1-1-2012

Accommodating Machine-To-Machine Traffic In IEEE 802.15.4: The Prioritized Wait Time Approach

Vida Azimi
Ryerson University

ACCOMMODATING MACHINE-TO-MACHINE TRAFFIC

IN IEEE 802.15.4: THE PRIORITIZED WAIT TIME APPROACH

By

Vida Azimi

A thesis
presented to the school of graduate studies at
Ryerson University
in partial fulfillment of the
requirements for the degree of

Master of Applied Science
(Computer Networks)

Department of electrical and computer engineering

Toronto, Ontario, Canada, 2012

Author's Declaration

I hereby declare that I am the sole author of this thesis.

I authorize Ryerson University to lend this thesis or dissertation to other institutions or individuals for the purpose of scholarly research.

Author's signature: _____

I further authorize Ryerson University to reproduce this thesis or dissertation by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

Author's signature: _____

ACCOMMODATING MACHINE-TO-MACHINE TRAFFIC IN IEEE 802.15.4: THE PWT APPROACH

Master of Applied Science

Computer Networks

Ryerson University

Abstract

Machine-to-Machine communication (M2M) refers to automated applications executing on smart devices or machines that communicate through a network with little or no human intervention at all. By enabling smart devices to communicate directly with one another, M2M communications technology has the potential to radically change the world around us and the way that we interact with objects. Many applications can benefit from M2M communications, such as transportation, health care, smart energy production, transmission, and distribution, logistics, city automation and manufacturing, security and safety, and others. This work describes an approach to implement M2M communications using the well-known IEEE 802.15.4 / ZigBee communications standard for low data rate wireless personal area networks. In order to achieve better performance for M2M traffic, we propose some improvements in the protocol. Our simulation results confirm the validity of the proposed approach under a wide range of network and traffic parameters.

Acknowledgments

First of all, I would like to express my thanks to my thesis supervisor Vojislav Mišić for his patient supervision, help and support leading towards this thesis.

Also I wish to express my sincere appreciation to Dr. Ngok-Wah (Bobby) Ma for his continued support and guidance.

Finally, I like to extend my gratitude to the members of the graduate school and Ryerson University for their valuable input.

I would like to thank all the committee members for their participation in my thesis defense.

I wish to convey the warmest thanks to my family for their endless support.

Ryerson University in TORONTO *Vida Azimi*

1 TABLE OF CONTENTS

List of Tables

List of Figures

Acronyms

3G	3rd Generation cellular communication systems
4G	4th Generation cellular communication systems (e.g., LTE)
3GPP	3rd Generation Partnership Project
APL	Application Layer (in ZigBee networks)
APS	Application Support Sub-Layer
CAP	Contention Access Period
CCA	Clear Channel Assessment
CCSA	China Communications Standards Association
CFP	Contention Free Period
CN	Core Network
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
CW	Contention Window
ETE delay	End-to- end delay
eUTRAN	Evolved Universal Terrestrial Radio Access Network
GBR	Guaranteed Bit Rate
ISM	Industrial, Scientific, and Medical RF band at 2400 - 2483.5 MHz
M2M	Machine To Machine (communications)
MAC	Medium Access Control layer
MTC	Machine Type Communication
NWK	Network Layer (in ZigBee)
PHY	Physical layer
QoS	Quality of Service

UE	User Equipment (a device connecting to the cellular network)
VLR	Visitor Location Register (in GSM networks)
VOIP	Voice Over IP
WLAN	Wireless Local Area Network
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
ZED	ZigBee-enabled device
ZDO	ZigBee Device Object

1. INTRODUCTION

Machines are becoming an important participant in communication networks, from industry to smart homes. Essentially, Machine-to-Machine communication (M2M), also called Machine Type Communications (MTC), refers to automated applications executing on smart devices or machines that communicate through a wired and/or wireless network with very little human intervention or none at all [1].

By enabling smart devices to communicate directly with one another, M2M communications technology has the potential to radically change the world around us and the way that we interact with objects, as the communication devices can be implanted in different environments such as cars, appliances, smart homes, vending machines, and other objects we encounter in our daily lives.

There are many applications that can benefit from M2M communications, such as transportation, health care, smart energy production, transmission, and distribution, logistics, city automation and manufacturing, security and safety, and others.

However, the development of advanced M2M networks is not a straightforward task. First, there are two alternative architectures that can be used for such networks. In the first, often referred to as cellular M2M, individual M2M devices are equipped with cellular wireless interfaces, be they 3G or 4G, and are thus able to communicate directly with existing mobile operator networks through cellular base stations. While offering significant potential, this solution is not perfect, primarily on account of its high cost and higher energy consumption, as will be shown in the results.

In the second architecture, often referred to as capillary, individual M2M devices are organized in wireless networks similar to wireless sensor networks, through which they send data to appropriate gateway that aggregate the data and send it over to the mobile operator network or, sometimes, directly to the M2M server through a wireline network. While much cheaper to implement and deploy, this architecture may suffer from insufficient performance compared to its cellular counterpart. Improving the performance of capillary M2M networks implemented using contemporary standards is the main topic of this thesis.

Thesis Contribution

This thesis deals with the use of IEEE 802.15.4 / ZigBee communications technology to service M2M traffic. In order to improve the performance of the network for M2M nodes, we propose improvements to the protocol which consist of small adjustments to the parameters of the protocol and should, therefore, be simple to implement in practice. Moreover, no changes would be required to allow existing IEEE 802.15.4 / ZigBee nodes to be used in improved networks. The results of our simulations show the versatility of the proposed improvements and demonstrate that a substantial advantage is obtained in terms of throughput, even though the delay appears to be about the same or even slightly longer than in the standardized solution. Still, the limits of the delay are sufficiently relaxed so that this impairment should not affect the performance of M2M traffic.

Thesis Organization

We begin by presenting the main properties of M2M communications (Section 2) and discussing the architectural options for implementing M2M networks, their relative advantages and disadvantages. We also present the rationale for focusing

on capillary M2M.

We then investigate the performance of wireless sensor networks used in the capillary approach to M2M networking, and describe the pertinent characteristics of the popular IEEE 802.15.4/ ZigBee network technology in Section 3.

In Section 4 we investigate the performance of such networks and describe a simple improvement that should render them better suited for use in the capillary part of M2M networks. Then, in Section 5 we analyze the performance of the improved solution in comparison to the standardized version of IEEE 802.15.4 using extensive simulations.

Finally, Section 6 summarizes the work and points out some promising directions for future work.

2. MACHINE- TO- MACHINE COMMUNICATIONS GENERAL CONCEPTS AND BACKGROUND

M2M is a paradigm of data communication which involves one or more intelligent or smart entities that do not necessarily need human intervention [2]. A common M2M scenario begins with a smart device (sensor, meter, or the like) used to capture an event or a series of events, or to measure some variable of interest (temperature, supply level, etc.). This last procedure oftentimes involves conversion of analog measurements to digital data. The data about the event or measurement is then sent through a network (wireless, wired or a hybrid of the two depending mainly on the required QoS [3] but also the cost) to an application (software program) [4] running on a server operated by the service provider or network operator. Afterwards, commands from the servers may be sent back to the devices, instructing them to undertake certain actions, change the parameters of their operation, or go to sleep for a predefined period of time. The devices involved in a M2M application are called M2M devices [2]. They need to have the required functionality, typically consisting of sending data automatically or upon request to the appropriate server, and responding to commands issued by the servers. In regular operation, M2M devices need little human intervention or, preferably, no human intervention at all. However, human involvement is still needed to interpret the results recorded by the servers, or to initiate an intervention in case of malfunction or failure. A typical example of such a device would be an electricity or gas meter with remote reading capability: it is installed by humans and maintained (i.e., serviced) by humans, but does not need human intervention for years unless a repair or a replacement is in order.

M2M Applications

M2M applications enable independent devices such as industrial meters to communicate with mobile applications.

Application that are capable of producing alerts like fire detector and personal security/anti-theft, wake up upon detecting the event that should be reported to the appropriate server or human operator, and send their alerts and notifications to appropriate response centers. During the rest of the time, the devices remain in idle state and they are effectively detached from the network.

Examples of M2M applications are shown in Table 2 below. In a competitive marketplace, M2M applications thus offer a vast potential for strategic differentiation of operators in all of these areas.

Table 1: M2M Application Examples (after [3] and [5]).

Categories	**M2M Applications**
Home	Heating control, Lighting control, Remote media control
Transportation	Emission control, Toll payment, Navigation, Road safety, Traffic control
Telemetry	Measurement of utility consumption , Parking meters , Vending machines
Tracking	Asset tracking, Cargo tracking
Fleet	Rental Vehicle monitoring Truck monitoring
eHealth	Remote patient monitoring, Mobile health, Remote diagnostics
Security	Surveillance applications, human/object tracking, etc.
Finance	Point of sale terminals

M2M Requirements

M2M applications have their own requirements. According to [4], some of the important M2M requirements are:

- Messages are typically short (i.e. tens to hundreds of bytes).
- Most of the traffic occurs in the uplink direction.
- Low mobility for some devices means that they are either stationary, move infrequently or move in a predefined region.
- Devices may be clustered into groups. This is required for charging, policing and multicasting.
- Some of the devices require battery operation.
- Data flow needs to be synchronized and monitored
- Security of exchanges between the devices and the server is critical.
- The number of M2M terminals is very large, which make all of the above quite difficult to achieve.

All of these are difficult to satisfy with the current networking technology, and substantial research effort will be needed to develop advanced technology capable of implementing M2M networks. As the result, there are many parameters governing the choice of what the best M2M solution will look like.

M2M System Architecture

The general architecture of a M2M application can thus be represented with the schematic shown in Figure 1. The architecture consists of three parts: the Device Domain which contains the M2M devices, the Network Domain which transports the messages between the M2M devices and the servers located in the Application Domain, which runs business applications that process collected data from devices

and issue commands when and where needed.

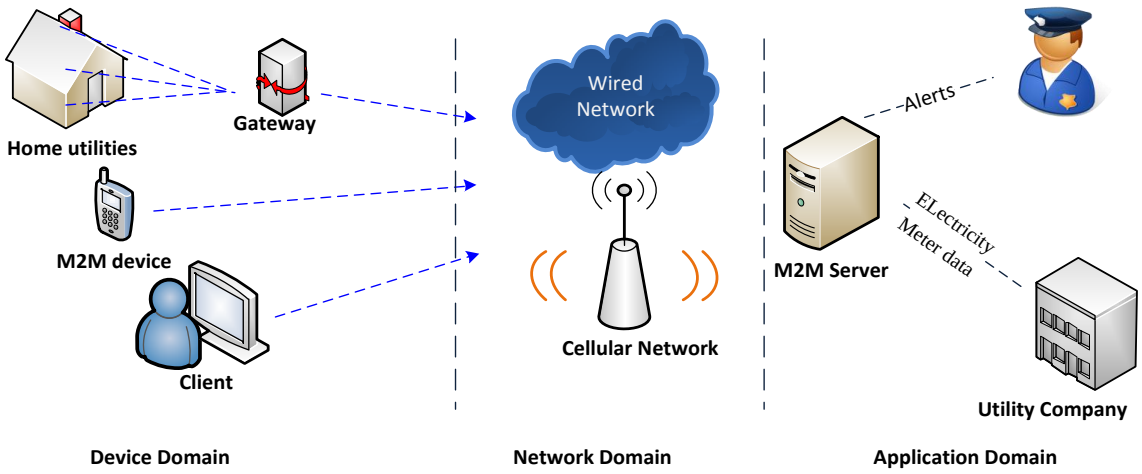


Figure 1: A general architecture of a M2M application

The major components of the architecture are described in Table 2.

Table 2: M2M Network Architecture

Major Components	Description
M2M Device	These devices are capable of sending data to the appropriate application servers and, if necessary, can respond to commands from the applications running on those servers.
Network	These networks connect M2M devices, possibly through a suitable (M2M) gateway to M2M applications running on appropriate servers. It can be wired or wireless, and it is typically operated by one or more network providers.
M2M Server	The server runs one or more applications that collect and process data obtained from M2M devices and take appropriate actions as needed, including alerting human operators when their intervention becomes necessary. Typically, M2M servers are operated by the service provider, e.g., a utility company.
M2M Applications	Contains the middleware layer where data travels through various application services and is used by the specific business-processing engines.

M2M Architectural Alternatives

The possible solutions with respect to the overall system architecture fall within two main categories:

First solution is the **cellular or direct M2M**, in which the M2M devices are connected directly to a cellular network such as LTE or WiMAX through a base station, as shown in Figure 2. Cellular M2M provides the ability to connect diverse devices and applications by enabling fixed assets (i.e. electric meters) or mobile assets (i.e. fleet vehicles). In addition, cellular technology is simple to integrate and cost effective to deploy.

The 3rd Generation Partnership Project (3GPP), an industry consortium focusing on the development of advanced cellular network technologies, is working on specifications to standardize the deployment of M2M applications in 3G networks.

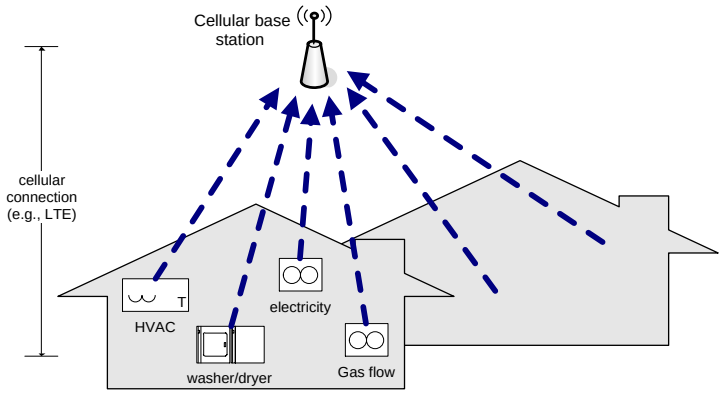


Figure 2: Cellular M2M Network (adapted from [21]).

The benefits of cellular M2M include the following:

1. There is ubiquitous access, as most areas in both urban and rural environment are covered by wireless cellular access;
2. High data transfer speeds are possible, again due to wireless cellular access – but the available speed of data transfers is probably an overkill for many M2M applications; and
3. There is no need to build an alternate infrastructure, since wireless

cellular infrastructure already exists, and consequently low price per service.

However, cellular M2M technology also suffers from the following disadvantages:

1. Each M2M terminal should be equipped with an appropriate cellular interface, which may be costly per terminal;
2. In urban areas, heavy contention with smart devices such as smartphones and tablets may lead to unpredictable quality of service, unless the current cellular protocols are amended to provide explicit support for M2M devices and their traffic;
3. At the same time, in sparsely populated rural areas, the performance of cellular systems may be insufficient to support the required quality of service; and
4. The need to provide direct cellular access may lead to excessive energy consumption – which is not a problem for devices (e.g., smart power meters) that are directly connected to AC power, but may reduce the operational life for battery-powered devices.

Second alternative is the **capillary or indirect M2M**, in which M2M devices are connected in a single- or multi-tier personal area network, which is ultimately connected to the base station through a suitable gateway, as shown in Figure 3. Individual personal area networks may be interconnected in a mesh or tree topology, with one or more tiers linked through suitable gateways.

The capillary solution ensures low cost per terminal, low energy consumption (since the transmission range is typically limited to tens of meters or so), and the possibility of battery-powered operation. Moreover, the design of capillary M2M networks can leverage the vast body of knowledge on wireless sensor networks that has been accumulated in recent years.

On the downside, the capillary solution limits the transmission speed, and it

may necessitate larger investments in infrastructure, since each neighborhood or, in extreme cases, each household needs to be equipped with a suitable M2M gateway. However, such gateways might be easily incorporated in smart power meters or similar devices.

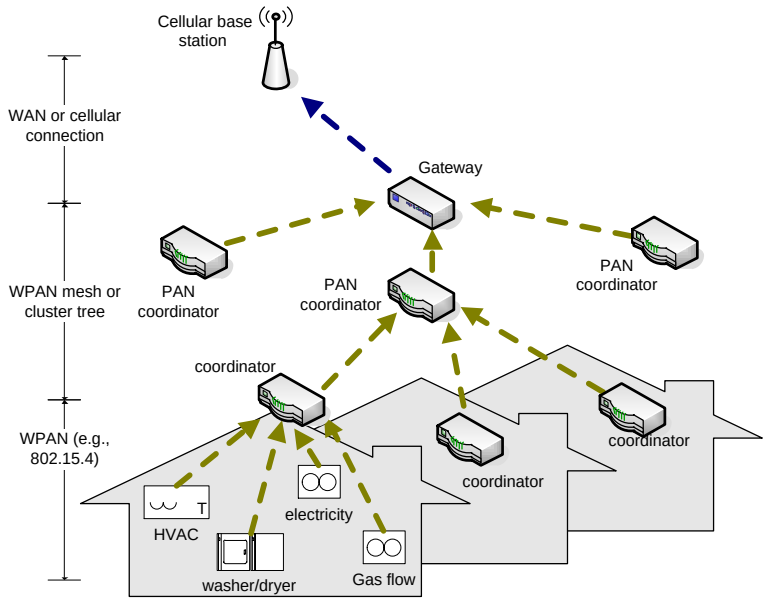


Figure 3: Capillary M2M Network (after [20])

Overall, the benefits of the capillary architecture outweigh their disadvantages, and the capillary architectures appears much better suited to gain wider use at the current state of technology than its cellular counterpart. On account of this, in this thesis we will focus on the performance of capillary M2M networks.

Another choice that we have to make is which particular communications technology is to be used to implement the capillary portion of the architecture. While there are many candidate technologies, not very many have found widespread usage in practice, and the most popular appears to be the IEEE 802.15.4 low data rate wireless personal area network (WPAN) technology [19]. In connection with the ZigBee standard which provides networking and application layer support, it offers low power operation, the ability to form complex networks, data transfer rate which is sufficient for M2M purposes, and devices that support it are widely available from a number of sources. It is worth noting that many existing projects on M2M communications actually use

IEEE 802.15.4 for wireless communications in the capillary path, precisely since IEEE 802.15.4 characteristics provide the best match for the requirements of M2M networks.

From operator point of view the main ZigBee key-values are [17]:

- Open standard protocol
- Standard for Application Messages
- Disappeared point-to-point tag-reader concept, no more limitations to star topologies (thousands of nodes)
- High Security Level (encryption and authentication at all protocol layers)
- Chipsets availability, low cost and low power solution
- Wireless Sensor Network evolution
- Easy integration in appliance/terminals in miniaturized peripherals with integrated antenna

Also ZigBee Gateway will enable:

- Easy connection of ZigBee networks (PAN) with the operator traditional network infrastructure and information technology
- Sensing and controlling things directly from the phone
- Creating extended operating networks

3. IEEE 802.15.4 AND ZIGBEE

IEEE 802.15.4

IEEE 802.15.4 is an IEEE communications technology standard which specifies the physical layer (PHY) and media access control (MAC) for low-rate wireless personal area networks (WPAN). It is the basis for ZigBee which is a network and application technology implemented on top of 802.15.4 PHY and MAC layers.

Physical Layer Characteristics

IEEE 802.15.4 networks utilize three RF (radio frequency) bands: 868 to 868.6 MHz, 902 to 928 MHz and 2400 to 2483.5 MHz; these will be referred to as 868, 915, and 2450 MHz bands, respectively. The last band is commonly known as the Industrial, Scientific and Medical (ISM) band and it is also used by a number of different communication technologies, including *b* and *g* variants of the 802.11 wireless LAN (also known as Wi-Fi) standards, various WPAN standards such as 802.15.1 (Bluetooth) and 802.15.3, but also other devices such as microwave ovens.

In the original standard [9], frequency bands at 868 and 915 MHz utilize Direct Sequence Spread Spectrum (DSSS) with a comparatively low chip rate and binary phase shift keying (BPSK) modulation, which result in maximum attainable data rates of only 20 kbps and 40 kbps, respectively. In that case, each data bit represents one modulation symbol which is further spread with the chipping sequence.

In the ISM (2450 MHz) band, Orthogonal Quadrature Phase Shift Keying (O-QPSK) modulation, in which four data bits comprise one modulation symbol spread further more with the 32-bit spreading sequence, is used before spreading. As a result, the maximum raw data rate in this band is 250 kbps.

Table 3: Frequency bands and data rates [19]

PHY option	frequency (MHz)	type of modulation	bit rate (kbps)	symbol rate (ksymbols/s)
868/915	868-868.6	BPSK	20	20
	902-928	BPSK	40	40
868/915 (2006)	868-868.6	ASK	250	12.5
	902-928	ASK	250	50
868/915 (2006)	868-868.6	O-QPSK	100	50
	902-928	O-QPSK	250	62.5
2450	2400-2483.5	O-QPSK	250	62.5

Note: PHY specifications from the 2006 standard (IEEE 2006) are optional.

The actual types of spread spectrum and modulation techniques, with the resulting data rates, are shown in

Table 3.

The original standard divided the available spectrum in the three bands into a total of 27 channels:

- channel $k = 0$, at the frequency of 868.3 MHz;
- Channels $k = 1 .. 10$, at frequencies $906 + 2(k - 1)$ MHz; and
- Channels $k = 11. 26$ in the ISM band, at frequencies $2405 + 5(k - 11)$ MHz.

Channel allocation in the ISM band is illustrated in Figure 4.

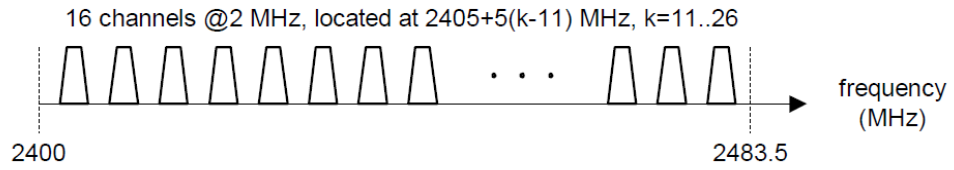


Figure 4: Channel allocation in the ISM band (2400 – 2478 MHz) [19]

Meanwhile WiFi uses the same frequency band as ZigBee, nevertheless WiFi uses higher power levels compared with ZigBee. Interference problem will cause loss of the data packets being transmitted. This will result in retransmission up until a

successful transmission is achieved. This, in turn, causes delay and mitigation in the delivery ratio. To prevent from interference problem between ZigBee and WiFi, we are using the last channel of the ISM band.

The physical layer of IEEE 802.15.4 is in charge of the following tasks [6]:

– *Activation and deactivation of the radio transceiver:* The radio transceiver may operate in one of three states: transmitting, receiving or sleeping. Upon request of the MAC sub-layer, the radio is turned ON or OFF. The turnaround time from transmitting to receiving and vice versa should be no more than 12 symbol periods, according to the standard (each symbol corresponds to 4 bits).

– *Energy Detection (ED):* Estimation of the received signal power within the bandwidth of an IEEE 802.15.4 channel.

This task does not make any signal identification or decoding on the channel. The energy detection time should be equal to 8 symbol periods. This measurement is typically used by the Network Layer as a part of channel selection algorithm or for the purpose of Clear Channel Assessment (CCA), to determine if the channel is busy or idle.

– *Link Quality Indication (LQI):* Measurement of the Strength/Quality of a received packet. It measures the quality of a received signal. This measurement may be implemented using receiver ED, a signal to noise estimation or a combination of both techniques.

– *Clear Channel Assessment (CCA):* Evaluation of the medium activity state: busy or idle. The CCA is performed in three operational modes:

1. Energy Detection mode: the CCA reports a busy medium if the detected energy is above the ED threshold.
2. Carrier Sense mode: the CCA reports a busy medium only is it detects a signal with the modulation and the spreading characteristics of IEEE 802.15.4 and which may be higher or lower than the ED threshold.

3. Carrier Sense with Energy Detection mode: this is a combination of the aforementioned techniques. The CCA reports that the medium is busy only if it detects a signal with the modulation and the spreading characteristics of IEEE 802.15.4 and with energy above the ED threshold.

– *Channel Frequency Selection:* The IEEE 802.15.4 defines 27 different wireless channels in three different RF bands: 868 MHz, 915 MHz, and 2.4 GHz (often referred to as the ISM – Industrial, Scientific, and Medical band). Each network can support only part of the channel set and, moreover, it is likely that a given physical device will support only a single frequency band. Hence, the physical layer should be able to tune its transceiver into a specific channel when requested by a higher layer.

Medium Access Control (MAC) Sub-layer

The MAC protocol supports two operational modes (Figure 5):

1. **The non-beacon-enabled mode**. When the ZigBee coordinator (ZC) selects the non-beacon enabled mode, there are neither beacons nor superframes. Medium access is ruled by an unslotted CSMA/CA mechanism.
2. **The beacon-enabled mode**. In this mode, beacons are periodically sent by the ZigBee coordinator (ZC) or ZigBee Router (ZR) to synchronize nodes that are associated with it, and to identify the PAN. A beacon frame delimits the beginning of a superframe (refer to Section0) defining a time interval during which frames are exchanged between different nodes in the PAN. Medium access is basically following the rules of Slotted CSMA/CA mechanism. However, the beacon-enabled mode also enables the allocation of contention-free time slots, called Guaranteed Time Slots (GTSs) for nodes requiring guaranteed bandwidth.

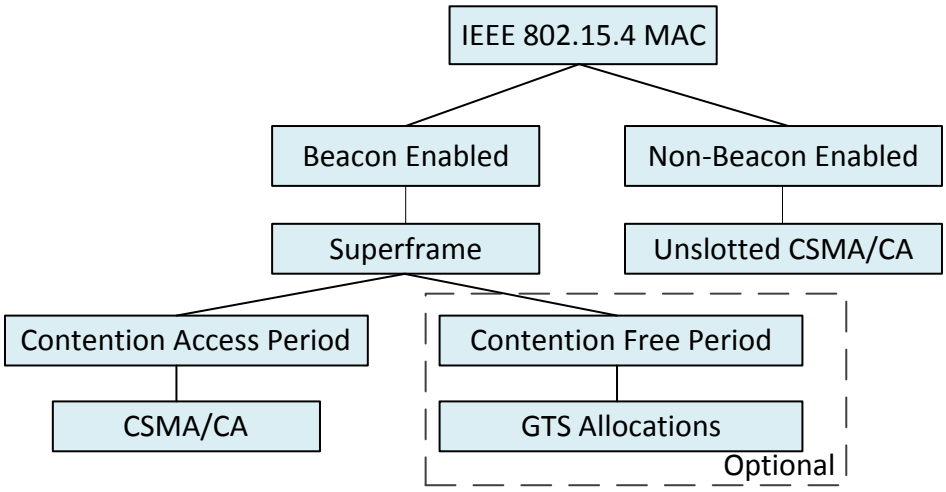


Figure 5: IEEE 802.15.4 Operational Modes

Superframe Structure

The superframe duration is defined between two beacon frames and has an active period and an inactive period. Figure 6 illustrates the IEEE 802.15.4 superframe structure. Time is measured in units of backoff periods, the exat duration of which depend on the actual RF band used. One unit time slot contains 3×2^{SO} backoff periods, where SO is the so-called superframe exponent which determines the duration of the active portion of the superframe. The active portion contains 16 time slots, as shown in the diagram below (where SO = 1).

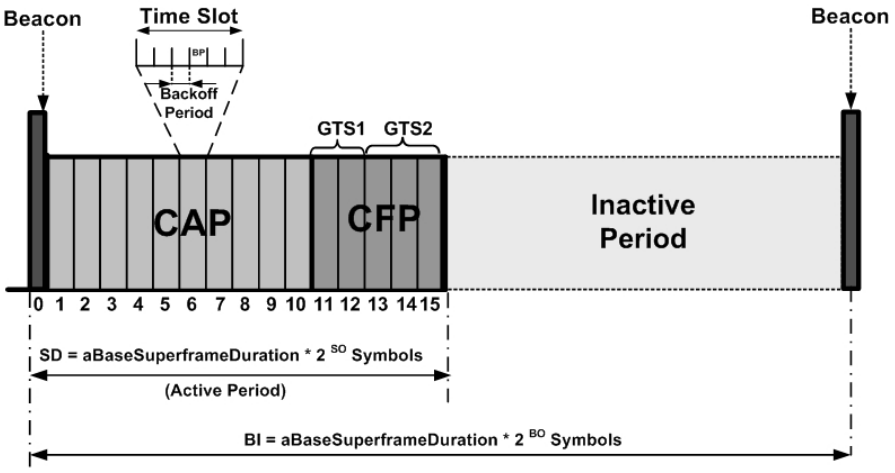


Figure 6: IEEE 802.15.4 Superframe structure

The active portion of the superframe structure is composed of three parts, the *Beacon*, the *Contention Access Period* (CAP) and the *Contention Free Period* (CFP):

– *Beacon*: the beacon frame is transmitted at the start of slot 0. It contains the information on the addressing fields, the superframe specification, the GTS fields, the pending address fields and other PAN related.

- *Contention Access Period* (CAP): the CAP starts immediately after the beacon frame and ends before the beginning of the CFP, if it exists. Otherwise, the CAP ends at the end of the active part of the superframe. The minimum length of the CAP is fixed at *aMinCAPLength = 440 symbols*. This minimum length ensures that MAC commands can still be transmitted when GTSs are being used. A temporary violation of this minimum may be allowed if additional space is needed to temporarily accommodate an increase in the beacon frame length, needed to perform GTS management. All transmissions during the CAP are made using the Slotted CSMA/CA mechanism. However, the acknowledgement frames and any data that immediately follows the acknowledgement of a data request command are transmitted without contention. If a transmission cannot be completed before the end of the CAP, it must be deferred until the next superframe.
- Contention Free Period (CFP): The CFP starts immediately after the end of the CAP and must complete before the start of the next beacon frame (if BO equals SO) or the end of the superframe. Transmissions are contention-free since they use reserved time slots (GTS) that must be previously allocated by the ZC or ZR of each cluster. All the GTSs that may be allocated by the Coordinator are located in the CFP and must occupy contiguous slots. The CFP may therefore grow or shrink depending on the total length of all GTSs.

In IEEE 802.15.4, CSMA/CA is used to access channels. There are two kinds of CSMA/CA mechanisms, the slotted and the unslotted CSMA-CA, which correspond to the beacon-enabled and non-beacon-enabled modes, respectively.

Slotted CSMA-CA

Nodes in clusters that operate in beacon-enabled mode must utilize the slotted CSMA-CA access mechanism, with a few exceptions. The flowchart shown in Figure 7 describes the slotted CSMA-CA algorithm which is executed when a packet is ready to be transmitted. The algorithm begins by setting the appropriate variables to their initial values:

3 Retry count NB, which refers to the number of times the algorithm was required to back off due to the unavailability of the medium during channel assessment, is set to zero.
4 Contention window CW, which refers to the number of backoff periods that need to be clear of channel activity before the packet transmission can begin, is set to 2.
5 Backoff exponent BE is used to determine the number of backoff periods a device should wait before attempting to assess the channel. If the device operates on battery power, in which case the attribute macBattLifeExt is set to true, BE (BackoffExponent) is set to 2 or to the constant macMinBE, whichever is less; otherwise, it is set to macMinBE, the default value of 3.

The algorithm then counts down for range 0.. $2^{BE} - 1$ number of backoff periods; this period is referred to as the Random Backoff Countdown (RBC) [7] . During the RBC period, channel activity is not assessed and the backoff counter is not stopped if such activity takes place, unlike the similar CSMA mechanism utilized in 802.11 networks, the countdown will be suspended during the inactive portion of the beacon interval, and will resume immediately after the beacon frame of the next superframe. A superframe consists of sixteen slots, which can be fixed or variable size is illustrated in Figure 8.

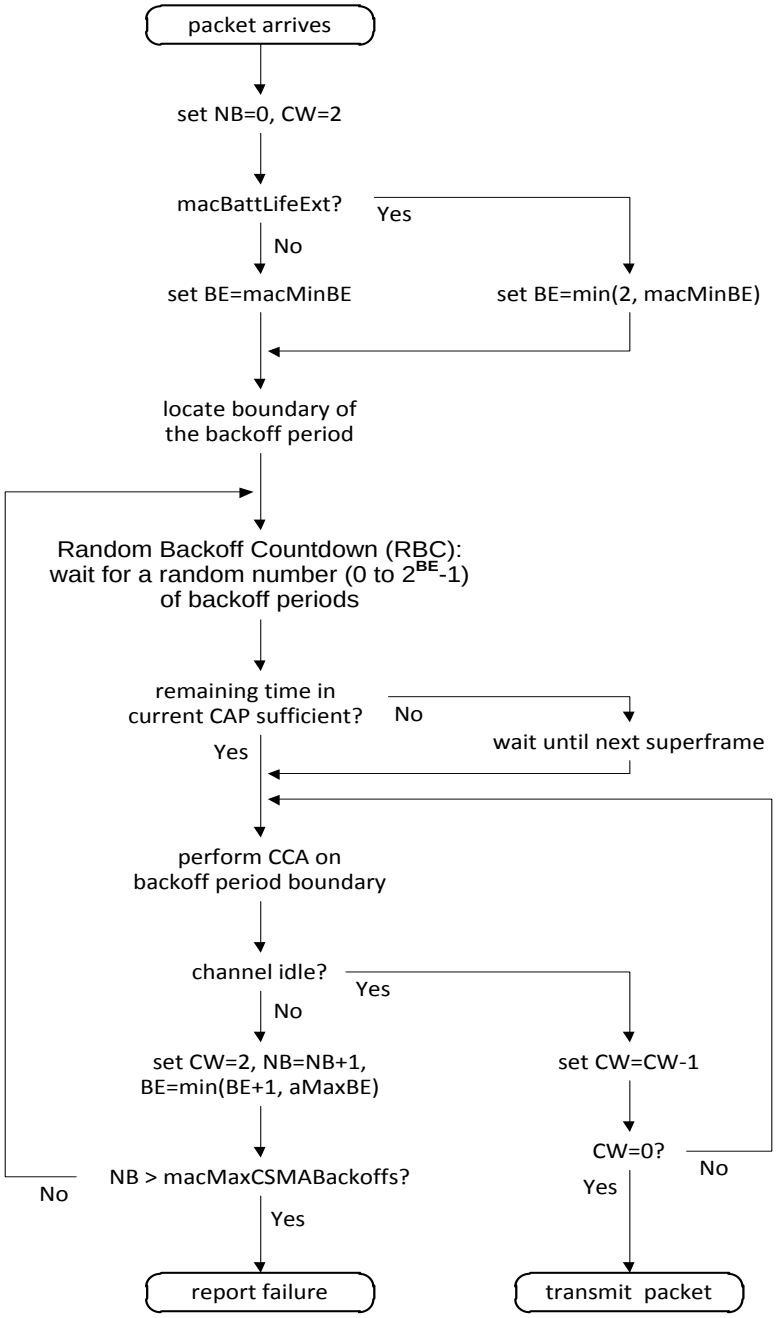


Figure 7: Operation of the slotted CSMA-CA algorithm (adapted from [19]).

IEEE 802.15.4 protocol in its beacon-enabled, slotted CSMA-CA uses superframes in which the first part is reserved for (optional) contention-free access, while the second part is used for contention-based access [7].

When the back-off count reaches zero, the algorithm checks the remaining time against the contention access period (CAP) window. It also checks to see if the area

of the current superframe is sufficient to accommodate the necessary number of Clear Channel Assessment or CCA checks, the actual packet transmission, and subsequent acknowledgment.

In this case, the algorithm proceeds to perform the CCA checks; otherwise, it pauses until the (active portion of the) next superframe. Figure below shows the active portion of a superframe in beacon-enabled mode.

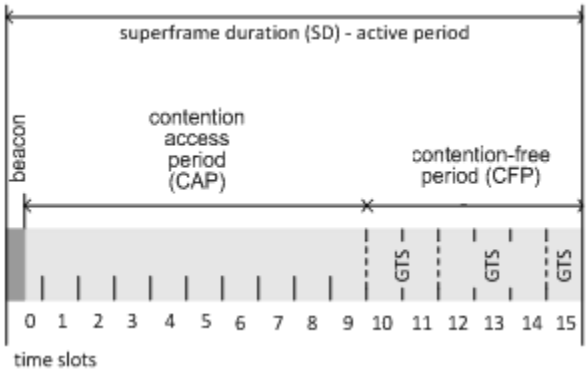


Figure 8: Active portion of the superframe in beacon-enabled mode (adapted from [19]).

If all CCA checks pass, the channel is deemed idle and the packet may be transmitted. Otherwise, if any of the CCAs detect activity on the channel, the node detects that there is an ongoing transmission by another node and the current transmission attempt is immediately aborted. The CSMA-CA algorithm is then restarted; the number of retries (NB), and the backoff exponent (BE), are incremented by one, while the CCA count, CW, is reset to two. Note that the backoff exponent (BE) cannot exceed *macMaxBE*, the default value of which is 5 if so the algorithm terminates with channel access failure status. Failure is reported to higher protocol layers, which can then decide whether to abort the packet in question or re-attempt to transmit it as a new packet.

Unslotted CSMA-CA

Medium access in the peer-to-peer topology uses a simpler, unslotted version of the CSMA-CA algorithm, which is described by the flowchart in Figure 9.

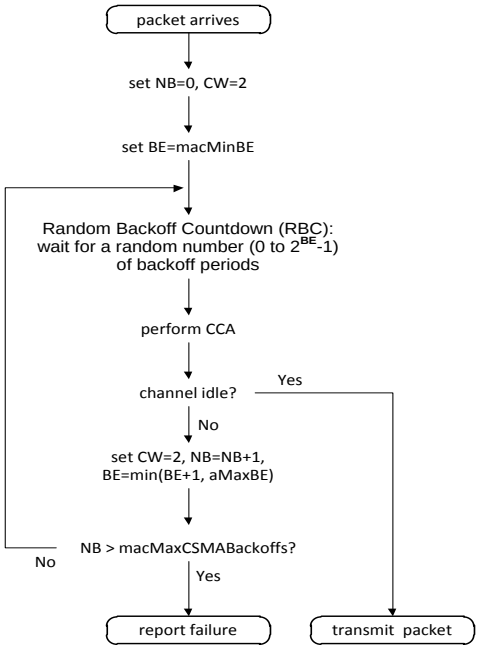


Figure 9: Operation of the unslotted CSMA-CA algorithm (adapted from [19]).

The meaning of parameters such as backoff retry count, NB, and backoff exponent, BE, is the same as in the slotted version of the algorithm described in Section 0 The main differences from that algorithm are as follows:

- While the countdown duration is determined in the same manner as in the slotted CSMA-CA algorithm, there is no synchronization to the backoff period boundary; the random backoff countdown begins immediately upon the arrival of the data packet from the upper layers of the protocol stack.
- Since there is no superframe, the node can perform the CCA check, followed by the packet transmission and subsequent acknowledgment (if requested), as soon as random backoff countdown is finished.
- When the random backoff countdown reaches zero, only one CCA check is performed and, if successful data packet transmission can begin immediately; neither of these activities need to be synchronized to the backoff period boundary.

An Overview of ZigBee

ZigBee standard provides a networking and application protocol for small range and low data rate networks that use IEEE 802.15.4 protocol's physical and medium access control layer functionality. ZigBee is a specification for a suite of high level communication protocols using small, low-power digital radios which builds upon the physical layer and medium access control defined in IEEE standard 802.15.4 for wireless personal area networks (WPANs). The low deployment cost of ZigBee allows the technology to be widely set up in wireless control and in longer battery life.

In general, a ZigBee network consists of a number of devices interconnected using one of the three topologies of Star, Tree or Mesh Network. These devices use the MAC and PHY functionality of IEEE 802.15.4 standard.

An outline of the ZigBee protocol architecture is shown in Figure 10.

The ZigBee NWK layer provides functionality which corresponds to the network layer of the OSI seven-layer protocol stack. To that end, it includes mechanisms for

- Starting a new network,
- Joining and leaving the network, and assigning addresses to newly associated devices,
- Discovery of one-hop neighbors and storage of pertinent information about them,
- Discovery and maintenance of routes between devices, and
- Routing of frames to their intended destinations.

Which 802.15.4 Specification provides only partial support for the first two of these functionalities.

The ZigBee APL layer consists of the application support sub-layer (APS), the application framework (AF), the ZigBee device object (ZDO) and manufacturer-defined application objects.

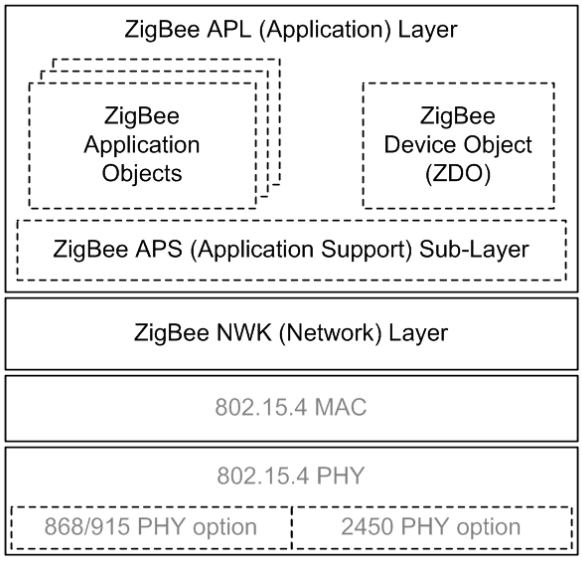


Figure 10: The ZigBee protocol stack and its relationship to IEEE 802.15.4 protocol layers (adapted from [19]).

The APS sub-layer allows a link between two devices based on their needs and services they provide, and provides facilities for subsequent operation and maintenance of that link. The ZigBee Device Object (ZDO) allows the device to define its role within the ZigBee network. This allows the device to initiate binding requests and respond to requests from other devices in the ZigBee network.

To that end, it makes use of the facilities provided by the NWK layer with respect to device and service discovery. The ZDO also allows the device to establish a secure relationship with other devices, in the manner that will be explained below. Application objects are beyond the scope of the ZigBee specification, which allows up to 240 such objects to be defined, each with a uniquely numbered endpoint. Endpoint 0 denotes the data interface to the ZDO itself, whereas endpoint 255 is used for broadcasts that target all application objects; the remaining 14 endpoints are reserved for future use.

Device Roles

Each ZigBee device must be capable of two jobs first joining a ZigBee network as a member, second leaving the ZigBee network to which it currently belongs. The request to join the network may originate from the lower layer of the network

protocol stack (i.e., the MAC layer of the underlying 802.15.4 firmware); alternatively, the application executing on the ZigBee device may explicitly request the device to join a specific network. The request to leave the network may originate from the ZigBee Coordinator (ZC), or from the application itself.

In addition, some ZigBee devices are capable to permit other devices to join an existing network and to permit a device to leave the network to which it currently belongs.

They can function as ZigBee coordinators, as ZigBee routers (ZR) or devices that have no such capabilities are often referred as end devices.) All devices can take part in the process of assigning logical addresses to other network devices, and are capable of maintaining a list of neighboring devices. The list of neighboring devices is useful to find information about potential routers which is needed to identify candidate parents and also during regular operation, when it stores the information needed to perform routing; this information may be updated after each received frame.

ZigBee coordinators have the additional capability to establish a new network, only if they are not already associated with an existing network. This begins with an energy scan, performed by the MAC layer, in order to learn about used and free channels. Once a suitable channel is found, the device undertakes an active scan. The channel with no detected networks, or the one with the lowest number of existing networks, should be used for the new network. The device then proceeds to assign a network address for the new network and informs the higher layers of the network protocol stack.

The new device can associate with the network by itself, if it is not a member of any network; alternatively, a new device can be invited by an existing device. In the latter case, the new device is referred to as the child, and the device that has allowed the child to join the network is referred to as its parent.

Also depend on the capabilities of device it may request to join the network as a router.

It may be rejected if already a specified number of routers exist. In this case, the device may join the network as an end device.

Network Topologies and Routing

In terms of network topologies, ZigBee supports three different topologies, referred to as star, tree, and mesh networks.

Star network

In a star network, one device or node functions as the ZigBee coordinator and its responsibilities include various tasks related to the creation and maintenance of the network. All communications must be routed through the ZigBee coordinator. The star topology corresponds to the single cluster with star topology of the 802.15.4 standard. Star networks operate in beacon-enabled, slotted CSMA-CA (when interacting with beacon devices) access mode, and the responsibilities of the ZigBee coordinator closely correspond to those of the PAN coordinator in the 802.15.4 standard.

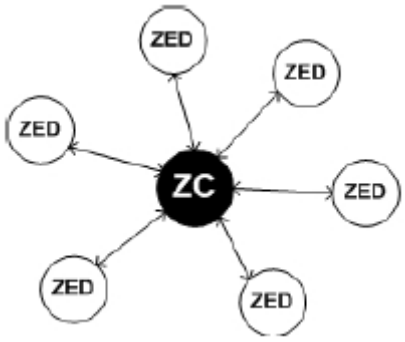


Figure 11: Star topology

Tree network

In a tree network, there is again one ZigBee coordinator which is responsible for the entire network. There are also a number of routers which transfer data and control

messages and, thus, extend the network. (Note that the role of a router requires that the device is capable of acting as a ZigBee router.) Since the ZigBee tree network operates in beacon-enabled, slotted CSMA-CA access mode, it closely corresponds to the multi-cluster tree which will define in section below. In this topology, individual clusters are essentially sub-networks, while the routers are master-slave bridges that double as coordinators for those clusters.

The routers repeat the beacon frames received from the ZigBee coordinator, after a suitable delay, and relay the data and command frames between the sub-networks. The beacon frame contains information about the device/sub-network depth, router capacity (i.e., whether the router is capable of accepting join requests from router-capable devices or not), end-device capacity (i.e., whether the router is capable of accepting join requests from router capable devices or not), and the time difference between the current beacon and the beacon transmission of the parent. For compatibility reasons, the beacon frame also includes the information about the version of the ZigBee protocol supported by the router device.

Typically, the beacon interval in a tree network will be much longer than the superframe duration, to allow a number of sub-networks to co-exist without interfering with each other. Also, device addresses are exclusive within the network, and each parent device is given a different subset of available addresses (i.e., an address sub-block) for its children. Some parents may exhaust their address sub-blocks before the others, and a new device may have to find a parent that still has unallocated addresses before it can join the network.

A notable characteristic of a ZigBee tree network is that the maximum values for the number of children a device may have, the depth of a tree, and the number of routers that a parent may have as children, may be prescribed and subsequently enforced.

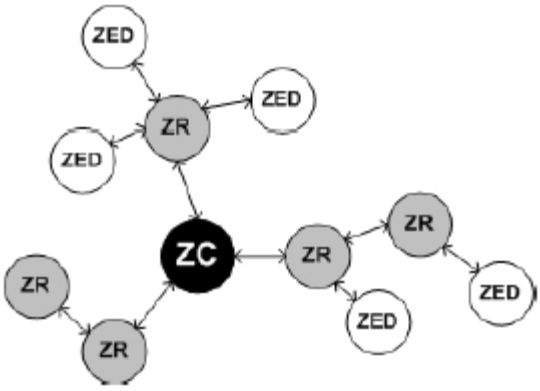


Figure 12: Cluster tree topology

Multi-cluster tree

Member of an existing cluster may decide (or be instructed by the coordinator) to extend the cluster. This member can then form a second cluster as its coordinator, and other nodes can join.

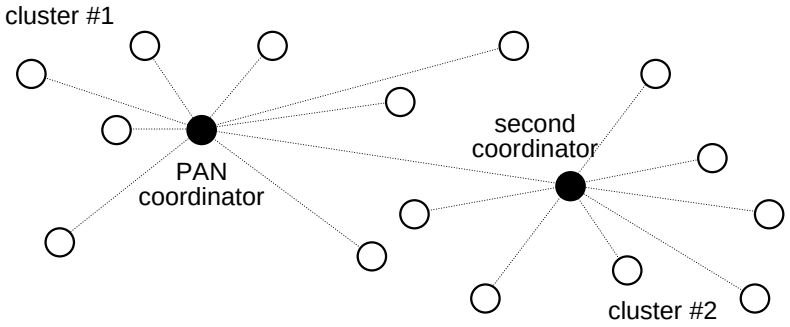
So the coordinator of the second cluster is still a member of the original cluster. The device broadcasts its own beacon frames and delayed with respect to the beacon frames which sent by the original coordinator.

This process can be repeated as many times as necessary, to form the so-called multi-cluster tree network. Figure 13(a) is shown an example of a two-cluster tree.

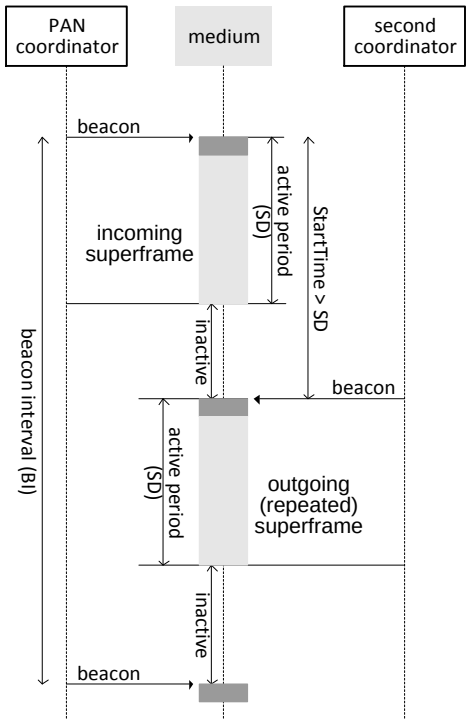
A notable characteristic of the multi-cluster tree is that all clusters use the same Radio Frequency RF channel on a time-division basis, which is accomplished in the following manner. The PAN coordinator (i.e., the coordinator of the first cluster) should set its timing parameters in such a way that the inactive period Beacon Interval (*BI)* – Superframe Duration (*SD*), is much longer than the active period *SD*. (In reality, this means that Beacon Order(*BO)* ≥ Superframe Order (*SO)* + 1). Each of the sub-cluster coordinators uses those same values, but delays its beacon for an interval equal to a preset value of *StartTime* ≥ *SD*. (In fact, those coordinators may simply repeat the beacon frame received from the PAN coordinator, after the appropriate delay.)

Note that the values of the beacon and superframe order, *BO* and *SO*, are the same for all clusters in the tree. Hence the active intervals of different clusters can be effectively interleaved within the beacon interval. It means certain number of clusters can use one channel.

Figure 13 (b) illustrates an example of such timing arrangement for a cluster tree with two clusters, and one PAN and one cluster coordinator.



(a) Topology of two-cluster tree



(b) Superframe timing in a two-cluster tree

Figure 13: A two-cluster tree (adapted from [19]).

Mesh network

A ZigBee mesh network operates in a peer-to-peer topology, using non-beacon enabled, unslotted CSMA-CA (when interacting with non-beacon devices) access mode. In this topology network operates in a full peer-to-peer mode, and virtually any device can function as a router. As we don't have beacon frames in a mesh network (or, indeed, any 802.15.4 peer-to-peer topology network) so it means that there are no superframes, and no active or inactive periods. Since incoming data may occur at any time, the devices cannot go to sleep for long periods of time. As a result, energy efficiency cannot be improved through the use of redundant nodes and/or activity management.

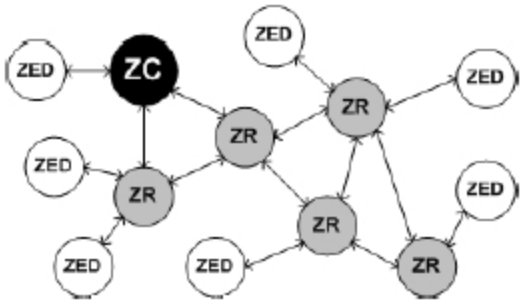


Figure 14: Mesh topology

Security and Privacy

Security functions and security management are implemented in both NWK and APL layers; Depending on the selected security level, the entire frame at the APL layer may be protected before it is passed on to the NWK layer; furthermore, the entire frame at the NWK layer may be protected before passing it on to the MAC layer for transmission.

When it comes to secure transmission of data, there are a number of properties that must be taken into consideration. These properties include:

- Authenticity, confirming the identity of a person or entity requesting service.

- Authorization, ensuring that the person or entity in question is authorized to perform the operation requested;
- Integrity, ensuring that source and destination data are the same; and
- Confidentiality, ensuring that communication between users if seen by a third party does not reveal the actual content of the communication[8].

A remarkable characteristic of the security approach adopted by the ZigBee standard is that it recognizes the limitations imposed by the low cost and low complexity (and, consequently, low computational capability) of practical devices. Specifically, different applications and protocols that contribute to the implementation of security procedures and services are not independent of one another, and there is no cryptographic task separation within a single device. This fact has a number of concerns:

- First, an open trust model must be adopted in which different applications and protocols can establish a trust relationship.

- Second, end-to-end security must be implemented on a device-to-device basis and cannot be applied between pairs of layers or applications on two communicating devices.

An important concept in security management is the difference between link and network keys. It is assumed that the destination device is always aware of the security arrangement used. Link keys may be attained by key transport (i.e., through communication with other nodes, possibly protected) or key establishment or update. Network keys may be obtained by key transport or pre-installation. Master key is a prerequisite to establishing and or updating link keys.

Security is a critical issue among M2M applications, especially when it comes to e-health applications. There is a need to guarantee system reliability. Data mining is a good way to realize smart capabilities without human intervention. Here are some of the important areas where data mining can be used:

Reliability in sensing and processing: M2M networks with large number of nodes are susceptible to node failure, resulting in unreliable sensing. Therefore mechanisms must be in place to detect the accuracy or reliability of these results.

One of the proposed methods [9] makes use of a machine learning algorithm called local vote decision fusion (LVDF) which is similar to the nearest neighbour distance based machine learning algorithm.

Quality of service: There is a need for efficient quality of service (QoS) in many applications, including but not limited to traffic safety, e-health, logistics, and others. For example, as mentioned in 0, there are applications which require QoS to compensate for high latency and low bandwidth networks. For emergency service messages, traffic needs to be prioritized against other regular and non-critical data. Considering that all types of devices and data are sharing the same network infrastructure, there is a need to guarantee QoS to meet the necessary application requirements. An existing method of providing QoS is to use a class-based approach where once the traffic is assigned to a class, certain QoS metrics will be guaranteed. Call admission control (CAC) based on machine learning techniques has been proposed in [13] for providing QoS to a network taking into account the dynamic demand of the bandwidth and the type of traffic classes to be supported. The machine learning algorithm in this case is capable of modeling the system behavior through learning based on observations of performance data over a period of time. Once it is trained, the model can automatically estimate and predict future system behavior and also make admission control decisions with high accuracy, resulting in a reliable system.

4. PERFORMANCE OF THE ORIGINAL PROTOCOL

To investigate the performance of capillary M2M networks, we have undertaken a simulation analysis of a ZigBee/IEEE 802.15.4 network with variable number of nodes and/or variable traffic along with tree topology and mesh topology. Upon analyzing these results, we will propose a simple improvement to allow efficient processing of M2M device traffic.

Performance Metrics

Several metrics can be defined to grade the performance of a technology against the elements of wireless networking. Some of these metrics have been carefully chosen to give an idea of behavior and the reliability of the Zigbee networks. A detailed explanation of these metrics follows:

End-to- End Delay

The end-to-end delay (ETE) is defined as the end-to-end delay of all the packets received by the 802.15.4 MACs of all WPAN nodes in the network and forwarded to the higher layer. As the number of nodes in the WANs increases the delay will increase. The delay for a packet is the time taken for it to reach the destination. And the average delay is calculated by taking the average of delays for every data packet transmitted. The parameter comes into play only when the data transmission has been successful.

Packet_Delay = Receive_Time_at_Destination – Transmit_Time_at_Source

Average_Delay = Sum_of_all_Packet_Delays / Total_Num_of_Received_Pkts

Network Throughput

Global MAC throughput is the total data traffic in bits/sec successfully received and forwarded to the higher layer by the 802.15.4 MAC in all the nodes of the WSN. It is known that throughput usually depends on many aspects of networks such as power control, scheduling strategies, routing schemes and network topology.

Therefore, throughput can be stated as:

$$Throughput\_of\_a\_Node = \frac{(Total\_Data\_Bits\_Received)}{2(Simulation\_Runtime)}$$

Similarly the throughput for the network can be defined as:

$$Network\_Throughput = \frac{(Sum\_of\_Throughput\_of\_Nodes\_Involved\_in\_Data\_Trans.)}{(Number\_of\_Nodes)}$$

Transmitting power

The transmitted power is the power that is transmitted from the antenna into space. In Annex F [4], the document states the IEEE 802.15.4 regulatory requirements that for the ISM band 2.4 GHz operating in United States, transmitted power of up to 1 watt is provided. Although IEEE 802.15.4 devices are generally envisioned to operate with a maximum transmitting power of approximately 0 dBm (1mW), a minimum of +10 dBm (0.01W) is allowed in this band.

Pt= 17 dBm= 0.05 W

Receiver Threshold (RXThresh)

The receiver threshold is the parameter used to specify the communication range of the wireless nodes and the threshold is the minimal power of the packet required for successful reception. If a packet reaches a node with a power level above the receiver threshold, the receiver will be within the transmission range of the sender. The receiver sensitivity is -85 dBm typical.

Simulation Model

Simulation and modeling are important approaches to developing and evaluating the systems in terms of time and cost. A simulation shows the probable behavior of a system based on its simulation model under different conditions. To study system behavior and performance by means of real deployment or setting up a test-bed may involve much effort, time and financial costs.

This section presents the structure of the IEEE802.15.4/ZigBee simulation model in Opnet Modeler simulator.

The Opnet Modeler is an industry leading discrete event network modeling and simulation environment. Opnet Modeler was chosen due to its accuracy and to its sophisticated graphical user interface. Internal architecture of a node is illustrated in Figure 15. The behavior of a node is defined using state transition diagrams. Operations performed in each state or transitions are described in embedded C/C++ code blocks.

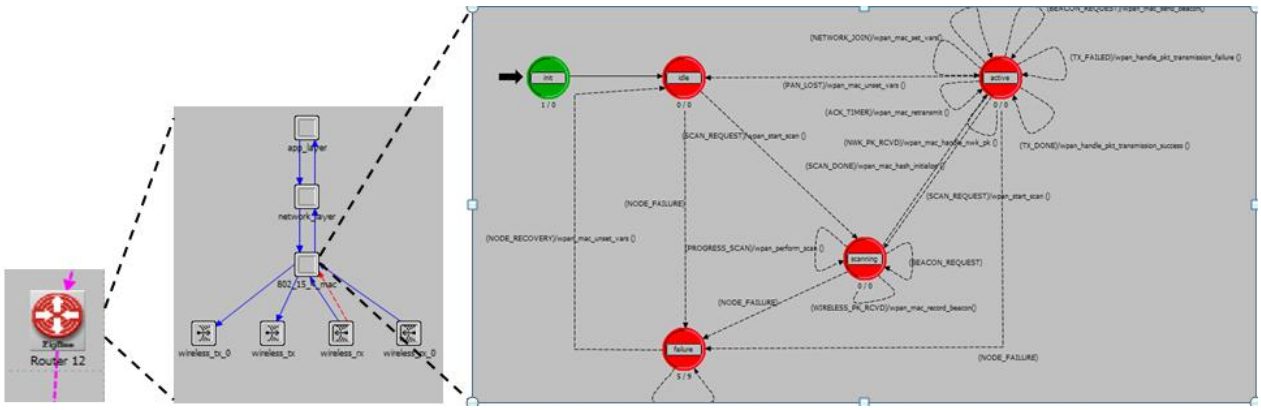


Figure 15: A ZigBee device Architecture

Impact of Variable Number of Devices in the Network

The IEEE 802.15.4 OPNET simulation is implemented and tested under the OPNET Modeler Wireless Suite provided under OPNET University Program license.

As a first step, we have developed a simulation of 5-node topology for the ZigBee Network using OPNET MODELER Simulator. We will extend this simulation model to larger network by increasing the number of nodes in the step of 5. Our simulation model implements the physical layer of the IEEE 802.15.4 standard with 250 kbps data rate, running at 2.4 GHZ frequency band. On the MAC layer CSMA-CA and Guaranteed Time Slot (GTS) mechanisms are supported.

The Application Layer can specify the destination and the method of data generation and the packet size. Which we have worked with variable bit rate and will have the results of experiments latter.

In a sensor network number of nodes is varied therefore the consideration of the number of nodes was one of the evaluation processes.

The set of diagrams shown below illustrates simulation of tree topology which we performed for variable end node devices of 5 to 15 nodes with the minimum possible number of routers. We have the results on End-to-End Delay and throughput of each one.

All sensor nodes were configured with CBR traffic, and for evaluation purpose, all nodes in a single scenario were assumed to be in the same personal area network (i.e. have the same Personal Area Network (PAN) ID). For simplicity the nodes will choose a random destination node within its own PAN to reach the coordinator.

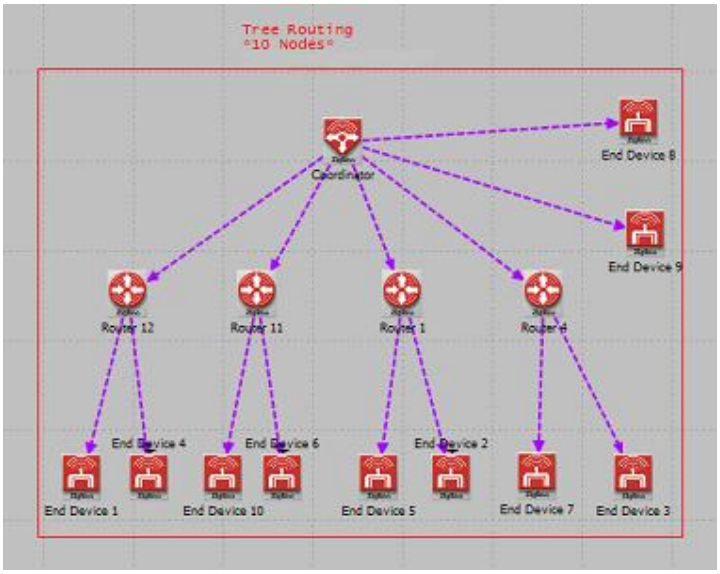


Figure 16: A ZigBee network in OPNET Modeler

Also in each WSN one of the coordinator's duties is to dictate the topology of that network, therefore in each topology the type of network (here Tree network) is set at the coordinator node. The simulation run time for all the scenarios is set to 10 minutes and the graphs are in "AS IS" mode.

The initial tree topology scenario considered consists of 5 ZigBee End devices (reduced function devices) and 1 coordinator (full function devices). Each device has been configured to fulfill the requirements of our experience which is shown in Table 4. Next scenario is a network of 10 and 15 Zigbee End devices with a pan coordinator. Figure 16 shows 10- nodes ZigBee devices in a Network of tree topology in Opnet Modeler simulator.

Table 4 is the list of network parameters that have been set on devices in each network topology. Table 5 is the network parameters that have been implemented at the coordinator nodes only.

These are available by R-Click on each node and choosing Edit Attributes from the pop-up menu.

Table 4: Mac,Physical and Application Layer Parameters

MAC Layer Parameters	
ACK wait duration(sec)	0.05 (Standard default)
Maximum number of retransmission	3 (Standard default)
Minimum value of the back-off exponent in the CSMA/CA (if this value is set to 0, collision avoidance is disabled during the first iteration of the algorithm)	3
Maximum number of back-offs the CSMA/CA algorithm will attempt before declaring a channel access failure.	4
Channel sensing duration (sec)	0.1(Standard default)
Physical Layer Parameters	
Data rate(Kbps)	250 (Standard default)
Reciever sensitivity (db)	-85 (Standard default)
Transmission band (GHz)	2.4 (Standard default)
Transmission power (W)	0.05 (Standard default)
Application Layer Parameters	
Packet interarrival time /Type (sec/constance)	1
Packet size/ Type (bits/constant)	1024
Stop time	Infinity (simulator default)

Table 5: Coordinator Network Layer Parameters

Coordinator Network Layer Parameters	
Maximum number of end devices and routers in one PAN	250 (Standard default)
Maximum number of routers in a single PAN	6
Route discovery timeout (sec) The duration of route discovery entries remaining in the table before they are removed. (Only used in mesh networks).	10
Pan ID	1

A. End-to-End Delay

A simulation of ETE delay of the four scenarios with increasing number of nodes was undertaken. Figure 17 shows the simulation results of the Application ETE delay for the tree topology.

It can be seen that the difference in delays between the 5 and 10 end nodes is very slight and it's less than 0.015 seconds. However, this delay increased to 0.025 seconds in the network of 15 E-nodes.

This is basically due to the differences in the routing techniques. Namely, there are only three hierarchical levels for the networks with 5 and 10 nodes. In the network with 15 nodes, there are more hierarchical levels. As the result, most of the traffic from E-nodes has to pass through at least two routers to get to the destination (coordinator) which makes it difficult to find a correlation of the delay performance of different networks sizes between these diagrams.

Also it is seen that the delay increases proportionally with the increase in the number of nodes; this is as expected since increasing the node numbers in WSNs will lead to higher traffic and hence higher delay.

This is basically due to the performance of CSMA/CA mechanism. Since device transmitting base on CSMA/CA listens to the network media before transmitting data.

If media is idle, device first transmits a signal of intent and waits for some time to check if media is clear before sending the actual data. If media is not idle, the device waits for a random period of time (backoff factor). If media is clear when backoff counter reaches zero, device transmits the data else the backoff factor is set again and the process is repeated.

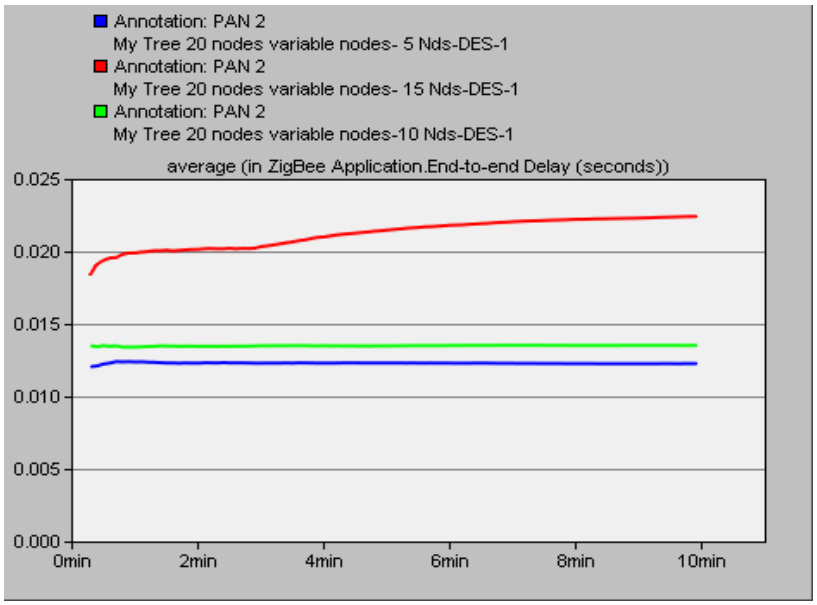


Figure 17: End-to- end Delay of Variable Number of Nodes vs. simulation time

B. Coordinator MAC Throughput

MAC throughput is the total data traffic in bits/sec successfully received and forwarded to the higher layer by the 802.15.4 MAC in all the nodes of the WSN. It is known that throughput usually depends on many aspects of networks such as power control, scheduling strategies, routing schemes and network topology. Figure 18 shows the global MAC throughput for all 3 simulation topologies. It can clearly be seen that when the number of nodes increases the MAC throughput increases. This is expected because the data being received by the MAC layer increases.

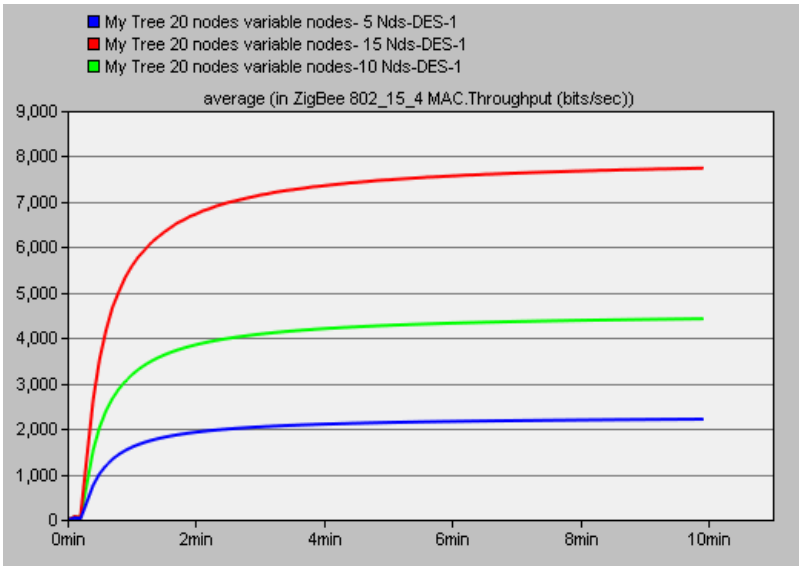


Figure 18: MAC Throughput of Variable Number of Nodes at Coordinator vs. simulation time

C. Media Access delay at the coordinator

Media Access delay is the total of queuing and contention delays of the data frames transmitted by all the 802.15.4 MAC.

For each frame, the media access delay is considered, the duration from the time that is inserted into the transmission queue (which is arrival time for higher layer data packets and creation time for all other frames types), until the frames is sent to the physical layer for the first time. Hence the method of queuing can have a great impact on Media Access Delay. It should be pointed out that there are different ways of queuing. As an example we can consider giving a low-priority class a longer waiting time compared to high-priority class, so the high-priority class is likely to access the medium earlier than the low-priority class.

Figure 19 shows the Media Access Delay at the coordinator for all 3 simulation topologies. The lowest delay is for 5 E-nodes network topology where increasing the number of E-nodes result in increase of delay.

At the beginning of the simulation for all 3 topologies, delay has its lowest amount and it's because in the beginning there is no data packet in the queue

and the queue is empty. The pulses during the simulation happen as the number of packets in the queue continuously changes. When there are fewer packets in the queue, the delay is less.

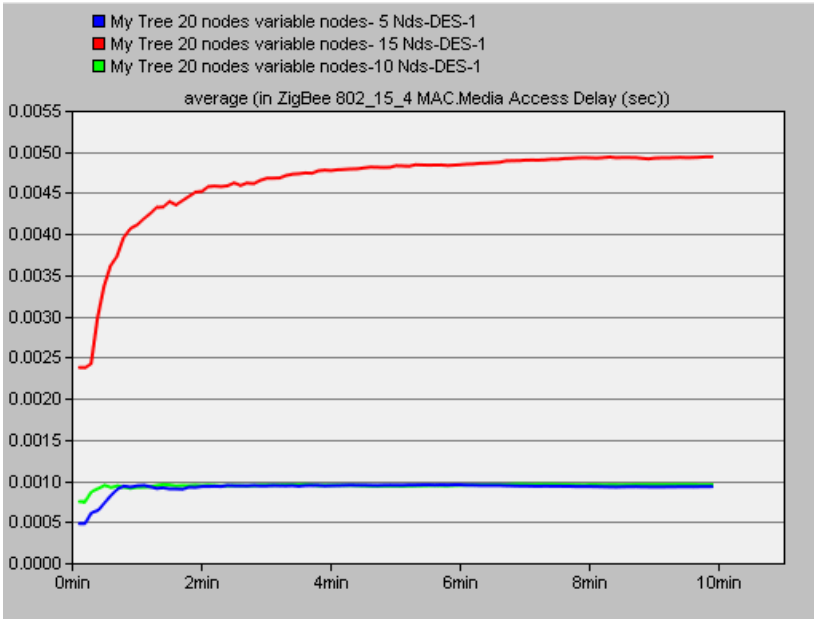


Figure 19: Media Access Delay at the Coordinator vs. simulation time

D. Global Media Access Delay

Figure 20 shows the Global Media Access Delay of all 3 network topologies. The amount of delay for 10 E-nodes topology is less than 0.010 and for 15 E-nodes topology is less than 0.030. Literally the delay increase is proportional to increase of the nodes.

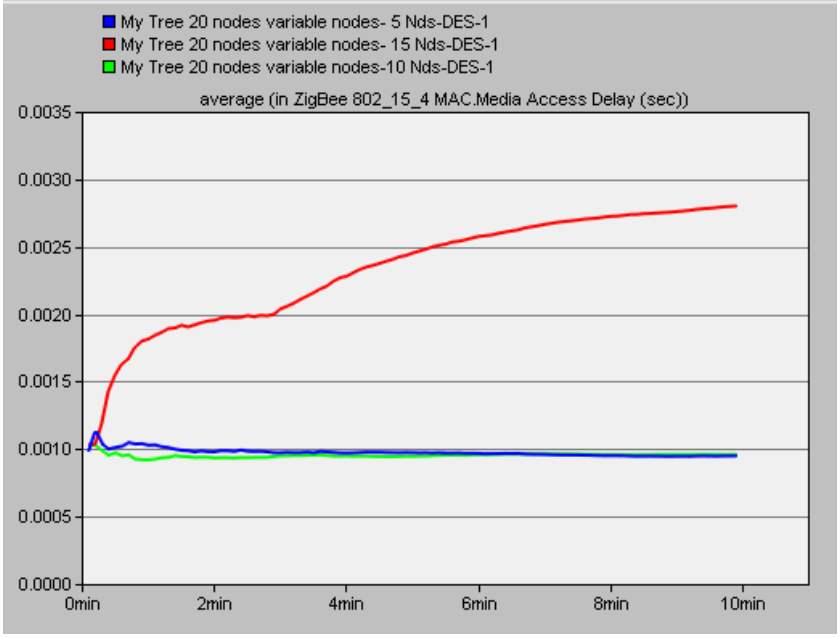


Figure 20: Media Access Delay of Global statistics vs. simulation time

E. Traffic at the Coordinator

We consider one of the Routers (router 17) and coordinator to study their behavior.

Figure 21 shows the traffic sent and received by the Coordinator to/from Router. As it is expected the exact amount of data has been sent and received by the coordinator. As we set the Packet size to 1024 bits and the packet interarrival time has set to 1 therefore coordinator send 1kbps and received same amount. The Network is in ideal mode and the result validates the accuracy of the simulation.

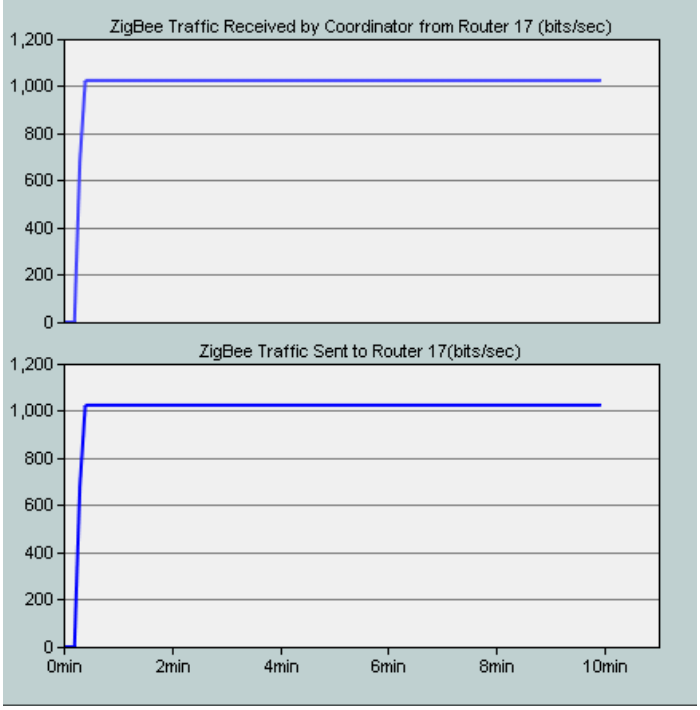


Figure 21: Traffic Send/ Receive at coordinator vs. simulation time

F. Conclusion

As the number of End nodes increases in the network, the throughput also increases however the Media Access Delay increases as well. Study of Media Access Delay at the Coordinator shows that the delay increases by increasing the number of nodes in the network, but does not have a linear dependency. In the next project we study variable bit rate and how it can have an impact on the network efficiency.

Impact of Variable Interarrival time in The 20 E-Nodes Network Topology

In this Project we simulate and demonstrate the impact of variable interarrival time (range of 1 .. 6) in the network topology of 20 end nodes. We consider CBR packet generator, packet size of 1024bits and data rate 250 Kbps on a tree

topology. The base scenario is the network with packet interarrival time set to 1 which is a default option.

A. Throughput at Coordinator

Figure 22 shows the throughput of the network at coordinator when the start times to send the packets are vary from 1 to 6 seconds. It is clear that the shorter the interarrival time is, the higher the network throughput we have.

The best result has been obtained when the Packet interarrival time is set to 1 second, meaning that we have a network capable of processing each packet in second, as the interarrival time between those two packets is one.

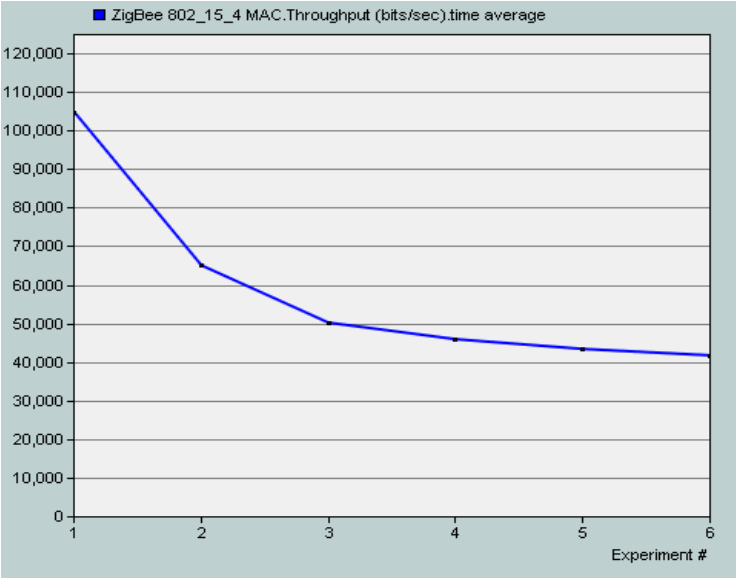
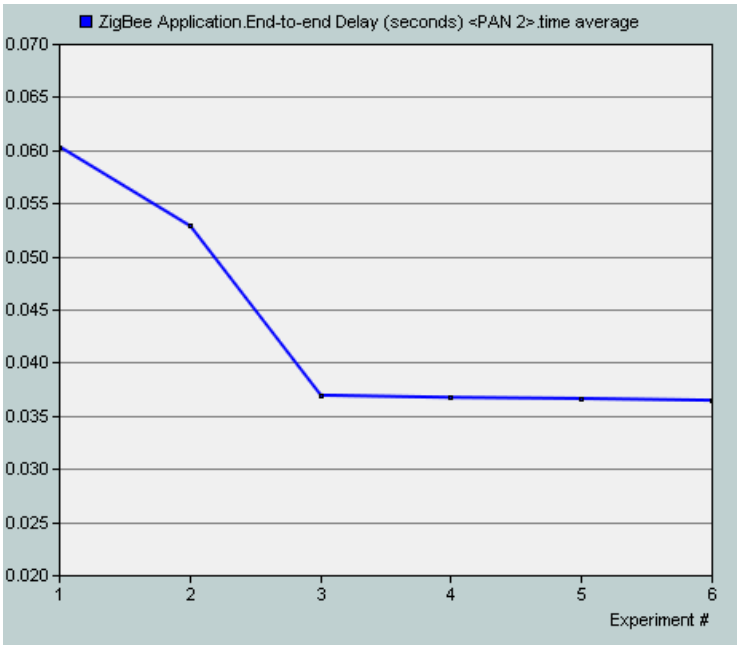


Figure 22: Throughput vs. Packet Interarrival Time (sec)

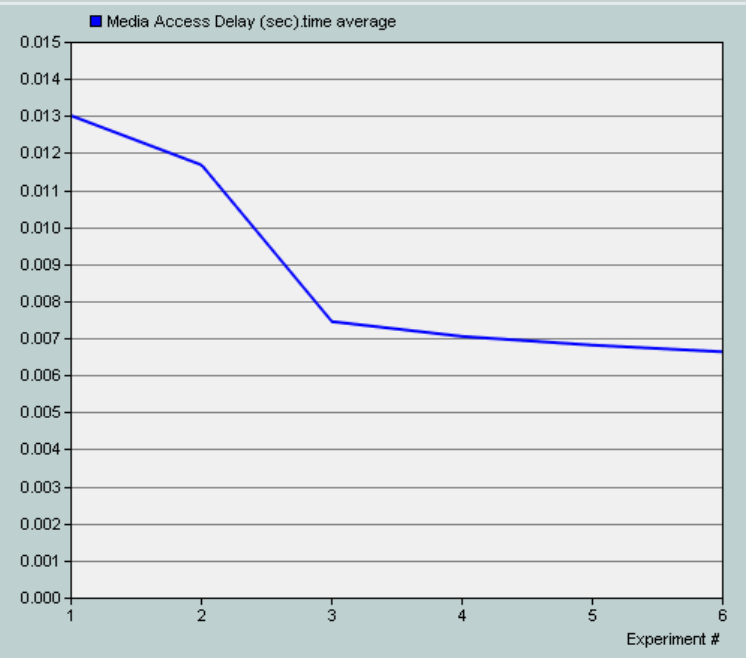
B. End-to-End Delay and Media Access Delay

(b): Media Access Delay vs. interarrival time(a) shows the End-to-End Delay of different Packet interarrival time in the network. As we compare this figure with Figure 22 (throughput at coordinator), both has a sharp decrease when interarrival time has been set to 3 seconds, and so does in (b): Media Access Delay vs. interarrival time (b) which shows the Media Access Delay of all WPAN nodes in the network. The amount of Delay we have in Media Access delay is because fewer packets can get through the MAC.

The performance of CSMA-CA algorithm and greater interarrival time cause packets to wait longer to get into the medium therefore the MAC layer can deliver with less delay which in here is around 0.007 second.



(a): End-to-End Delay vs. interarrival time



(b): Media Access Delay vs. interarrival time

Figure 23: (a) ETE delay, (b) Media access delay

C. Conclusion

In this part of simulation we have investigated the impact of different interarrival time – effectively, the traffic volume of packets in the network. The shorter interarrival time means more packets are processed in a given interval. The results show that shorter interarrival time leads to larger throughput but on the other hand introduces more delay; moreover, the delay increases in a nonlinear fashion which is not preferable in M2M network that we considered in this experiment.

Performance vs. Topology of the Network

In this part we evaluate the performance of two different topologies of ZigBeenetworks, namely that of networks in Mesh and Tree topology. The number of nodes is not high but it corresponds well to the requirements of the neighborhood area network scenario where the power meter in each home is equipped with a ZigBee/IEEE 802.15.4 interface. The meters are, in turn, connected to a neighborhood controller (possibly installed near a power transformer) within the 100 ft (30 meters) transmission range; this controller would then route meter data to the central utility servers.

We consider a network of 15 nodes (randomly spread) with CBR packet generator, packet size of 1024bits and data rate 250 Kbps. As the main role in a ZigBee network is been dictated from Pan oordinator therefore the topology type has to be set up in the coordinator.

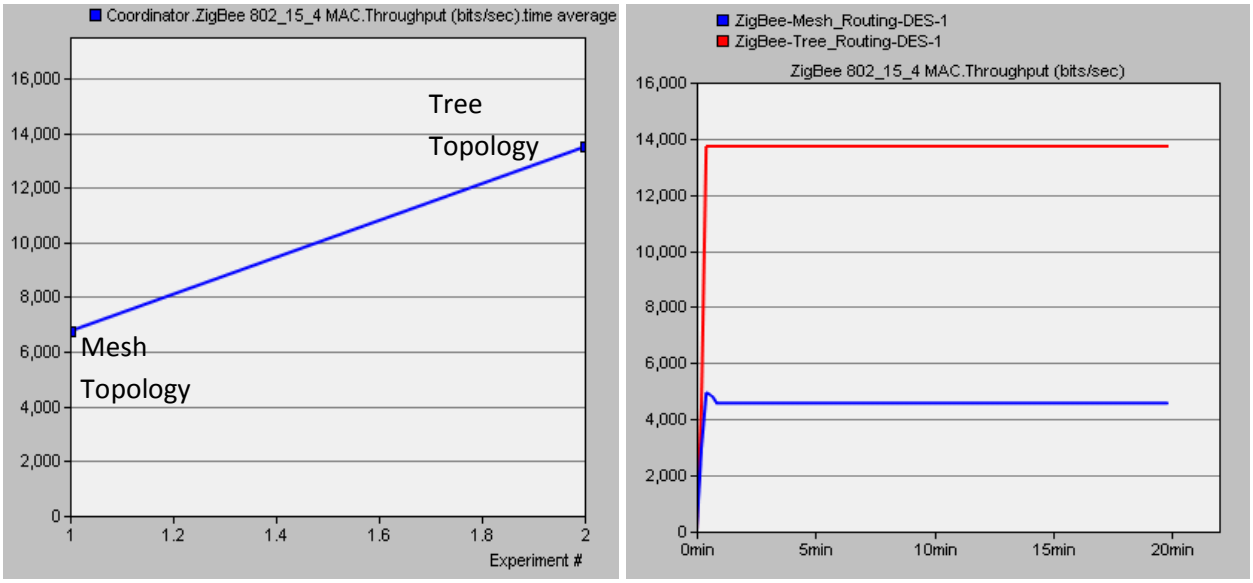


Figure 24: Throughput of Mesh/ Tree Topology at Coordinator

Fig. 24 shows the throughput at the Coordinator for the network in both Mesh and Tree topology modes. As the diagrams show, the throughput in Tree topology is about two and half times higher than Mesh topology.

The other parameter is End-to-end delay in the network, shown in Fig. 25.

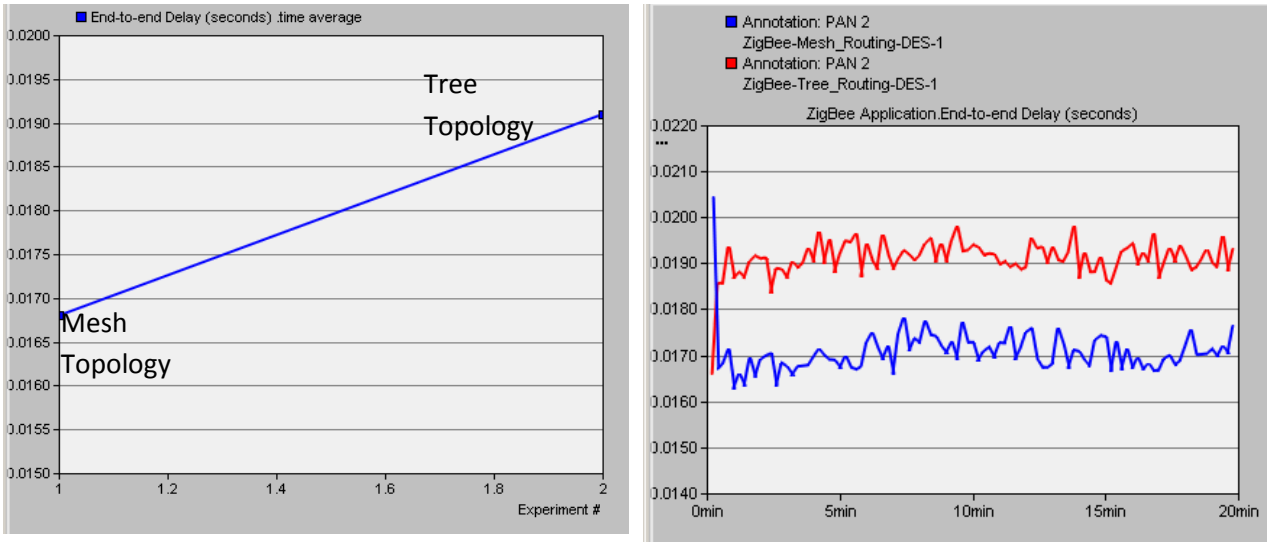


Figure 25: End-to-end Delay Mesh/Tree topology

Conclusion

We can see in the result Figure 25, tree topology has less delay between nodes than Mesh topology. Since tree topology has less inter-node path than mesh topology therefore the amount of delay for end-to-end delay is more than mesh topology in the network.

However mesh as compared to tree topology is more resilient to faults but it's more complex and since Mesh topology provide more paths between nodes than Tree topology we observed less delay between nodes. Therefore Tree topology is more efficient in the network. Overall, the results show that ZigBee network technology, operating atop IEEE 802.15.4 MAC and PHY layers, is a viable alternative for implementing the capillary M2M neighborhood area networks. Moreover, the results show that the ZigBee technology is capable of supporting a reasonable number of data sources (in this case, home power meters) with satisfactory quality of service.

5. THE IMPROVED PROTOCOL AND ITS VALIDATION

In this chapter CSMA-CA algorithm with **Prioritized wait time (PWT)** method is proposed and evaluated through experimental and analytical evaluations. The goal is to setup a high priority for M2M traffic while reducing the impact on ordinary traffic. Experimental evaluation is aimed to investigate the condition to improve packet transfer success rate while trying to keep the network desired delay threshold.

The number of parameters of the IEEE 802.15.4 protocol that can be changed in order to alter its performance is actually only two, namely:

1. The number of CCA (Clear Channel Assessment) checks, which is 2 for slotted, beacon-enabled CSMA-CA, and 1 for non-slotted, non beacon-enabled CSMA-CA.

2. The range of backoff exponents, which in both slotted and unslotted CSMA-CA is between 3 and 5, resulting in the values of actual backoff durations between 0 and 7, and 0 and 31 backoff slots, respectively.

Since the number of CCAs is already quite small, not much can be done to reduce it. Therefore, about the only adjustable parameter is the range of backoff exponents, which is determined by MAC parameters minBackoffExponent and MaxBackoffExponent. This is the essence of our PWT approach.

In Non-PWT, all nodes regardless of their type (i.e. M2M and Ordinary) have similar minBackoffExponent and maxBackoffExponent values: 3 and 5, respectively. Therefore Non-PWT scenario is considered as the benchmark method for evaluation of the PWT method.

In PWT, nodes are classified as M2M and Ordinary. For Ordinary nodes, the behavior of the CSMA-CA algorithm is not changed. For M2M nodes, the range of backoff exponent values is changed by adjusting the value of minBackoffExponent to

1 and maxBackoffExponent to 3, respectively. In this manner, M2M nodes will wait for shorter time to access the medium, and thus will get preferential treatment over Ordinary nodes. We note that a similar solution has been proposed as part of the 802.11e (and also 802.11p) standard for wireless LANs, where traffic prioritization is obtained by adjusting the range of possible random backoff values in a much wider range, for no less than four traffic categories.

An added benefit of the proposed change is that virtually no change is required on the receiver side, and only a slight change (possibly implementable in firmware) is required on the transmitter side. Moreover, existing networks and network devices that use IEEE 802.15.4 require no change at all, and can be freely mixed with modified networks as needed.

To evaluate the impact of the proposed changes, both scenarios have been applied over the network and their behaviour has been observed through simulation. Section 5.1 describes network setting for two different scenarios. Section 5.2 depicts simulations of two scenarios for different scale of networks and last section is the result summary.

Comparing PWT and Non- PWT simulation

In this section, simulation results for scenarios of Non-Prioritize Wait Time and Prioritize Wait Time are compared, using parameter values from the following Table.

Table 6: Simulation Parameters

Non-PWT scenario parameters			**PWT scenario parameters**	
Data rate		250 Kbps		250 Kbps
Number of Retransmission		5		5
BE	The BEs determines the number of backoff periods the device shall wait before accessing the channel.	Min =3 Max= 5	The BEs determines the number of backoff periods the device shall wait before accessing the channel.	M2M-Min =1 M2M-Max= 2 Ordinary-Min=3 Ordinary-Max=5
aUnitBackoffPeriod	(= 20 Symbols, for IEEE 802.15.4)		(= 20 Symbols, for IEEE 802.15.4)	
Backoff period	Range of 0 and (2^BE-1)		Range of 0 and (2^BE-1)	
CCA	Clear Channel Assessment	2	Clear Channel Assessment	2
Packet Size(bits)		1024		1024
Packet type		constant		constant
Packet interval time (sec)		1		1

A network size of 500m x 500m is used to compare the performance of Non-PWT with new method of PWT, keep the network desired delay threshold and also prioritize the generated traffic from two different types of M2M and Ordinary devices.

Simulation of network

The simulation has been conducted for two major scenarios, in which M2M devices form a minority and majority of all the nodes in the network, respectively.

Network populated with 40 percent of M2M devices

Nodes are of two different types, M2M devices which form minority of the network and we want them to have higher priority during data transmission. In addition, the ordinary devices which form majority of the network should have lower priority than M2M devices. The described network consists of 40% M2M devices.

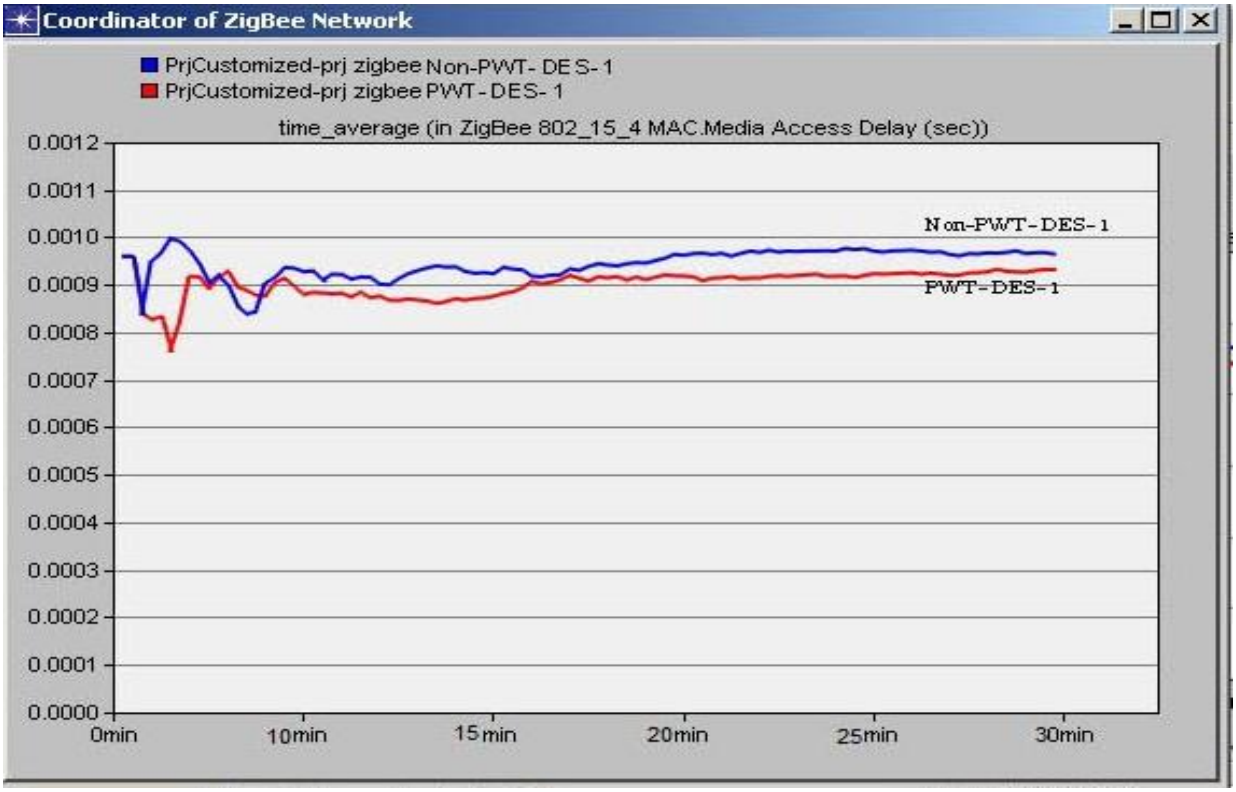


Figure 26 : Media Access delay vs. simulation time comparing Non-PWT and PWT scenarios

Simulation result shown in Figure 26, illustrate the Media access delay of the network for proposed scenario of PWT and Non-PWT. Also details of the result from Figure 26 has been transferred into excel sheet shows in Table 7.

Table 7: Numerical result comparing Media access delay of Non-PWT and PWT

Time (sec)	PrjCustomized-prj zigbee **Non PWT**-DES-1: Coordinator.ZigBee 802_15_4 **MAC.Media Access Delay**(sec)	PrjCustomized-prj zigbee **PWT**-DES-1: Coordinator.ZigBee 802_15_4 **MAC.Media Access Delay** (sec)
6	0.0096	0.0096
12	0.0096	0.0096
18	0.0084	0.0084
24	0.00951111	0.0082667
30	0.00966667	0.0083333
42	0.00991111	0.0082222
48	0.00971429	0.009181
54	0.00943333	0.0091667
60	0.00903704	0.0089185
....	....	....
66	0.0092	0.0091467
450	0.00971892	0.0091784
456	0.00971022	0.009184
462	0.00976491	0.0091895
468	0.00974199	0.0091532
474	0.00976068	0.0092
480	0.00971139	0.0092321
....	....	....
540	0.00965693	0.0092494
546	0.00965037	0.0092593
552	0.00967326	0.0092747
558	0.00966667	0.0093246
564	0.00968315	0.0092817
570	0.00971631	0.0092738
576	0.00965895	0.009266
582	0.009675	0.0092972
588	0.00967973	0.0093223
594	0.00964626	0.0093197
Average/second	0.0094418	0.0090197

Furthermore, to investigate the ETE delay of the network and result gathering, we have run the simulation to illustrate ETE delay for both scenarios. Duration of simulation was set for 30 minutes with both scenarios running simultaneously

during the simulation. As shown in Figure 27, running both scenarios over the network does not have much effect on ETE Delay parameter. The maximum amount of network delay is approximately 0.006 second for both scenarios.

This shows the average of the End-to-end delay particularly at the coordinator; in order to get more specific result and have better analysis of what is the effect Prioritized wait time has on the End-to-end result, we observed each individual device separately.

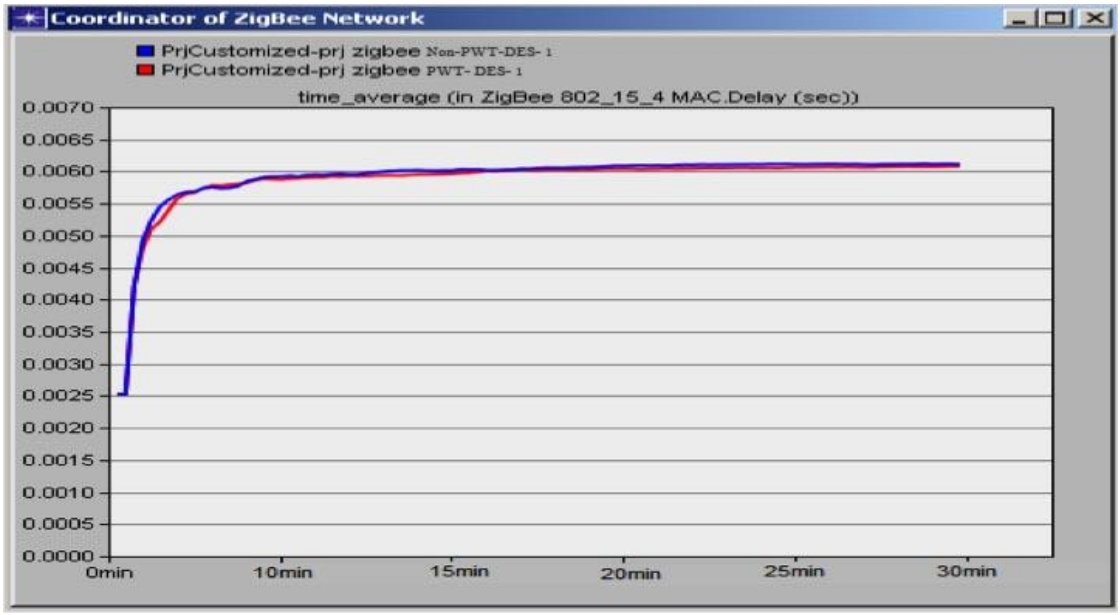


Figure 27: Delay vs. simulation time, Non-PWT and PWT scenarios

Performance analysis for each type of device

This section consists of detailed analysis of PWT using both M2M delay and Ordinary delay.

In order to achieve an in-depth analysis of the network behavior using both devices, the experiment evaluates delay for each device under the given condition.

Delay of M2M devices

Behaviour of all M2M devices has been observed separately in terms of end to end delay and media access delay.

Figure 28 shown below, depicts the results for one individual M2M devices.

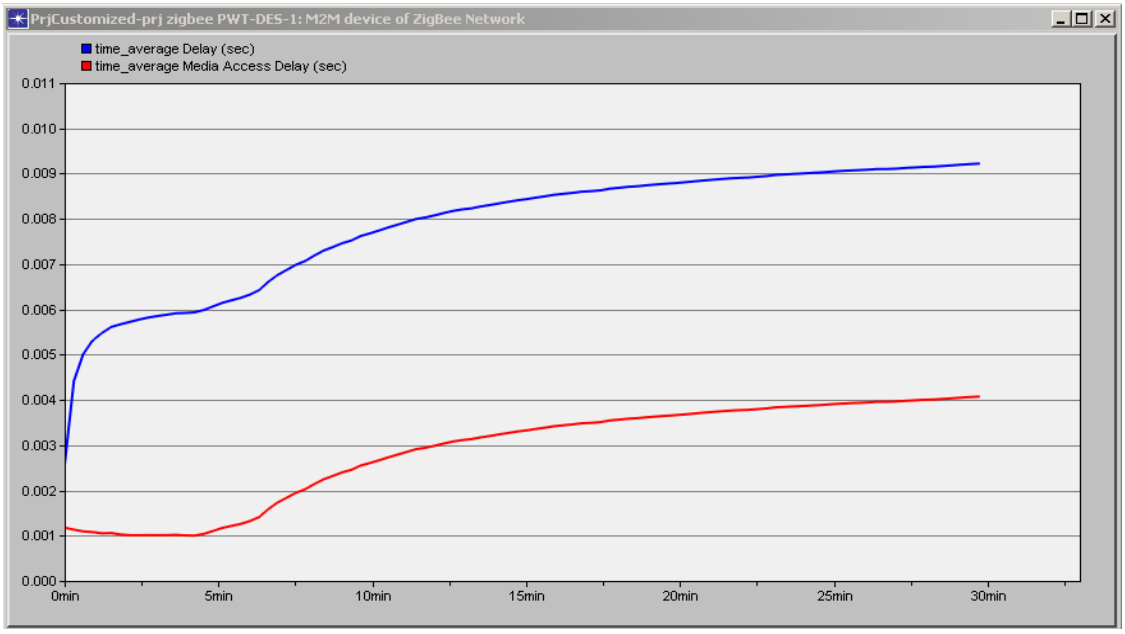


Figure 28: Both, Media access delay and ETE delay for a M2M device vs. simulation time

Comparing delay for M2M device with same result for ordinary devices shown in Figure 29, we can see the difference which is the effect of Prioritized wait time approach. Also we expected such a result after analysis of the Media access delay at the coordinator shown in Figure 26.

Analysis of each individual device makes this observation more clear, therefore to get strong findings we have repeated this experience for each device. Afterward to obtain the total delay we did some small calculation and the ordered result has been put into the Table 8.

Delay of ordinary devices

Behaviour of all ordinary devices in Prioritized Wait Time scenario has been observed separately in terms of end-to-end delay and media access delay.

It should be noted that ordinary devices have different backoff exponent than M2M devices according to PWT scenario. The amount of backoff exponent for ordinary devices is greater than M2M devices. Figure 29 illustrates the result for an ordinary device in the network.

Since according to Prioritized wait time (PWT) scenario, ordinary devices has to wait longer in order to access the channel therefore the media access delay as seen in the figure is greater than same result in each M2M device.

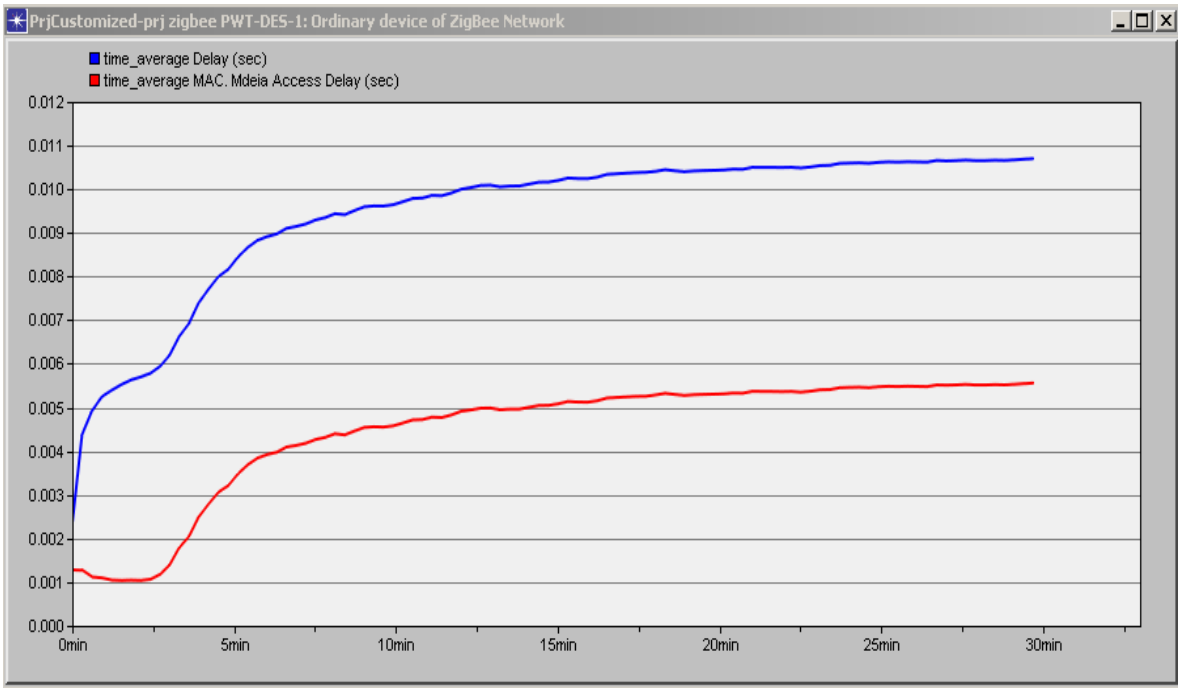


Figure 29: Media access delay and delay for ordinary devices vs. simulation time

Total delay calculation

This observation has been repeated for all devices in order to calculate the total delay. Based on the definition of ETE delay and Media access delay in OPNET Modeler (Simulator program used in this experiment), which also brought up earlier we have (1);

$$D_{\text{Total delay for a device (sec)}} = \text{ETE Delay (sec)} + \text{Media Access Delay (sec)} \qquad (1)$$

Also, average delay for M2M devices, has been calculated by adding all individual delays and dividing it by total number of M2M devices (2);

$$N = [1 \ldots i]$$

$$D_{\text{Average delay of all M2M devices in the network}} = \frac{D1 + D2 + D3 + \ldots + Di-1 + Di}{i} \qquad (2)$$

This practice was done for ordinary devices as well.

To validate the result, various scale of network was considered for simulation, the nodes increased up to 30 nodes. The result of both type of devices are organized into two categories refer to each scenario.

Table 8, represents average delay of all M2M devices on the network of 10, 15... 30 nodes affect by both scenario of PWT and Non-PWT. Comparing numbers in table below allows to investigate the amount of delay in M2M devices imposed by methods. In PWT scenario we claimed that decrease in number of backoff exponent on M2M devices creates higher priority than the other devices in data transmission.

Table 8: Delay analysis of M2M devices and Ordinary devices in PWT vs. Non-PWT

Average total Delay(sec) : ETE Delay + MA Delay			
Network scale: #Nodes	PrjCustomized-prj zigbee **Non PWT**-DES-1: ZigBee Network.802_15_4 MAC	PrjCustomized-prj zigbee **PWT**-DES-1: ZigBee Network.802.15.4 MAC **Ordinary devices**	PrjCustomized-prj zigbee **PWT**-DES-1: ZigBee Network.802.15.4 MAC **M2M devices**
10	0.0188	0.0213	0.0168
15	0.0281	0.0345	0.0255
20	0.0369	0.0459	0.0338
25	0.0461	0.0528	0.0423
30	0.0558	0.0682	0.0509

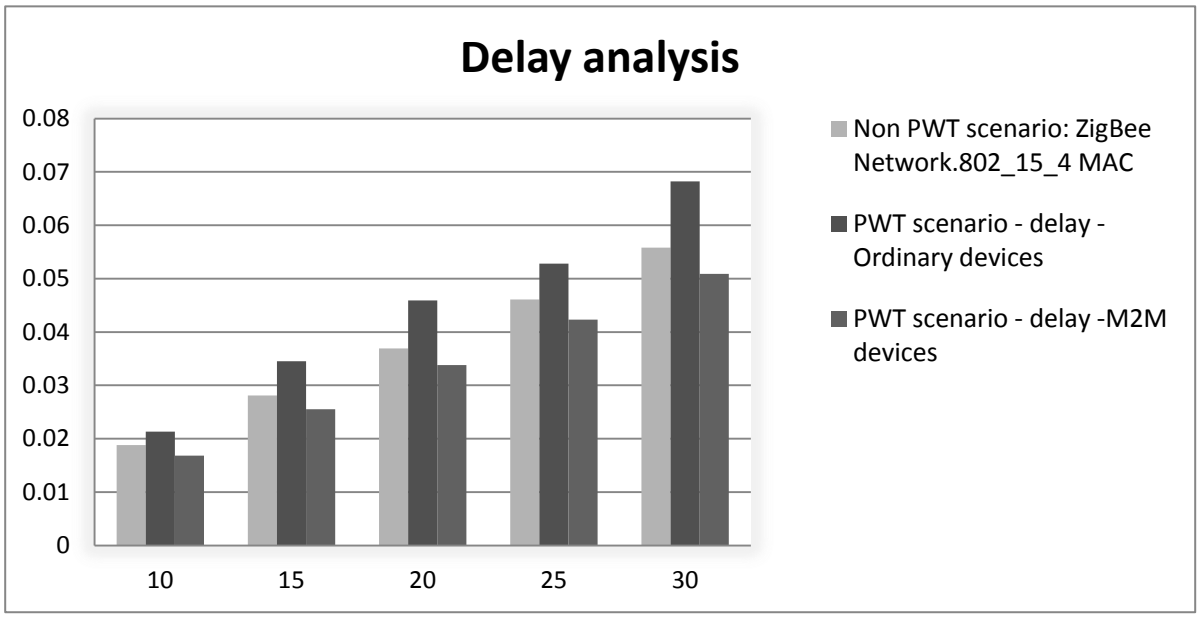


Figure 30: Delay analysis of M2M devices and Ordinary devices in PWT vs. Non-PWT

As inferred from tables, amount of delay for M2M in PWT is less than Non-PWT scenario.

Throughput

In order to investigate the behaviour of the network responding to proposed scenario, throughput of both methods is essential. Default code in node process model has been customized in order to achieve this purpose. Figure 31, illustrate throughput for both scenarios in network of 10 to 30 nodes.

The impact of various backoff exponents for M2M devices is shown in the diagram below. In Prioritized Wait Time scenario which each type of devices (M2M and Ordinary) are organized into separate group shows 20 percent of improvement in the network of 30 nodes. It's because of forming of two separate groups for devices to access the channel, therefore competition is less and packet collision decrease.

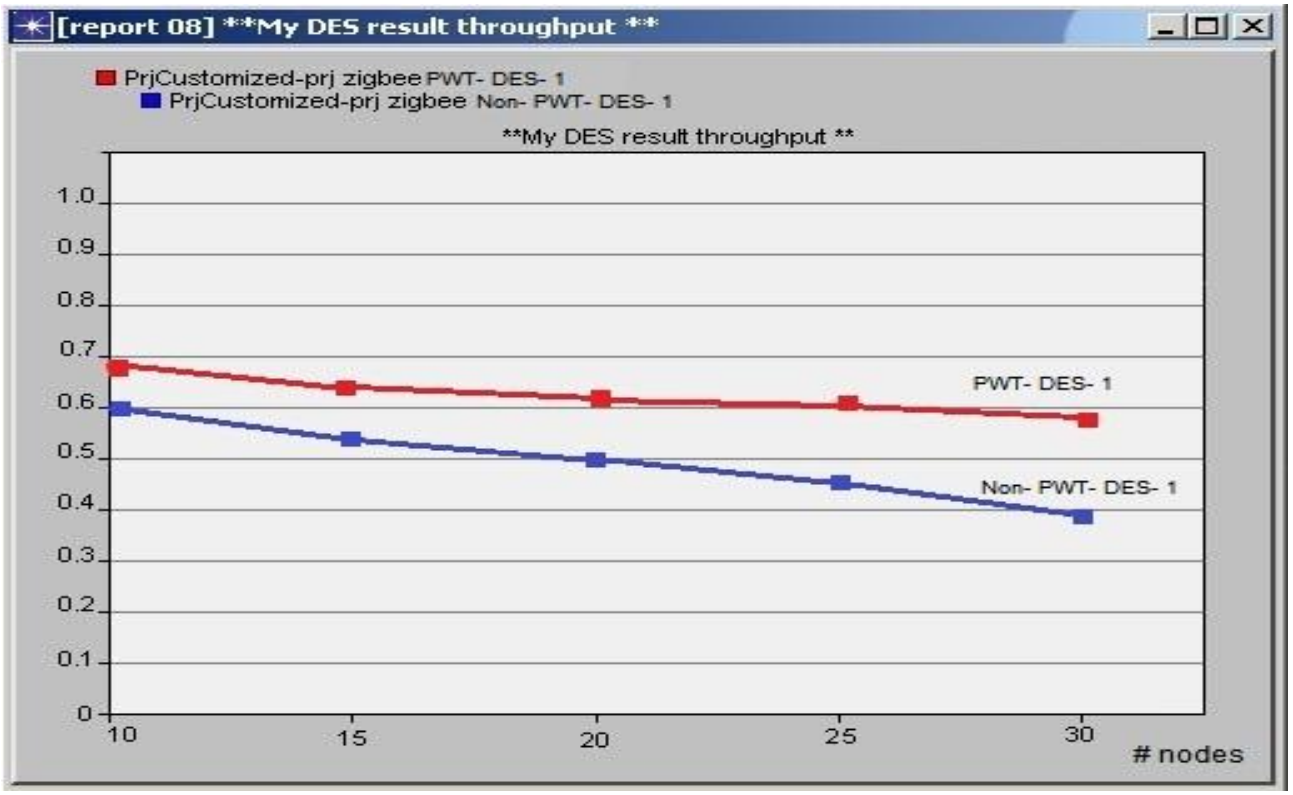


Figure 31: Throughput of Both scenarios vs. number of nodes.

Network populated with 60 percent of M2M devices

In this section a network with majority of M2M nodes has been considered to evaluate the response of PWT method. A network size is same as the previous network, 500m x 500m is used to compare the performance of Non-PWT with method of PWT, keep the network desired delay threshold and also prioritize the generated traffic from two different types of M2M and Ordinary devices.

Also, ordinary devices which form minority of the network and should have lower priority than M2M. Network has 60% of M2M devices and the remaining 40% are ordinary devices. Simulation parameters are mentioned in Table 6.

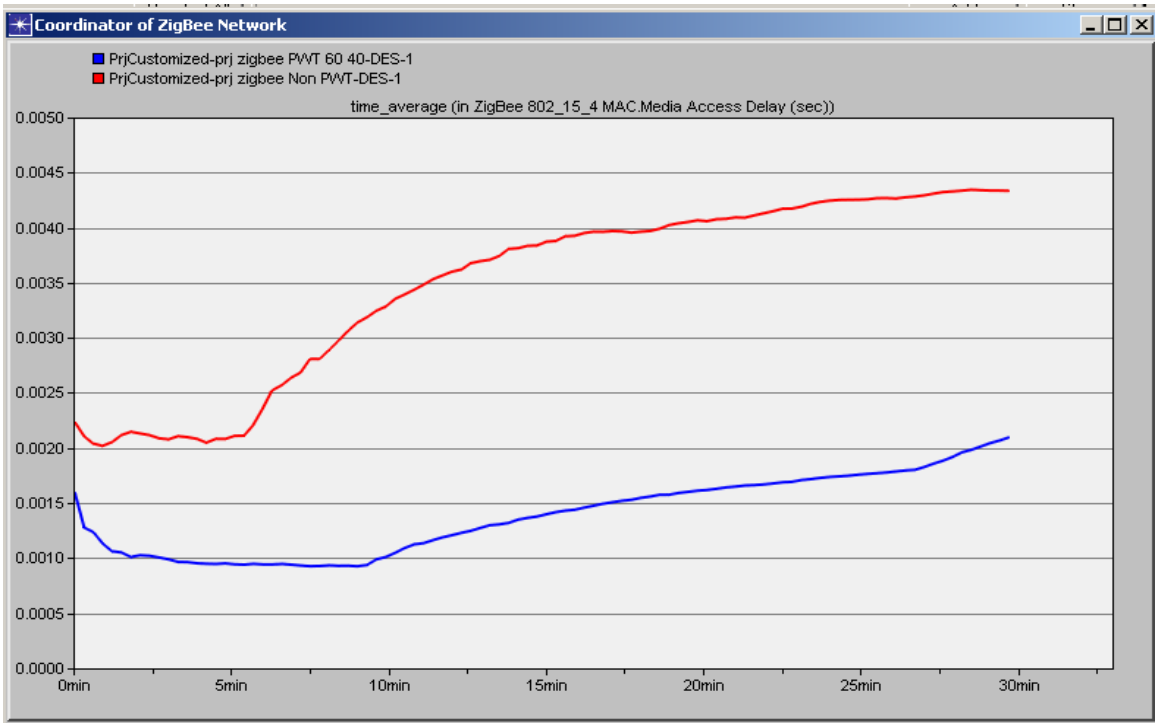


Figure 32: Media access delay in a network with 60% M2M devices vs. simulation time

By allocating smaller value of backoff exponent to M2M devices in the network, aggregate media access delay got affected as the result shown in Figure 32, media access delay on the network running PWT scenario is less than Non- PWT.

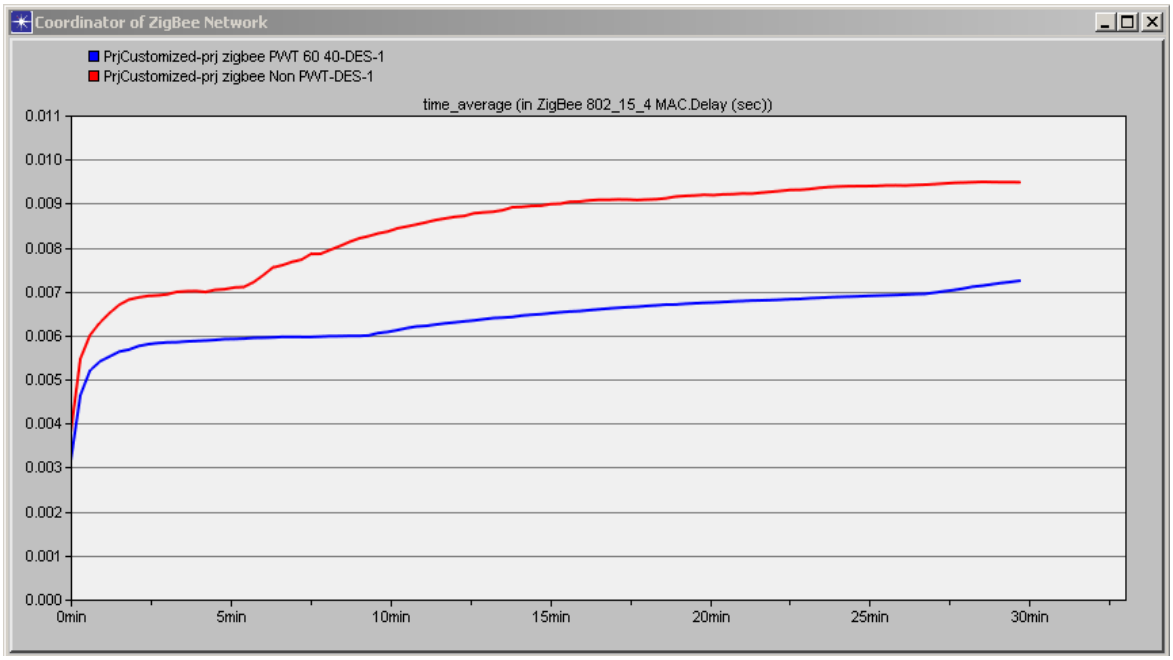


Figure 33: End-to-end delay in a network with 60% M2M devices vs. simulation time

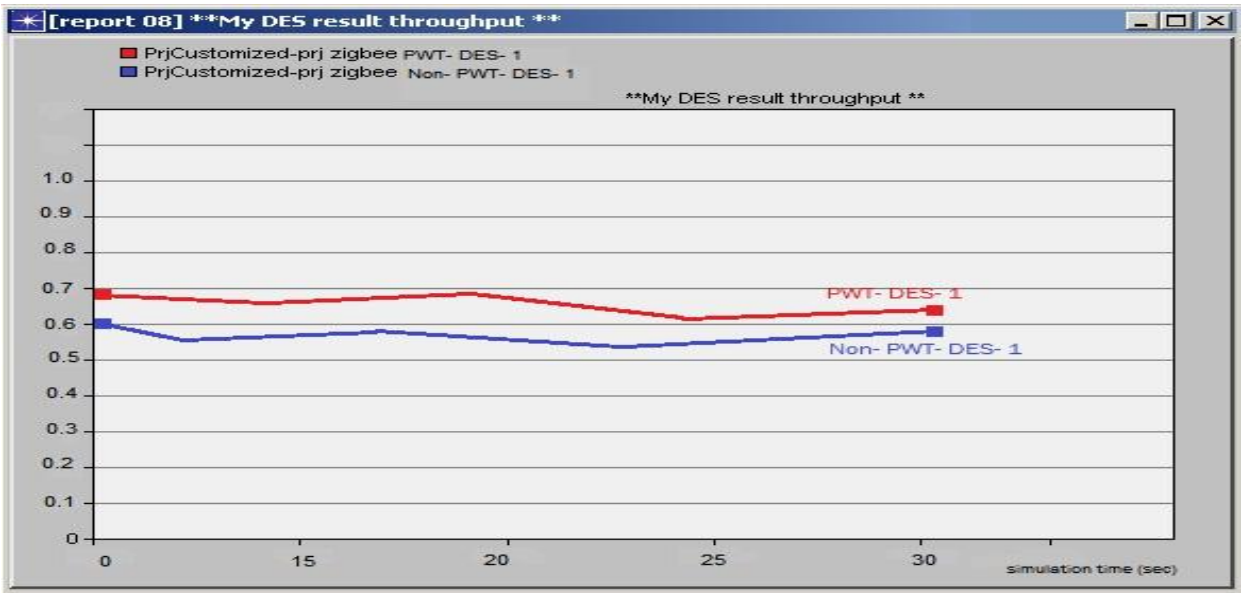


Figure 34: Throughput of Both scenarios in a network with 60% M2M devices vs. simulation time

In terms of ETE delay, PWT scenario still has better performance than Non-PWT. Figure 33, shows ETE delay for both scenarios in the network. In Prioritized Wait Time the devices has been organized into two categories and each category has specific backoff exponent which defines high priority and low priority to access the media. Therefore M2M devices may wait for less period of time to access the media

and meanwhile ordinary devices are not in compete with them. Organizing the access time for devices creates an ordered traffic thus there is less collision and consequently less need to retransmit the data packets.

Figure 34, illustrates the actual throughput in both PWT and Non-PWT scenario. Prioritized Wait Time shows 10 percent of improvement in the results for the network of 30 nodes. This simulation has been run for 5 times in order to gather the data.

SUMMARY

Some of the results in this Section may come as a surprise, as it may seem that we can obtain a reduction in total (i.e., end-to-end) delay while not sacrificing throughput. The explanation is, in fact, quite simple. First, let us note that the number of nodes and the traffic characteristics indicate that the network is working in its regular regime, far from saturation. Therefore, a linear increase in performance may be possible without any degradation.

Second, the original IEEE 802.15.4 protocol suffers from a number of problems which are explained in detail in ref. [19]. Reduction of the range for random backoff countdowns, which is the essence of the PWT approach, does not affect the areas of problematic behavior; instead, it actually allows better performance to be obtained at virtually no expense.

If the number of nodes is increased further, we will eventually bring the network closer to saturation, in which case the PWT protocol may still result in some performance improvements but they will not come for free. However, as long as the number of nodes is kept within reasonable range, this degradation will not occur. We stress that the `reasonable range', in this case, is more than sufficient for practical purposes, due to the limited transmission range of IEEE 802.15.4 devices which means that such networks will almost never have too many nodes.

Proposed scenario PWT has been compared to Non- PWT scenario over various scale of network considering M2M as minority of devices (40 percent M2M device and 60 percent ordinary). Network has been analyzed in terms of effect of both scenarios on ETE delay and media access delay, as observed PWT does not have much impact on Media access delay and ETE delay. Therefore, applying smaller value of backoff exponent for M2M devices and applying greater value to ordinary devices does not increase the network delay. As a result the purpose of trying to keep the network delay below the desired threshold (or, rather, below the value that would be obtained in an 802.15.4 network with non-modified devices) is successfully achieved.

Total delay of all devices has been calculated and compared when M2M devices in the network are running under the PWT scenario. Analysis of delay in M2M device and delay of ordinary device indicates a slight difference. It can be concluded that M2M devices have less delay than Ordinary devices in the network.

Study of network in terms of throughput also indicates a 20 percent improvement in the last simulation of 30 nodes in PWT scenario. By categorising devices and allocating appropriate backoff exponent to each category creates a priority for each category while it results in improvement of successful packet transfer rate.

In the next section, where the network consists of 60% of M2M devices running the PWT protocol and 40% of Ordinary devices running the unmodified protocol, there is still decrement in ETE delay. The larger number of nodes utilizes a smaller range of backoff exponent, and channel access is achievable in a shorter period of time.

Overall, the PWT modification is successfully shown to improve the performance of the network for M2M device traffic, without degrading the performance of the network for the traffic from Ordinary (i.e., wireless sensor) nodes. This confirms the validity of the proposed modification.

6. CONCLUSION AND DIRECTIONS FOR FUTURE RESEARCH

SUMMARY

In this work, the performance of capillary M2M networks running ZigBee/IEEE 802.15.4 has been analyzed. Network with variable number of nodes and variable traffic along with tree topology and mesh topology has been considered into simulation.

Then, based on CSMA-CA algorithm a scenario for highlighting M2M traffic of the network in wireless sensor networks has been proposed. The proposed scenario specifically aim to create priority for M2M device to transfer their data to the coordinator, while keep the balance for other devices as well.

The suggested scenario, Prioritize Wait Time is a method for balanced channel access delay between M2M devices and ordinary devices meanwhile it gives higher priority to M2M devices. It not only considered the importance of having short period of delay to access channel, but also considers data rate and successful packet transfer as the criteria to achieve data transmission scheme with better quality.

FUTURE RESEARCH DIRECTIONS

Considering dynamic join or disjoin of a few number of devices will add some challenging condition to the problem, where some nodes join or disjoin to the network. This will cause different load for both types of nodes which have been considered in the network.

For this purpose a function can be defined which determines a dynamic analysis in certain period of time over the network to adjust the pre-configured algorithm.

BIBLIOGRAPHY

1. David Boswarthick. M2M activities in ETSI. Presentation at SCS Conference, July 2009; Available from: www.pole-scs.org.
2. Service requirements for machine-type communications (M2M); stage 1, release 11. *Technical Report TR 22.368 V11.0.1*, 3GPP, Sophia Antipolis, France, Feb. 2011.
3. Sokele, M., Hudek, V., Mincu, A. I. *Opportunities for implementation machine-to machine services via 3G mobile networks*. in *Proceedings of the 7th International Conference on Telecommunications (ConTEL)*, 2003.
4. Bob Emmerson. M*2M: the Internet of 50 billion devices*, in *M2M Magazine*. January 2010.
5. Beale, M. and Y. Morioka. *Wireless machine-to-machine communication*. in *Proc. 41st European Microwave Conference (EuMC)*. pp. 115-119, 2011.
6. S. Palat and Ph. Godin. The LTE Network Architecture: A comprehensive tutorial. In S. Sesia, I. Toufik, M. Baker (eds.), *the UMTS Long Term Evolution: From Theory to Practice*, John Wiley & Sons, 2009.
7. Saad Z. Asif. *Next Generation Mobile Communications Ecosystem: Technology Management for Mobile Communications*. John Wiley & Sons, 2010.
8. Ian F. Akyildiz, David M. Gutierrez-Estevez, Elias Chavarria Reyes The evolution to 4G cellular systems: LTE-Advanced. *Physical Communications* **3**:217-244, 2010.
9. *IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirement Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs).* IEEE Std 802.15.4a-2007 (Amendment to IEEE Std 802.15.4-2006), 2007: p. 1-203.
10. Bob O'Hara and Al Petrick. *802.11 Handbook: a Designers Companion*. IEEE Press, 1999.
11. *E-health architecture: analysis of user service models. technologies and applications supporting eHealth*. ETSI technical report TR 102 764 V1.1.1, February 2009.
12. Katenka, N., E. Levina, and G. Michailidis, Local Vote Decision Fusion for Target Detection in Wireless Sensor Networks. *IEEE Transactions on Signal Processing* **56**(1):329-338, 2008.

13. Harri Holma and Antti Toskala, eds. *LTE for UMTS OFDMA and SC-FDMA Based Radio Access*. 2009, John Wiley & Sons. 61
14. *Business Models, Use cases & Technical Requirements.* EXALTED (Expanding LTE for Devices) project deliverable WP2 - D2.1, May 2011.
15. Y. Chen and W. Wang. Machine-to-machine communication in LTE-A. *VTC 2010-Fall*, 2010.
16. Tacshik Shon and Yongsun Park. A Hybrid Adaptive Security Framework for IEEE 802.15.4-based Wireless Sensor Networks*.* KSII Transactions on Internet and Information Systems **3**(6):597-611, Dec. 2009.
17. Roberto De Boins and T.I.R. Trends. *M2M and Sensor Networks:*. in *ETSI Workshop on Machine to Machine Standardization*. 4 - 5 June 2008. Sophia Antipolis, France.
18. Zhong Fan and Siok Tan. M2M communication for E-Healht: Standards, Enabling Technologies and Research Challenges, in *6th International Symposium on Medical Information and Communication Technology (ISMICT)*, May 2012.
19. J. Mišić and V. B. Mišić., *Wireless Personal Area Networks; Performance, Interconnections, and Security with IEEE 802.15.4*. Chichester. UK: John Wiley and Sons, 2008
20. V. B. Mišić, J. Mišić, X. D. Lin, and D. Nerandžić. "Capillary Machine-to-Machine Communications: The Road Ahead", *11th International Conference on Ad Hoc Networks and Wireless AdHocNow*, Belgrade, Serbia, July 2012.
21. V. B. Mišić, J. Mišić, and D. Nerandžić. "Extending LTE to Support Machine-Type Communications", *IEEE Int. Conf. on Communications ICC 2012 – Workshop on Telecommunications: From Research to Standards (T2S)*, Ottawa, ON, June 2012.