International Journal of Security and Its Applications
Vol. 11, No. 12 (2017), pp.27-34
http://dx.doi.org/10.14257/ijsia.2017.11.12.03

Security Solution for Secure Communication for Cross Layer Design in WSN

Rakesh Kumar Saini[1] and Ritika[2]

[1,2] *Department of Computer Applications, DIT University, Dehradun, India*
[1]*rakeshcool2008@gmail.com*, [2]*riti_79@rediffmail.com*

Abstract

Wireless Sensor Network is a new technology that can solve problems of traditional network in many applications. Cross-layer design play a very important role for applications of wireless sensor network. Improved security is very important for the success of communication between sensor nodes in wireless sensor network because the data collected is often sensitive and the network is particularly vulnerable. Many Security approaches have been proposed to provide security solutions against various threats to the Cross-layer modification techniques in Wireless sensor network. In this seminal, we overview the previous schemes for the security of cross-layer communication in wireless sensor network. In this paper we propose a new security model that will be more secure as compare to existing security scheme. Proposed Security model will provide more security between cross layer communication in WSN.

Keywords*: Cross-layer design, WSN Protocol Stack, Sensor nodes, Wireless Sensor Network*

1. Introduction

In Wireless sensor network, sensor nodes work together in open environment. Sensor nodes sense the environment and pass sense data to base station via internet and satellite [1]-[2]. There is more difficult to provide an efficient and scalable security solution. While designing the security mechanism for WSN it is to be kept in minds that the following are the inbuilt limitations of the sensor nodes in wireless sensor network.

i. Vulnerability of channels
ii. No infrastructure in Wireless sensor Network
iii. Network topology change dynamically
iv. Sensor nodes have limited energy
v. Sensor nodes have limited computational capabilities
vi. There is large dense distribution of sensor nodes

In WSN it is necessary to allow only specific sensor node to access your wireless sensor network. Every sensor node that is able to communicate with a wireless sensor network is assigned a unique Media Access Control (MAC) address. In Wireless network, Wireless routers usually have a mechanism to allow only devices with particular MAC addresses to access to the wireless sensor network. Low deployment costs of sensor nodes make wireless sensor networks attractive to users. Deployment of sensor nodes in open environment also gives attackers the tools to launch attacks on the wireless sensor

Received (May 31, 2017), Review Result (November 17, 2017), Accepted (November 30, 2017)

ISSN: 1738-9976 IJSIA

network [3]-[4].The design flaws in the security mechanisms of the 802.11 standard also give rise to a number of potential attacks, both passive and active. These attacks enable intruders to eavesdrop on, or tamper with, wireless transmissions. Sensor nodes are fast, scalable, low energy efficient and highly distributed in open environment so there is security is must for quality of service in wireless sensor network [5].

There is need of security solution for cross layer design in wireless sensor network because there is one layer can communicate with another layer non-adjacently. Wi-Fi Protected Access (WPA) should be used for encryption of data in wireless sensor network. In this paper we proposed a security solution that will provide security to layers in wireless sensor network [6]-[7].

2. Basic Requirement of Security in Wireless Sensor Network

Basic security requirement that are necessary for secure communication in wireless sensor network are:

i. Authenticity

ii. Availability

iii. Integrity

iv. Privacy

v. Nonrepudiation

vi. Security Attacks

vii. Survivability

i. Authenticity

Authenticity means data communicated between sensor nodes and base station are authentic and correctly identified. Authenticity means data that are coming from source sensor node to destination sensor node is authentic or not.

ii. Availability

Availability is very important for maintaining an operational network. Availability means utilization of recourses by sensor nodes for sending data from one sensor node to another sensor node.

iii. Integrity

Integrity assures that the data received at base station is not corrupted. When sensor nodes pass sense data to the base station then integrity assures that sense data of sensor nodes received at base station successfully without any loss of sense data.

iv. Privacy or Data Confidentiality

When data communicated between sensor nodes and base station and similarly communicated data between base station and end user then privacy insures that data should be able to acces only by base station and end user. Confidentiality is the protection of transmitted data from passive attacks.

v. Nonrepudiation

When the sender transmit data to destination, Nonrepudiation ensure that destination can prove that the message sent by authorize sender. Similarly, when data is received, the sender can prove that the data received by the authorize receiver.

vi. Security Attacks

Security attacks are attacks that are changes in transmitted data without permission by third party. These attacks are two types-

(a) Passive attacks

In Passive attacks, attacker monitors the transmission between sender and receiver but not perform any changes in data that are communicated between sender and receiver.

(b) Active attacks

In Active attack, attacker performs some changes of the data that are communicated between sender and receiver without permission.

vii. Survivability

Survivability means capability of transmission of data without any delay and without any loss of data.

3. Proposed Security Model

We proposed a Security model for secure communication between layers. Proposed Security model (Figure 1) will be more secure as compare to existing security scheme in wireless sensor network. In this security model we are using a Security filter between cross layer design and cross layer optimization handler. When Sensor node want to send sense data to Base station then first check whether channel free or not if channel is free then sense data forward to Security filter. Security filter check the sense data and give a token (time slot) to packet node. After receiving token from security filter sensor node forward sense data to Cross layer optimization handler (CLOH). Cross layer optimization handler is used for merging layers for communication non-adjacently. Cross layer optimization handler Combine the resources and provide communication between layers.

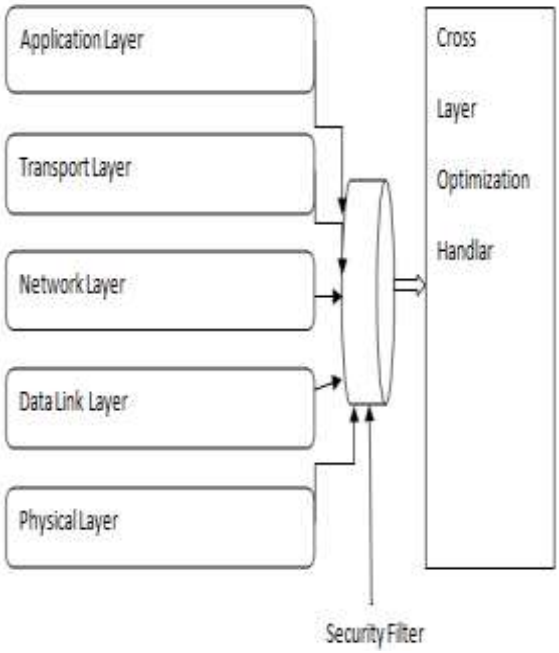

Figure 1. Proposed Security Model for Cross Layer Design

Notations used:

SF – Security Filter

P_N – Packets node

CLOH - Cross layer Optimization Handler

T_s -Time Slot

Ch – Channel

BS-Base Station

Algorithm for security of data

1. If Sensor node want to send data to base station
2. Check Channel Ch whether it is free or not
3. If Ch=0 then set Ch=P_N
4. Set SF = P_N
5. Set P_N=T_S
6. P_N dispatch from SF to CLOH buffer
7. CLOH Check Ch is free or not
8. If Ch=0 then
9. Dispatch P_N from CLOH to BS
10. Repeat Step 1 to 9

4. Related Work

Many researchers studied the security issues in wireless sensor network. There is a considerable amount of surveys in the literature that discuss WSN technologies in general [1]-[7].The complete literature survey of security issues in cross layer discuss in [8]-[10]. Djallel Eddine Boubiche *et al.* [8] introduce a protocol for security in distributed environment for secure communication. Proposed protocol improves security between sensor devices. Geethapriya Thamilarasu *et al.* [9] have proposed the cross-layer scheme for improvement security between sensor devices in open environment. Proposed security scheme provide secure communication between layers. Proposed security scheme is suitable only for communication between wireless sensor devices. Pedro Pinto, Antonio Pinto *et al.* [10] have proposed a security mechanism that provides secure transmission of data packets between sensor devices. Proposed security mechanism improves performance of wireless sensor network. This scheme avoids the useless data transmission and allows useful data communication between layers. Proposed security mechanism increase performance of wireless sensor network.

5. Performance Analysis of Proposed Security Model

We develop a simulation environment to evaluate the efficiency of Security model. For this purpose we are using QualNet 5.0.2 simulation modeling tool. The performance of proposed Security model is verified with cross layer design in the experiment. In this experiment we deploy some sensor nodes in open environment and check the performance of security model. We are using some parameters in this simulation (Table 1).

Table 1. Simulation Parameters

Parameters	Value
Source Sensor nodes	1,2,3,4,5,6,7,8,9,10
Destination node (Base Station)	11
Packets Send	40000
Terrain Range	100m x 100m
No. of nodes	10
Frequencies	2.4GHz
Traffic Type	CBR
Channel Type	Wireless channel
Protocols	AODV

In this simulation environment (Figure 2) Source sensor nodes 1,2,3,4,5,6,7,8,9,10 are co-operately pass their data to the destination node 11 (Base Station). Running simulation is shown in Figure 3. In running simulation sensor nodes are sending packets to destination node 11(Base Station). In Figure 4 shown the result, total packets received by destination sensor node 11 or Base Station. Total packets send by source sensor nodes was 4000.By using Security model, Base station received 100% packets from sensor nodes 1, 2,3,4,5,6,7,8,9,10. Base Station received 4000 packets from Source sensor nodes. By implementing security model with cross layer design we are getting 100% secure data at Base Station.

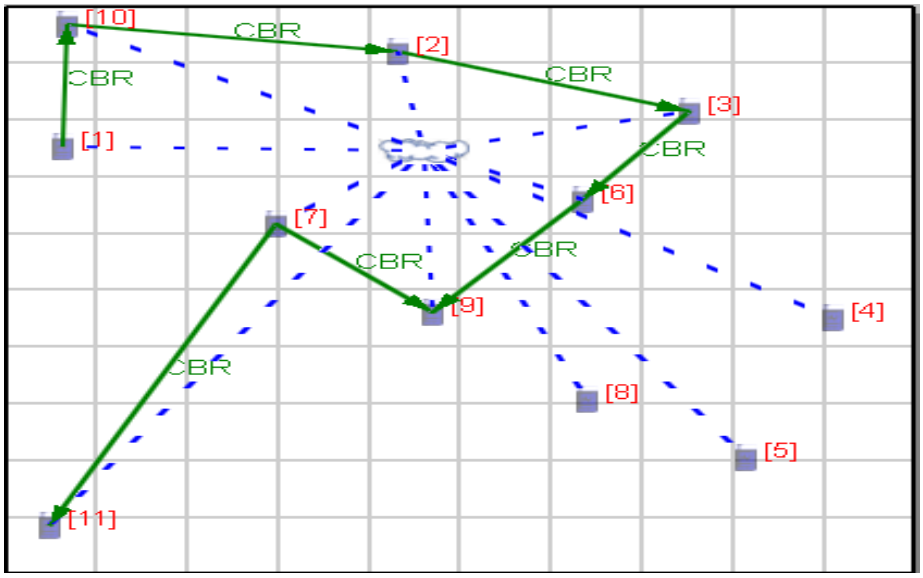

Figure 2. Simulation Setup

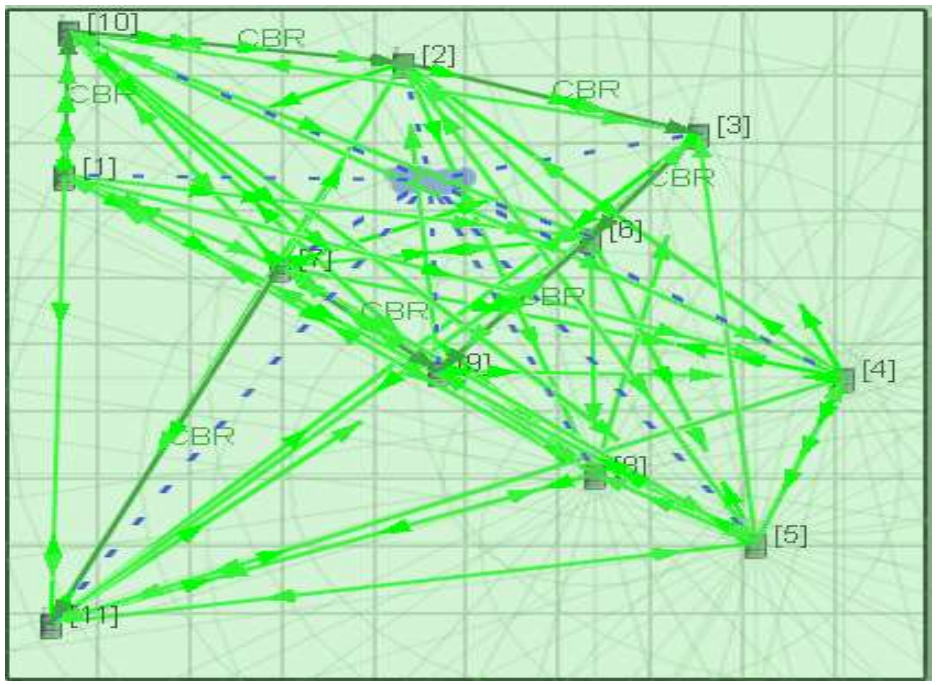

Figure 3. Running Simulation

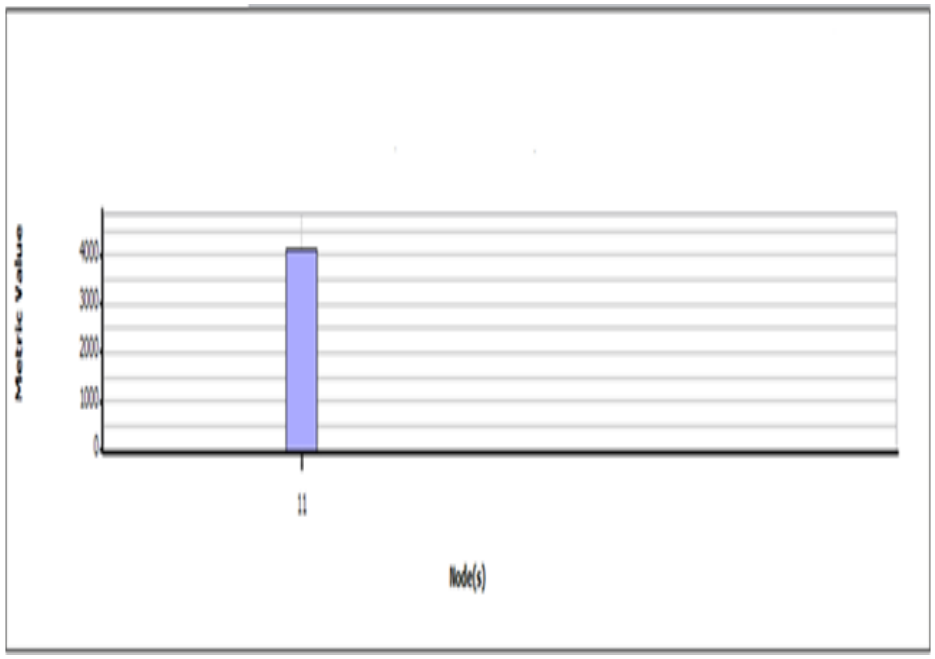

Figure 4. Total Packets Received by Base Station

6. Conclusion

Security is an important requirement for secure communication between cross layer in wireless sensor network. In this paper we proposed a new security model for secure communication between cross layer for WSN.The proposed security model is very useful for different applications of wireless sensor network such as Military application, Health application and industrial monitoring application and so on. In this paper we evaluate performance of proposed security model by using Qualnet 5.0.2 Simulator tool and find that proposed security model provide 100% security between layers communication.

References

[1] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks", Computer communication, vol. 30, **(2007)**, pp. 2826-28410.
[2] J. N. Al-Karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey", IEEE Wireless Communication, vol.11, no.6, **(2004)**, pp. 6-28.
[3] A. S. Zahmati and B. Abolhassani, "EPMPLCS: An Efficient Power Management Protocol with Limited Cluster Size for Wireless Sensor Networks", Proc. 27th International Conference on Distributed Computing Systems (ICDCS 2007), submitted for publication.
[4] W. B. Heinzelman, "An Application-Specific Protocol Architecture for Wireless Micro sensor Networks", IEEE Transactions on Wireless Communications, vol. 1, no. 4, **(2002)**, pp.660 - 670.
[5] W. R. Heinemann, A. Chandrakasan and H. Balkrishnan, "Energy-Efficient Communication Protocol for Wireless Micro sensor Networks", in Proceedings of 33rd Hawaii International Conference on System Science, vol. 2, **(2000)**, pp.1-10.
[6] A. S. Zahmati, B. Abolhassani, A. A. Behesti Shirazi and A. S. Bakhtiari, "An Energy-Efficient protocol with Static clustering for Wireless Sensor Network", proceedings of world academy of science, Engineering and Technology, ISSN 1307-6884, vol. 22, **(2007)**.
[7] S. Ghiasi, A. Srivastava, X. Yang and M. Sarrafzadeh, "Optimal Energy Aware Clustering in Sensor Networks", SENSORS Journal, vol. 2, no. 7, **(2002)**, pp. 258-269.
[8] D. E. Boubiche, S. Boubiche and A. Bilami, "A Cross-Layer Watermarking-Based Mechanism for Data Aggregation Integrity in Heterogeneous WSNs", IEEE Communications Letters, vol.19. no.5, **(2015)**.
[9] G. Thamilarasu, R. Sridhar, "Exploring Cross-layer techniques for Security: Challenges and Opportunities in Wireless Networks", Proc.IEEE, **(2007)**.
[10] P. Pinto, A. Pinto and M. Ricardo, "Cross-Layer Admission Control to Enhance the Support of Real-time Applications in WSN", IEEE Sensors Journal, Vol.X.No.X, XX.

Authors

Rakesh Kumar Saini, he received the MCA degree from UPTU, Lucknow, India in 2005 and M.Tech (Computer Science and Engineering) degree from UTU, Dehradun, India in 2012 and Pursuing PhD from DIT University, Dehradun, India in 2014.He is having 12 Years of teaching experience. He is author of around 10 books. His research interests include Wireless Sensor Network, Energy-Efficiency in Wireless Sensor Network.

Ritika, she received the Ph.D. degree in Computer Science from GKU, University, Haridwar in the year 2010, M.Tech degree in Computer Science and Engineering from UTU, Dehradun and MCA from GKU Dehradun. She is life time membership of ISCA, CSI, IEEE, IAENG, ISCA and IETE. She was Chairman of Computer Society of India Dehradun Chapter in the year 2013. She specializes in core areas of computer science and holds experience of more than 14 years.

