ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

Performance Analysis of QoS Parameters in IEEE 802.15.4 (Zigbee)

Shinderpal Kaur[1], Dr. Mahendra Kumar[2]
PG Scholar[1], Deputy Dean Research[2]
Department of Electronics and Communication
Guru Kashi University, Talwandi sabo, Bathinda, Punjab, India

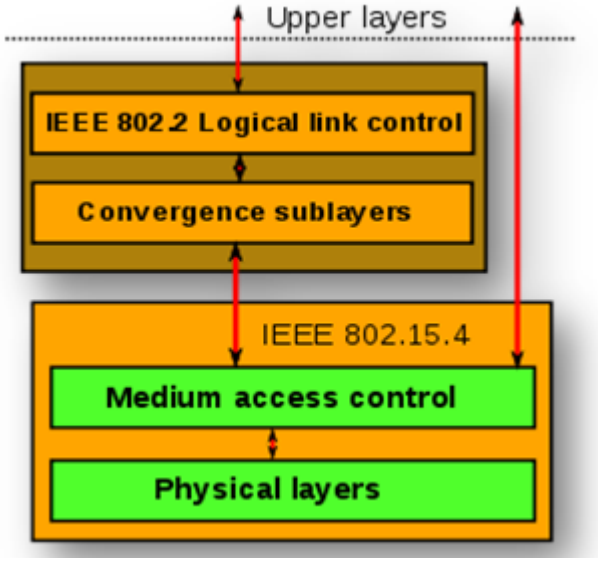
Abstract:
Wireless Sensor Network (WSN) consists of a large population of sensor nodes capable of computation, communication and sensing. In this paper author have studied performance of IEEE802.15.4 (ZigBee) using various parameters. Author found that the throughput was decreases with respect increase in number of nodes and packet drop also increases with increase in number of nodes.

Keywords: Wireless sensor network, throughput, packet drop, ZigBee, IEEE 802.15.4

I. INTRODUCTION

ZigBee [1]is an IEEE 802.15.4 based standard specification for a suite of high level communication protocols used to create personal are networks with small, low power digital radios, such as for home automation, medical device data collection and other low power low bandwidth needs, designed for small scale projects which need wireless connection. The technology defined by the ZigBee specification is intended to be simpler and less expensive than other wireless personal area networks (WPANs), such as Bluetooth or Wi-Fi. Applications include wireless light switches, electrical meters with in home displays, traffic management systems and other consumer and industrial equipment that requires short –range low-rate wireless data transfer. Its low power consumption limits transmission distances to 10-100 meters line-of-sight, depending on power output and environmental characteristics [2]. ZigBee devices can transmit data over long distances by passing a data through a mesh network of intermediate devices to reach more distant ones. ZigBee is typically used in low data rate applications that require long battery life and secure networking (ZigBee networks are secured by 128 bit symmetric encryption keys.) ZigBee has a defined rate of 250 kbits/s, best suited for intermittent data transmissions from a sensor or input device. ZigBee was conceived in 1998, standardized in 2003 and revised in 2006. The name refers to the waggle dance of honey bees after their return to the beehive[3].ZigbEE is a low-cost, low power, wireless mesh network standard targeted at the wide development of long battery life devices in wireless control and monitoring applications. ZigBee device have low latency which further reduces average current. ZigBee chips are typically integrated with radios and with microcontrollers that have between 60-256 KB of flash memory. ZigBee operates in the industrial, scientific and medical radio bands: 2.4 GHz in most jurisdictions worldwide; 784 MHz in China, 868 MHz in Europe and 915 MHz in the USA and Australia. Data rates vary from 20 kbits/s (868 MHz€) to 250 kbits/s (2.4 GHz band). The ZigBee network layer natively supports both star and tree networks and generic mesh networking. Every network must have one coordinator device, tasked with its creation, the control of its parameters and basic maintenance. Within star networks, the coordinator must be the central node. Both trees and meshes allow the use of ZigBee routers to extend communication at the network level. ZigBee builds on the physical layer and media access control defined in standard IEEE 802.15.4 for low rate WPANs. The specification includes four additional key components: network layer, application layer, ZigBee device objects (ZDOs) and manufacturer defined application objects which allow for customization and favor total integration. ZDOs are responsible for some tasks, including keeping track of device roles, managing requests to join a network, as well as device discovery and security. ZigBee is one of the global standards of communication protocols formulated by the significant task force under the IEEE 802.15 working group. The fourth in series, WPAN low rate/ZigBee is the newest and provides specification for devices that have low data rates, consume very low power and are thus characterized by the long battery life. Other standards like Bluetooth and IrDA address high data rates applications such as voice [4], video and LAN communications. IEEE 802.15.4 is a technical standard which defines the operation of low-rate wireless personal area networks (LR-WPANs). It specifies the physical layer and media access control for LR-WPANs, and is maintained by the IEEE 802.15 working group, which defined the standard in 2003[5]. It is the basis for the ZigBee, ISA100.11a, Wireless HART ,Mi Wi, SNAP, and Thread specifications, each of which further extends the standard by developing the upper layers which are not defined in IEEE 802.15.4[6][7]. Alternatively, it can be used with 6LoWPAN, the technology used to deliver the IPv6 version of the Internet Protocol (IP) over WPANs, to define the upper layers. IEEE standard 802.15.4 intends to offer the fundamental lower network layers of a type of wireless personal area network (WPAN) which focuses on low-cost, low-speed ubiquitous communication between devices. It can be contrasted with other approaches, such as Wi-Fi, which offer more bandwidth and require more power. The emphasis is on very low cost communication of nearby devices with little to no underlying infrastructure, intending to exploit this to lower power consumption even more. The basic framework conceives a 10-meter communications range with a transfer rate of 250 kbit/s. Tradeoffs are possible to favor more radically embedded devices with even lower power requirements, through the

definition of not one, but several physical layers. Lower transfer rates of 20 and 40 kbit/s were initially defined, with the 100 kbit/s rate being added in the current revision. Even lower rates can be considered with the resulting effect on power consumption. As already mentioned, the main identifying feature of IEEE 802.15.4 among WPANs is the importance of achieving extremely low manufacturing and operation costs and technological simplicity, without sacrificing flexibility or generality. Important features include real-time suitability by reservation of guaranteed time slots, collision avoidance through CSMA /CA and integrated support for secure communications. Devices also include power management functions such as link quality and energy detection. IEEE 802.15.4-conformant devices may use one of three possible frequency bands for operation (868/915/2450 MHz).



Protocol architecture

FigURE.1. IEEE 802.15.4 protocol stack

Devices are conceived to interact with each other over a conceptually simple wireless network. The definition of the network layers is based on the OSI model; although only the lower layers are defined in the standard, interaction with upper layers is intended, possibly using an IEEE 802.2 logical link control sublayer accessing the MAC through a convergence sublayer. Implementations may rely on external devices or be purely embedded, self- functioning devices

DEVICE TYPES

- ZigBee Coordinator (ZC): The most capable device, the Coordinator forms the root of the network tree and might bridge to other networks. There is precisely one ZigBee Coordinator in each network since it is the device that started the network originally (the ZigBee Light Link specification also allows operation without a ZigBee Coordinator, making it more usable for over-the-shelf home products). It stores information about the network, including acting as the Trust Center & repository for security keys.
- *ZigBee* Router *(ZR)*: As well as running an application function, a Router can act as an intermediate router, passing on data from other devices.
- ZigBee *End Device (ZED)*: Contains just enough functionality to talk to the parent node (either the Coordinator or a Router); it cannot relay data from other devices. This relationship allows the node to be asleep a significant amount of the time thereby giving long battery life. A ZED requires the least amount of memory, and, therefore, can be less expensive to manufacture than a ZR or ZC.

2. EXPERIMENTAL SETUP

The main objective of this simulation study was to evaluate the performance analysis of QoS parameters in IEEE 802.15.4. In this simulation three scenario are set up in which mobile and fixed nodes are used. In Application Traffic packet size is reduced to 512 (constant) bits from 1024 bits. After reducing the packet size throughput and packet drops are compared graphically. Snapshots of these scenario are as following:

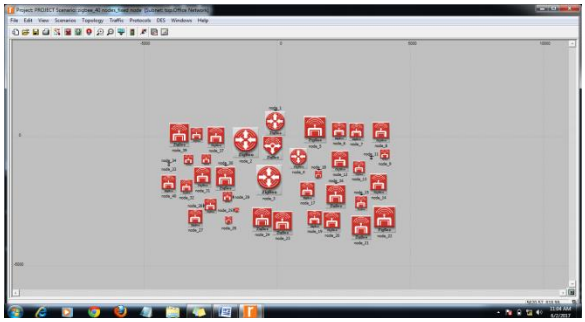


Figure.2. ZigBee_40nodes_fixed nodes

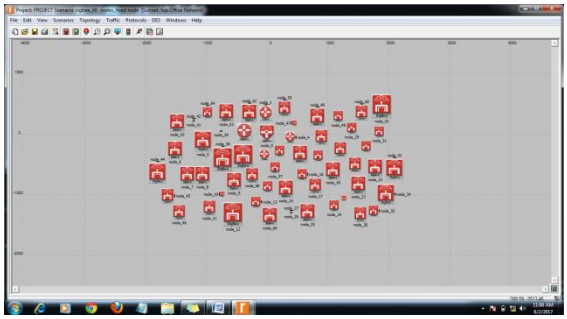


Figure.3. ZigBee_60nodes_fixed nodes

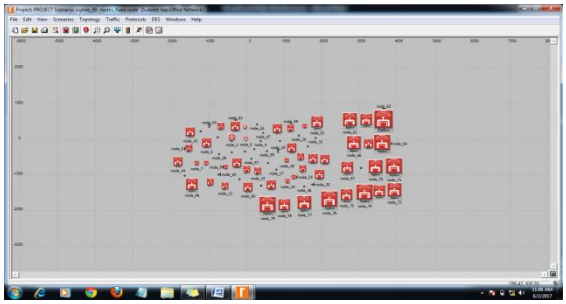


Figure.4. ZigBee_80nodes_fixed nodes

These are three scenarios that are simulated using OPNET Simulator. In this paper throughput and packet drops are compared graphically by reducing the bit rate to 512 bits from 1024 bits.

3. RESULTS

3.1 Throughput

Throughput or network throughput is the rate of successful message delivery over a communication channel. The data these messages belong to may be delivered over a physical or logical link, or it can pass through a certain network node. Throughput

is usually measured in bits per seconds (bit/s or bps), and sometimes in data packets per second (p/s or pps) or data packets per time slot. Comparison graph of throughput in ZigBee fixed nodes and mobile nodes are as following:

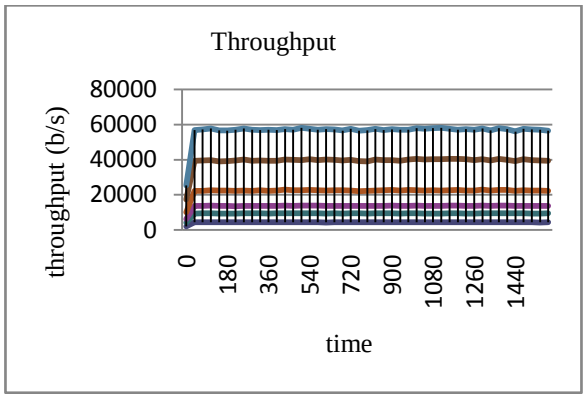


Figure.5. Throughput mobile nodes vs. fixed nodes

3.2 PACKET DROP

A packet drop attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes. The packet drop attack is very hard to detect and prevent.

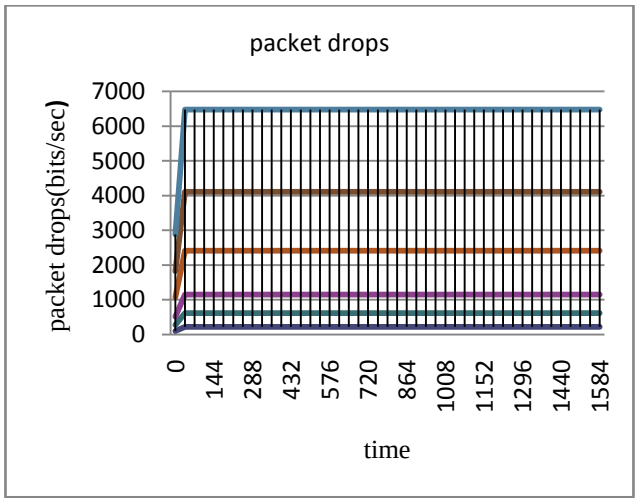


Figure.6. Packet drops mobile nodes vs. fixed nodes

4. CONCLUSION AND FUTURE WORK

ZigBee will play an important role in the future in the areas such as home automation, smart lighting, traffic management etc and will make computer and communication technology more useable and accessible to users. These networks are easy to deploy which is cheaper as compared to other technologies. ZigBee technology is very useful from the perspective of the security as the devices maintain a list of trusted devices within the network and frame integrity to protect data from being modified by the parties without cryptographic keys. Due to its emergence, researchers are facing many challenges in the development and deployment of the technology but due to the intensive research, all the problems are being sorted out day by day and the technology is becoming less prone to the problems and also becoming more reliable and sustainable. In this paper packet size is reduced and seen the effects on throughput and packet drops. In future other values can be used to note the effect on these terms.

5. REFERENCES

[1]. "ZigBee: Brief introduction". Noor UI Mushtaq. Retrieved 2016-11-05.

[2]. "ZigBee specification FAQ". ZigBee Alliance. Retrieved 14 June 2013.

[3]. "ZigBee Wireless Networking". Drew Gisleson.

[4]. "IEEE 802.15.4". Ieee 802. Retrieved 2012-10-18.

[5]. IEEE 802.15 WPAN™ Task Group 4,

[6]. Gascón, David (February 5, 2009). "Security in 802.15.4 and ZigBee networks"

[7]. *"ISA100 Committee Home Page".*