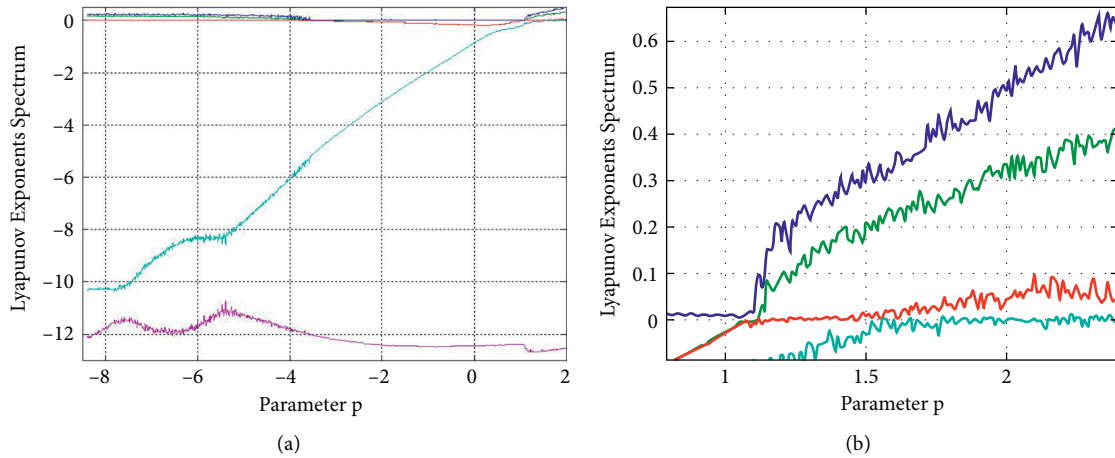


FIGURE 8: The Lyapunov exponents of the 5D hyperchaotic system for p parameter varying between (a) -8 and 3 and (b) -1.5 and 2.5 .

5. Random Number Generator Design and Its Statistical Test

5.1. RNG Design with a 5D Hyperchaotic System. Many chaotic systems are used to generate pseudo-random numbers as a source of entropy because they are complex and very sensitive to the initial conditions. In this section, an RNG design is proposed for PMU data encryption which is implemented in Raspberry 3.

A 5D hyperchaotic system developed in the proposed RNG design is given in equation (11), where $\sigma, r, \beta, p,$ and q are the parameters and $x, y, z, u,$ and w are the state variables. To visualize dynamic behaviors and solutions of the proposed 5D hyperchaotic system, the differential equations given in equation (11) are worked out using the MATLAB ODE45 function. The obtained phase portraits of the 5D hyperchaotic system are depicted in Figure 9 for x, y, z and x, y, w . For this experiment, the parameters are set to $\sigma = 10, r = 28, \beta = 8/3, p = 2,$ and $q = 8$ as well as the initial state is chosen as $(0, -0.01, 9, 1, 0)$.

RNG design steps using the proposed 5D hyperchaotic system are given in Algorithm 1. As it can be seen in the

algorithm, for RNG design, parameters and initial values of the hyperchaotic system are needed. Any change in these parameters and initial values results in different random numbers. Therefore, initial conditions are crucial in RNG. Next, the time step (Δh) is determined in order to discretize the hyperchaotic time series using the Runge-Kutta-4 (RK4) method. The floating number outputs ($x, y, z, u,$ and w) are converted to 32-bit binary numbers [45]. The last 16 bits of these binary numbers which must pass NIST-800-22 randomness test are used to generate 1 Mbit random numbers which are then used in one communication session. For this aim, 1 Mbit is extracted from the last 16 bits of each output and tested. If these numbers do not pass the test, then the last 8 bits of each output are considered for the test.

To prove the randomness of the generated number series, NIST-800-22 tests are employed. NIST-800-22 has 16 different tests such as runs, discrete Fourier transform, and linear complexity test. These tests need a minimum of 1 Mbit binary numbers. For successful results, the P value must be greater than 0.001 for all NIST-800-22 tests [46]. NIST-800-22 is applied to the random numbers generated in Step 11.

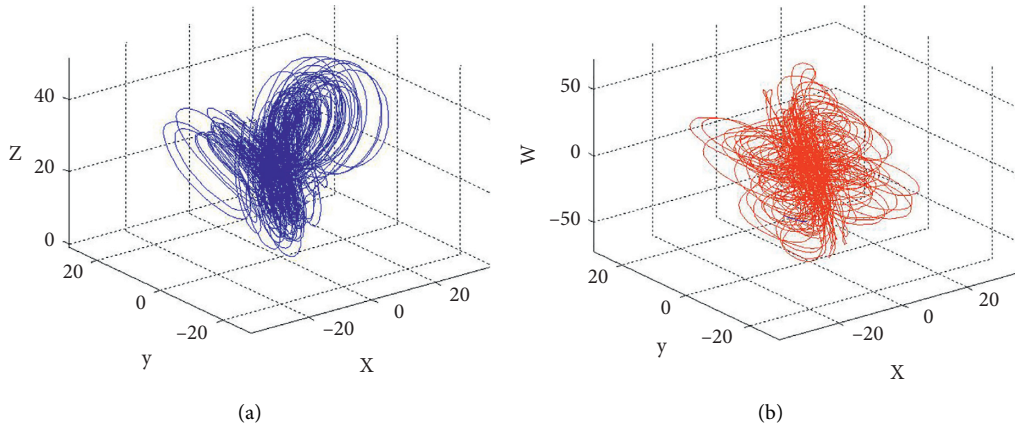


FIGURE 9: The phase portraits of the 5D hyperchaotic system for x, y, z (a) and x, y, w (b).

Input: parameters and initial condition of chaotic systems

Output: random numbers tested statistically

- (1) Accepting system parameters and initial condition of the 5D Lorenz hyperchaotic system
- (2) Determination of the value of Δh
- (3) Sampling with determination Δh value for RK4
- (4) **WHILE** (maximum 1 MBit data) **DO**
- (5) Solving the 5D hyperchaotic system using RK4 algorithm
- (6) Obtaining time series as float numbers (x, y, z, u , and w)
- (7) Convert float numbers to 32-bit least binary numbers
- (8) Select LSB-8-bit least binary numbers from RNG from y and u phases
- (9) Select LSB-16-bit least binary numbers from RNG from z and w phases
- (10) **END WHILE**
- (11) Apply NIST-800-22 tests for each minimum 1 MBit data
- (12) **IF** (test results==pass) **THEN**
- (13) Successful results
- (14) Ready tested random numbers for RNG applications
- (15) **ELSE**
- (16) Go to Step 4
- (17) **END IF**
- (18) **EXIT**

ALGORITHM 1: Random number generation algorithm pseudo-code

5.2. *Statistical Tests.* The NIST-800-22 test results of obtained random numbers from y, z, u , and w are shown in Table 2. The random numbers obtained from y, z, u , and w successfully passed all the tests, but the random numbers from w are only used for PMU data encryption.

ENT is another randomness test that has five different tests, which define the randomness of bit sequences, proposed by Walker [47]. The tests include arithmetic mean, entropy, correlation, chi-square, and Monte Carlo pi estimation [48]. The average values of the ENT test results of the random numbers from $y(8), z(16), u(8)$, and $w(16)$ are shown in Table 3 in which successful results can be seen for all tests.

The proposed microcomputer with a hyperchaotic system method is compared with some studies in the literature in Table 4. When the results in the table are considered, it is seen that the numbers obtained provide randomness for ENT tests. The proposed method produces good results in

general. Stoyanov et al. had the best results in the arithmetic mean test because the ideal result is 127.5, but the entropy test result is not good according to other methods except from [50]. Entropy, correlation, and Monte Carlo test results are the best in [51] with 7.9999, 0.000108, and 3.14062, respectively [49, 50]. In the proposed method, test results are suitable and acceptable for cryptographic applications because the random numbers passed all tests.

6. PMU Data Encryption Application and Its Security Analysis

6.1. *PMU Data Encryption Application with the 5D Hyperchaotic System.* Mobile random number generators (RNGs) are important for real-time stream cipher-based applications. Nowadays, some RNGs are implemented by using high-cost hardware such as FPGA and computers. In this work, a low-cost RNG is designed by means of 64-bit

TABLE 2: RNG NIST-800-22 test results for y, z, u , and w outputs.

Statistical tests	y (8)	z (16)	u (8)	w (16)
Frequency (Monobit) test	0.2142	0.9712	0.2974	0.0945
Block frequency test	0.7545	0.7000	0.0581	0.4610
Cumulative sum test	0.3829	0.4886	0.3897	0.1016
Runs test	0.6075	0.9904	0.8611	0.8342
Longest run test	0.4854	0.9275	0.9225	0.4248
Binary matrix rank test	0.7728	0.1876	0.5529	0.2004
Discrete Fourier transform test	0.1323	0.9414	0.4140	0.0289
Nonoverlapping templates' test	0.3973	0.0168	0.0202	0.0533
Overlapping templates' test	0.5982	0.8957	0.5830	0.7414
Maurer's universal statistical test	0.2457	0.7903	0.3924	0.7780
Approximate entropy test	0.7247	0.9430	0.9008	0.6912
Random excursion test	0.2953	0.6938	0.8843	0.4569
Random excursion variant test	0.6888	0.6522	0.6050	0.3386
Serial test-1	0.6993	0.9187	0.0464	0.8103
Serial test-2	0.2423	0.4510	0.0129	0.9127
Linear complexity test	0.9728	0.2036	0.6666	0.6098

TABLE 3: ENT test results for y, z, u , and w outputs.

Statistical tests	y (8)-the last 8 bits	z (16)-the last 16 bits	u (8)	w (16)	Ideal results	Results
Arithmetic mean	127.3353	127.1994	127.322	127.3249	127.5	Successful
Entropy	7.9985	7.9985	7.9985	7.9985	8	Successful
Correlation	-0.0051725	0.0031184	0.0030067	-0.00061494	0.0	Successful
Chi-square	253.6648	265.2769	262.594	252.6899	190-300	Successful
Monte Carlo	3.1396 Error = -0.00062338	3.149 Error = 0.0023713	3.1383 Error = -0.0010512	3.1352 Error = -0.0020291	3.14159 (Pi)	Successful

TABLE 4: Comparing the ENT test results of the proposed method with different works.

	Arithmetic mean	Entropy	Correlation	Chi-square	Monte Carlo
y (8)	127.3353	7.9985	-0.0051725	253.6648	3.1396 Error = -0.00062338)
z (16)	127.1994	7.9985	0.0031184	265.2769	3.149 Error = 0,0023713
u (8)	127.322	7.9985	0.0030067	262.594	3.1383 Error = -0,0010512
w (16)	127.3249	7.9985	-0.00061494	252.6899	3.1352 Error = -0,0020291
Stoyanov and Kordov [49]	127.5013	7.9975	-0.000147	—	3.140569 Error = 0.03
Seetharam and Rhee [50]	122.885	7.7133	-0.058927	—	3.088126 Error = 1.70
Akhshani et al. [51]	127.7714	7.9999	0.000108	255.19	3.14062 Error = 0.031

quad-core ARM Cortex-A53 microprocessor-based "Raspberry Pi 3" (1.2GHz, 4 cores, 1GB RAM) microcomputer.

In this section, the PMU data encryption and decryption system using the RNG designed with the 5D hyperchaotic system and that passed all the NIST-800-22 tests is presented. The block diagram of the encryption processes is given in Figure 10. One PMU generates 108 byte data. Within the application server, digital chaos keys are created and ready for use in packet encryption. The encrypted packets generated by the encryption are sent back to the application server via the Ethernet port of Raspberry Pi.

An example of PMU data consisting of 108 characters is as follows. Also, original and encrypted PMU data input/output ports in Raspberry Pi 3 are given in Figure 11.

```
aa01003600f14893334f003 d70a4080047c3659cbfc8
e73947c3631cbfc8e52b47c365574027a0 d447c368643f065
a850000000042a9
```

In the encryption application, the PMU data are converted to a binary format. In Figure 12, some bits of binary 864-bit original PMU data series, produced from the Raspberry Pi 3 output, on the oscilloscope screen are given. The binary PMU data are encrypted with the tested RNG which obtained the 5D Lorenz hyperchaotic system using a stream cipher scheme based on XOR.

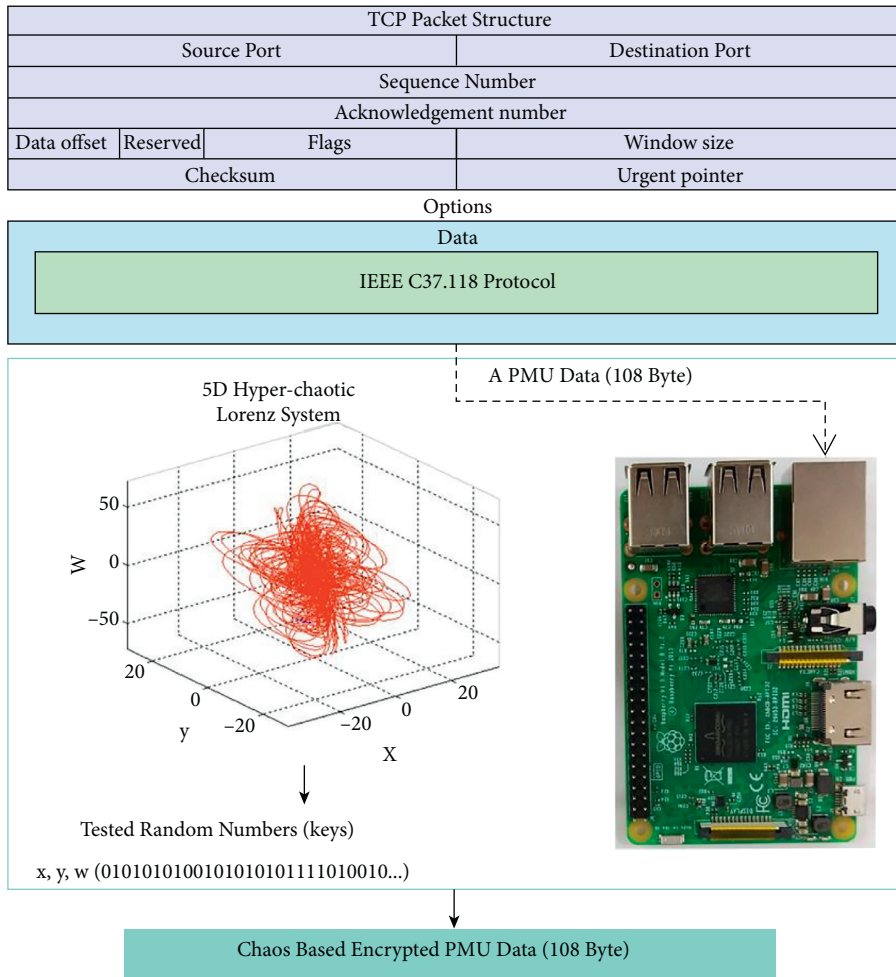


FIGURE 10: Microcomputer with a hyperchaotic system encryption process.

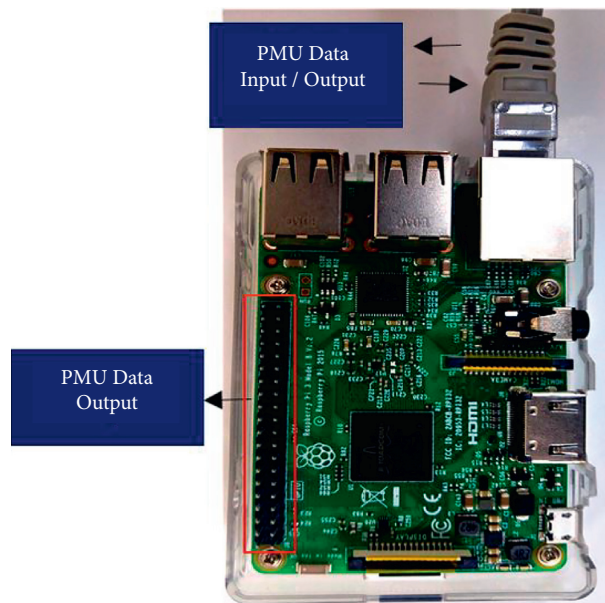


FIGURE 11: PMU data input/output ports in Raspberry Pi 3.

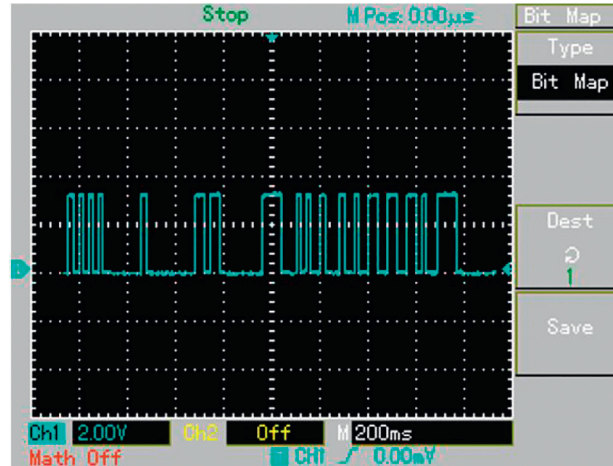


FIGURE 12: Original PMU data.

Some bits of encrypted binary 864-bit PMU data are shown Figure 12. The size of the encrypted data is the same as 864 bits because the encryption process is done bit by bit.

Also, PMU data consisting of all encrypted characters are as follows. Some of them are shown in Figure 13 as binary data.

```
c db 9940e7acc83304a7b45eb40617c53409cb959f f461
539f8fba898b9ea df7 a048f d1 d14b1be5b995b0576e407
e df 6eea721f14b40f
```

In the decryption process, the same random numbers used in the encryption are needed. The parameters and initial values of the hyperchaotic system are very important. If the same random numbers cannot be obtained, it will cause different values, and true PMU data decryption will be impossible. After true random numbers and use of XOR, the decrypted PMU data can be taken.

6.2. Security Analyses and Performance Assessment

6.2.1. Histogram Analysis. In the histogram analysis, rates of 1s and 0s in the original and encrypted data are evaluated. There are 864 bits of data as 1s and 0s in PMU data. If the difference between 1s and 0s is very little or nothing, the result of encryption is quite successful. Histogram distribution (number of 1s and 0s) of PMU data is given in Figure 14 for original and encrypted data. The number of 0s is 690, and the number of 1s is 174 in the original PMU data. Encrypted PMU data bit series contains 425 0s and 439 1s. The difference between bits decreased from 516 to 14 after the encryption.

6.2.2. Key Length Analysis. In encryption applications, the length of the key also determines the security level. The numbers of differential equations, initial values, and system parameters make key lengths longer. For one-variable nonlinear system, the length of the key can be 10^{14} values. Chaotic system (11) in this paper has 5 ($x, y, z, u,$ and w) 10^{70} and 5 ($\sigma, r, \beta, p,$ and q) 10^{70} different values, thus 10^{140} key

length in total. The encrypted PMU data with the proposed chaotic system (11) will be highly secure because of the enormous key length. The decryption of PMU data only with this long key reveals the security level of the proposed system.

6.2.3. Key Sensitivity Analysis. Chaotic systems have very complicated and sensitive dynamic features, so they have come into prominence also in security applications such as cryptology and data hiding. The same parameters are needed for the decryption in many applications, and thus, the chaotic system and all of its properties must be clearly known such as initial conditions and parameters. The true results cannot be obtained in a small mistake. It will lead to different results because of this problem.

6.2.4. Encryption-Decryption Times and Memory Usage. Besides little encryption-decryption time, memory usage, and usability in real-time applications, another significant criterion is speed. We used 64-bit quad-core ARM Cortex-A53 microprocessor-based “Raspberry Pi 3” which has 1.2 GHz, 4 cores, and 1 GB RAM microcomputer board in this work and compared some stream cipher algorithms with our chaos-based method. Table 5 details the encryption, decryption times and memory usage. Salsa20 algorithm spends the most time for encryption and decryption. Encryption time is 311 ms, while decryption time is 314 ms. Also, considering the size of memory it occupies, one can conclude that it is quite disadvantageous for real-time applications.

Trivium method produces good results in terms of time criteria, but memory usage is not good according to Pycube algorithm. In the microcomputer-based technique, on the contrary, encryption-decryption times and memory usage are very good according to other methods. Encryption time is 0.097 ms, while decryption time is 0.113 ms. Memory usage is 408 bytes in our method. These results are very suitable for real-time applications, especially in smart grids.

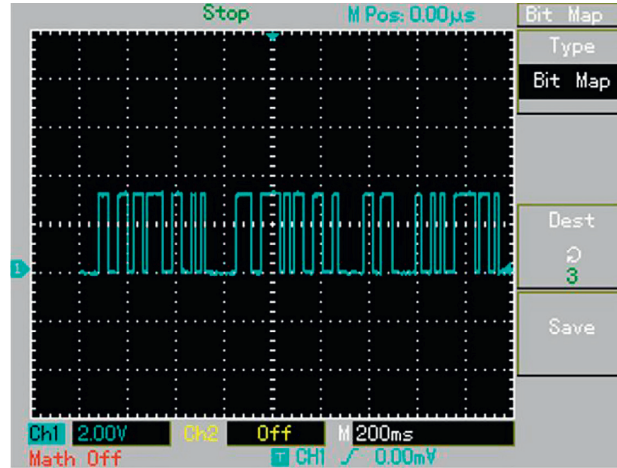


FIGURE 13: Encrypted PMU data.

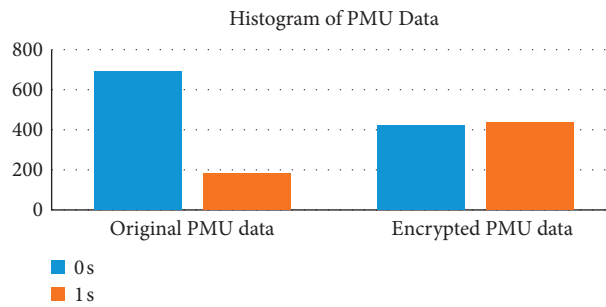


FIGURE 14: Histogram distribution of PMU data.

TABLE 5: The encryption-decryption time and memory usage comparison of encryption algorithms.

Stream cipher algorithms	Encryption time (ms)	Decryption time (ms)	Memory usage (byte)
Chaos	0.097	0.113	408
RC4	84.3	85	6396
Trivium	30	30.5	74448
Salsa20	311	314	201116
Pycube	39.3	40	5767

7. Conclusion

In this study, it is the first time in the literature using a microcomputer with a hyperchaotic system encryption algorithm for allowing PMU devices used in the smart grid to make secure two-way communication. The proposed security methodology is realized into a cryptographic engine ensuring a secure communication layer between PMU and PDC components via developed application server software. The application server communicates with IEEE C37.118.1 compliant PMU devices via the Wireshark platform in real time. The results are evaluated by the completeness of accurate data exchange among PMU packages, total time durations of different encryption algorithms, the complexity

of encryption-decryption processes by using sensitivity and histogram analyses, and, finally, strength of cryptography with NIST tests.

The results show the measured delays of encryption and decryption durations are 0.21 ms in total, the proposed microcomputer-based encryption algorithms can provide a shorter delay while performing encryption and can be directly embedded as encryption hardware units into the encrypted protocol of IEC 61850-90-5 compliant PMU and PDC devices which obligated to acceptable delay time below 3 ms for power system protection and measuring functioning. While proposed algorithms can be used in TCP or UDP over IP-based IEEE C37.118, IEC 61850, and IEC 61850-90-5 communication frameworks, they can also be

embedded into electronic cards, smartcards, or smart tokens which are utilized for authentication among smart grid components.

Data Availability

All data are generated by the authors. One can repeat their results by the description provided in this manuscript.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Scientific and the Research Council of Turkey (TUBITAK) (Grant no. 117E284) and Scientific Research Committees of Sakarya University of Applied Sciences (Grant no. 2019-1-1-093).

References

- [1] M. A. Pai and D. Chatterjee, *Computer Techniques in Power System Analysis*, McGraw-Hill Education, Noida, India, 2014.
- [2] J. Vlach, V. Jiri, and K. Singhal, *Computer Methods for Circuit Analysis and Design*, Springer Science & Business Media, Berlin, Germany, 1983.
- [3] A. R. Bergen, *Power Systems Analysis*, Pearson Education, Noida, India, 2009.
- [4] M. Damrudi and N. Ithnin, "Parallel RSA encryption based on tree architecture," *Journal of the Chinese Institute of Engineers*, vol. 36, no. 5, pp. 658–666, 2013.
- [5] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "Analysis of IEEE C37. 118 and IEC 61850-90-5 synchrophasor communication frameworks," in *Proceedings of 2016 IEEE Power and Energy Society General Meeting (PESGM)*, pp. 1–5, IEEE, Boston, MA, USA, July 2016.
- [6] A. Apostolov, "Impact of iec 61850 on the interoperability and reliability of protection schemes," in *Proceedings of 2013 IEEE Power & Energy Society General Meeting*, pp. 1–5, IEEE, Vancouver, Canada, July 2013.
- [7] X. Dong, H. Lin, R. Tan, R. K. Iyer, and Z. Kalbarczyk, "Software-defined networking for smart grid resilience: opportunities and challenges," in *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, pp. 61–68, Denver, CO, USA, October 2015.
- [8] J. Abawajy and R. J. Robles, "Secured communication scheme for scada in smart grid environment," *Journal of Security Engineering*, vol. 7, no. 6, p. 12, 2010.
- [9] M. N. Kurt, Y. Yilmaz, and X. Wang, "Real-time detection of hybrid and stealthy cyber-attacks in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 498–513, 2018.
- [10] L. Coppolino, S. D'Antonio, and L. Romano, "Exposing vulnerabilities in electric power grids: an experimental approach," *International Journal of Critical Infrastructure Protection*, vol. 7, no. 1, pp. 51–60, 2014.
- [11] F. Dachselt and W. Schwarz, "Chaos and cryptography," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 12, pp. 1498–1509, 2001.
- [12] Z. Wei, A. Akgul, U. E. Kocamaz, I. Moroz, and W. Zhang, "Control, electronic circuit application and fractional-order analysis of hidden chaotic attractors in the self-exciting homopolar disc dynamo," *Chaos, Solitons & Fractals*, vol. 111, pp. 157–168, 2018.
- [13] M. Varan and A. Akgul, "Control and synchronisation of a novel seven-dimensional hyperchaotic system with active control," *Pramana*, vol. 90, no. 4, p. 54, 2018.
- [14] A. Argyris, D. Syvridis, L. Larger et al., "Chaos-based communications at high bit rates using commercial fibre-optic links," *Nature*, vol. 438, no. 7066, pp. 343–346, 2005.
- [15] I. Dalkiran and K. Danisman, "Artificial neural network based chaotic generator for cryptology," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 18, no. 2, pp. 225–240, 2010.
- [16] M. Alçın, İ. Pehlivan, and İ. Koyuncu, "Hardware design and implementation of a novel ann-based chaotic generator in FPGA," *Optik*, vol. 127, no. 13, pp. 5500–5505, 2016.
- [17] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a dna sequence," *Optics and Lasers in Engineering*, vol. 56, pp. 83–93, 2014.
- [18] T. Stojanovski and L. Kocarev, "Chaos-based random number generators-part i: analysis [cryptography]," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 3, pp. 281–288, 2001.
- [19] T. Stojanovski, J. Pihl, and L. Kocarev, "Chaos-based random number generators. part ii: practical realization," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 3, pp. 382–385, 2001.
- [20] M. Z. Yildiz, O. F. Boyraz, E. Guleryuz, A. Akgul, and I. Hussain, "A novel encryption method for dorsal hand vein images on a microcomputer," *IEEE Access*, vol. 7, pp. 60850–60867, 2019.
- [21] A. Akgul, I. Moroz, I. Pehlivan, and S. Vaidyanathan, "A new four-scroll chaotic attractor and its engineering applications," *Optik*, vol. 127, no. 13, pp. 5491–5499, 2016.
- [22] S. Akkaya, I. Pehlivan, A. Akgül, and M. Varan, "The design and application of bank authenticator device with a novel chaos based random number generator," *Journal of the Faculty of Engineering and Architecture of Gazi University*, vol. 33, no. 3, pp. 1171–1182, 2018.
- [23] M. A. Jafari, E. Mliki, A. Akgul et al., "Chameleon: the most hidden chaotic flow," *Nonlinear Dynamics*, vol. 88, no. 3, pp. 2303–2317, 2017.
- [24] A. Akgul, S. Kacar, and B. Aricioglu, "A new two-level data hiding algorithm for high security based on a nonlinear system," *Nonlinear Dynamics*, vol. 90, no. 2, pp. 1123–1140, 2017.
- [25] A. G. Phadke and J. S. Thorp, *Synchronized Phasor Measurements and Their Applications*, Vol. 1, Springer, Berlin, Germany, 2008.
- [26] K.-S. Cho, J.-R. Shin, and S. H. Hyun, "Optimal placement of phasor measurement units with GPS receiver," in *Proceedings of 2001 IEEE Power Engineering Society Winter Meeting*, pp. 258–262, IEEE, Athens, Greece, September 2001.
- [27] A. G. Phadke, "Synchronized phasor measurements—a historical overview," vol. 1, pp. 476–479, in *Proceedings of IEEE/PES Transmission and Distribution Conference and Exhibition*, vol. 1, pp. 476–479, IEEE, Yokohama, Japan, October 2002.
- [28] W. Lewandowski, J. Azoubib, and W. J. Klepczynski, "GPS: primary tool for time transfer," *Proceedings of the IEEE*, vol. 87, no. 1, pp. 163–172, 1999.
- [29] J. Chen and A. Abur, "Placement of PMUS to enable bad data detection in state estimation," *IEEE Transactions on Power Systems*, vol. 21, no. 4, pp. 1608–1615, 2006.

- [30] D. N. Kosterev, J. Esztergalyos, and C. A. Stigers, "Feasibility study of using synchronized phasor measurements for generator drooping controls in the colstrip system," *IEEE Transactions on Power Systems*, vol. 13, no. 3, pp. 755–761, 1998.
- [31] J. Bertsch, C. Carnal, D. Karlson, J. McDaniel, and K. Khoi Vu, "Wide-area protection and power system utilization," *Proceedings of the IEEE*, vol. 93, no. 5, pp. 997–1003, 2005.
- [32] Z. Zhong, C. Xu, B. J. Billian et al., "Power system frequency monitoring network (FNET) implementation," *IEEE Transactions on Power Systems*, vol. 20, no. 4, pp. 1914–1921, 2005.
- [33] Z. Miljanić, I. Djurović, and I. Vujošević, "Optimal placement of PMUS with limited number of channels," *Electric Power Systems Research*, vol. 90, pp. 93–98, 2012.
- [34] N. M. Manousakis and G. N. Korres, "Optimal allocation of phasor measurement units considering various contingencies and measurement redundancy," *IEEE Transactions on Instrumentation and Measurement*, vol. 69, no. 6, pp. 3403–3411, 2019.
- [35] R. Sodhi, S. C. Srivastava, and S. N. Singh, "Optimal PMU placement method for complete topological and numerical observability of power system," *Electric Power Systems Research*, vol. 80, no. 9, pp. 1154–1159, 2010.
- [36] R. Emami and A. Abur, "Robust measurement design by placing synchronized phasor measurements on network branches," *IEEE Transactions on Power Systems*, vol. 25, no. 1, pp. 38–43, 2009.
- [37] G. N. Korres, N. M. Manousakis, T. C. Xygkis, and J. Löfberg, "Optimal phasor measurement unit placement for numerical observability in the presence of conventional measurements using semi-definite programming," *IET Generation, Transmission & Distribution*, vol. 9, no. 15, pp. 2427–2436, 2015.
- [38] M. Korkali and A. Abur, "Impact of network sparsity on strategic placement of phasor measurement units with fixed channel capacity," in *Proceedings of 2010 IEEE International Symposium on Circuits and Systems*, pp. 3445–3448, IEEE, Paris, France, June 2010.
- [39] K. E. Martin, G. Brunello, M. G. Adamiak et al., "An overview of the IEEE standard C37.118.2-synchrophasor data transfer for power systems," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1980–1984, 2014.
- [40] K. Amare, V. A. Centeno, and A. Pal, "Unified PMU placement algorithm for power systems," in *Proceedings of 2015 North American Power Symposium (NAPS)*, pp. 1–6, IEEE, Charlotte, NC, USA, October 2015.
- [41] F. Zhang, R. Chen, X. Wang, X. Chen, C. Mu, and X. Liao, "Dynamics of a new 5d hyperchaotic system of lorenz type," *International Journal of Bifurcation and Chaos*, vol. 28, no. 3, Article ID 1850036, 2018.
- [42] Q. Yang and C. Chen, "A 5d hyperchaotic system with three positive lyapunov exponents coined," *International Journal of Bifurcation and Chaos*, vol. 23, no. 6, Article ID 1350109, 2013.
- [43] Q. Yang and M. Bai, "A new 5d hyperchaotic system based on modified generalized lorenz system," *Nonlinear Dynamics*, vol. 88, no. 1, pp. 189–221, 2017.
- [44] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, "Determining lyapunov exponents from a time series," *Physica D: Nonlinear Phenomena*, vol. 16, no. 3, pp. 285–317, 1985.
- [45] A. Akgül, C. Arslan, and B. Arıcıoğlu, "Design of an interface for random number generators based on integer and fractional order chaotic systems," *Chaos Theory and Applications*, vol. 1, no. 1, pp. 1–18, 2019.
- [46] J. Soto, "Statistical testing of random number generators," in *Proceedings of the 22nd National Information Systems Security Conference*, vol. 10, p. 12, NIST, Gaithersburg, MD, USA, October 1999.
- [47] J. Walker, "Ent: A pseudorandom number sequence test program," 2008, <http://www.fourmilab.ch/random>.
- [48] I. Jang and H. S. Yoo, "Pseudorandom number generator using optimal normal basis," in *Proceedings of International Conference on Computational Science and its Applications*, pp. 206–212, Springer, Glassgow, UK, May 2006.
- [49] B. Stoyanov and K. Kordov, "A novel pseudorandom bit generator based on chirikov standard map filtered with shrinking rule," *Mathematical Problems in Engineering*, vol. 2014, Article ID 986174, 4 pages, 2014.
- [50] D. Seetharam and S. Rhee, "An efficient pseudo random number generator for low-power sensor networks [wireless networks]," in *Proceedings of 29th Annual IEEE International Conference on Local Computer Networks*, pp. 560–562, IEEE, Tampa, FL, USA, November 2004.
- [51] A. Akhshani, A. Akhavan, A. Mobaraki, S.-C. Lim, and Z. Hassan, "Pseudo random number generator based on quantum chaotic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 1, pp. 101–111, 2014.