Header Encryption of IEEE802.15.4

[1]Hemin Nilesh Dalal
[1]h.dalal@vikes.csuohio.edu

[2]Nisarg V Soni
[2]n.v.soni@vikes.csuohio.edu

[3]Abdul Razaque
[3]a.razaque@csuohio.edu

Department of Electrical and Computer Science
Cleveland State University, Cleveland, OH

Abstract*— In this paper, we mainly focus on the security of 802.15.4 MAC (Media Access Control) which used in Zigbee technology. Today, 802.15.4 Medium Access Control (MAC) is used in personal area networks, for example industrial automation, medical, home automation. However, encryption on MAC data payload have been introduced, but Medium Access Control (MAC) header is still non-encrypted. Authentication of MAC header is certainly done with the use of Data Integrity by giving Message Authentication Code or Message Integrity Code (MIC). Medium Access Control (MAC) header frame has three fields: frame control, addresses and auxiliary security. Among all of these fields of MAC header which includes frame control, sequence number, source and destination addresses and auxiliary security header (ASH) must be encrypted to secure it against some attacks like ACK attack, replay protection attack, snooping attack, denial of service attack, CTS replay, RTS replay. Auxiliary security header have the details about the security of data payload which must not be known to intruders. Our aim for securing it is multi level security. This header field has a total of 40 bytes. For encryption of these 40 bytes of Medium Access Control (MAC) header, we have used Advance Encryption Standard (AES) algorithm, which creates best confusion and diffusion. Advance Encryption Standard algorithm has three types of frame structure: 128 bits, 192 bits, 256 bits. To encrypt these 40 bytes of Medium Access Control (MAC) header we have used two Advance Encryption Standard (AES) algorithms of 192 bits and 128 bits which both are working parallel together.

***Index Terms*—WSN, AES, Encryption, Header, Security, Attacks,**

I. INTRODUCTION

The wireless sensor network is being used in many personal area networks like medical, automation and industries. There are a number of wireless sensor network [1] (WSN) available in market e.g. Bluetooth, Wi-Fi, Wi-Max. Among all WSN (wireless sensor network), Zigbee [2] is the most preferable one for a personal area networks because of low data rate and low power consumption. At the same time, security must be concerned. Zigbee uses 802.15.4 MAC frame from which the data payload is sent to the upper layer (data link layer). However, some research has been done [3-5] for the security of this data payload but security of the MAC header has not been concerned. [6] Advance Encryption Standard (AES) algorithm of 128 bits encrypted the data payload. [7] AES has both features of encryption and authentication. [7] Although PAN Id and MAC address is authenticated with the use of Message Integrity Code (MIC), the encryption is still missing.

802.15.4 Specification MAC frame have these fields: Frame control (2B), Sequence number (1B), Destination address (11B), Source address (11B), Auxiliary Security Header (ASH) (15B), Data payload (0-X B) and cyclic redundancy check CRC (2B).

Frame control of 802.15.4 specification [8] contains frame type (3 bits), security enabled (1 bit), frame pending (1 bit), acknowledgement request (1 bit), personal area network (PAN) ID (1 bit), some reserved (3 bits), destination addressing mode (2 bits), frame version (2 bits) and source addressing mode (2 bits). Sequence number specifies the sequence identifiers, e.g. beacon sequence number and data sequence number for the frame. Destination and source address have destination and source PAN ID and addresses. Auxiliary Security Header specifies information required for security processing. This field shall be present only if security enabled field of frame control is set to one. Data payload contains the actual data and it will be encrypted when security enabled of frame control is set to one.

Some attacks [9] may occur at the 802.15.4 specification MAC header. Same-nonce attack [9] is defined as follows. In cryptography, a nonce is an arbitrary number that may only be used once. It is similar in spirit to a nonce word, hence the name. It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks. If such a thing happens, a security attack is possible. Note that the nonce is also used as the frame counter. There is a chance of having same key and the same nonce.

In addition replay-protection attack [9], which is one kind of denial-of-service attacks. An attacker can send many frames containing different large frame counters to a receiver who performs replay protection and raises the replay counter up as the largest frame counter in the receiver so far. Then, when a normal station sends a frame with a reasonable size of frame counter that is smaller than the replay counter maintained at the receiver, the frame will be discarded for the replay-protection purpose. In other words, the service is denied.

Furthermore, ACK attack [9] can also be there. When a sender sends a frame, it can request an ACK frame from the receiver by setting the bit flags in the outgoing data frame. The eavesdropper can forge the ACK frame by using the unencrypted sequence number from the data frame. If an attacker does not want a particular frame to be received by the receiver, it can send interference to the receiver at the same time when the sender is sending the data frame. This leads to the rejection of the frame. The adversary can then send a duplicate ACK frame fooling, the sender that the receiver successfully received the frame. Therefore, a sender cannot be sure if the received frame is coming from the receiver or from the attacker even if the receiver received the ACK frame. In addition, attacks on source and destination address (part of MAC header) can be there, like IP spoofing [10]. IP Spoofing involves modifying the

packet header with a forged (spoofed) source IP address, a checksum, and the order value. Attacker may also behave as a receiver node so that it can receive the data by altering the actual destination address. ACK frame, as well as data frame, are part of frame control field. The above attacks lead to the necessity of encryption of 802.15.4 specification MAC header. Furthermore, the paper presents a detailed description of mathematical calculations in AES algorithm which are sub bytes, shift row, mix column and add-key to encrypt the MAC header to prevent it from intruder.

To secure this, some algorithms or ciphers have been introduced to do mathematical calculations with the plaintext to create confusion and diffusion at the source side so that cryptanalysts (attacker) cannot alter or use the data. To encrypt the 802.15.4 MAC header, we proposed to use Advance Encryption Standard algorithm. This MAC header has 40 Bytes [ ] in a MAC header. We are proposing to use two AES algorithms: one of 128 bits (16 Bytes) and other is of 192 bits (24 Bytes) to encrypt this 40 Bytes.

The rest of the paper is organized as follows. Section II. Related work. Section III. Problem Identification and significance. Section IV Design and methodology. Section V Implementation. Section VI Experimental Results, and Section VII concludes entire paper.

II. RELATED WORK

To secure the 802.15.4 specification MAC frame, cryptographic algorithms, like Advance Encryption Standard, have been used. Here, MAC header contains first 40 Bytes are, MAC payload is of variable bytes as mentioned above. Moreover, Cyclic Redundancy Check (CRC) comes in the MAC footer part. To encrypt the data payload, one cipher suits called Advance Encryption Standard have been used.

Frame control of 2 bytes, have the following format: Frame type (3 bits), gives the details of frame type i.e. whether the frame is a beacon frame, data frame, ACK frame or any other frame. Security enable (1 bit) provides the detail of encryption of MAC data payload i.e. whether MAC data payload is encrypted or not. Frame pending (1bit) gives the information of whether there is any pending frame or not.

The acknowledgment request (1bit) describes the details of the ACK request, i.e. whether acknowledgement from the receiver is requested or not. PAN Id compression (1 bit) gives the details of PAN Id compression of source and destination address, i.e. the presence of PAN Id in the frame. Destination addressing mode (2 bits), which gives the details of address length of destination Frame version (2 bits), informs whether the frame is compatible with IEEE frame format or the frame version is of IEEE. The source addressing mode (2 bits) gives the details of address length of source

To encrypt the MAC data payload, Advance Encryption Standard is used. At the same time, data integrity (authentication) [6] is also done for MAC header. Advance Encryption Standard has three frames: 128 bits, 192 bits, 256 bits [11]. For the security purpose of MAC data payload, the 128 bit AES algorithm is used.

There are four objectives of security services: access control, data encryption, frame integrity, and sequential freshness. [8] They are explained as follows. Access control provides a list of valid devices from which the device can receive the frames. This mechanism prevents the unauthorized devices to communicate to the network. Data encryption prevents messages from the unauthorized access via encryption algorithms. Only the devices that share the secret key can decrypt the messages and communication. Frame integrity prevents changes from being made by an invalid intruder and to provide assurance that the messages from the source device have not been altered by the invalid intruder.

By using this Advance Encryption Standard 128 bits encryption method, MAC data payload has completely encrypted and MAC header has authenticated.

III. PROBLEM IDENTIFICATION AND SIGNIFICANCE

However, MAC payload is encrypted, but certainly MAC header is not encrypted as it also requires encryption to protect it from same-nonce attack, replay protection attack, denial of service attack, and an ACK attack; which are attacks on frame control and sequence number and IP spoofing attack which occurs on destination and source addresses.

As of now, 802.15.4 medium access control had an encryption over the data payload part, but in this paper we proposed encryption of header part, which shows the improvement in the most important part of network communication: security. Encryption of header part improves the security level of whole 802.15.4 medium access control frame to 4-5 % then before and most importantly provides protection from attacks likes same-nonce attack, replay protection attack, denial of service attack, ACK attack and IP spoofing attacks which poses on header part.

IV. DESIGN AND METHODOLOGY

Cryptography is the essential part for the secure network communication. In AES algorithm, there are three frame structures: 128 bits, 192 bits, and 256 bits as mentioned above. Some mathematical calculations like sub bytes, shift row, mix column, and add key are used for numbers of rounds. Each frame structure has different number of round for the calculations; 10 rounds, 12 rounds, and 14 rounds respectively for 128 bits, 192 bits and 256 bits frame structure.

There are three modes of operation in AES : counter mode (CTR mode) that is used for providing the encryption, cipher block chaining message authentication code (CBCMAC) mode that provides just the authentication, and the CTR+CBC-MAC (CCM) mode that combines both the CTR and the CBC-MAC mode of operations and provides both the authentication and encryption of the message. Finally, the possible MIC (message authentication code) bit lengths can be 32, 64, and 128 bits.

A. Encryption by AES algorithm

As discussed above, some mathematical calculations are done in AES algorithm. Figure 1 shows all the steps to be performed in AES for all the frames.

Each and every round has some calculation: sub bytes, shift rows, mix column, add round key. Because of these numbers rounds, AES provides the best confusion and diffusion. To encrypt 40 Bytes (320 bits) of MAC header we proposed to use two AES algorithm: one is of 128 bits and other is 192 bits. Both these algorithm will work parallel together.

Auxiliary Security Header will only present in the frame when the security enable bit is set in the frame control field,. i.e. MAC data payload is encrypted. As encryption of MAC data payload will always be there, Auxiliary Security Header will be present in MAC header frame. Auxiliary Security Header, which is of 15 Bytes, includes all the detail information of

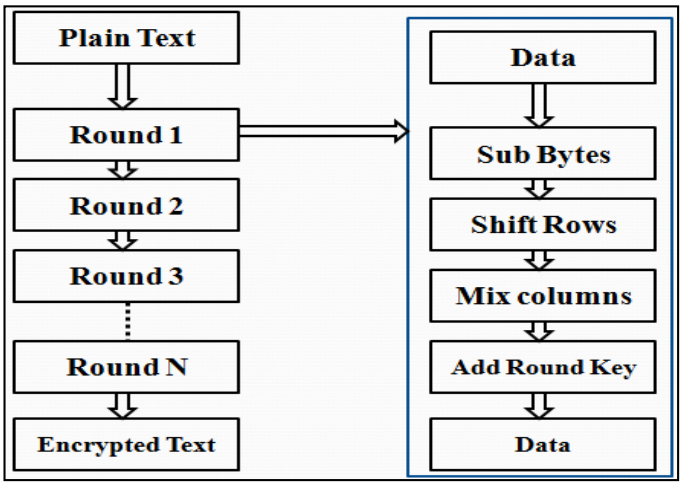

Fig. 1. AES algorithm for all frames and steps in one round

security like security level (3b), key identifier (2), reserved bits of 3 bits, key source (9b), and key index (1b). This information might be stolen without encryption, which leads to encryption of all the 40 Bytes of MAC header.

V. IMPLEMENTATION

We are proposing to implement two AES algorithm which work parallel together. To secure 40 Bytes (320 bits), of MAC header, we are using one AES of 128 bits and other AES of 192 bits. AES frame of 128 bits (16 Bytes) includes 10 rounds and each round includes some mathematical calculations like sub bytes, shift rows, mix column, add round key except 10th round as mentioned above in paper.

The AES algorithm bits of 128 encrypts first 16 bytes of MAC header bytes (72 bits) of source address and 15 bytes (120 bits) of auxiliary security header which includes frame control (2 bytes), sequence number (1 bytes), and 2 bytes (16 bits) of destination address.

Encryption in 192 bits AES algorithm is same as 128 bits AES encryption except number of rounds and length of the key is differed. The numbers of round are 12 and length of the round-key is 24 bytes (192 bits). Moreover, the last round does not have the mix-column operation as in 128 bits AES encryption. The second AES algorithm encrypts remaining 9 bytes (72 bits) of source address and 15 bytes (120 bits) of auxiliary security header. Figure 2 shows the process flow of one round of AES algorithm.

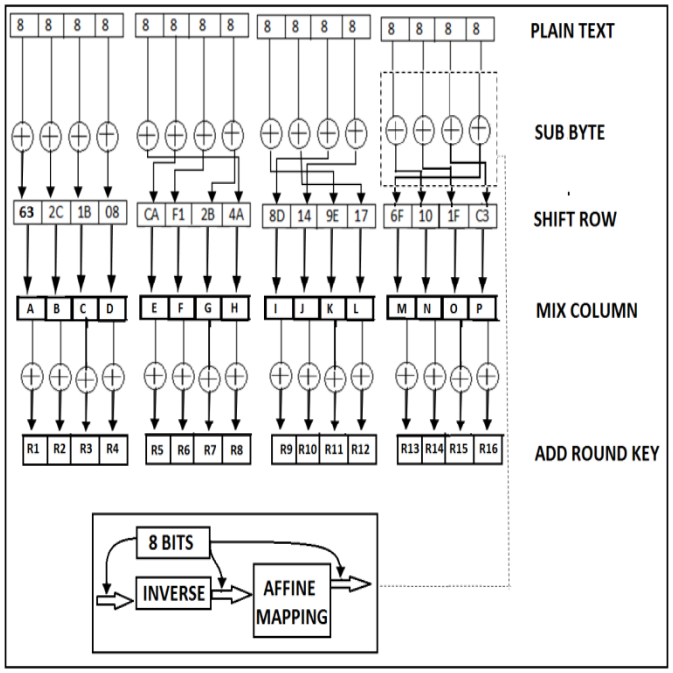

Fig. 2. One round process of AES algorithm

A. Sub-bytes

Considering first 128 bits of MAC-header: 16 bits of frame counter, 8 bits of sequence number, 88 bits of destination address and first 16 bits of source address. Figure 3 and Figure 4 show the first 128 bits of MAC header before and after sub byte operation in first round.

00	2C	1B	08
CA	F1	2B	4A
8D	14	9E	17
6F	10	1F	C3

Fig. 3. First 128 bits of MAC header before sub byte operation

63	71	AF	C5
74	A1	F1	D6
5D	FA	0B	F0
A8	CA	C0	2E

Fig. 4. First 128 bits of MAC header after sub bytes operation in first round

Here, input of inverse block is X [i] = 63 i.e. 01100011 (b), so inverse of it is Y[i] = 9C i.e. 10011100. Affine mapping is one mathematical permutation in which following calculations are done. Figure 5 shows the fixed affine mapping matrix, which is obtained after inverse process in sub byte operation.

$$\begin{bmatrix} z0 \\ z1 \\ z2 \\ z3 \\ z4 \\ z5 \\ z6 \\ z7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} y0 \\ y1 \\ y2 \\ y3 \\ y4 \\ y5 \\ y6 \\ y7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Fig. 5. affine mapping matrix

The output of sub byte operation can be taken directly by referring S-Box [11], which is fix matrix of 256 hexadecimal entries.

B. Shift row

The result is of sub byte is followed by shift operation. Shift row is a mathematical operation which shifts each byte in row of 4 bytes. In first 4 bytes, there is no shifting. In second, third and fourth row, one, two and three times shift to the left is done respectively. Figure 6 describes the shift operation.

63	71	AF	C5
A1	F1	D6	74
0B	F0	5D	FA
2E	A8	CA	C0

Fig. 6. Row Shift operation

The main function of shift row operation is to provide "diffusion" over all the 128 bits i.e. only one change in single bit creates the diffused result.

C. Mix column

Further, the result of shift row operation is followed by mix column operation. Each bytes in a group of four are, multiplied with some constant matrix to create the result. Here, multiplication is done by converting all the hexadecimal into polynomial function. For example, the first row (4 bytes) are multiplied with the constant matrix. The main function of mix column is to provide more and more diffusion in the result, so that attacker cannot identify the actual data. Figure (6) shows the mix column operation for the first four bytes in which A, B, C, and D are the results. Polynomial equivalent of 01, 02, 03 are 1, X, X+1 respectively.

Matrix multiplication is done like,

A= (02*63) + (03*71) + (01*AF) + (01*C5) (1)

B= (01*63) + (01*71) + (02*AF) + (03*C5) (2)

C= (01*63) + (01*71) + (02*AF) + (03*C5) (3)

D= (03*63) + (01*71) + (01*AF) + (02*C5) (4)

$$\begin{bmatrix} A \\ B \\ C \\ D \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} + \begin{bmatrix} 63 \\ 71 \\ AF \\ C5 \end{bmatrix}$$

Fig. 7. Mix column operation for first 4 bytes

From above equations, it is clear that changing in only one bit will change the whole result i.e. it provides the best diffusion.

D. Add Round key

Finally, the result of mix column is followed by the add-round key operation. Round key is added in the 128 bits data after each and every round. The results after adding the round key is shown in figure (8).

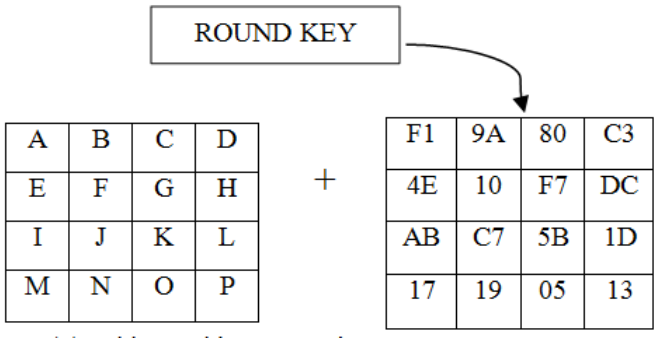

Fig. 8. Add round key operation

Here, addition of matrix is done like,

A'= A + F1, B'= B + 9A, C'= C + 80 etc.

Each and every round have its own key which is added at the end of the round. These mathematical operations are permutated with all of the 16 bytes and result is then followed by the second round. This process is continued up to the 10th round. But last round does not have mix column operation. Encryption in 192 bits AES algorithm is same as 128 bits AES encryption except number of rounds and length of the key is differed as mentioned in s section.

Moreover, this round key can be added at the beginning as well as at the end of the round. As a consequence, it provides efficient security. This is called “key widening”. [12]

VI. EXPERIMENTAL RESULTS

We simulate AES 128 and 192 bit algorithm for 802.15.4 MAC header security using turbo C programming language. To validate our idea, we use case study, let's take a scenario of a closed network which contains 100 nodes, in which 10 %(10 nodes) are malicious nodes which leads to propose some malicious attacks in the network, and 90 %(90 nodes) are legitimate nodes. This malicious attacks could be happened to target MAC header or Mac payload. As there is 10 attacker nodes in the network counters number of attacks on Mac frame structure.

TABLE 1: PARAMETERS OF CASE STUDY

Used Parameters	Details of Parameters
Total Number of Nodes	100
Legitimate Nodes	90
Malicious Nodes	10
Number of Attacks	1000
Total bytes of MAC frame	500
Bytes in payload part	460
Bytes in header part	40
Security(%) with payload Encryption	90%
Security(%) with payload and Header Encryption	95-98%

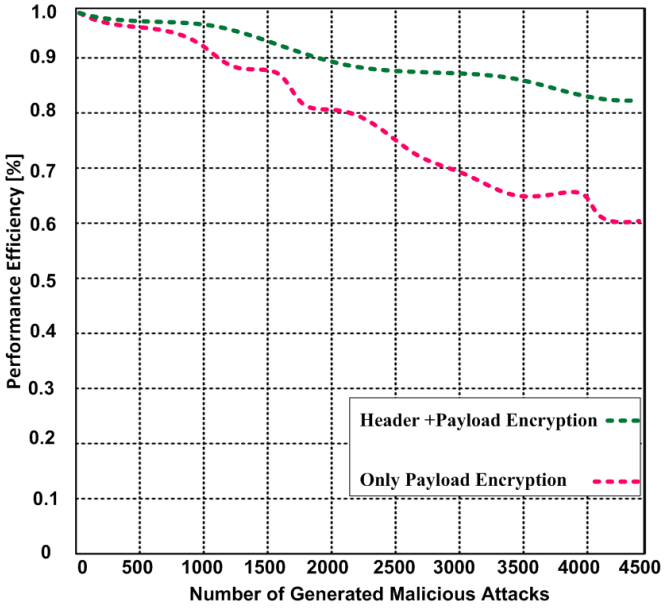

Fig. 9. 802.15.4 MAC frame security using AES

Before encryption of header only payload security is there, content of payload is fully secured with AES CTR, but header is not, which helps attacker to gain access of data by manipulating header information with ease. As shown in figure although payload is secured but some attacks like same-nonce attack, replay protection attack, denial of service attack, ACK attack and IP spoofing can degrade the security, so header security is also essential to secure the frame structure and to provide double security to payload by securing auxiliary security header which contains security information of payload. Let's take an assumption, the total number of bytes in the frame is 500, out of which 40 bytes is of header part and remaining 460 bytes is of data payload part.

Without an encryption of payload, security of the frame was around 90% which increased up to 95-98% with consideration of header encryption. By efficient implementation of AES-CTR 128 and 192 bit algorithm these attacks on Mac header is successfully reduced at some optimized level. Parameters of the case study are explained in table 1, and figure 9 gives the graphical representation of increased security with encryption whole 802.15.4 medium access control header frame.

VII. CONCLUSION

In this paper we introduced an approach to extend security of 802.15.4 medium access control header. As we discussed in sections above, some attacks which may occurs on frame control, sequence number, addresses and auxiliary security header leads to serious problems. By efficient implementation of two AES frames of 128 and 192 bits algorithm MAC Header (40 Bytes) encrypted, to secure it from such attacks like, same-nonce attack, replay protection attack, denial of service attack, ACK attack. As a consequence, we can improve the security of 802.15.4 medium access control (MAC) frame.

REFERENCES

[1] Yick, Jennifer, Biswanath Mukherjee, and Dipak Ghosal. "Wireless sensor network survey." Computer networks 52, no. 12 (2008): 2292-2330.

[2] Kinney, Patrick. "Zigbee technology: Wireless control that simplyworks." In Communications design conference, vol. 2, pp. 1-7. 2003.

[3] Vidgren, Niko, Keijo Haataja, Jose Luis Patino-Andres, Juan Jose Ramirez-Sanchis, and Pekka Toivanen. "Security threats in ZigBee-enabled systems: vulnerability evaluation, practical experiments, countermeasures, and lessons learned." In System Sciences (HICSS), 2013 46th Hawaii International Conference on, pp. 5132-5138. IEEE, 2013.

[4] Yang, Bin. "Study on security of wireless sensor network based on ZigBee standard." In Computational Intelligence and Security, 2009. CIS'09. International Conference on, vol. 2, pp. 426-430. IEEE, 2009.

[5] Yüksel, Ender, Hanne Riis Nielson, and Flemming Nielson. "Zigbee-2007 security essentials." In Proc. 13th Nordic Workshop on Secure IT-systems, pp. 65-82. 2008.

[6] Xiao, Yang, Hsiao-Hwa Chen, Bo Sun, Ruhai Wang, and Sakshi Sethi. "MAC security and security overhead analysis in the IEEE 802.15. 4 wireless sensor networks." EURASIP Journal on Wireless Communications and Networking 2006, no. 2 (2006): 81-81.

[7] Sastry, Naveen, and David Wagner. "Security considerations for IEEE 802.15. 4 networks." In Proceedings of the 3rd ACM workshop on Wireless security, pp. 32-42. ACM, 2004. 1989.

[8] http://cdn.rohde:schwarz.com/pws/dl_downloads/dl_application/application_notes/1gp105/1GP105_0E_Generation_of_IEEE_80215_Signals.pdf.

[9] Sokullu, Radosveta, Ilker Korkmaz, Orhan Dagdeviren, Anelia Mitseva, and Neeli R. Prasad. "An investigation on IEEE 802.15. MAC layer attacks." In Proc. of WPMC. 2007.

[10] Yang, Jie, Yingying Chen, and Wade Trappe. "Detecting spoofing attacks in mobile wireless environments." In Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on, pp. 1-9. IEEE, 2009.

[11] Zeghid, Medien, Mohsen Machhout, Lazhar Khriji, Adel Baganne, and Rached Tourki. "A modified AES based algorithm for image encryption." International Journal of Computer Science and Engineering 1, no. 1 (2007): 70-75.

[12] Zeghid M, Machhout M, Khriji L, Baganne A, Tourki R. A modified AES based algorithm for image encryption. International Journal of Computer Science and Engineering. 2007 May;1(1):70-5.

[13] Chodowiec P, Gaj K. Very compact FPGA implementation of the AES algorithm. InCryptographic Hardware and Embedded Systems-CHES 2003 2003 Jan 1 (pp. 319-333). Springer Berlin Heidelberg.