International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 24 Issue 12 – SEPTEMBER 2017.

Secure and Energy Efficient Communication with Certificate-Less Effective Key Management Techniques in Dynamic Wireless Sensor Network

Aathira s [#1] and Aby k Thomas [*2]

[#]*Department of ECE, Hindustan Institute of Technology and Science, Chennai, India*

[*] *Department of ECE, Hindustan Institute of Technology and Science, Chennai, India*

***Abstract*— In the modern world because of the applications of wireless sensor network has been an active area of research. Due to the nature of data transmitted, the network has to be secure and efficient. In this paper a combination of CL-EKM and FAF-EBRM is used in order to attain security and efficiency in the network. In CL-EKM the node compromises are minimized by updating the information of nodes leaving or joining the cluster hence maintaining the secrecy of the data. According to the link weight and forward energy the next hope is selected, and for local topology a reconstruction mechanism is used in FAF-EBRM. Combination of both of these FAF-EBRM and CL-EKM results in high energy efficiency and PDR.**

***Index Terms*— Wireless sensor networks, forward energy, link weight.**

I. INTRODUCTION

The dynamic wireless sensor network are used for monitoring application because of its characteristics such as node mobility, wider network, and accurate services. Because of the nature of the data transmitted the network has to be efficient and secure. Securing the data requires efficient encryption protocol and efficiency of the network depends upon how it deals with energy.

Generally in a network the problems regarding security and efficiency is considered separately. As we mentioned earlier to address security efficient key management techniques are used based on both certificate and certificate-less[3]-[6] and [1] key management techniques respectively, where in those concentrated on the field of security alone and they lacked in efficiency of the network. On the other side the Energy-Balanced Routing Method [2] only concentrated on the efficiency of the network and lagged in the security features.

In this paper we consider Certificate-Less Efficient Key Management for the security of the data transmitted along with an Energy-Balanced Routing Method to increase the efficiency of the network. The CL-EKM is characterized by node mobility. When a node leaves or joins a cluster, a key update is generated and ensure forward and backward secrecy. For the compromised nodes it supports efficient key revocation and minimize the impact of compromised nodes. According to the link weight and forward energy the next hop is selected, and for local topology a reconstruction mechanism is used in FAF-EBRM.CL-EKM and FAF-EBRM combined together gives a guaranteed security and energy efficiency.

II. RELATED WORK

A. Certificate-Less Efficient Key Management Technique.

In CL-EKM the user's will have a private key which is a combination of a partial private key generated by KGC(key generation centre) and a secret value of the user. The use of full private/public key removes the need of certificates[12]. Removal of certificates doesn't mean the exact removal but the certificate used here will be implicit certificates. The implicit certificates remove the user's full responsibility on key. Thus removing the key escrow problem and computational overhead. The system flow of CL-EKM can be systemized as network model, pair-wise key generation, cluster formation and key-update. The network is considered as heterogeneous dynamic network, the network consist of different processing capability nodes and also both stationery and mobile nodes. The nodes are termed as cluster head(CH) and member node according to their processing capabilities. High processing capability nodes are termed as CH and low processing nodes are member node. H-sensors are connected with L-sensors through multi-hop or directly. The L-sensors are connected with sink node through H-sensors. After the deployment of the network, the L-sensors forms cluster with H-sensors through a hello message. The L-sensor can joins or leaves a cluster and the routing table is updated according to movement of the sensors. The Base Station(BS) creates a list of legitimate nodes which contain the information of false nodes or failure nodes. There are four types of key authentication used in this proposal they are namely: a certificate-less public/private key pair, an individual key, a pair-wise key and a cluster key. In this paper we utilizes the main algorithm of CL-HSC scheme in deriving certificate-less public/private keys and pair-wise keys[7]. After the deployment of network, to trigger the pair-wise key setup a

hello message is broadcasted. The broadcasted message contains an identifier and public key. At first, the setup of pair-wise key is long term, that key is used after for the derivation of the pair-wise key encryption. To encrypt the sensed data a short term key as session key is used. If the authentication of pair-wise key is successful the sensors forms the cluster and shares a common cluster key. So the whole cluster have same cluster key with nodes and all the nodes shares pair-wise key with each other nodes in the cluster. Cryptanalysis and mitigate damages are reduced with the frequent update of keys. The main two key updates are updates of pair-wise key update and cluster key . The pair-wise key is not exposed without a compromised node, if there is a compromised node the pair-wise master key establishment process is executed. The cluster key is updated only by H-sensor and nodes are considered malicious if L-sensors tries to update the key. The data is transmitted once all these keys are authenticated.

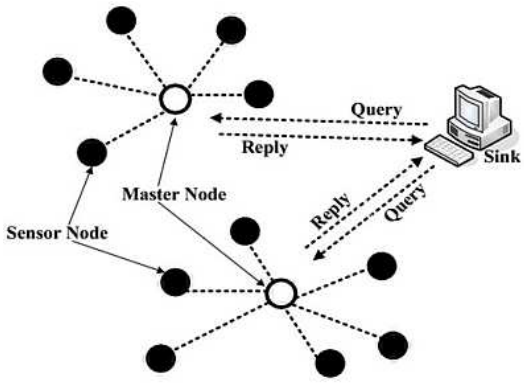

Fig :1 Dynamic Wireless Sensor Network

B. Forward Aware Factor-Energy Balanced Routing Method

The energy consumption is an important factor in wireless sensor network (WSN). In order to balances the energy the network topology, routing protocol and algorithm is the fundamental and important key works in dynamic wireless sensor network.

Multiple mechanisms are used in the network topology and routing protocols to achieve the energy balancing. The system modules are: network topology, Forward Aware Factor, Reconstruction mechanism, Performance evaluation. The sensing field for the sensor nodes are rectangular sensing field and the range of the nodes will be within that rectangular field. The energy level of each sensor node will differ and they varies and decreases as the time goes with the exhaust of full energy nodes die. To quantify the forward transmission area, forward energy density is based on transmission mechanism of WSN. All these factors are taken into consideration in this proposal. According to link weight and forward energy density the neighboring nodes are selected. Before selecting the CH, nodes calculates the FED (Forward Energy Density) and nodes with higher FED is taken as CH. The CH collects data from neighboring nodes and then forward it to sink node. The weight of edge between neighbors is calculated by communication launch node. Apart from the normal routing procedure a reconstruction mechanism is used. Every time a node finishes transmission checks the energy density and if the energy density less than the required level those nodes are replaced with new set of nodes. Before the reconstruction mechanism the low energy density nodes are replaced by new set of nodes. According to mechanism, here we balances the energy by replacing the dead nodes with new set of nodes.

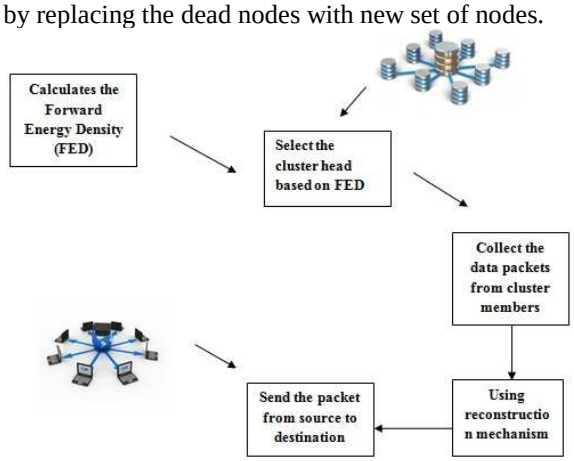

Fig:2 System Architecture

III. SIMULATION

As we know that the real networks are more complex and system that contains more nodes and connection. The existence of the link between nodes represents the weight of the network and also describes the property and intensity of connections. In this section Packet reception ratio (PRR) and energy consumption are taken. PRR can be defined as the ratio between received packets by the destination to the transmitted packets by the source. Energy consumption can be used as factor to know whether the energy is balanced in whole
network.

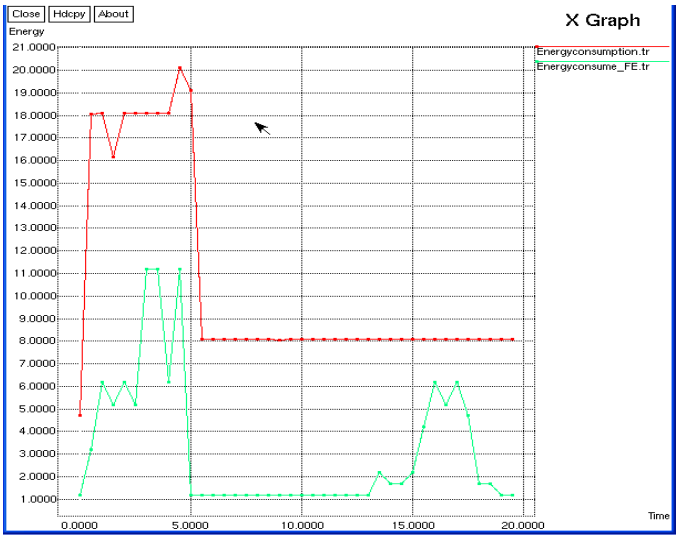

Fig 3: Energy consumption graph

The X-graph in the fig 3 is simulated between the axis energy and time. The red line in the fig 3 indicates that the energy consumption of the CL-EKM where as the green line in the fig 3 indicates the energy consumption of the combined proposal of CL-EKM and FAF-EBRM. The energy consumption of the red is high where as compared with the green line. Thus this shows that energy consumption compared with CL-EKM implemented alone is higher to CL-EKM and FAF-EBRM implemented together.

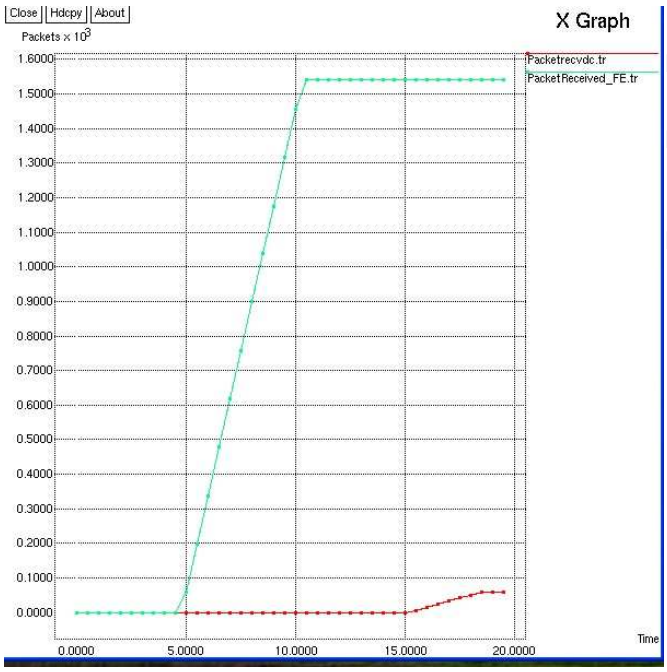

Fig 4: Packet Reception Ratio

The X-graph in the fig 4 is simulated between the axis of packets and time. The green line in the fig 4 indicates for CL-EKM and red line indicates CL-EKM combined with FAF-EBRM. The green line shows that after a certain interval only the packets are transmitted efficiently where as the red line indicates the packet reception is uniform and constant at all the time. PRR indicates both security and efficiency of the network. Thus the CL-EKM combined with FAF-EBRM shows that they have a good and constant PRR.

IV. CONCLUSION

We developed a combined proposal of CL-EKM and FAF-EBRM in order to attain security and energy efficiency. The method is based on energy balanced routing method which uses forward aware factor, this can select energy saving path for the nodes to reach next hop with help of link weight and forward energy density. Further more, a spontaneous reconstruction mechanism is used in local topology is designed in order to accept the nodes joins the secure cluster head in WSN. The experimental results has proved that the proposed method is better compared separately along with CL-EKM and FAF-EBRM in terms of PRR and energy consumption. Apart from PRR and energy consumption, it also gives a better results in functional lifetime of the network and high QoS.

REFERENCES

[1] Seung-Hyun Seo, Salmin Sultana, Elisa Bertino," Effective key management in dynamic wireless sensor networks " January 2015.
[2] Degan Zhang, Guang Li, Ke Zheng, Xuechao Ming, and Zhao-Hua Pan, " An energy-balanced routing method based on forward aware factor for wireless sensor networks" February 2014.
[3] M. Rahman and K. El-Khatib, "Private key agreement and secure communication for heterogeneous sensor networks," J. Parallel Distrib. Comput., vol. 70, no. 8, pp. 858–870, 2010.
[4] M. R. Alagheband and M. R. Aref, "Dynamic and secure key management model for hierarchical heterogeneous sensor networks," IET Inf. Secur., vol. 6, no. 4, pp. 271–280, Dec. 2012.
[5] D. S. Sanchez and H. Baldus, "A deterministic pair wise key pre distribution scheme for mobile sensor networks," in Proc. 1st Int. Conf. Secure Comm, Sep. 2005, pp. 277–288.
[6] I.-H. Chuang, W.-T. Su, C.-Y. Wu, J.-P. Hsu, and Y.-H. Kuo, "Two layered dynamic key management in mobile and long-lived cluster based wireless sensor networks," in Proc. IEEE WCNC, Mar. 2007, pp. 4145–4150.
[7] S. Seo and E. Bertino, "Elliptic curve cryptography based certificate less hybrid signcryption scheme without pairing," CERIAS, West Lafayette, IN, USA, Tech. Rep. CERIAS TR 2013-10,2013.[Online].