IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 7, Issue 8, August 2019

Security Scheme Wireless Sensor Network using Cryptography Scheme

V. Bhuvaneshwari[1], **V.Uthaman**[2]

M.C.A., M.Phil., SET[2]

Abstract: The factors restricting the development of Wireless Sensor Networks (WSNs) included its cost, power consumption and safety.New block cipher algorithm in single byte for wireless sensor network with excellence of many cipher algorithms is studied. The child keys are generated through the developed discrete Logistic mapping, and the Feistel encrypting function with discrete chaos operation is constructed. The single byte block is encrypted and decrypted through one turn permutation, being divided into two semi-byte, quadri-Feistel structural operation, and one turn permutation again. The amount of keys may be variable with the turns of Feistel structural operation. The random and security of the child key was proven, and the experiment for the block cipher in wireless sensor network was completed. The result indicates that the algorithm is more secure and the chaos block cipher in single byte is feasible for wireless sensor network.

Keywords: WSN Architecture, AES Algorithm, Cryptography

I. INTRODUCTION

Wireless sensor networks are quickly gaining popularity due to the fact that they are potentially low cost solutions to a variety of real-world challenges. Their low cost provides a means to deploy large sensor arrays in a variety of conditions capable of performing both military and civilian tasks. But sensor networks also introduce severe resource constraints due to their lack of data storage and power. Both of these represent major obstacles to the implementation of traditional computer security techniques in a wireless sensor network. The unreliable communication channel and unattended operation make the security defenses even harder. Indeed, as pointed out in wireless sensors often have the processing characteristics of machines that are decades old (or longer), and the industrial trend is to reduce the cost of wireless sensors while maintaining similar computing power. With that in mind, many researchers have begun to address the challenges of maximizing the processing capabilities and energy reserves of wireless sensor nodes while also securing them against attackers. All aspects of the wireless sensor network are being examined including secure and efficient routing, data aggregation, group formation, and so on. In addition to those traditional security issues we observe that many general-purpose sensor network techniques assumed that all nodes are cooperative and trustworthy. This is not the case for most, or much of, real-world wireless sensor networking applications, which require a certain amount of trust in the application in order to maintain proper network functionality. Researchers therefore began focusing on building a sensor trust model to solve the problems beyond the capability of cryptographic security. In addition, there are many attacks designed to exploit the unreliable communication channels and unattended operation of wireless sensor networks. Furthermore, due to the inherent unattended feature of wireless sensor networks, we argue that physical attacks to sensors play an important role in the operation of wireless sensor networks. Thus, we include a detailed discussion of the physical attacks and their corresponding defenses, topics typically ignored in most of the current research on sensor security. We classify the main aspects of wireless sensor network security into four major categories: the obstacles to sensor network security, the requirements of a secure wireless sensor network, attacks, and defensive measures. We also give a brief introduction of related security techniques and summarize the obstacles for the sensor network security. The security requirements of a wireless sensor network are listed as below: 1.1. Obstacles of Sensor Security. A wireless sensor network is a special network which has many constraints compared to a traditional computer network. Due to these constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks. Therefore, to develop useful security mechanisms while borrowing the ideas from the current security techniques like (AES)

1. 1. WSN Architecture:

In a typical WSN we see following network components –

[A]. Sensor motes (Field devices) – Field devices are mounted in the process and must be capable of routing packets on behalf of other devices. In most cases they characterize or control the process or process equipment. A router is a

DOI 10.17148/IJIREEICE.2019.7803

special type of field device that does not have process sensor or control equipment and as such does not interface with the process itself.

[B].Gateway or Access points – A Gateway enables communication between Host application and field devices.

[C].Network manager – A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super) frames management of the routing tables and monitoring and reporting the health of the network.

[D].Security manager – The Security Manager is responsible for the generation, storage, and management of keys Wireless Sensor Network with resource constrained nodes makes them extremely vulnerable to variety of attacks. Attackers can eavesdrop on our radio transmissions, inject bits in the channel, replay previously heard packets and many more. Securing the Wireless Sensor Network needs to make the network support all security properties: confidentiality, integrity, authenticity and availability. Attackers may deploy a few malicious nodes with similar hardware capabilities as the legitimate nodes that might collude to attack the system cooperatively. The attacker may come upon these malicious nodes by purchasing them separately, or by "turning" a few legitimate nodes by capturing them and physically overwriting their memory.

Also, in some cases colluding nodes might have high-quality communications links available for coordinating their attack. Sensor nodes may not be tamper resistant and if an adversary compromises a node, she can extract all key material, data, and code stored on that node. While tamper resistance might be a viable defense for physical node compromise for some networks, we do not see it as a general purpose solution. Extremely effective tamper resistance tends to add significant per-unit cost, and sensor nodes are intended to be very inexpensive.

1.2 AES Algorithm

3.1 AES (Rijndael) Overview Rijndael (pronounced as in "rain doll" or "rhine dahl") is a block cipher designed by Joan Daemen and Vincent Rijmen, both cryptographers in Belgium. Rijndael can operate over a variable-length block using variablelength keys; the version 2 specification submitted to NIST describes use of a 128-, 192-, or 256-bit key to encrypt data blocks that are 128, 192, or 256 bits long; note that all nine combinations of key length and block length are possible. The algorithm is written in such a way that block length and/or key length can easily be extended in multiples of 32 bits and it is specifically designed for efficient implementation in hardware .software on a range of processors. The design of Rijndael was strongly influenced by the block cipher called square, also designed by Daemen and Rijmen.3.2 In Depth Rijndael is an iterated block cipher, meaning that the initial input block and cipher key undergoes multiple rounds of transformation before producing the output. Each intermediate cipher result is called a State.

For ease of description, the block and cipher key are often represented as an array of columns where each array has 4 rows and each column represents a single byte (8 bits). The number of columns in an array representing the state or cipher key, then, can be calculated as the block or key length divided by 32 (32 bits = 4 bytes). An array representing a State will have Nb columns, where Nb values of 4, 6, and 8 correspond to a 128-, 192-, and 256-bit block, respectively. Similarly, an array representing a Cipher Key will have Nk columns, where Nk values of 4, 6, and 8 correspond to a 128-, 192-, and 256-bit key, respectively. An example of a 128-bit State (Nb=4) and 192-bit Cipher Key (Nk=6) is shown below

II. PROPOSED SYSTEM

In this paper, the security algorithm is developed more efficient than the works in literature. Security algorithm using chaotic systems was implemented on WSN to provide secure communication on WSN. It was simulated on OPNET Modeller simulator and then it was compared with Skipjack algorithm in which TinySEC protocol was used in ZigBee standards. Comparison was made on average end to end delay figures, energy consumption and memory usage rates.

The rest of paper is organized as follows: Section 2 includes information about chaotic map and system model which are used for encryption. Section 3 presents the simulation of the proposed security model and performance evaluation according to simulation results. The conclusion section presents assessments and comments on the recommended method.

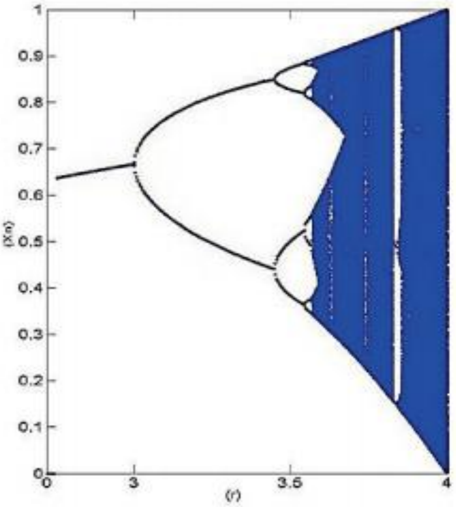


Fig.1 The logistic map branch diagram

2.1.The system model of chaotic based encryption 2.1 Chaotic map

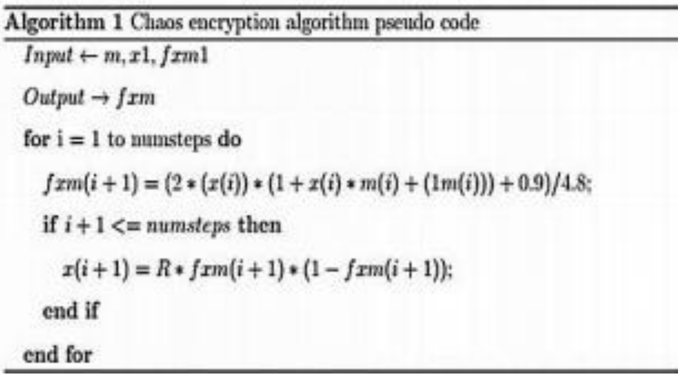
There are many chaotic systems as discrete time and continuous time in the literature [16, 17]. Continuous systems can be divided into chaotic and hipper chaotic systems. For encryption application, in this paper is used discrete time chaotic system that is one dimensional logistic map, because it is basic and high encryption effective. Keys are obtained by Logistic map in encryption. For Logistic Map, bifurcation diagram is given in Fig. 1. In Eq. (1), the system parameter r was examined between 0÷4 values. As seen in Fig. 1, if the parameter r is between 0 and 3, the result is 1, if the parameter r is between 3 and 3,4, the result is 2. If the value r is around 3,5; 4 results are produced by chaotic system. And if the value r is less than 3,5699 and near the entering chaos the result is 8. As a result, bifurcation diagram in Fig. 1 shows that for r value must be chosen only 3,5699÷4 so that the system can enter chaos.

$$X[n+1] = r^* X[n] * (1-X[n])$$

In equation, the parameter x is system variable and the value n is the number of iterations. In application, the number of data to be encrypted must be equal to the number of keys for encryption. Exemplarily, for 1000 bits original data there must be 1000 keys that are produced by chaotic system (Logistic Map).

2.2 Communication using chaotic encryption:

Secure communication model of chaos based encryption algorithm is encrypted are transmitted with nonlinear function to communication channel. Then, data encrypted in the block diagram can be decrypted with the inverse of the function. In order to decrypt data encrypted in the application, one needs to know keys produced for each bit and the order of these keys, the chaotic system used, parameters in the chaotic system and initial values, and also non-linear equation and all parameters employed in this equation. In improved application, for Logistic Map, pseudo code (Algorithm 1) structure is given in above for encryption. Keys are provided with chaos generator (Logistic Map) in encryption. Also, a non-linear equation was used in order to increase security in encryption.



Algorithm 1 Chaos encryption algorithm pseudo code

```
$Input \leftarrow m, x1, fxm1$
$Output \rightarrow fxm$
for i = 1 to numsteps do
    $fxm(i+1) = (2*(x(i))*(1+x(i)*m(i)+(1m(i)))+0.9)/4.8;$
    if $i+1 <= numsteps$ then
        $x(i+1) = R*fxm(i+1)*(1-fxm(i+1));$
    end if
end for
```

X value in Eq. (2) represents the keys produced with chaos generators and m value represents the data to be encrypted in bits.

$2x\ (1 + x\mathrm{m} + (1 - m) + 0{,}9)/4{,}8.$

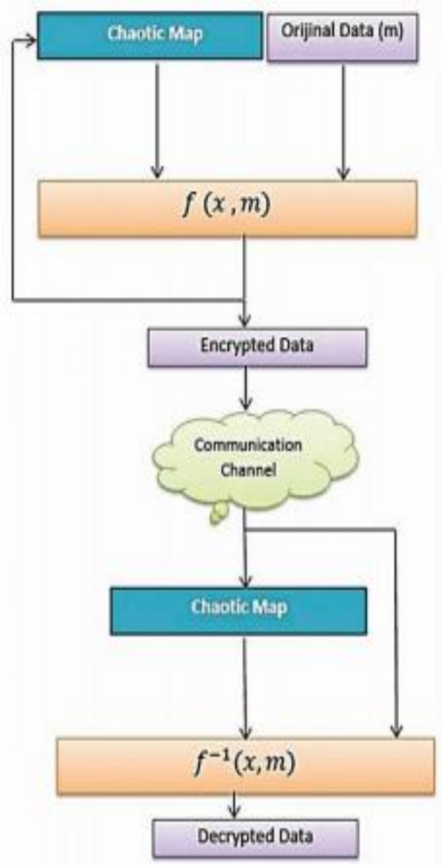


Figure The system model of chaotic-based encryption block diagram

III. RESULT AND DISCUSSION

The simulation environment we created the 100 wireless sensing nodes for communication purpose for transfer the information one nodes to another nodes. Chaotic based encryption algorithm is implemented for sending the image through wsn technology. The image data as a input as the size of 256 *256

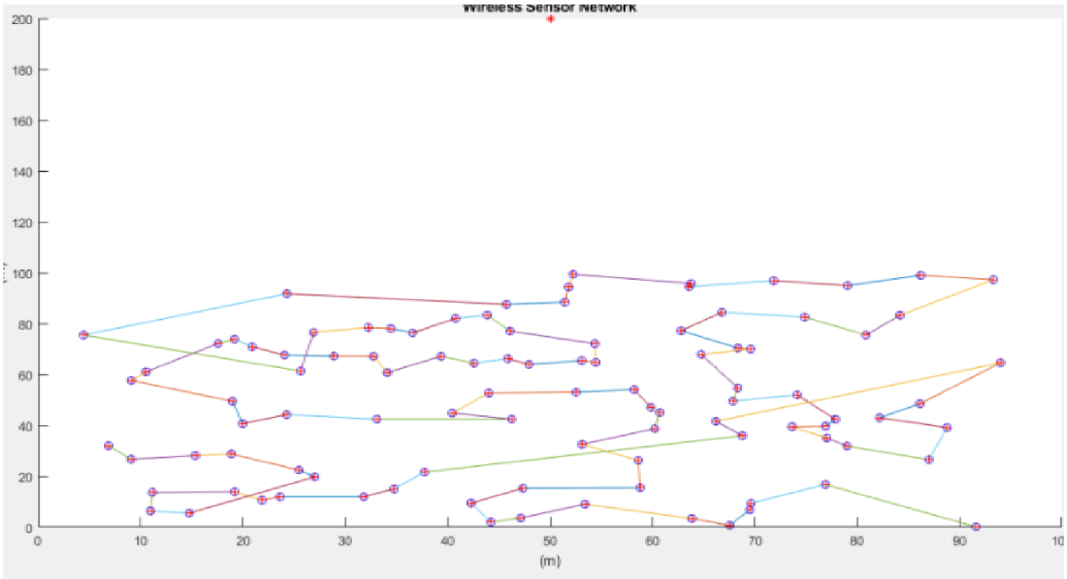


Figure: inputimage

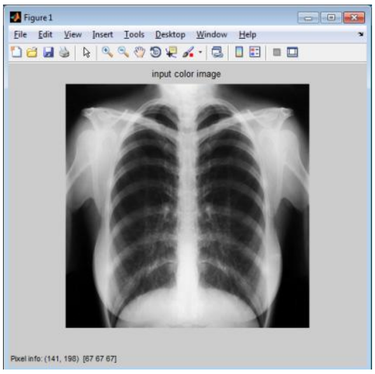


Figure 1
File Edit View Insert Tools Desktop Window Help
input color image
Pixel info: (141, 198) [67 67 67]

Figure: input image

The logistic map is created using the encryption algorithm

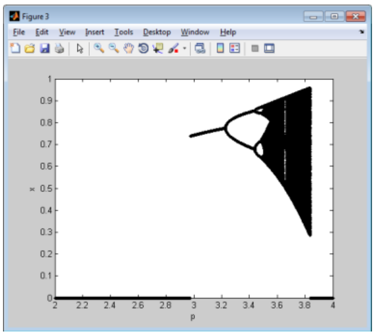


Figure: logistic map

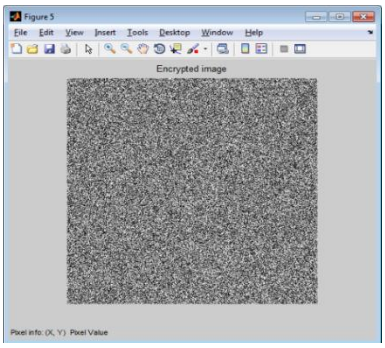


Figure 5
File Edit View Insert Tools Desktop Window Help
Encrypted image
Pixel info: (X, Y) Pixel Value

Figure: encryption image

Histogram Analysis

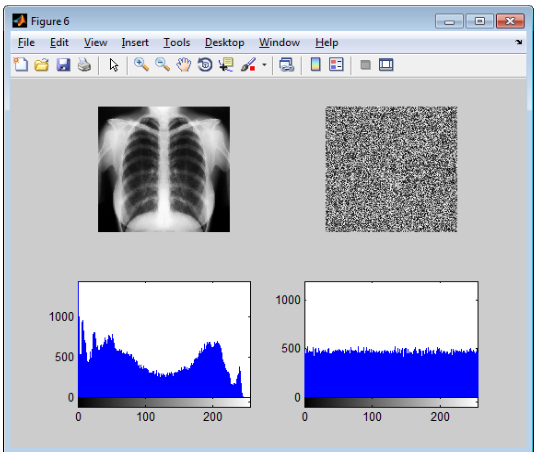


Figure: Histogram analysis

DOI 10.17148/IJIREEICE.2019.7803

IV. CONCLUSION

Encryption techniques are the basic approaches to protecting the privacy of data in wireless sensor networks. Since the sensor nodes have limited resources, the algorithms that consume less energy and memory are required. In this paper, we propose MBCC, a modified version of BCC, which is a resource efficient algorithm, based on the chaos theory to reduce operation time as compared to BCC by reducing the number of permutation calls. Our tested evaluation results show that the time for encrypting a 32-byte data is decreased from 220.74 milliseconds in BCC to 34.02 milliseconds in MBCC. In addition, MBCC outperforms BCC by 84.83% with respect to energy efficiency. On the other hand, due to modifications made to MBCC, higher ROM usage in is observed compared to BCC. However, MBCC performs.The proposed algorithm can be further improved by carrying a performance study on the security metrics in various rounds in the MBCC. It is required to probe the possibility of reducing algorithm rounds while preserving the minimum-security criteria. Further analysis of the selection of different effective criteria is required to determine the period of key change for the sensor nodes.

Further research is required for the security assessment of cryptographic systems. Cryptanalytic attacks such as side-channel attacks (e.g. power-analysis attacks, timing attack, and cache-side channel attacks), chosen plaintext attack (e.g. differential cryptanalysis) and dictionary attacks are complementary to the security attack analysis provided in this work.

REFERENCES

[1]. G. A. Fink, D. V. Zarzhitsky, T. E. Carroll, and E. D. Farquhar, Security and privacy grand challenges for the Internet of Things", in proc. of the International Conference on Collaboration Technologies and Systems (CTS), Atlanta, GA, USA, 2015, pp. 27-34.

[2]. A. Jafari, M. Shirali, and M. Ghassemian, "A testbed evaluation of MAC layer protocols for smart home remote monitoring of the elderly mobility pattern", in proc. CMBEBIH, Singapore, 2017, pp. 568-575.

[3]. H. Rezaie and M. Ghassemian, "An adaptive algorithm to improve energy efficiency in wearable activity recognition systems", IEEE Sensors Journal, Vol. 17, no. 16, pp. 5315-5323, 2017.

[4]. A. Bhave and S. R. Jajoo, "Secure communication in wireless sensor networks using hybrid encryption scheme and cooperative diversity technique", in proc. of the 9th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 2015, pp. 1-6.

[5]. S. Pérez, J. L. Hernández-Ramos, S. N. Matheu-García, D. Rotondi, A. F. Skarmeta, L. Straniero, and D. Pedone, "A lightweight and flexible encryption scheme to protect sensitive data in smart building scenarios", IEEE Access, Vol. 6, pp. 11738-11750, 2018.

[6]. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications", IEEE Internet of Things Journal, Vol. 4, no. 5, pp. 1125-1142, 2017.

[7]. X. J. Tong, Z. Wang, Y. Liu, M. Zhang, and L. Xu, "A novel compound chaotic block cipher for wireless sensor networks", Communications in Nonlinear Science and Numerical Simulation, Vol. 22, no. 1-3, pp. 120-133, 2015.

[8]. W. K. Koo, H. Lee, Y.H. Kim, and D. H. Lee, "Implementation and analysis of new lightweight cryptographic algorithm suitable for wireless sensor networks", in proc. of the International Conference on Information Security and Assurance. (ISA), Busan, South Korea, 2008, pp. 73-76.

[9]. M. Dener, "Security analysis in wireless sensor networks", International Journal of Distributed Sensor Networks, Vol. 10, no.10, 2014.

[10]. J. Daemen and V. Rijmen, "The design of Rijndael: AES-the advanced encryption standard", Springer Science & Business Media, 2013.

[11]. Y. Liu, S. Tian, W. Hu, and C. Xing, "Design and statistical analysis of a new chaotic block cipher for wireless sensor networks", Communications in Nonlinear Science and Numerical Simulation, Vol. 17, no. 8, pp. 3267-3278, 2012.

[12]. Sun SPOT World. (2009). [online] Available at:http://www.sunspotdev.org/docs/Yellow/SunSPOT-TheoryOfOperation.pdf [Acc14 Apr. 2018].

[13]. M. S. Baptista, "Cryptography with chaos", Physics letters A, Vol. 240, no. 1-2, pp. 50-54, 1998.

[14]. T. Xiao-Jun, W. Zhu, and Z. Ke, "A novel block encryption scheme based on chaos and an S-box for wireless sensor networks", Chinese Physics B, Vol. 21, no. 2, 2012.

[15]. G. Zaibi, F. Peyrard, A. Kachouri, D. Fournier-Prunaret, and M. Samet, "Efficient and secure chaotic S-Box for wireless sensor network", Security and Communication Networks, Vol. 7, no. 2, pp. 279-292, 2014.

DOI 10.17148/IJIREEICE.2019.7803