IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 2)
Available online at: www.ijariit.com

Designing a two-layer security algorithm for smart grid

Gagandeep Sharma
gagan1152398@gmail.com
Adesh Institute of Engineering and Technology, Faridkot, Punjab

Puneet Jain
puneetjain88@gmail.com
Adesh Institute of Engineering and Technology, Faridkot, Punjab

Ravinder Singh
ravindersinghsbs@gmail.com
Adesh Institute of Engineering and Technology, Faridkot, Punjab

ABSTRACT

Smart Grid (SG) is the next generation power grid which provides flexibility, reliability, and efficiency in generating, controlling, and distributing the electricity. The SG provides two-way communication between supplier and consumers and sensitive information is communicated on the network. The attackers try to steal this information to attack the grids and consumers for their benefits. Some of the most popular smart grid attacks are the key-based attack, data-based attack, impersonation-based attack, physical-based attack. To overcome these issues, the cryptography algorithms and steganography algorithms are used. The cryptography algorithms are scrambled the message and transform into another form. The cryptography algorithms are categorized into two types. These are an asymmetric and asymmetric cipher. In the symmetric cipher same key is used for encryption/ decryption purposes. The symmetric cipher is further divided into types known as a block cipher and stream cipher. In the block cipher, the message is divided into fixed chucks and the same key, rounds are applied on each chuck. In the stream cipher, the plaintext and key bitwise XOR operation are performed. On the other hand, in asymmetric algorithms, two different keys are known as the public and the private key is used for encryption/ decryption purposes. In this thesis, a two-layer security algorithm is designed using lightweight cryptography and steganography algorithm which provide confidentiality as well as authentication. In which three algorithms are hybrid which includes PICO, Genetic Algorithm, and LSB algorithm. Initially, the secret data is encrypted using a lightweight PICO algorithm and initialization vector key is generated using a lightweight genetic algorithm. Further, the encrypted data is hidden in the image using the LSB algorithm. The proposed technique simulation results show that the proposed technique consumes less memory, provide high avalanche effect and embedding capacity.

Keywords*— PICO, Lightweight algorithm, Steganography, RSA, LIZARD, CBC mode*

1. INTRODUCTION

Smart Grid (SG) is the next generation power grid which provides flexibility, reliability, and efficiency in generating, controlling, and distributing the electricity [1-3]. The SG provides two-way communication between supplier and consumers and sensitive information is communicated on the network [4]. The attackers try to steal this information to attack the grids and consumers for their benefits. Some of the most popular smart grid attacks are explained below [5]:

1.1 Key-based attack

In the smart grid, for registration and authentication, a secret key has been used by consumers/suppliers. The attackers have applied known and unknown key attack on the smart grid to grab the secret keys.

1.2 Data based attack

In the smart grid, the load balancing between demand and generation is required. The attackers try to modify this information. Further, the data-based attack is categorized into a number of attacks, which include modification attack, data integrity attack, chosen-plaintext attack, chosen ciphertext attack, repudiation attack.

1.3 Impersonation-based attack

In the smart grid, the adverse, 13ry can read smart meter data which coming from smart homes to read how much electricity consumption is done. The attackers are tries to monitor and modify this information. The impersonation-based attack can be categorized as a man-in-the-middle attack, eavesdropping attack, replay attack, redirection attack.

1.4 Physical based attack

In this attack, the attackers target the hardware used in the smart grid which includes battery vehicle, a local aggregator, and a gateway or proxy server. This attack is categorized into 4 types such as a differential attack, malware attack, collusion attack, and inference attack.

To overcome these issues, the cryptography algorithms and steganography algorithms are used [6]. The cryptography algorithms are scrambled the message and transform into another form. The cryptography algorithms are categorized into two types. These are a symmetric and asymmetric cipher. In the symmetric cipher, the same key is used for encryption/ decryption purposes [7]. The symmetric cipher is further divided into types known as a block cipher and stream cipher. In the block cipher, the message is divided into fixed chucks and the same key, rounds are applied on each chuck. In the stream cipher, the plaintext and key bitwise XOR operation are performed. On the other hand, in asymmetric algorithms, two different keys are known as the public and the private key are used for encryption/ decryption purposes [8].

In this paper, a two-layer security algorithm is designed using lightweight cryptography and steganography algorithm which provide confidentiality as well as authentication. In this paper, three algorithms are hybrid which includes PICO [9], Genetic Algorithm [10], and LSB algorithm [11]. Initially, the secret data is encrypted using a lightweight PICO algorithm and initialization vector key is generated using a lightweight genetic algorithm. Further, the encrypted data is hidden in the image using the LSB algorithm. The proposed technique simulation results show that the proposed technique consumes less memory, provide high avalanche effect and embedding capacity. The rest of the paper defines as Section 2 explains the related work is done in the smart grid for security purposes. Section 3 describes the proposed technique in details. Section 4 presents the experimental results. The conclusion is drawn in section 5.

2. RELATED WORK IN THE SMART GRID FOR SECURITY PURPOSES

In this section, the existing security algorithms are deployed for the smart grid is discussed below.

The authors [12, 13], is reviewed the four conventional symmetric algorithms for the smart grid on the basis of block size, key size, number of rounds, and memory used. These algorithms are DES, 3DES, AES, and BLOWFISH. Further, based on the performance parameter in terms of encryption time, decryption time, memory used, total simulation time conclude that AES performs best as compared to other algorithms.

The authors [14], hybrid the steganography algorithm with BCH error correction algorithm to improve robustness against the attacks in the cognitive radio smart grid.

The authors Jiang, *et al.* [15], is hybrid the AES algorithm with audio steganography to provide covert communication between transmitter and receiver. To achieve this, the secret data is encrypted with the AES algorithm in the initial phase: Further, hide the encrypted secret data bits in the audio packets.

Li, et al. [16], is used the homomorphic encryption algorithm for privacy-preserving in the smart grid. Therefore, the input and intermediate results are not discovered.

From the literature, it is found that in the smart grid conventional cryptography algorithms which include 3DES, AES, Blowfish is used for security purposes. These algorithms are provided with good security. On the other hand, these algorithms are provided memory complexity. To overcome this issue, lightweight ciphers are being deployed to improving security and memory complexity. In our work, we are deployed lightweight cipher PICO for data encryption. The encryption algorithm is worked in CBC mode which provides authentication as well. In the CBC mode, the initialization vector (IV) is played an important role. Thus, the IV is generated using a genetic algorithm to improve memory complexity. Next, one more layer of steganography algorithm is embedded in secret data.

3. PROPOSED TECHNIQUE FOR SMART GRID SECURITY

In this section, the proposed technique is explained. The block diagram of the proposed technique is shown in figure 1. Initially, the secret data is read and divided into fixed chunks of size 64 bit. Next, 128-bit key is readied and 128-bit IV is generated using Genetic algorithm. These three parameters are input to a lightweight encryption algorithm PICO. The cipher message which is generated in the output. The cipher message bits and cover image are input to the data embedding algorithm. In the data embedding algorithm, the secret data is hidden in the cover image using the LSB technique and stego image is generated in the output.

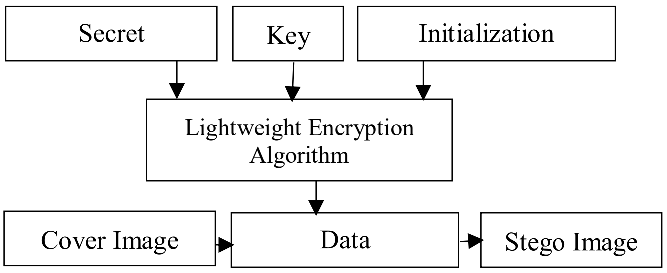

Fig. 1: Block Diagram for the Proposed Technique

The components of the proposed technique are explained below.

3.1 Lightweight PICO Algorithm

PICO is a lightweight Substitution-Permutation network (SPN) [9]. The algorithm is processed 64-bit block size, 128-bit key size, and a total of 32 rounds. The block diagram is shown in figure 2. Initially, the 64-bit plaintext and 64-bit of key XOR operation are performed. Next, the XOR output is passed through S-box. The s-box substitute the bits according to the look-up table as shown in table 1. Further, the bits of s-box output is shuffle. The shuffling position of the bits is shown in table 2. This criterion is followed 32 times to produce cipher text. On the other side, key scheduling is done on the fly on each round as shown in table 3.

Table 1: S-Box

X	S[X]
0	1
1	2
2	4
3	D
4	6
5	F
6	B
7	8
8	A
9	5
A	E
B	3
C	9
D	C
E	7
F	0

Table 2: Bit Shuffle

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0,10	1,5	1,12	2,6	2,12	3,0	3,11	0,1	3,3	0,15	2,9	0,2	3,12	2,2	1,8	1,4
1	3,8	0,6	1,1	1,15	2,4	3,5	0,12	2,14	1,14	3,4	0,11	0,4	1,7	2,3	2,8	3,15
2	0,8	2,7	0,3	2,11	3,9	3,1	1,0	1,9	2,5	2,10	3,13	3,2	0,0	0,9	1,2	1,10
3	3,10	3,7	0,7	1,3	1,13	0,14	2,15	2,0	2,1	0,5	3,14	2,13	0,13	3,6	1,6	1,11

Table 3: Key Scheduling

$K^0K^0 \quad = \quad K^{63}, K^{62}, \dots \dots \dots \dots \dots \dots \dots$

$K^{63}, K^{62}, \dots \dots \dots \dots \dots \dots \dots K^0K^0$

$L^1L^1 \quad = \quad K^{127}, K^{126}, \dots \dots \dots \dots \dots \dots \dots$

$K^{127}, K^{126}, \dots \dots \dots \dots \dots \dots \dots K^{64}K^{64}$

For j=0 to 31 rounds

$L^2L^2 \quad = \quad \left(K^j \; XOR \; (RCS \; L^1, 3)\right) XOR \; L^1$

$\left(K^j \; XOR \; (RCS \; L^1, 3)\right) XOR \; L^1$

$k^{j+1}k^{j+1} \quad = \quad \left(L^2 \; XOR \; (LCS \; K^j, 7)\right) XOR \; J$

$\left(L^2 \; XOR \; (LCS \; K^j, 7)\right) XOR \; J$

$L^1L^1 = L^2 \; L^2$

Where *RCS*is *Right Circular Shift* and *LCS*is *Left Circular Shift*.

3.2 Genetic Algorithm

The initialization vector is generated using a genetic algorithm. The motivation is taken from this paper [10]. The genetic algorithm simpler operation such as crossover and mutation are performed to generate 64-bit. In the genetic algorithm, the seed point and original key is input. On these inputs, the genetic algorithm is performed which generate a 64-bit random key. The generation algorithm flow is shown in figure 2.

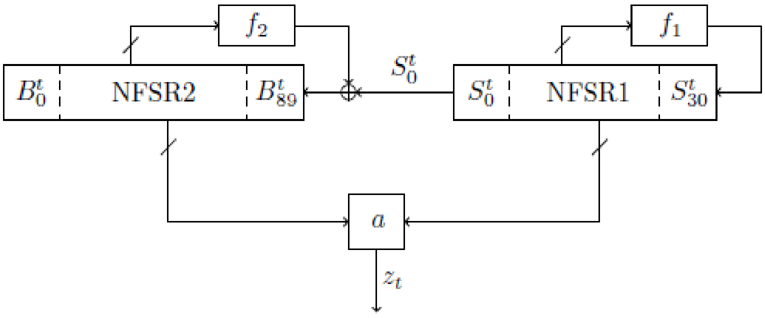

Fig. 2: Block Diagram of Key Generation for Genetic algorithm

Table 4: The pseudo-code

```
1. Read 64-bit seed and 128-bit key.
2. Initially, XOR operation is performed of seed point with a key.
3. Count the number of 0’s in.
4. If the odd number of 0’s
The XOR output bit-stream is performed crossover (bit-swap).
Else
The XOR output bit-stream is performed crossover alternatively (bit-swap).
5. Count the number of 1’s in the random bit stream. According to the count index, flips the bit stream from that index.
```

3.3 LSB Data Hiding Algorithm

In the LSB data hiding algorithm, the cover image pixel *k*-LSB bits are replaced with secret data *k*-bits [11]. As the *k* value is increased, embedding capacity improves but on the other influence the variability in the cover image. The LSB is explained with an example in table 5. As shown in the table, only one-bit variability in the cover image pixels when 1-bit secret data is embedded in each cover pixel but on the other side, to hide 8bits, 8 pixels are required.

Table 5: LSB Data Hiding

Cover Image Pixels			
10101100	00001100	11110000	11001100
00001111	10101010	01010101	10001110
Secret Data Bits:10101100			
Stego Image Pixels			
1010110**1**	0000110**0**	1111000**1**	1100110**0**
0000111**1**	1010101**1**	0101010**0**	1000111**0**

4. EXPERIMENTAL RESULTS

In this section, the proposed technique experimental results are explained. The technique is simulated in MATLAB 2013a. The standard dataset plaintext, key, and cover images are used for the proposed technique. The following performance analysis parameters are measured for the proposed technique and compared with existing techniques.

4.1 Memory Complexity

This parameter is measured how much memory is used in the algorithm [17]. In our work, we used this parameter to measure how much memory used in the s-box for the proposed technique as compared to existing conventional techniques.

Table 6: Memory Complexity

Algorithm	AES	PICO
S-box Memory (in bits)	2048	64

4.2 Avalanche Effect

Avalanche effect parameter is measured the plaintext/key sensitivity on the cipher text bit stream [9]. Basically, this parameter measure how much cipher text bit stream change, with a change in the one-bit in the key. For the proposed technique, the sensitivity is shown in table 6. The result shows that the proposed technique achieved a higher PSNR 51.56%.

Table 7: Avalanche Effect

Plaintext (in Hex)	Key (in Hex)	The ciphertext (in Hex)	Avalanche Effect
[0000000000000000]	[0000000000000000 0000000000000000]	[455520479934A601]	51.56%
	[1000000000000000 0000000000000000]	[69DC5C79CDDF0A52]	

4.3 PSNR

This parameter has measured the quality of stego image after data embedding [18]. It is measured in dB. It is determined as
Here, P defined the Peak value, MSE represents the Mean square error. In our work, we have hidden 2048bits data in 4KB cover image file and PSNR is shown for different images in table 7. The table shows that the proposed technique achieves better PSNR.

Table 8: PSNR for Different Cover Images

Cover Images (.jpg)	PSNR (in dB)
Lena	56.92
Baboon	57.12
Barbara	56.89
Cameraman	56.99
Pepper	57.01

4.4 Embedding Capacity

The embedding capacity parameter is measured how much secret data bits are embedded in the cover image. In our work, 2048 bits are embedded in the cover image.

5. CONCLUSION AND FUTURE WORK

In this paper, initially, an overview of the smart grid are attacks are discussed. Further, to overcome this attacks cryptography and steganography algorithms are studied and proposed two-layer security algorithm for smart grid security. To achieve this, a lightweight PICO algorithm in CBC mode is worked and encrypted information is embedded in the cover image using LSB technique. For the CBC mode, the IV is generated using a genetic algorithm. In the last, on the standard dataset image, experimental results are performed and various performance analysis parameter is measured. We have achieved less memory complexity, high avalanche effect, PSNR, and embedding capacity.

6. REFERENCES

[1] Abbasinezhad-Mood, D., and Nikooghadam, M. (2018). Design of an enhanced message authentication scheme for the smart grid and its performance analysis on an ARM Cortex-M3 microcontroller. Journal of information security and applications, 40, 9-19.

[2] Fang, X., Misra, S., Xue, G., and Yang, D. (2012). Smart grid—the new and improved power grid: A survey. IEEE communications surveys and tutorials, 14(4), 944-980.

[3] Guerrero, J. M., Vasquez, J. C., Matas, J., De Vicuña, L. G., and Castilla, M. (2011). Hierarchical control of droop-controlled AC and DC microgrids—a general approach toward standardization. IEEE Transactions on industrial electronics, 58(1), 158-172.

[4] Otuoze, A. O., Mustafa, M. W., and Larik, R. M. (2018). Smart grids security challenges: Classification by sources of threats. Journal of Electrical Systems and Information Technology.

[5] Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., and Shu, L. (2018). A systematic review of data protection and privacy preservation schemes for smart grid communications. Sustainable Cities and Society, 38, 806-835.

[6] Varsha, R. S. (2015). Data Hiding Using Steganography and Cryptography. International Journal of Computer Science and Mobile Computing, 4(4), 802-805.

[7] Singh, P., and Shende, P. (2014). Symmetric Key Cryptography: Current Trends. IJCSMC, 3(12), 410-415.

[8] Tripathi, R., and Agrawal, S. (2014). Comparative study of symmetric and asymmetric cryptography techniques. International Journal of Advance Foundation and Research in Computer (IJAFRC), 1(6), 68-76.

[9] Bansod, G., Pisharoty, N., and Patil, A. (2016). PICO: An Ultra-Lightweight and Low Power Encryption Design for Ubiquitous Computing. Defense Science Journal, 66(3).

[10] Banerjee, B., and Patel, J. T. (2016). A Symmetric Key Block Cipher to Provide Confidentiality in Wireless Sensor Networks. INFOCOMP, 15(1), 12-18.

[11] Samidha, D., and Agrawal, D. (2013, January). Random image steganography in the spatial domain. In Emerging Trends in VLSI, embedded system, nano electronics and telecommunication system (ICEVENT), 2013 international conference on (pp. 1-3). IEEE.

[12] Mouachi, R., Ait-Mlouk, A., Gharnati, F. and Raoufi, M., 2017. A Choice of Symmetric Cryptographic Algorithms based on Multi-Criteria Analysis Approach for Securing Smart Grid. Indian Journal of Science and Technology, 10(39).

[13] Abood, O.G., Elsadd, M.A. and Guirguis, S.K., 2017, December. Investigation of cryptography algorithms used for security and privacy protection in a smart grid. In Power Systems Conference (MEPCON), 2017 Nineteenth International Middle East (pp. 644-649). IEEE.

[14] Abuadbba, A., Khalil, I., Ibaida, A., and Atiquzzaman, M. (2016). Resilient to shared spectrum noise scheme for protecting cognitive radio smart grid readings− BCH based steganographic approach. Ad Hoc Networks, 41, 30-46.

[15] Jiang, Y., Zhang, L., Tang, S. and Zhou, Z., 2013, August. Real-Time Covert VoIP Communications over Smart Grids by Using AES-Based Audio Steganography. In Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing (pp. 2102-2107). IEEE.

[16] Li, F., Luo, B., and Liu, P. (2010, October). Secure information aggregation for smart grids using homomorphic encryption. In Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on (pp. 327-332). IEEE.

[17] Karim, S. M., Rahman, M. S., and Hossain, M. I. (2011, December). A new approach for LSB based image steganography using the secret key. In Computer and Information Technology (ICCIT), 2011 14th International Conference on (pp. 286-291). IEEE.