ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Secured Transmission in cloud based Wireless Sensor Network Using Enhanced Tiny Encryption Algorithm (ETEA)

Balamurugan, B., Venkata Krishna, P., Rajya Lakshmi, G.V., Anusha, K.

School of Information Technology and Engineering, VIT University, Vellore, Tamil Nadu, India.

ARTICLE INFO

Article history:
Received 12 November 2014
Received in revised form 26 December 2014
Accepted 29 January 2015
Available online 10 February 2015

Keywords:
Cloud computing, Tiny encryption algorithm, linear feedback shift register, wireless Sensor networks, and energy consumption.

ABSTRACT

Several Critical applications like military, health monitoring and home automation use Wireless Sensor networks (WSN) in their design for communication to control processes in real time. Due to the distributed nature of these networks, the communication in the networks is vulnerable to the interception. Therefore, Cryptography is essential for secure communication. But in WSN, energy consumption plays a vital role as sensors are degradable energy devices making the existing security schemes and techniques incompatible. We consider the lightweight cryptographic techniques that allow the sensor devices to use less energy compared to regular cryptographic techniques. One of the simplest and hard to break algorithms of Light Weight algorithms is the Tiny Encryption Algorithm (TEA). However, TEA has few weaknesses and this project proposes an enhancement to the original Tiny Encryption Algorithm by making use of Linear Feedback Shift Register to improve its robustness. Another challenge in WSN is its vast data generation by sensors placed on different locations. To accommodate the ever increasing data avalanche and process it, cloud storage is utilized for WSN.

To Cite This Article: Balamurugan, B., Venkata Krishna, P., Rajya Lakshmi, G.V., Anusha, K.., Secured Transmission in cloud based Wireless Sensor Network Using Enhanced Tiny Encryption Algorithm (ETEA). ***Aust. J. Basic & Appl. Sci.,*** *9(6): 30-33, 2015*

INTRODUCTION

Wireless sensor networks (WSN) is framed through the distributed wireless network of sensing and computation nodes for gathering information frequently without any infrastructure .Its measured for its Battery-power in wireless communication, as battery lifespan is the central concern. Sensors sense the environment for signal, eventually converting them in to a form that can be stored and processed for any outcome. They work collaboratively to process the data and communication which is necessary for data processing (Aitsaadi, N., 2010). As specified earlier, due to the distributed nature of these networks, the communication in the networks is vulnerable to interception. Concerning the security of wireless sensor networks, there are several attacks and vulnerability as it communicates the information through Internet. Wireless sensor network application constitutes many application for instance automobile application challenges to be in endeavor. Sensor measures the attributes such as Distance, Direction, and Speed in a real time application like Military Information Integration, Habitat monitoring Application. In addition the humidity, soil makeup, temperature, chemicals, light, vibrations, motion are calculated with the help of wireless sensor network in farmland cultivation. The Seismic data, Acoustic data were crucial components in the health application to manipulate huge data storage efficiently. The accuracy and integrity of the depends upon the adequacy and capacity of the sensors. Wireless sensors networks deployed in military are used for critical and emergency purposes, any breach of communication will lead to disaster.

We encounter the constraints with the cloud service Infrastructure (IaaS) it has the capacity given to nodes is to provision processing, networks, storage and basic resources where the client is capable of deploying and running the software, which can even include interface between hardware and software and further application software's. Cloud computing is a collective framework which enables easy on-demand network access to a common pool of computing resources like networks, applications, services and storage which can be any time provisioned and used with minimal management effort or a service provider support. These types of cloud services bolsters availability and comprises of necessary characteristic as broad net work access, resource pooling, and rapidly elasticity and it possess service models. As a multitenant facility, the cloud brings

Corresponding Author: Balamurugan, B., School of Information Technology and Engineering, VIT University, Vellore, Tamil Nadu, India.

unique challenge to maintaining security, data integrity, and clean operation. Different customers, perhaps competitors, sit on the same physical server, separated by the logical boundaries of a virtual machine.

The cryptanalysis is technique of analyzing and breaking cipher, so it can be multiethnic process for secured transmission in the wireless sensor network; it cracks to take cipher text provided by adversary, and given by the plaintext. We analyze the strength of encryption with the help of symmetric algorithm where it categorizes into stream ciphers and block ciphers. It encode single bit of plain text at a time, whereas block ciphers consider a number of 64 bits and generate keys. There are many light weight algorithms, the Tiny Encryption Algorithm being the simplest algorithms, which is a block cipher. It is cryptographic algorithm designed to reduce the space complexity and maximize speed.

Literature Survey:

Energy consumption in Wireless sensor Network is directly proportional to the number of process it can complete in a particular time. Security in WSN is considered to be an overhead in terms of energy consumption. Reducing the processes of WSN is the primary goal; hence, efficient security algorithm is in a great demand (Yajie Ma, 2013). The performance and QOS (Quality of Service) of the WSN is based on the maximum TTL (Time To Live) of each node using an high time complexity Cryptographic algorithm for Encryption/Decryption will reduce the longevity of the node exponentially (Alaus, L., 2009). Lighter algorithms on the other hand will lead to security failures leading to disaster, as WSN are used for deploying critical applications. Public-key cryptosystems consists of several phases that occur concurrently or successively and each of the phases leads to complexity of the entire algorithm (Abdelhalim, M.B., 2000) the security properties like computational efficiency, time bounding, binding of functionality can be found out by measuring the cryptosystems. Cryptanalysis is done on every algorithm to find out its efficiency and time and space complexity. Wireless sensor networks generates huge volume of data every second. In critical applications all the sensor generated data must be retained as historical data ,as it might be helpful for future decisions. Information management in wireless sensor networks has become hectic, as information is created every second in gigabytes (L'Ecuyer, P., F. Panneton, 2000). The advent of cloud will facilitate the data management in WSN LFSR (Linear Feedback Shift Register) has several operations and can be applied in several field of engineering for generating pseudo-random variables with the aid of an irreducible polynomial. The combination of LFSR with other cryptographic algorithms will lead to an improved version in terms of complexity (execution time, area)(Sad, *et al*., 2013).

Proposed Work:

Tiny encryption algorithm (TEA) function using two 32-bitunsigned integers and generates into a 128-bit key and 64bit blocks. It has a Feistel structure of 64 rounds, typically implemented in pairs named as cycles. It has a particularly simple key schedule, combining all of the key material in a proper way for each cycle. Based on the symmetry of the rounds, the various multiples of a magic constant are used to prevent simple attack. The magic constant, 9E3779B9 16 is chosen to be 2^{32} ∅, where ∅ is called the golden ratio. However, in the proposed algorithm, the number of rounds was reduced to 32 to preserve the energy of the sensors considering the power constraints of the wireless sensor networks. Also, a Linear Feedback Shift Register is used to improve the strength of the encryption algorithm. TEA has few limitations. As markedly, it suffers from equivalent keys with the each key is equivalent to three others, it states that the effective key size is only 126 bits. As a result, TEA is not potential using hash function in cryptographic.

To overcome the security threat we use linear feedback shift register (LFSR).LFSR is a shift register whose each input bit is a linear function of its previous state. The frequently practiced linear function of single bit is XOR gate. Hence, an LFSR is effective to use as shift register whose input bit is considered by the exclusive-or (XOR) of some bits of the overall shift register value. Values are obtained from LFSR at different intervals firstly we get a value named seed. In addition, there are 'n' number of finite states is registered and repeats the cycle in the linear function. However, an LFSR with aproper feedback function can produce a sequence of bits which appears random that has a long in a cycle. We use many key generators for making TEA more secured. The Enhanced Tiny Encryption Algorithm (ETEA) has advantages as the number of passes is reduced; hence, the total time taken for completion of the Encryption/Decryption process is reduced. The whole process of the secure data communication between the sensor nodes and base station is synchronized, ETEA as it maintains the session time for each communication.

Linear Feedback Shift Register:

TEA-LFSR is designed to generate 32 different keys from a single key using a PRNG called Feedback shift register. The shift register shifts every bit to right every time it generates a key and performs a XOR on the first two bits and the resultant bit is the starting bit of the next key. This way, it generates 32different keys which will be used in the following modules of encryption and decryption.

Encryption:

In an encryption stage, the (plain text) input which is a message or information is encrypted using a modified generated encryption key, which specifies the process of how the message is to be encoded. This is a normal algorithm with the use of an encryption key which turns it into an Unreadable cipher text(ibid).Other unauthorized user may be an adversary that can see the cipher text , it should not be able to define the information about the original message. Here by, an authorized user is able to decode the cipher text using a decryption algorithm that requires a secure decryption key that adversaries do not have access. As a traditional method for an encryption scheme does the key-generation algorithm to randomly produce keys .The proposed algorithm is designed to take a block of data given for encryption and make it go through the Feistel pair of cycles for 32 rounds, in which for each round, a different key is used which are generated. Finally it integrates the blocks of ciphered data and returns it to the user and it is explained as:

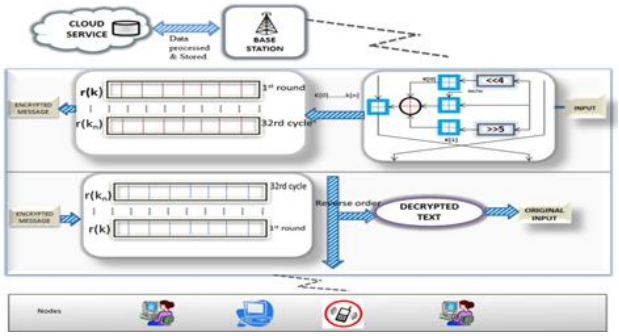

Fig. 1: Enhanced Tiny Encryption Algorithm in Wireless Sensor Networks.

Tiny Encryption with LFSR:

The inputs to the encryption algorithm are a plaintext block and a key K.

The plaintext is P = (L [0], R[0]) and the cipher text is C = (L [64], R [64]).

The plaintext block is divided into two parts, L [0] and R[0]. Each part is used to encrypt the other half over 64rounds of processing and then integrate to produce the cipher text block. Each round i has inputs L [i-1] and R [i-1], resulting from the previous round, as well as a sub key K[i] resultant from the 128 bit overall K. The sub keys K[i] are varied from each other. The key generation F is defined by,

F (Ki) = ((M << 4) K[j]) ⊕ (M delta[i]) ⊕ ((M >> 5) K[k]).

The algorithm is modified with linear feedback shift register(LFSR), as it is called as a random function. Random function is defined by, R (keys) - keys are chosen randomly in the block by using XOR gates and generate an encrypted key in a sequence order. (i.e. E (k1, K2, k3…….k64)

Decryption:

This module takes the ciphered text given from the previous module and decrypts it into deciphered text using the same keys used by the encryption module which are generated by LFSR. It follows the Feistel structure followed by the encryption module in reverse order. It integrates the generated blocks of deciphered or the plain text and returns it to the user.

D(Kj) = E(K2j) ; j = 32; 31….. 1.Define the Communication map C by C: BS* BS → N and C: N *N →BS, where BS is the Base station and N ∈Ni; i = 1; 2…… n is the nodes.

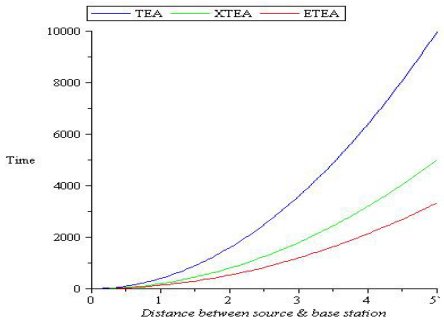

Fig. 2: Time Comparison of three algorithms.

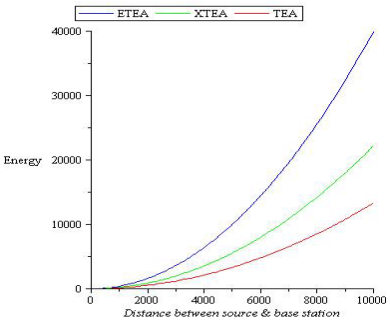

Fig. 3: Energy Comparison of three algorithms.

Let D = D 2 C and D = fBR$_1$,BR$_2$……BR$_m$ where D is the data and BR is the break operation. Again BR1 =τ_j ; j = 1; 2…… 32. Next j = kj ; j = 1; 2….. 64 where kj is defined by,

kj = ((τ_j<< 4)kj) ⊕ (τ_j[i]) ⊕((τ_j>> 5)k[j + 1])

where<< , >>, ⊕ are respective left shift, right shift and logical XOR operators and i; j are index. The Random function R (kj) ; j = 1; 2… 64 and R(kj) = E(k2j)
where E(kj) are encrypted keys and D(kj) = D(k2j) ; j =1; 2…… 32 where D(kj) are decrypted keys.Let dn be the distance between sensor and base station and assume dn be equidistance for n 2 Z+. Let ln be the size of the message from each sensor and again assume ln be equalsize for n € Z+. Let EETEA be the energy of the ETE Aalgorithm. Now the time taken for message from sensor to base station is given by,
$Time=d_n * l_n / E(_{ETEA})$

The experimental studies of ETEA Algorithm with that of XTEA and TEA algorithms by considering the respective energies 0.0075J, 0.0050J, 0.0025J it proves ETEA Algorithm takes minimum time from sensors node to base Station in Cloud environment which is shown in Fig 2.On the other hand, for the same three algorithms by assuming the Time 2500sec; 4500sec; 7500sec our ETEA Algorithm has more energy efficient which is shown in Fig 3.

Conclusion:

As specified in the literature, there are many lightweight algorithms suitable for the wireless sensor networks, considering it as resource-constrained network. Tiny Encryption Algorithm is one of the simplest in terms of processing time, but less efficient algorithm compared to other proven Algorithms like RSA and DES. The paper has overcome the limitations of TEA by enhancing it using LFSR and still maintaining its timeliness of encryption and decryption. Cryptanalysis is performed for the key attacks. The paper includes a random key generation method suitable for the Tiny Encryption Algorithm. Here, different key is used for a round and so making the algorithm more robust and making the cryptanalysis of the algorithm difficult. The improvement in the strength of the algorithm against the cryptanalysis makes the power consumption tolerable, while the usage of the algorithm can be migrated from a lower level secure wireless sensor networks to a medium level secure wireless sensor networks. The paper deduces an efficient yet fast security algorithm for WSN.

REFERENCES

Abdelhalim, M.B., M. El-Mahallawy, M. Ayyad, A. Elhennawy, 2000. ”Implementation of a modified lightweight cryptographic TEA algorithm inRFID system,” Internet Technology and Secured Transactions (ICITST).

Aitsaadi, N., N. Achir, K. Boussetta, G. Pujolle, 2010. ”*Multi-Objective WSN Deployment: Quality of Monitoring, Connectivity and Lifetime*,”Communications (ICC), 2010 IEEE International Conference on, 1(6): 23-27.

Alaus, L., D. Noguet, Palicot, Jacques, 2009. *A new reconfigurable Linear Feed Back Shift Register organization to improve SDR design,”* Signals, Circuits and Systems (SCS), 2009 3rd International Conference on, 1(6): 6-8.

L’Ecuyer, P., F. Panneton, 2000. *A new class of linear feedback shift register generators,”* Simulation Conference, 2000. Proceedings. Winter, 1: 690-696.

Sad, *et al*., 2013. ”*Increasing network lifetime in an energy-constrained wireless sensor network*.”IJSNet 13(1): 44-56.

Yajie Ma, YikeGuo, Dilshan Silva, Orestis Tsinalis and Chao Wu, 2013. *Elastic Information Management for Air Pollution Monitoring in Large-Scale M2M Sensor Networks,”* International Journal of Distributed Sensor Networks, Article ID 251374, 14.