Middle-East Journal of Scientific Research 24 (6): 1926-1931, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.24.06.23558

Advanced Cryptographic Algorithm to Secure the Sensor Node Data in Wireless Sensor Networks

[1]M. Rajalakshmi, [2]C. Parthasarathy and [3]R.V. Indrajith

[1]Department of CSE, SCSVMV University, Kanchipuram, India
[2]Department of IT SCSVMV University Kanchipuram, India
[3]Department of CSE SKPC Kanchipuram, India

Abstract: The wireless sensor networks have grown rapidly in many applications. In some specific applications like in military, the sensor nodes data must be confidential during the transmission. The purpose of this research is to develop new advanced cryptographic algorithm to protect the sensor node data in wireless sensor networks. The sensor nodes are having the resource constraints such as processing speed, the memory size and power to limit the applicability of existing cryptographic algorithms for WSN. The lifetime of energy efficiency and battery plays an important role in the life of the network. Providing good security algorithm consumes more energy used by a node, so it is necessary to minimize the energy consumption of each security algorithms that are implemented in WSN. It is important one to choose the most energy efficient and appropriate encryption algorithm for WSNs. In this paper, an advanced encryption algorithm is implemented in order to achieve the goal of security and resource constraints of wireless sensor networks. It is not only simple algorithm but also enough security as a good encryption algorithm. The main aim of this research is to design and analysis of secure and lightweight efficient algorithms for deployment on resource constrained scenarios to secure the data in wireless sensor networks. This Energy Efficient Cryptographic (EECA) algorithm provides confidentiality, authenticity and integrity which are the main security services in wireless sensor networks. Simulation results show that the encryption algorithm proposed to the runtime capability, execution time and memory capacity is reduced in comparison with the various existing algorithms in WSN.

Key words: Wireless sensor networks · Cryptographic algorithms · Sensor nodes · Security

INTRODUCTION

Symmetric or secret key cryptography, a single or only one key is used for both encryption and decryption. Sender uses the key using some set of rules to encrypt the plaintext and sends the cipher text to the receiver. The receiver uses the same key or rule set to decrypt the message and recover the plaintext. Secret key cryptography is also called symmetric key algorithm. The distribution of the key is biggest difficulty in this approach. Stream cipher or block cipher is the general category of Secret key cryptography algorithm. Stream ciphers operate on a single bit at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same cipher text when using the same key in a block cipher whereas the same plaintext will encrypt to different cipher text in a stream cipher. Encryption is the process of encoding plain text and converts it to non-readable format called cipher text. Decryption is the process of decoding cipher text converting it to plain text. There are two types of cryptography namely: Symmetric Key Cryptography and Asymmetric Key Cryptography. Same key is used both for encryption as well as decryption process in symmetric key cryptography. Whereas in asymmetric key cryptography separate keys are used, one for encryption process and the other for decryption process.

Cryptography Different Goals: Authentication: The process of proving one's identity. It identify whether the person is authorized one to access the data.

Privacy/confidentiality: Ensuring that authorized person only can read the message.

Corresponding Author: M. Rajalakshmi, Department of CSE, SCSVMV University, Kanchipuram, India.

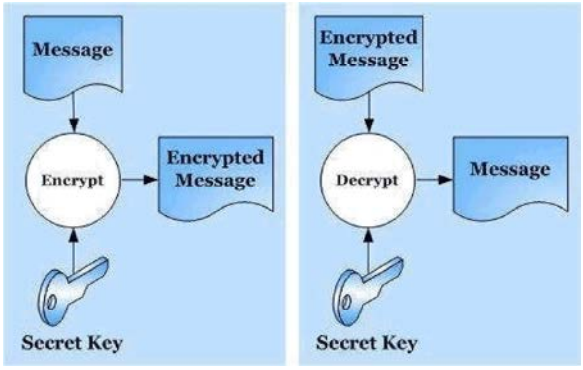

Fig. 1: Encryption and Decryption

Integrity: Received message has not been altered in any way from the original.

Non-Repudiation: A mechanism to prove that the sender really sent this message.

Typesof Cryptography: Cryptography is a process which is associated with scrambling plaintext (ordinary text, or clear text) into cipher text (a process called encryption), then back again (known as decryption). The common types are Secret Key Cryptography which is also known as Symmetric Key Cryptography and Public Key Cryptography which is also known as Asymmetric Key Cryptography.

Secret Key Cryptography: In secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver uses the same key to decrypt the message and recover the plaintext. Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher uses one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same cipher text when using the same key in a block cipher whereas the same plaintext will encrypt to different cipher text in a stream cipher.

Public Key Cryptography: Public or asymmetric key cryptography consist of two keys or of key pairs: one private key and one public key. One is used for encryption and the other for decryption. An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key.

Literature Review: Ritika Chehal *et al*. [1] proposed a cost effective symmetric key cryptographic algorithm for small amount of data. For a very minimal amount of data DES, AES and IDES were cost effective therefore these were not designed for small amount of data. They proposed an algorithm which was designed in a quite simple manner and involves all the security issues. It was used for both encryption and decryption but as public key cryptography was more secured; therefore secret key cryptography not fulfills the security issue completely.

Sonal Sharma [2] proposed a new symmetric key generation algorithm using sum of subset problem. They focused on information security which was the process of protecting information and it protects its availability, privacy and integrity. It increased the strength of the key while keeping the size of the key optimized. Hence encrypted data was more difficult to crack by a brute force technique and overhead of data encryption was also comparable to existing algorithms. It could be used for symmetric encryption of data while maintaining the integrity and security of the data.

Darpan Anand *et al*. [3] explored identity-based cryptography techniques and applications. They reviewed the identity based encryption applications in the field of various networks as ad- hoc networks. The scheme also used in mobile networks and other wireless networks. They also discussed that under what parameters identity based cryptography was used with its benefits and limitations. The main limitation was that the available methods were restricted to fixed output block, which was a trace for crackers.

Gerand Murphy *et al*. [4] worked on hardware-software implementation of public key cryptography used for Wireless Sensor Network (WSN). Protocols were used to ensure synchronization of keys between the devices in a network. These protocols required a significant communication and suffered from overhead. Using a hardware/software code sign approach, they had successfully mapped a public key cryptosystem based on Rabin's scheme. Their implementation was focused on efficient architectures which executes the public key algorithms using minimal resources. The limitation of such a cryptosystem was that they not provide the guarantee of confidentiality for the session keys.

Ashwak M.ML-Abiachi *et al*. [5] provides a competitive study of cryptography techniques over block cipher. Cryptography process seeks to distribute an estimation of basic cryptographic primitives across a number of confluences. It reduces the security assumptions on individual nodes, which established a level of fault-tolerance, opposing to the node alteration. It obtained a high security during the encryption and decryption process. It was based upon text contents and simplified the key management process. The complexity of this block cipher cryptographic model does not allow a graph to exchange the data in secured means.

Jingjing Lan *et al*. [6] proposed a Random Number Generator (RNG) for low power cryptographic applications. It was widely used in cryptographic systems as the cryptographic keys generator. These keys were most important component in the system because the security of the cryptographic system relies entirely on its quality. They also presented the good statistical quality and low energy consumption RNG including a serial-to-parallel shift register, a 32-bit register and a pseudo random number generator (PRNG) module which could be suitable for low-power, flexible cryptographic applications. They also suggested that it could be implemented completely in digital circuit and required no external components.

Research Objectives: Privacy is one of the key issues addressed by information Security. Through cryptographic encryption methods, one can prevent a third party from understanding transmitted raw data over unsecured channel during signal transmission. The cryptographic methods for enhancing the security of digital contents have gained high significance in the current era. Breach of security and misuse of confidential information that has been intercepted by unauthorized parties are key problems that information security tries to solve. This paper sets out to contribute to the general body of knowledge in the area of classical cryptography by developing a new hybrid way of encryption of plaintext.

Hybrid Cryptography: Symmetric key algorithm has a disadvantage of key distribution [7] and asymmetric algorithm need much computation so the power of the sensor is wasted in it [7] and it is not feasible to use as power is wasted then sensor will be of no use. Thus the algorithm which combines both the algorithm i.e. asymmetric and symmetric so the advantages of both the algorithm can be utilized in it. A hybrid cryptosystem is a protocol using multiple ciphers of different types together, each to it's best advantage. One common approach is to generate a random secret key for a symmetric cipher and then encrypt this key via an asymmetric cipher using the recipient's public key. The message itself is then encrypted using the symmetric cipher and the secret key. Both the encrypted secret key and the encrypted message are then sent to the recipient. The recipient decrypts the secret key first, using his/her own private key and then uses that key to decrypt the message. This is basically the approach used in PGP. Some of the hybrid algorithm like DHA+ECC [8] is used in WSN.

Proposed Algorithm: The proposed algorithm architecture of encryption and decryption method mentioned in the Figure 2 and procedure of the algorithm were as follows:

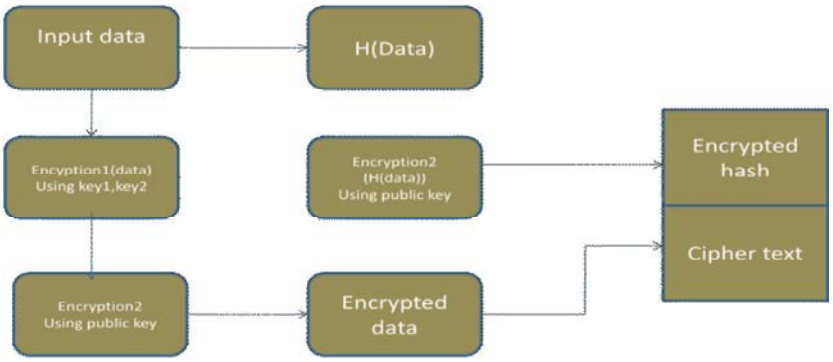

Fig. 2: Encryption method

Proposed Key Generation Steps:

- Select or create any private key of Size 64 bits.
- Divide 64 bytes into 4 blocks of 16 bytes likes Block1, Block2, Block3 and Block4.
- Apply XOR operation between Block1 and Block3. Results will store in new Block13.
- Apply XOR operation between Block4 and Block13.Results will store in new Block413.
- Apply XOR operation between Block413 and Block2. Results will store in new Block2413.
- Exit

Encryption 1:

- Compute Cipher text for each block of input data
- Assign integer value to an each block of input value.
- Generate Key 1 and Key 2 from a random generator.
- Multiply the key 1 with the plain text to get Cipher text 1.
- Add the key 2 to the cipher text 1 to get Cipher text 2.
- Perform modulus operation on cipher text 2 to get final Cipher text.

Encryption 2:

- Select n × n square matrix.
- Select any integer value say e.
- Make plain text as blocks according to the n matrix. And transpose all blocks.
- Multiply Plain text with selected square matrix and e value.
- Perform modulus operation with derived message.
- The remainder is the Cipher text.

Decryption Method:

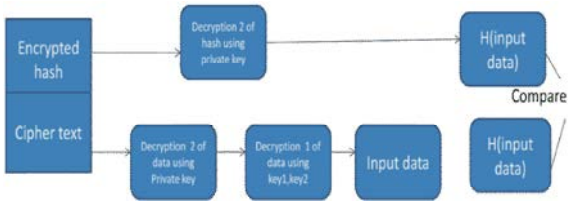

Fig. 3: Decryption method

Decryption 1:

- Compute Plain text for each block of input data
- Assign integer value to each block of cipher text.
- Obtain the Plain text 1 by subtracting the key 1 from the cipher text.
- Find the Inverse of key1. Multiply the inverse key to the plain text 1 obtained from step 3 to get plain text 2.
- Perform modulus operation on plain text 2 to get final Plain text.

Decryption 2:

- Receiving Cipher text and square matrix n'.
- Arrange encrypted message as n blocks.
- Calculate with cipher text using square matrix n' and private key e'.
- Perform modulus operation with calculated message.
- The remainder value is called Plain Text.

RESULTS AND DISCUSSION

The encryption/decryption algorithm EECA is compared on the basis of execution time of algorithm. Table 1 shows the results of time consumed by the various algorithms [9]. It illustrates the execution time in milliseconds taken by each algorithm to encrypt/decrypt the message of various different sizes mentioned in Table 2 and Figure 4 & 5 below. The graph shows that the proposed EECA algorithm takes minimum time to execute than RSA, DES and AES. The overall performance evaluation of RSA, DES, AES and new proposed EECA algorithm are mentioned in Figure 4 and Figure 5.

Implementation: Encryption is the formal name for scrambling program. The normal data, unscrambled, called plaintext or clear text and transform them so that unintelligible to the outside observer, the transformed data is called enciphered text or cipher text. Using encryption security professional can virtually nullify the value of an interception and the possibilities of effective modification and fabrication. Encryption is clearly addressing the need for confidentially of data [10]. Additionally, it can used to ensure integrity, that the data cannot be read generally cannot be easily changed in the meaningful manner. The following figure shows the EECA Algorithm encryption time and decryption time.

Table 1: Key generation timing of algorithm

Algorithm	Key generation time
RSA	6 Sec
DES	12 Sec
AES	8 Sec
Proposed EECA Algorithm	4 Sec

Table 2: Comparison of Data Execution Time

No. of Bits	RSA	DES	AES	Proposed EECA Algorithm
50	270 ms	245 ms	250ms	210 ms
75	290 ms	280 ms	275ms	260 ms
100	310 ms	300 ms	305ms	290 ms
200	400ms	395 ms	390ms	350 ms

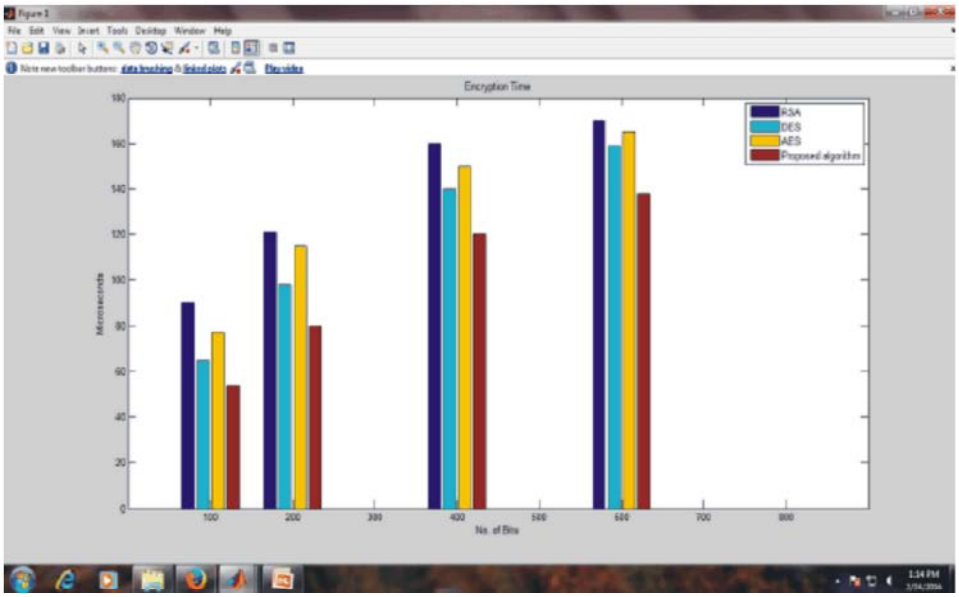

Fig. 4: EECA Encryption time

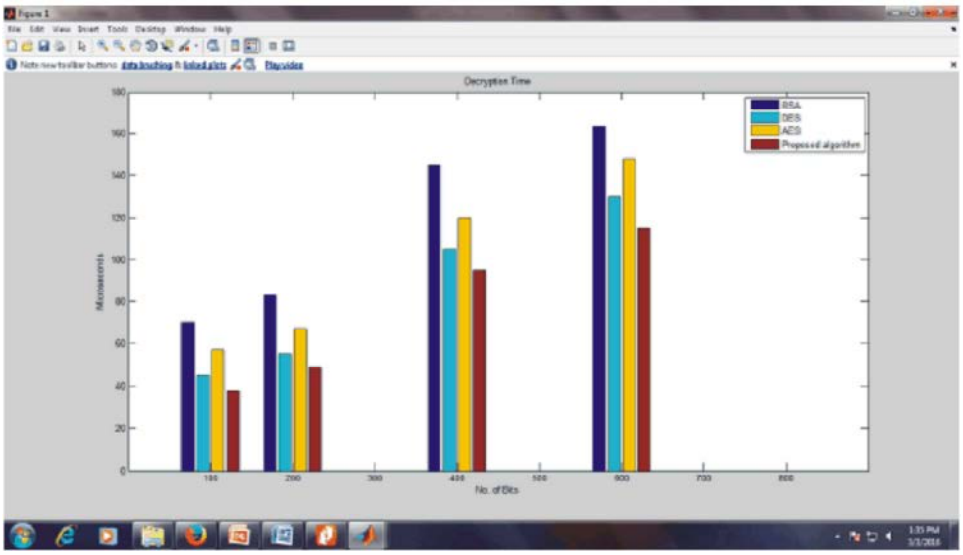

Fig. 5: EECA Decryption time

CONCLUSION

A new security algorithm EECA has been designed for better security. It provides three cryptographic primitives– integrity, confidentiality and authentication. The encryption and decryption of any data has a secure key, which is used for data encryption. For this purpose both symmetric and asymmetric keys are used. The result of the proposed EECA algorithm shows that processing time is more efficient than other algorithms. Thus the proposed EECA Encryption Algorithm provides a more secure and convenient technique for secure data transmission for all kind of application. The result of the research plan shows that processing time for encryption and decryption is more efficient than other algorithms.

REFERENCES

1. Ritika Chehal and Kuldeep Singh, 2012. Efficiency and Security of data with symmetric Encryption Algorithms, International Journal of Advanced Research in Computer Science and Software Engineering, 2(8): 2277-128X.

2. Sonal Sharma, Prashant Sharma and Ravi Shankar Dhakar, 2011. RSA algorithm using modified subset sum cryptography, IEEE transaction on Computer and Communication Technology, pp: 457-461: 978-1-4577-1385-9.
3. Darpan Anand, Vineeta khemchandani and Rajendra K. Sharma, 2013. Identity-Based Cryptography Techniques and Applications, IEEE Computer Society on Computational Intelligence and Communication Networks, pp: 343-347: 978-0-7695-5069-5.
4. Gerand Murphy, Aidan keesan,Rachit Agarwal and Emanuel popovici, 2006. Hardware-Software Implementation of public-key cryptography for Wireless Sensor Networks, IEE Insh Signals and systems conference, Dublin, pp: 1-6.
5. Ashwak M. ML-Abiachi, Faudziah Ahmad and Ku Ruhana, 2011. A Competitive study of Cryptography Techniques over Block Cipher, pp: 415-419: 978-1-61284-705-4.
6. Jingjing Lan, Wang Ling Gah, Zhi Hui kong and Kiat seng Yeo, 2010. A random number generator for low power cryptographic application. IEEE transaction on SoC design Conference, pp: 328-331: 978-1-4244-8633-5.
7. Yong Wang, Garhan Attebury and Byrav Ramamurthy, 2006. Survey of Security Issues In Wireless Sensor Networks, IEEE Communications Surveys & Tutorials, pp: 223-237.
8. Mohd. Rizwan beg1 and Shish Ahmad, 2012. EnergyEfficient PKI Secure Key Management Technique in Wireless Sensor Network using DHA & ECC, International Journal of Ad hoc, Sensor& Ubiquitous Computing (IJASUC) 3(1): 256-262.
9. Quist-Aphetsi kester, 2013. A cryptographic algorithm based on words database, International Journal of science, Engineering and Technology Research, 2(4): 969-973:2278-7798.
10. Haifaa Abd Al-Zahra Atee, 2011. Applying & Evaluation Cryptography Files using symmetric Cryptography Algorithms of Block Cipher Type, Al-Mustansiriyah J. su, 22(5).