Adaptive Security Protocol for Wireless Body Area Network
بروتوكول امني مطور لشبكة (BAN) اللاسلكية

Dr. SAIF M. KH. AL-ALAK
Computer Science Department, College of Science for Women, Babylon University
E-mail: saif.shareefy@gmail.com
Dr. MOHAMMED ABDULLAH NASER
E-mail: mohamed_1276@yahoo.com
Computer Science Department, College of Science for Women, Babylon University
AHMED M. HUSSEIN
E-mail: ahmed_mar81@yahoo.com
Computer Science Department, College of Science for Women, Babylon University

Abstract

The need for Wireless Body Area Network (WBAN) technology has been increased rapidly. It has been adopted in many applications such as medical and military. Due to the nature of WBAN environment and transmitted data (sending data over unsecure wireless network and the sensitivity of data), there are several security challenges in WBAN, which restrict WBAN utilization. One of the security challenges in WBAN is replay attack.Also the WBAN adopted Advanced Encryption Standard (AES) in CCM (Counter with CBC-MAC) mode for the message confidentiality and message authenticity. However, brute force attack can break AES secret key in a reasonable time within high speednew technologycomputers.This paper suggested a security protocol to improve the WBAN robustness against replay attack by using Multiple Key-Protocol-Advanced Encryption Standard to show its improvement for key strength against secret key breaking.The mathematical calculations proved that the suggested multiple key protocol increases the secret key strength and security system complexity.

Keywords: AES, CCM,nonce, replay attack, WBAN.

ملخص البحث

ازدادت الحاجة لاستخدام تقنيةشبكة الجسم اللاسلكيةالمسماة بـ (WBAN) بشكل كبير. تم اعتمادتلك التقنية في عدة تطبيقات منها الطبية والعسكرية . بسبب طبيعة البيئة التي تعمل فيها هذه الشبكات ونوع البيانات المرسلة من خلالها (اذ انها تُرسل عبر شبكة وايرليس غير آَمنة بالاضافة الى حساسية واهمية تلك البيانات)، فان هناك عدة تحديات تتعلق بالامنية قادت التقويض عمل وتقليل فائدة هذا النوع من الشبكات اللاسلكية. واحدة من تلك التحديات الامنية في شبكة (WBAN) هو الهجوم المسمى بهجوم الاعادة (replay attack). اضافة الى ان (WBAN) يستخدم نظام السرية والتوثيق المسمى (AES-CCM)ذات المفتاح السري الوحيد . من ناحية اخرى، أن خوارزية تشفير الــ(AES) ممكن كسرها من قبل الهجوم من نوع (brute force attack) فيمدّةزمنية معقولةبأستخدامحاسباتذات تقنيةحديثة وسرعةعالية.في هذاالبحثتم إقتراحنظامأمنيلتحسينقوة (WBAN) ضدّالهجمات المشار اليها في اعلاه . حيث يتم استخدام التشفير(AES)متعدّد المفاتيحلاظهار قدرته في تحسينقوّةهذا النظامضدّ محاولاتكسرالمفتاحالسري. أثبتتالحساباتالرياضيةأنّالنظامالمقترح ذو المفتاح المتعدّد يزيدمن قوّةالمفتاحالسريوتعقيدالنظامالأمني.

1. Introduction

Recently, Wireless Body Area Network (WBAN) has been used in many applications, such as health care, medical, and military applications [1][2] [3]. The IEEE 802.15[4] standard is used as a platform for many specifications and applications. WBAN [5] is one of the most interesting specification which is IEEE 802.15 based.

The WBAN adopted Advanced Encryption Standard (AES) [6] in CCM*[7] security mode for the message confidentiality and message authenticity. The secret key length for AES algorithm is set to 128-bit. Many types of secret key attack like brute force attack[8] are used to break the secret key. Secret key strength and security system complexity can be increased by using Multiple-Key Protocol (MKP) [9], which provides multiple keys for the node depending on its security level (number of secret keys). This paper analyzed the strength of secret key belong to MKP in terms of time complexity.

The WBAN has a possibility of replay attack. For this purposenonce is sending to ensure no messagewould be under replay attack. The length of nonce is related to the message size,[10][11] that means the length of nonce is decreased by message size increasing and vice versa. The strength of nonce is increased when its length increase and vice versa. The MKP increases the strength of nonce as explainedin the analyzedresult. The objective of this paper is to show the security improvement over WBAN by implementing MKP-AES. We computed the Randomness for MKP-AES protocol in [13].

The rest of paper is organized as follows.Second sectionshows the typical architecture of WBAN. Third section defines the security options of BAN. The fourth section explains the AES algorithm. The fifth section explains CCM security mode. The sixth section analyzes the MKP in terms of key strength and nonce length. The seventh section computes the nonce length with different levels of security and various message sizes.

2. WBAN Architecture

In order to understand the fundamental of WBAN architecture, the medical model (as example) is explained briefly. Figure 1 illustrates the architecture of WBAN, where it consists of following parts:

1-WBAN: It includes a small network of nodes close to the person body.
2-Gatway: It collects the data about the person from WBAN and sends it over the network.
3-Network (Internet): It can be LAN, MAN, and WAN etc.
4-Applications: It a GUI that used by the observer (doctors or any authorized person).

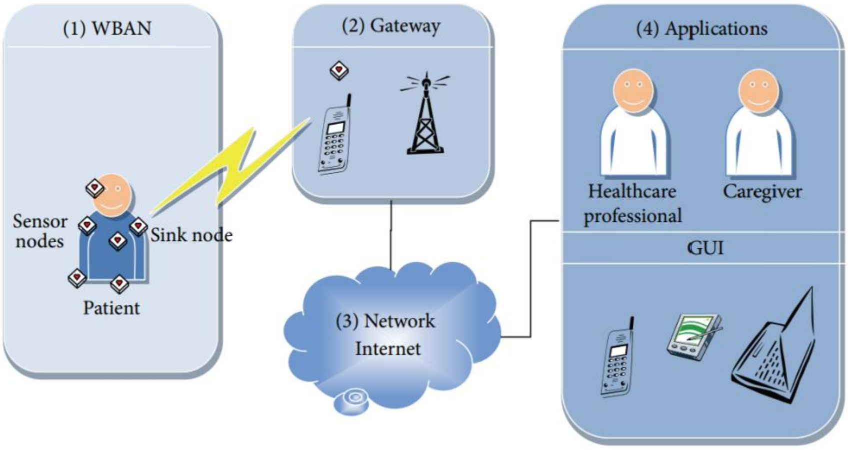


Figure 1:WBAN Architecture

3. WBAN Security Issues

WBAN is built over IEEE 802.15 standard, which consists of two layers: physical (PHY) and media access control (MAC). The IEEE 802.15 standard provides some security protection for its data. In MAC sub layer, messages are ciphering before sending, and deciphering after receiving by AES algorithm in Counter mode (CTR)[11]. Data integrity is computed using Cipher Block Chaining – Message Authentication Code (CBC-MAC algorithm)[11]. The nonce is used to protect data against replay attack. The standard employs a combination of CTR mode and CBC-MAC algorithm,which is known as CCM* mode. The standard provides different choices of security, by optionally run either one of the algorithms (AES-CBC-MAC with different key length (32, 64, and 128) and (AES-CTR) as such inTable 1).

Table 1.IEEE802.15 security options

Security Option	Algorithms
No	None
MIC-32	CBC-MAC: key 32-bit
MIC-64	CBC-MAC: key 64-bit
MIC-128	CBC-MAC: key 128-bit
CTR	AES-CTR
AES-CCM-32	AES-CTR and CBC-MAC: key 32-bit
AES-CCM-64	AES-CTR and CBC-MAC: key 64-bit
AES-CCM-128	AES-CTR and CBC-MAC: key 128-bit

4. AES Algorithm

Rijndael[12]is a symmetric cryptosystem that announced by NIST as advance encryption standard. AES employs a single secret key with length 128, 192, and 256-bit. The block size is set to 128-bit for all different key length. AES is ciphering a message by performing sequence of transformations on the blocks of message. Also key is rounding in another sequence of transformation which number of times is specified by the key length. The key rounds are 10, 12 and 14 for 128, 192 and 256-bit key length respectively. AES is deciphering a ciphered message by applying a sequence of transformations that inversing the ciphering operation to get the original message.

4.1.AES Ciphering

AES Block ciphering is run a sequence of functions that will change the shape of blocks. The sequence of transformations is repeated on each block many times influence on the key length. The ciphering transformations include the following tasks:

- SubBytes: In this transformation, each byte is replaced with another byte from substitution table which is called S-box as illustrated inFigure 2(a).
- ShiftRows: The transformation performs a cyclically shifting for the last three rows of input block over different number of bytes (offset) as shown in Figure 2(b).
- MixedColumns: This transformation considers each column to be multiply by a specified matrix to produce new column this can be seen inFigure 2(c)Figure
- AddRoundKey: Each column of input block is XOR with one column of the state key to produce new block as seen in Figure 2(d).

4.2. AES Key Expansion

The secret key is expanded to schedule for each round. The key is treated as 4-byte words. The expansion transformations are following:

- Sub Word: This transformation uses the S-box to substitute each byte with new one.
- Rot Word: The transformation applies a cyclic permutation on input key.
- Rcon[i]: The round constant word array is XOR with key to produce a new schedule key.

4.3. AES Deciphering

In deciphering operation all the transformations in the ciphering operation are inversed to produce the original message.

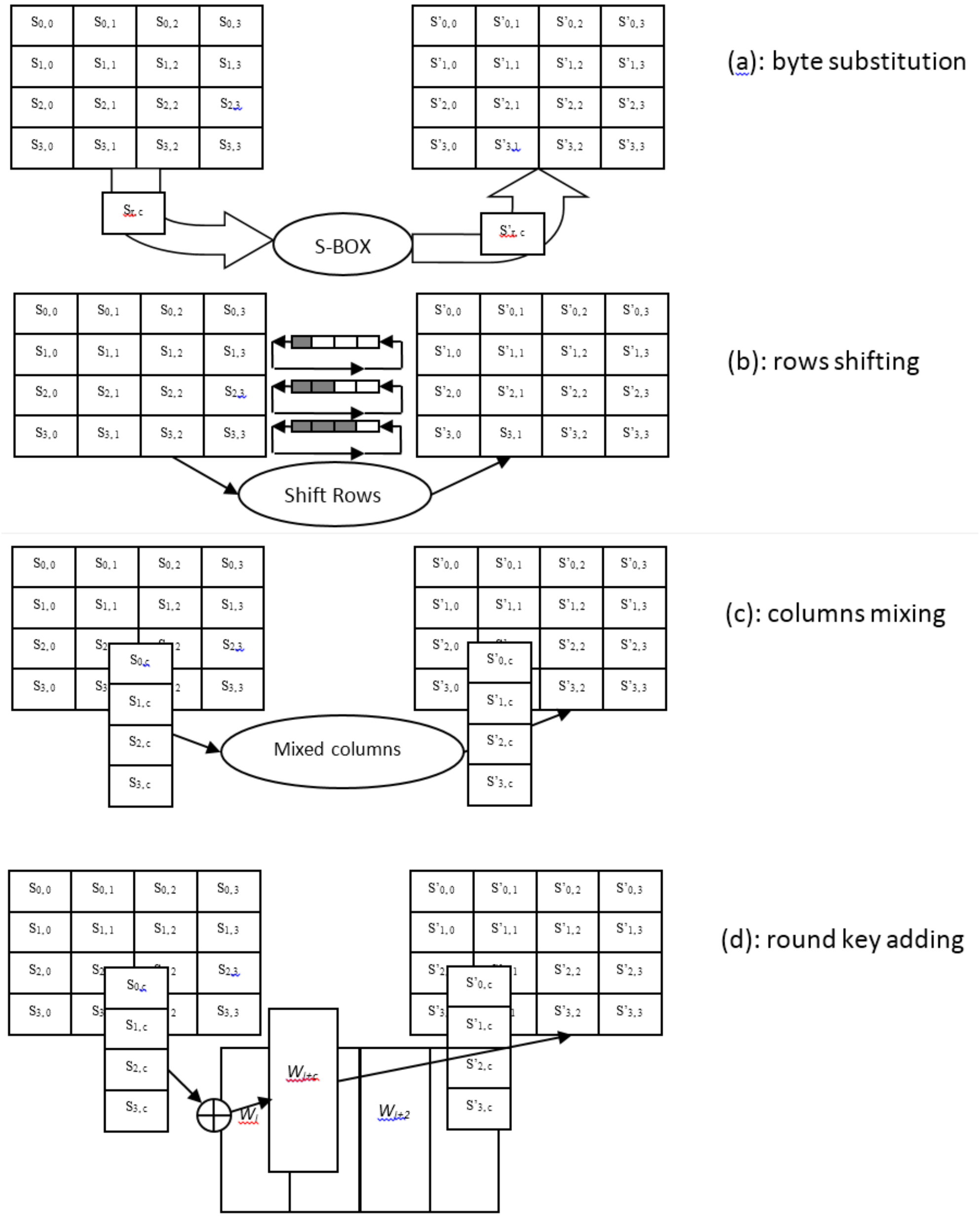


Figure 2:AES Ciphertransformation

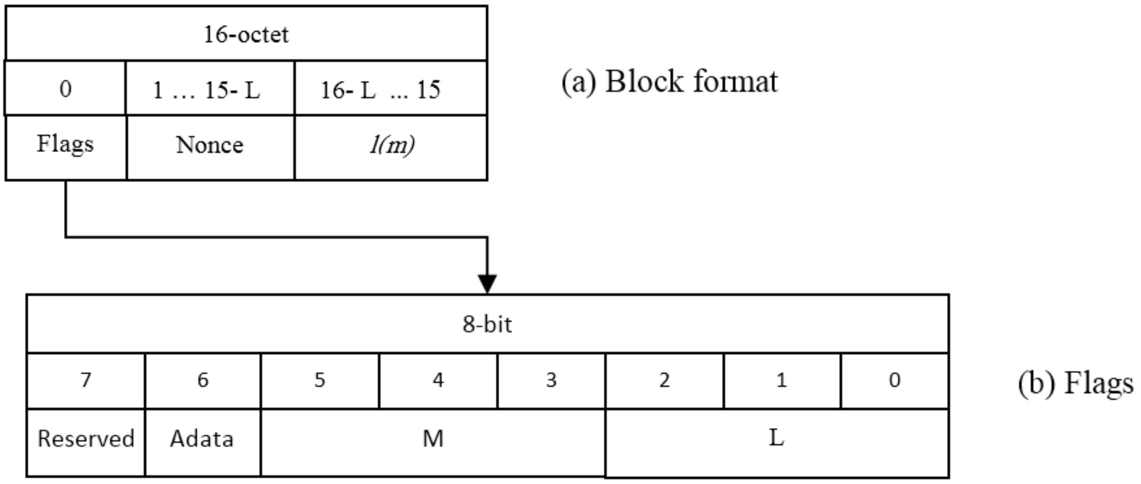
5. AES-CCM Mode

WBAN uses CCM* mode which is composed of AES-CTR and AES-CBC-MAC to provide message confidentiality and integrity.

Two parameters (L and M) are important to run CCM mode in WBAN. They are coded as (L-1) and ((M-2)/2) respectively, where each one is stored as 3-bit. M (refers to the size of tag in byte unit) and L (refers to the number of bytes that needed to represent the size of message) where $M \in \{4, 6, 8, 10, 12, 14, 16\}$ and $L \in \{2, 3, 4, 5, 6, 7, 8\}$.

The length of: message, nonce and the tag are computed by (L and M) parameters. The message size (*l (m)*) is less than 2^{8*L}bytes, the nonce length is equal to (15-L) bytes, and the tag length is equal to (8*M) bits. The size of additional authentication data (*l (a)*) is less than 2^{64} bytes and it is independent of Mand Lparameters.

To perform data authentication a sequence of blocks B_0, B_1, B_2 ... $B_n$should be produced which is the input to AES-CBC-MAC algorithm. The first block (B_0) is structured as shown inFigure 3(a). The first octet assigned for the flags, then (15- L) octets for nonce, then (L) octets assign to store the message length (*l (m)*). The flags octet includes (L) and (M) parameters in the first 6 bits (each parameter coded in 3-bit), then one bit is set to one when additional authentication data is enabled as shown in Figure 3(b). The last bit is reserved for future use which is set to zero. The message is breaking to sequence of 128-bit blocks (B_1, B_2 ... B_n).



16-octet		
0	1 … 15- L	16- L ... 15
Flags	Nonce	*l(m)*

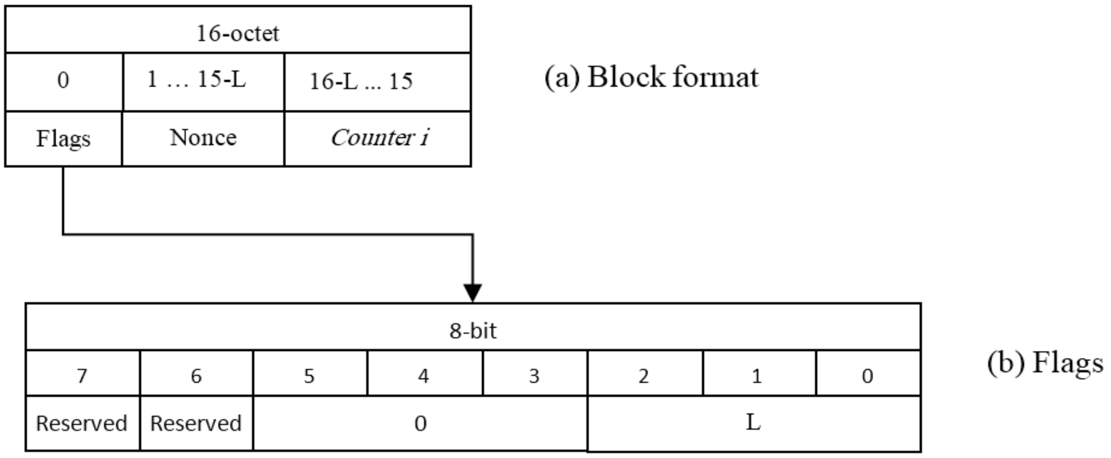
(a) Block format

8-bit							
7	6	5	4	3	2	1	0
Reserved	Adata	M			L		

(b) Flags

Figure3: Block (B_0) and flags format

Also, before starting AES-CTR algorithm, a sequence of blocks (A_0, A_1 ...) is generated, where each block is formatted as shown in Figure 4. In the flag octet, first 3-bit assigned for L. The next 3-bit in addition to two reserved bits are set to zero. The (A_i) blocks are distinct from (B_i) blocks because the value of 3-bit assigned to M will have none zero value in (B_i) blocks, but the same bits are set to zero in (A_i) blocks. For the octets from 16-Lto 15 are assigned to counter and from 1 to 15-L are assigned to nonce.



16-octet		
0	1 … 15-L	16-L ... 15
Flags	Nonce	*Counter i*

(a) Block format

8-bit							
7	6	5	4	3	2	1	0
Reserved	Reserved	0			L		

(b) Flags

Figure 4: Block (Ai) and flags format

The CCM mode is implemented by running CTR and CBC-MAC together as shown in Figure5Figure 5. The block (*B_0*) is encrypted (E) by AES and key (K) to compute (X_1). The authentication code is computed as: where i = 1 to nas shown in Figure 5a. The ciphertext is produced by XOR plaintext blocks with a sequence of blocks (*S_1, S_2 ...)*, which are computed as: S_i= E_K (A_i), where i = 0...∞as shown in Figure5. The block (A_0) is not used to cipher plaintext, but it is XOR with (X_{n+1}) to compute message authentication code.

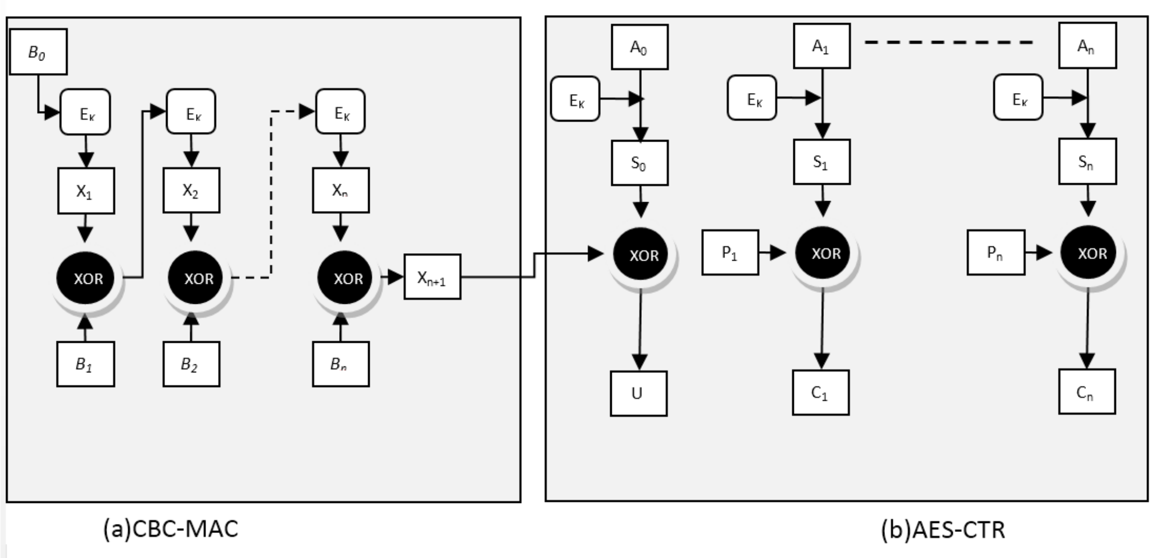


Figure5: Message encryption and authentication by AES-CCM

6. . Multiple Key Protocol

The MKP protocol provides multiple secret keys for the BAN to improve the network security. It adopts the ECC system to generate the secret keys. As illustrated in Figure 6, two lists (A, B) are generated. First list (A1 … An) is generated from initial value (A0) according to the EQUATION 1, and the second list (B1 … Bn) is generated from initial value (B0) according to the EQUATION 2. The secret keys (K1 … Kn) is computed from the two lists (A, B) as pointed in EQUATION 3.

$A_i = ECC\ (A_{i-1}),\ i> 0$ Equation 1

$B_i = ECC\ (B_{i-1}),\ i> 0$ Equation 2

where

ECC: Elliptic Curve Encryption

A, B: first and second list respectively

$K_i = A_{n-i+1}\ Xor\ B_i,\ i> 0$ Equation 3

where

K: secret key

A, B: first and second list respectively

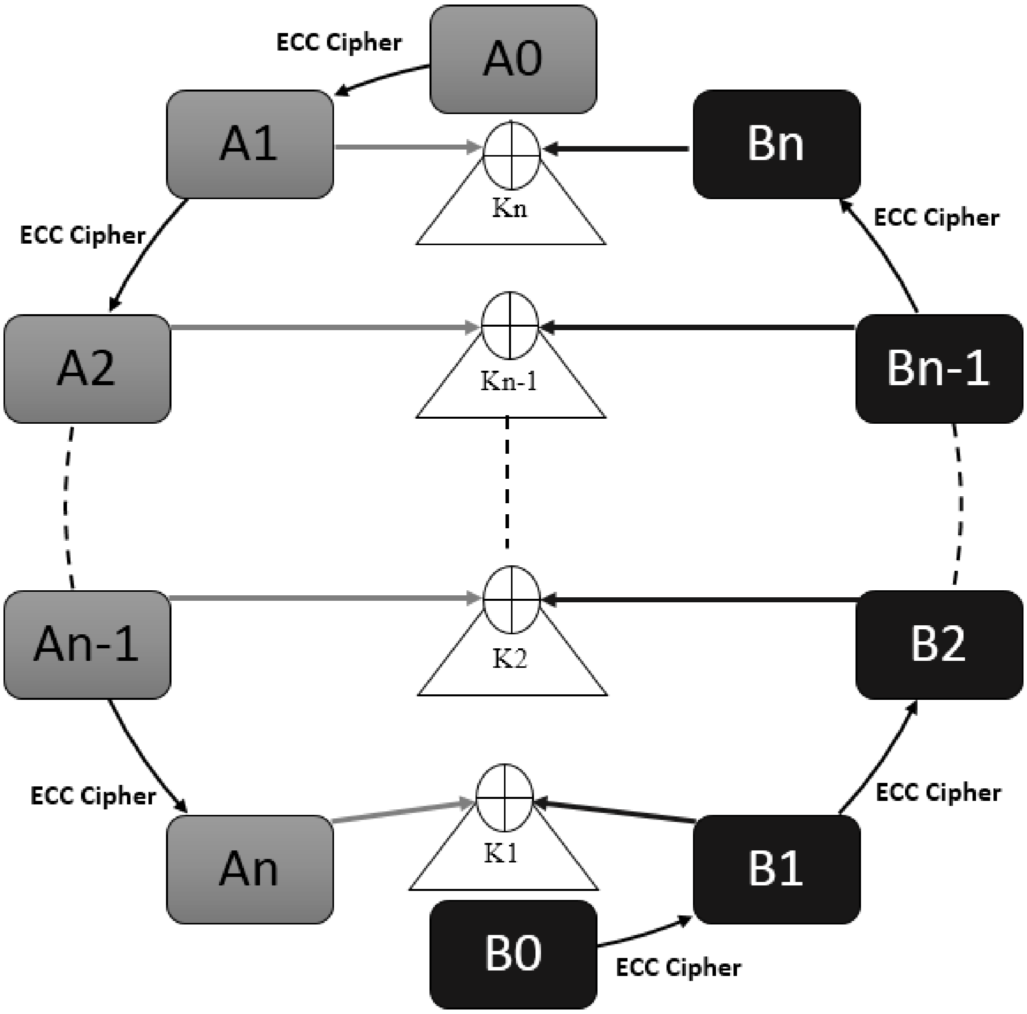


Figure 6: Multiple Secret Key Generation Protocol

7. Analysis of MKP-AES

MKP employs ECC to generate multiple keys to be used for ciphertext production. AES uses one secret key to cipher the plaintext message; however MKP uses (n) keys to do that. Moreover, the message is broken into (n) sub messages, where one key (K_i) is assigned to each sub message. The security level of the connection is computed by the number of generated keys.

The secret key strength and cryptosystem system complexity is very important because it refers to security system robustness. Brute force attack is trying to break the secret key by estimating the key based on its length. Secret key strength is limited to its length. The time complexity of secret key is computed by its length as notated in Equation 4, where (*len*) is the length of the key.

Time complexity = $O\ (log_2\ (len/2))$………….. Equation 4

len : number of bytes to represent the key

For BAN network, 128-bit secret key is assigned for AES. The 128-bit key length time complexity is computed as O ($log_2 64$), which is less secure than required. However, MKP provides (n) keys that mean the time complexity for key would be increased by (n) times as referred in Equation 5.

MKP Time complexity = O (n $log_2 64$)……….. Equation 5

n: number of secret keys

In addition to confidentiality and authenticity, BAN has a protection against a replay attack. Nonce is used to distinguish among messages. The strength of nonce belongs to its length. The attacker should try 2^S times(Sis the length of nonce) to break the nonce. The length of nonce (S) in WBAN is computed by the counter length (L) (see Equation 6).

$S = 15 - L$ …………….. Equation 6

S: number of bytes to represent the nonce
L: parameter

The MKP provide a single nonce for all sub messages. The length of nonce is computed by security level (n) (number of secret key) and message size (m). The message is divided into (n) groups of sub messages; each sub message has (B) blocks as quoted inEquation 7. The number of bytes for counter representation (L) is computed by number of blocks per group (B)as referred in Equation 8.

$B = m/n$ (where m>n) ………….. Equation 7
$L = (\log_2 B)/8$ ………. Equation 8

B: number of blocks per each group
m: message size (number of blocks)
n: number of group (number of secret keys)
L: parameter

From Equation 6, 7 and 8, it founded that MKP trades the length of nonce (S) to the message size and security level (number of secret key). The message size (m), which is measured by number of blocks, should be greater than the level of security (n).

The perfect state is when the value of (L) is equaled to 1, where the maximum nonce length (S) is 14. By substitution in Equation 7 and 8, it found that the maximum nonce length when the number of blocks per group (B) is 256.

8. Result

In this paper, nine different security levels ($n=2^i$, i=0 to 8) have been proposed, where the level of security refers to the number of secret keys and number of groups at that level, and 24 messages which have different size ($m=2^j$ blocks, j=9 to 32 and block size is 16-byte), to compute the nonce length. In each level the number of secret keys equivalents to the level of security as shown in Figure 7.

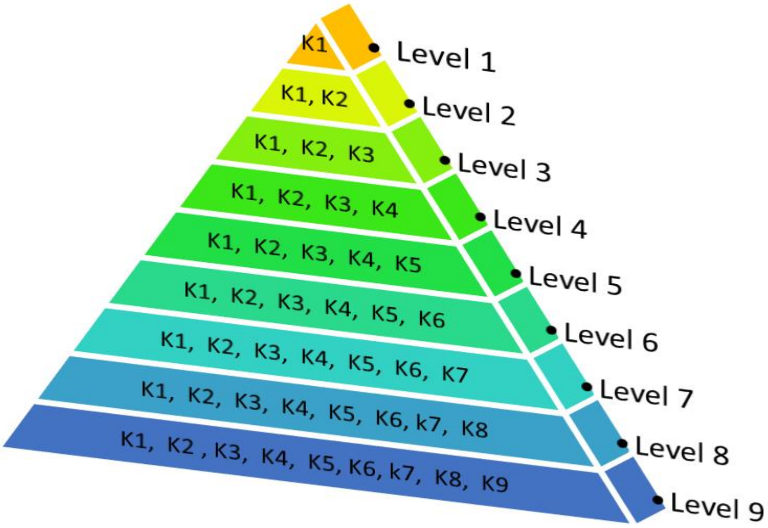


Figure7 : Secret Keys for nine levels of security

According to Equation 8, the parameter (L) is computed based on the number of blocks per group (B). The number of secret key influences the value of parameter (L). The increasing of the number of secret keys leads to decrease the value of parameter (L) as illustrated in Figure 8.

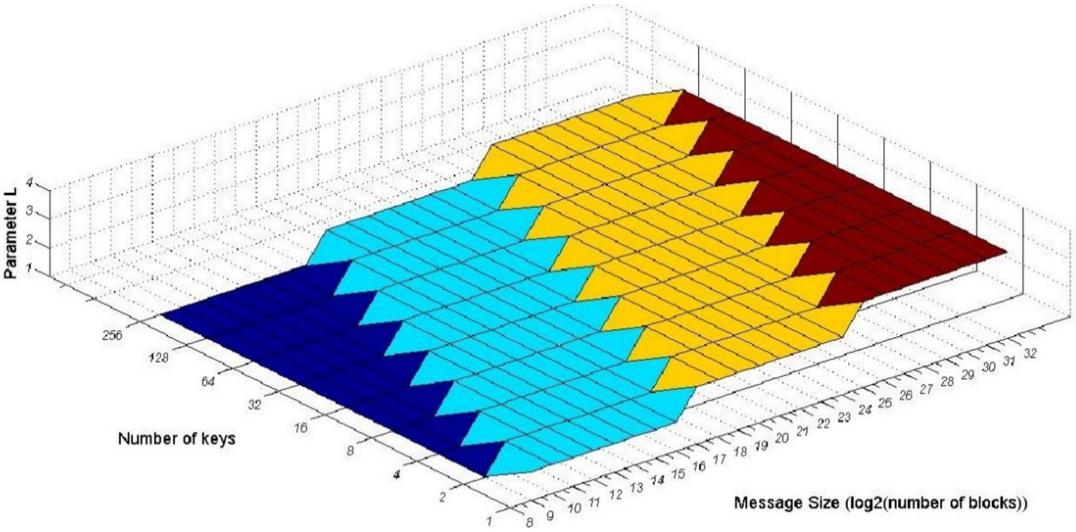


Figure8:Impact number of Secret keys on Parameter (L)

The first level of security is considered as the original state with one group of blocks.

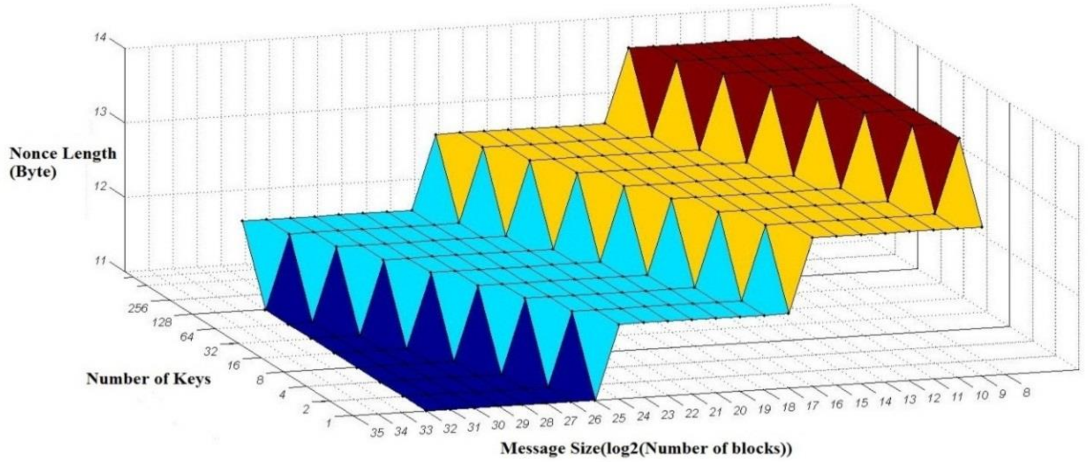


Figure:9:shows the messages with size from 2^9 to 2^{16} had maximized their nonce length with number of secret keys (2^i (i=1 to 8)) respectively.

The nonce length for messages with size from 2^{17} to 2^{24} blocks, had increased to become 13-byte, after grouping their blocks to (2^i (i=1 to 8) groups)) respectively. The messages with the size from 2^{25} to 2^{32} blocks had increased their nonce length from 11to12 bytes.

The computed result shows that for number of secret key(n), the list of messages (G_1, G_2 ...) get nonce length incremental, where the size of each message (m) is computed in Equation 9.

$log_2(m) = 8 + log_2(n) + 8*j$ Equation 9

Where: j =0, 1 … and n=2, 4, 8, 16 …

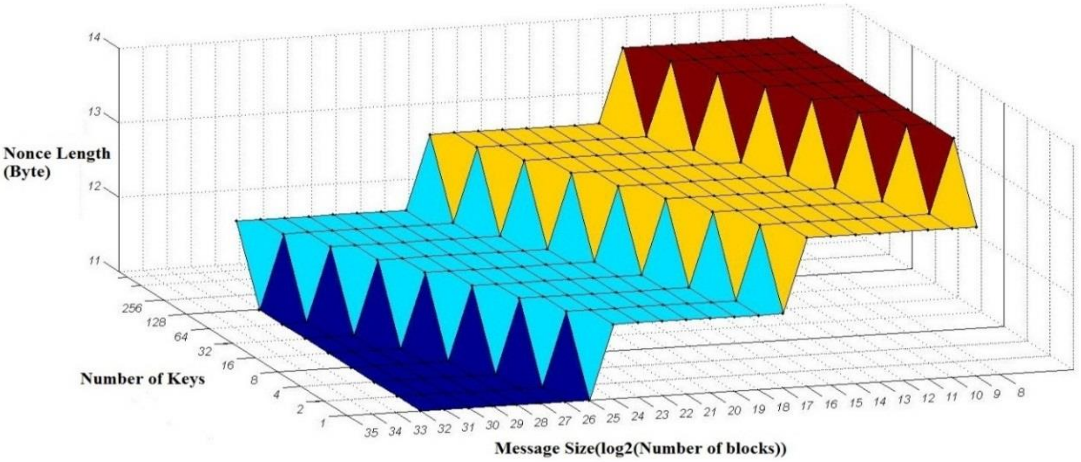


Figure9: Nonce length incremental over different number of secret key

9. Conclusion

The analysis of MKP in this paper proved that the MKP increases the security strength of theWBANwhen using higher level of security (number of secret key). When the level of security is increased then the time complexity will be higher as computed to the previous level because the number of secret keys equals to the level of security. Also, the nonce length increases during higher level of security, where the sub messages have less size than original message that gives more byte for nonce in block fragment.

10. References

[1] Filipe, L., Fdez-Riverola, F., Costa, N., & Pereira, A. (2015). Wireless Body Area Networks for Healthcare Applications: Protocol Stack Review. International Journal of Distributed Sensor Networks, 501, 213705.

[2] Khan, J. Y., &Yuce, M. R. (2010). Wireless body area network (WBAN) for medical applications. New Developments in Biomedical Engineering. INTECH.

[3] Qadri, S. F., Awan, S. A., Amjad, M., Anwar, M., &Shehzad, S. (2013). APPLICATIONS, CHALLENGES, SECURITY OF WIRELESS BODY AREA NETWORKS (WBANS) AND FUNCTIONALITY OF IEEE 802.15. 4/ZIGBEE.

[4] Man, L.A.N., Committee, S., Computer, I.: IEEE Standard for Information technology-Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements--Part 15.4: Wireless MAC and PHY Specifications for Low-Rate WPANs, http://profsite.um.ac.ir/~hyaghmae/ACN/WSNMAC1.pdf.

[5] Hamalainen, M., Paso, T., Mucchi, L., Girod-Genet, M., Farserotu, J., Tanaka, H. & Ismail, L. N. (2015, March).ETSI TC SmartBAN: Overview of the wireless body area network standard. In Medical Information and Communication Technology (ISMICT), 2015 9th International Symposium on(pp.1-5). IEEE.

[6] FIPS, N.: 197: Announcing the advanced encryption standard (AES). Information Technology Laboratory, National Institute of Standards and Technology, Nov. (2001).

[7] Dworkin, M.: NIST Special Publication 800-38B, (2004).

[8] Bernstein, D.J.: Understanding brute force. (2005).

[9] Al-alak, S., Ahmed, Z., Abdullah, A., Subramiam, S.: AES and ECC Mixed for ZigBee Wireless Sensor Security. International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering Vol:5, No:9, 2011

[10] Housley, R., Drive, S.K., Whiting, D., Ferguson, N.: Submission to NIST : Counter with CBC-MAC (CCM) AES Mode of Operation Submitter : Authors :,
http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ccm/ccm.pdf.

[11] Rogaway, P.: Evaluation of Some Blockcipher Modes of Operation. (2011).

[12] Daemen, J., Rijmen, V.: AES Proposal : Rijndael,
http://ftp.csci.csusb.edu/ykarant/courses/w2005/csci531/papers/Rijndael.pdf.

[13] S. Al-Alak, Z. Zukarnain, A. Abdullah, and S. Subramiam, "Randomness improvement of AES using MKP," Research Journal of Information Technology, vol. 5, pp. 24-34, 2013.