IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2321-8843; ISSN(P): 2347-4599
Vol. 2, Issue 2, Feb 2014, 273-278

EFFICIENT SECURITY & ENERGY SAVING PROTOCOL

JIAUR RAHMAN AHMED[1] & MEENAKSHI BANSAL[2]

[1]Research Scholar, Department of Computer Engineering, Yadvindra College of Engineering, Talwandi Sabo, Bathinda, Punjab, India

[2]Assistant Professor, Department of Computer Engineering, Yadvindra College of Engineering, Talwandi Sabo, Bathinda, Punjab, India

ABSTRACT

Effective and efficient security providing for any sensor network is one of the major goal for complete data communication. But wireless sensor provides a significant computation and communication in the wireless network. During data communication another major aspect to save the energy for reduce the communication cost. Data secrecy is one of the most important key concept during transmission and reception. Generally a data secrecy maintains two major task-key establish and encryption of message. So the four parameter is equally likely important for secure, reliable and low cost data communication. Therefore ESESP provides the best way for best data communication.

KEYWORDS: Data Secrecy, Cryptography, Energy Efficient Key, Virtual Energy, Stream, Cipher, RC4, Confidentiality

INTRODUCTION

A **sensor** node is an electronic device capable of monitoring physical or environmental conditions like temperature, sound, pressure etc. A wireless sensor network composed of lots of sensor nodes performing some processing with gathering sensory information and communicating with the other connected nodes in the network and to cooperatively pass their data through the network to a main location. A sensor node should be small in size, consume extremely low energy, operate in high volumetric densities, be autonomous and operate unattended, and be adaptive to the environment.

In ESESP protocol wireless sensor networks are established for low cost, low energy and operate in high densities with adaptive environment. But the major issue to established a best network is to infrastructure the networks path and weight according to energy distribution. Without having the energy distribution it is impossible for the sensor device to transmit the data from one node to another. ESESP provides an example of six wireless sensor node networks having some coordinates. But for maintain the adjacency path the dijktras algorithm follows for shortest one.

Security is the major aspect of data communication for all types of network. It is equally likely important issue for wireless senor network for secure data transmission. ESESP gives the best way to solve the security cum reliable data communication. For optimum security any security protocol can be used as it used the RC4 algorithm.

For the best transmission of data communication it is most important issue to manage the energy utilization so that it would be cost effective. For that ESESP provides the best policy to reduce the utilization available energy of each and every sensor nodes so that they can conserve the energy for future if needed. So simply ESESP is the latest and very cost efficient protocol for wireless sensor network providing these features.

General Algorithm for ESESP

At the Transceiver End

Step 1: Initialization the Sensor nodes in the wireless sensor network

Step 2: Find the adjacency matix for possible path from possible nodes

Step 3: Initialization the flag status set and reset respectively to n nodes

Step 4: Declare the energy of each packet to respective sensor nodes

Step 5: For massage=set, flag status=reset;

Continue encryption of key in each node until reached destination.

Step 6: Calculate energy level in each node

Step 7: Send encrypted message using RC4 algorithm

At the Receiver End

Step 1: Receive the encrypted message

Step 2: Decrypt the message with decrypted key using RC4 algorithm

Step 3: Calculate energy level after receiving

Step 4: Flag status cheked and verified

Step 5: Stop.

Practical Implementation of ESESP

Figure 1(a) shows the sensor network containing the six sensor devices connected with a directed graph. The blue color represent the each node an empty node or initialization of the nodes. "→" shows the direction from source to destination address of sensor networks. Red color significant of digit represent the flag status of sensor networks before transmitting the data transmission.

On the other hand the figure 1(b) shows the shortest path from source 1 to destination 4 via possible sensor nodes i.e. the path is 1→2→3→4. And after transmitting the data the processed nodes are represented with colour green. For finding the shortest path the disktras algorithm is used. Now the major goal is to provide the security. RC4 algorithm is used for cryptographic technique which is discussed bellow.

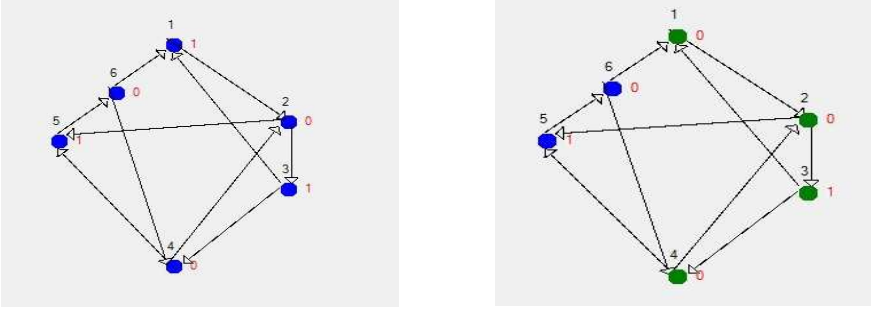

Figure 1: (a) Before Transmission Data (b) Node 1 to 4 Data Transmission

Message Encryption

Message security is one of the major goal of this protocol. ESESP protocol initially used the concept of RC4 algorithm or algorithm of swapping. Following Steps shows the steps of RC4 algorithm.

RC4A uses two state arrays S1 and S2 and two indexes *t1*and *t2*. Each time *i* is incremented then

- The basic RC4 algorithm is performed using S1 and *t1*, but in the last step, S1 [*i*] + S1 [*t1*] is looked up in S2.
- Second, the operation is repeated (without incrementing *i* again) on S2 and *t2*, and the output is S1 [S2 [*i*] + S2t*2*]].

Thus, the algorithm is:

- i=:0;
- t1=:0;
- t2=:0;

While I

i=: i+1;

t1=t1+S1 [i];

swap the values of S1 [i] and S1 [t1]

return S2 [S1 [i] + S1 [t1]];

t2=:t2+S2 [i];

swap values of S2 [i] and S2 [t2]

return S1 [S2 [i] + S2 [t2]];

end while;

After Implementing Algorithm the message encryption follows:

Table 1

Plain Text	Encrypted Text
Hello how are you What are you doing??? This is a test notepad. This notepad is used to test the program This is program made by me.. in this program we have lot many thinggs. This program contains three modules. Hello how are you... What are you doing??	ᶍ £<ō̄ çHø ȉ°©ƥnƝtŭ£̊³^ẍĐi ȔŅ˽ơƣå²êǺÁ˛ÇĄ üȔčȒĉÆz Ì ėâĬɧĬĐɋĺĖ˙ʍĄĝń'ŕ½ȒŢöŢŞ¥ũŒĦîʄŶ ȡɖľȷĐ¥ηųƈƛȉTñƱ

Energy Saving Technique Using Flag

In this protocol for optimum security dynamic key encryption technique is being used means each and every sensor devices changes their keys using energy. So it is an important aspect to save energy but not hampering on the dynamic key establishment. The concept of flag set and reset removes this limitation. Following shows how these become an effective method.

Table 2

Sensor Nodes	1	2	3	4	5	6	Total Cost
No Flag but message carries	Cost of key encryption and loss of energy	Cost of key encryption and loss of energy	Cost of key encryption and loss of energy	Cost of key encryption and loss of energy	Cost of key encryption and loss of energy	Cost of key encryption and loss of energy	Encryption Cost= 6 times
Flag containing no message	1	0	1	0	1	0	Key encryption cost=3 times
Flag containing message	Flag=0 Encryption cost=0	Flag=0 Encryption cost=0	Flag=1 Encryption cost=positive	Flag=0 Encryption cost=0	Flag=1 Encryption cost=positive	Flag=0 Encryption cost=0	From node 1 to node 6 the encryption cost of key= 2times

Energy Calculation: For energy saving technique we have to calculate the initial energy with final energy into each sensor devices so that we can reduce the energy by this protocol. Using this protocol for above example the energy levels are:

Table 3

Sensor Nodes	Energy after 1st Packed	Sensor Nodes	Energy after 2nd Packed	Energy Loss
1	1977	1	1954	23
2	1992	2	1949	43
3	1957	3	1949	8
4	1977	4	1954	23
5	2000	5	2000	0
6	2000	6	2000	0

RESULTS

The result is shown after implementing the ESESP protocol.

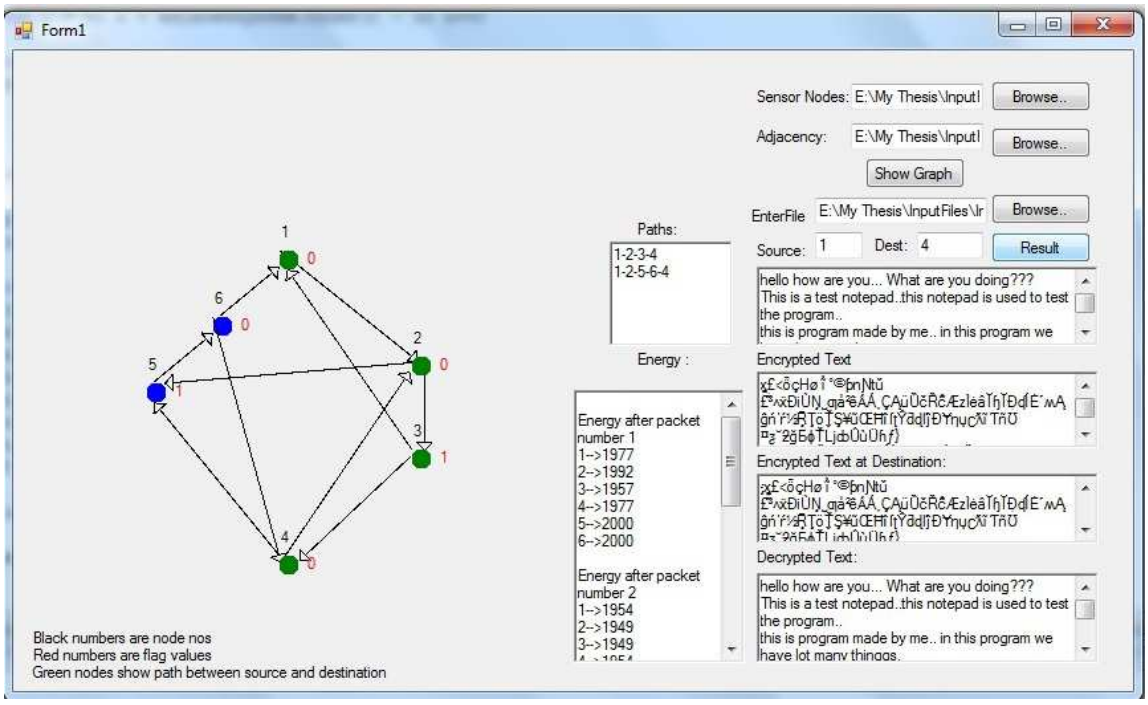

Figure 2

CONCLUSIONS

ESESP protocol is the optimum solution for simultaneous problem arises in wireless sensor network with best utilization of energy using message encryption technique with shortest path. It complies the relevant possibilities for sensor devices in wireless sensor network.

REFERENCES

1. K. Ravi Chythanya, S.P.Anandaraj, S. Padmaja, “Virtual Energy-Efficient Encryption and Keying (VEEEK) for Wireless Sensor Networks” International Journal on Computer Science and Engineering (IJCSE) 8 August 2011.
2. S. Uluagac, R. A. Beyah, Yingshu Li, A. Copeland “VEBEK: Virtual Energy Based Encryption and Keying for wireless sensor networks” IEEE Transaction on Mobile Computing vol. 9 No 7 pp.994-1007 July 2010.
3. Geng Yang 1, Chunming Rong2, Christian Veigner2, Jiangtao Wang1, and Hongbing Cheng, “Identity-Based Key Agreement and Encryption for Wireless Sensor Networks” IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.5B, May 2006.
4. Kwang-Jin Paek, Ui-Sung Song, Hye Oung Kim, and Jongwan Kim, “Energy-Efficient Key-Management (EEKM) Protocol for Large-Scale Distributed Sensor Networks” Journal of Information Science and Engineering 24, 1837-1858 (2008).