A Novel Security Scheme for Improving Reliable Transmission using Energy Based Routing

[1]M. Siva Sangari, [2]Mrs.P. Brundha
[1]PG Student, [2]Assistant Professor,
[1&2]Francis Xavier Engineering College,
Tirunelveli, Tamilnadu, India.

Abstract – **In wireless sensor networks, the technical challenges that the network suffer are security and energy consumption, because sensors have some complications and energy limitations. A novel security scheme known as Channel Informed Encryption (CIE) is proposed mainly for security purpose. In this scheme, the transmission of information from sensor to target through a wireless channel is prevented from eavesdroppers. Thus the information reached to target is highly secured. Also, this scheme becomes effective by using EEBR protocol finding the suitable energy efficient path for transmission. Hence, energy consumed by sensors are minimized which maximizes lifetime of networks.**

Index Terms – **eavesdroppers, energy efficiency, perfect security, wireless sensor networks.**

I. Introduction

In present, WSNs are active area for research. It is more practical to produce numerous sensors which are less expensive. These are named as sensor nodes which are distributed over a particular area and some nodes are grouped together to form cluster. Each cluster is governed by a node known as cluster head. The sensor nodes and cluster head along with base station (BS) constitute the network known as wireless sensor network (WSN). These networks find its applications in data logging, landslide detection, water quality monitoring and health care monitoring and in some military applications. The size of sensor node may vary and costs according to their complexity.

One of the important resources of WSN is the energy which determines the lifetime of nodes. WSN can be deployed in various environments even though in remote regions. Energy consumption of sensors should be minimized optimally and thus nodes will be energy efficient in order to increase the network's lifetime. The notable characteristics of WSN are mobility, communication and its ability to deal with node failure.

II. Related works

There are several approaches which are considered to solve the problem in secure communication in WSNs [2]-[6]. In military applications, designing of sensor networks are highly concentrated as security problem. This is a notable challenge because the topology of node changes frequently due to node failure [2]. Node failure is mainly because of environmental changes. Thus security is very difficult to achieve in these networks.

In [3], transmission of information is done using TBMA (Type-Based Multiple Access) protocol. Here, Multiple Access Channel (MAC) is used where the information from several sensors are transmitted simultaneously. This leads to the consequence of information overlapping. Even though, this scheme reduces complexity in achieving security, but the energy consumed across the entire network is very high due to energy wastage.

In WSN, sensors are propagated over a certain area and each sensor collects the information from individual sensors and transmits it through wireless channel to fusion centre. The fusion centre combines those information and produce final estimation [4]. WSN suffers from many constraints such as limited bandwidth and range. The organization of WSN depends only upon the arrangement of sensors and fusion centre [5]. Distributed detection in networks became one of the troubles for designing sensor as detection problems are static in nature.

In [6], the scenario is that there is a channel which links sensor and fusion centre for communication purpose. Here both PAC and MAC are considered. A significant amount of energy is spent when sensor is ready to transmit. This leads to high energy consumption.

III. Proposed Scheme

A. Node Configuration

Sensor node is a basic node in WSN with qualities such as mobility, transmit and receive information using some wireless channels. These channels are responsible for creating wireless environment. The nodes are configured based on the fact that all the sensor nodes in the network are able to transmit information directly to each other nodes present in the network. The parameters namely channel type and number of nodes is considered.

B. Channel Assignment for Transmission

Sensor nodes grouped together and form the cluster. The node with higher energy level gathers the information from other neighboring nodes in network and transmits it to fusion centre. The wireless channel plays an important role in transmitting information. Here, the channel considered is non-interfering parallel channels where the information from several clusters is passed through it without any overlapping. This is the major reason for choosing this wireless channel. The added advantage of this wireless channel is that it can easily bond the sensor and fusion centre even though they are far away from each other.

C. Proposed Channel Informed Encryption

Information coming from sensors is encrypted before reaching fusion centre. Here, public key cryptography is used. This provides better secrecy in transmission. The public key is generated for encryption and private key is just for decryption. Thus, encryption takes place in sensor node and encrypted information is transmitted to fusion centre through non-interfering parallel channel. The information from every cluster is collected and fused into final information in the fusion centre.

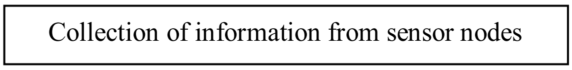
Meanwhile, eavesdroppers which are unauthorized party tries to extract encrypted information from fusion centre. Since, it is highly secured; the attempt of eavesdropping information gets failed. Thus fusion centre decrypts the incoming information using private key and starts finding the location of target. GARP (Geographic Assisted Routing Protocol) is used to find the target location. On using this protocol, each node in network resolve their location and source is well-known about the location of destination. By this, after finding the location of target, the decrypted information is sent to it. Thus the information is highly secured without the interference of eavesdroppers.

D. Energy Efficient Routing

On transmitting information, sensor node consumes more energy. In order to overcome this demerit, EEBRP (Efficient Energy Based Routing Protocol) is used. This protocol is mainly used to reduce the energy consumed by sensors during transmission process. Here, sensors are propagated over an area and their information is collected. Then, the possible efficient route for transmitting information is identified.

The routing path is selected with less number of intermediate nodes. Further, transmission may be done using the selected path. By this, the energy consumed by the sensor during transmission is gained, which results in better energy efficiency.

Routing may be shown by steps in Fig. 1.



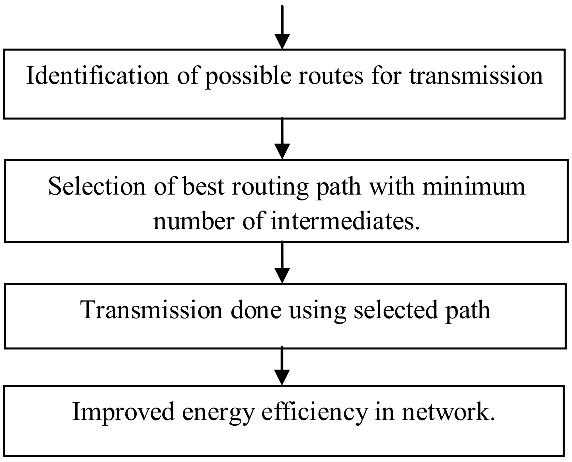

Identification of possible routes for transmission
Selection of best routing path with minimum number of intermediates.
Transmission done using selected path
Improved energy efficiency in network.

Fig. 1 Steps followed in energy efficient routing

IV. Results

In this section, the performance analyses are obtained with the help of Network Simulator. The performance of routing and energy consumption for proposed method is compared with the existing method.

In Fig. 2, energy consumed by sensors for both proposed and existing scheme is compared.

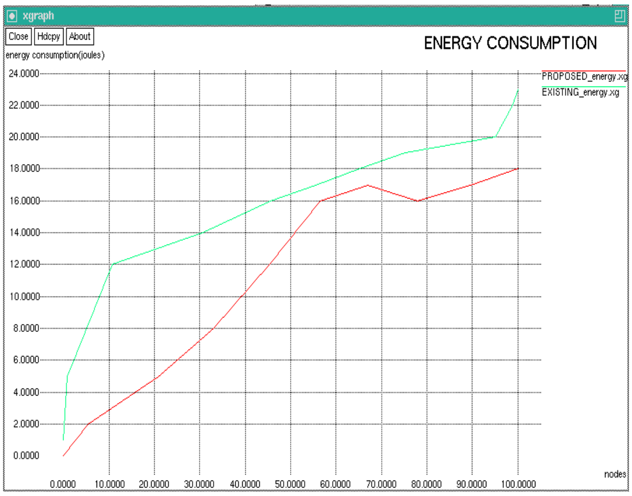


Fig. 2 Comparison of energy consumption

In Fig. 3, routing performance can be analyzed in terms of WEP for proposed and existing method.

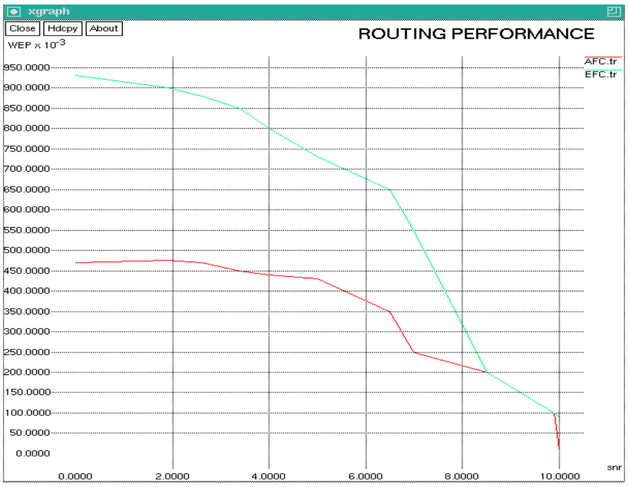


Fig. 3 Performance analysis of routing

In Fig. 4 and Fig. 5, the graph may be plotted using two parameters namely throughput and Packet Delivery Ratio.

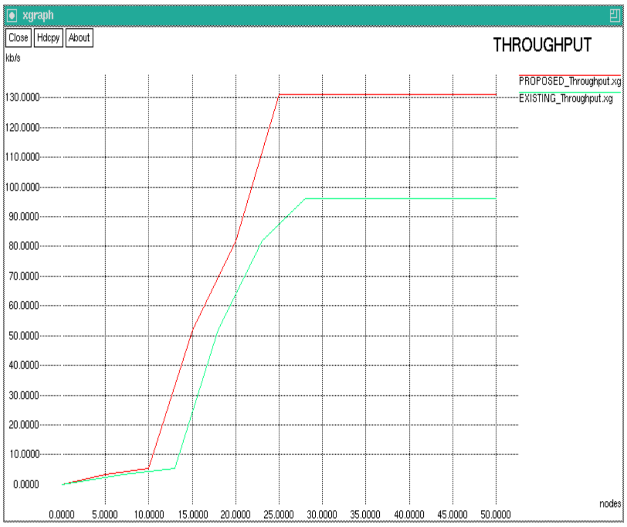


Fig. 4 Performance analysis of throughput

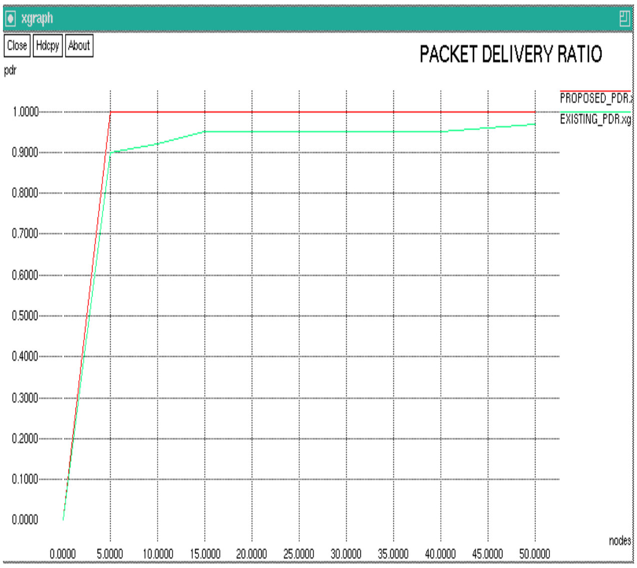


Fig. 5 Performance analysis of PDR

V. Conclusion

The proposed scheme has the advantage of obtaining perfect secrecy by ignoring unauthorized centre from target. Also by using efficient energy based routing protocol, sensors transmit information to target through efficient routing path that leads to better energy efficiency. The performances are measured in terms of WEP. The comparison for proposed scheme with conventional TBMA scheme is shown with increasing number of nodes. This proves that the proposed scheme obtains perfect secrecy and less energy consumption than conventional scheme.

ACKNOWLEDGEMENT

First of all I thank the almighty for giving us the knowledge and courage to complete the research work successfully. Next I express my gratitude to our respected Assistant Professor Mrs.P.Brundha for following me to do research work effectively. Finally, I wish to express my gratitude to my family and my friends, for providing unending support in every aspect possible, to ease my path on this journey.

REFERENCES

[1] H. Jeon, J. Choi, S. W. McLaughlin and J. Ha, “Channel Aware Encryption and Decision Fusion for Wireless Sensor Networks”, IEEE Trans. Inf. Forensics Security, Vol. 8, No. 4, Apr. 2013.

[2] X. Chen, K.Makki, K.Yen and N. Pissinou, “Sensor network security: A survey”, Commun. Surveys Tuts., Vol.11, No. 2, pp. 52-73, Second Quarter, 2009.

[3] H.Jeon, D.Hwang, J.Choi, H.Lee, and J.Ha, “Secure type-based multiple access”, IEEE Trans. Inf. Forensics Security, Vol. 6, No. 3, pp. 763-774, Sep. 2011.

[4] T.C.Aysal and K.E.Barner, “Sensor data cryptography in wireless sensor networks”, IEEE Trans. Inf. Forensics Security, Vol. 3, No. 2, pp.273-289, Jun. 2008.

[5] V.Nadendla, “Secure Distributed Detection in Wireless Sensor Networks via Encryption of Sensor Decision”, M.S.thesis. Louisiana State University and Agricultural and Mechanical College, Baton Rouge, LA, USA, 2009.

[6] S.Marano, V.Matta, and P.K.Willett, “Distributed detection with censoring sensors under physical layer secrecy”, IEEE Trans. Signal. Process, Vol. 57, No. 5, pp. 1976-1986, May 2009.

[7] C.Shannon, “Communication theory of secrecy systems”, Bell Syst. Tech. J., Vol. 28, No. 4, pp. 656-715, 1949.

[8] Y. Liu, S. C. Draper, and A. M. Sayeed, “Exploiting channel diversity in secret key generation from multipath fading randomness”, IEEE Trans. Inf. Forensics Security, Vol. 7, No. 5, pp. 1484–1497, Oct. 2012.

[9] J. Wallace and R. Sharma, “Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis,” IEEE Trans. Inf. Forensics Security, Vol. 5, No. 3, pp. 381–392, Sep. 2010.

[10] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. Mandayam, “Information-theoretically secret key generation for fading wireless channels,” *IEEE Trans. Inf. Forensics Security*, Vol. 5, No. 2, pp. 240–254, Jun. 2010.

[11] www.google.com

AUTHOR(S) PROFILE

M. Siva Sangari is doing M.E Network Engineering in Francis Xavier Engineering College, Tirunelveli. She has completed her B.E Electronics and Communication Engineering in Francis Xavier Engineering College, Tirunelveli in the year 2012.She is a member in Computer Society of India. Her areas of interest are Wireless Communications and Digital Communication.

Mrs. P. Brundha is working as an Assistant Professor, Department of Computer Science and Engineering in Francis Xavier Engineering College, Tirunelveli. She has completed her B.E Computer Science and Engineering in P.S.R Engineering College, Sivakasi and M.E Computer Science and Engineering in Manonmaniam Sundaranar University, Tirunelveli. Her areas of interest are Compilers and Network Security.