ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

Enhanced Security Technique of Wireless Sensor Network using Hybrid Cryptography

[1] K.Sethu Selvam, [2] Dr.S.P.Rajagopalan
[1] Research Scholar, Vels University,Pallavaram, Chennai, India
Professor, G.K.M College of Engineering and Technology, Perungalathur, Chennai, India

Abstract: **- Wireless sensor network (WSN) is a collection of a sensor which is deployed remotely to sense the complicated area. It is used in various fields like military surveillance, disaster management and etc. Security is the most vital in the network. Cryptography plays an important role in network security. The traditional cryptographic technique cannot be applied to wireless sensor network because of its resource limitation. The proposed model is a hybrid cryptography which is a combination of both symmetric and asymmetric cryptographic techniques. The key is generated with the help of ECC and securely transmitted through ECDH protocol. Confidentiality of data is done through AES, Blowfish and ECC. Hashing technique MD5 is used for Integrity of data. It provides high security in an efficient manner. It requires less memory, energy and computation time.**

Keywords: **WSN, Hybrid Cryptography, AES, ECC, Blowfish, MD5.**

I. INTRODUCTION

Sensor is a tiny and low cost device. The primary work of sensor is sensing the zone and sending that information to the base station. Wireless sensor network (WSN) is a group of sensor which is used to sense the critical environment. The application of WSN is in military application, battle field, disaster management and monitoring the environment. WSNs are pertaining to information and resource has to be secured against attacks and misbehavior. The Security goals are Authentication, Integrity, Availability, Confidentiality and Freshness. Among all, authentication and Integrity are important principles in military application. Cryptography is a technique to provide security for network. They are broadly classified into Symmetric key and Asymmetric key. In Symmetric key Cryptography, a single key is used for encryption and decryption. Eg: DES, AES, Blowfish, Twofish. In Asymmetric key cryptography, a pair of key is used. Public key is used for encryption and private key is used for decryption. Ex: RSA, ECC, ECDSA, ECDH and etc Hashing Technique is also one of cryptography function. It is used to secure the data transmission. It is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash function) which is also designed to be a one-way function, that is, a function which is infeasible to invert. Cryptographic hash functions have many information-security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication. They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption [31].

Hybrid Cryptography:

Hybrid cryptography is combination of Symmetric and Asymmetric key cryptography to benefit from strength of each form of encryption.

Table 1 shows Comparison of Symmetric key and Asymmetric key

Symmetric Key	**Asymmetric Key**
➢ Single Key	➢ A pair of key
➢ Less secure method	➢ High level secure
➢ Less Complexity	➢ More Complexity
➢ Less Resource Consuming	➢ High resource Consuming
➢ Fast	➢ Slow

In this paper, section 2 discuss related work, section 3 describes proposed system, section 4 show the simulation results and section 5 is conclusion.

II. RELATED WORK

1) Subasree Security Protocol Architecture[7][25]

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

The given plain text can be encrypted with the help of ECC and the derived cipher text can be communicated to the destination through any secured channel. Simultaneously, the Hash value is calculated through MD5 for the same plain text, which already has been converted into the cipher text by ECC. This Hash value has been encrypted with DUAL RSA and the encrypted message of this Hash value also sent to the destination. There are two disadvantages. First, the message is encrypted by Asymmetric Encryption Algorithms (ECC and DUAL RSA Public key encryptions) that are slow compared to symmetric encryption. Second, if an attacker determines a person's private key, his or her entire messages can be read.

2) Kumar Security Protocol Architecture [7][11]

The given plain text is encrypted first with AES algorithm and then with ECC algorithm. The Hash value of this encrypted cipher text is taken through the MD5 algorithm. On the other side, the Hash value is first evaluated and integrated. Thereafter, the decryption of cipher text is done by AES and ECC decryption algorithms. Hence, the plaintext can be derived. However, the execution time of this protocol is long because the plaintext is encrypted sequentially by both AES and ECC.

3) Kady Security Protocol Architecture [7][28]

The plaintext is divided into n blocks Bi. Each block consists of 128 bits. Then, it is divided into two parts p1 blocks, and P2 blocks. The first n/2 blocks are encrypted using (AES and ECC). In parallel, the remaining n/2 blocks are encrypted using XOR-DUAL RSA algorithm. Then hashing each two half using MD5 In the Decryption Phase The decryption phase the cipher text is divided into n blocks each block consists of 128 bits, Then it will divided into two parts ci blocks and Ci blocks. Hashing is used to identify whether the source node receive the same cipher text or not. In the case of the hash values are the same at the source and sink nodes, the first n/2 blocks are decrypted using AES and ECC algorithms The remaining n/2 blocks are decrypted using XOR-DUAL RSA algorithm

4) Zhu Security Protocol Architecture[7][30]

The plaintext is encrypted with Symmetric cipher algorithm, and the key and digital signature belonged to the Symmetric encryption algorithm are encrypted with Asymmetric key algorithm. The sender encrypts the plaintext P with the key AES belonged to the AES algorithm. To ensure the security of the cipher algorithm and simplify the key management, the sender uses the key K AES only once. The receiver obtains the original information P after signature verification. The main disadvantage of this protocol, this protocol suffers from low security level since that the message is encrypted in a single phase which leads to less complexity.

5) Hatem Security Protocol Architecture [7]

The plaintext is divided into n blocks Bi. Each block consists of 128 bits. Then, it is divided into two parts p1 blocks, and P2 blocks. The first n/2 blocks are encrypted using (AES and ECC). The remaining n/2 blocks are encrypted using RSA and Blowfish algorithm. Then hashing each two half using MD5 In the Decryption Phase The decryption phase the cipher text is divided into n blocks each block consists of 128 bits, Then it will divided into two parts. Hashing is used to identify whether the source node receive the same cipher text or not. In the case of the hash values are the same at the source and sink nodes, the first n/2 blocks are decrypted using AES and ECC algorithms. The remaining n/2 blocks are decrypted using RSA and Blowfish algorithm.

III. PROPOSED SECURITY ARCHITECTURE

Enhanced Hybrid Cryptography Protocol (EHCP)

Encryption Phase:

The plaintext is divided into n blocks. Each block consists of 128 bits. Then, it is divided into three parts P1,P2 and P3. This protocol uses padding with null for the last block to be 128 bits. First block P1 are encrypted using AES encryption algorithm. AES encryption is done by four steps (SubBytes step, ShiftRows Step, Mixcolumn Step and AddRound Key). AES 128 bit key operation is performed in 10 rounds. Elliptic Curve Cryptography (ECC) algorithm is used for protecting secret key which is highest secure public key algorithm. Moreover, according to the mathematical problem on which ECC can be solved by full exponentiation rather than sub-exponentiation for other public key systems, ECC needs smaller key size than other algorithms and that refers to less memory size. Second block P2 are encrypted using ECC algorithm. Blowfish is a symmetric key block cipher algorithm. Third block P3 are encrypted using Blowfish algorithm.

ECDH - Elliptic Curve Diffie Hellman is a key agreement protocol that allows sender and receiver to establish a shared secret key that can be used for private key algorithms. Both sender and receiver exchange some public information to each other. Hashing technique MD5 is used for authentication purpose.

Algorithm:

Encryption Steps: (Sender)

1. Plain text is divided into 3 parts as P1, P2 and P3 .
2. Public and Private keys are generated using Elliptic Curve Cryptography (ECC).

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

3. Key exchange is performed by Elliptic Curve Diffie-Hellman (ECDH).
4. Encrypt first part of Plain text P1 using AES algorithm (Cipher text C1).
5. Encrypt second part of Plain text P2 using Blowfish algorithm (Cipher text C2).
6. Encrypt third part of Plain text P3 using ECC algorithm (Cipher text C3).
7. Compute hash value of Plain text using MD5 hashing technique.

At the last step of encryption process, Key information, Cipher text and hashing values are sent to receiver at the same time. The receiver may be a node or sink.

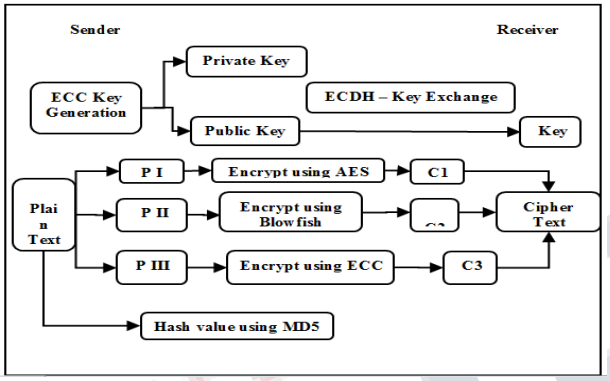
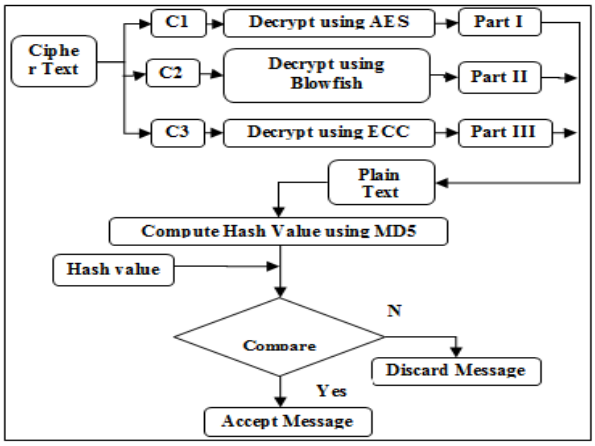


Fig-1 shows Encryption phase

Decryption phase

The cipher text is divided into n blocks. Each block consists of 128 bits. Then it will be divided into three parts C1, C2 and C3. Cipher text C1 is decrypted by using AES algorithm. Cipher text C2 is decrypted by using Blowfish algorithm. And Cipher text C3 is decrypted by using ECC algorithm. These plain texts are concatenated. Then compute the hash value of plain text using MD5 algorithm. In this proposed method (EHCP), compare received and computed hash values, if it is same, the receiver accept the message otherwise discard the message.
Fig-2 shows Decryption phase



Algorithm

Decryption Steps: (Receiver)
1) Divide Cipher text into 3 parts as C1,C2 and C3
2) Decrypt cipher text C1 using AES (P1)
3) Decrypt cipher text C2 using Blowfish (P2)
4) Decrypt cipher text C3 using ECC (P3)
5) Concatenate P1, P2 and P3 plain text
6) Compute hash value of plain text using MD5
7) Compare hash values. If it is same, accept message otherwise discard the message.

IV. RESULTS AND DISCUSSION

In order to prove the numerical results of the proposed protocol (EHCP), it is tested as the security protocol in WSN. The simulation is done using the network simulator ns2. Table II shows that time of encryption for different size of plain text. Fig-3 shows that time of encryption is compared with existing protocol to EHCP method.

TABLE II. TIME OF ENCRYPTTON (MS)

Size of plain text (bytes)	Subasree Protocol	Kumar Protocol	Zhu Protocol	Kady Protocol	Hatem Protocol	EHCP
1512	3251	4137	1806	253	105	102
5676	4521	5106	2713	385	315	301
10257	5121	5723	3183	415	389	363
25716	7109	7532	5602	501	403	395
158713	8320	8596	6317	585	465	450

Fig-3 Time of Encryption compared to other protocols

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

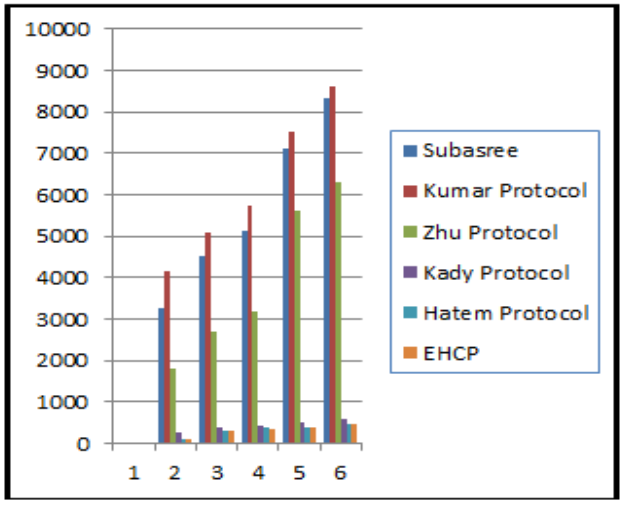


Table III shows that time of decryption for different size of plain text. Fig-4 shows that time of encryption is compared with existing protocol to EHCP method.

TABLE III. TIME OF DECRYPTTON (MS)

Size of plain text (bytes)	Subasree Protocol	Kumar Protocol	Zhu Protocol	Kady Protocol	Hatem Protocol	EHCP
1512	2301	1839	865	812	803	721
5676	2891	2097	912	878	865	813
10257	3109	2132	987	919	909	879
25716	7109	4313	1013	981	963	891
158713	8320	5137	1312	1031	989	927

Fig-4 Time of Decryption compared to other protocols

V. CONCLUSION

In this paper, a hybrid security protocol (EHCP) for WSNs is proposed. The proposed hybrid protocol (EHCP) tries on trap those intruders by splitting the plain text and then applies three different cryptographic techniques. First, it takes the advantages of the combination of both Symmetric and Asymmetric cryptographic techniques using AES, Blowfish and ECC algorithms. Second, it is utilized since it is more robust and cannot be easily attacked. In addition, Hashing is also used for data integrity using MD5 which has to be ensured that the original text is not being altered in the communication medium. The attractiveness of the proposed protocol, compared to other existing security protocols is that it provides better security for a shorter encryption and decryption time, and smallest cipher text size. It is a reducing processing overhead and achieving lower memory consumption that is appropriate for all WSN applications.

REFERENCES

1) Abdul.Elminaam D. S., H. M. Abdul kader, M. M. Hadhoud, ”Tradeoffs between Energy Consumption and Security of Symmetric Encryption Algorithms”, International Journal of Computer Theory and Engineering (IJCTE),VOL.1 No.3, pp: 342- 350, August 2009. (ISSN: 1793-821X).

2) Abdul.Elminaam D. S., H. M. Abdul kader, M. M. Hadhoud." Evaluating the Performance of Symmetric Encryption Algorithms ".International Journal of Network Security (IJNS), VOL.10 No.3, pp: 216- 222, May 2010.

3) Ahmed Al-Riyami, Ning Zhang, And John Keane, “An Adaptive Early Node Compromise Detection Scheme for Hierarchical WSNs”, IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011,978-1-4577-0590-8/11/$26.00 ©2011 IEEE MIT, Anna University, Chennai. June 3-5, 2011

4) Al-alak S., Z. Ahmed, A. Abdullah and S. Subramiam," AES and ECC Mixed for ZigBee Wireless Sensor Security", World Academy of Science, Engineering and Technology, 2011

5) Dawahdeh Z, Yaakob N.S., “A New Modification for Menezes-Vanstone Elliptic Curve Cryptosystem”, Journal of Theoretical and Applied Information Technology, Vol.85, pp. 290-297 (2016).

6) Dubal M. J., T. R. Mahesh, and P. A. Ghosh, "Design of a new security protocol using hybrid cryptography architecture," In Proceedings of 3rd International Conference on Electronics Computer Technology (ICECT), vol. 5, 2011.

7) Hatem M. Abdul Kader, Mohie M. Hadhoud, Salah M El-Sayed, Diaa Salama AbdElminaam, “Performance Evaluation Of New Hybrid Encryption Algorithms To Be Used For Mobile Cloud Computing”, International Journal Of Technology Enhancements And Emerging Engineering Research, VOL 2, Issue 4 63 ISSN 2347-4289

8) Henry Nunoo-Mensah , Kwame Osei Boateng, James Dzisi Gadze,” Tamper-aware authentication framework for

9) Hossain Md. A., Islam Md. K., Das S. K. and Nashiry Md. A., "Cryptanalyzing of message digest algorithms MD4 and MD5", International Journal on Cryptography and In-formation Security (IJCIS), vol. 2, no.1, March 2012.

10)Ijaz Ali Shoukat, 1Kamalrulnizam Abu Bakar and Subariah Ibrahim, "A Generic Hybrid Encryption System (HES)", Research Journal of Applied Sciences, Engineering and Technology 5(9): 2692-2700, 2013 ISSN: 2040-7459; e-ISSN: 2040-7467 © Maxwell Scientific Organization, 2013 ISSN 2229-5518.

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

12)Mohamed Elhoseny, Hamdy Elminir, Alaa Riad, Xiaohui Yuan, "A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic encryption", Journal of King Saud University – Computer and Information Sciences (2016) 28, 262–275.

13) Nejla Rouissi, Hamza Gharsellaoui, "Improved Hybrid LEACH Based Approach for Preserving Secured Integrity in Wireless Sensor Networks", Available online at www.sciencedirect.com.

14)Panda .M, "Security in Wireless Sensor Network using Cryptography Techniques", American Journal of Engineering Research (AJER), Vol. 3, pp. 50-56 (2014).

15)Pei-Yih Ting, Jia-Lun Tsai, and Tzong-Sun Wu,"Signcryption Method Suitable for Low-Power IoT Devices in a Wireless Sensor Network", Ieee Systems Journal.

16) Pooja Lal Mundaniya & Naveen Choudhary," High Security by using Triple Wrapping Feature and their Comparison", Global Journal of Computer Science and Technology: Information & Technology Volume 15 Issue 2 Version 1.0 Year 2015, Online ISSN: 0975-4172 & Print ISSN: 0975-4350.

17)Prathusha laxmi b, Chilambuchelvan a, "GSR: Geographic Secured Routing using SHA-3 Algorithm for Node and Message Authentication in Wireless Sensor Networks", https://doi.org/10.1016/j.future.2017.05.015

18) Ramasubba Reddy .B, Saritha .A ,BalaKonda Reddy B," Secure Data Transmission Using Virtual Private Networks", International Journal of Advanced Engineering Research and Science (IJAERS)

19) Rawya Rizk and Yasmin Alkady, "Two-phase hybrid cryptography algorithm for wireless sensor networks", Journal of Electrical Systems and Information Technology, pp- 296–313, (2015), Available online at www.sciencedirect.com

20) Ren .W, and Miao .Z, "A new security protocol using hybrid cryptography," In Proceedings of the 9th International Conference Computer Engineering Conference (ICEN-CO), 9th International, pp. 109-115, 2013.

21)Rounak Sinha, Hemant Kumar Srivastava, Sumita Gupta, "Performance Based Comparison Study of RSA and Elliptic Curve Cryptography", International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013

22) Selva Reegan .A, Baburaj E," Polynomial and multivariate mapping-based triple-key approach for secure key distribution in wireless sensor networks", http://dx.doi.org/10.1016/j.compeleceng.2016.10.018 Elsevier Ltd.

23) Shaikh Ammarah P. "Security Enhancement Algorithm for Data Transmission using Elliptic Curve Diffie - Hellman Key Exchange", International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868.

24) Shiva Prakash and Ashish Rajput,"Hybrid Cryptography for Secure Data Communication in Wireless Sensor Networks", 2nd International Conference on Computer, Communication and Computational Sciences (RACCCS-2017).

25)Subasree S and Sakthivel N. K, "Design of a new security protocol using hybrid cryptography algorithms," IJRRAS, vol. 2, no. 2, pp. 95-103, February 2010.

26)Surbhi Aggarwal,Neha Goyal, Kirti Aggarwal, " A review of Comparative Study of MD5 and SHA Security Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 104 – No.14, October 2014

27)Thwe Thwe Ngwe, Su Wai Phyo," Hybrid Cryptosystem For Data Security", International Journal of Advances in Electronics and Computer Science, ISSN: 2393-2835, Volume-2, Issue-6, June-2015.

28) Yasmin Al28, Mohmed I. Habib, Rawya Y. Rizk, "A New Security Protocol Using Hybrid Cryptography Algorithms", 978-1-4799-3370-9/13/$31.00 ©2013 IEEE.

29) Yassine Maleh, Abdellah Ezzatib , Youssef Qasmaouic, Mohamed Mbida, "A Global Hybrid Intrusion Detection System for Wireless Sensor Networks", Available online at www.sciencedirect.com.

30) Zhu .S," Research of hybrid cipher algorithm application to hydraulic information transmission," In Proceedings International Conference on Electronics, Communications and Control (ICECC), 2011.

31) Cryptographic function from Wikipedia, the free encyclopedia.