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

Metin Varan[a], Akif Akgul*[b], Fatih Kurugollu[c], Ahmet Sansli[d], Kim Smith[e]

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

Department of Computer Engineering, Faculty of Engineering, Hitit University, 19030, Corum, TURKEY

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

Department of Computer and Information Science Engineering, Sakarya University, 54050, Sakarya, TURKEY

[a]*mvaran@subu.edu.tr*
[b]*akifakgul@hitit.edu.tr (*corresponding author)*
[c]*f.kurugollu@derby.ac.uk*
[d]*asansli@sakarya.edu.tr*
[e]*a.k.smith@derby.ac.uk*

Abstract

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 pace 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 secure 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 have 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 which the acceptable delay time for power system protection and measuring applications and quality metering applications are 2ms and 10ms 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, it can also be embedded into electronic cards, smartcards, or smart tokens which are utilized for authentication among smart grid components.

Keywords:
Smart grid, microcomputers, microcomputer-based encryption, Phasor Measurement Unit (PMU).

---

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 cut-off, commissioning, load shedding 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 cyber-attack 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 a various type 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 developing 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 realtime 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 are crucial as any incorrect information can cause severe damage to physical equipments. 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 built-in encryption algorithm and periodic refreshing of secret keys which can easily detect unauthorized modifications [6]. On the other hands, 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 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 cyber-attacks [7]. The symmetrical and asymmetric encryptions based privacy and authentication methods are also currently used among PLC and RTU units in grid automation systems [8]. Another security application in grid is based on control of grid components, especially controlling the data package of PMUs, in regards to damaging data by external or internal attacks or malfunction reasons by using Kalman filter method [9]. Protection

against cyber attacks 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 in 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 helps 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 been also used as a random number generator [18, 19, 20] in cyber security applications like encryption [21, 22, 23] and data hiding [24]

In this work, a novel microcomputer-based 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, via an application server software, which communicates with IEEE C37.118.1 compliant PMU devices via the WireShark platform in realtime, 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 like PMUs.

The paper is organized as follows: In Section 2, methodologies for modern power system analysis is 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 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 upon 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 sub- stations 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 is given as

$$\mathrm{x\,(t)} = \mathrm{X_m cos\,(\omega t + \varphi)} \tag{1}$$

where ω and φ the resemble frequency of 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.

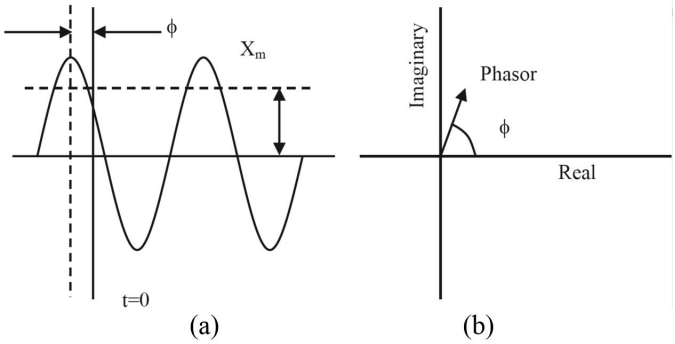


Figure 1: A sinusoid (a) and its representation as a phasor (b). The phase angle of the phasor is arbitrary, as it depends upon the choice of the axis $t = 0$.

Phasor representation is only possible for a pure sinusoid 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 kf_0 representation into Fourier series is shown as follows;

$$\begin{aligned} \mathrm{x\,(t)} &= \mathrm{a_k cos\,(2\pi kf_0 t) + b_k sin\,(2\pi kf_0 t)} \\ &= \left\{ \sqrt{\mathrm{a_k^2 + b_k^2}} \right\} \cos\left(2\pi \mathrm{kf_0 t} + \varphi\right) \ \text{where} \varphi = \arctan\left(\frac{-\mathrm{b_k}}{\mathrm{a_k}}\right) \end{aligned} \tag{2}$$

Here, the Fourier series coefficients a_k and b_k measure the amount of $\cos(2\pi \mathrm{kf_0 t})$ and $\sin(2\pi \mathrm{kf_0 t})$ present in the function $\mathrm{x(t)}$. Phasor representation of the signal becomes as;

$$\mathrm{X_k} = \frac{1}{\sqrt{2}} \left\{ \sqrt{\mathrm{a_k^2 + b_k^2}} \right\} \mathrm{e^{j\varphi}} \tag{3}$$

The complex form of Eq. (3) is constituted as follows,

$$\mathrm{X_k} = \frac{1}{\sqrt{2}} \left(\mathrm{a_k - jb_k}\right) \tag{4}$$

Using the relationship of the Fourier series coefficients with DFT, the phasor representation of

the k^{th} harmonic component is given by

$$\mathrm{X_k}{=}\tfrac{1}{\sqrt{2}}\tfrac{2}{\mathrm{N}}\sum_{\mathrm{n}=0}^{\mathrm{N}-1}\mathrm{x}\ (\mathrm{n}\Delta\mathrm{T})\,\mathrm{e}^{-\frac{\mathrm{j2kn}}{\mathrm{N}}} \tag{5}$$

$$\begin{aligned}\mathrm{X_k}{=}&\frac{\sqrt{2}}{\mathrm{N}}\sum_{\mathrm{n}=0}^{\mathrm{N}-1}\mathrm{x}\ (\mathrm{n}\Delta\mathrm{T})\left\{\cos\left(\frac{2\pi\mathrm{kn}}{\mathrm{N}}\right)-\mathrm{j}\sin\left(\frac{2\pi\mathrm{kn}}{\mathrm{N}}\right)\right\}\\ &\mathrm{x}\ (\mathrm{n}\Delta\mathrm{T}){=}\mathrm{x_n}\ \text{and}\ \theta=\frac{2\pi}{\mathrm{N}}\end{aligned} \tag{6}$$

where N is the number of samples in the data window, n is the sample number, $\mathrm{x_n}$ is the input sample, and θ refers to the sample angle. Then Eq. (6) becomes as follows;

$$\mathrm{X_k}{=}\tfrac{\sqrt{2}}{\mathrm{N}}\sum_{\mathrm{n}=0}^{\mathrm{N}-1}\mathrm{x_n}\left\{\cos\left(\mathrm{kn}\theta\right)-\mathrm{j}\sin\left(\mathrm{kn}\theta\right)\right\} \tag{7}$$

While separating sin and cosine part of $\mathrm{x_n}$ respectively as $\mathrm{X_{kc}}$ and $\mathrm{X_{ks}}$ in form of

$$\mathrm{X_k}{=}\mathrm{X_{kc}}{-}\mathrm{jX_{ks}}$$

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

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

Finally $\mathrm{X_k}$ is used to represent the phasor in most of the phasor computations. Phasor calculation is a continuous process so that updating phasor estimation as newer data samples are acquired. This is the simplest way for continuous phasor calculation and known as non-recursive phasor update method.

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

In Eq. (9), r = -1,1,2,3,.. 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 total number of samples i.e. N remains same.

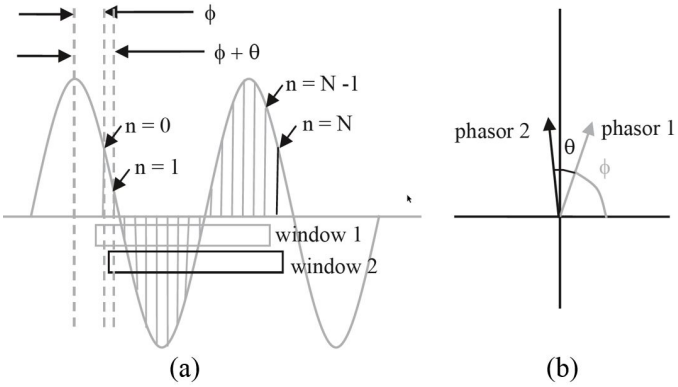


Figure 2: Non-recursive update of phasor estimates with N sample windows.

As seen in Figure 2, phasor 1 is calculated with samples n = 0,...,N-1, while phasor 2 is calculated with samples n =1,2,...,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 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".

$$\begin{aligned} &X^{N+r}=X^{N+(r-1)}+ \\ &\frac{\sqrt{2}}{N}\sum_{n=0}^{N-1}\left(x_{N+r}-x_r\right)\left\{\cos n\theta - j\sin n\theta\right\} \end{aligned} \tag{10}$$

In Eq. (10), r = 0,1,2,3,.. when r represents the present state, (r-1) represents the past state. As seen in Eq.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 non-recursive 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 systems(GPS) receivers, take highly precise measurements of voltages and currents within defined time-stamps. Here, the GPS receivers coordinate the synchronization of the several current and voltage measurements [26]. PMUs use recursive algorithm for calculating symmetrical components of voltage and current like 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.1 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]. Processings data of PMUs are used as improving for stability coordinations [29], power system state estimation [30], remedial action schemes [31] and disturbance monitorings [32]. On the other hand, linearization mainly occurs when the state vector, as well as the PMU measurements are 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 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 IEEE-14 bus system has been established by depth first search method [35, 36, 37, 38]. In this study, an IEEE-14 busbar system is used and the optimum PMU placement is installed on studied busbar system. Then after, a microcomputer-based 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 the busbars $\{1, 4, 6, 8, 10 \text{ and } 14\}$, 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.

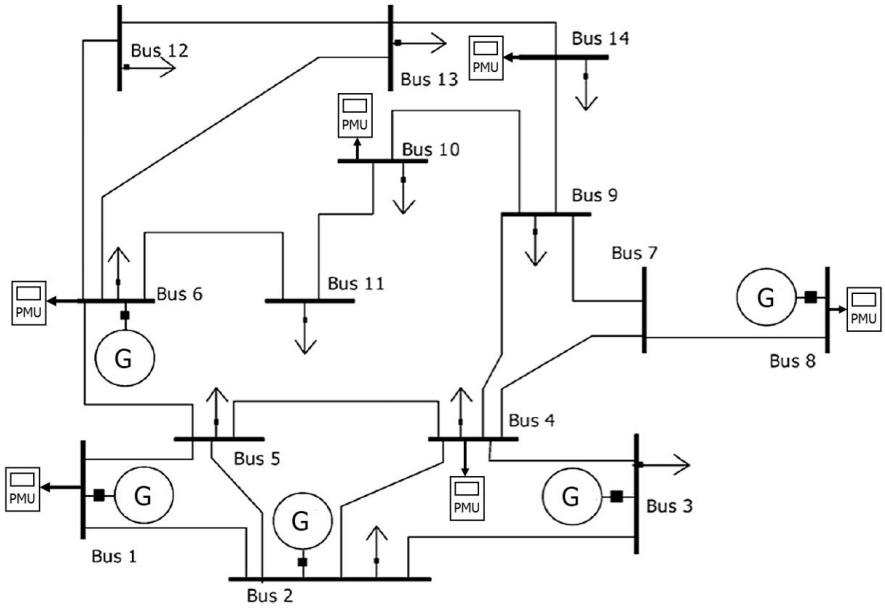


Figure 3: IEEE-14 Busbar PMU Built-in Model with Depth First Search Algorithm

Table 1: Measurable Phasor Lines of 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

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 16 bit CRC data integrity controller. The phasor data consists of frequency (f), voltage magnitude ($\mathrm{m\_V}$), voltage phase angle (δ_V), current magnitude ($\mathrm{m\_I}$) and current phase angle (δ_I) of the busbar.

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

3. A Novel Security Methodology For Smart Grids

Getting a correct phasor calculation in the studied IEEE-14 busbar system depends on an appropriate placing of PMU devices with adequate numbers. A correct phasor calculation depends also 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 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 grid uses 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-base application at PMU sides and a server-base application software at PDC side handles together the microcomputer-based hyperchaotic encryption processes of captured PMU data.

As seen in Fig.5, the Rasp3 unit operates as one of the PMU devices that encrypts the digital phasor packet data in harmony with IEEE C37.118.1 protocol using the chaos encryption engine. While connecting remained PMU units on IEEE-14 bus system except the 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.

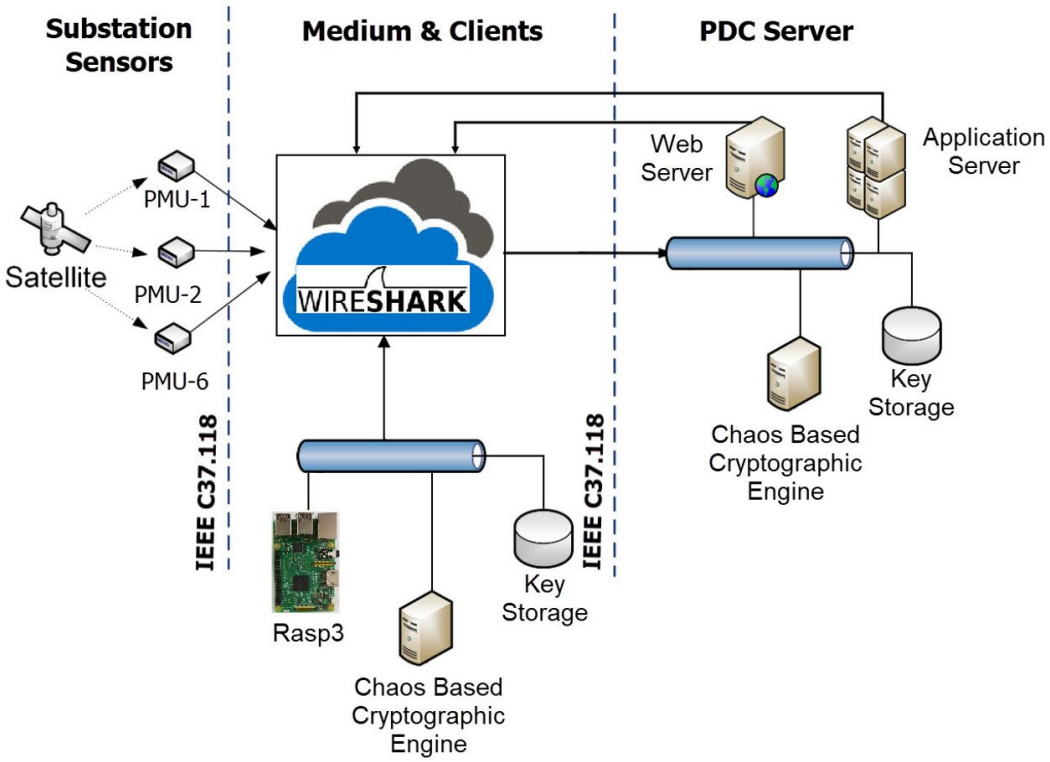


Figure 5: Overall PMU Based Chaotic Cryptography Scheme

As seen in Fig.6, studied realtime data acqusition of PMU devices are acquired by IEEE C37.118.1 compliant WireShark platform. The application server both manages PMU and PDC sides with a chaotic cryptographic engine.

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

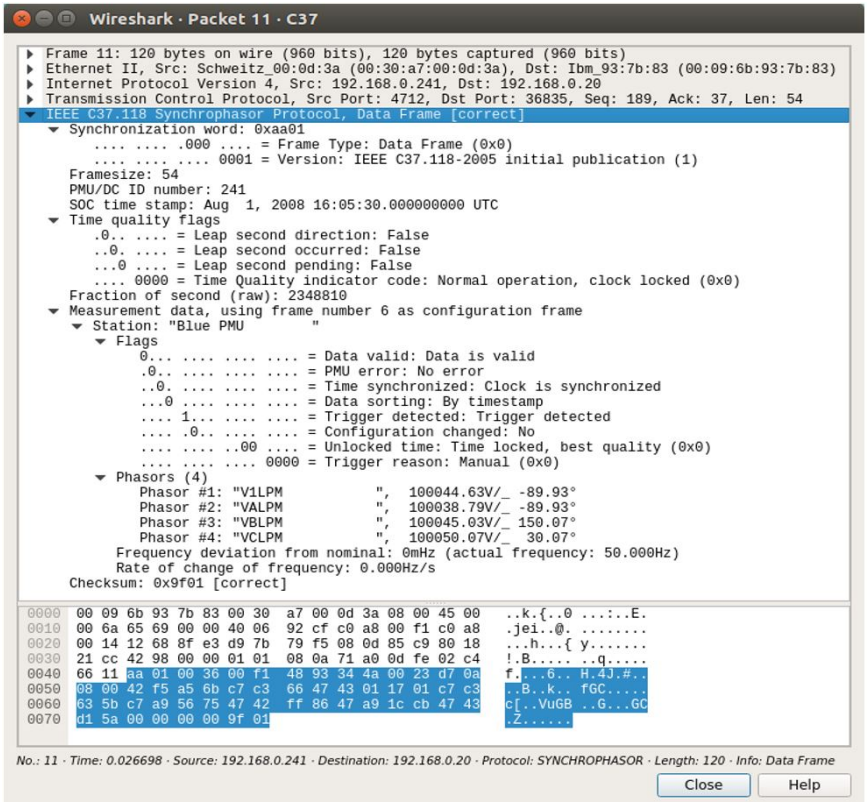


Figure 6: Studied IEEE C37.118.1 Frames Captured by Wireshark Network Protocol Analyzer Software

same sequence using the same chaotic system. Then, PMU data is 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 are used [41, 42, 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 V. 5D hyperchaotic Lorenz system is set as follows:

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

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

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

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

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

$$J = \begin{bmatrix} -\sigma & \sigma & 0 & 1 & 0 \\ r & -1 & 0 & 0 & -1 \\ 0 & 0 & -\beta & 0 & 0 \\ 0 & 0 & 0 & p & 0 \\ 0 & q & 0 & 0 & 0 \end{bmatrix} \tag{13}$$

We study the dynamics around the original equilibrium point E0 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;

$$(\lambda - \mathrm{p})\left(\lambda + \tfrac{8}{3}\right)\left(\lambda^3 + 11\lambda^2 + (q - 270)\,\lambda + 10q\right) = 0 \tag{14}$$

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

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 5D hyperchaotic system are gathered by using Matlab ODE45 solver and the phase portraits of the hyperchaotic system are depicted in Fig. 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.

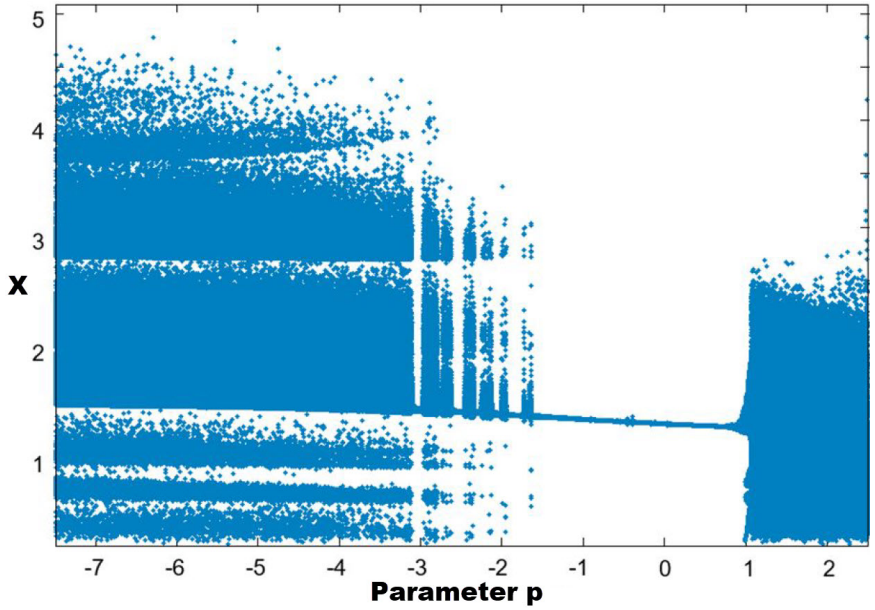
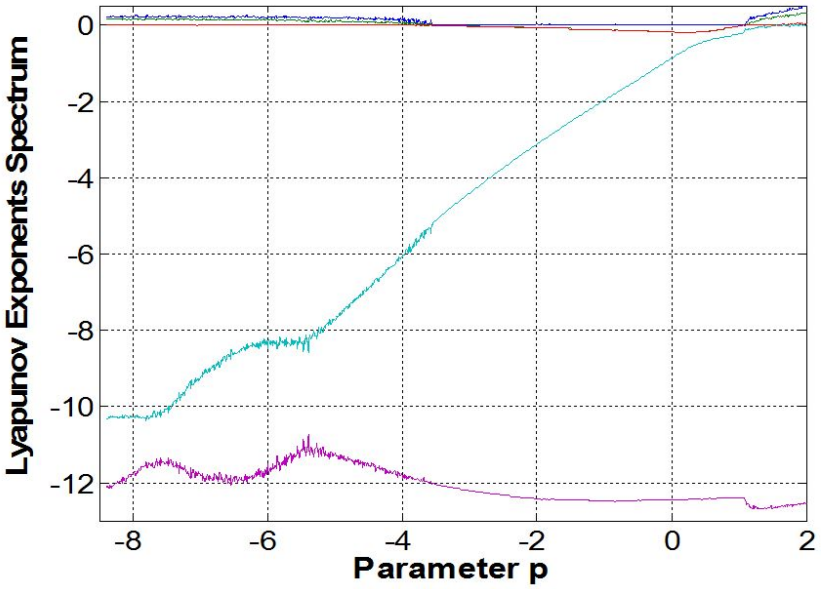


Figure 7: Bifurcation diagram for p parameter varies between -8 and 3.

In Figure 8a and 8b , it is also revealed that the system falls into 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.



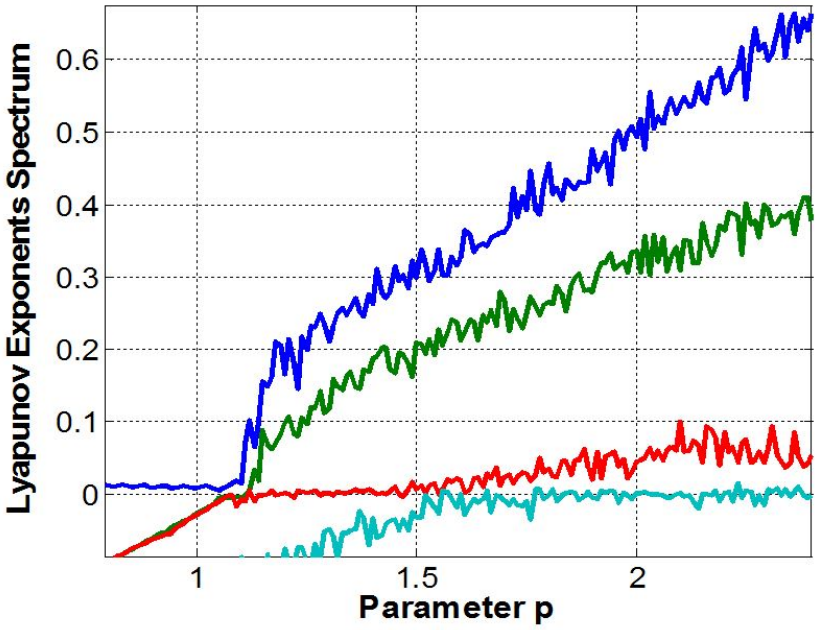
(a)

5. Random Number Generator Design And Its Statistical Test

5.1. RNG design with a 5D hyperchaotic system

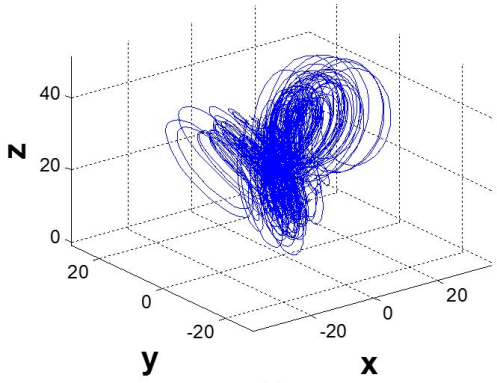
Many chaotic systems are used to generate pseudo random numbers as a source of entropy because they are complex and very sensitive to the initial conditions. In this section, an RNG design is proposed for PMU data encryption which is implemented in Raspberry 3.

A 5D hyperchaotic system developed in the proposed RNG design is given in Equation 11, where σ, r, β, p, q are the parameters and x, y, z, u, w are the state variables. To visualize dynamic behaviors and solutions of the proposed 5D hyperchaotic system, the differential equations given in Eq. 11 are worked out using Matlab ode45 function. The obtained phase portraits of 5D hyperchaotic system are depicted in Fig. 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 $(0, -0.01, 9, 1, 0)$.



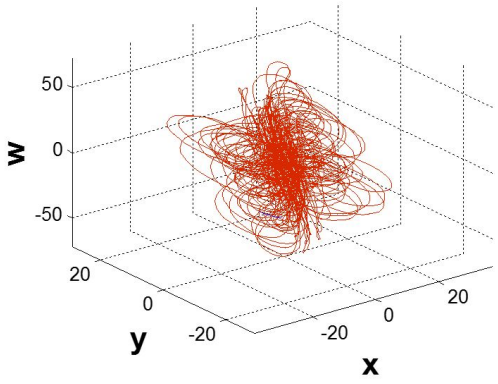
(b)

Figure 8: The Lyapunov exponents of 5D hyperchaotic system for p parameter varies between a) -8 and 3, b)-1.5 and 2.5.



(a)

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



(b)

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

in order to discretize the hyperchaotic time series using Runga-Kutta-4 (RK4) method. Then, the obtained floating numbers based on outputs of separate from each set of bits (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 1Mbit random numbers are then used in one communication session. For this aim, a 1Mbit 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 is considered for the test.

To prove the randomness of the generated number series NIST-800-22 tests are employed. The NIST-800-22 have 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]. The NIST-800-22 are applied to the random numbers generated in step 11.

Algorithm: Random Number Generation Algorithm Pseudo code

Input: Parameters and initial condition of chaotic systems
Output: Random numbers tested statistically
1: Accepting system parameters and initial condition of 5D Lorenz hyperchaotic system
2: Determination of the value of Δh
3: Sampling with determination Δh value for RK4
4: WHILE (minimum 1MBit 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 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 1MBit data
12: IF (test results == pass) **THEN**
13: Successful results
13: Ready tested random numbers for RNG applications
14: ELSE
15: Go to step 4
16: END IF
17: EXIT

5.2. Statistical Tests

The NIST-800-22 tests 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 are only used from w for PMU data encryption.

ENT is another randomness test that has five different tests, which define the randomness of a 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 can be seen the successful results for all tests.

The proposed microcomputer-based 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 have the best results in arithmetic mean test because the ideal result is 127.5. But, the entropy test result is not good according to other methods except from [49].

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-Sums 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
Non-Overlapping 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-Excursions Test	0.2953	0.6938	0.8843	0.4569
Random-Excursions 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

Entropy, correlation and Monte Carlo test results are the best in [50] with $7.9999, 0.000108$ and 3.14062, respectively. [51] and [49] haven't the Chi-square test result. In the proposed method, test results are suitable and acceptable for cryptographic application because of the random numbers passed all tests.

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 et al. [51]	127.5013	7.9975	-0.000147	-	3.140569 error=0.03
Seetharam et al. [49]	122.885	7.7133	-0.058927	-	3.088126 error=1.70
Akhshani et al. [50]	127.7714	7.9999	0.000108	255.19	3.14062 error=0.031

6. PMU Data Encryption Application And Its Security Analysis

6.1. PMU Data encryption application with 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 like FPGA, computers, etc. In this work, a low-cost RNG is designed by means of 64-bit quad-core ARM Cortex-A53 microprocessor based "Raspberry Pi 3" (1.2 GHz, 4 cores, 1 GB RAM) microcomputer.

In this section, PMU data encryption and decryption system using the RNG designed with 5D hyperchaotic system and passed all the NIST-800-22 tests is presented. The block diagram of the encryption processes is given in Fig. 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.

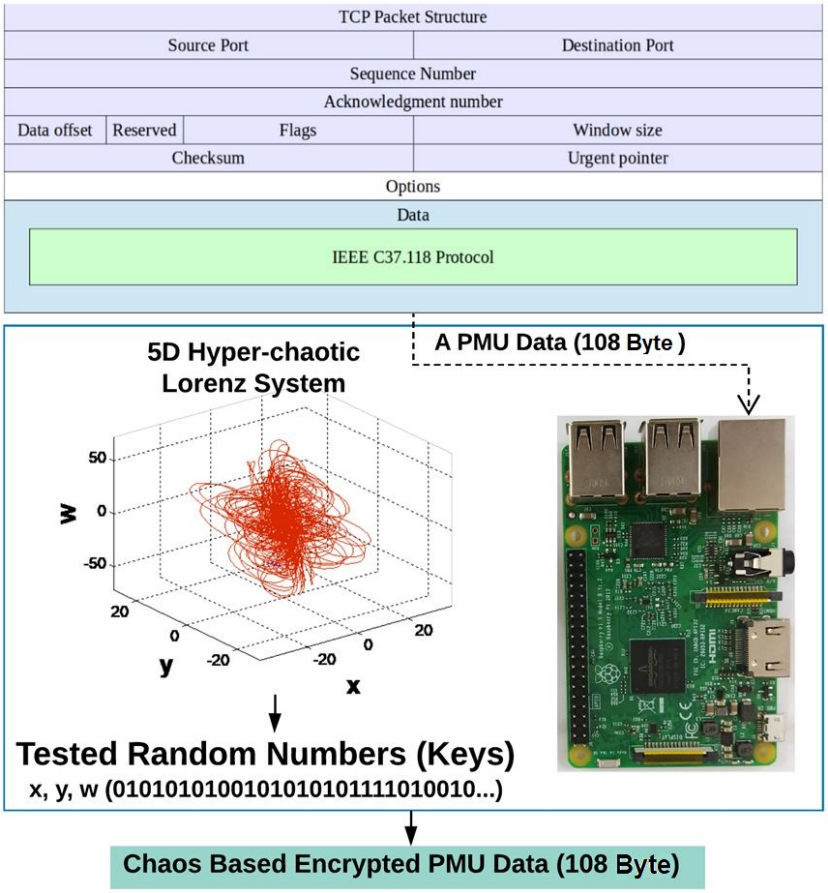


Figure 10: Microcomputer-based with a Hyperchaotic System Encryption Process

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

$aa01003600f14893334f003d70a4080047c3659cbfc8e73947c3631cbfc8e52b47c365574027a0d447c368643f065a850000000042a9$

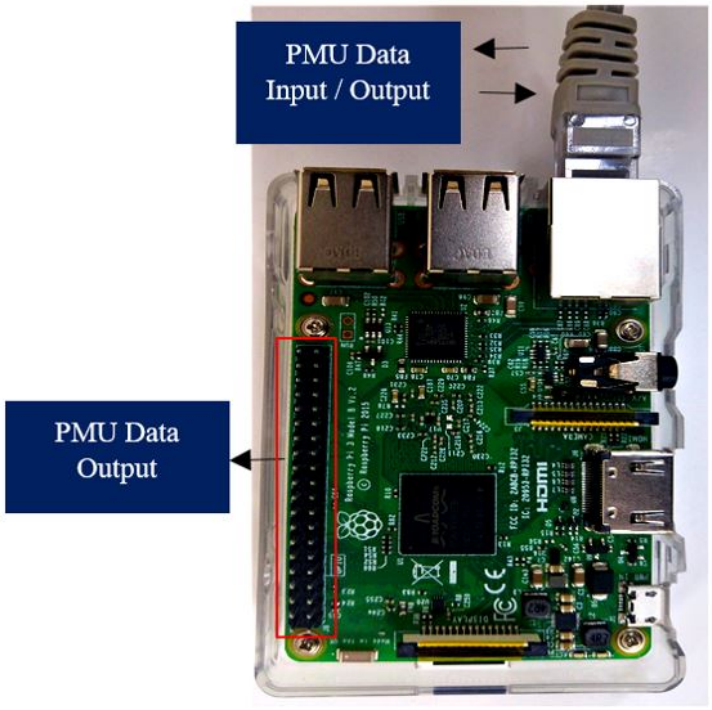


Figure 11: PMU Data Input / Output Ports in Raspberry Pi 3

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

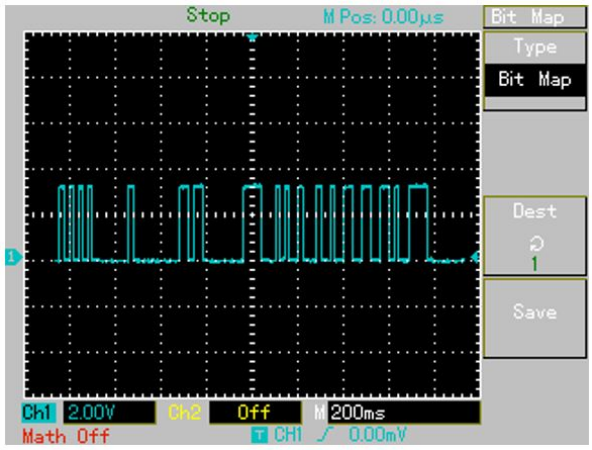


Figure 12: Original PMU Data

Some bit of encrypted binary 864 bit PMU data is shown Fig. 12. The size of the encrypted data is same as 864 bit, because of the encryption process is done for bit by bit.

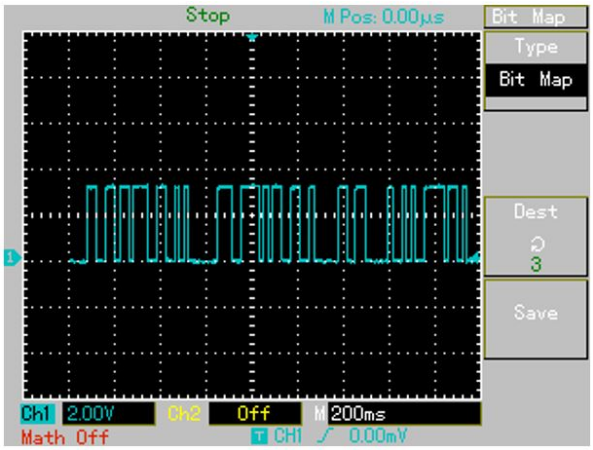


Figure 13: Encrypted PMU Data

Also, PMU data consists of all encrypted characters is as follows. Some of them are shown in Fig. 13 as binary data.

$cdb9940e7acc83304a7b45eb40617c53409cb959ff461539f8fba898b9eadf7a048fd1d14b1be5b995b057$
$6e407edf6eea721f14b40f$

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 data as 1s and 0s in a 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 Fig. 14 for original and encrypted data. The number of 0s is 690, the number of 1s is 174 in original PMU data. Encrypted PMU data bit series contains 425 0s and 439 1s. Difference between bits decreased from 516 to 14 after the encryption.

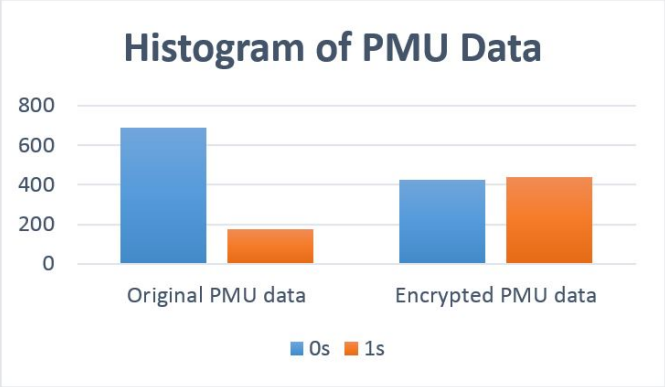


Figure 14: Histogram distribution of PMU Data

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. The chaotic system (11) in this paper has 5 (x, y, z, u and w) 10^{70} and 5 (σ, r, β, 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 like initial conditions and parameters. In a very tiny mistake cannot be reached the true results and will lead to different results because of a little mistake will cause another one.

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 have 1.2 GHz, 4 cores, 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.

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

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 other hand, 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 byte in our method. These results are very suitable for real-time applications, especially in smart grids.

7. Conclusion

In this study, it is the first time in the literature using microcomputer-based with a hyperchaotic system encryption algorithm for allowing PMU devices used in 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 a developed application server software. The application server communicates with IEEE C37.118.1 compliant PMU devices via the WireShark platform in realtime. 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 analysis and finally strength of cryptography with NIST tests.

The results show that measured total delay of 0.21 ms including both encryption and decryption durations, the proposed microcomputer-based encryption algorithms can provide a shorter delay while performing encryption and can be directly embedded as encryption hardware units into 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, it can also be embedded into electronic cards, smartcards, or smart tokens which are utilized for authentication among smart grid components.

Acknowledgment

This work is supported by the Scientific and the Research Council of Turkey (TUBITAK) under Grant No. 117E284. This work is also supported by Scientific Research Committes of Sakarya University of Applied Sciences with Grant Number 2019-1-1-093.

Conflict of Interest

The authors declare that they have no conflict of interest.

References

[1] M. A. Pai, D. Chatterjee, Computer techniques in power system analysis, McGraw-Hill Education (India), 2014.

[2] J. Vlach, V. Jiří, K. Singhal, Computer methods for circuit analysis and design, Springer Science & Business Media, 1983.

[3] A. R. Bergen, Power systems analysis, Pearson Education India, 2009.

[4] M. Damrudi, N. Ithnin, Parallel rsa encryption based on tree architecture, Journal of the Chinese Institute of Engineers 36 (5) (2013) 658–666.

[5] R. Khan, K. McLaughlin, D. Laverty, S. Sezer, Analysis of ieee c37. 118 and iec 61850-90-5 synchrophasor communication frameworks, in: 2016 IEEE power and energy society general meeting (PESGM), IEEE, 2016, pp. 1–5.

[6] A. Apostolov, Impact of iec 61850 on the interoperability and reliability of protection schemes, in: 2013 IEEE Power & Energy Society General Meeting, IEEE, 2013, pp. 1–5.

[7] X. Dong, H. Lin, R. Tan, R. K. Iyer, Z. Kalbarczyk, Software-defined networking for smart grid resilience: Opportunities and challenges, in: Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, 2015, pp. 61–68.

[8] J. Abawajy, R. J. Robles, Secured communication scheme for scada in smart grid environment, Journal of Security Engineering 7 (6) (2010) 12.

[9] M. N. Kurt, Y. Yılmaz, X. Wang, Real-time detection of hybrid and stealthy cyber-attacks in smart grid, IEEE Transactions on Information Forensics and Security 14 (2) (2018) 498–513.

[10] L. Coppolino, L. Romano, et al., Exposing vulnerabilities in electric power grids: An experimental approach, International Journal of Critical Infrastructure Protection 7 (1) (2014) 51–60.

[11] F. Dachselt, W. Schwarz, Chaos and cryptography, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 48 (12) (2001) 1498–1509.

[12] Z. Wei, A. Akgul, U. E. Kocamaz, I. Moroz, W. Zhang, Control, electronic circuit application and fractional-order analysis of hidden chaotic attractors in the self-exciting homopolar disc dynamo, Chaos, Solitons & Fractals 111 (2018) 157–168.

[13] M. Varan, A. Akgul, Control and synchronisation of a novel seven-dimensional hyperchaotic system with active control, Pramana 90 (4) (2018) 54.

[14] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. Garcia-Ojalvo, C. R. Mirasso, L. Pesquera, K. A. Shore, Chaos-based communications at high bit rates using commercial fibre-optic links, Nature 438 (7066) (2005) 343.

[15] I. Dalkiran, K. Danisman, Artificial neural network based chaotic generator for cryptology, Turkish Journal of Electrical Engineering & Computer Sciences 18 (2) (2010) 225–240.

[16] M. Alçın, İ. Pehlivan, İ. Koyuncu, Hardware design and implementation of a novel ann-based chaotic generator in fpga, Optik 127 (13) (2016) 5500–5505.

[17] R. Enayatifar, A. H. Abdullah, I. F. Isnin, Chaos-based image encryption using a hybrid genetic algorithm and a dna sequence, Optics and Lasers in Engineering 56 (2014) 83–93.

[18] T. Stojanovski, L. Kocarev, Chaos-based random number generators-part i: analysis [cryptography], IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 48 (3) (2001) 281–288.

[19] T. Stojanovski, J. Pihl, L. Kocarev, Chaos-based random number generators. part ii: practical realization, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 48 (3) (2001) 382–385.

[20] M. Z. Yildiz, O. Boyraz, E. Guleryuz, A. Akgul, I. Hussain, A novel encryption method for dorsal hand vein images on a microcomputer, IEEE Access 7 (2019) 60850–60867.

[21] A. Akgul, I. Moroz, I. Pehlivan, S. Vaidyanathan, A new four-scroll chaotic attractor and its engineering applications, Optik 127 (13) (2016) 5491–5499.

[22] S. Akkaya, I. Pehlivan, A. Akgül, 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 33 (3) (2018) 1171–1182.

[23] M. A. Jafari, E. Mliki, A. Akgul, V.-T. Pham, S. T. Kingni, X. Wang, S. Jafari, Chameleon: the most hidden chaotic flow, Nonlinear Dynamics 88 (3) (2017) 2303–2317.

[24] A. Akgul, S. Kacar, B. Aricioglu, A new two-level data hiding algorithm for high security based on a nonlinear system, Nonlinear Dynamics 90 (2) (2017) 1123–1140.

[25] A. G. Phadke, J. S. Thorp, Synchronized phasor measurements and their applications, Vol. 1, Springer, 2008.

[26] K.-S. Cho, J.-R. Shin, S. H. Hyun, Optimal placement of phasor measurement units with gps receiver, in: 2001 IEEE Power Engineering Society Winter Meeting. Conference Proceedings (Cat. No. 01CH37194), Vol. 1, IEEE, 2001, pp. 258–262.

[27] A. G. Phadke, Synchronized phasor measurements-a historical overview, in: IEEE/PES transmission and distribution conference and exhibition, Vol. 1, IEEE, 2002, pp. 476–479.

[28] W. Lewandowski, J. Azoubib, W. J. Klepczynski, Gps: Primary tool for time transfer, Proceedings of the IEEE 87 (1) (1999) 163–172.

[29] J. Chen, A. Abur, Placement of pmus to enable bad data detection in state estimation, IEEE Transactions on Power Systems 21 (4) (2006) 1608–1615.

[30] D. Kosterev, J. Esztergalyos, C. Stigers, Feasibility study of using synchronized phasor measurements for generator dropping controls in the colstrip system, IEEE Transactions on Power Systems 13 (3) (1998) 755–761.

[31] J. Bertsch, C. Carnal, D. Karlson, J. McDaniel, K. Vu, Wide-area protection and power system utilization, Proceedings of the IEEE 93 (5) (2005) 997–1003.

[32] Z. Zhong, C. Xu, B. J. Billian, L. Zhang, S.-J. Tsai, R. W. Conners, V. A. Centeno, A. G. Phadke, Y. Liu, Power system frequency monitoring network (fnet) implementation, IEEE Transactions on Power Systems 20 (4) (2005) 1914–1921.

[33] Z. Miljanić, I. Djurović, I. Vujošević, Optimal placement of pmus with limited number of channels, Electric Power Systems Research 90 (2012) 93–98.

[34] N. M. Manousakis, G. N. Korres, Optimal allocation of phasor measurement units considering various contingencies and measurement redundancy, IEEE Transactions on Instrumentation and Measurement.

[35] R. Sodhi, S. Srivastava, S. Singh, Optimal pmu placement method for complete topological and numerical observability of power system, Electric Power Systems Research 80 (9) (2010) 1154–1159.

[36] R. Emami, A. Abur, Robust measurement design by placing synchronized phasor measurements on network branches, IEEE Transactions on power systems 25 (1) (2009) 38–43.

[37] G. N. Korres, N. M. Manousakis, T. C. Xygkis, J. Löfberg, Optimal phasor measurement unit placement for numerical observability in the presence of conventional measurements using semi-definite programming, IET Generation, Transmission & Distribution 9 (15) (2015) 2427–2436.

[38] M. Korkali, 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, IEEE, 2010, pp. 3445–3448.

[39] K. Martin, G. Brunello, M. Adamiak, G. Antonova, M. Begovic, G. Benmouyal, P. Bui, H. Falk, V. Gharpure, A. Goldstein, et al., An overview of the ieee standard c37. 118.2—synchrophasor data transfer for power systems, IEEE Transactions on Smart Grid 5 (4) (2014) 1980–1984.

[40] K. Amare, V. A. Centeno, A. Pal, Unified pmu placement algorithm for power systems, in: 2015 North American Power Symposium (NAPS), IEEE, 2015, pp. 1–6.

[41] F. Zhang, R. Chen, X. Wang, X. Chen, C. Mu, X. Liao, Dynamics of a new 5d hyperchaotic system of lorenz type, International Journal of Bifurcation and Chaos 28 (03) (2018) 1850036.

[42] Q. Yang, C. Chen, A 5d hyperchaotic system with three positive lyapunov exponents coined, International Journal of Bifurcation and Chaos 23 (06) (2013) 1350109.

[43] Q. Yang, M. Bai, A new 5d hyperchaotic system based on modified generalized lorenz system, Nonlinear Dynamics 88 (1) (2017) 189–221.

[44] A. Wolf, J. B. Swift, H. L. Swinney, J. A. Vastano, Determining lyapunov exponents from a time series, Physica D: Nonlinear Phenomena 16 (3) (1985) 285–317.

[45] A. AKGÜL, C. ARSLAN, B. ARICIOĞLU, Design of an interface for random number generators based on integer and fractional order chaotic systems, Chaos Theory and Applications 1 (1) (2019) 1–18.

[46] J. Soto, Statistical testing of random number generators, in: Proceedings of the 22nd National Information Systems Security Conference, Vol. 10, NIST Gaithersburg, MD, 1999, p. 12.

[47] J. Walker, Ent: A pseudorandom number sequence test program, 2008, Access available at http://www. fourmilab. ch/random.

[48] I. Jang, H. S. Yoo, Pseudorandom number generator using optimal normal basis, in: International Conference on Computational Science and Its Applications, Springer, 2006, pp. 206–212.

[49] D. Seetharam, S. Rhee, An efficient pseudo random number generator for low-power sensor networks [wireless networks], in: 29th Annual IEEE International Conference on Local Computer Networks, IEEE, 2004, pp. 560–562.

[50] A. Akhshani, A. Akhavan, A. Mobaraki, S.-C. Lim, Z. Hassan, Pseudo random number generator based on quantum chaotic map, Communications in Nonlinear Science and Numerical Simulation 19 (1) (2014) 101–111.

[51] B. Stoyanov, K. Kordov, A novel pseudorandom bit generator based on chirikov standard map filtered with shrinking rule, Mathematical Problems in Engineering 2014.