International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

An Efficient Cryptography Key Management for Secure Communications in Smart Metering

Abdul Khadar Asundi, Pradeep Basavaraj Jyoti, Mudakapla Shadaksharappa Nagaraj, Shabana Sarmas Sultan

Abstract*: Smart Grid (SG) is used in power systems to enhance environmental sustainability and increase the efficiency of energy management. In Smart Grid systems, Smart Meter (SM) is one of the most important devices. The SM is an advanced energy meter that receives data from the load devices of end users and computes the customer's energy consumption. After that these smart meter transfers the information to the utility company and/or system operator. The secure data transmission is the main issue between the smart meters to the smart grid. Because the advanced metering architecture is vulnerable to the cyber-attacks. In order to ensure the security of smart meter data, the cryptography based encryption techniques are used in the SG. In this paper, the secure data transmission between the SM and the SG is performed by RSA cryptography. The communication over the devices performed by Binary Phase Shift Keying (BPSK). Here, the data from the SM encrypted using RSA encryption technique and then it transmitted using BPSK to SG. At last, at the smart grid the RSA decryption technique is used to decrypt the power values from various loads. The introduced RSA based encryption key management mechanism used to provide the end to end security in the smart metering communications. The access of the data is limited by providing the key to the authorized end users for enhancing the confidentiality of the data transmission. This proposed method is named as BPSK-RSA methodology. The performance of this BPSK-RSA methodology evaluated using energy consumption of the load devices. Then the performance of BPSK-RSA methodology is compared with DFT based CHE in terms of Mean Square Error (MSE). By taking the average, the MSE of BPSK-RSA methodology is improved at 5.02% than the DFT based CHE. The performance of the BPSK-RSA methodology is also compared with ECC-SM method in terms of Packet Delivery Ratio (PDR), Throughput (TH) and End to End Delay (EED). The PDR, TH and EED of BPSK-RSA methodology are improved at 2.95%, 6.24% and 19.64% than the ECC-SM method at 100 smart meter placement.

***Index Terms*: Smart Grid, Smart metering, Binary Phase Shift Keying, RSA cryptography, energy consumption.**

I. INTRODUCTION

The traditional power grid system had some issues like large maintenance costs, scalability issues and lack of system monitoring. Due to these drawbacks the traditional power grid system is replaced by a next generation electronic system, which is called as called Smart Grid (SG) [1-2]. Traditionally the power grid adopts only one-way supply model in power distribution. But the smart grid provides the dual way interaction between the users and the power authority. Also, it uses the advanced control capabilities to create, distribute and consume the electricity effectively compared to the power grid [3-4]. SG is a global networked cyber-physical system, it is effectively constructed to provide the global electric energy flow in the main electric lines and also in the single households [5]. The integration of sensors and advanced communication technologies with conventional power grid is called as a smart grid. SG is used for efficient power generation, monitor the real-time power consumption, accurate billing, and enable demand response [6]. With modern communication technologies and automated control, the SG has become a next generation electricity grid to provide better reliability and efficiency. The electric power grid infrastructure enhanced by designing an overlay communication and computing network in SG [7]. SG represents the bi-directional communication power flow between the two concerned entities, i.e. Consumer and Grid [8]. The smart meters are introduced at end-users for transferring the energy information to the grid. Based on this, the smart grid gathers the real time energy demand from the users that helps to fulfil the load requirements [9]. SM has the capacity of monitoring and controlling power consumption by end users. SM gathers the data from the smart appliances of the home and then it conveys the resident's information about the usage of electricity [10]. SM allows people to organize their daily routines based on the bill details and also provide information that helps them to decrease their monthly power consumption bills [11]. A reliable and real time information about the SG becomes a crucial factor for providing reliable power to the end users of the generating units [12]. The security in the data network is an issue in terms of data confidentiality and integrity. Here, the smart grid lags in data protection from the unauthorized users [13]. The conventional methods which are associated with the SG's data transmission are given as follows: A hybrid hierarchical network is introduced for cost effective data transmission and this is a combination of wired (copper cable/optical fiber) and wireless (cellular/IEEE 802.15.4) standards. This proposed formulation is generic and also it addresses real world scenarios with asymmetric sensor data generation, unreliable wireless link behavior, non-uniform cellular coverage, etc. [14].

Manuscript published on 30 August 2019.
***Correspondence Author(s)**
Abdul Khadar Asundi, Department of Electrical and Electronics Engineering, Ballari Institute of Technology and Management, Ballari, India.
Pradeep Basavaraj Jyoti, Department of Electrical and Electronics Engineering, PDIT, Hospet, India.
Mudakapla Shadaksharappa Nagaraj, Department of Electrical and Electronics Engineering, Bapuji Institute of Engineering and Technology, Davangere, India.
Shabana Sarmas Sultan, Department of Electronics and Communication Engineering, Govt. Polytechnic Ballari, Davangere, India.

The top-k query is a cluster topology sensor network, which is used in smart grid to transfer the data from one side to the other side. The query routing is optimized by using the local indices in top k-query as well as it is used to cut down the data traffic inside the cluster [15]. Generally, the SM is placed outside of the house and this SM is protected only by using the mechanical lock. The hacker can hack the information from the SM. Additionally, the data transmission between SM to the operator is insecure. So, here the secure communication among the smart meter to the utility is improved by using the cryptography technique.

The main contributions of this research work are stated as follows:

- Here the security of the communication is enhanced by using the RSA cryptography technique. The introduced RSA is used to overcome the threats against the cyber-attacks.
- The data transmission through the smart meter to grid utility is performed using BPSK technique. The complexity of the BPSK modulation scheme is less. Besides, the data transmitted using BPSK can transmitted at high distance due to the 180° phase shift.
- The combination of the BPSK with RSA cryptography techniques used to enhance data transmission security in the smart metering architectures.
- The proposed methodology is evaluated in terms of energy consumption of load devices at the end users.
- The organization of the entire paper is given as follows: The works related to the smart metering communications is described in section 2. The smart metering communication using BPSK with RSA cryptography is clearly explained in section 3. The performance of the BPSK-RSA methodology is evaluated in the section 4. Then the conclusion is given in the section 5.

II. LITERATURE REVIEW

Z.A. Khan et al. [16] presented the stochastic load modelling of smart meter data, and this process has four stages, those are data clustering, curve smoothing and linearization of curves, optimizing the linear curves and finally energy classification. This approach made the smart meter data into a manageable level that is made by linearizing energy consumption patterns. The extended k-means clustering and particle swarm optimization used in data clustering and optimizing the linear curves respectively. The processing time over the SG is less as well as it decreases the complexity among the load profiles with other uncertainties. The highly nonlinear complex load profiles are difficult to process by the linear system. K. V. Deshpande and A. Rajesh [17] presented the Machine to Machine (M2M) communications for smart metering applications. The Improved M2M Clustering Process (IMCP) based clustering technique introduced in the M2M communications. The evolved Node B (eNB) can control a number of M2M devices. In a network, the congestion will happen when all M2M devices access the eNB. Because of that, the clustering was utilized to reduce the number of devices accessing the eNB and also it saved the overall system's energy. The communication of this M2M network can be easily hacked, because there is no security technique used in this method. S. Aleksic and V. Mujan [18] presented the holistic framework for computing the environmental impact of SMs and Information and Communication Technology (ICT) equipment needed for home area network and advanced metering infrastructure. The energy based life cycle assessment (E-LCA) method presents the environmental impact of the ICT equipment. The fundamental laws of thermodynamics used in this paper for estimating the accurate environmental effects. However, to reduce the cumulative embodied energy consumption, more SM are required. U. B. Baloglu and Y. Demir [19] introduced the lightweight data aggregation technique in smart metering architecture. Initially, the information from the SMs collected in terms of time series. Then the collected data perturbed and encrypted using a Decisional Diffie-Hellman (DDH) scheme. This scheme was used to communicate with smart meters and privacy preserving nodes. Privacy protection is required in this smart metering, because the data transmission between the metering devices and task scheduler is considered as open to attacks from the malicious users. J.-S. Chou and G.A.N. Yutami [20] presented the structural equation modelling for analyzing the data which were surveyed from the Indonesia households. The interacting factors in consumer acceptance of SMs are determined by the structural equation modelling. The Consumer Adoption Propensity (CAP) index developed for the smart meter development which measures the consumers' tendency to accept and adopt residential smart meters based on the analytical results of SEM. This research work excludes some factors such as climate and natural resources. Wang, H.J et al. [21] has introduced the Long Term Evolution (LTE) based smart grid communication network. In this LTE, orthogonal frequency division multiple access (OFDMA) is used for downlink. Here, there are three channel estimation (CHE) schemes are analysed such as Least Square (LS), Minimum Mean Square Error (MMSE) and Discrete Fourier Transform (DFT). In this work, the clear description about the transmitted data using LTE network is not provided. Wu, F et al. [22] has introduced the Authenticated Key Agreement (AKA) scheme with elliptic curve cryptography (ECC) for the smart grid communication. The negligible probability of the attacker is provided by using the formal proof for AKA. In this smart grid, the secure communication is enabled among SM and service provider through the wireless communication channel. The ECC cryptography used in this SM communications has more complexity and also it is difficult to implement.

III. BPSK-RSA METHODOLOGY

In this BPSK-RSA methodology, the power grid is used for distributing the power to the number of loads (for example house 1, house 2 and house 3) which is present in certain areas.

Retrieval Number: I7846078919/19©BEIESP
DOI: 10.35940/ijitee.I7846.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Here, 3 houses have been considered as a load for this paper and the SM is used to monitor the day by day utilization of power in the smart grid. SM helps to measure the electricity used by the loads and the communication through the SM to the SG is performed by BPSK modulation. Only the mechanical lock generally secures the smart meters. The hackers can easily access the user's data. So, the RSA cryptography is used to enhance the security of the smart grid communication. The following Fig. 1 illustrates the block diagram of the BPSK-RSA methodology.

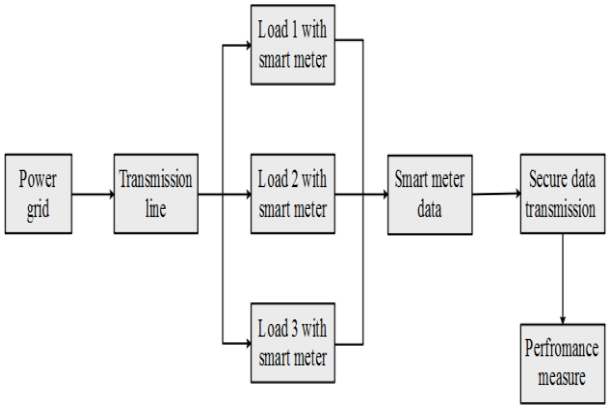


Fig. 1. Block diagram of the BPSK-RSA methodology

A. Smart meter

The power grid technology is considered the smart grid as the main source for transmission and distribution of the power to the respective loads. In that, the SM is considered as the main component. The SM is an electricity meter which reads and records a user's power consumption. The conventional metering system collects the readings from the service providers. But in smart metering system, the meters send the readings directly to end users for impartial and error-free billing purpose. The transmit/receive power is monitored by each device and also these devices create alarm (i.e., notification) and connect or detach a customer energy source when the error occurs in the SG. The smart meters are required for every premise and household, because the smart meter provides accurate billing, power usage monitoring of household devices and power on/off to the utility company. The power supply of a premise can be remotely terminated using a termination function of smart meters. This smart meter provides a data collection service for the remote monitoring interface known as Advanced Metering Infrastructure (AMI). The AMI uses the smart meters for data collection, measuring and analyzing the electricity and it also offers two-way communication with service providers. The AMI system has various technologies and applications which consists of smart meters, home area network, meter data management systems, wide area communications infrastructure, and user gateways. These are integrated to perform as one system. The smart meter has two different standards such as the American National Standards Institute (ANSI) and International Electro Technical Commission (IEC).

a. The architecture of smart meter

The smart meter has various modern components such as data computation using software system, hardware system for supporting the digital reading with several electrical and electronic sub devices and energy utility reading by a calibration mechanism. The smart meter architecture is given in Fig. 2. The general components that are available in the SM systems are data communication, supervisory module, system-on-chip metering system, module for power management, transformer driver, module for computing the forms of tampering, voltage reference, clock that works in real time, etc. The main component of the SM is system-on-chip processor. In its front end, the analog to digital converter used for supporting the differential inputs. The sensors with low-input receive its gains from integrated gain stage. The SoC chip with hardware multiplier is greatly boosted the many intensive applications, when carrying the energy computation. The smart meter used for several calculations of voltage, power factor, frequency, reactive and active power, voltage RMS current, etc. These performances are in active process when the SM is in operating mode.

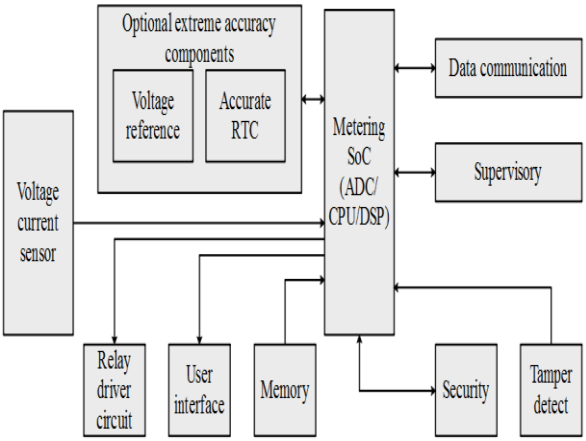


Fig. 2. Smart Meter Architecture

B. Security using RSA cryptography in smart grid

In SG, communications and nodes are monitored potentially which subject to capture and surreptitious use by an adversary. e.g. an attacker or an unauthorized user modifies customer data or which may affect by any type of attack on SG network. A number of security attacks such as jamming and access restriction, NAN sniffing and eavesdropping, energy theft attack and spoofing affect the smart meter's data. Because of these attacks, the RSA cryptography is introduced in the smart grid to secure the data from an attacker. The RSA cryptography mainly depends on the algebraic operations on large integers. The RSA cryptography has three different steps, those are key generation, encryption and decryption. At first, the data from the smart grids are encrypted using RSA encryption and then this data are transferred to BPSK modulation, that help to transmit the data from the one place to another place. The process of the secure data transmission through the BPSK using RSA is given in the Following Fig. 3.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

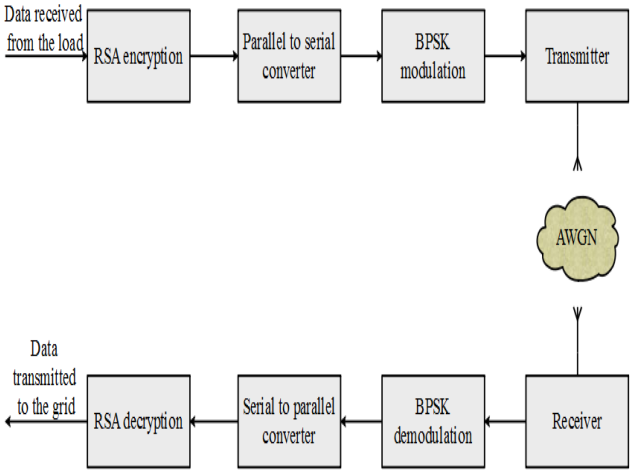


Fig. 3. Secure data transmission using BPSK with RSA

a. Key generation

Input: Create or select two large prime numbers.

Output: Two different keys. One is public key and another one is private key.

- Create two different prime numbers which are represented as a *and b.* Compute the modulus that is $m = a \times b$, Where a *and b.* are the prime numbers.
- Compute the $\phi(m)$ that is $\phi(m) = (a-1) \times (b-1)$.
- An integer e is selected as a public key and this key should satisfy the $1 < e < \phi(m)$ and $gcd(\phi(m), e) = 1$.
- The private key d is selected which satisfies the
- Public $key = (e, m)$. The public key e is used for encryption.
- Private $key = d$. The private key is used for decryption.

b. RSA encryption

Input: The plain text that is the smart meter data from the loads to encrypt and public key.

Output: The encrypted cipher text.

- Obtain a public key (m, e).
- Denote the message (p) as an integer which is in the interval of $[0, m-1]$.
- Calculate cipher text $cip = p^e mod m$, Where cip represents the cipher text from the RSA encryption and m is the modulus.
- Send this cipher text to transmitter of BPSK modulation.

C. BPSK modulation

BPSK is the basic digital modulation technique which is used at the transmitter side. Here, the BPSK is used for modulating the data from the RSA encryption. The encrypted power value which is obtained from the smart meter is given as the input to the BPSK modulation. The carrier phase is adjusted with respect to the information signal that is in digital form and it keeps frequency and amplitude of carrier constant. So, the modulated signal is divided into two phases, logical '1' and '0'. This BPSK has two phases of the carrier with the same frequency, but these two results are separated by 180º phase shift. The block diagram of the modulator is shown in Fig. 4.

The modulated signal lasts same as the carrier with the initial phase 0º at the transmission of logical '1' and also the modulated signal changes with 1800 when the logical '0' is transmitted in the BPSK modulation. The form of the BPSK signal is given in the Eq. (1).

If binary '0'
If binary '1'
(1)

Where, the carrier frequency is represented as f_c and the peak amplitude is denoted as A_p .

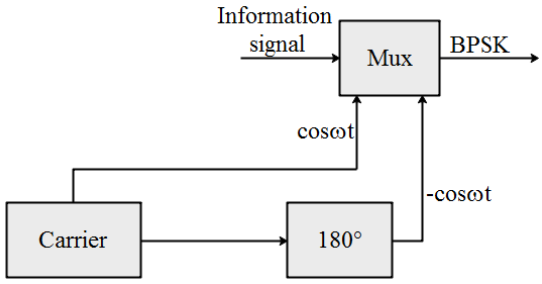


Fig. 4. Block diagram of the BPSK modulation

The modulated BPSK signal is transmitted to the BPSK demodulation with the addition of AWGN noise, which is described in the following section.

D. BPSK demodulation

The block diagram of BPSK receiver is shown in the Fig. 5 which contains noise contaminated BPSK input signal, regenerated carrier signal, balanced modulator and low pass filter. The BPSK signal, recovery signal and low pass FIR filter are multiplied using the balanced modulator. The possible outputs of the balance modulator re $cos(\omega t)$ and $-cos(\omega t)$.

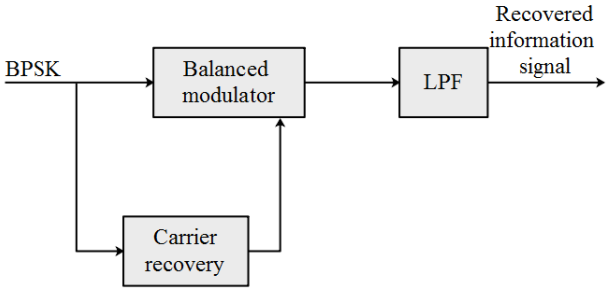


Fig. 5. Block diagram of the BPSK demodulation

Due to the 180° phase shift of the carrier, the BPSK modulation scheme is considered as a robust technique. So, the BPSK modulation can use in any of the long distance communication and data transmission.

a. AWGN channel model

The term AWGN (Additive White Gaussian Noise) denotes an unwanted electric signal which always exist in the electrical systems. Here, the term additive denotes the added signals. AWGN is a channel model which affects the communication by adding the white noise with a constant spectral density and a Gaussian distribution of amplitude. This AWGN is a best channel model for satellite and deep space telemetry. In BPSK, the analog levels $\sqrt{Eb}$ and $-\sqrt{Eb}$ represents the binary digits 1 and 0 respectively.

The noise value (n) follows the Gaussian probability distribution function which is given in the Eq. (2).

$$P(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \times e^{\frac{(x-\mu)^2}{2\sigma^2}}$$

$$\mu = 0 \text{ and } \sigma^2 = \frac{N_0}{2} \quad (2)$$

Where, the variance of the Gaussian random variable is denoted as σ^2, μ specifies the mean and noise spectral density is N_o .

In digital modulation, the number of bit errors is the number of received bits over a AWGN channel. The BER is the ratio of the number of bits in error to the total number of transferred bits. BER is a unit less performance parameter. Therefore, the BER for BPSK is given by the following Eq. (3).

$$Pb = \frac{1}{2} e_r f_c \left(\sqrt{\frac{E_b}{N_o}} \right) \quad (3)$$

Where, the complementary error function is specified as $e_r f_c$, E_b is the energy per bit, N_o is the noise density and $\frac{E_b}{N_0}$ is the signal to noise ratio.

The general formula for the probability of error or BER of MPSK for AWGN channel is given as in Eq. (4).

$$. Pb = \frac{1}{m} e_r f_c \left(\sqrt{\frac{mE_b}{N_o}} \right) sin \frac{\pi}{M} . \quad (4)$$

Where, $M = 2^m, m = 2,3,4,...$

For BPSK, the m is 2.

E. RSA decryption

The RSA decryption receives the data from the BPSK demodulation and it is decrypted by RSA. By using the binary phase shift keying the power used by the loads (i.e., house) are known by the smart grid.

Input: The encrypted cipher text and private key.

Output: The plain text.

- The original plain text that is power value is recovered by using private key (d) .

$$p_d = cip^d mod m$$

Where, p_d is the data transmitted through the BPSK.

IV. RESULTS AND DISCUSSION

The simulation of the BPSK-RSA methodology was performed using the Matlab/Simulink R2018a. In this BPSK-RSA methodology, the power grid was used to transfer the essential power to the load which is present in the certain area. The overall Simulink model of the BPSK-RSA methodology is given in the following Fig. 6. The major components present in the model are power grid, pole mounted transformer, load requirement, main breaker, BPSK modulation and demodulation module and RSA encryption module. The inputs given to the Simulink model of the BPSK-RSA methodology are voltage, current and energy from the power grid. The output taken from Simulink model is the energy consumption of respective loads. Initially, the energy is given by the power grid and then this energy is step down by using the pole mounted transformer. This energy divided into the load requirements. The load requirement module is used for analyzing the energy consumption in smart grid. Here, the BPSK block is used for transmitting the data to the end users and this data transmission is secured by using the RSA encryption module.

The specifications of the three phase source, three phase transformer, linear transformer and main breaker are given in Table 1, 2, 3 and 4 respectively.

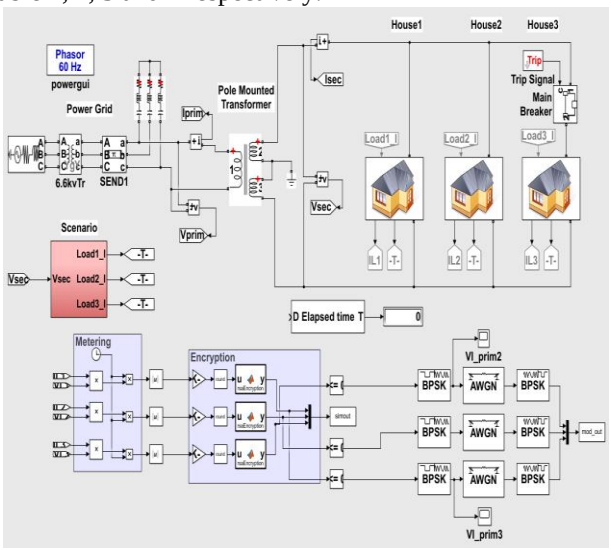


Fig. 6. Simulink model of BPSK-RSA methodology

Table I. Specification of the three phase source

Phase to phase voltage (Vrms)	66×103
Frequency	60 Hz
3-phase short circuit level at base voltage (VA)	100×106
Base voltage (Vrms Ph-Ph)	25×103

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

X/R ratio	7

Table II. Specification of the three phase transformer

Nominal power and frequency [VA, Hz]	10×10^6, 60
Winding 1 parameter [V1, R1, L1]	66×10^3, 0.002, 0.08
Winding 2 parameter [V2, R2, L2]	6.6×10^3, 0.002, 0.08
Magnetization resistance Rm	500
Magnetization Inductance Lm	500

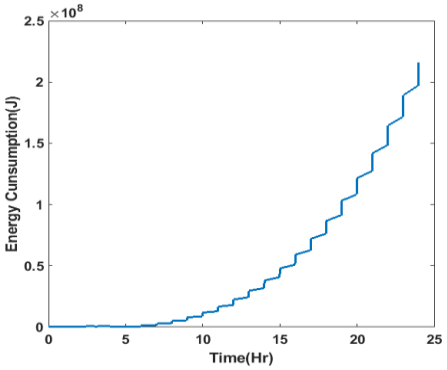
Table III. Specification of the linear transformer

Nominal power and frequency [VA, Hz]	75×10^3, 60
Winding 1 parameter [V1, R1, L1]	6600, 0.0005, 0.0002
Winding 2 parameter [V2, R2, L2]	100, 0.00005, 0.0002
Winding 3 parameter [V3, R3, L3]	100, 0.00005, 0.0002
Magnetization resistance Rm	50
Magnetization Inductance Lm	50

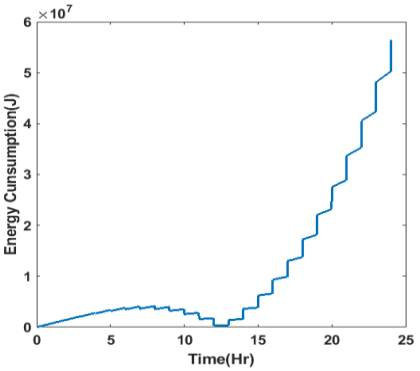
Table IV. Specification of the main breaker

Initial status	1
Breaker resistance	0.001
Snubber resistance	1×10^6
Snubber capacitance	inf

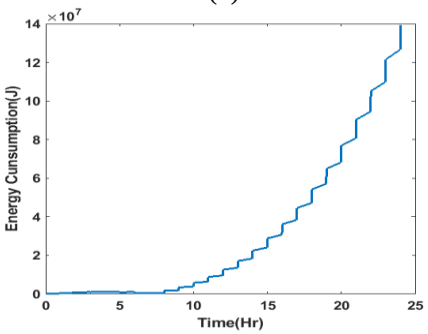
Fig. 7 a, b and c show the Energy from the smart meter of load 1, 2 and 3 respectively. Here, the loads are considered as a house and the houses have different load requirement. For example, the house 1 has one washing machine, one refrigerator and one two AC coolers. Second house has one mixer/grinder, one AC cooler and one washing machine and third house has one washing machine, one geyser, one mixer and two ACs. The main breaker of the model is used as a switch which handles the on/off conditions of the loads. By using the main breaker, the various process like the system with one load or two load or three loads is analysed. The energy values from the SM which are shown in Fig. 7 that are given as the input to the RSA decryption to enhance the security over the communication.



(a)



(b)



(c)

Fig. 7. (a) Energy from the smart meter for load 1, (b) Energy from the smart meter for load 2, (c) Energy from the smart meter for load 3

Fig. 8 (a), 9 (a) and 10 (a), show the RSA encrypted energy consumption from the load 1, load 2 and load 3 respectively. By using this RSA cryptography, the data from the SM are secured in the communication process. Because the hacker can modify the data of the customer and the system may affect by any type of attack when the system has an unsecured SG network. There are so many attacks to affect the data from the SM such as jamming and access restriction, NAN sniffing and eavesdropping, energy theft attack, spoofing. From these attacks, data from the end user to the SG is secured by the RSA cryptography through the BPSK communication. The transferred energy values to the SG is shown in Fig. 8 (b), 9 (b) and 10 (b), that are decrypted energy values of BPSK demodulation to the load 1, load 2 and load 3 respectively.

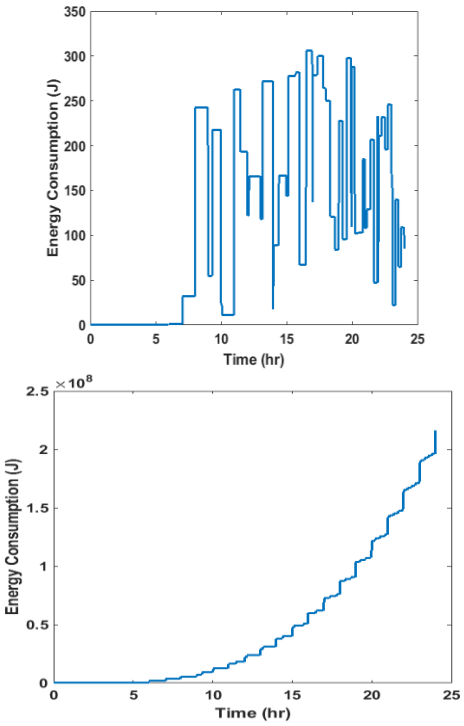
The communication performance of the BPSK is analysed in terms of Mean Square Error (MSE). MSE is defined as the averaging the squared intensity of the original input to the resultant output. The MSE is expressed in the following equation (5).

$$MSE = \frac{1}{n}\sum_{1=1}^{n}\left(p_d - p\right)^2 \tag{5}$$

Where, n is the number of data points; p_d is the decrypted power value of RSA (output) and p is the given input power value. The following Fig. 11 shows the MSE analysis of BPSK-RSA methodology.

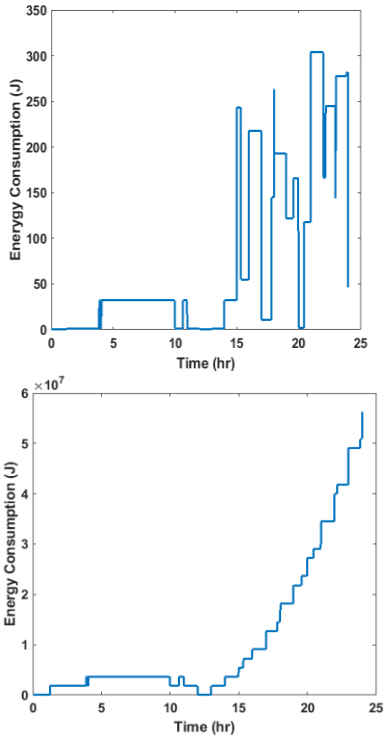
Retrieval Number: I7846078919/19©BEIESP
DOI: 10.35940/ijitee.I7846.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)



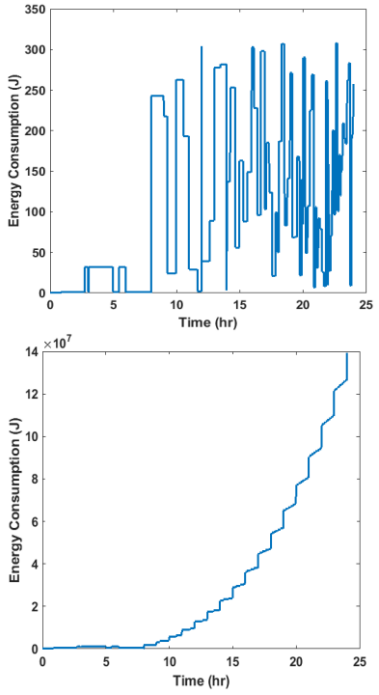
(a) (b)

Fig. 8. (a) Encrypted energy at grid 1, (b) Decrypted energy at grid 1



(a) (b)

Fig. 9. (a) Encrypted energy at grid 2, (b) Decrypted energy at grid 2



(a) (b)

Fig. 10. (a) Encrypted energy at grid 3, (b) Decrypted energy at grid 3

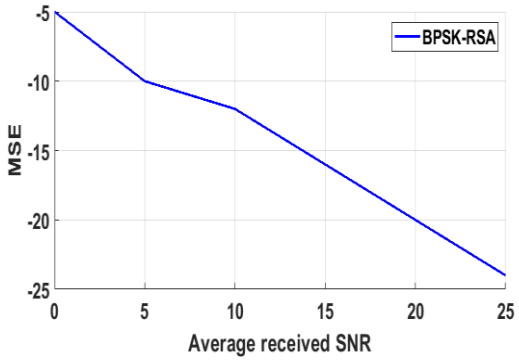


Fig. 11. MSE performance of BPSK-RSA methodology

The comparative analysis of the BPSK-RSA methodology with the existing methodology called DFT based CHE method [21] is shown in the Table 5.

Table V. Comparative analysis of MSE

SNR	DFT based CHE [21]	BPSK-RSA methodology
0	-6	-5
5	-10.5	-10.09
10	-13	-12.45
15	-17	-16
20	-21	-20.02
25	-25	-24.3

From the analysis, conclude that the BPSK-RSA methodology gives better performance when compared to the DFT based CHE method. Because, the noise present in the output of DFT based CHE method is higher than the noise present in the BPSK-RSA methodology signal.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

So, the MSE of BPSK-RSA methodology is higher than the DFT based CHE method.

Table VI. Comparative analysis of SM communication performance

No of SM	PDR		TH (bps)		EED (ms)	
	ECC-SM method [22]	BPSK-RSA methodology	ECC-SM method [22]	BPSK-RSA methodology	ECC-SM method [22]	BPSK-RSA methodology
20	100%	100%	43.72	51.25	5.24	4.92
40	99.53%	99.66%	86.73	93.12	6.19	5.73
60	97.46%	97.73%	125.34	132.94	6.27	5.52
80	94.66%	96.12%	158.21	169.32	9.37	7.91
100	90.32%	92.98%	182.09	193.45	9.98	8.02

The comparative analysis of PDR, TH and EED of the BPSK-RSA methodology with ECC-SM method [22] is shown in Table 6. The ECC algorithm is more complex and it is difficult to implement than the RSA algorithm. The robustness of the RSA is higher than the ECC. Meanwhile, the data rate provided by the BPSK is high in this BPSK-RSA methodology. So, the performance of the PDR, TH and EED are high when compared to the ECC-SM method [22].

V. CONCLUSION

The modern trend in the SG is to implement the secured wireless communications in smart grids to create the communication between the SM to the utility as well as to monitors the customer's energy consumption. In this paper, security in communications is developed by RSA cryptography. Then the BPSK is utilized to enable the data transmission between the SM to the SG. Initially, the observed energy from the smart meter is encrypted using RSA encryption. Then these energy values are transferred using BPSK modulation and demodulation. In the end, the values from the BPSK is decrypted by using RSA decryption. Based on this, the observed energy values from the load devices are transferred to the smart grid. The BPSK-RSA methodology is used for enabling the secure communication among the SM and the end users to avoid the cyber-attacks. From the comparison, conclude that the BPSK-RSA methodology provides better results when compared to the DFT based CHE method and ECC-SM method. Furthermore, the security of the data transmission from smart meter to the smart grid can be enhanced by novel encryption technique.

REFERENCES

1. E. Fadel, V. C. Gungor, L. Nassef, N. Akkari, M. A. Malik, S. Almasri, and I. F. Akyildiz. (2015). A survey on wireless sensor networks for smart grid. *Computer Communications, 71*, pp. 22-33.
2. S. Katyara, M.A. Shah, B. S. Chowdhary, F. Akhtar, and G. A. Lashari. (2018). Monitoring, Control and Energy Management of Smart Grid System via WSN Technology through SCADA Applications. *Wireless Personal Communications*, pp. 1-18,
3. B. Lang, J. Wang, and Z. Cao. (2018). Multidimensional data tight aggregation and fine-grained access control in smart grid. *Journal of information security and applications, 40*, pp. 156-165.
4. M. Yigit, V. C. Gungor, E. Fadel, L. Nassef, N. Akkari, and I. F. Akyildiz. (2016). Channel-aware routing and priority-aware multi-channel scheduling for WSN-based smart grid applications. *Journal of Network and Computer Applications, 71*, pp. 50-58,
5. S. Kurt, H.U. Yildiz, M. Yigit, B. Tavli, and V. C. Gungor, (2017). Packet size optimization in wireless sensor networks for smart grid applications. *IEEE Transactions on Industrial Electronics, 64(3)*, pp. 2392-2401.
6. S. Tonyali, R. Munoz, K. Akkaya, and U. Ozgur. (2018). A realistic performance evaluation of privacy-preserving protocols for smart grid AMI networks. *Journal of Network and Computer Applications, Vol.119*, pp.24-41, 2018.
7. U. Baroudi, M. Bin-Yahya, M. Alshammari, and U. Yaqoub, (2018). Ticket-based QoS routing optimization using genetic algorithm for WSN applications in smart grid. *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-14.
8. A. Usman, and S.H. Shami, (2013). Evolution of communication technologies for smart grid applications. *Renewable and Sustainable Energy Reviews, 19*, pp. 191-199.
9. S. Misra, S. Bera, T. Ojha, and L. Zhou. (2015). ENTICE: Agent-based energy trading with incomplete information in the smart grid. *Journal of Network and Computer Applications, 55*, pp. 202-212.
10. D. M. Menon, and N. Radhika, (2015). Design of a Secure Architecture for Last Mile Communication in Smart Grid Systems. *Procedia Technology, 21*, pp. 125-131.
11. K. Seethal, D. M. Menon, and N. Radhika, (2015). Design of a Secure Smart Grid Architecture Model using Damgard Jurik Cryptosystem. *Research Journal of Applied Sciences, Engineering and Technology, 9(10)*, pp. 895-901.
12. F. Salvadori, C. S. Gehrke, A. C. De Oliveira, M. De Campos, and P. S. Sausen. (2013.) Smart grid infrastructure using a hybrid network architecture. *IEEE Transactions on Smart Grid, 4(3)*, pp. 1630-1639.
13. C. Rottondi, G. Verticale, and A. Capone. (2013). Privacy-preserving smart metering with multiple data consumers. *Computer Networks, 57(7)*, pp. 1699-1713.
14. B. Fateh, M. Govindarasu, and V. Ajjarapu. (2013). Wireless network design for transmission line monitoring in smart grid. *IEEE transactions on smart grid, 4(2)*, pp. 1076-1086.
15. W. Hui, G. Zhitao, Y. Tingting, and X. Yue. (2014). Top-k query framework in wireless sensor networks for smart grid. *China Communications, 11(6)*, pp. 89-98.
16. Z. A. Khan, D. Jayaweera, and M. S. Alvarez-Alvarado. (2018). A novel approach for load profiling in smart power grids using smart meter data. *Electric Power Systems Research, 165*, pp. 191-198,
17. K. V. Deshpande, and V. Rajesh. (2017). Investigation on IMCP based clustering in LTE-M communication for smart metering applications. *Engineering science and technology, an international journal, 20(3)*, pp. 944-955.
18. S. Aleksic, and V. Mujan. (2018). Exergy cost of information and communication equipment for smart metering and smart grids. Sustainable Energy, *Grids and Networks, 14*, pp. 1-11.
19. U. B. BALOGLU, and Y. DEMİR. (2018). Lightweight Privacy-Preserving Data Aggregation Scheme for Smart Grid Metering Infrastructure Protection. *International Journal of Critical Infrastructure Protection, 22*, pp. 16-24.
20. J. S. Chou and I. G. A. N. Yutami. (2014). Smart meter adoption and deployment strategy for residential buildings in Indonesia. *Applied Energy, 128*, pp. 336-349.
21. H. J. Wang, Y. Zhen, Q. H. Ou, H. Y. Zhang, W. Q. Yang, and Y.D. Xia. (2015). Comparison of Downlink Channel Estimation Schemes for LTE-Based Smart Grid Communications. *In: Proc. of Applied Mechanics and Materials, 713*, pp. 962-965.
22. F. Wu, L. Xu, X. Li, S. Kumari, M. Karuppiah, and M. S. Obaidat. (2018). A Lightweight and Provably Secure Key Agreement System for a Smart Grid with Elliptic Curve Cryptography. *IEEE Systems Journal*, pp. 1-9.

AUTHORS PROFILE

Abdul khadar A Received B.E in E&EE from UBDT College of Engineering Davangere, Karnataka, India. He holds M Tech. degree in Electrical Power System from NIE Mysore, Karnataka, India in year 2006 respectively. Currently he is pursuing Ph.D in Electrical Engineering from Visvesvaraya Technology University Belagavi, Karnataka, India. Currently he is an Associate Professor in the department of Electrical and Electronics Engineering at Ballari Institute of Technology and Management, Ballari. He has published there journals and conference proceedings.

Pradeep B Jyoti received his Ph.D in Electrical Engineering from Jawaharlal Nehru Technology University Hyderabad, Telangana, India. He is Currently Professor in the department of Electrical and Electronics Engineering at Prouda Devaraya Institute of Technology, Hosapete. He has maore than 25 years of teaching experience. He has published many research articles in leading journals, conference proceedings.

M S Nagaraj received his Ph.D in Electrical Engineering from Visvesvaraya Technology University Belagavi, Karnataka, India. He is Currently Professor in the department of Electrical and Electronics Engineering at Bapuji Institute of Engineering and Technology, Davaangere. He has more than 25 years of teaching experience. He has published many research articles in leading journals, conference proceedings.

Shabana S S is working in Govt. Polytechnic Ballari