WIRELESS COMMUNICATION WITHOUT PRE-SHARED SECRETS USING SPREAD SPECTRUM TECHNIQUE

Bhagyashree.G[1], T.S.Vishwanath[2]

[1]*M. TechScholar, E&CE dept., BKIT, Bhalki. Karnataka, India, email-* ***bhagyagc27@gmail.com***
[2]*Prof. Department of E&CE, BKIT, Bhalki, Karnataka India, email-* ***tsvrec1@yahoo.com***

Abstract

The wireless communication using spread spectrum relies on the assumption that some secret is shared among source and destination node before communication or transmission has started. This problem is called the circular dependency problem (CDP). This CDP exists in large networks, where nodes frequently join and leaves the network. In this work we have introduced an efficient and reliable mechanism called Advanced Encryption Standard (AES) Algorithm, to overcome circular dependency problem (CDP). This is an efficient algorithm to make successful transmission of data without pre-sharing any secret key. We have evaluated this by simulation in Matrix Laboratory (MATLAB).

Keywords: -*Spread spectrum, CDP, AES and MATLAB.*

----------***----------

1. INTRODUCTION

The Wireless sensor network is a group of specialized transducers with communications infrastructure for monitoring and recording conditions at diverse locations. It provides a bridge between the real physical and virtual worlds. Wireless sensor network consists of three main components: nodes, gateway and software.
Privacy has been the most important issue in wireless communication, using a spread spectrum can avoid the problem for some extent. Spread spectrum is a form of wireless communication in which the frequency of the transmitted signal is deliberately varied.
In this work we are going to propose the system with less or negligible security issues using Advanced Encryption Standard algorithm in a wireless sensor network with the spread spectrum communication.

Key properties of this project has been depicted as follows

- Presence of energy usage overhead is nil.
- Loss of data is completely removed.
- Efficient communication in terms of time, bandwidth and security.
- Receiver synchronization is not required.
- Real time Spread-spectrum communication at 100 mega chips per second over a 200 MHz bandwidth.
- No need of key establishment before communication has started.

Using AES algorithm makes the communication more reliable than any other algorithm. And it is also an improved version of older algorithms.
Implementation of this work is analyzed in simulation graphs obtained from MATLAB.

2. SYSTEM MODEL

Communication nodes in a network share the same medium with adversary (opposition). In this section we described the goals, types of participants and assumption we made in this work.

A. Communication and adversary

We considered the wireless sensor network with some fixed number of nodes,which included source, adversary or jammer, routing and destination nodes. Under our system a jammer was within the range of sender and receiver and could possibly add or modify some bits of message, could jam and reply with previously collected message.
We have evaluated the jammer in terms of the delay occurred by its attacks at the process of receiver decoding.
We considered some attacks by the jammer in the system; they were jamming, replay attack, modification, and insertion. Which we discussed in detail before.

B. Assumptions

Every communication either wired or wireless communication makes some assumptions, like wise wehave made some assumptions in this work, are follows,

- The sender, jammer and receiver share the same channel and information like MAC address, key length, communication protocol and encoding/decoding scheme.
- We consider that the jammer will not block the message completely.

3. ARCHITECTURE

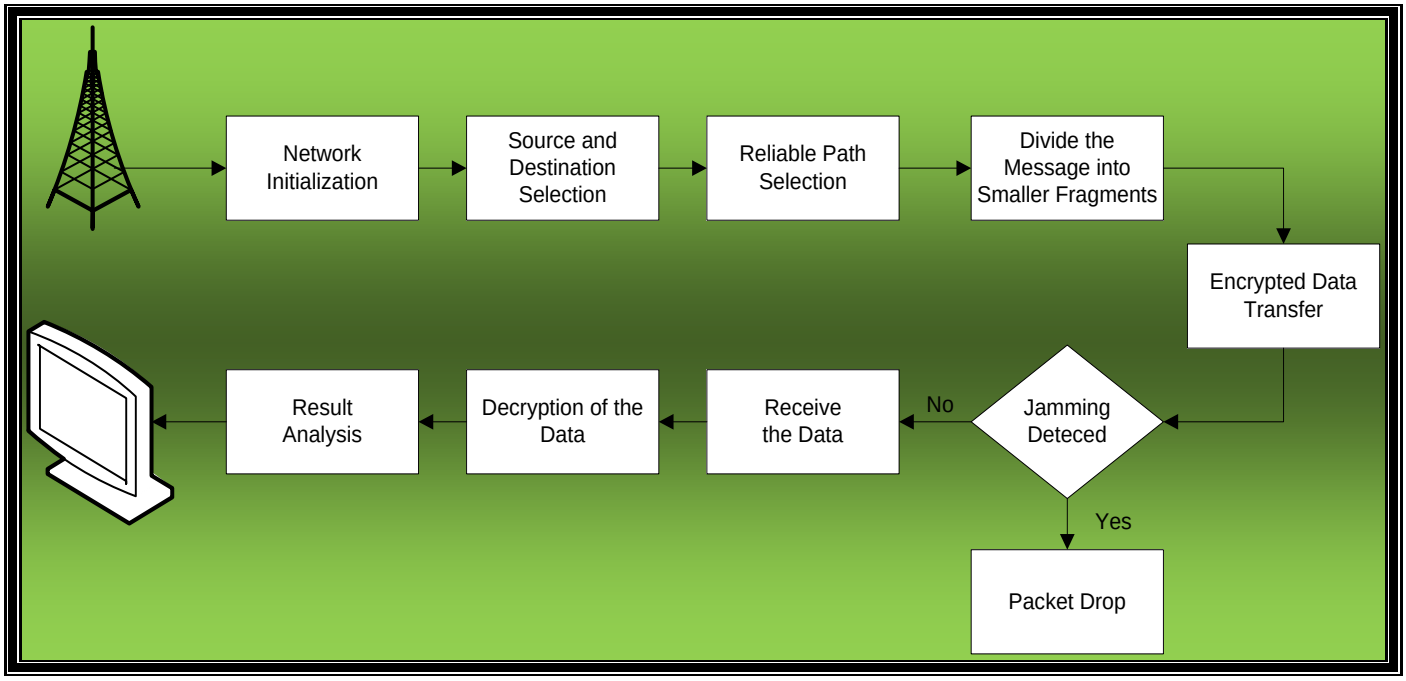

Figure 1: Block diagram for proposed system

This is a system architecture which we are going to run by implementing on MATLAB simulation. As we can see in above figure it includes some stepwise procedure to be followed. The steps which involve in this model are as follows,

- Network initialization.
- Source and destination selection.
- Data encryption.
- Reliable path calculation.
- Detection of jammer.
- Decryption of data.
- Result analysis.

4. ADVANCED ENCRYPTION STANDARD

Cryptographic methods are of two types symmetric and asymmetric. Symmetric types of methods use only one key in encryption and decryption process.

An Asymmetric methods use more than one key to encrypt and decrypt the message. AES algorithm is asymmetric type of cryptography. AES uses 128 bit of key where as DES uses 64 bit key which is symmetric method.

The AES algorithm has ten round of encryption, each round includes following steps;

- Substitute bytes
- Shift rows
- Mixed columns
- Add round key

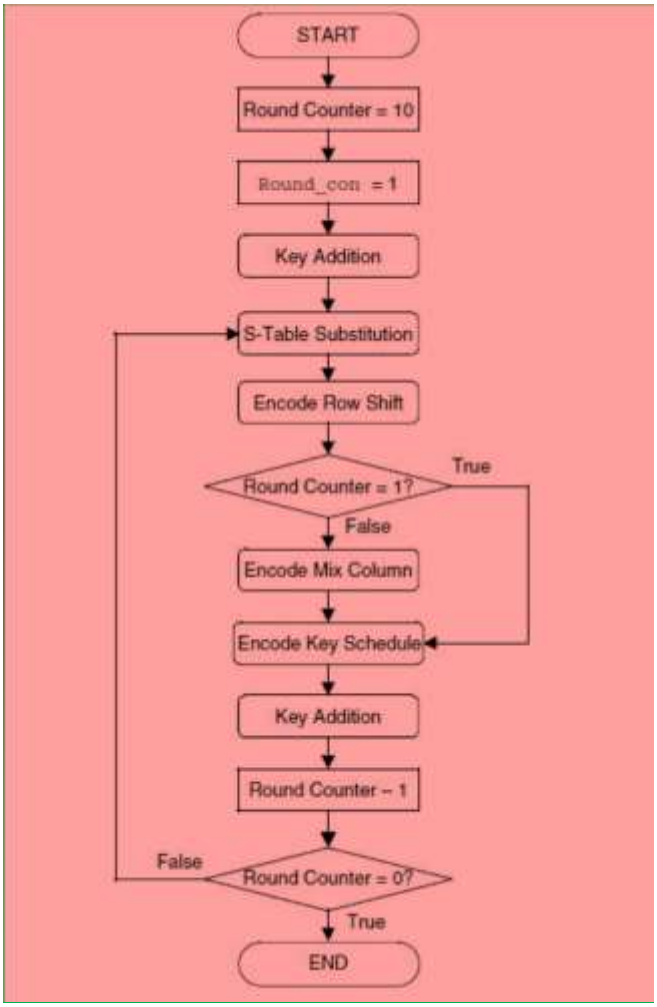

Figure 2: AES flow chart

AES has a simple procedure to follow, the methods are processed step wise can be illustrated as follows

1. Subbyte is considerd as a lookup in a table. Lookup tabble helps to substitute the 16 byte input data which are substituted by the curresponding values found in the table.
2. Shift rows operation pocesses rows, a simple rotate with a different rotate width is performed.
3. Mixed column operation is opposite to shift rows. It pocesses o columns. Transformation in the cipher that takes all of the columns of the state and mixes their data to produce new column.
4. Add round key is a simple process. The curresponding bytes of the input data and expanded key are XORed.

5. SIMULATION RESULT ANDDICUSSION

The implementation of AES using Matlab simulation results in simulation results as

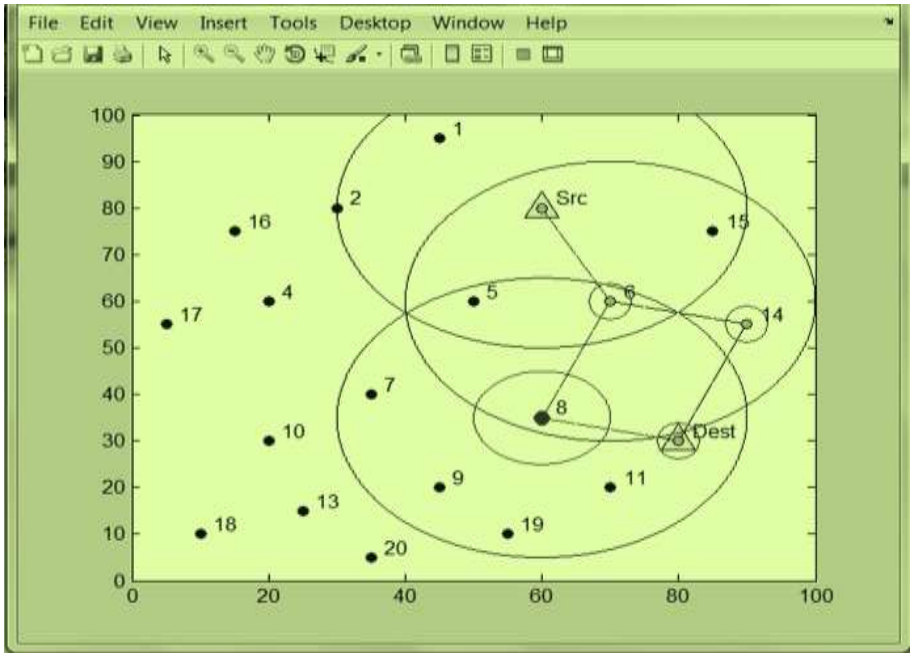

Figure 3 : The first figure shows the simulation result for the transmission of data in two paths one with jammer and another without jammer.

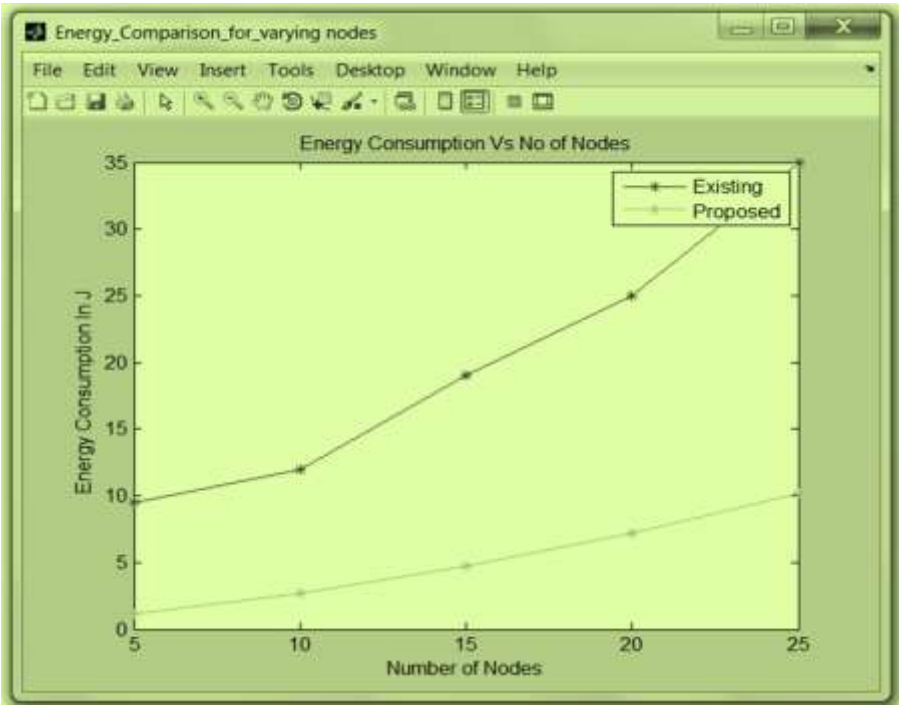

Figure 4: The graph shows the results of comparision of energy consumssion v/s number of nodes.this gives us the evrage of enegy used.

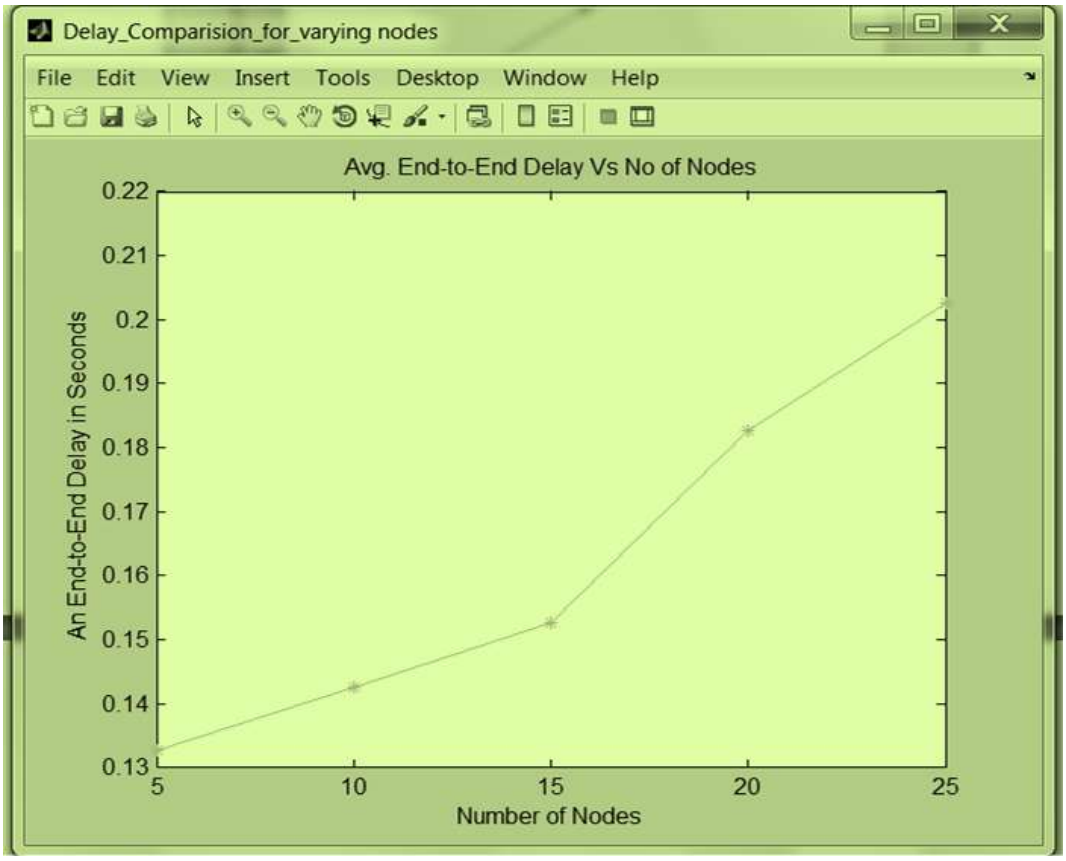

Figure 5: This result shows the graph with end-to-end delay in Y-axis and number of nodes in X-axis.this result is a comparision between end-to-end delay and number of nodes in the wireless sensor nwtwork.

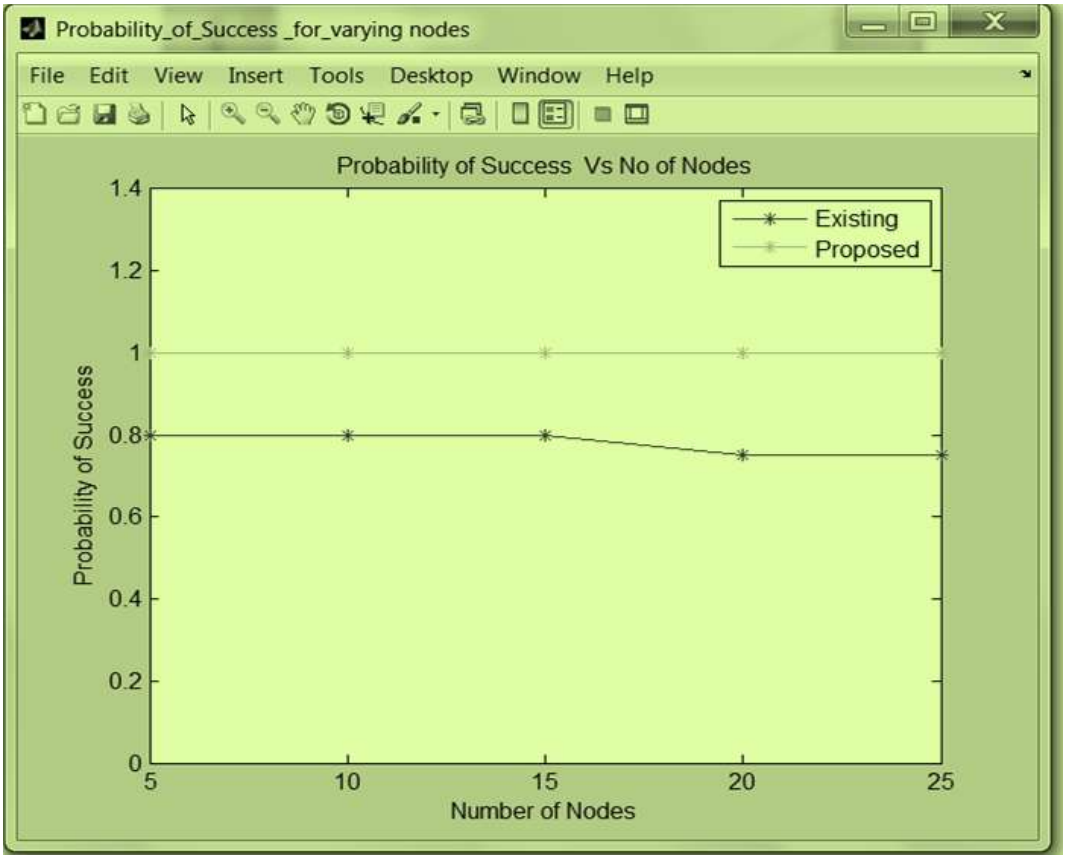

Figure 6: This graph has probability of success of the proposed work at Y-axis and number of nodes present in the network at X-axis.Also shows the existing and proposed results comparision.

All these simulation results displays the performance of proposed work interms of energy,time and security.
Thse results also compares the existing and proposed work result which makes the user to know which is more efficient method to use. Analyzation of these simulation results conclude dat AES (Advanced Encryption Standard) is a better algorithm than any other existig method in tems of efficiency including security.

6. CONCLUSION

The propsed work lasts with accuracy ,efficiency and security. Use of AES algorithm gives the wireless communication with less complexity and high security data transmission in a wireless sensor network. We gain a transimmion with no data loss. The above simulation results have been analyzed in MATLAB envirnment.

REFERENCES

[1]G.Lin and G. Noubir, "On Link Layer Denial of Service Data Wireless LANs", Wireless comm.. Mobile Computing, Vol 5, no.3, pp 273-284, 2005.
[2]Wenyuan Xu, Wade Trappe, Yanyong Zhang, "Jamming Sensor Networks: Attack and DfenceStrategis", IEEE Network, vol.20,no.3, pp. 41-47, 2006.
[3]William Stallings, "Cryptography and network security principles and practices", pp 134-165. 2007.
[4]Radhapoovendra,Minggyan Li, Koutsopouls," Optimal jamming attacks &network defense policies in wireless sensor network",Proc.IEEE INFOCOM, 2007.
[5]MarioStrasser, Christina popper, Srdjancapkun, Mario Cagalji, "Jamming-resistance Key Establishment using Uncoordinating Frequency Hopping", Proc.IEEESymp.Security and Privacy (ISSP) 2008.
[6]A.Cassola, T.Jin, G.Noubir, and B>Thapa, "Spread Spectrum Communication without Any pre-Shared Secrets," technical report, http://www.ccs.neu.edu/home/bthapa/techreport/trek.pdf, 2013
[7]Ettus Research, "Universal Software Radio Peripheral," http://www.ettus.com, 2013.