ISSN No:-2456-2165

AMPC: A Lightweight Hybrid Cryptographic Algorithm for Wireless Sensor Networks

Md. Navid Bin Anwar
Department of Computer Science &Engineering
American International University - Bangladesh
Dhaka, Bangladesh

Maherin Mizan Maha
Department of Computer Science &Engineering
American International University - Bangladesh
Dhaka, Bangladesh

Abstract:- Wireless sensor network (WSN) is a group of several autonomous sensor nodes attached to each other. Wireless sensor networks are commonly used in a lot of applications and are expected to have a cheap deployment cost. The network of sensors continues to grow aiding the need of the system. Due to that, sensors become vulnerable to attacks and need strong security mechanism. To strengthen the security of data which are transmitted through sensors in WSN, different cryptographic schemes are used. As WSN has limited energy source, therefore, complex cryptographic algorithms may require excessive computational time which not only make the data transmission slow but the life time of sensor network will be significantly affected. To overcome these challenges a new hybrid cryptographic scheme, AES and Modified Playfair Cipher (AMPC), is introduced in this paper.

Keywords:- AES, hybrid cryptography, playfair cipher, sensor, modified playfair cipher, AMPC, Diffie-Hellman, wireless sensor network.

I. INTRODUCTION

A WSN includes a dense number of sensor nodes, where the nodes are installed according to the topologies to cover the sensing areas. The nodes sense the environment and collect data then it forward to a central node or sink node. As the nodes are continuously passing data among each other, there comes a security issue of data integrity. The security also becomes compromised due to dense sensor population and hard to access the locations of the sensors. A security breach in a dense network is hard to point out as it is complex to identify the compromised node. Same goes for maintainability, a broken or backdated node can easily be attacked due to its untraditional placement. To remedy the problem a strong data encryption scheme should be implemented to mitigate the security breach.

An encryption algorithm or scheme is a vessel for providing security to electronic data transport. Mathematical measures are taken to form algorithms which prevent data fraud. The main goal is to alter the actual data in such way that it cannot be revived without a key. The altered data is then sent to receiver end along with the key so that the receiver can revive the actual data. The actual data is referred as plaint text and the altered data is called cipher text. The general method can be divided in two ways – stream cipher and block cipher. A stream cipher encrypts data bit by bit however, a block cipher is an encryption technique that encrypts a block of text, rather than encoding one bit at some random minute as in stream figures. Various cryptographic schemes exist at present. For WSN, hybrid cryptography measures are preferred at present as it increases complexity of the encryption algorithm [1]. While cryptographic schemes secure data which can decrypted with a key, secure transmission of the key is also crucial. At present popular secure key exchange algorithms are Rivest Shamir Adleman (RSA), Elliptic Curve Cryptography (ECC) and Diffie Hellman [2].

Hybrid cryptography is merging of different cryptographic schemes [3]. The new altered scheme provides better security. The altered scheme produces a cipher text which is complex than usual to break increasing data security.

The proposes hybrid cryptographic scheme, AMPC, consisting of AES (Block Cipher) cryptographic scheme and Playfair (Stream Cipher) cryptographic scheme for data encryption, according to the finding, no previous work has been done on which merges the mentioned algorithm as hybrid. The proposed scheme also used Diffie-Hellman key exchange scheme to secure the key exchange process. The remaining parts of the paper are arranged as follow, section 2, presented literature review. Section 3 provides a short overview of cryptoghraphic techniques. A brief of proposed scheme is presented in section 4. The result of the work has been represented in section 5 and conclusion in given in section 6.

ISSN No:-2456-2165

II. RELATED WORKS

A. Faquih, P. Kadam, and Z. Saquib have examined parcels proposed security instruments for wireless sensor network [4]. Different cryptography procedures are talked about, for example, symmetric key and open key, which further contains different cryptographic methods. The author found that symmetric cryptography is definitely not an ideal answer for take care of this issue so open key is utilized as the arrangement. Open key it's seen that ECC is a product base stage for run of the mill WSN yet it is unpredictable. In this way, the new cryptography like matching and (Identity Based Cryptography) IBC are considered for giving ideal answer for open key. Despite the fact that it gives security however it is all the more way complex. They have concluded that Hybrid cryptography innovation is an answer for security in WSN.

Ali Abdulridha Taha, Dr. Diaa Salama AbdElminaam, Prof.Dr. Khalid M Hosny [5] proposed hybrid cryptography algorithm, which was developed to secure the data and information. The data is transmitted through the cloud. They worked with several cryptographic schemes like Triple DES, Blowfish and a modified Hill cipher proposed by Krishna, A. V. N., and Babu A. Vinaya [6]. They experimented with a variety of hybrid cryptographic scheme with the above mentioned three and measured their overall performance.

Rawya Rizk and Yasmin Alkady [7] proposed two phased hybrid cryptography algorithm by integrating AES and ECC algorithm. The authors compared the performance of their algorithms against some previous customized cryptographic schemes. Their scheme achieved lower energy consumption.

Er. Parvin Shaikh and Dr. SonaliPatil [8] proposed a hybrid cryptographic scheme with chaffing and winnowing algorithm and AES. They mainly tested their schemes efficiency by measuring encryption and decryption time for different sets of users. Their test started from 50 users to 600 users. Their results showed a performance hype of their proposed scheme over AES alone.

III. CRYPTOGRAPHIC ALGORITHMS

As previously mentioned, the art of providing security through customized algorithms can be identified as cryptography. While different cryptographic techniques provide security through a variety of techniques, they can be grouped into several types as shown in the diagram of Figure 1.

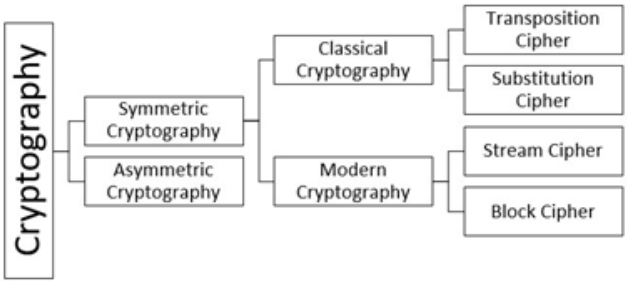

Fig 1:- Types of Cryptography

This paper shows work with AES algorithm which is a block cipher and playfair cipher, which is a stream cipher. A stream cipher encrypts data bit by bit however, a block cipher is an encryption technique that encrypts a block of text. The modified method then uses Diffie Hellman key exchange protocol for a secure exchange of keys.

A. AES Cryptographic Algorithm

AES algorithm is a block Cipher; it is a symmetric cipher also. It was a chosen algorithm by U.S government to protect their classified information [9]. The algorithm can work with data and key size of 128, 192, and 256 bits. Data length is divided into four blocks. The blocks are then integrated into an array. The data is passed through n rounds (n = 10, 12, 14). The rounds administrate some transformations namely, Bytesub transformation, Shiftrows transformation, Mixcolumns transformation, Addroundkey transformation. The process is shown visually in Figure 2. And the last round skips Mixcolumns transformation step.

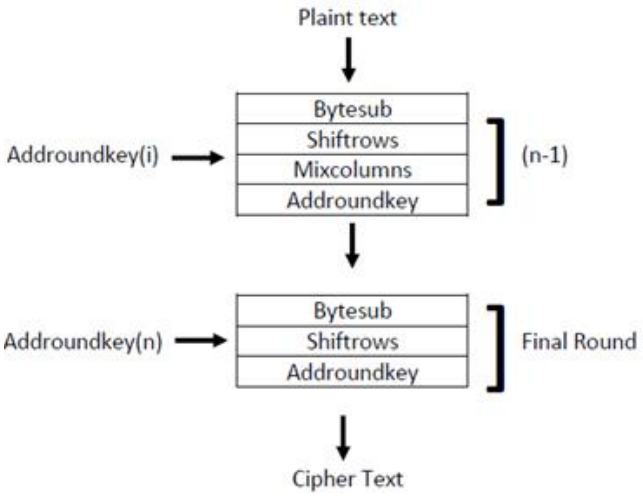

Fig 2:- AES algorithm- Encryption Structure

B. Playfair Cipher

Playfair cipher is a digraph stream cipher, which encrypts a text two character at a time [10]. In doing so, a 5 by 5 key matrix is designed at first. The double characters in the key gets omitted then is entered in the matrix. The remaining characters of alphabet then are entered in the matrix. Then the encryption is done through three rules.

ISSN No:-2456-2165

For the ease of this hybrid algorithm, the traditional playfir cipher was modified. The modified playfair cipher uses a 6 by 6 matrix instead of 5 by 5 matrix. This enables the encryptions of 24 English alphabets and also 10 numbers. An example of generated matrix with modified Playfair Cipher having keyword is "Puzzle" has been given in figure #. As it can be seen, the matrix has accommodated numbers. As 36 characters has been used, letter 'J' wasn't omitted. The sole purpose of this modification was to include encryption of numbers with playfair cipher as in most wireless sensor networks numeric data is needed transport. Plain text as "35 degree Celsius" or a long binary string can be converted using this modified playfair cipher. For that, the binary string would need to be converted to hexadecimal form

C. Deffie Hellman

Diffie-Hellman key exchange, exponential key exchange is a digital encryption algorithm. It raises numbers to a certain power to develop decryption key, which should never be directly transmitted. The idea is to make breaking and revealing the actual key mathematically hard [11].

Let's assume two end users, User A and User B. While communicating over a private channel to them, they mutually agree on a positive whole numbers. Let the numbers be p and q. Here, p is a prime number and q is a generator of p. q is a number which is raised to positive whole-number powers (Less than p). This operation never produces the same result for any other set of numbers. The value of p may be large but the value of q is commonly kept small.

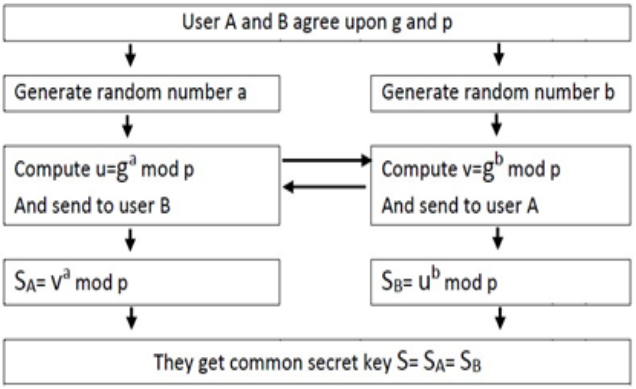

Fig 3:- Diffie Hellman Key Exchange Process

As it can be seen in figure 3, the critical calculation computes a common secret key for both parties by not even sharing the actual key. The process makes key exchange safe and prevent 3rd party from prying.

IV. PROPOSED SCHEME

As discussed earlier AMPC scheme merges AES block cipher, fast cryptographic technique [9], and Playfair cipher (stream cipher) to achieve more security with minimum computational delay.

Let's assume node A and B are going to exchange data. Firstly, with D-H key exchange method both nodes share their public key keeping their private key secret and then generate their common secret key. The key is then used to generate the first version of cipher text using AES encryption system. The resultant cipher text is then again encrypted using the same key with the help of a modified playfair cipher cryptographic algorithm.

The modified playfair cipher uses a 6 by 6 matrix instead of 5 by 5 matrix. This enables the encryptions of 24 English alphabets and also 10 numbers. An example of generated matrix during the process has been given in figure 4.

P	U	Z	L	E	A
B	C	D	F	G	H
I	J	K	M	N	O
Q	R	S	T	V	W
X	Y	0	1	2	3
4	5	6	7	8	9

Fig 4:- Modified Key Matrix for Playfair Cipher

Here the letter J doesn't need to be substituted. The sole purpose of this modification was to include encryption of numbers with playfair cipher as in most wireless sensor networks numeric data is needed transport.

ISSN No:-2456-2165

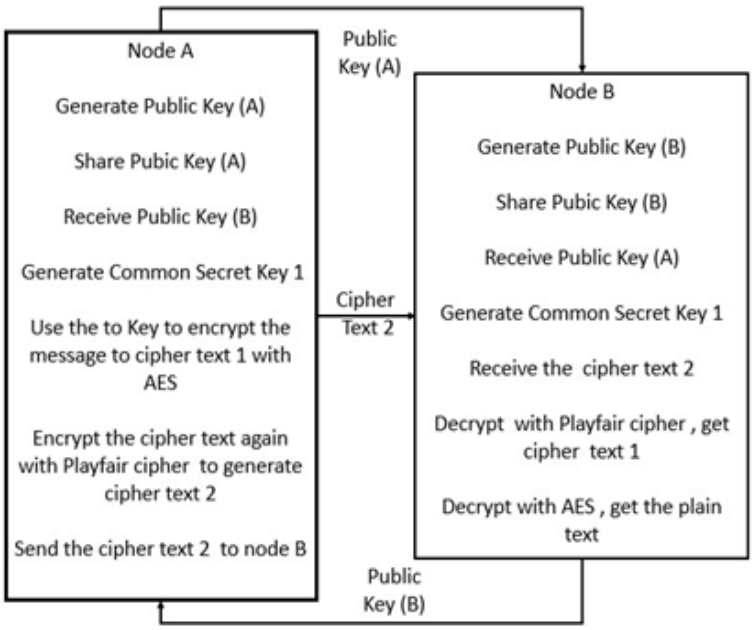

Fig 5:- Process flow of the proposed scheme

The computational steps of AMPC has been given below-

Step 01: Node A generates Public Key (A)
Step 02: Node B generates Public Key (B)
Step 03: Node A shares Pubic Key (A) with Node B
Step 04: Node B shares Pubic Key (B) with Node A
Step 05: Node A and B generates common secret key 1
Step 06: Node A uses key 1 to encrypts the message to cipher text 1 with AES
Step 07: Node A Encrypts the cipher text again with Playfair Cipher to generate cipher text 2
Step 08: Node A sends the cipher text 2 to node B
Step 09: Node B receives the cipher text 2
Step 10: Node B decrypts cipher text 2 with Playfair cipher and gets cipher text 1
Step 11: Node B decrypts cipher text 1 with AES and retrieves the actual message

The process above has been represented in Figure 5.

V. RESULT ANALYSIS

The performance of AMPC is measured in a computer with the following configurations - Intel® Core™ i7 6500U CPU and 2.5GHz processor and 8 GB of RAM on Windows 10 operating system for plaintext file size of 500 kb and implemented with C++.

The performance analysis, comparing the processing time, of AMPC was done with different hybrid cryptographic schemes, triple DES & Krishna [5], THCA [7] and Chaffing & Winnowing with AES [8]. Processing time is calculated with a fixed length of file for both cases, encryption and decryption.

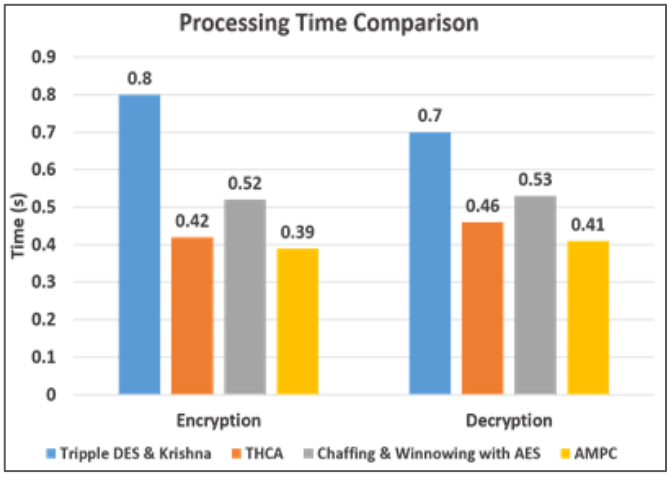

Fig 6:- Comparison between proposed & existing schemes

From the figure 6, it can be seen clearly that the processing time of AMPC outweigh other hybrid schemes. As the processing time , during encryption and decryption, of AMPC is much lower than other schemes.

VI. CONCLUSION

The proposed hybrid cryptographic algorithm, AMPC, strengthen the security of WSN as there are two cryptographic algorithms, AES and modified PlayFair, are used for data security and another algorithm, Diffie-Hellman, is used for secure the key exchange process. In addition, AMPC requires less operational time compared to other existing hybrid algorithms, therefore, it facilitates fast data transmission with lower energy consumption. To recapitulate, AMPC scheme is an optimum solution to overcome the limitations of WSN which provides more security with minimum computational delay.

REFERENCES

[1]. Y. Maleh, A. Ezzati, "An Advanced Study on Cryptography Mechanism for Wireless Sensor Networks," Mediterranean Telecommunications Journal, Vol. 6, No. 2, pp. . June 2016. Accessed On: Sept. 2016.[Online].Available: https://arxiv.org/abs/1609.05323
[2]. R. Alvarez, J. Santonja, A. Zamora, "Algorithms for Lightweight Key Exchange," In Proceedings of the 10th International Conference on Ubiquitous Computing and Ambient Intelligence, Gran Canaria, Spain, 29 November-2 December 2016, Part II. pp. 536-543.
[3]. J. V. D. Bogaert, "What is hybrid cryptrography?", ESUS.COM, Apr. 2014. [Online]. Available: https://esus.com/hybrid-cryptography [Accessed: 20 Apr. 2014]
[4]. A. Faquih, P. Kadam, and Z. Saquib, "Cryptographic techniques for wireless sensor networks: A survey," 2015 IEEE Bombay Section Symposium (IBSS), 2015.
[5]. Ali Abdulridha Taha, Dr. Diaa Salama Abd Elminaam, Prof.Dr. Khalid M Hosny, " NHCA: Developing New Hybrid Cryptography Algorithm for Cloud Computing Environment," (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 8, No. 11, 2017. DOI: https://doi.org/10.14569/IJACSA.2017.081158
[6]. Krishna, A. V. N., and Babu A. Vinaya. "A modified hill cipheralgorithm for encryption of data in data transmission." Computer Sciences and Telecommunications, Vol 3, 78-83, 2007. DOI: https://doi.org/10.5815/ijcnis.2012.05.07
[7]. Rawya Rizk and Yasmin Alkady. "Two-phase hybrid cryptography algorithm for wireless sensor networks." Journal of Electrical Systems and Information Technology 2 ,296–313, 2015 . DOI: https://doi.org/10.1016/j.jesit.2015.11.005
[8]. Er. Parvin Shaikh and Dr. SonaliPatil. " Performance Evaluation of Hybrid Cryptography System." International Journal of Engineering Trends and Technology – Vol 54– 12,2017. DOI: https://doi.org/10.14445/22315381/IJETT-V54P235
[9]. Margaret Rouse 2014, "Advanced Encryption Standard (AES)"Retrieved from https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard
[10]. Singh, Simon (2000). The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography.
[11]. Hershey, J. E. Cryptography Demystified. New York: McGraw-Hill, pp. 162-166, 2003.