ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

Security and Timing Analysis of Hybrid Algorithm for ZigBee in Wireless Sensor Network

Smita S. Kulkarni[1], Amol D. Bhoi[2]
Student[1], Assistant Professor[2]
Department of E & TC
G.H. Raisoni Institute of Engineering Technology, Wagholi, Pune, India

Abstract:
In Wireless Sensor Network sensor nodes are used for monitoring and controlling action. These sensors interact with sensitive data and may operate in averse condition, hence security of this network gains higher importance. For providing security AES and ECC algorithm from symmetric and asymmetric cryptographic techniques respectively are chosen. In this paper security of WSN is enhanced by applying ECC and AES algorithm serially. In this data obtained from the sensors are encrypted with ECC and AES algorithm using ZigBee. Performance of the WSN is evaluated in each of the algorithm for time requirement and compared with other algorithms.

Keywords: WSN (Wireless Sensor Network), AES (Advanced Encryption Standard, ECC (Elliptic Curve Cryptography, ZigBee, Hybrid, Symmetric, Asymmetric, Cryptography.

I. INTRODUCTION

A Wireless Sensor Network (WSN) consists of various sensor nodes that gathers data from remote sensor locations, processes data and communicate through radio signals. As sensor network uses limited power resources, small memory size, and deployment in remote area. This leads to necessity of security for WSN.Algorithms used for security depends on key size, computational time, power requirement.

A ZigBee is a protocol from Wireless Senor Network which provides secure transmission of data. ZigBee requires low power and low cost. It is built over IEEE 802.15.4 standard. ZigBee is applied for various domains as building/home automation, health care, smart energy, telecom services etc.

It uses Carrier Sense Multiple Access\Collision Avoidance (CSMA\CA) protocol for scanning the channel. ZigBee uses AES (Advanced Encryption Standard) algorithm for encryption of plain text before sending over channel. It provides confidentiality by using 128 bit key size. Message Authentication Code is used for Data Integrity. This security of ZigBee can be break by attacking the cipher text. ZigBee uses only AES algorithm for providing security but, NIST researchers predicts that there is a possibility of breaking cipher text from AES within nearest future. Hence there is necessity to increase security of ZigBee by some other technique. This can be done by using ECC algorithm with AES. i.e. by using hybrid algorithm for ZigBee.

In this paper we attempted to increase security of ZigBee by incorporating ECC and AES algorithm. In this system, 8 bit input data from temperature, humidity and smoke is applied to ECC algorithm which encrypts it with 16 bit shared key. This cipher text is again encrypted with 128 bit key from AES algorithm of ZigBee and transmitted through wireless channel.

II. LITERATURE SURVEY

Different algorithms from cryptography are studied by various researchers. Their literature is reviewed in next paragraphs. Multiple Key Protocol (MKP) for ZigBee modifies AES algorithm by adding key for each block. This key is generated by using ECC. MKP uses parallel operations for authentication and encryption which increases throughput of the system and reduces run time [8].

Security protocol by using ECC, Dual-RSA and MD-5 from symmetric and asymmetric algorithms. It gives improved security by using hybrid algorithm. Two drawbacks for this system are, it is time consuming, and entire data can be stolen if private key is known [14] [15].

Hybrid security protocol uses AES and ECC algorithm sequentially with MD-5 algorithm. Its drawback is higher execution time [15] [16]. Security authentication protocol for authentication of nodes and key establishment. It uses ECC for protocol generation [12].

It also shows how ECC is better in comparison with RSA by considering key size, security level and computational speed. Advantages of ECC algorithm over RSA algorithm are studied [3] [13].

III. METHODOLOGY

A] Design:

This system uses ECC and AES algorithm for ZigBee in following way:

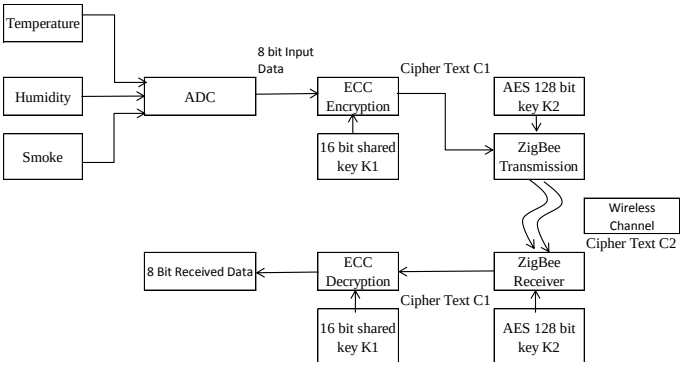

Figure.1. Block diagram ECC and AES Algorithm for ZigBee

The block diagram of proposed system is shown in Fig 1. In the system input is applied from temperature, humidity and smoke to ADC, converted 8 bit input is given to ECC algorithm for encryption, where 16 bit shared key K1 (Public key of receiver and Private key of sender) is applied and the cipher text C1 is used as input to ZigBee transmission where the cipher text is again AES encrypted with 128 bit key K2,which gives output as cipher text C2. This Cipher text C2 is passed through wireless communication channel. Here Rayleigh channel is used for transmission. At receiver end, received cipher text C2 is AES decrypted and C1 is obtained. This C1 is applied to ECC decryption algorithm having shared key as K1 (Public key of sender and Private Key of receiver) to recover original data.

B] Principle of Operation:

i) Elliptic Curve Cryptography (ECC) Algorithm in detail:

ECC is one type of asymmetric cryptography technique. It uses two different keys, one for encryption and other for decryption [4].

Curve that satisfy following equation is, Elliptic Curve equation

$$y^2 = x^3 + ax + b \qquad (1)$$

For an elliptic curve $E_q(a,b)$ having parameters a, b and q where q is large prime number. G is the base point from the elliptic curve whose order is large value of n.

Discrete logarithm problem is considered for ECC. Shared secret key generation for ECC is given from Diffie-Hellman key exchange. It takes full exponential time. ECC requires reduced key size than RSA.

Discrete logarithmic problem for ECC is given as,

$$Q = x \times P \qquad (2)$$

Where P is fixed prime on elliptical curve. $x$is a number of times P added to itself. It is very hard to find x if $P$and Q are given.

Encryption and Decryption with ECC.

$P_m$it is the plain text considered as x-y point. $G$is the base point from $E_p(a,b)$ elliptical curve.

User A selects private key $nA, where\ nA < n$ and generates public key

$$PA = nA \times G \qquad (3)$$

Cipher text is formed as,

$$C_m = \{PA, P_m + nAPB\} \qquad (4)$$

At B, B multiplies PA with its private key nB and subtract it from second point.

$$P_m + nA \times PB - \mathrm{PA} \times nB \qquad (5)$$
$$= P_m + nA(nB \times G) - (nA \times G)\, nB$$
$$= P_m$$

For attacker it is hard to find nA with $(nA \times G)$ and G are given.

ii) AES Algorithm in detail:

This is one type of symmetric algorithm uses block cipher method. It operates over variable block with variable key size.128, 192 or 256 bits is used for block/key [2]. AES algorithm is in built in ZigBee protocol for providing security. Variable key size is the advantage of AES [9], whereas it is predicted by NIST researchers the key of AES maybe break in forthcoming years due to rapid development of technology[5][6].

Encryption in AES is done in following manner.

1) Byte Substitution: input bytes are substituted with S-box value, result is 4X4 matrix.
2) Rows Shifting: Each of 4 rows are shifted to left.
3) Columns Mixing: A math function takes input from one column and outputs four new different bytes.
4) Add round key: 128 bits from matrix are Ex-ORed with 128 bits of round key.

For decryption above operations are performed in reverse order.

IV. SYSTEM IMPLEMENTATION

For implementation of system MATLAB is used. Fig 2 shows flowchart of system. In Encryption technique of hybrid algorithm Elliptic Curve E and Base Point G are initialized as public parameters. Private keys for user A and B are generated and public key for both are calculated from private keys. These keys are further used in shared secret keys for encrypting and decrypting of data. Cipher text obtained from ECC algorithm again mixed with key from AES algorithm to get cipher text C2, which is transmitted over wireless channel.

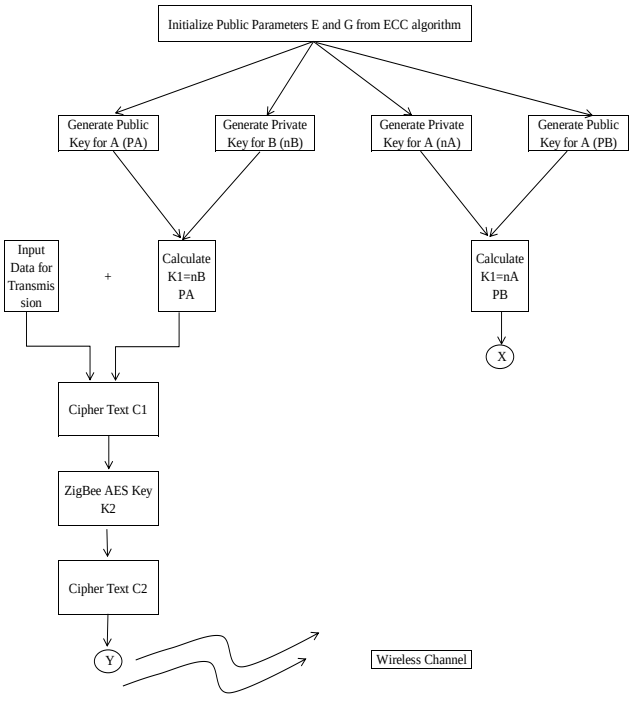

Figure.2. Encryption flowchart in hybrid algorithm

Decryption technique in hybrid algorithm is explained in Fig 2.2.

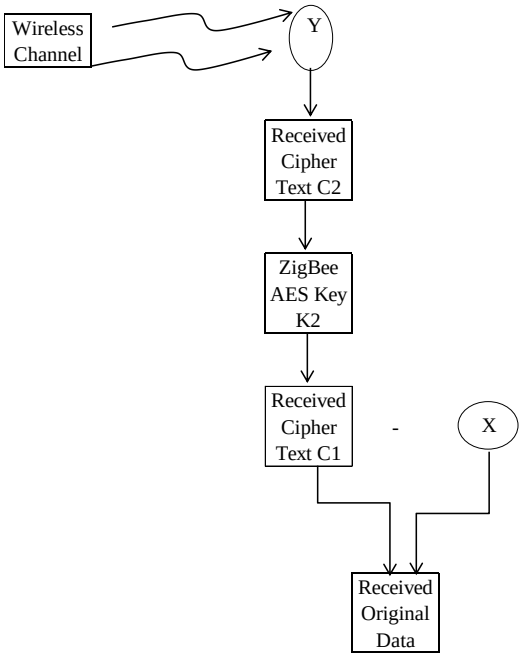

Figure.3.Decryption flowchart in hybrid algorithm

In decryption received cipher text C2 is decrypted with AES key to get back Cipher text C1. Shared secret key is subtracted from C1 to get back original data.

V. RESULTS

Elliptic Curve Cryptography uses elliptic curve, in which coefficients and variables are selected from finite field element. Elliptic Curve for $a = 0.5\ and\ b = 0.8$ is plotted. Fig 3 shows elliptic curve for above values of a and b. Base point G is selected from this curve. Value of G is selected as 1.51 for further calculations.

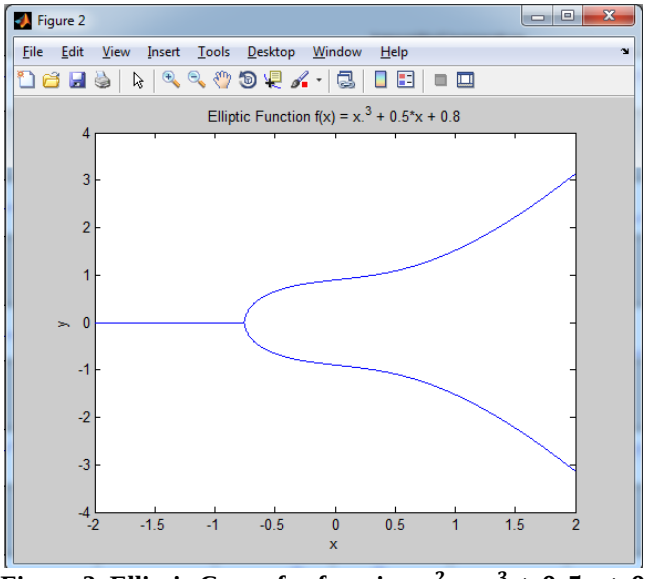

Figure.3. Elliptic Curve for function $y^2 = x^3 + 0.5x + 0.8$

8 bit digital data from temperature input is given to ECC encryption. In next step cipher text is obtained by adding it to product of secret key and base point G. The result & public key is sent to receiver for decoding. The Fig 4 shows the result of ECC.

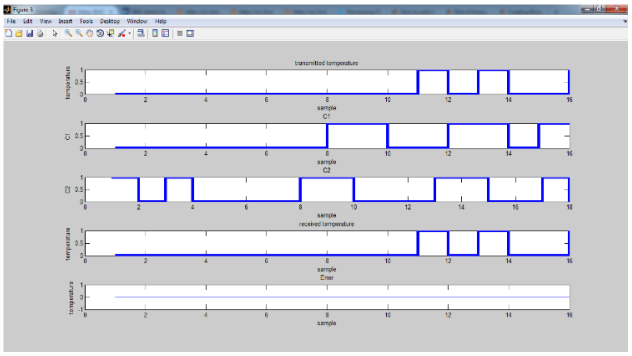

Figure.4. ECC Encrypted and decrypted temperature data in digital

The obtained result of ECC is combined with AES with 128 bit AES key. The final encrypted data is transmitted using ZigBee. The wireless channel used is Rayleigh. The AES encrypted data using ZigBee is as shown in Fig 5

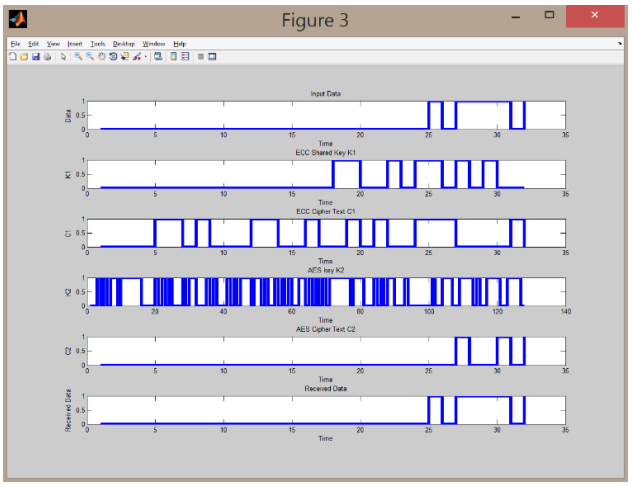

Figure.5. AES and ECC Encrypted and decrypted temperature data

Time required for encryption and decryption of AES and ECC algorithm are compared in following table, Table I.

Table.I. Comparison between algorithms for time requirement

Compared Algorithm	Encryption Time	Decryption Time
ECC	6.40E-05	3.23E-04
AES	9.56E-04	9.50E-04

Time requirement of AES encryption and decryption is more than ECC encryption and decryption time. Due to combining of algorithms decryption time is increased by 3%.

VI. CONCLUSION

In WSN, the security can be enhanced by combining ECC and AES algorithm Security of ZigBee which uses AES algorithm is increased by mixing it with ECC algorithm. Also timing requirement for each algorithm is evaluated. It is observed that by combining ECC and AES algorithm, encryption and

decryption time is increased. In further work power consumption of implemented algorithm can be evaluated.

VII. REFERENCES

[1].Li Chunqing, Zhang Jiancheng, "Research of ZigBee's data security and protection", International Forum on Computer Science-Technology and Applications 2009, IEEE, 2009, pp 298 - 302.

[2].P.D. Khambre, S.S.Sambhare, P.S. Chavan, "Secure Data in Wireless Sensor Network via AES" " International Journal of Computer Science and Information Technologies, Vol. 3 (2) , 2012

[3].Kristin Lauter, "The Advantages of Elliptical Curve Cryptography for Wireless Security", IEEE Wireless Communications 2004

[4].G.V.S. Raju and RehanAkbani,"Elliptic Curve Cryptosystem and its Applications ", IEEE 2003.

[5].MengQianqian and BaoKejin, "Security analysis for wireless networks based on ZigBee", IEEE,vol 1, 2009, pp 158 - 160.

[6].Bin Yang, "Study on security of wireless sensor network based on ZigBee standard." International Conference on Computational Intelligence and Security, IEEE, 2009, pp 426 - 430.

[7].MadhumitaPandaSecurity in Wireless Sensor Networks using Cryptographic Techniques", American Journal of Engineering Research (AJER) 2014

[8].Saif Al-alak, Zuriati Ahmed, Azizol Abdullah and ShamalaSubramiam, "AES and ECC Mixed for ZigBee Wireless Sensor Security", International Scholarly and Scientific Research & Innovation 5(9) 2011

[9].https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

[10]. William Stallings, "Cryptography and Network Security-Principles and Practice" NY: Prentice Hall, 2011

[11].https://msdn.microsoft.com

[12].Sunil Gupta, Harsh Kumar Verma and AL Sangal, "Authentication Protocol for Wireless Sensor Networks" International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering 2010.

[13].G. Jai Arul Jose and C. Sajeev," The security of elliptic curve cryptography over RSA cryptography" Elixir Comp. Sci. &Engg. 2011

[14].S. Subasree and N. K. Sakthivel, "Design of a New Security Protocol using Hybrid Cryptographic Algorithms" IJRRAS 2010

[15].S. Aruna, D. Anitha, Promit Roy and RiddhiDatta, " Survey of Hybrid Cryptography Algorithms in WSN using ZigBee", IJCTA 2016

[16]. N. Kumar, "A Secure communication wireless sensor networks through hybrid (AES+ECC) algorithm", von LAP LAMBERT Academic Publishing, vol. 386, 2012.