International Journal of Engineering Trends and Applications (IJETA) – Volume 2 Issue 2, Mar-Apr 2015

RESEARCH ARTICLE OPEN ACCESS

A Power Efficient Mac Protocol and Fault-Tolerant Event Boundary Detection in Wireless Sensor Networks

K. Madan Mohan [1], R. Sudha [2], K. Shalini [3], T. Poongothai [4]
PG Scholar [1], Communication Systems
Assistant Professor [2]
PG Scholar [4], Embedded Systems Technologies
Department of Electronics and Communication Engineering
Sri Shakthi Institute of Engineering and Technology
PG Scholar [3], Power Electronics and Drives
Department of Electrical and Electronics Engineering
C.S.I College of Engineering, Ooty
Tamil Nadu – India

ABSTRACT

Wireless sensor networks represent a key technology enabler for enhanced health care and assisted living systems. Recent standardization efforts to ensure compatibility among sensor network systems have produced the IEEE 802.15.4 standard, which specifies the MAC and physical layer behaviour. Energy and network life time are two critical factors for WSN performance. IEEE 802.15.4 is a standard used for low data rate Wireless Personal Area Networks (WPANs). Medium Access Control layer (MAC) of IEEE 802.15.4 plays an important role in the performance of Wireless Sensor Network (WSN). The unique feature of this MAC layer is the super frame structure. Event boundary detection is in and of itself a useful application in wireless sensor networks (WSNs). Typically, it includes the detection of a large-scale spatial phenomenon such as the transportation front line of a contamination or the diagnosis of network health. In this paper, we propose a cross-layer framework to prolong the network lifetime, to improve the energy and to lower the latency of WSNs and further we present SEBD, a fully distributed and light-weight Secure Event Boundary Detection scheme, which implements secure and fault-tolerant detection of event boundaries in an adversarial environment. An efficient key establishment protocol is first proposed which establishes location based keys at each sensor node to secure the communications. The idea of location-based keys also effectively minimizes the impact of node compromise such that a compromised node cannot impersonate other nodes at locations other than where it is. Then a collaborative endorsement scheme is designed to allow multiple nodes collectively endorsing a valid boundary claim for increased resilience against node compromise. SEBD further develops an enhanced statistical model that supports localized detection and shows a much better accuracy and fault tolerance property as compared to previous models. The security strength and performance of SEBD are evaluated by both analysis and simulations and we have considered hierarchical topology and peer to peer beacon enabled network to evaluate QoS. The performance metrics are evaluated using simulation results.

Keywords:- IEEE 802.15.4, Wireless Sensor Networks, Medium Access Layer, Hierarchical and peer to peer topology, Event boundary detection

I. INTRODUCTION

Wireless Sensor Networks are a new class of ad hoc networks that will find increasing deployment in recent years. Sensor networks enable reliable monitoring and analysis of the unknown and untested environment. Ease of deployment, extended range, fault-tolerance and mobility are some of the advantages of wireless sensor networks. Wireless sensor nodes are expected to be extremely small and battery operated. Protocols for these networks must be designed in such a way that the limited power in the sensor nodes should be used in the most efficient manner. The ageing population in many developed countries highlights the importance of novel technology-driven enhancements to current health care practices. Recent technological developments in the fields of sensing, actuation, processing, wireless communication, and information management have increased interest in technology-enhanced health care. For example is the use of wireless sensor networks to monitor hospital patient vital signs to allow the patient's greater freedom of movement. A major enabling technology of enhanced health care systems is wireless sensor networks (WSN). The large scale adoption of WSN technology for health care systems will depend on the Quality-of-Service

(QoS) provided by these networks, namely the reliability, latency, and efficiency. Further we propose a Secure Event Boundary Detection (SEBD) scheme, which allows secure detection of event boundaries in a localized manner, and is highly resilient against both node compromise and random measurement fault. In SEBD, with an efficient key establishment protocol, each sensor node establishes a unique secret key shared only with the sink, and several pairwise secret keys each shared with one of its neighbours. Those keys are bound to a node's physical location so even if the node is compromised, the impact is effectively confined to that particular node and at its particular
Location only. In SEBD, each node senses its local environment independently. Once an event of interest is detected, senor nodes first exchange their measurements among neighbours and benign nodes suppress possible faulty measurements following a majority rule. To enhance fault tolerance and prevent fabrication, once a node is detected as a boundary node, a number of its neighbours will collaboratively endorse the corresponding boundary claim message. A neighbour node endorses a boundary claim message only if the contained information is consistent with its own knowledge. The sink accepts a claim only when it contains a required number of valid endorsements. A nonparametric statistical boundary detection model is also developed, which is seamlessly integrated with the proposed security mechanism. It facilitates localized boundary node determination, and helps to suppress random measurement fault and malicious false readings. It shows a much higher accuracy and better fault-tolerance and compromise-resilience as compared to previous schemes

A. Why 802.15.4 MAC?

A new standard IEEE 802.15.4 was uniquely designed to suit personal wireless networks requirement consuming low power, provides low data rate and low cost. IEEE 802.15.4 is a short-range wireless technology intended to provide applications with relaxed throughput latency requirements in wireless personal area networks (PANs). The IEEE 802.15.4 standard has received considerable attention as a low data rate and low power protocol for wireless sensor network (WSN) applications in industry, control, home automation, health care, and smart grids. The key features of 802.15.4 are low complexity, low cost, low power consumption, and low data rate transmissions. Among all, the IEEE 802.15.4 MAC is the most promising for wireless sensor networks because of several reasons: It is well layered and provides a combination of link management mechanisms that can be enabled selectively depending on the user configuration.. It is the first standard which allows simple sensors and actuators to share standard wireless platform.

B. Device Classes

There are two kinds of devices used in WBAN which can be classified as Reduced Functionality Device (RFD) and Full Functionality Device (FFD). Star topology is an example for RFD. Device can communicate only with the Network Coordinator and devices cannot become a Coordinator as shown in Fig. 1(a). Any topology i.e., Peer-to - peer or Cluster- Tree can be used as an example for FFD. All devices have the Network Coordinator capability and device can communicate with any other device as in Fig 1(b).

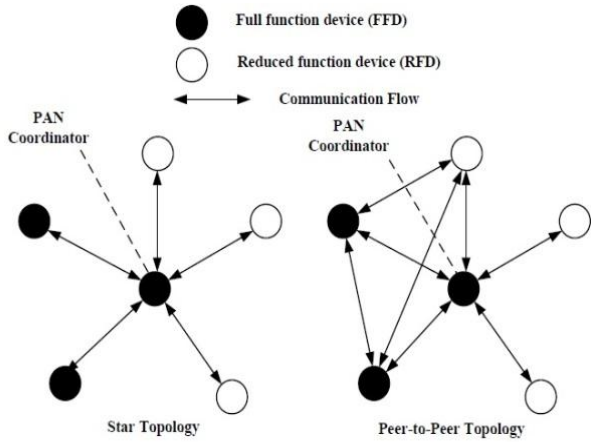

Fig 1.Network Topologies of IEEE 802.15.4

(a) Star topology (b) peer-to-peer topology

II. IEEE 802.15.4 ARCHITECTURE

The Architecture for 802.15.4 standard is entirely based on OSI model in the network. Each layer is responsible for one part of the standard and offers services to higher layers. 802.15.4 Standard defines both Physical and MAC layers of ZigBee Standard as shown in Fig. 2. Main features of PHY layer are activation and deactivation of the radio transceiver, Energy Detection (ED), Link Quality Indication (LQI) for received packets and Clear Channel Assessment (CCA). MAC sub-layer provides an interface between the Service Specific Convergence Sub-layer (SSCS) and PHY. MAC Sub-layer handles all access to the physical radio channel and is responsible for providing services to the Application layer through two groups: MAC Data Service and MAC Layer Management Entity. MAC Layer Management Entity (MLME) is the Management Entity included in MAC Sublayer. This is accessed through MLME-SAP. MLME also responsible for maintaining a database of managed objects referred to as the MAC sub-layer PIB. MAC data service is accessed through the MAC Common Part Sub-layer (MCPS) data SAP.

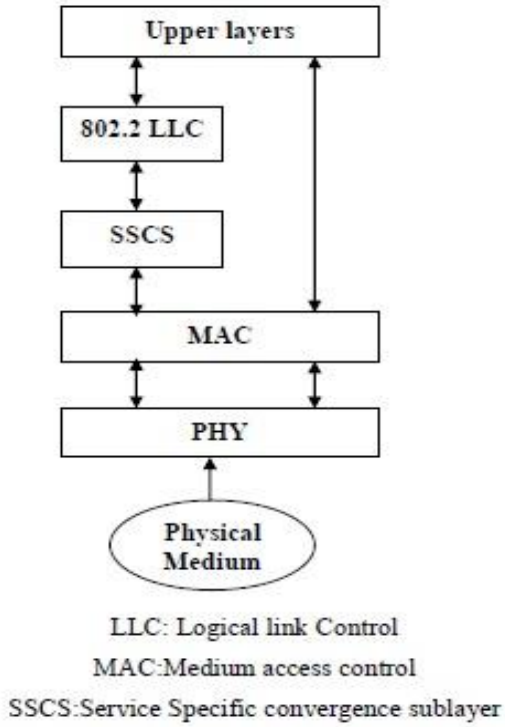

Fig 2. IEEE 802.15.4 LR-WPAN device architecture

A. PHY Layer

The PHY layer specification dictates how IEEE 802.15.4 may communicate with each other over the wireless channel. Use of frequency bands are allowed with varying data rates. The bit rates are 20 Kbps in the European for 868 MHz band (868-868.6 MHz) with a single channel between this band, 40 Kbps in the North American for 915 MHz band (902-928 MHz) with 10 channels and 250 Kbps in the worldwide for 2.45 GHz band (2.4-2.4835 GHz) with 16 channels between this band. All these frequency bands are based on Direct Sequence Spread Spectrum (DSSS) spreading technique. The 865 MHz and the 915 MHz radio map each data symbols onto a 15-chip PN sequence, followed by binary phase-shift keying (BPSK) for chip modulation. On the other hand, 2.45 GHz Industrial Scientific Medical (ISM) radio band maps each 4 bits of information onto a 32 chip PN sequence followed by offset orthogonal phase shift keying (O-QPSK).

B. 802.15.4 MAC Operational modes

MAC layer is responsible for Beacon Management, Channel Access, Frame Validation, Acknowledged Frame delivery, Association and Dissociation. The MAC supports two operational modes Beacon and Non-Beacon.

Non-Beacon Enabled mode: A network node can send data to the coordinator at its will by using unslotted CSMACA and to receive data from the coordinator, the node must power up and poll the coordinator. Advantage is that the node's receiver does not have to regularly power-up to receive the beacon. The disadvantage is the coordinator cannot communicate at will with the node but must wait to be invited by the node to communicate.

Beacon Enabled mode: The network is fully synchronized as the coordinator sends out periodic packets or beacons. This mode uses the Superframe structure of 802.15.4 MAC.

C. Superframe Structure

Key feature of 802.15.4 MAC layer are the superframe structure, which allows devices to access channels in a Contention Access Period (CAP) or a Collision Free Period (CFP) and the beacon based synchronization mechanism .The format of the superframe structure is determined by the coordinator. Structure of superframe is described by the values of macBeaconOrder (BO) and macSuperframeOrder (SO) as in Fig. 4. MacBeaconOrder defines the interval at which the coordinator shall transmit its beacon frames. MacSuperframeOrder defines the length of active portion of the superframe along with the beacon.

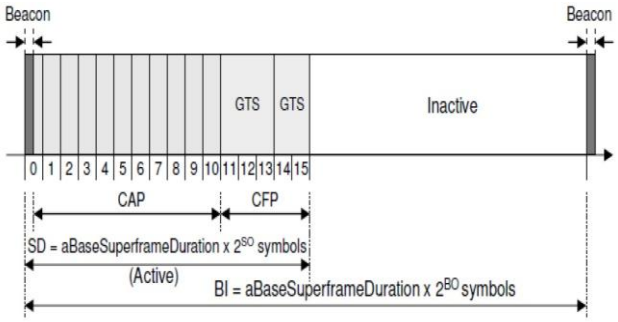

Fig 3. Superframe structure in IEEE 802.15.4 standard

III. SEBD: THE SCHEME

A. Problem Identification

In this part, we describe how the event boundary detection schemes proposed under trustworthy environments would fail in adversarial environments. In adversarial environments, sensor nodes could be compromised and controlled by the attacker these compromised nodes will lie about their measurements and result in severe security threat, which greatly jeopardizes boundary detection functionality of a WSN. Both faulty nodes and compromised nodes may inappropriately cause non boundary nodes (including themselves) to be recognized as boundary nodes due to the nature of statistical method used by most of exiting schemes. However, the damage caused by the compromised nodes is much worse than that of faulty nodes. This is because a *faulty* node is still a benign node, and would suppress its own measurements after referring to other measurements in its neighbourhood. However, a *compromised* node will always lie about its measurements, report itself as a

boundary node when it is not, and suppress such claims when it is1. A collection of compromised nodes could prevent the event boundary from being correctly detected by presenting false measurement information. Moreover, compromised nodes may collude to fabricate non-existing events and event boundaries. They may claim such boundaries appearing at any location of the network as desired by the attacker, not necessarily at their own actual locations.

B. Contributions

This paper makes the following contributions:

We introduce the problem of securing event boundary detection in WSNs for applications related to large-scale spatial phenomena monitoring, and show how existing boundary detection schemes would fail in adversarial

Environments. We assume that sensor nodes are similar to the current generation of sensor nodes in their computation and communication capability and power resource and they are loosely synchronized. We assume that even if sensor nodes may execute certain sleeping strategy for energy conservation, they can still wake up periodically or be woken up by certain events to work collaboratively, according to certain wakeup mechanism. We assume that sensor nodes can make random measurement errors, and

Such nodes are called *faulty* nodes. Furthermore, we assume that sensor nodes can be compromised and controlled by then adversary, whose purposes are to 1) prevent event boundary from being correctly detected; 2) collude to fabricate no existing events and event boundaries.

C. Overview of SEBD

The proposed SEBD is designed to be robust against node compromise and random fault. SEBD consists of two key components: the underlying location-aware key management framework, and the corresponding distributed statistic boundary detection model that is seamlessly built upon the former. Key management framework in SEBD exploits the static and location-aware nature of WSNs. By leveraging robot assisted secure bootstrapping technique, a secure location aware key management is efficiently realized through embedding location information into the keys. In SEBD, each node possesses two different types of location-aware symmetric keys: 1) a *unique secret key* shared between the node and the sink that is used to provide node-to-sink authentication and data confidentiality; 2) a set of *neighbour pairwise key*s shared with each of the neighbour nodes respectively for node-to-node authentication and data confidentiality. In our design, a sensor, after having detected an event of interest, proceeds to find out whether or not it is a boundary sensor. More specifically, SEBD detects an event boundary in three essential stages: In 1) *local sensing and measurement adjusting* stage, each node exchanges its event measurement in the neighbourhood. Then, every node adjusts its own measurement result according to *the majority rule*. Next, in 2) *distributed boundary detection* stage, each node independently determines whether or not it is a boundary node according to the updated measurements distribution in its neighbourhood and the predefined statistic model. Lastly, in 3) *final message composition* stage, a boundary node constructs an overall synthesized endorsement from the individual ones it collected from its neighbours. The sink only accepts a boundary claim with a valid overall synthesized endorsement.

IV. PROPOSED ARCHITECTURE

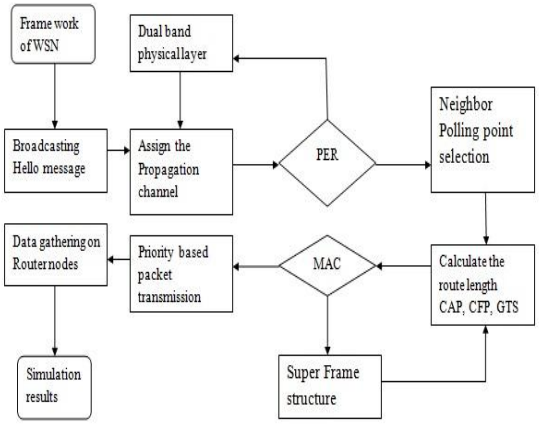

Fig 4. Architecture of Proposed System

The working sensor networks (WSN) is shown in Fig. 7 which describes all the modules involved. Initially the network is created by assigning the nodes in the framework of WSN. Then the assigned nodes are broadcasted for their route request and route reply. In the PHY layer, propagation channel is assigned using two ray models. Then it is routed using LEACH protocol for selection of neighbour polling point.

Low Energy Adaptive Clustering Hierarchy (LEACH) , a wireless sensor network routing protocol which employed as a widely known communication protocol in today's era based on the concept of hierarchical routing. The prime focus of this protocol is to enhance the energy utilization. It works as a stand in protocol for wireless sensor network which help to deal with consumption of energy at particular level. LEACH protocol, network nodes are arranged in cluster, random algorithm select some number of node that act as cluster head. Cluster head accumulates data and aggregate to the base station. LEACH has two phase protocol as in Fig 8.

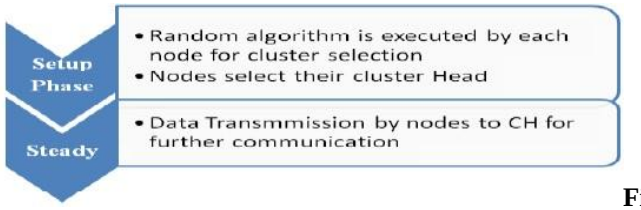

Fig 5. Phases of LEACH

In the MAC protocol superframe structure, changes has been made for power efficiency and GTS is allocated for proper delivery. The entire connection is established using peer-to-peer network topology and priority based packet transmission is obtained. The obtained data of router nodes are gathered and their performance metrics are analysed using simulation results.

V. SIMULATION RESULTS

The simulations have been performed using GloMoSim a scalable wireless networks simulator. The simulation parameters are listed in the Table. To evaluate the performance of beacon enabled peer-to-peer topology using leach routing protocol is analysed using the following performance metrics.

Packet Delivery Ratio

It is the ratio of the number of data packets successfully delivered to the destination nodes to the total number of data packets sent by source nodes.

Average End-to-End Delay

It indicates the length of time taken for a packet to travel from the CBR (Constant Bit Rate) source to the destination. It represents the average data delay an application or a user experiences when transmitting data.

Throughput

It is the number of bits passed through a network in one second. It is the measurement of how fast data can pass through an entity (such as a point or a network).

Energy Consumption

This is amount of energy consumed by devices for the periods of transmitting, receiving, idle and sleep. The unit of energy consumption used in the simulations is mJoule.

Network Lifetime

This is defined as the minimum time at which maximum number of sensor nodes will be dead or shut down during a long run of simulations.

VI. RESULTS FOR POWER EFFICIENCY

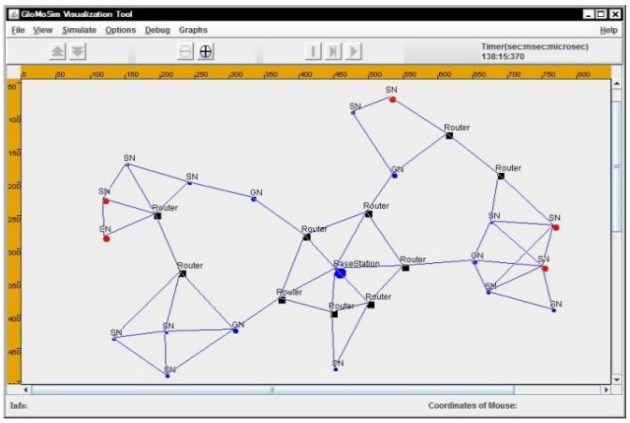

Fig 6. Simulation of Sensor Network

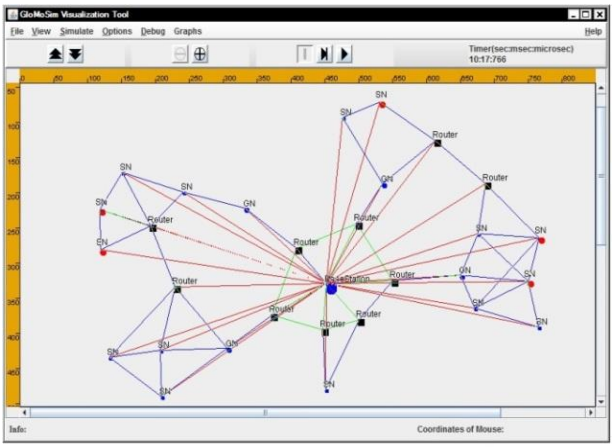

Fig 7. Routing Information of all the nodes in the network

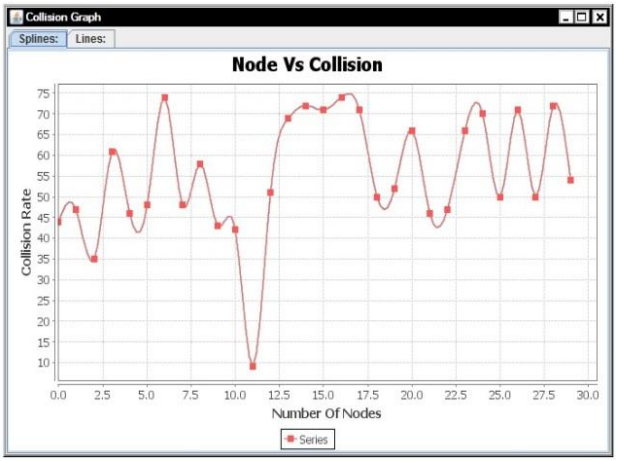

Fig 8. Simulated Result of Node Vs Collision

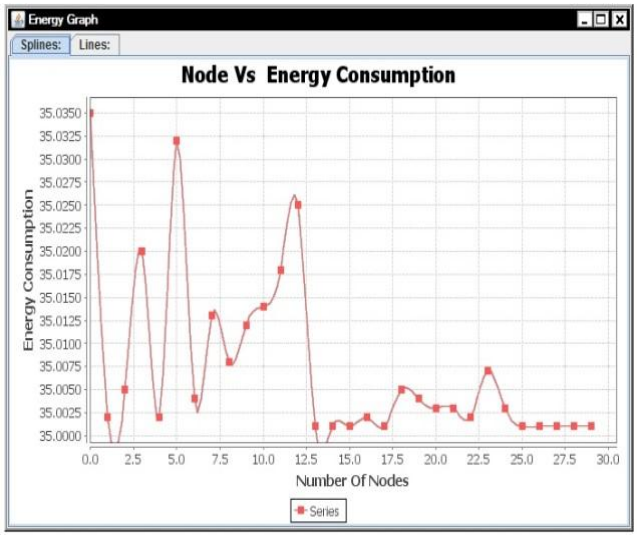

Fig 9. Simulated Result of Node Vs Energy Consumption

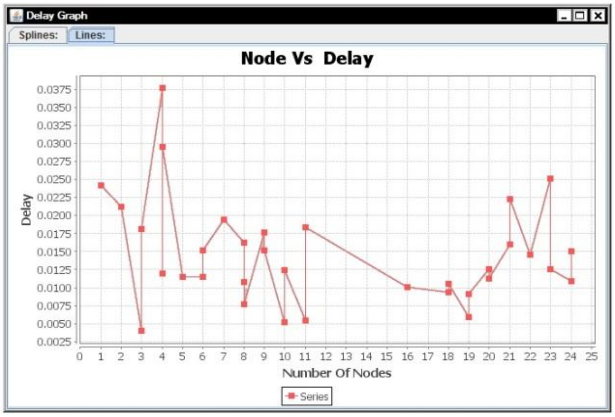

Fig 10. Simulated Result of Node Vs Delay

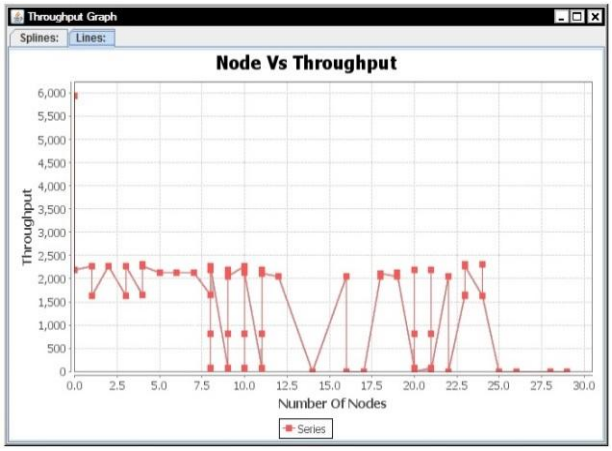

Fig 11. Simulated Result of Node Vs Throughput

VII. RESULTS OF EVENT BOUNDARY DETECTION

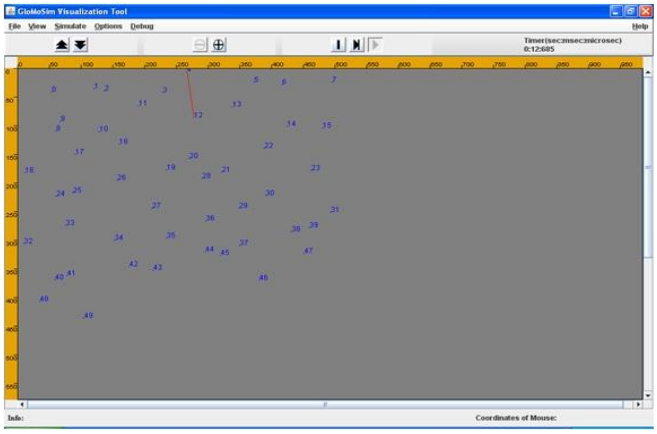

Fig 12. Red line access its neighbour node

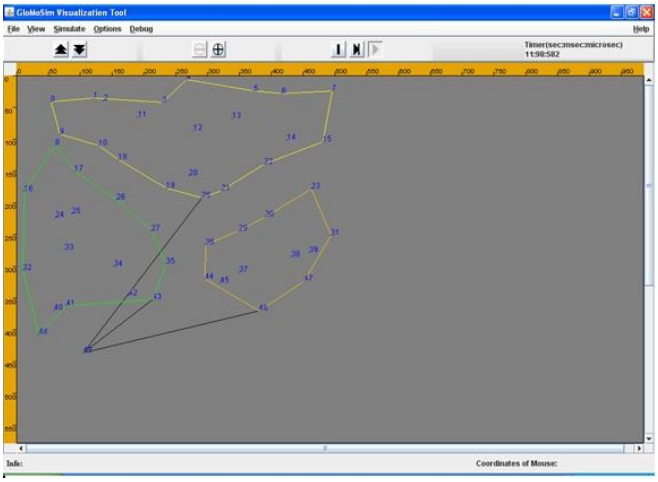

Fig 13. Black colour-sink node connectivity Yellow,Green,Orange-Boundary Formation

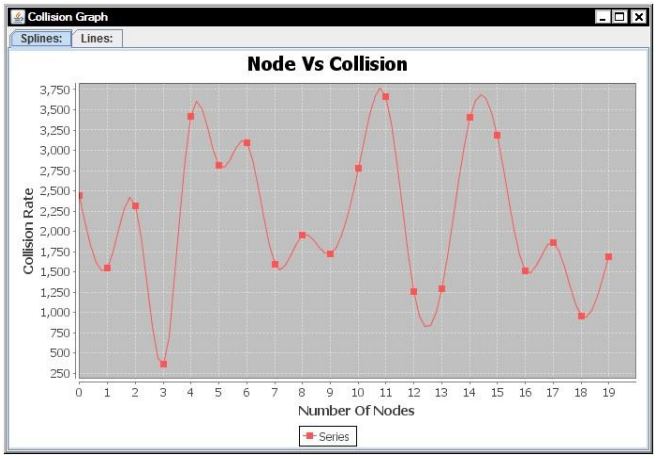

Fig 14. Simulated Result of Node Vs Collision

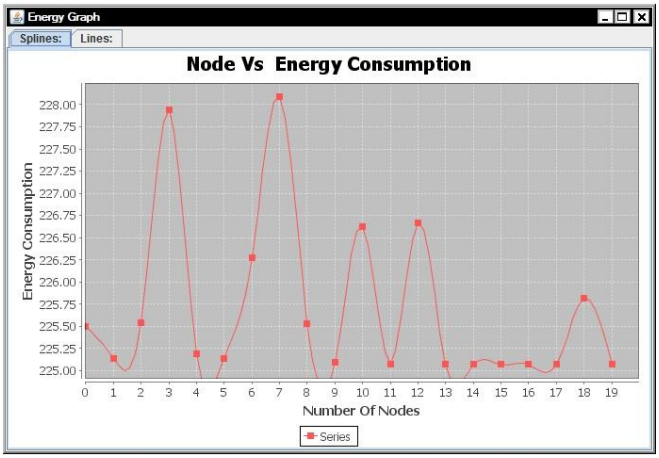

Fig 15. Simulated Result of Node Vs Energy Consumption

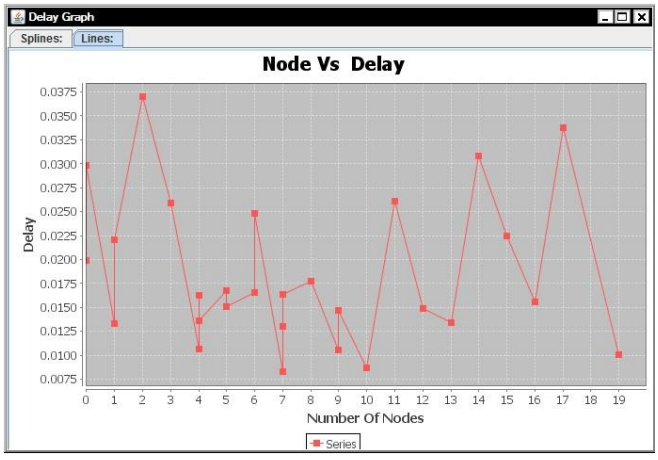

Fig 16. Simulated Result of Node Vs Delay

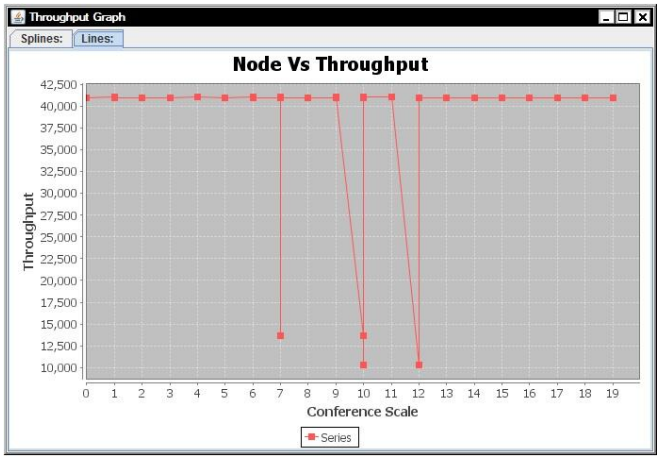

Fig 17. Simulated Result of Node Vs Throughput

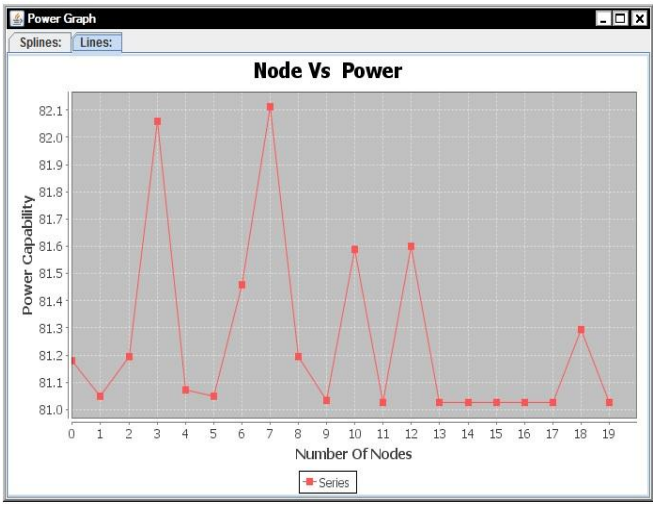

Fig 18. Simulated Result of Node Vs Power

VIII. CONCLUSION AND FUTURE WORK

Wireless sensor networks are mainly designed for application requiring very low power consumption and medium communication ranges. In this paper effectiveness of 802.15.4 networks supporting WSN applications were investigated using simulation results. Furthermore, the effectiveness of fault-tolerant detection also identified using simulation results. Moreover, in the simulation results the evaluation of per node sensor of throughput, energy consumption, collision, delay and power capacity are done. Henceforth, the identification of power capacity and fault-detection is performed successfully using simulation results. The Quality of Service parameters can be evaluated for the entire network and fault tolerance detection can also be included in the future work.

REFERENCES

[1] IEEE 802.15.4, Part 15.4: " Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low - Rate Wireless Personal Area Networks (LR-WPANs)," September 2006, revision of IEEE Std 802.15.4-2003.

[2] J. KO,C. Lu, M. B. Srivastava, J.A.Stankovic , W.Trevis and Welsh, "Wireless sensor networks for healthcare," Proceedings of the IEEE, vol.98, no.11, pp.1947–1960. 2010. (

[3] Dilmaghani S.R.; Bobarshad, H.; Ghavami, M.; Choobkar, S.; and Wolfe, C.; (2011): "Wireless Sensor Networks (WSNs) for Monitoring Physiological Signals of Multiple Patients". *IEEE Transaction* on biomedical circuits and systems, vol. 5, no. 4, August 2011.

[4] J. Zheng and M.J .Lee , " A Comprehensive Performance Study of 802.15.4" in Sensor Netw orks , IEEE Press, 2006, ch.4, pp.218-237.

[5] G. Lu, B. Krishnamachari and C. S. Raghavendra, "Performance evaluation of the IEEE 802.15.4 MAC for low-rate low-power wireless networks,"in *Proc. Workshop EWCN*, Apr. 2004, pp. 701–706.

[6] B. Krishnamachari and S. Iyengar, "Distributed bayesian algorithms for fault-tolerant event region detection in wireless sensor networks," *IEEE Trans. Computers*, vol. 53, no. 3, pp. 241–250, Mar. 2004.

[7] M. Ding, D. Chen, K. Xing, and X. Cheng, "Localized event detection in sensor networks," in *Proc. IEEE INFOCOM*, Mar. 2005.

[8] T. Clouqueur, K. Saluja, and P. Ramanathan, "Fault tolerance in collaborative sensor networks for target detection," *IEEE Trans. Computers*, vol. 53, no. 3, pp. 320–333, 2004.

[9] UCLA Parallel Computing Laboratory. GloMoSim- Global Mobile Information Systems Simulation Library, Webpage,February2006. http://pcl.cs.ucla.edu/projects/glomosim/.

[10] The IEEE 802.15.4 Web Site, 2006.Available: http://www.ieee802.org.

Madan Mohan. K was born in the Nilgiris, Tamilnadu, India. He has received his B.E.degree in Electronics and Communication engineering from M.P.N.M.J Engineering College, Anna University, Chennai in the year 2013.He is currently pursuing his M.E .(Communication Systems) in Sri Shakthi Institute of Engineering and Technology, Anna University, Chennai. He has published six International Conferences. His research interests include Pervasive computing and wireless sensor network, Communication and networking.

Sudha.R was born in Coimbatore, Tamilnadu, India. She has received her B.E.degree in Electronics and Communication engineering from Bharathiar University in the year 2004 and M.E degree in Communication Systems from the Anna university in the year 2006. She started her teaching career in 2006. She has published Seven International Journals and 2 International Conferences. Her research interest includes Antenna,Signal Processing,Comunication Systems.

Shalini.K was born in the Nilgiris, Tamilnadu, India. She has received her B.E. degree in Electrical and Electronics Engineering from C.S.I. College of Engineering, Anna University, Chennai, in the year 2010 and M.E. degree in power electronics and drives from the same Institution in the year 2014. She has published two International Journals and four International Conferences. Her research interests include input power-factor-correction techniques, high-frequency soft-switching power converters and power converters for telecommunications applications. She is an active member of IET Student forum.

Poongothai. T was born in the Salem, Tamilnadu, India. She has received her B.E.degree in Electronics and Communication engineering from Pavai College of technology, Anna University, Chennai in the year 2013.She is currently pursuing her M.E .(Embedded System Technologies) in Sri Shakthi Institute of Engineering and Technology, Anna University, Chennai.Her research interests include Embedded networking Protocols and wireless sensor network.

.
.