# Comparative Study of Security Algorithms in Wireless Transmissions

Rajarshi Godse, Jai Lohani, Devanshu Maratha and Tukaram Patil
Department of Computer
Engineering
Pimpri Chinchwad
College of Engineering
Pune, India

## ABSTRACT

Wireless networks and wireless sensor networks (WSNs) provide great benefits over the traditional approaches for several applications. These include smart homes, healthcare, environmental monitoring, and homeland security. WSNs can be integrated with the Internet Protocol (IP) to develop the Internet of Things (IoT) for connecting everyday life objects to the internet. Hence, major challenges of WSNs include:

- To efficiently utilize low-power nodes to implement security during data transmission among several sensor nodes.
- To resolve security issues during data transmission over a long coverage range.

Encryption is a vital process to ensure the confidentiality of the information transmitted over the insecure wireless channel.

In this paper, a study of various algorithms for secure wireless transmission was performed. To facilitate energy-efficient data encryption, a method based on efficient key generation mechanism was required. The proposed TBSA based system gives an outstanding performance by fulfilling all the necessary security requirements. The experimental results showed that the proposed TBSA algorithm consumed less energy in comparison with some other existing methods.

## General Terms

Wireless Transmission, Network Security, Data Transmissions.

## Keywords

Energy efficiency, Encryption, Decryption, AES, DES, SHA Algorithms.

## 1. INTRODUCTION

In a wireless network, one of the most important issues is how to securely transmit the data from the source to the appropriate destination. The cryptographic algorithms are a means of transferring the secret information between one party and another. In general, a plain text message is encrypted using a cryptographic algorithm. Through encryption, the original message becomes cipher text and it's original content is completely protected. This is done by the help of the cipher key. The cipher text can then be sent safely to the recipient. When the recipient is ready to reveal the message, he or she can do so by applying a decryption algorithm, which will reveal the original plaintext. Only the recipient can apply the decryption algorithm because, ideally, only the recipient knows the keys necessary for decrypting the cipher text. Keys are used to personalize and secure a cryptographic algorithm to only the sender and recipient.

In WSNs, nodes have limited resources such as:

- restricted power supply
- limited memory
- limited data processing capability

The existing techniques (such as AES, DES etc) are not precisely developed by keeping in view the specification of WSNs.

So these methods require more energy for their implementation. Hence, security algorithms which could consume less energy for data encryption should be utilized in order to make efficient use of available resources.

Energy-efficient security algorithm implementation is based on :

- Efficient key generation mechanism for data encryption
- Capability of network to support communication among large no. of nodes
- Wide coverage range.

Hackers are on the rise since it is very easy to intercept data during wireless transmission. Hence, highly secured wireless systems need to provide a balance between level of security, and energy efficiency.

### 1.1. Requirements of Security:

**Authentication:**
Basically, authentication permits the destination node to verify if the information was transmitted from the appropriate source node.

**Trustworthiness:**
It is the ability of a system to authenticate the identity and ascertain trust in a third party.

**Data Freshness:**
Data freshness implies that the information is fresh and nobody can replay old information.

**Confidentiality and Privacy:**
Confidentiality refers to the state of keeping secret.

Privacy refers to the state of being free from public attention.

**Secure Localization:**
The secured localization is very important for tracking the actual source node for data transmission.

**Integrity:**
An integrity mechanism is very significant to protect the original data from external attacks.

**Non-Repudiation:**
It is the ability of a system to validate occurrence or non-occurrence of an action from the source nodes.

**Availability:**
This property allows reliable access of system resource in timely manner to valid nodes in the network. It is very essential that network resources should be available to the appropriate nodes.

**Access Control:**
To keep out potential attackers, it is needed to recognize each user and each device so as to enforce security policies. Therefore, noncompliant sensor nodes within the network need to be blocked or given only limited access. This process is known as network access control (NAC).

To develop a secured system, it is extremely crucial that the system should fulfill all the above mentioned security requirements that could oppose different security attacks like replaying, data modification, impersonation, and eavesdropping among others.

## 2. RELATED WORK

**Hash Functions**
A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes.

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. Some well-known hash functions are MD4, MD5, SHA-1 and SHA-2.

## 3. GOALS AND OBJECTIVES

The main goal of the study is to facilitate a secure wireless transmission system. Furthermore, the most suitable algorithm should be selected based on the application and level of security required. An algorithm is selected based on its energy efficiency and its level of complexity.

## 4. ALGORITHMIC SURVEY

### 4.1. SHA Algorithm

This Algorithm uses the hash functions to generate the key value pair. A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes. One use is a data structure called a hash table, widely used in computer software for rapid data lookup. Hash functions accelerate table or database lookup by detecting duplicated records in a large file.

### 4.2. DES Algorithm

DES is a block cipher. It encrypts the data in a block of 64 bits. It produces 64 bit cipher text. The key length is 56 bits. Initially the key is consisting of 64 bits. The bit position 8, 16, 24, 32,40,48,56, 64 discarded from the key. DES is based on two fundamental attributes of cryptography: Substitution (confusion) and transposition (Diffusion). DES consists of 16 steps, each of which called as a Round.A basic flow within the algorithm can be given by the figure

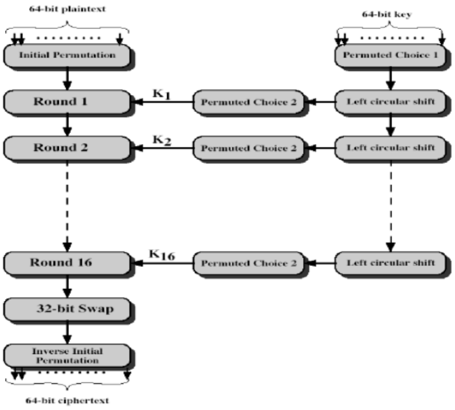

**Figure 1- Working of DES algorithm**

### 4.3. AES Algorithm

The basic unit for processing in the AES algorithm is a byte (a sequence of eight bits), so the input bit sequence is first transformed into byte sequence. In the next step a two dimensional array of bytes (called the State) is built. The State array consists of four rows of bytes, each containing Nb bytes, where Nb is the block size divided by 32(number of words). All internal operations (Cipher and Inverse Cipher) of the AES algorithms are then performed on the State array, after which its final value is copied to the output (State array is transformed back to the bit sequence).The input and output for the AES algorithm each consist of sequences of 128 bits (digits with values of 0 or 1). These sequences will sometimes be referred to as blocks and the number of bits they contain will be referred to as their length. The Cipher Key for the AES algorithm is a sequence of 128, 192 or 256 bits. The AES algorithm consists of ten rounds of encryption. First the 128-bit key is expanded into eleven so-called round keys, each of them 128 bits in size. Each round includes a transformation using the corresponding cipher key to ensure the security of the encryption. After an initial round, during which the first round key is XORed to the plain text (Addroundkey operation), nine equally structured rounds follow.The basic design of the AES Algorithm is shown below.

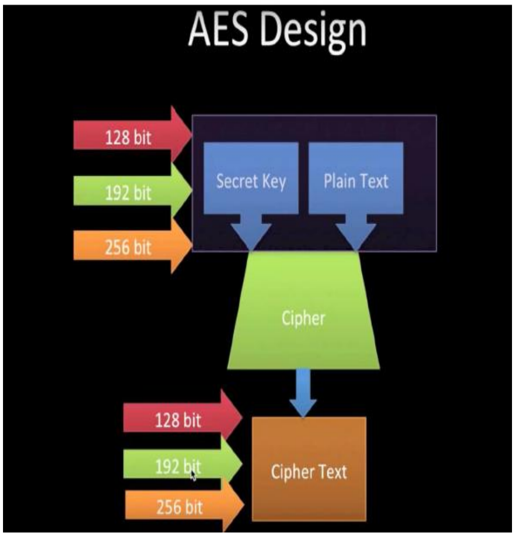

**Figure 2- Design of AES algorithm**

## 4.4. Triangle Based Security Algorithm (TBSA)

It is based on efficient key generation mechanism and facilitates energy-efficient data encryption. It is based on the non-right angle triangle key generation procedure.

The authentication key (K) generated is used to provide unique authentication for data transmission.

### 4.4.1. Methodology for Implementation

Consider a node that transmits the data collected at time (t).Consider the node’s unique identification (ID) is represented as (u). Consider a triangle STU, which does not include a right angle. ‘t’ and ‘u’ are acting as

two sides of the STU triangle as shown. Addition of these two i/p values divided by 2 is acting as the corresponding angle (α) for the third side (s) of triangle STU.

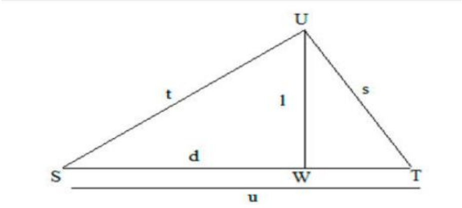

**Figure 3- Triangle STU used for key generation**

The encryption for the TBSA takes in M, K, t and u, and generates the cipher-text C by using Equation (1)

$$C = (u \oplus t)*M/K \qquad (1)$$

The receiver performs decryption on C to obtain M by using Equation (2).

$$M = C* K/(u \oplus t) \qquad (2)$$

The key generation mechanism is shown below.

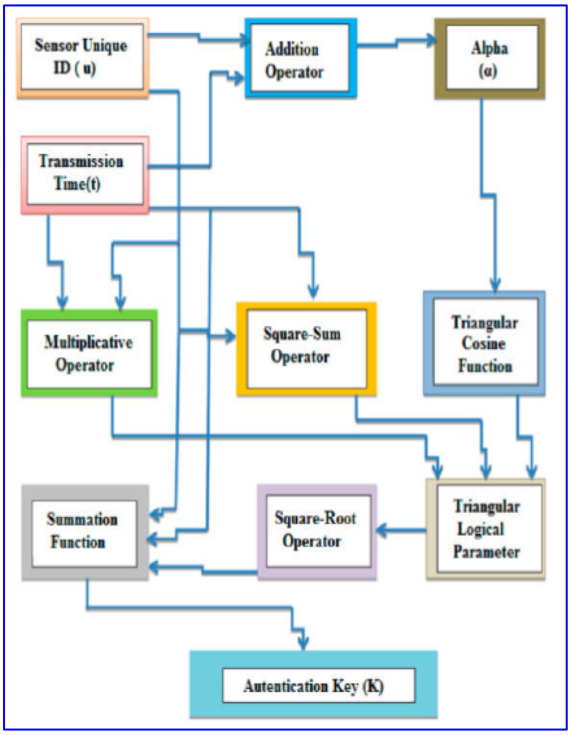

**Figure 4- Key generation mechanism**

### 4.2.2. Applications:

- The TBSA Algorithm is used where symmetric encryption is required.
- It can be used in household applications such as home automation systems.
- It can be used in WSNs for applications such as health monitoring, assisted living, etc

## 5. COMPARATIVE ANALYSIS

Among all the algorithms that we have discussed so far, each algorithm is unique in its own way. Some algorithms focus more on the security aspects while there are some other algorithms that focus on the energy efficiency parameters. It depends on the user which algorithm he/she wants to use for the efficiency in the data transmission.

The given table compares the algorithms with respect to the key sizes, speed and security.

**Table 1- Comparison of various algorithms**

| Algorithm | Key Size | Speed | Speed Depends on Key | Security |
|---|---|---|---|---|
| DES | 56 bits | Slow | Yes | Insecure |
| AES | 128,192, 256 bits | Fast | Yes | Secure |
| TBSA | Unique for each node | Fast | Yes | Insecure |

As there are several areas such as IOT where there are many nodes in the network and they transmit the data within the network. Here the power consumption is an important aspect as compared to the security in transmission.[3]

**Table 2- Energy consumption comparison of various algorithms**

| Method | Energy Consumption (Microjoules/byte) |
|---|---|
| SHA | 0.76 |
| DES | 2.80 |
| AES | 1.80 |
| TBSA | 0.20 |

So an Algorithm which transmits data with least energy consumption should be used. The table shown above shows the comparison with respect to Energy Consumption.[11]

## 6. CONCLUSION

In Wireless Networks, because of the limited computational power of nodes, an efficient security mechanism based on effective key generation mechanism which could accomplish all major data security requirements and consumes less processing time for data encryption is well needed. The proposed algorithm TBSA is based on a simple and efficient key generation procedure. Although it is less secure as cipher length is same as message length and the aattacker may determine the key by capturing the node's unique ID, it is suitable for some specific applications such as home automation system and assisted living.

Hence, the TBSA is the most energy-efficient algorithm for data encryption than all the compared approaches.

## 7. REFERENCES

[1] Raj, S. Pravin, and A. Pravin Renold. "An enhanced elliptic curve algorithm for secured data transmission in wireless sensor network." In *Communication Technologies (GCCT), 2015 Global Conference on*, pp. 891-896. IEEE, 2015.

[2] Prema, G., and S. Natarajan. "An enhanced security algorithm for wireless application using RSA and genetic approach." In *Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on*, pp. 1-5. IEEE, 2013.

[3] Pirbhulal, Sandeep, Heye Zhang, Md Eshrat E Alahi, Hemant Ghayvat, Subhas Chandra Mukhopadhyay, Yuan-Ting Zhang, and Wanqing Wu. "A Novel Secure IoT-Based Smart Home Automation System Using a Wireless Sensor Network."*Sensors* 17, no. 1 (2016).

[4] Karsanbha, Gohil Rikitaben, and Mary Grace Shajan. "AES Algorithm for Secured Wireless Communication." In *National Conference on Recent Trends in Engineering & Technology*, pp. 13-14. 2011.

[5] Katkade, Pradnya, and G. M. Phade. "Application of AES algorithm for data security in serial communication." In Inventive Computation Technologies (ICICT), International Conference on, vol. 3, pp. 1-5. IEEE, 2016

[6] Savitha, S., and S. Yamuna. "Implementation of AES algorithm to overt fake keys against counter attacks." In Computer Communication and Informatics (ICCCI), 2016 International Conference on, pp. 1-5. IEEE, 2016.Plagiarism Check Report.

[7] Alexandru-Corneliu Olteanu*, George-Daniel Oprina*, Nicolae ğăpuú* and Sven Zeisberg,"Enabling mobile devices for home automation using ZigBee".2013 19th International Conference on Control Systems and Computer Science

[8] Luigi Coppolino , Valerio D'Alessandro , Salvatore D'Antonio , Leonid Lev † and Luigi Romano , " My Smart Home is Under Attack" 2015 IEEE 18th International Conference on Computational Science and Engineering.

[9] Makkad, Ritu Kaur, and Anil Kumar Sahu. "Novel design of fast and compact SHA-1 algorithm for security applications." In *Recent Trends in Electronics, Information & Communication Technology (RTEICT), IEEE International Conference on*, pp. 921-925. IEEE, 2016.

[10] Ratna, Anak Agung Putri, Prima Dewi Purnamasari, Ahmad Shaugi, and Muhammad Salman. "Analysis and comparison of MD5 and SHA-1 algorithm implementation in Simple- O authentication based security system." In *QiR (Quality in Research), 2013 International Conference on*, pp. 99-104. IEEE, 2013.

[11] Bhanot, Rajdeep, and Rahul Hans. "A review and comparative analysis of various encryption algorithms."*International Journal of Security and Its Applications* 9, no. 4 (2015): 289-306.