DOI: http://dx.doi.org/10.30684/etj.37.3B.1

Nabaa A. Hasan
Computer Science Department,
University of Technology,
Baghdad, Iraq.
nabaa_alkhafagi@yahoo.com

Alaa K. Farhan
Computer Science Department,
University of Technology,
Baghdad, Iraq.
110030@uotechnology.edu.iq

Received on: 13/02/2019
Accepted on: 01/05/2019
Published online on: 25/10/2019

Security Improve in ZigBee Protocol Based on RSA Public Algorithm in WSN

Abstract-*ZigBee is consuming low energy and providing the protection in Wireless Sensor Networks. ZigBee pro is supporting most applications. In spite of improved the security, ZigBee pro weak in key administration. In this paper, we depend on Logistic Map Diffie Hellman (LMDH) and SubMAC for Wireless Sensor Networks by ZigBee. In addition, we will improve the security in ZigBee by using the Rivest-ShamirAdleman (RSA) algorithm instead of Advanced Encryption Standard (AES). LMDH used for improved key administration schema (protect key distribution) and SubMAC used for providing authentication and prevented Man-In-The-Middle (MITM) and Replay attacks, LMHD did not provide this service, so we use SubMAC to overcome with this problem, and use RSA to improve the security by encrypting the network key and ensure that the connection is secure between the nodes and then we can send the data safely. And the results ensure: the proposed is extra effective when compare with ZigBee pro from where the execution time and power consumption, in addition, it proved that security is improving.*

Keywords-: *Key management, Logistic Map, LMDH, MITM, Wireless Sensor Network, ZigBee Pro.*

How to cite this article: N.A. Hasan and A.K. Farhan, "Security Improve in ZigBee Protocol Based on RSA Public Algorithm in WSN," *Engineering and Technology Journal*, Vol. 37, Part B, No. 3, pp. 67-73, 2019.

1. Introduction

Nowadays, Wireless sensor networks become important feature and very used of our daily life in most applications, recently, in monitoring health, environmental, agricultural and other applications. Most Challenges facing us how secure the messages that transmitted in WSN, Because the sensor nodes transmit sensitive and private information, must be secured so that ZigBee Pro [1] will ensure safety and low energy consumption for WSN. Sensors node have limited memory and low capacity .Therefore, limitations of the sensor must be considered. We will use LMDH for safety key distribution, and SubMAC for supporting the authentication and integrity to send message without any modification to the network, then we use RSA for improving the security in ZigBee.

ZigBee pro [2] (Last specification of ZigBee is called Zigbee2007) is suitable for WSN and improve security. Nevertheless, the improved key administration in ZigBee pro remains weak, especially in key Distribution.

In this essay: we implement logistic map and Diffie-Hellman (LMDH) for overcome on the ZigBee Pro weakness and to make LMDH is more efficiently, we used SubMAC [3] to provide the endorsement beside the prohibition Man-In-The-Middle attack, and RSA to improve the security and reduce time computation during encryption and deception process. The proposed abled to improve the security and support the endorsement in ZigBee pro for Wireless Sensor Networks. The remainder of the essay arranged in this way. Part 2 show related work. Part 3, 4 and 5 discussed Logistic Map, Diffie Hellman and RSA. Part 6 shows the proposed improved key management mechanism. Part 7 display environment, and discussed the results of proposed to estimate the efficacy of our suggested. In part 8 we estimated the schema in terms of security. Lastly, we deduce this essay in part 9.

2. Related Work

I. ZigBee pro

ZigBee depends on (IEEE 802.15.4). ZigBee pro is a criterion specific in (ZigBee 2007). ZigBee pro is improving the security in (Zigbee2006) by using two types of safely methods: a standard security method, appropriate to the resident security in (Zigbee2006) and high security method, appropriate with commercial security in (Zigbee2006). The security in ZigBee relies on Advanced Encryption Standard (AES-128) [4] algorithm. But in our proposed system, we will use RSA to improve the security and reduce run time. ZigBee' security consists of the modes and Transport, Device administration, and protect the frame. ZigBee used (master, network, and links) as a keys for security Administration. Table 1: show the three types of ZigBee' keys. Unencrypted key sending will cause the problem in security and this weakness of ZigBee. [5].

Table1: Security Keys

Keys	Layer	Message	Creation
Master key	Application layer	Unicast	Key-transport,pre-installation
Network key	Application/Network layer	Broadcast	Key-transport, pre-installation
Link key	Application layer	Unicast	Key-transport, pre-installation, Key establishment (Master key)

II. ECDH

[6] Kyung C et al. Used elliptic curve Diffie Hellman (ECDH) [7] to improve the key administration schema and SubMAC for Wireless Sensor Networks to overcome the vulnerabilities of key management of ZigBee. ECDH used for providing the safely of key distribution and SubMAC to avoid the vulnerabilities in ECDH, especially the endorsement and Man-In-The-Middle attack. By SubMAC, the endorsement for sending the packets and prevent Man-In-The-Middle and Replay attacks is achieving .

III. Chaotic encryption depends on ZigBee for the wireless network.

[8] Qiang H et al. Based on the chaotic theory, they presented a compound chaotic cryptographic system, which is based on the optical instability model and Logistic model, used as a chaotic sequence cipher. The complicated degree of chaotic sequences and cryptographic specific property are strengthened .They suggested a combination chaotic cryptographic schema, it depends on the optic imbalance mode and Logistic mode that use like chaotic series encrypt. The complicated degree of chaotic series and cipher specified property are supported.ZigBee becomes very important to the improvement of industrial automation, in particular the security in ZigBee become Focus of attention .The suggested schema is showed: it is need a few memory and it provided high security and the run time in encryption is very fast.

3. Logistic Map

It suggested by Pierre Verhulst (in 1845). Logistic Map is easy, nonlinear, and dynamic. It is a type of Chaotic Maps. Robert M. Used it (in 1979), and Made it very popular.Logistic Map is a Complicated polynomial of a chaotic schema where its action able appears from nonlinear Dynamic of simplest calculation. Logistic Map's equation shows as follows

$$\boldsymbol{xn+1} = \boldsymbol{r}\ \boldsymbol{xn}\ (\ 1-\ \boldsymbol{xn}\ ) \qquad (1)$$

Where $\boldsymbol{xn}$ shows the value between 1 and 0, and $\boldsymbol{r}$ displays the value between 0 and 1 [9].

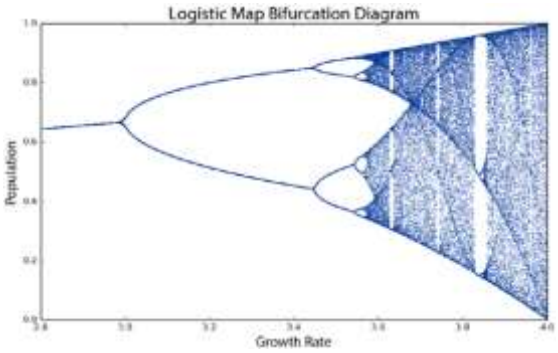

Figure 1. Bifurcation schema of logistic map.

4. Diffie Hellman [10]

Usually, there is a problem that everyone faces when sending data that is important, how to protect this data and send it in a safe way. Therefore, there were several ways to encrypt and how to exchange keys between the sender and the receiver, but the problem appeared exchange keys, how to send the message without exposure during transmission to modify and change and understood only by the sender and the recipient [11]. In 1976, Diffie and Hellman proposed algorithm usage to generate a shared private key among two people. Where it used like a schema for exchange encrypted keys for using in public cryptography algorithms as AES .

Diffie-Hellman protocol key exchanging [12]:

- Two parties concur for using prime value Pr and Q {1,….,Pr-1},
- This parties generate their private keys, named a, b {1,…, Pr-1}.
- User A compute his public key X=q^a mod p.
- User B computes his public key Y=q^b mod p.
- User A and user B exchange their public keys, to be used for private generation of common Secret key.
- User A compute the secret key SA=Y^a mod p. User B computes his secret key SB=X^b mod p.
- SA=SB.

5. Rivest-Shamir-Adleman (RSA)

In 1978, RSA suggested by Ron Rivest, Adi Shamir, and Leonard Adleman [13]. It is among the finest known public key cryptosystems for

key interchange or digital signature or cryptography of information. RSA uses not fixed size cryptography block and the size of the key is not fixed. RSA asymmetric encryption algorithm depends on number theory, it is a block cipher system. It uses two prime values to create the public and private keys. This keys use to encoder and decoder. Transmitter encrypts the packet by recipient public key, when the packet transfer to the recipient, the recipient will able to decrypt it with his private key .RSA procedures can be analyzed in three steps; key creation, encryption and decryption.

I. Key creation step [14]

1. Select two big prime values P & Q from the logistic map
2. Calculate N= P× Q .
3 .Compute: R = (P-1) × (Q-1) .
4. Select public key E, GCD (E, R) =1 .
5. Calculate the private key D by the relation D × E = 1 mod R; D is kept as private for two parties .

II. Encryption

Plain-text: M < N
Cipher-text: C= M^E mod N .

III. Decryption

Cipher-text: C
Plaint-text: M=C^D mod N.

6. Proposed System

We suggest using Diffie Hellman depend on Logistic Map to exchange the keys generated from logistic map. Fig. 2 shows the key exchange process. Where XA, XB public keys and SA, SB secret keys Fig. 3. Displayed a packet arrangement schema in the direction of the endorsement in criterion safely method. The Update Device and Transport Key requests communication among (Coordinator and Router) must secure. The Transport Key request sends from (the Router to the End Device) must not safely. Figure. 4 display the packet arrangement schema for the endorsement step in the criterion safely method.

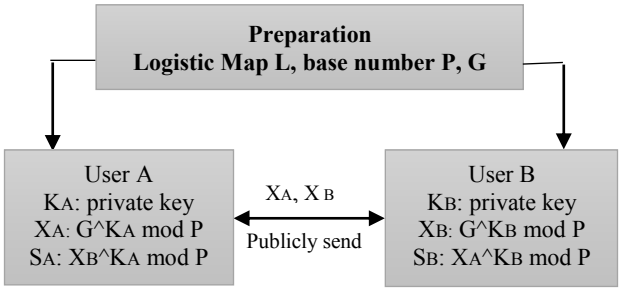

Figure 2. LMDH

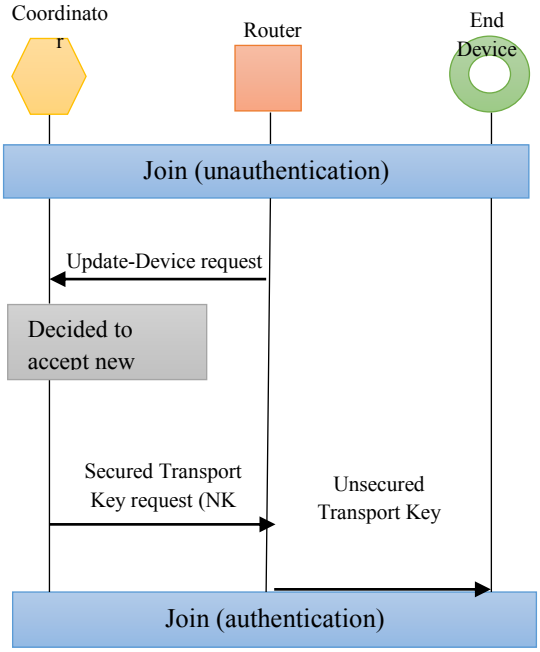

Figure 3. Authentication in standard security method.

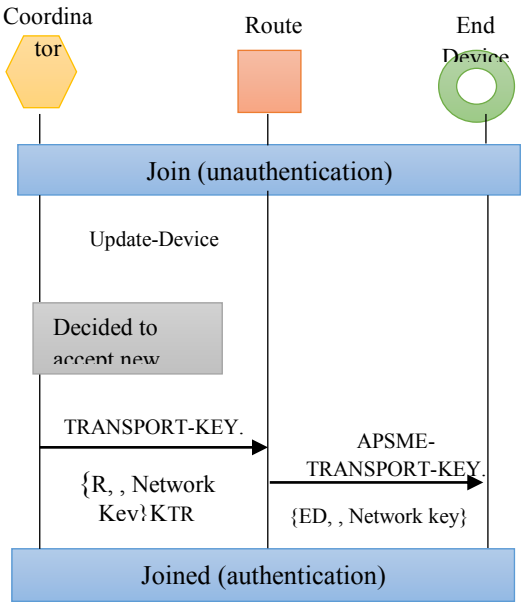

Figure 4. Message arrangement schema (standard security method).

Router to Coordinator
UPDATE-DEVICE. Request: {CO, ED} KTR

- CO: - 64-bit Coordinator address.
- ED: - 64-bit End Device address.
- KTR: - 128-bit key between Coordinator and Route

Coordinator to Router
TRANSPROT-KEY. Request: {R, Network Kev} KTR

- R: the address of router (64 bit)
- Network-key: the active of network key (16 values).
- KTR: among the Coordinator and Router (128 bit).

Router to End Device Transport Key.-request: {ED, Network Key}

- ED: 64-bit End Device address.
- Network-key: the activity of Network-Key (16 octets).

Update Device-request and Transport Key-request are encrypted through KTR amidst (coordinator and router.) Now, AES algorithm use. But, the Transport Key-request, transmitted from (router to the end device) did not safely. This appears safely weak.

We used LMDH to make network-key secure. SubMAC used for supported the packet endorsement, in addition it achieve the integrity, But there is still the risk of attack and detection of the value of network key, so it will encoded by RSA algorithm to improve the security and sent by the sender. The recipient will decrypt to check the integrity. Figure. 4 show the suggested key administration in criterion safely method.

Coordinator to End Device ED, XA, NS, SubMAC (XA, NS, ED)

- ED: 64-bit End Device address.
- XA: Coordinator creates value for the key.
- NS: 1octet nonce value.
- SubMAC (XA, NS, ED): transmitted packet SubMAC.

Coordinator creates XA for active network key, and transmitted ED, XA, NS, SubMAC (XA, NS, ED) to the End Device. The End Device generates SubMAC (XA, NS, ED) for comparing with the sending SubMAC (XA, N.S, ED). If they similarity, the End Device ensure to send the packet that did not editing. On the other hand, the End Device cancels sending packet. , If the examine is succeeded, End Device calculate k'=XAKB then calculate k' again but by Matyas Meyer Oseas (MMO) Hash Function [15]. Where 160bit of K' convert to 128bit for the network-key, nk.

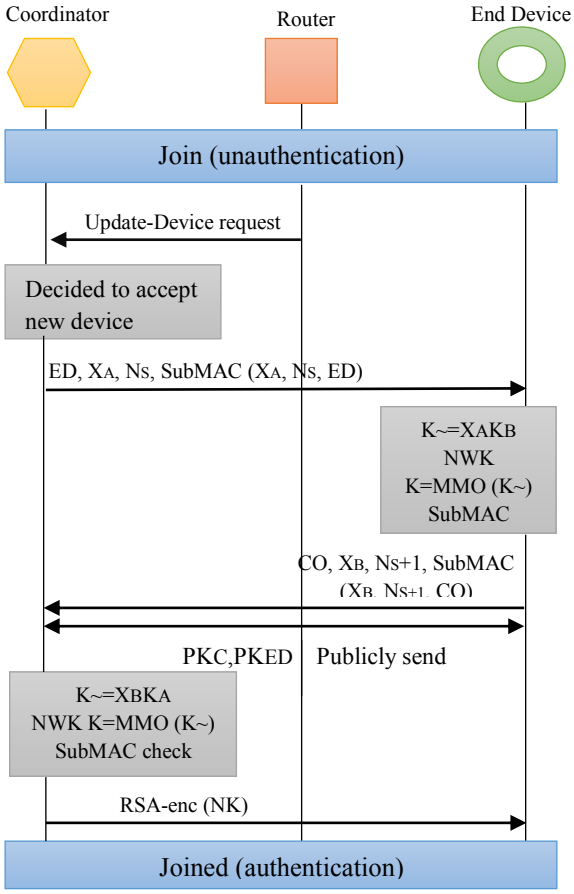

Figure 5. The proposed system to improve security in ZigBee by RSA algorithm.

End Device to Coordinator CO, XB, NS+1, SubMAC (Nk)

- CO: the address of coordinator (64 bit).
- XB: the public key of the end device.
- NS+1: addition 1 to sending nonce.
- SubMAC (Nk): SubMAC used network key

The End Device transmitted CO, XB, NS+1, SubMAC (Nk) to the Coordinator. Coordinator calculates K'=XBKA like End Device, and calculate Nk= MMO (K') to create the Network-key after that it creates the SubMAC, therefore. SubMAC is compare with the sending SubMAC (Nk).Packets endorsement are examined. A SubMAC construct by choosing several bits from (HMAC). We minimized the costs by sending just the section from (HMAC), instead of taking all the HMAC. SubMAC ensure packet integrity and endorsement. The proposed system chooses 8 bits only from 16 bytes. Then the Coordinator and End Device exchange their public keys (PKC, PKED). The public key used in encryption operation.

Coordinator to End Device RSA-enc (NK)

- RSA-enc (NK): encrypted the network key by public key of End Device.

Then, the public key of End Device encrypted the Network key, RSA-enc (NK): is send to (End Device) for examine packet integrity and declare is successes Network key creation and encrypted. Then End Device decrypted RSA-Dec (NK) through the private key of the End Device then examine NK to ensure the safety of Network key achieves .

7. Experimental Results

I. Programming Environment

The proposed system was written in c# language version 2013 on widows10 .

II. Effectiveness analyses of improved Key mechanism

We suggest improved key management mechanism by LMDH for secures key allocation and SubMAC to beat on the weakness of LMDH and improve the security by using RSA. The result was implemented five times .

In every of the former two steps with Coordinator, Router, and End Device. Median execution time in criterion safely method [6] is 0.5156 seconds, and in standard-ECDH [6] it is 0.5778 seconds; the contrast is 0.0622 seconds. While this difference compare to the median execution time of criterion safely method, added 12%. Although, the variation, 0.0622, either in suggesting key administration in a proposed system [16] (using LMDH) is 0.3593 Seconds. Note that, in our proposal's time is significantly reduced when compared to previous values. Figure 6: show the result of run time. The use of the logistic map instead of elliptic curve helped to reduce the complexity of the calculations and the use of special equations (addition or doubling), and thus reduce the time .

The second comparison in terms of time. The time of encoding and decoding in the RSA and AES algorithms, where the time of encryption with RSA and AES is 5.3928, 7.2853 seconds and the time of decryption in RSA, AES is 5.2234, 9.4456 seconds. When comparing the time in both algorithms, the time in RSA is approximately half the time in the AES algorithm. This indicates that our suggested system improves security and reduces time by half. As shown in the Figure 7 .

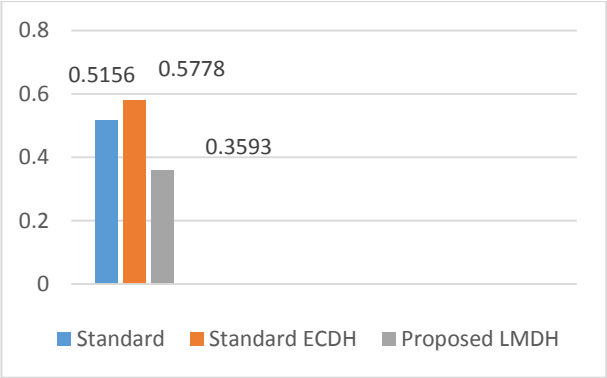

Figure 6: Result of Run –Time.

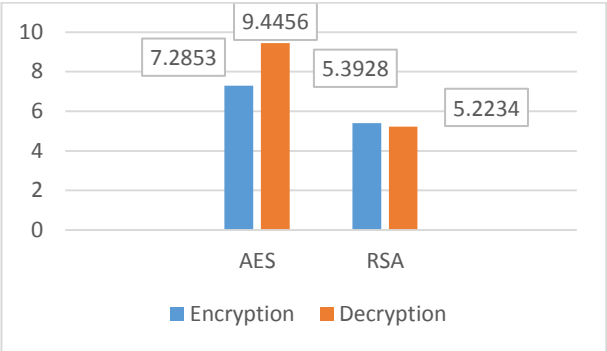

Figure 7: Run-Time in encryption and decryption for RSA and AES algorithms.

Then, we compute power consumption in End Device, Router and Coordinator. Table2 show details the values. While suggesting key distribution in safely method (stander ECDH) [6] is comparable to the criterion safely method, it absorbs more power .In particular, receiver state in the Coordinator display extreme distinction is 0.001447mJoule.Although, the Coordinator has enough Memory and power, thus the distinction is slight. Another distinction is 0.001412mJoule in receiver state in the End Device. In, receiver state in the Coordinator display extreme distinction is 0.001447mJoule. Although, the Coordinator has enough Memory and power, thus the distinction is slight. Another distinction is 0.001412mJoule in receiver state in the End Device. Our proposed [16] consumes close value in the Coordinator and in End Device in transmitted and received mode. In End Device, the energy has reduced compared with the standard security method and stander ECDH in transmitted. In received mode increase few. The sensor node uses two AA alkaloid batteries. An AA alkaloid battery contains a maximum of 3000mAh, so the total energy is 6000mAh. The formal voltage of an AA battery assumes 1.5 volts. The amount of electric power is 9Wh, Product Of 6Ah and 1.5 V and this is converted into 32,400J, 3600 X into 32, 400J, 3600 X 9(J) [17]. The difference is slight compared to 32,400J.

Table 2: Energy consumption.

NO.	Standard	Standard ECDH	Proposed LMDH
End Device: T	0.000217	0.000899	0.000391
End Device: R	0.020517	0.021929	0.009590
Router: T	0.049272	0.050564	0.000873
Router: R	0.000435	0.001348	0.017365
Coordinator: T	0.000365	0.000853	0.000482
Coordinator: R	0.020515	0.021962	0.007775

8. Security Analysis

We will discuss our improved key administration for ZigBee Pro. It is supporting the security characterize and overcome on several attacks. The endorsement. Nevertheless, the suggested system by SubMAC exceed this weakness and Improve the security and reduce run time

I. Confidential

ZigBee pro has important problem with confidentiality, due to the fact that master and network-key didn't secure the sending among The suggested system confirms on the Confidentiality of the keys by LMDH and the confidential increase when we are using RSA, because when just use LMDH may can detect about the value of network key when created. This is due to the reason that the public key participates in the channel, so the attacker may get the value of network key, but when encrypt the network key by RSA, this operation becomes very difficult .

II. Packet endorsement and integrity

In spite of LMDH did not secure sending data for key creation, it safely creates Keys. However, LMDH does not support authentication. By the SubMAC can check if any change occurs, our proposed confirms packet endorsement and integrity.

III. Man in the Middle Attack

LMDH have weakness to avoid (Man-In-The-Middle Attack). Nevertheless, the suggested system used SubMAC to overcome this attack, because the attacker did not realize the SubMAC and he not able to edit the SubMAC packet, despite of he take XA or XB (public keys) only and can edit them .Our suggestion examined the modification of sending packet by SubMAC.

ZigBee Pro has weakness in key administration in standard security methods, and by LMDH, this weakness solved. But LMDH could not avoid Man-In-The-Middle Attack and did not support

improves the safety, then we use RSA to improve (Router and the End Device). Besides, the use of logistic map in our proposed system help to reduce the attacks, because the logistics are sensitive to any change in values, if occur any change that leads to a change in the results, and thus this means attacker impossible to predict or try to compute any results and if he try it will be endless attempts .

IV. Replay attacks

The proposed system supported freshness by used, a nonce to overcome on the Replay - attack. When the packet sends more than once, the attacker may Misuse key generation data. Our suggestion change -nonce-value when a new key is created among (End Device and Coordinator) to avoid this problem. Consequently, the suggestion achieved the–freshness, also overcome on the Replay - attack.

9. Conclusion

The paper improves the security and reduce the time in encryption and decryption operations by using the RSA algorithm instead of the AES algorithm. And using LMDH and SubMAC help to achieve the effectiveness and the security also. LMDH use of secured key distribution, in addition, enhancement the weakness in LMDH, by SubMAC, the suggested system able to achieve the endorsement and integrity. And by nonce number the freshness achieves.

Our scheme in comparison with ZigBee Pro and proposed ECDH provides effectiveness by obtaining less execution time and few power consuming in criterion safely method .

The proposed system supported authentication, and integrity. Accordingly, our scheme prevented (The Man-In-The-Middle and Replay attacks). As a result, our suggestion provides effectiveness and safely when it compared with ZigBee pro.

References

[1] T. Alhmiedat, "Low-power Environmental Monitoring System for ZigBee Wireless Sensor Network", VOL. 11, NO. 10, Oct. 2017.

[2] ZigBee Alliance, "ZigBee-2007 Specification," San Ramon, CA 94583January 2008.

[3] N. Challa, H. Cam, and M. Sikri, "Secure and Efficient Data Transmission over Body Sensor and Wireless Networks," EURASIP Journal on Wireless Communications and Networking, VOL 2008, Article ID 291365, 18 pages, February 2008.

[4] S.M. Soliman, B. Magdy and M.A. Abd El Ghany, "Efficient Implementation of the AES Algorithm for Security Applications," IEEE, 2016.

[5] C. Alcaraz, and J. Lopez, "A Security Analysis for Wireless Sensor Mesh Networks in highly Critical Systems," IEEE. Transactions on Systems, MAN, and Cybernetics, Part C: Applications and Reviews, Vol. 40, No. 4, July 2010.

[6] K. Choi, M. Yun, and K. Chae and M. Kim, "An Enhanced Key Management Using ZigBee Pro for Wireless Sensor Networks," IEEE, 2012.

[7] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, Vol. 48, No. 177, January 1987.

[8] Q. He, Q. Qi, Y. Zhao, W. Huang, and Q. Huang, "The Application of Chaotic Encryption in Industrial Control Based on ZigBee Wireless Network," IEEE, 2008.

[9] V.C. Preduna, F.M. Jimenez and A.P. Manguillot, "The logistic map of matrices," Universitat Politecnica de Valencia, September 13, 2012.

[10] W. Diffie, and M. E. Hellman, "New Direction in Cryptography," IEEE Transactions on Information Theory, 1976.

[11] W. Jirakitpuwapat and P. Kumam, "The Generalized Diffie-Hellman Key Exchange Protocol on Groups," Springer International Publishing AG 2018.

[12] M. Ahmed, B. Sanjabi, D. Aldiaz, A. Rezaei, and H. Omotunde, "Diffie-Hellman and Its Application in Security Protocols," Certified International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 1, Issue 2, November 2012.

[13] G. Singh and Supriya "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," International Journal of Computer Applications (0975 – 8887) VOL 67, No.19, April 2013.

[14] U. Somani, K. Lakhani and M. Mundra, "Implementing Digital Signatures with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 1st International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, India, pp. 211-216, 2010.

[15] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone, "Handbook of applied cryptography," 1996.

[16] A.K. Farhan, N.A. Hasan, "Improved key management using ZigBee Pro and logistic map for wireless sensor networks," 3st International Scientific Conference on Integration between government institutions and private sector institutions - constraints and prospects for success, Baghdad, Iraq, 2019.

[17] K. Choi, M.-H. Kim, K.-J. Chae, J.-J. Park, and S.-S. Joo, "An Efficient Data Fusion and Assurance Mechanism using Temporal and Spatial Correlations for Home Automation Networks," IEEE Transactions on Consumer Electronics, VOL. 55, No. 3, August 2009.