Lightweight and Low-Energy Encryption Scheme for Voice over Wireless Devices

Firas Hazzaa, *Member, IEEE,* Sufian Yousef, Erika Sanchez, Marcian Cirstea, *Senior Member, IEEE*
Faculty of Science and Technology, Anglia Ruskin University, Cambridge, UK
firas.hazzaa@pgr.anglia.ac.uk

***Abstract*—In this work, a novel lightweight and low energy encryption algorithm for voice over wireless networks is being developed and tested. The new encryption algorithm has to meet the QoS requirements of voice traffic and to be suitable for wireless devices. The goal of the research was to reduce the execution time and power consumption of the encryption process compared with the standard algorithm and at the same time at least to maintain or to increase its security level. The proposed algorithm employs similar methods with those used in the Advanced Encryption Standard algorithm (AES), with some changes and enhancements considering the limitations of wireless devices. The test results show significant improvements in new design metrics. A range of simulation scenarios are setup; testing data is analyzed to test delay, energy and security. Also, the comparison between the new algorithm and the standard one shows a significant amount of time and energy consumption reduction being achieved (approximately 35%), with good-level of complexity, making it more suitable for the wireless environment.**

Keywords—wireless devices; secure communication; voice encryption; AES encryption; wireless network security

I. Introduction

Wireless network is a set of wireless nodes that connect with wireless links and are not connected by cables of any kind. The use of a wireless network enables enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations.

In recent years, wireless platforms became a popular topic of research. Particularly, wireless networks have received serious attention because they present many advantages such as, convenience (when the wireless nature of such networks allows users to access network resources from nearly any convenient location within their primary networking environment), as well as mobility, productivity, deployment, expandability and cost. Also, voice over wireless networks and more generally multimedia applications are very relevant and play an important role in enabling people to communicate with convenience.

However, the security of the connections between devices and networks is crucial. According to Steve Morgan [1], the cost of cyber security reached $84 bn in 2015 and it is expected to reach $125 bn in 2020. The important challenges for supporting real time applications in the wireless networks are the security issues. Unfortunately, conventional multimedia traffic management algorithms, developed mainly to guarantee delay and distortion constraints while usually neglecting security requirements, make them much more susceptible to attacks like eavesdropping, data tampering and so on. On the other hand, internal constraints in wireless devices, like limited computational and power capabilities, make the implementation of current security and cryptography algorithms very difficult. Encryption algorithms consume a significant amount of computing resources such as CPU time and battery power in mobile devices [2]. Furthermore, voice over wireless channels is critical, because it is a real time transmission and thus more sensitive to delay.

One of the principles of security is confidentiality, which can be achieved by encryption. Encryption algorithms have been used in many applications and protocols. They have been used to encrypt data transferred into the network and could be used to encrypt the IP address as well. The routing information and request-response packets between wireless nodes could also be encrypted. These features have made the encryption very important in security.

Many previous research works have been conducted to address security issues related to real time traffic. They were able to develop some algorithms to deal with real time limitation issues such as delays. [3] proposed a new encryption / decryption algorithm based on AES scheme. They suggest some modification on two AES functions, to increase the security of the encryption strength and keep the execution time at the same level to maintain the QoS of real time traffic. In [16], a Symmetric Dual key Dynamic block algorithm (SDD) for digital video in the partial encryption technology has been proposed. This algorithm meets the requirements of real time with high level of complexity at a considerable speed. Moreover, [15] suggests a 5 rounds AES encryption algorithm for multimedia and real time applications in wireless sensor network. The results showed a reduction of the execution time.

Unfortunately, all of these research results are not suitable for application with wireless networks because of the sensitive requirements these have, such as: delays, throughput and power consumption in network nodes (power limitation). The fact is that there is always a tradeoff between the QoS and the security level in encryption and network security, meaning that high security requires more processing time and consumes more energy and vice versa; these aspects have not been addressed efficiently in most network security environments.

In this paper, the development of a new Encryption algorithm is presented. The work is based on the Advanced Encryption Standard (AES) algorithm. This then becomes lightweight and suitable for voice-over-WNet and helps to get a good tradeoff between security and QoS metrics by modifying some functions of the AES algorithm. Fig. 1 illustrates the AES algorithm which has ten rounds/iterations, each of them with four functions: Sub-Byte, Shift Row, Mix Column and Add Round Key.

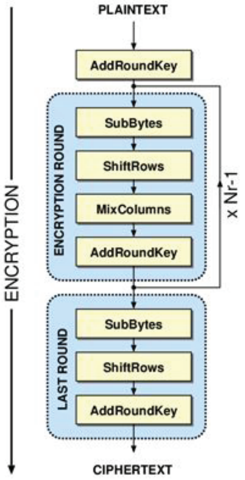


Fig.1 AES algorithm [16]

During the modification of these functions, the focus will be on the delay and power consumption metrics. The paper is organized as follows: the second part focuses on methodology, the third and fourth parts explains the proposed algorithms and their results and finally, the last section draws the conclusions.

II. METHODOLOGY

Usually in the network environment the encryption occurs in the nodes, so this paper focuses on the encryption process in the nodes and the effect it has in terms of delay and power consumption. To achieve the objectives of this research, a deep review of the published work has been done to select the most suitable encryption algorithm, and to determine the QoS parameters. The objectives were built upon claims by [15], [4] and [3], stating that AES is not suitable for real time applications and wireless nodes limitations. As we explained, the proposed algorithm uses similar functions with the ones used in AES but with some enhancements. The AES algorithm has four functions: Sub-byte, Shift row, Mix column and Add round key. Our solution proposes the modification of the Sub-byte and Mix column functions. Sub-byte function enhancement aims to increase the security and the complexity of the AES algorithm, keeping the execution time approximately the same, by modifying the SubByte Transformation in AES. The Mixcolumn enhancement, in addition to reducing the number of rounds in AES algorithm processes, aims to decrease the power consumption and execution time and to keep the security and complexity at the same level as the original AES. The testing has been conducted in a laboratory environment using a wireless laptop running Visual Studio 2015 using Console app to avoid any load on the processor. The proposed algorithm has been tested on an audio file with different sizes. After testing, the security and performance analysis has been conducted to measure the new algorithm's strength.

To validate and evaluate the new algorithm, a comparison with the standard AES algorithm has been carried out, to compare the security strength parameters such as the randomness and frequency histogram. Also, time and power consumption are compared. The algorithm's power consumption can be measured by calculating the total of computing cycles which are used in processes related to cryptographic tasks. For the calculation of the total energy cost of encryption, the techniques used are similar with those defined in [10], based on the following equations:

$$\boldsymbol{B}\ \mathit{cost\_encry}\ (\mathit{ampere\text{-}cycle}) = \tau * I \qquad (1)$$

$$\boldsymbol{T}\ \mathit{energy\_cost}\ (\mathit{ampere\text{-}seconds}) = \frac{\boldsymbol{B}\ \mathit{cost\_encry}\ (ampere-cycle)}{F\ (cycle/sec)}$$

$$\boldsymbol{E}\ \mathit{cost}\ (\mathit{Joule}) = T\ \mathit{energy\_cost}\ (\mathit{ampere\text{-}seconds}) * V \qquad (2)$$

Fig 2 illustrates the research design and shows the algorithm design steps.

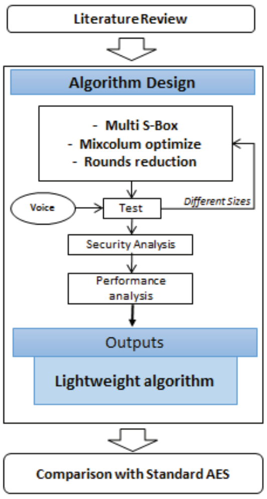


Fig.2 Research Design

III. PROPOSED ALGORITHM

A. Proposed New SubByte Transformation

The goal of the proposed method is to use multi S-box in the transformation process for SubByte function using dual keys, instead of a fixed structure for the S-Box used in the AES. The aim is to make the new algorithm lightweight and secure, so it is very important to increase the complexity level in SubByte layout, since the other AES functions will be modified to achieve the tradeoff between the security and the time and power consumption. Based on the claim in [5] that using single S-box remains vulnerable to cryptanalysis, the proposed SubByte function solves the problem of the fixed structure which will lead to the generation of more secure block ciphers. Each byte in the State matrix will be encrypted using different S-Box tables created by the first key, and this in turn increases the security of the AES block cipher system, because multi S-box function provides non-linearity and would be more difficult for the intruder to analyse the output using linear equation [5],[3]. A typical single S-box alone does not have much cryptographic strength. The key benefit of the proposed function is that a number of S-Boxes could be generated. The second key represents a random distribution of the S-Boxes created by the first key. This key will be in the form of a set of sequence S-Boxes tables arranged randomly, chosen by the two parties (sender and recipient). This operation leads to the increase of the degree of complexity within the same delay time during the encryption and decryption processes in the proposed SubByte function. Algorithms 1 and 2 are based on and demonstrate the aforementioned processes.

ALGORITHM 1

```
I/P: Randomly (8) values as { Rndm_Key[k], Cons_c[k] , k=1,2,………,8 }
O/P:   Diverse (8) S-Boxes { (S-box[m][n])k ; (S-1-box[m][n])k ; k=1,2,…..,8 }
1. Choice 8 keys Rndm_Key[k]    // to create a unique S- box when each key has the inverse to recreate Inverse S-box
2. Choice Eight different values Cons_c[k]
3. For each key Rndm_Key[k]  & relates constant Cons_c[k] generate its own S-box[m][n]
(S-box[m][n])k= Rndm_Key[k] * mulp[r][c] + Cons_c[k]
Where mulp[r][c] represent the multiplicative inverse in GF(28)
4. Use ( S-box[m][n])k in encryption operation.
```

ALGORITHM 2

```
I/p :plain text Block  { State[Row][Colum] :; r,c=1,2,3,4}
      8 S-Box{(S-box[m][n])k ; (S-1-box[m][n])k ;  k=1,2,…..,8 .
     matrix of Key sharing  {Key-Enc\Dec[4][4]}
O/p: cipher text Block {State[Row][Colum] ; r , c =1,2,3,4}
    using new S- box[m][n] to encrypt each block :
1. For Each Row in State matrix, Do
2. For Each Colum in State matrix, Do
3. Y = (Stat [Row][Colum])&0x0f;
    X = (Stat [Row][Colum]>>4)&0x0f;
     X, Y =  the index of row and colum  in S-Box
4.  State[Row][Colum]  encrypt by using the index of each
    S-Box ,; Key_Enc[4][4] : State[Row][Colum]=(S-box[x][y] )
```

Algorithm 2 will add much more complexity because each key (Rndm_key and Cons_c) needed for generating the S-boxes consist of 128 bits; this leads to a number of possible generated s-boxes potentially being:

$$complexity\ (key\ space) = 2^{128} * 2^{128} = 2^{256} \qquad (3)$$

In addition, there is a random distribution of the S-Boxes which adds more complexity. The use of another key leads to much more complexity as:

$$random\ distribution\ \ sbox = 8!$$

The total complexity (new key space) for this algorithm will therefore be of a high level, adding more security for this operation. This means that it is very difficult to find which S-box was used in the encryption, thus adding more resistance.

B. Modification of Mix Column Function

MixColumn function is the third function in the AES algorithm which accounts as the most computationally expensive operation, where the input matrix is multiplied Over *GF(28)*. The key matrix used in forward and inverse MixColumn transformation functions, that operate on State matrix, is single and with fixed dimension [4*4]. The proposed scheme tends to improve MixColumn transformation by splitting the key matrix into four parts, each part representing a different key with dimension [2*2]. The State matrix is also divided into four parts with [2*2] dimension, each part corresponding to one of the keys into a similar position in the key matrix.

In the product matrix and in each part, any element is the sum of the products of the elements of one row and one column. In this case, the individual additions and multiplications are executed in *GF(2)* and *GF(28)*. The transformation can be defined by the following matrix multiplication between the State and key matrices. The proposed algorithm to improve MixColumn transformation is shown in Fig.3. It is assumed that all four parts of the keys are fixed. The reason is to reduce the keys exchanging operation between the sender and receiver in the network which cost more load in the network. Especially in wireless sensor networks and mobile ad hoc networks, when the nodes enter and leave frequently, this causes a repetition of the rekeying operation between them.

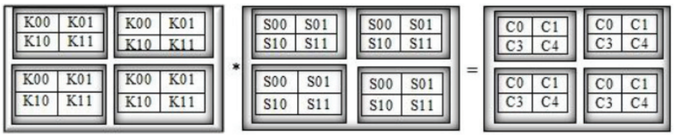


Fig.3. process of Multiplication in proposed MixColum function

Where:

$$C0 = (K00 * S00 + K01 * S10)\ mod\ (irred.polyn.)$$
$$C1 = (K00 * S01 + K01 * S11)\ mod\ (irred.polyn.)$$
$$C3 = (K10 * S00 + K11 * S10)\ mod\ (irred.polyn.)$$
$$C4 = (K10 * S01 + K11 * S11)\ mod\ (irred.polyn.)$$

This method will reduce the number of operations needed to multiply two matrices because it reduces the summation and multiplication process, consequently leading to the reduction of the time and energy consumption needed for this function, as shown in Algorithm 3.

ALGORITHM 3

```
I/p :plain text Block  { State[Row][Colum] :; r,c=1,2,3,4}. and The mix colum k- encryption Mix_Key[r][c], r,c = 1,……,4
O/p: Ciphertext text Block  C_Blok[r][c], r,c =1,…..,4 .
1: Divided plain Block[r][c] and Mix_Key[r][c] into 4 portions each one of size 2*2, for each portion of Mix_Key[2][2] calculate its inverse matrix.
2: Multiplication of each portion of P_Block[2][2]* Mix_Key[2][2] to produce C_Matrix[2][2].
3: Rebuild the C_Block[r][c] r,c=1,..,4, from each portion of C_matrix[2][2]
```

C. Proposed Nine-Rounds Iteration

The high complexity that has been achieved in section (A) for Sub-Byte transformation, allowed the reduction of the number of rounds in the AES algorithm, making it more suitable for MANET, which has nodes with power limitation. Therefore, in this section, the aim is to decrease the power consumption and execution time and keep the security and complexity at the same level.

Reducing the number of rounds in the new algorithm processes will decrease the power consumption and at the same time reduces the execution time and keeps the complexity the same because the complexity was already increased in the S-

Box stage as mentioned in section (A). As explained, [15] suggest five rounds AES, which is still critical in term of security. [4] confirmed that the last successful attack was on seven rounds. So, nine rounds are proposed for the iteration algorithm, to be more secure and resist differential attack. The mathematical model of the new encryption algorithm below illustrates the proposed model:

$$P = power \quad T = time$$
$$P(Enc) = \sum P(round)$$
$$T(Enc) = \sum T(round)$$
$$So, \text{ by reducing the number of rounds to } 9$$
$$New \text{ } algorithm \text{ } power = 0.9 * P \qquad (4)$$
$$New \text{ } algorithm \text{ } time = 0.9 * T$$

Implementing this new algorithm decreases the power consumption by up to 10% and reduces the execution time to 10% as well, while keeping the security at the same level, because the complexity of the algorithm has already been dealt with during the S-Box generation stage and not the round stage. The AES algorithm has traditionally implemented ten rounds, each round consisting of four functions. The proposed new algorithm is implementing 9 rounds to perform the encryption process. Algorithm 4 below illustrates the newly proposed AES algorithm.

ALGORITHM 4. PROPOSED AES

```
I/P: plaintext Block {State [Row][Col]Row, Col=1,2,3,4}.
With 1-16 S-boxes, generated in algorithm 1.
O/P: cipher text C {[Row][Colum]Row Colum=1,..,4}

    Encrypt using nine rounds
  for (i = 0; i<8; i++)
  SubBytes();   // subbytes transformation proposed in algorithm (2)
  ShiftRows();
   MixColumns();  // mixcol proposed in algorithm (3)
       AddRoundKey();
  Last round;
End.
```

D. New Overall Design Framwork

The new design has added new features to the functions of the algorithm, as stated in sections A, B and C, which make a reliable tradeoff between the security and QoS parameters.

The power and time consumption have been reduce,d as explained in sections B and C. and the security has been increased in A. The new overall key space of the new algorithm will be as follow:

$$Dual \text{ } Key: \quad 2^{128} * 2^{256} * 8! \qquad (5)$$

The attacker needs to know two keys at the same time and it is very difficult to guess all of them together; so, even if one key is hacked, it will be more complicated to find another. Also, theoretically, if the attacker uses the Brute-force attack to find all the keys, then a huge time will be needed for it to be successful, greater than $5.3*10^{23}$ years. Therefore, in this case the security level for this algorithm is maintained or increased.

As mentioned before, the new algorithm is more suitable for a wireless environment because of the new features. The following section provides more analysis linked back to these facts. Fig.4 demonstrates the proposed enhancement in the new algorithm. The modified functions, as shown in Fig.4, are: new SubByte and new MixColumn with nine rounds.

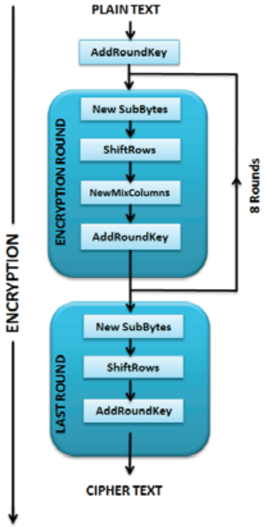


Fig.4. New Encryption algorithm (Author)

IV. RESULTS AND ANALYSIS

A. Test Results

The results show that significant improvements in the proposed algorithm were achieved. Table 1 shows the power consumed by the new algorithm for the encryption and decryption process.

Table 1. POWER CONSUMED BY NEW ALGORITHM

File Size	Encryption Power (μ J)	Decryption Power (μ J)
128 K	0.023	0.024
540 K	0.071	0.079
1.48 M	0.201	0.207

To evaluate, and after testing the standard AES, a comparison between the Standard AES and the new encryption algorithms is provided.

Table 2. ENCRYPTION POWER FOR AES AND NEW ALGORITHM

File Size	Standard AES (μ J)	New algorithm (μ J)
128 K	0.035	0.023
540 K	0.109	0.071
1.48 M	0.298	0.201

From Table 2, it can be seen that there is a clear reduction in power consumption for the new algorithm. The amount of reduction reaches nearly 35% for the new algorithm, compared with the standard AES. This proves that the proposed Mixcolumn enhancement and nine-round iteration have reduced the executing cost of the encryption operation.

Table 3 shows the comparison of features for both algorithms. It can be seen that there are many important differences between them. Also, it is clear that the file size is still the same, which will therefore not affect the memory size and the bandwidth of network paths.

Table 3. A COMPARISON BETWEEN THE TRADITIONAL AES AND THE NEW ALGORITHM

Property	**AES**	**New Algorithm**
S_box	Single	Multi
Num. of keys	1	2
Key space	2^{128}	$2^{128}*2^{256}*8!$
Block length	16 Bytes	same
No. Rounds	10	9
Encryption time	**T**	**0.65 T**
Power consumption	**P**	**0.65 P**
Output = input size	Yes	Yes

The new algorithm has a high level of security because the complexity of finding the keys is increased, after adding more keys. Each key has 2^{128} of complexity, as mentioned in Table 3, in addition to using eight S_Boxes which increased the complexity by 8!; this complexity was multiplied by the number of rounds, 10 rounds in the standard and 9 rounds in the new AES. Meanwhile, the execution time and power consumption have decreaded by 35% and this is because of reducing the rounds and new mixcolumn function. To prove the security strength, the next section evalutes in detail the security metrics of the proposed algotithm and compares them with those of the standard AES.

B. Security Analysis:

A security analysis has been conducted to test the security level of the new algorithm. Many security parameters have been measured, such as the randomness of the encrypted data like Entropy, Histogram and Floating frequency test. The poker test and frequency test are carried out as well. Cryptools 1.4 for cryptography and cryptanalysis [15] had been used to carry out these tests. All the tests have been conducted on an audio file format (.wav) of 540K size as a sample.

Table 4. ENTROPY ANALYSIS

Audio file size / Byte	before	AES algorithm			New algorithm		
	Entropy	Entropy	Max. possible Entorpy	Possible byte value	Entropy	Max. possible Entorpy	Possible byte value
540k	7.79	7.99	8	256	7.99	8	256

Table 4 shows the Entropy test result for the encrypted file in both the AES standard and the newly proposed algorithm. The new algorithm achieved a good performance compared to the standard algorithm, which was 7.99 of the maximum possible value of = 8. This means that there is a significant randomness in the newly proposed algorithm, keeping the diffusion in the cipher and leading to more complexity in the relationship between the cipher and the plaintext.

The figures below show the security analysis for the encrypted file for both the standard AES and the proposed algorithm. Fig. 5 represents the Binary Histogram of the orginal audio file (computer.wav) before the encryption

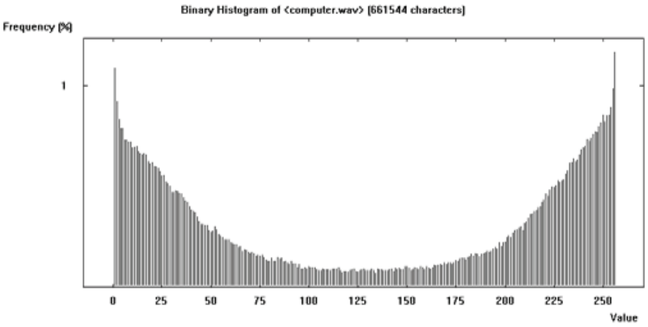


Fig.5. Binary Histogram of the audio file before encryption

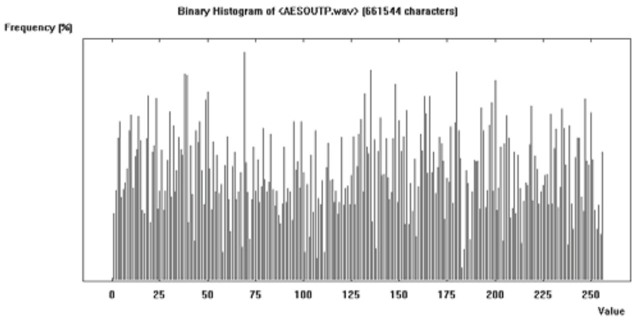
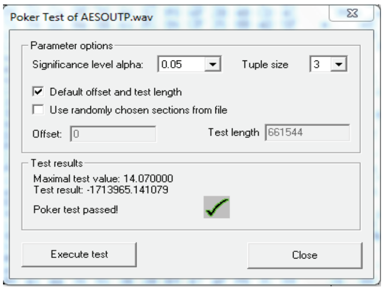


Fig.6. Binary Histogram of the audio file after encryption by new algorithm

Fig.6 illustrates the Binary Histogram of the encrypted file using the proposed algorithm. It is clear that there is a considerable difference between the orginal file and the output of the proposed algorithm, implying a strong security level.

All the figures above and the analysis carried out demonstrate that considerable security level has been achieved through the newly proposed encryption algorithm. In addition to the previous analysis, some tests have been carried out, such as frequency test and poker test, to test the randomness of the output audio file. These tests have been carried out on the encrypted audio file and both of these tests were passed, as shown in Fig 7.


Poker Test of AESOUTP.wav

Parameter options

Significance level alpha: 0.05 Tuple size 3

☑ Default offset and test length

□ Use randomly chosen sections from file

Offset: 0 Test length 661544

Test results

Maximal test value: 14.070000
Test result: -1713965.141079

Poker test passed! ✓

Fig.7. Poker test result

From all above analysis and tests, it is clear that the newly proposed algorithm has achieved a significant security level and it has a good resistance to different attacks such as brute-force, chosen cipher text and ciphertext only attack, because of the confusion and the diffusion characteristics it has. Also, the high randomness which apears in the above means that reducing one encryption round, (making it 9 rounds), did not affect the security level. Security level include: binary Histogram, Floating frequency and randomness. All these metrics have been measured and comparied with the standard AES, achieving the same strength.

Table 5. presents a comparison of our work with published works in this area. It contains the work reference, power saving percenatge and security level against the standard AES.

Table 5. COMPARISON

Work ref.	**Power saving (%)**	**Overall Security against AES**
[15]	40 %	low
[3]	0 %	high
Our research	35 %	Same/high

This means a significant tradeoff between security and QoS metrics has been achieved in the proposed algorithm, making it more suitable for wireless devices.

V. CONCLUSION

A new encryption algorithm for wireless networks has been developed in this research. The main objectives were achieved by reducing the execution time and power consumption and maintaining/increasing the security level, comparing with the standard algorithm (AES) and published work. Also, the security analysis proved the high complexity and randomness of the new algorithm which resists different types of known attacks. The new algorithm is very useful for wireless devices and it achieves a considerable tradeoff between security, time and power consumption, thus it is recommended for any wireless network where the resources are limited.

Further development of the algorithm can be performed in the future, such as increasing the SybeByte function complexity or involving or adding third key in the algorithm to increase the security level, depending on the resources and limitations of the network.

REFERENCES

[1] S. Morgan, "Cyber Security Cost," Forbes, available online on: https://www.forbes.com/sites/stevemorgan, US, 2017.

[2] P. Gope, T. Hwang, " A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application in WSN," *IEEE Transactions on Industrial Electronics, Industrial Electronics Society,* vol. 63, no. 11, pp. 7124-7132, 2016.

[3] N. Ali, A. Rahma, S. Yousef and M. Jaber, "Random Key Permutation Stream Algorithm Based on Modified Functions in AES Algorithm," International Journal of Engineering and Technology, vol. 4, no. 6, pp. 367 - 373, June 2014.

[4] B. Bahrak and M. R. Aref, "Impossible differential attack on seven-round AES-128," *IET Information Security, Institution of Engineering and Technology,* vol. 2, no. 2, pp. 28-32. [avalible online on]: https://ieeexplore.ieee.org/document/4558840/, July 2008.

[5] L. S. Abhiram, B. K. Sriroop and H. L. Punith.Kumar , "FPGA implementation of dual key based AES encryption with key Based S-Box generation," India, 2015.

[6] Liang and Han, "Multimedia Traffic Security Architecture for the Internet of Things," *IEEE Network,* pp. 35-40, 2011.

[7] A. Popov, "Prohibiting RC4 Cipher," Internet Engineering Task Force, WA, USA, 2015.

[8] D. Salama and M. Hadhoud, "Evaluating the effect of symmetric Algorithms on Power consumption for Different Data types," *International Journal of Network Security,* vol. 11, no. 2, pp. 78-87, 2010.

[9] J. Wang, Q. Gao, P. Cheng, Y. Yu, “Lightweight Robust Device-Free Localization in Wireless Networks," *IEEE Transactions on Industrial Electronics, IES,* vol. 61, no. 10, 2014.

[10] W. Jiehong and I. Detchenkov, "A Study on the Power Consumption of Using Cryptography Algorithms in Mobile Devices," China, 2016.

[11] P. Hamalainen, T. Alho and M. Hannikainen, "Design and Implementation of Low-area and Low-power AES Hardware core," Croatia, 2006.

[12] Ayyappadas, Devassy, S. George and A. Devassy, "Survey of Symmetric Cryptographic Algorithms," *Journal of Electronics and Communication Engineering (IOSR-JECE),* pp. 65-75, 2014.

[13] s. Cheng, P. Chen and C. Lin, "Traffic-Aware Patching for Cyber Security in Mobile IoT," *IEEE Communications Magazine,* vol. 55, no. 7, pp. 29 - 35, 2017.

[14] w. Hu and Cao, "Quality-Aware Traffic Offloading in Wireless Networks," *IEEE TRANSACTIONS ON MOBILE COMPUTING,* vol. 16, no. 11, March 2017.

[15] A. Msolli, A. Helali and H. Maaref, "Image encryption with the AES algorithm in wireless sensor network," Tunisia, July 2016.

[16] A. S. Rahma and B. Z. Yaco , "Real-Time Partial Encryption of Digital Video using Symmetric Dynamic Dual Keys Algorithm," *Engineering and Technology Journal,* vol. 30, no. 5, pp. 710-728, 2012.

[17] R. Chandramouli, S. Bapatla and K. P. Subbalakshmi, "Battery power-aware Encryption," *ACM Transactions in Information and System Security,* vol. 9, no. 2, pp. 162-180, 2006.

[18] R. D. Pietro, S. Guarino and Verde, "Security in wireless ad-hoc networks," *Elsevier- Computer Communications,* vol. 51, pp. 1-20 [available at ScienceDirect], 2014.

[19] Emmanouis and Christos, "Security model for emergency real-time communications in autonomous networks," *Springer- Information Systems Frontiers, A Journal of Research and Innovation,* vol. 14, no. 3,pp.541–553[online]:https://link.springer.com/article/10.1007/s10796-010-9259-8, 2012.

[20] D. He, C. Chen, S. Chan, J. Bu, “Security Analysis and Improvement of a Secure and Distributed Reprogramming Protocol for WSN," *IEEE Transactions on Industrial Electronics, Industrial Electronics Society,* vol. 60, no. 11, Sep. 2012.

[21] M. Nagendra and M. C. Sekhar, "Performance Improvement of Advanced Encryption Algorithm using Parallel Computing," *International Journal of Software Engineering and Its Applications,* vol. 8, no. 2, pp. 287-296. [availble online]: https://pdfs.semanticscholar.org/. 2014.