OULUN YLIOPISTO
DEPARTMENT OF COMMUNICATIONS ENGINEERING
DEGREE PROGRAMME IN WIRELESS COMMUNICATION ENGINEERING

EVALUATION OF LONG TERM EVOLUTION AND IEEE 802.15.4K FOR SUBURBAN ENERGY SMART METERING

Author _____
Avvaru Aravind

Supervisor _____
Prof. Matti Latva-aho

Instructor _____
Dr. Jussi Haapola

Accepted _____ /_____ /2013

Grade _____

Aravind P. (2013) Evaluation of Long Term Evolution and IEEE 802.15.4k for Suburban Energy Smart Metering. Department of Communication Engineering, University of Oulu, Oulu, Finland. Master's thesis, 69 p.

ABSTRACT

Smart grid is a concept to modernize the present day electricity power network with efficient transmission, distribution and consumption of energy to the end devices by application of information and communication technologies. Recently, smart meters have been introduced in smart grids for dynamic pricing and to satisfy the present day demands using real-time communication technologies. Communication technologies in smart meters are used to exchange information with the grid. The communication between smart meters and the grid have certain predefined requirements that are specified by the standard organization bodies e.g., national institute of standards and technology (NIST). The feasibility of the communication technology can be concluded, if the requirements set by such standard organizations are satisfied. In this thesis firstly, the feasibility of long term evolution and institute of electrical and electronics engineers (IEEE) 802.15.4 wireless personal area networks are studied using NIST specific smart grid use cases. Secondly, the thesis provides a solution for the fragment and cyclic redundancy check (CRC) checksum sizes in the medium access layer of low energy critical infrastructure monitoring (LECIM) IEEE 802.15.4k draft amendment standard. Finally, the energy consumed for transmission while using wireless sensor node (i.e., LECIM node) for the obtained results of fragment and CRC checksum sizes is evaluated.

Keywords: Smart grids, Smart metering, LTE, IEEE 802.15.4k, Fragmentation analysis, Error correction coding, CRC, Energy Analysis.

TABLE OF CONTENTS

FOREWORD

This master's thesis has been carried out at the centre for wireless communications (CWC), University of Oulu Finland in the project smart grids and energy markets (SGEM) work package (WP) 6 supported by funding agency TEKES. I wish to express my gratitude to the TEKES for funding my master thesis research through the project SGEM. The WP-6.1 in the project SGEM proposes new information and communication technologies (ICT) in network management, and in information security.

I would like to thank my thesis instructor Dr. Jussi Haapola for his patience, invaluable advices, help, corrections and suggestions with regular meetings. Without him it would be impossible to complete this thesis. I would like to express my heartfelt thanks to my thesis supervisor, Professor Matti Latva-Aho for giving me this opportunity and his confidence on me. I would like to thank M.Sc. Juha markkula for helping me in practically providing the Opnet LTE model simulation results. Furthermore, I would also like to thank M.Tech. Animesh Yadhav who has helped me during coffee breaks when I am stuck with the matlab simulations and B.E. Kamaldeep Singh for his moral support during the entire thesis.

Finally, I wish to thank the almighty god for the completion of this master thesis.

Oulu, February 14, 2013

Avvaru Aravind

LIST OF ABBREVIATIONS AND SYMBOLS

ACK	Acknowledgement
A/D	Analog to digital conversion
ARQ	Automatic Repeat Re-Quest
AM	Amplitude Modulation
AMI	Advanced Metering Infrastructure
AMR	Automated Meter Reading
AMM	Advanced Meter Management
ASK	Amplitude Shift Keying
AuC	Authentication Center
AP	Aggregation Point
BPSK	Binary Phase Shift Keying
BCCH	Broadcast Control Channel
BLE	Battery Life Extension
BI	Beacon Interval
BE	Backoff Exponent
BER	Bit Error Rate
BO	Beacon Order
BW	Bandwidth
CAP	Contention Access Period
CC	Chase Combining
CCA	Clear Channel Assessment
CCCH	Common Control Channel
CFP	Contention Free Period
CN	Core Network
CRC	Cyclic Redundancy Check
CSS	Chirp Spread Spectrum
CW	Contention Window
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA-CD	Carrier Sense Multiple Access with Collision Detection
CP	Cyclic Prefix
D/A	Digital to analog conversion
DFT	Discrete Fourier Transform
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
DTCH	Dedicated Traffic Channel
DVB	Digital Video Broadcasting
DQPSK	Differential Quadrature Phase Shift Keying
EDGE	Enhanced Data rates for GSM Evolution
ECC	Error Correction Codes
eNodeB	Evolved Node B
EPC	Evolved Packet Core
EPS	Evolved Packet System
E-UTRAN	Enhanced Universal Terrestrial Radio Access Network
FCS	Frame Check Sequence
FFD	Full Function Device

FFT	Fast Fourier Transform
FDD	Frequency-division duplex
FEC	Forward Error Correction
FTP	File Transfer Protocol
FSK	Frequency Shift Keying
3GPP	Third Generation Partnership Project
GBR	Guaranteed Bit Rate
GF	Galois Field
GSM	Global System for Mobile Communication
GTS	Guaranteed Time Slot
GPRS	General Packet Radio Service
GGSN	Gateway GPRS Support Node
GUTI	Global Unique Temporary Identity
HSPA	High Speed Packet Access
HSDPA	High Speed Downlink Packet Access
HSS	Home Subscription Server
HTTP	HyperText Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
ITU	International Telecommunication Union
ICT	Information and Communication Technologies
IDFT	Inverse DFT
IFFT	Inverse FFT
IP	Internet Protocol
IP-GW	IP Gateway
IMS	IP Multimedia Sub-System
IMSI	International Mobile Subscriber Identity
IR	Incremental Redundancy
ISI	Inter Symbol Intereference
LECIM	Low Energy Critical Infrastructure Monitoring
LFSR	Linear Feedback Shift Register
LQI	Link Quality Detection
LSB	Least Significant Bit
LTE	Long Term Evolution
M2M	Machine to Machine
MAC	Medium Access Control
MCCH	Multicast Control Channel
MHR	MAC Header
MFR	MAC Footer
MLS	Maximum Length Sequences
MM	Mobility Management
MME	Mobility Management Entity
MMSE	Minimum Mean Square Error
MPDU	MAC Protocol Data Unit
MSB	Most Significant Bit
MSDU	MAC Service Data Unit
MTCH	Multicast Traffic Chanel
NB	Number of Backoff

NIST	National Institute of Standard and Technology
OFDM	Orthogonal Frequency Division Multiplexing
O-QPSK	Offset QPSK
OVSF	Orthogonal Variable Spreading Factor
PAN	Personal Area Network
PAPR	Peak to Average Power Ratio
PD-SAP	Physical Data Service Access Point
P-GW	Packet Gateway
PCH	Paging Channel
PBCH	Physical Broadcast Channel
PCFICH	Physical Control Format Indicator Channel
PCRF	Policy and Charging Resource Function
PCCH	Paging Control Channel
PDCCH	Physical Downlink Control Channel
PDSCH	Physical Downlink Shared Channel
PER	Packet Error Rate
PHICH	Physical Hybrid ARQ Indicator Channel
PL	Path Loss in dB
PLC	Power Line Communication
PLME	Physical Layer Management Entity
PN	Pseudo Noise
PPDU	Physical Layer Protocol Data Unit
PRACH	Physical Random Access Channel
PSSS	Parallel Sequence Spread Spectrum
PUCCH	Physical Uplink Control Channel
PUSCH	Physical Uplink Shared Channel
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
QOS	Quality of Service
RAN	Radio Access Network
RF	Radio Frequency
RFD	Reduced Function Device
RLC	Radio Link Control
RTU	Remote Terminal Unit
RNC	Radio Network Controller
RRM	Radio Resource Management
RS	Reed Solomon
SAP	Service Access Point
SAE	System Architecture Evolution
SAE GW	SAE Gateway
SD	Superframe Duration
SECDED	Single Error Correct Double Error Detect
SFD	Start Frame Delimiter
SG	Smart Grid
S-GW	Serving Gateway
SC-FDMA	Single Carrier Frequency Division Multiplexing Access
SGSN	Serving GPRS Support Node

SIP	Session Initiation Protocol
SO	Superframe Order
SUN	Smart Utility Networks
TDD	Time-Division Duplex
USIM	Universal Subscriber Identity Module
UMTS	Universal Mobile Telecommunication System
UWB	Ultra Wideband
UL-SCH	Uplink Shared Channel
VOIP	Voice Over Internet Protocol
XOR	Exclusive OR
WCDMA	Wideband Code Division Multiple Access
WPAN	Wireless Personal Area Network
Wi-Fi	Wireless Fidelity
WSN	Wireless Sensor Network
WIMAX	Worldwide Interoperability for Microwave Access

α	gaussian field element
A	free space pathloss constant
A_i	weight distribution of the code
B_i	weight distribution of the dual code
a, b, & c	data driven constant in Erceg pathloss model
$c(t)$	raised cosine pulse
d	hamming distance
d_{pl}	distance separation between the transmitter and receiver
d_{pl0}	reference distance separation between the transmitter and receiver
D	distance between transmitter and receiver
Δf	frequency subcarrier spacing
ϵ	bit error rate
e	number of errors
e_b	energy consumption per bit
e_{tx}	energy required for transmission
e_{rx}	energy of the received bit
e_{te}	energy required for the transmitter electronics
e_{ta}	energy of the transmit amplifier
η_{amp}	transmitter efficiency
f_c	carrier frequency in megahertz
$g(x)$	generator polynomial
γ	memory digits in convolution code
γ_{pl}	pathloss component
G_{ant}	antenna gain
h_{bs}	base station height in meters
h_{ms}	mobile station height in meters
i	weight of the code
k	message length of the code
l	output frequency domain symbols
$L(x)$	error location polynomial
L_p	free space path loss
m	number of correctable errors in the code
M	number of orthogonal subcarriers in SCFDMA
μ_σ	mean of σ
N	number of subcarriers
n	block length of the code
n_t	n transmit pair antennas
P_{ue}	probability of undetected error
PL	pathloss
PL_f	free space pathloss
$p(t)$	half sine pulse
Q	bandwidth expansion factor
r_m	receive antenna pairs
$s(t)$	time domain representation of OFDM signal
$s(x)$	syndrome polynomial
t	time in seconds
t_c	number of errors correctable by the code

T_c	chip duration in seconds
$W(x)$	error evaluation polynomial
$X(k)$	kth subcarrier of the signal
y, z	zero mean Gaussian random variable of unit standard deviation N[0,1]
$\cos$	cosine function
$\sin$	sine function
$\log$	logarithm function
Π	pi

1. INTRODUCTION

A standard electrical grid network consists of transmission lines, substations, transformers and devices that can deliver electricity from power plant to the end users. The electrical power grid network is primitively developed and designed as a centralised unidirectional system of electric power transmission, distribution with demand driven control. With the enhancements in information and communication technologies (ICT), many new possibilities to control and manage the energy transmission, distribution, and consumption are yielded which further led to the invention of smart grid (SG). SGs are introduced to generate, consume and distribute energy efficiently in the electricity grid network. The term SG was first coined and used by Massoud Amin, S. and Wollenberg, B.F. [1]. SG can be defined as an advanced digital two way communication power flow power system consisting of self healing network with resilient architecture, and sustainable generation with foresight prediction under different uncertainties [2]. The main key applications of SG are in smart metering, distributed automation, demand response and wide area monitoring. The application of SG to the present electrical power grid network is to enhance and improve the efficiency, reliability both in transmission and distribution side. The application wide area monitoring is used to monitor real time generation and transmission in the electrical power grid. The distributed automation refers to intelligent control of devices in distribution side. The application demand response relates to implementation of dynamic demand mechanisms which are used to manage energy consumption in response to supply. The smart metering enables the operator to monitor and remotely read the energy usage with the help of metering systems. In the last two decades, smart metering has gained more attention. Distribution utilities are replacing the traditional mechanical meters with smart meters. Smart meter is an electrical consumption measurement device which records electrical energy and power usage and send them back to the utility in specific intervals of time [3]. The functionalities of the smart meters are improved with new approaches in metering systems. The previously used metering systems in the electrical grid network are called automated meter reading (AMR) systems. AMR systems use only one way communication to remotely read energy usage and does not permit the operator to control and manage them. Advanced metering infrastructure (AMI) is the newer version of AMR systems in SG which use smart meters to measure, collect and analyze the energy usage with bidirectional communications.

The smart meter requires communication technology to interact with the utility. Different communication technologies are proposed for the use in smart meters and can be seen in the recent literature [4]. Some of them include wired communication (e.g, power line communication (PLC) [5]) or wireless communication (e.g., general packet radio service (GPRS) [6], bluetooth technology [7], and peer to peer technology [8]). The use of a particular communication technology in smart meters depends on the communication requirements. The communication requirements for smart metering can be obtained from the documents released by national institute of standards and technologies (NIST) [9]. If the requirements set by such standard organizations are satisfied, the usage of a particular communication technology can be concluded.

In this thesis, we study the feasibility of long term evolution (LTE) and institute of electrical and electronics engineers (IEEE) 802.15.4k [10] wireless sensor networks (WSN) in smart meters. The feasibility is studied in order to understand the usage

of the particular communication technologies in smart meters and to analyse whether smart meter traffic effects LTE and WSN traffic. The feasibility of the chosen communication technologies (i.e., LTE and WSN) is concluded by comparing the output simulation results with the NIST [9] smart metering use case requirements. The delivery ratio requirement for smart metering application is tightly bound [9]. In order to conclude the chosen communication technology (i.e., LTE, and WSN) the delivery ratio is bounded during simulations and latency values of LTE and WSN are evaluted. The simulated latency results are compared with NIST [9] requirements. If the requirements are satisfied by LTE and WSN, we can conclude that the chosen communication technology can be used in smart meters. Here we wish to evaluate the feasibility of long range WSN communication systems. The reason for choosing long range WSN communication systems is their simpler architectural topology, ease of installation and also to support thousands of devices in a single network. But long range WSN communication systems rather instigate more communication challenges. The communication challenges include heavy coding, low-order modulation, lower data rate and higher channel usage time. The heavy coding and low-order modulation are required so as to combat the signal attenuation in suburban and urban environments. The higher coherence time is due to longer packet and sometimes can be detrimental for multiple access/contention access mechanisms causing collisions in WSN communication systems. Hence it is required to break the longer packet in to several pieces or fragments known as fragmentation. Fragmentation reduces the channel coherence time relatively lowering the packet error rate (PER). Fragmentation also reduces the transmission time per each packet. But fragmentation introduces overhead while preserving the functionality. The impact of the frame check sequence (FCS) size in the proposed fragmentation scheme of the draft IEEE 802.15.4k [10] standard (i.e., low energy critical infrastructure monitoring (LECIM) node) is analyzed in this thesis. The optimal tradeoff between overhead and the undetected errors is evaluated using fragment and packet undetected error probabilities. The energy consumption per bit for the chosen fragment and FCS sizes for different bit error rates is also evaluated in the last part of the thesis.

This thesis is organized as follows: Chapter 1 gives introduction to smart grids and the thesis problem formulation, Chapter 2 provides an overview of the third generation partnership project (3GPP) standard LTE architecture [11] used for cellular communication in uplink and downlink directions. The chapter also analyse the LTE communication technology as an potential candidate for the smart meters. Chapter 3 provides an overview on IEEE 802.15.4 standard [12] type WSN. While choosing communication technology (e.g. WSN), the reliability of the sent data is crucial. Chapter 4 discusses the error control or recovery mechanisms, that are used in WSN to mitigate errors that occur in wireless communication channel. Chapter 5 presents the numerical results for average load and delay in smart meters using LTE and WSN technologies. The numerical results signify the feasibility of the communications technologies. Chapter 6 discusses why longer frame structure cannot be used in WSN while handling smart meter traffic. Chapter 6 also details the proposed fragmentation algorithm in the draft IEEE 802.15.4k [10] standard. The impact of fragment and FCS size is studied using undetected error probability. Chapter 7 concludes the importance of the obtained simulation results of LTE and WSN in smart meters along with the fragment and FCS size in the proposed fragmentation scheme of WSN.

2. LONG TERM EVOLUTION OVERVIEW

2.1. Introduction

The 3GPP LTE is the 4th generation mobile technology standard by international telecommunication union (ITU) [11]. It is a successor of the global system for mobile communication (GSM), enhanced data rates for GSM evolution (EDGE), universal mobile telecommunication system (UMTS), and high speed packet access (HSPA) standards. The Table 1 show the evolution of mobile technologies with respect to latency, bandwidth, downlink and uplink speeds.

Table 1. Evolution of mobile communication technologies [13]

Technology	GSM	UMTS	HSPA	LTE
Max downlink speed (bps)	10-150 K	384 K	14 M	100 M
Max uplink speed (bps)	10-150 K	128 K	5.7 M	11 M
Latency (s)	600 ms	150 ms	100 ms	10 ms
Bandwidth (Hz)	200 KHz	5 MHz	5 MHz	1.4 to 20 MHz

From the Table 1, it is evident that performance of LTE is superior compared with previously known communication technologies. The data rate, and latency are some of the key characteristics which makes LTE an excellent candidate for SG use. The LTE has sufficient system capacity to handle smart meter traffic without hindering other devices in the network.

2.2. Architecture of LTE

The architecture of the LTE network is depicted in the Figure 1. It is mainly composed of core network (CN) and radio access network (RAN). The CN consist of evolved packet core (EPC) and service domain. The RAN is composed of user equipment and evolved universal terrestrial radio access (E-UTRAN).

There are two routers present in CN of EPC. The first router called packet data network gateway (P-GW) router which is used to connect the external services. The second router is divided into service gateway (S-GW) and mobility management entity (MME). The S-GW provides data transport service to the eNodeB from the CN. The MME performs the control functions and is connected to the database home subscription server (HSS). The S-GW and P-GW are the core elements in the network architecture and termed as system evolution architecture gateways (SAE GW). The E-UTRAN in RAN is a mesh of evolved NodeB's (eNodeB) which are connected each other using an interface called X2. The user equipment, E-UTRAN and EPC are connected through internet protocol (IP) [14]. Since the network components are connected through IP, thus LTE supports packet switching unlike circuit switching in previous generation mobile communication systems.

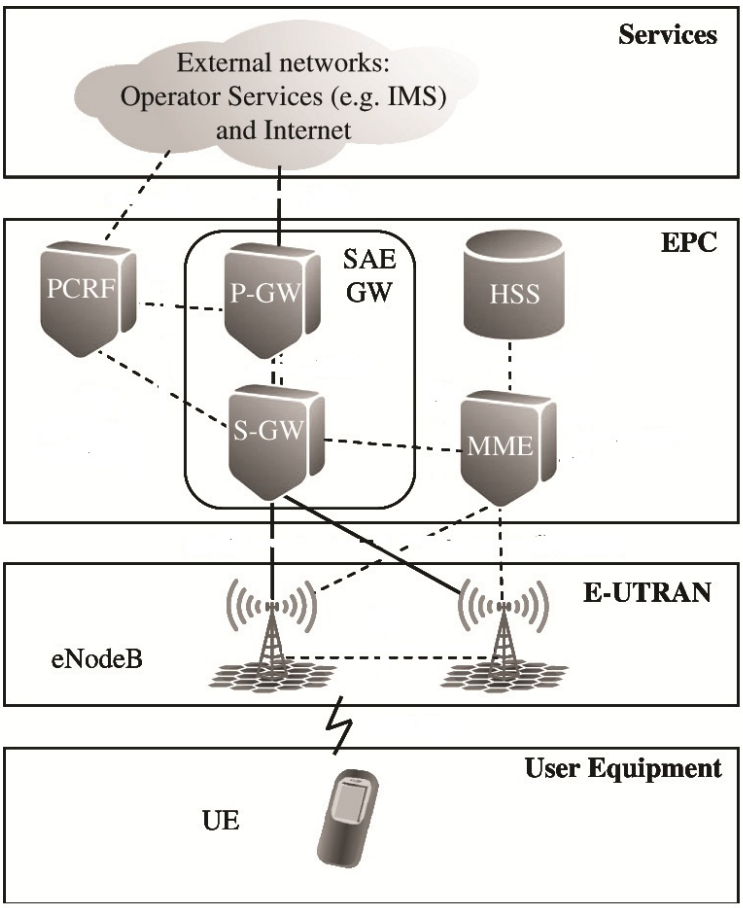

Figure 1. LTE architecture [14].

2.2.1. Functions of each component in the LTE architecture

2.2.1.1. User Equipment

The device used to communicate with the base station is the user equipment. The user equipment contains universal subscriber identity module (USIM). USIM is a separate module inserted into a removable smart card of UE called the universal integrated circuit card. USIM is used to authenticate and derive security keys for accessing the radio interface transmission. The main functions of user equipment are setting up the network and maintaining the communication link with the base station.

2.2.1.2. evolved Node B

The evolved Node B (eNodeB) is the radio base station that control radio related functions in the fixed part of LTE system. The main functions of the eNodeB are:

- It acts as a termination point for all the radio related protocols towards the UE.

- It is responsible for control plane functions, radio resource management (RRM) (e.g., allocating resources, maintaining quality of service (QOS), and monitoring usage of resources).
- It plays an important role in mobility management (MM). eNodeB performs the required signal level measurements to handover the UE's inbetween cells.

2.2.1.3. Mobility Management Entity

Mobility management entity (MME) is control element of EPC. It is used only in control plane. The main functions of MME are

- Authentication and security: MME performs the authentication procedure whenever the user equipment registers for the first time. A detailed authentication procedure named 'EPS-AKA' is presented in [15]. The MME initiates the authentication procedure when needed or periodically. The MME also assigns each UE a temporary identity called global unique temporary identity (GUTI). GUTI reduces the transmission of permanent UE identity (i.e., international mobile subscriber identity (IMSI)) over the radio interface to protect user equipment's privacy.
- Mobility management: The MMEs keep track of the user equipment location and its service areas. MME requests the appropriate resources to be setup from the eNodeB and S-GW for the UE. MME also participates in control signalling for handover of UE between the eNodeBs and S-GWs.
- Managing profile subscription and service connectivity: Whenever a UE registers to the network, MME automatically sets up a default bearer providing the basic IP connectivity to UE. Then MME retrieves the subscription profile from the home network. The subscription profile details the packet data network connections that are needed to be allocated to the user equipment.

2.2.1.4. Packet Data Network Gateway

Packet data network gateway (P-GW) is a router between the evolved packet system (EPS) and external packet data networks. The EPS comprises of EPC, E-UTRAN and user equipment. P-GW assigns the IP address to the UE using the dynamic host configuration protocol (DHCP). The user plane traffic between P-GW and external networks is in the form of IP packets. The P-GW also controls the user plane tunnel data delivery in the uplink and downlink of S-GW.

2.2.1.5. Serving Gateway

The main functions of the serving gateway (S-GW) are user plane tunnel management and switching. A tunnel is created between P-GW and eNodeB when UE is connected

to the network. Tunnel management of S-GW refers to swapping the tunnel connection from one eNodeB to another eNodeB during the UE mobility. The S-GW also sets up, clear, or modifies bearers for the UE based on the requests from MME, P-GW, and policy and charging resource function (PCRF).

2.2.1.6. Home Subscription Server

Home subscription server (HSS) is the subscription data repository of all permanent users (subscribers). The subscriber profile is stored in HSS. The subsequent authentication keys derived from permanent user key used for user authentication are stored in authentication center (AuC) which is a part of the HSS.

2.2.1.7. Services Domain

The service domain offer different kinds of services (e.g., web browsing, voice, and data streaming) to various subsystems in LTE. There are mainly three categories of services offered in the service domain. The offered services in the service domain are

- IP based multimedia services (IMS): The IMS based services are offered in the LTE network with session initiation protocol (SIP). The more details of the IMS architecture is defined in [16].
- Non-IMS based operator services (Non-IMS): The architecture for Non-IMS based services is not defined by the 3GPP. A server can be attached to the network via some agreed protocol that is supported by an application in the UE (e.g., video streaming).
- Other services: The other services include (e.g., services offered through internet) are not provided by the mobile operator. The architecture depends on the offered service. The architecture for providing other services is not addressed in 3GPP.

2.3. Downlink communication

The RAN of the LTE architecture in the downlink communication uses orthogonal frequency division multiplexing access (OFDMA). OFDMA is also used in other radio communication systems (e.g., worldwide interoperability for microwave access (WIMAX) [17], digital video broadcasting (DVB) [18]). OFDMA is multi user channel access technique based on the OFDM. The OFDM approach was first proposed by R.W.Chang [19]. The basic principle of OFDM is to divide the available spectrum into parallel narrowband channels referred as subcarriers and transmit information on these parallel channels at a reduced signaling rate [20].

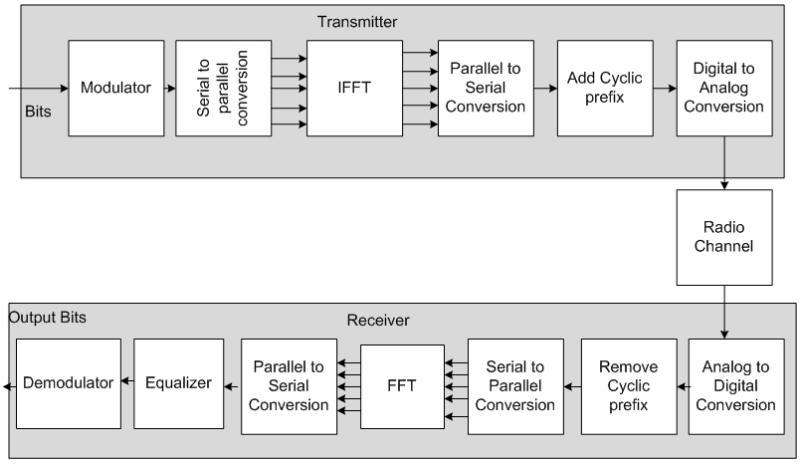

Figure 2. OFDM transmitter and receiver block diagram [20].

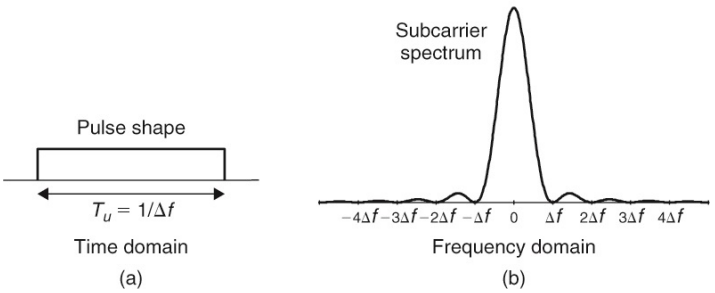

Figure 3. (a) Pulse shape in time domain. (b) Single subcarrier spectrum in frequency domain. [21].

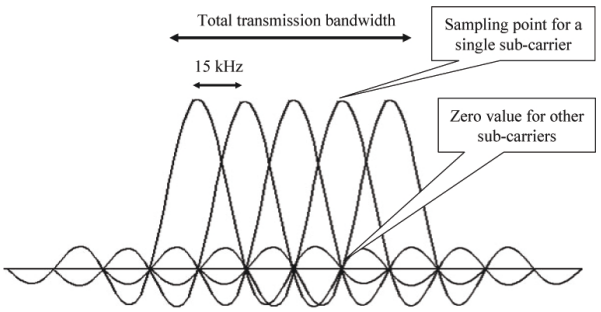

Figure 4. OFDM transmission [14].

The Figure 2 shows the block diagram of OFDM transmitter and receiver used in RAN of LTE downlink system. At the transmitter in Figure 2, the data bits are firstly modulated either using quadrature amplitude modulation (QAM) or phase shift keying (PSK) and are then converted to parallel data streams through demultiplexing. The parallel data streams are mapped to different subcarriers. The shape of a single sub-carrier in time domain and spectrum in frequency domain is shown in Figure 3. LTE

comprises maximum of 2048 subcarriers in the available bandwidth with spacing of 15 KHz within each other. The placing of subcarriers in an OFDM transmission with spacing of 15 KHZ is shown in Figure 4. The subcarriers are made orthogonal using fast fourier transform (FFT) technique. The FFT converts the signal from time domain to frequency domain. The parallel data streams which are obtained after modulation are subjected to inverse FFT. The output of IFFT is the sum of signal samples. Cyclic prefix (CP) is added to the IFFT output symbols to avoid inter symbol interference (ISI). The addition of CP refers to prefixing symbols with a copy of the end of the symbol as shown in Figure 5. CP also helps to preserve the orthogonality between subcarriers. The CP added output symbols from IFFT are then converted to analog and transmitted to the receiver.

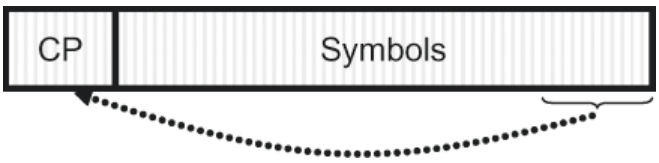

Figure 5. Cyclic Prefix [22].

At the receiver, the analog signal is converted back to digital form and CP is removed. The digital signal is then subjected to FFT which reverses the effect of IFFT at the transmitter. The output signal is equalized. The main purpose of equalization is to avoid ISI during signal transmission. The equalized symbols are then demodulated back in to output as bits.

OFDM baseband signal can be represented by:

$$s(t) = \sum_{k=0}^{N-1} X(k) * e^{j2\Pi k\Delta ft}, \tag{2.1}$$

where *s(t)* is the time domain representation of OFDM signal, *N* represents the number of subcarriers, *X(k)* is the kth subcarrier, Δf is the subcarrier spacing and *t* is time in seconds.

2.4. Uplink communication

The uplink communication in the 3GPP LTE standard [11] occurs from user equipment to the eNodeB. Single carrier- frequency division multiple access (SC-FDMA) is the modulation technique used in uplink communication. Due to high peak to average power ratio (PAPR) caused by OFDM signals in downlink communication of LTE, SC-FDMA is selected for the uplink communication. The block diagram of SC-FDMA transmitter and receiver is presented in Figure 6.

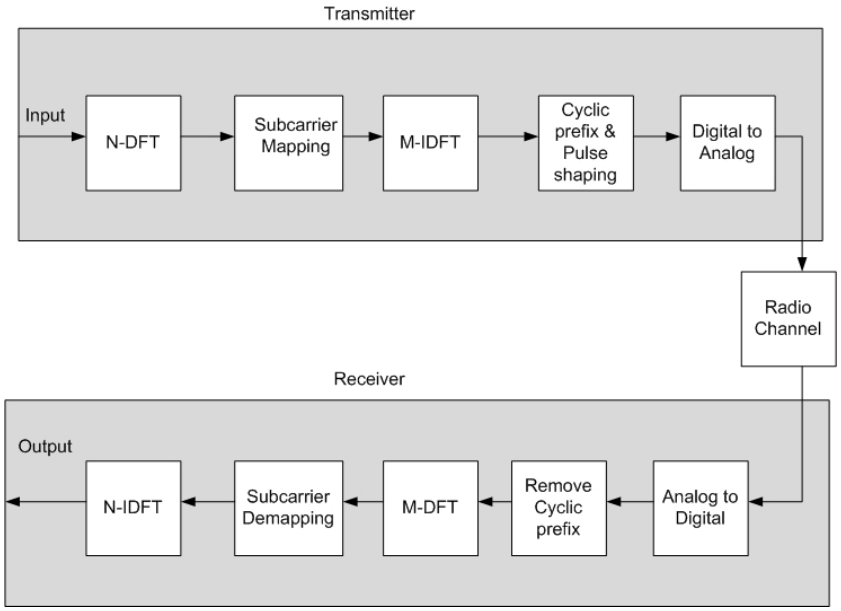

Figure 6. SC-FDMA transmitter and receiver block diagram [22].

At the transmitter, the input data bits are modulated before performing N-point discrete fourier transform (DFT). The common modulation schemes used are quadrature phase shift keying (QPSK), binary phase shift keying (BPSK), 16-ary QAM, and 64-QAM. The modulation scheme is chosen, depending on the radio channel. The modulated data symbols are then converted into N parallel data streams. Then N-point DFT is performed on the parallel streams. DFT converts the time domain modulated symbols to frequency domain symbols. The obtained N output frequency domain symbols are mapped to M orthogonal subcarriers, where M is an integer multiple of l. M can be represented as $M=l*Q$ where Q is the bandwidth expansion factor or the maximum number of users that can be supported in the system For example, if there are l = 64 output frequency domain symbols and M= 256 orthogonal subcarriers then Q = 4 users can be supported. After the subcarrier mapping, the complex frequency domain symbols are converted back to time domain signals using inverse DFT (IDFT). Cyclic prefix (CP) is then added to time domain signal to avoid inter symbol interference (ISI) similar to downlink communication. CP also helps to maintain the periodicity of the signal. To maintain the desired spectrum at the receiver pulse shaping is performed at the transmitter. The pulse shaped signal is converted to analog signal using digital to analog (D/A) converter. The analog signal is transmitted to the receiver through the radio channel.

At the receiver, the analog signal is converted back to digital form using analog to digital (A/D) converter followed by CP removal. The time domain signal is converted to frequency domain symbols. The subcarrier demapping is performed. Once the subcarrier demapping is done the symbols are subjected to frequency domain equalization. The most commonly used equalizer is the minimum mean square error (MMSE) frequency domain equalizer. The frequency domain equalized signal is then converted to time domain using IDFT. The output symbols are finally demodulated to data bits.

2.5. Challenges for implementing LTE in smart meters

The implementation of LTE in smart meters pose many research challenges. Some of the key challenges are:

- Flexible architecture approach: The network architecture should be designed highly flexible. The devices should have the ability to connect to a aggregation point (AP) (e.g., direct and indirect method) or among themselves (e.g., Ad-hoc). The direct and indirect architectures used in smart meters [23] while using LTE are shown in Figure 7. In direct method shown in Figure 7 a), the smart meter has the broadband access module along with the device and they communicate directly with the base station. Relay nodes are used to extend the coverage area.

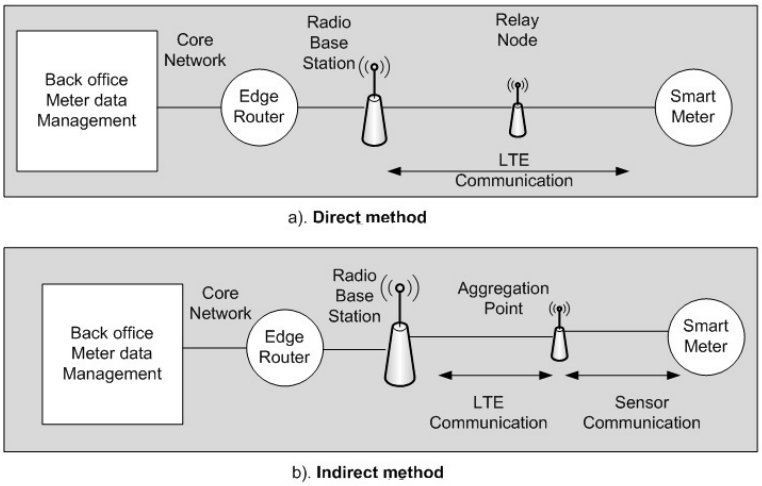

Figure 7. LTE Architectures for smart metering [23].

In indirect method shown in Figure 7 b), the smart meter communicates with the AP and then AP communicates with the base station. In this thesis for evaluating LTE in smart meters, direct communication architecture is considered. The average load and delay posed by the smart meter traffic when smart meters use LTE is discussed in Section 5.1.3.

- Congestion control: As there would be a major increase in the usage of LTE the eventuality of congestion may also increase. The feasibility study of the smart meter traffic without hindering LTE background applications is studied in Section 5.3. The congestion in the LTE traffic when used in smart meters can happen at:
  - Radio network part: As there is increase in the number of UE's, the usage of same channels by different UE's can cause collisions.
  - EPC network part: The another bottleneck in the network architecture is in the core devices, which communicate with the radio network access part.

The components (e.g., MME, S-GW and P-GW) are responsible for attachment of UE's and will send, and receive traffic simultaneously causing congestion to the network.

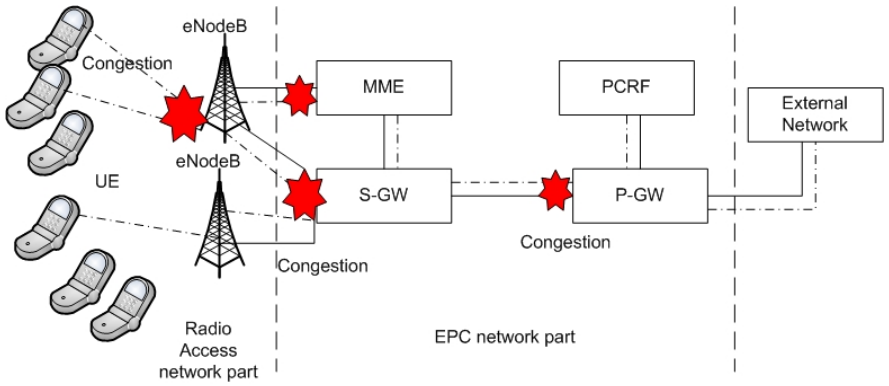

Figure 8. Congestion in LTE network architecture.

- Traffic scheduling: Smart meters connect (or reconnect) to the wireless broadband network (i.e., LTE) during the exchange of information. The traffic generated by smart meters is generally regarded to be periodic. Hence, the traffic generated by the smart meters by connecting and reconnecting for specific instances of time is called time controlled traffic. Smart meters are connected only for a specific duration in time controlled operation. The duration of the connected intervals can be configured to be different for each smart meter and can be dynamically adjusted by the network as needed. In scenarios related to critical alarm indication, data from the smart meter should be reported immediately and not be queued until the next scheduled connected period. Therefore, within framework of time controlled operation, the smart meters shall be allowed to send messages outside its assigned interval and the system should allow for such unscheduled transactions to be processed.

3. SURVEY ON IEEE 802.15.4 STANDARD WIRELESS SENSOR NETWORKS

3.1. Introduction

A wireless sensor network (WSN) is a collection of nodes which have the ability of actuation, sensing, computing and communication. Sensor nodes in WSN communicate through wireless channels in real time providing information to utility and the end users. There are two types of nodes defined by the IEEE 802.15.4 [12] standard type WSN. They are full-function device (FFD) and reduced-function device (RFD). FFD is a node which can operate as personal area network (PAN) coordinator, or as an end node but RFD operates only as end node. Sensor networks have architectures of star, peer to peer, mesh and cluster tree. The star and peer to peer topologies are the most commonly used, and are shown in Figure 9.

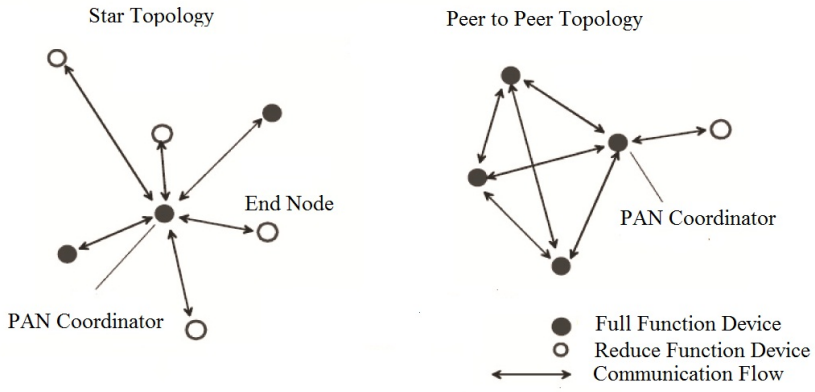

Figure 9. Star, and Peer to Peer Topology for IEEE 802.15.4 type WSN [12].

Communication between the nodes in a star topology is established using single central controller known as personal area network (PAN) coordinator. All the devices connected in the network will use unique address or an extended address which is assigned by the PAN coordinator. Other nodes in the network can communicate through the PAN coordinator. In peer to peer network topology, any node can communicate with any other node as long as they are in range of one another. An example of peer to peer communication topology is cluster tree network topology. In cluster tree network topology all the devices are FFDs. An RFD can connect to a cluster tree network as a leaf node at the end of a branch because RFDs do not allow other devices to associate.

In IEEE 802.15.4 [12] standard, the architecture of sensor node is defined in terms of blocks called layers. Each layer is part of the IEEE 802.15.4 [12] standard. They are physical, MAC and upper layers. In this chapter, the functionalities of the physical and MAC layer are studied with respect to the standard 802.15.4 [12]. The physical layer consist of radio frequency (RF) transceiver with low level control mechanism and provides mainly two kinds of services, PHY data and management service at service access points (SAPs). The physical layer is connected to MAC layer using the physical data service access point (PD-SAP) and physical layer management entity (PLME)

SAP. The MAC also has MAC data and MAC management service. The MAC layer is connected similarly to upper layers using MAC sublayer management entity (MLME) and MAC common part sublayer (MCPS) SAP.

3.2. Physical layer (PHY)

The requirements of physical layer in a sensor node can be mainly classified in to communication aspect requirements and practical hardware implementation possibilities [24]. The communication requirements specify that the radio technology used should be containable in a device, cheap and communicate effectively with upper layers using minimum power levels. The radio technology should also be interference limited as sensor nodes are densely deployed in WSN. The IEEE 802.15.4 [12] specify the frame formats and PHY profiles that can be used in physical layer of sensor nodes.

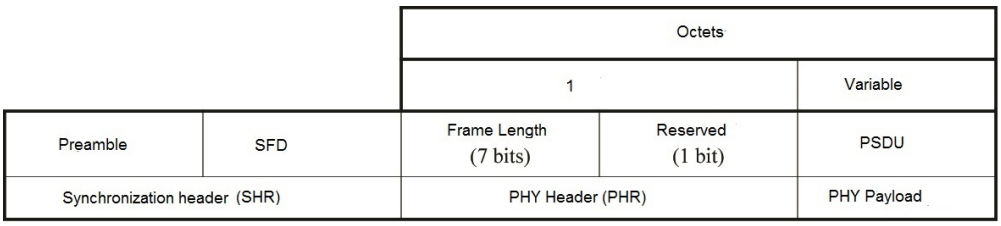

Figure 10. Physical Layer Protocol Data Unit of IEEE 802.15.4 Sensor Networks [12].

With respect to frame format, the data transmission and reception in the physical layer of sensor node occurs through physical layer protocol data units (PPDU). The generic frame format of PPDU specified by 802.15.4 [12] standard is shown in Figure 10. The PPDU consist of synchronization header (SHR) which is used to synchronize and lock on to bit stream, PHY header (PHR) which contains the frame length information, and a variable length payload which carries the MAC sublayer frame. The SHR is composed of preamble and start frame delimiter (SFD). The PHR consist of frame length and reserved field. The PSDU field is of variable length ranging from 1 to 128 and 129 to 2048 Bytes depending on the PHY profile [12] and it contains the data of the PHY packet.

- Preamble field - The preamble field is used by transceiver to obtain chip and symbol synchronization with an incoming message.
- SFD field - The SFD field indicates the end of SHR and start of packet data.
- Frame Length field - The frame length field specifies the total number of octets contained in the Physical layer service data unit (PSDU). The value ranges from 0 to *aMaxPHYPacketSize* (127 octets [12], 2048 in [10] and [25]).
- PSDU field - The PSDU field carries the data of the PPDU.

The IEEE 802.15.4 [12] standard specifies the PHY profiles that can be used in the physical layer of sensor nodes. Some of the generic PHY profiles supported by

IEEE 802.15.4 [12] standard are offset phase shift keying (O-QPSK), binary phase shift keying (BPSK), and amplitude shift keying (ASK). The PHY profiles specific to 802.15.4k [10] LECIM standard are direct sequence spread spectrum (DSSS) and frequency shift keying (FSK). Different PHY profiles result in different bit rate and symbol rate performances. The different PHY alternative profiles with their respective bit rate and symbol rates are shown in Table 2.

Table 2. Data rates and bit rates in PHY alternatives of 802.15.4 [12] standard

PHY Profile Modulation	Frequency Band (MHz)	Bit Rate (Kb/s)	Symbol Rate (Ksymbol/s)
BPSK	902-908	40	40
ASK	902-908	250	50
O-QPSK	902-908	250	62.5
FSK	917 -923.5	12.5	12.5
CSS	2400-2483.5	250	166.6
O-QPSK	2450 DSSS	250	62.5

Smart metering devices are mainly characterised by large path loss, minimal infrastructure requirements, and low energy. These requirements must be satisfied while considering the PHY profile. The generic requirements for choosing PHY profile are data rate, bandwidth efficiency, error performance and design complexity with less interference. In general, IEEE 802.15.4 [12] standard supports BPSK, OQPSK, ASK, and CSS PHY profiles. In this thesis, we focus on low energy critical infrastructure monitoring (LECIM) network application (i.e., smart metering). DSSS and FSK PHY profiles are mainly designed for LECIM applications (e.g., smart metering). The DSSS PHY profile data rate is band and region specific. DSSS PHY uses different frequency bands in different countries [10]. The DSSS PHY profile uses either BPSK or OQPSK modulation depending the *phyLECIMDSSSPPDUModulation* [10]. The FSK PHY profile uses narrow bandwidth with low data rate devices to enable high sensitivities for reduction in the possibility of collisions. The performance of the chosen PHY profile transmission decides the signal level, and the modulation scheme (i.e.,constellation mapping and encoding).

3.3. 802.15.4 MAC layer Family

Introduction

The layer above the PHY is MAC sublayer. The generic requirements of MAC layer are framing, medium access, reliability, flow control, and error control. The main functions of the MAC layer specified by IEEE 802.15.4 [12] are generating network beacons if the node is a coordinator, synchronizing to the network beacons, supporting PAN association and disassociation, device security and employing carrier sense multiple access - collision avoidance (CSMA-CA) mechanism for channel access. The generic frame format in MAC layer is shown in Figure 11 along with the description of the fields.

<table>
<tr><td>Octets:
1/2</td><td>0/1</td><td>0/2</td><td>0/1/2/8</td><td>0/2</td><td>0/1/2/8</td><td>0/1/5/6/1
0/14</td><td colspan="2">variable</td><td>variable</td><td>2</td></tr>
<tr><td rowspan="2">Frame Control</td><td rowspan="2">Sequence Number</td><td>Destination PAN Identifier</td><td>Destination Address</td><td>Source PAN Identifier</td><td>Source Address</td><td rowspan="2">Auxiliary Security Header</td><td colspan="2">Information Elements</td><td rowspan="2">Frame Payload</td><td rowspan="2">FCS</td></tr>
<tr><td colspan="4">Addressing fields</td><td>Header IEs</td><td>Payload IEs</td></tr>
<tr><td colspan="7">MAC Header - MHR</td><td colspan="2">MAC Payload</td><td>MFR</td></tr>
</table>

Figure 11. MAC Frame Format of IEEE 802.15.4 Sensor Networks [12].

- MAC Header (MHR)
  - Frame control - The frame control contains information defining the frame type, addressing fields and control flags.
  - Sequence number - The sequence number field specifies the sequence identifier of the frame.
  - Destination PAN identifier - The destination PAN identifier specifies the unique PAN identifier of the receipt of the frame. A value of 0xffff in this field shall represent the broadcast PAN identifier.
  - Destination address - The destination address field specifies address of the intended recipient of the frame. A value of 0xffff will be accepted by all the devices listening to the channel.
  - Source PAN identifier - The source PAN identifier specifies the unique PAN identifier of the originator of the frame.
  - Source address - The source address field specifies the address of the originator of the frame.
  - Auxiliary security header - The auxiliary security header specifies the information required for security processing.
  - Header information element - Header information element consist of length field, element ID and type. The type field is set to zero for header information element.
- MAC payload
  - Frame payload - The frame payload contains the information specific to individual frame types. The individual frame formats used in the 802.15.4 [12] MAC layer are beacon frame, data frame, acknowledgement frame, and command frame. The payload data constitutes the data of the specific frame format used.
  - Payload information element - The payload information element consist of length field, group id and type field. The type field is set to one for payload information element.
- MAC Footer (MFR)

– FCS - The frame check sequence (FCS) field contains the 16-bit ITU-T cyclic redundancy check (CRC). The FCS is calculated for both MHR and MAC payload. The evaluation of CRC code is detailed in Section 4.1.1.

The IEEE 802.15.4 MAC supports two modes of operation. They are beacon-enabled mode and nonbeacon-enabled mode. PANs that wish to use the superframe structure are referred to beacon-enabled PANs otherwise called as nonbeacon-enabled PANs. The frame format of the superframe structure is defined by the PAN coordinator.

3.3.1. Superframe structure

The structure of superframe is shown in Figure 12. The superframe structure consist of beacon, active and optional inactive portions. The active portion consist of contention access period (CAP) and optional contention free period (CFP). In CFP the node may request the PAN coordinator to allocate guaranteed time slots (GTS). In the inactive period coordinator can enter into sleep mode.

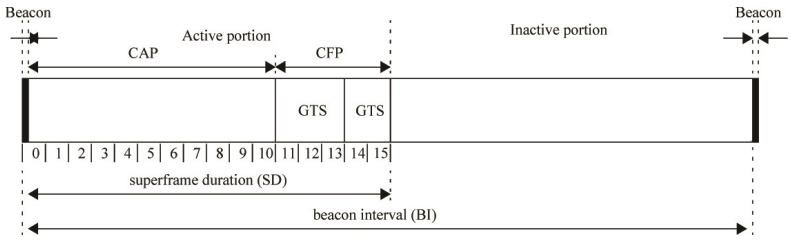

Figure 12. Superframe Structure of IEEE 802.15.4 Sensor Networks [12].

The structure of the superframe is characterized by *beacon interval (BI)* and *superframe duration (SD)*. The *BI* specifies the time between two consecutive beacons. The *SD* corresponds to the active period in the superframe structure. The *BI* and *SD* are defined by

$$\begin{aligned} BI &= aBaseSuperframeDuration * 2^{BO} \\ SD &= aBaseSuperframeDuration * 2^{SO} \end{aligned} \tag{3.1}$$

where beacon order (BO) and superframe order (SO) are *macBeacondOrder* and *macSuperframeOrder* respectively. In a beacon enabled PAN, the *macBeaconOrder* and *macSuperframeOrder* ranges from 0 to 14. If both *macBeacondOrder* and *macSuperframeOrder* equals to 15, coordinator will not transmit beacon frames, and hence referred as nonbeacon enabled PANs.

3.3.2. CSMA-CA algorithm

Sensor nodes use CSMA-CA algorithm for accessing the channel. The CSMA-CA algorithm is used during the CAP of the superframe structure before the transmission of

data or MAC command frames. During the transmission of beacon frames, acknowledgement frames and data, CSMA-CA is not employed.

If beacon enabled mode is used by PAN, the CSMA-CA algorithm is slotted i.e., the backoff period boundaries of every device in the PAN are aligned with the superframe boundaries of the PAN coordinator. In slotted CSMA-CA, node that transmits data frames during the CAP shall first locate the boundary of the next backoff period. If non-beacon enabled mode is used or a beacon cannot be located in a beacon enabled network, unslotted CSMA-CA algorithm is used. In unslotted CSMA-CA, the backoff periods of one device are not synchronized with any other device backoff period in the PAN. But, both slotted and unslotted CSMA-CA algorithms use units of time called backoff periods, which is *aUnitBackoffPeriod* equal to 20 symbols.

There are three main variables used by CSMA-CA algorithm to update for every transmission attempt. They are 1) Number of backoffs (NB), 2) Contention window (CW), and 3) Backoff exponent (BE). NB is the number of times CSMA-CA algorithm was required to backoff. CW is the contention window length defining the number of backoff periods required for the channel to be clear before transmission. CW is used only in slotted CSMA-CA. BE is the number of backoff periods required for a device to wait before attempting to assess the channel. BE enables the computation of backoff delay.

The Figure 13 shows the flow diagram of slotted operation mode of CSMA-CA algorithm.

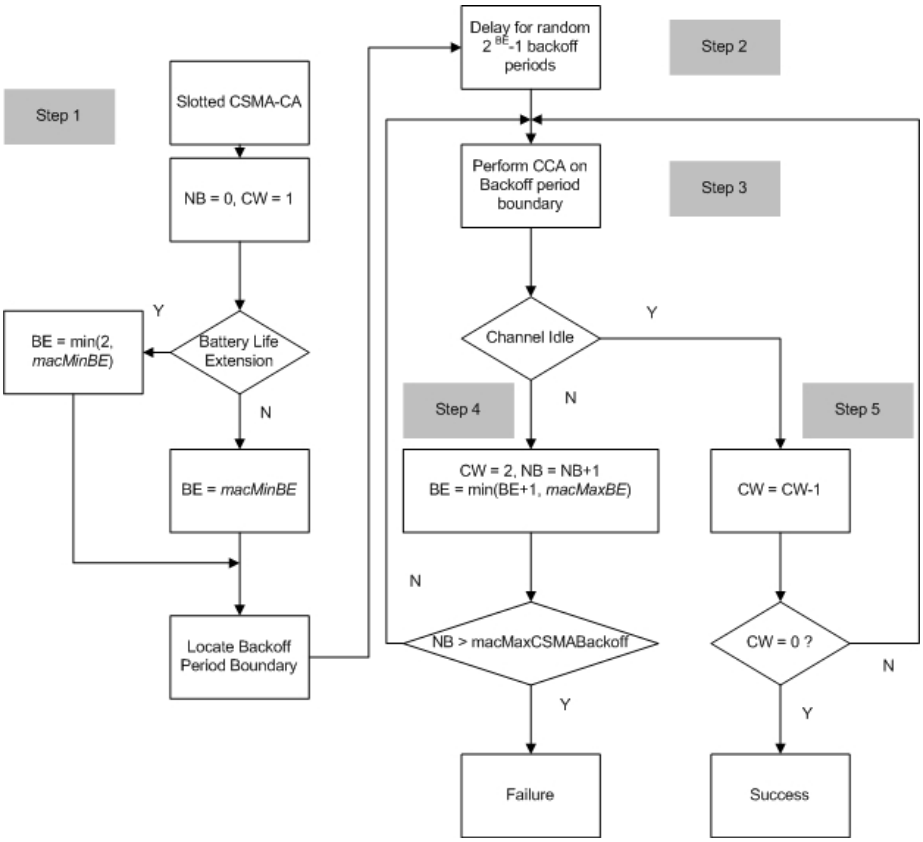

Figure 13. Slotted CSMA-CA algorithm [12].

The slotted CSMA-CA is carried out in the following steps:

- Step 1: NB, BE, and CW variables are initialized. The boundary of the next backoff period is located. The value of BE is decided by the battery life extension (BLE). If BLE is set to zero then BE is initialized to *macMinBE*. If BLE is set to one then BE is initialized to min(2,*macMinBE*).
- Step 2: A Random delay of $2^{BE} - 1$ backoff periods is introduced for each node in the sensor network.
- Step 3: After the random backoff delay, the slotted CSMA-CA shall request the PHY to perform clear channel assessment (CCA). CCA is the ability of the PHY to analyze whether the channel is free for transmission.
- Step 4: If the channel is busy, the MAC sublayer shall increment both NB and BE by a value 1. The algorithm ensures that BE cannot be more than *macMaxBE* with NB not more than *macMaxCSMABackoff*. If NB is more than the *macMaxCSMABackoff*, CSMA-CA algorithm will terminate with channel access failure status.
- Step 5: If the channel assessed is found to be idle, the MAC sublayer would check for the expiration of CW before transmission. If CW is not equal to zero CSMA-CA algorithm returns to CW=CW-1. If it is equal to zero the MAC sublayer shall begin the transmission on the boundary of the next backoff period.

The Figure 14 shows the unslotted operation mode of CSMA-CA algorithm.

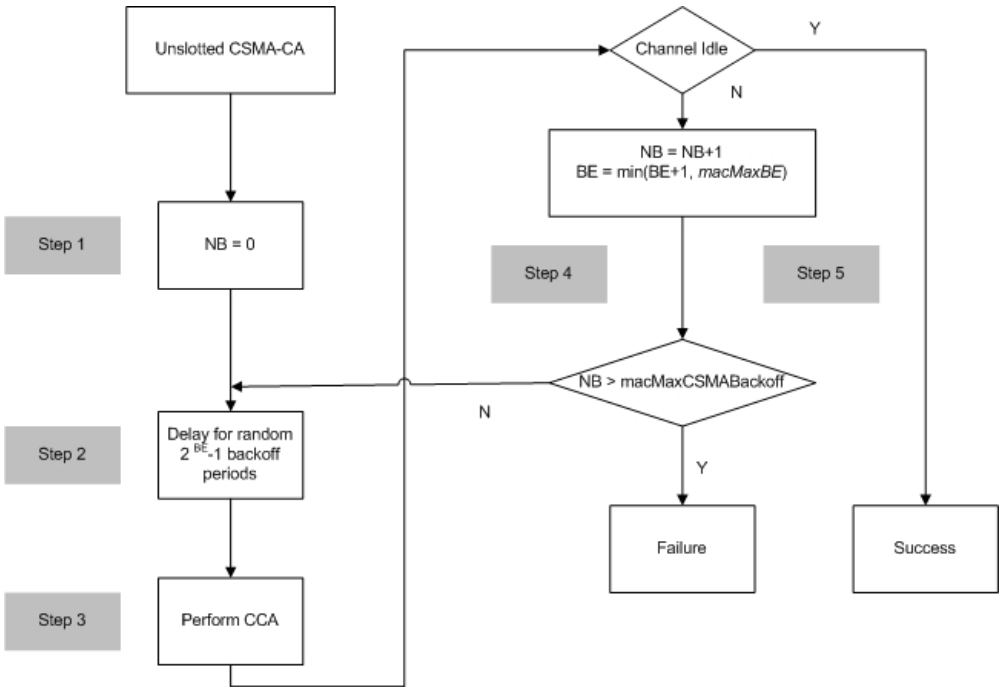

Figure 14. Unslotted CSMA-CA algorithm [12].

The unslotted CSMA-CA algorithm follows the steps:

- Step 1: variable NB is initialized.
- Step 2: The algorithm is delayed for random backoff period value which is equal to $2^{BE} - 1$.
- Step 3: CCA is performed by sending a request to the PHY.
- Step 4: If the channel is idle the data is transmitted.
- Step 5: If the channel is busy, update the variables NB and BE. The algorithm ensures that NB < *macMaxCSMABackoff* and returns to step 2. If NB is greater than *macMaxCSMABackoff* then unslotted CSMA-CA returns with a failure status.

4. ERROR CONTROL ALGORITHMS

4.1. Introduction

In this thesis we wish to study the feasibility of long range IEEE 802.15.4k [10] devices in smart meters. The long range WSN devices suffers from higher signal attenuation and increased channel coherence time. Due to higher channel coherence time and attenuation the bit error rate (BER) and PER is also increased. This chapter provides the background to understand the underlying mechanisms used to overcome the channel pathloss and propagation effects in WSN devices. The mechanisms are known as error control or mitigation algorithms. Error control algorithms are used to detect and correct the transmission errors at the receiver. Error control algorithms [26] are broadly classified in to forward error correction (FEC) and automatic repeat request (ARQ). FEC [27] scheme uses error correcting code to add redundant bits to the original message. When the receiver detects an error in the received bits, it attempts to determine the error locations and corrects the errors using checksum. If the exact locations of the errors are determined the received bits will be correctly decoded. If the receiver fails to determine the exact location of errors, the received bits will be decoded incorrectly. In ARQ [27] system, a code with good error detecting capability is chosen. At the receiver the syndrome vector of the received codeword is computed. The syndrome vector is obtained from the parity check matrix. The parity check matrix is matrix of redundant bits which are chosen to be added to the original message by transmitter. If the syndrome vector is zero the received codeword is assumed to be error free. The receiver notifies the transmitter via a return channel, that the transmitted codeword has been successfully received. If the syndrome vector is not zero, errors are detected in received codeword. Then the transmitter is instructed, through a return channel, to retransmit the same codeword. Retransmission is used to receive the codeword successfully.

There are three kinds of ARQ [27]. They are

- Stop and wait: In stop and wait scheme, transmitter sends a codeword to the receiver and waits for an acknowledgement (ACK) from the receiver. A positive ACK from the receiver signals that the codeword has been successfully received (i.e.,no errors are detected). A negative ACK from the receiver indicates that received vector has been detected in error. The transmitter resends the codeword. Retransmissions occur until positive ACK is received by the transmitter.

- Go back N: In go back N scheme codewords are transmitted continuously. The transmitter does not wait for an ACK after sending the codeword. When there is a negative ACK for the Nth codeword. The transmitter backs up to the codeword that was negatively acknowledged and resend that codeword and the N-1 succeeding codewords.

- Selective repeat: In selective repeat codewords are transmitted continuously. But the retransmission takes only to the negatively acknowledged codewords.

Hybrid ARQ (H-ARQ) is essentially a combination of FEC and ARQ system in an optimal manner [27]. The function of FEC scheme is to reduce the frequency of

retransmission by correcting the error patterns. ARQ is used for retransmitting the corrupt codeword. The H-ARQ scheme combines both. The H-ARQ schemes [28] are further classified into

- Type I, chase combining (CC) [26] - When receiver requests for retransmission, the retransmissions consist of same set of coded bits as the original transmission. In other words the coding technique used in the original transmission will not be altered even for retransmission. In Type I H-ARQ systems, the receiver combines each received codeword with any of the previous transmissions of same codeword to make decoding easy.
- Type II, incremental redundancy (IR) [29] - The retransmissions are not identical to the original transmission. The coded redundant bits are different than the previous transmission. Multiple sets of redundant bits are generated by the transmitter for the same information bits.
- Type III [26] - The type III scheme is similar to incremental redundancy but uses puncturing techniques to create a set of bits. In puncturing some of the parity bits are removed to improve the efficiency of coding. The removed parity bits are known at the receiver.

4.1.1. Error detection

Error detection is performed in ARQ mechanisms using error detecting codes. Some of the examples of error detecting codes are

- Cyclic redundancy check (CRC) codes. In CRC codes, a group of error control bits are appended at the end of the original message. The error control bits are obtained as the result of polynomial division of the original message using the generator polynomial. If the remainder of the polynomial division is zero or some other known preset value at the receiver then the original data message is not corrupted, if not the receiver requests for retransmission.

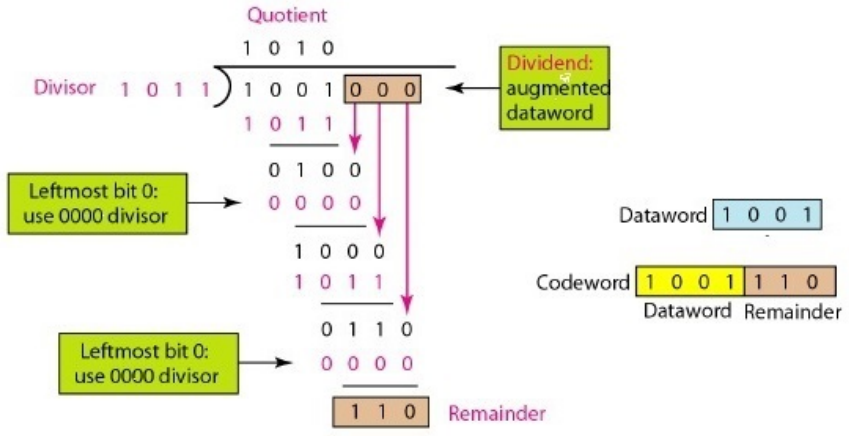

Figure 15. Polynomial Division at transmitter [30].

An example of CRC coding is shown in Figure 15, the dataword "1001" is transmitted. The control bits "110" are obtained by division of the original data message with the predefined generator polynomial "1011". The codeword transmitted is a combination of original message and remainder of the polynomial division. The polynomial division using the same generator polynomial is evaluated at the receiver with the transmitted codeword as shown in Figure 16.

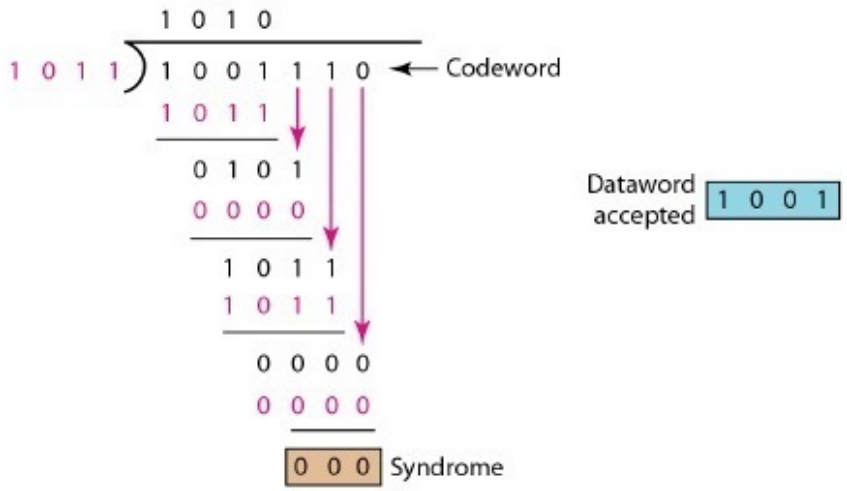

Figure 16. Polynomial Division at Receiver [30].

If the syndrome is zero, the codeword received is not corrupted due to the communication channel. If the reminder is not zero, the receiver discards the received codeword and requests for retransmission. Even if the remainder or syndrome is equal to zero there can be a possibility of error in the received codeword, which is termed as undetected error. Undetected error is used as a performance criteria for evaluating CRC codes. In this thesis to evaluate the appropriate CRC size in MAC frame of IEEE 802.15.4k [10], undetected error probability is used. The section 6.2 details the analysis of undetected error probabilities for 8, 16, 24, and 32 bit generator polynomials of CRC codes.

4.1.2. Error correction

Error correction is performed in FEC using error correcting codes (ECC). ECC are used to correct the errors. ECC are classified mainly into block and convolutional codes. The difference between block and convolutional codes, is the calculation of checksum value which is attached along with the data for protection. In block codes the parity or check bits are calculated only from the information bits but in convolutional codes the parity bits are obtained using the previous information blocks as in Figure 17.

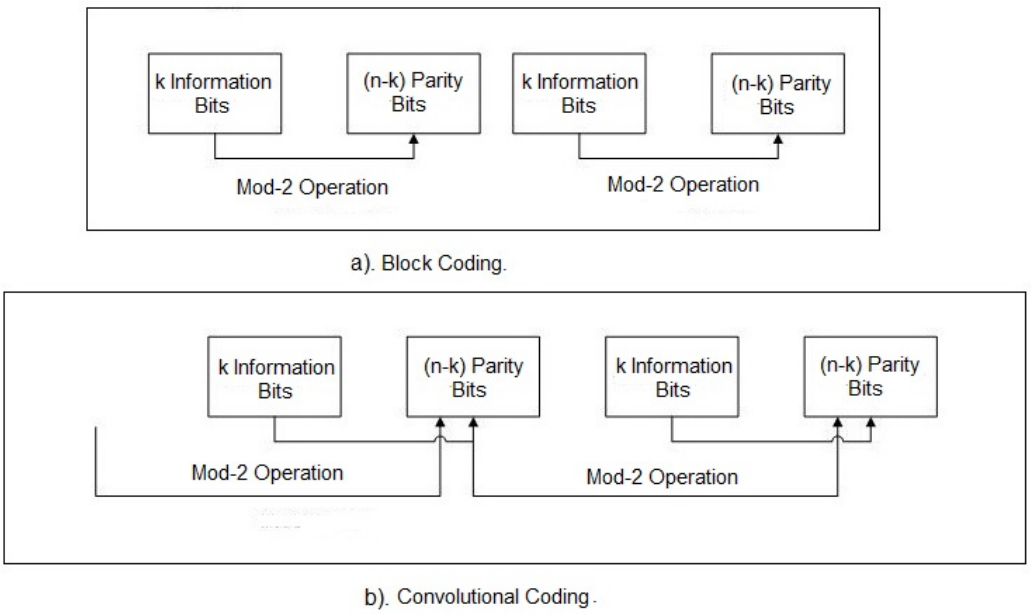

Figure 17. Classification of Error Correction Codes.

4.1.2.1. Block Codes

In block codes, the encoder divides the information sequence into message blocks of k information bits (i.e., symbols) each. Each k information bit or symbol block is treated as the original message. Error correction bits are appended for every block of this message. Some of the examples of block codes are reed solomon (RS) codes, Hamming codes, Hadamard codes, golay codes and reed-muller codes.

4.1.2.2. Reed Solomon codes

Reed Solomon codes are systematic linear block codes developed by Irving Reed and Gustave Solomon [31]. It is called as systematic code, because the original message block codeword is left intact even after encoding and decoding.

RS code is defined as (*n,k*) code, where n represents the block length in symbols and *k* represent the message length in symbols. Symbols can contain *m* bits. The encoder takes *k* symbols where each symbol can contain a maximum of 8 binary bits. The message symbols *k* are represented in Galois Field (GF) polynomial. The message polynomial is multiplied with x^{n-k} to allow space for the parity symbols. The multiplied message polynomial is divided using a code generator polynomial derived from the GF. The remainder is appended to form the transmitted message symbols.

The block length *n* for a given code is given by:

$$n \leq 2^m - 1 \tag{4.1}$$

The number of errors *t* which the code can correct is given by:

$$t_c = \begin{cases} (n-k)/2 & \text{for}(n-k)\text{even} \\ (n-k-1)/2 & \text{for}(n-k)\text{odd} \end{cases} \tag{4.2}$$

RS codes are based on finite fields, called GF. GF consist a set of elements (i.e., numbers) based on the primitive elements usually denoted by α. The primitive elements can take values 0, α^0, α^1, α^2, $\cdots$, α^{N-1}. GF consist of set, which even after addition, subtraction, multiplication and division operations on the elements will not leave the set [32]. The values of the message and parity symbols of RS code are elements of GF. Thus for a code based on m-bit symbols, the GF has 2^m elements. The IEEE 802.15.4 [12] standard uses RS(63,55) code in the MAC layer. To detail out RS(63,55) would be tedious. To understand RS coding easily, a worked out example of RS(15,11) [33] is detailed in this chapter.

Lets take RS(15,11) code, where the block length is 15 symbols. 11 of 15 symbols are information and the remaining are parity symbols. The number of bits in each symbol is obtained using Eq (4.2). So each symbol can consist of maximum 4-bit word and the code is based on the GF with $2^4 = 16$ elements. The field generator polynomial p(x) with no factors for GF(16) is given by:

$$p(x) = x^4 + x + 1 \tag{4.3}$$

In this example, we wish to transmit data message of binary numbers 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 using RS(15,11) coding. The message polynomial in GF is represented by

$$x^{10} + 2x^9 + 3x^8 + 4x^7 + 5x^6 + 6x^5 + 7x^4 + 8x^3 + 9x^2 + 10x + 11 \tag{4.4}$$

The message polynomial is obtained by multiplying the binary message numbers with the polynomial of degree power value 10. The message polynomial is then multiplied with x^4 to allow space for the 4 parity words. Hence the resulting polynomial is given by

$$x^{14} + 2x^{13} + 3x^{12} + 4x^{11} + 5x^{10} + 6x^9 + 7x^8 + 8x^7 + 9x^6 + 10x^5 + 11x^4 \tag{4.5}$$

The code generator polynomial which is used for the evaluating parity bits can be seen from Table 3. The number of errors that can be detected and corrected for RS(15,11) using the Eq (4.2) is 2. The code generator polynomial that can correct two error words requires four consecutive elements of the field as roots [33]. Hence, the code generator polynomial can be given by

$$\begin{aligned} g(x) &= (x+1)(x+2)(x+3)(x+4) \\ &= (x^2+3x+2)(x+4)(x+8) \\ &= (x^3+7x^2+14x+8)(x+8) \\ g(x) &= x^4+15x^3+3x^2+x+12 \end{aligned} \tag{4.6}$$

Using the Table 3 the generator polynomial can be chosen as

$$g(x) = \alpha^0 x^4 + \alpha^{12} x^3 + \alpha^4 x^2 + \alpha^0 x + \alpha^6 \tag{4.7}$$

Table 3. The field elements for GF(16) with $p(x) = x^4 + x + 1$

Index form	Polynomial form	Binary form	Decimal form
0	0	0000	0
α^0	1	0001	1
α^1	α	0010	2
α^2	α^2	0100	4
α^3	α^3	1000	8
α^4	α+1	0011	3
α^5	$\alpha^2 + \alpha$	0110	6
α^6	$\alpha^3 + \alpha^2$	1100	12
α^7	$\alpha^3 + \alpha + 1$	1011	11
α^8	$\alpha^2 + 1$	0101	5
α^9	$\alpha^3 + \alpha$	1010	10
α^{10}	$\alpha^2 + \alpha + 1$	0111	7
α^{11}	$\alpha^3 + \alpha^2 + \alpha$	1110	14
α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$	1111	15
α^{13}	$\alpha^3 + \alpha^2 + 1$	1101	13
α^{14}	$\alpha^3 + 1$	1001	9

The Eq (4.5) shows the message polynomial. The Eq (4.7) is the generator polynomial. The determination of parity bits for the block is calculated using polynomial division. The remainder of the polynomial division is obtained. The reminder polynomial using polynomial division of generator polynomial and the message polynomial can be given by

$$r(x) = 3x^3 + 3x^2 + 12x + 12 \tag{4.8}$$

The encoded polynomial or the transmitted polynomial after RS(15,11) coding can be given as

$$x^{14}+2x^{13}+3x^{12}+4x^{11}+5x^{10}+6x^9+7x^8+8x^7+9x^6+10x^5+11x^4+3x^3+3x^2+12x+12 \tag{4.9}$$

The polynomial derived in Eq (4.9) is the output polynomial at the encoder. In IEEE 802.15.4 [12] standard the systematic RS code is over GF(2^6), RS(63,55) is used for encoding, where 63 represents the block length n in symbols, and 55 represent the message symbols k generated from 330 bits. The primitive and generator polynomial used for encoding the data in IEEE 802.15.4 [12] standard is

$$p(x) = 1 + x + x^6 \tag{4.10}$$

$$g(x) = x^8 + 55x^7 + 61x^6 + 37x^5 + 48x^4 + 47x^3 + 20x^2 + 6x^1 + 22 \tag{4.11}$$

The RS encoded polynomial or the transmitted polynomial derived in Eq (4.9) can be decoded either by berleykamp massey or euclidean algorithm. The general decoder structure for RS code using Berleykamp massey algorithm is shown in Figure 18.

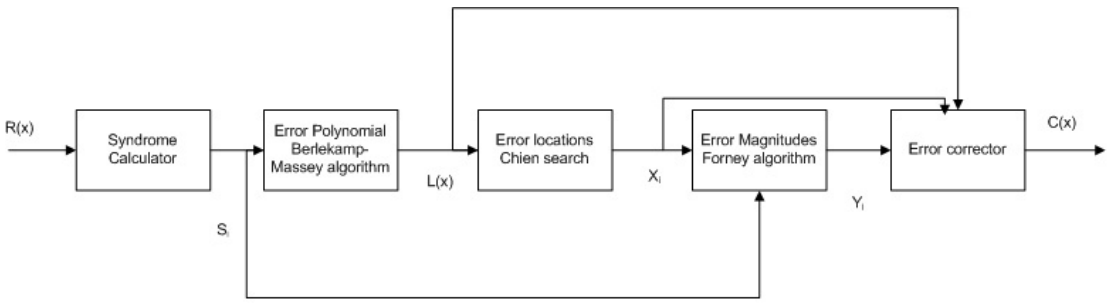

Figure 18. Reed Solomon decoder [33].

In decoding of the RS encoded codeword, the first step is the evaluation of syndrome components. Syndrome calculation is similar to parity evaluation and is calculated for $2t$ syndrome components (i.e., $s_0, s_1, \cdots, s_3$ for RS(15,11) code). If the remainder of the polynomial division is equal to zero for all syndrome components, it can be inferred that the transmitted polynomial shown in Eq (4.9) was not subjected to any errors. Otherwise the error location polynomial is derived using the syndrome polynomial and error evaluation polynomial. The error location location L(x) and syndrome s(x) polynomials are related by

$$L(x)s(x) = W(x)\mathrm{mod}X^{2t}, \tag{4.12}$$

Where syndrome polynomial s(x), error location polynomial L(x), and error evaluation polynomials W(x) are given by

$$\begin{aligned} s(x) &= s_0 + s_1x^1 + s_2x^2 + \cdots + s_{2t-1}x^{2t-1} \\ L(x) &= 1 + L_1x + L_2x^2 + L_3x^3 + \cdots + L_ex^e \\ W(x) &= 1 + W_1x + W_2x^2 + W_3x^3 + \ldots + W_{e-1}x^{e-1}, \end{aligned} \tag{4.13}$$

where e represent the number of errors. The Berleykamp Massey algorithm [34] is used for evaluation of error location and syndrome polynomial. The error locations are obtained using chien search algorithm [35]. The error magnitudes are evaluated using Forney algorithm [36]. The error correction is done by adding the corrupted symbol to correct the error.

4.1.2.3. Convolution codes

Convolution codes are developed by Elias [37]. In block codes *k* information symbols are encoded in to *n* information symbols. But in convolution codes, encoding scheme takes in to consideration of the current and previously sent messages. In order to utilize preceding messages convolution codes use memory element at the encoder. The decoding algorithm of the convolution codes is done using Viterbi algorithm [30].

The generalized convolution encoder consist of input shift register that outputs n_0 binary digits for every k_0 information digits presented at its input. As a block of k_0 digits enter the register, the n_0 modulo-2 adders feed the output register with the n_0 digits and these are shifted out. The code rate is given by $R_c = k_0/n_0$. It is visible that the encoding of n_0 digits not only depend on k_0 but also the previous $(N-1)k_0$ digits which constitutes the memory $\gamma = (N-1)k_0$ of the encoder. Hence the convolution code is represented as (n_0, k_0, N) code. The parameter N denotes the constraint length. To understand the encoding scheme, N submatrices G_1, G_2, ..., G_N containing k_0 rows and n_0 columns. The submatrix G_i describes the connection between the k_0 input register and n_0 output register. In IEEE 802.15.4 [12] standard PPDU is encoded using convolution coding. The code rate is $R_c = 1/2$ which means that $k_0 = 1$ and $n_0 = 2$.

$$\begin{aligned} g_0 &= 010 \\ g_1 &= 101 \end{aligned} \tag{4.14}$$

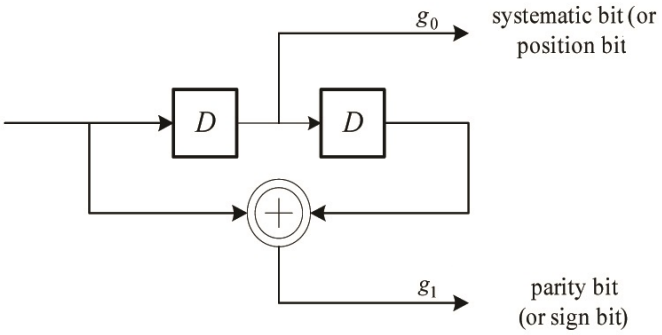

Figure 19. PPDU convolutional encoder [12].

The Figure 19 shows the convolution encoding scheme performed at PHY layer. The transmitted PPDU is encoded using the convolutional encoder with the generator polynomial in Eq (4.15). The generator polynomials represents the connection of memory elements with the modulo-2 adders.

4.1.3. Sensor networks

Sensor networks (IEEE 802.15.4 [10]) can use three kinds of mechanisms for error recovery [38]. They are ARQ, error correction coding (ECC), and HARQ. The basic ARQ protocols, stop-n-wait, goback-N, and selective repeat are also used for higher reliability [27]. ECC uses ARQ with coding for the retransmitted packet during adverse channel conditions. Different coding schemes can be used for sensor networks to overcome errors in wireless communication channels. Some of them include BCH [39], RS codes [40], turbo codes [41]. The error correction capability is obtained in WSN devices at the expense of a high redundancy in the transmitted data and complex decoding circuitry [41].

The IEEE 802.15.4k [10] standard MAC layer fragmentation simulations are performed in Section 6.3. The simulations use ARQ with CRC coding to analyze the fragment and FCS values. The reason to chose ARQ based error mitigation algorithm is to reduce the complexity of the decoding compared to FEC algorithm. The paper [42] discusses the competitiveness of FEC and ARQ algorithm using BCH block coding. It can be inferred from the conclusions of the paper [42] that ARQ outperforms the capabilities of FEC. Hence ARQ is chosen as the error mitigation algorithm in this thesis. ARQ scheme uses an error detection code to determine the corrupted fragment or packet and then retransmit. Here, in the simulations we chose CRC code as error detection code because they do not have built in error correction capability unlike any other block or convolutional coding and are much easy to implement. The WSN devices are also power limited and produce low signal to noise ratio. To overcome these challenges binary linear block codes (i.e., CRC codes) are chosen and are found to be efficient [27] compared to RS, BCH codes in this scenarios. Hence the proposed algorithm in Section 6.3.0.1 uses ARQ based CRC coding to evaluate the undetected error probabilities for each fragment and packet.

5. SIMULATION RESULTS

5.1. LTE Model

In this chapter, the simulation results of smart meters using LTE and WSN in suburban environments are discussed. The simulations are performed in Opnet modeler v16.1 [43]. The simulations show the load and delay profile of smart meter traffic when implemented using LTE. The results show that LTE and WSN can handle smart meter traffic requirements [9] without hindering their respective background applications.

5.1.1. Topology description

The LTE simulations are done in suburban environment. The suburb of Jääli, in Kiminki is chosen as a model for implementing LTE in smart meters. The suburban environment is chosen, as it largely consist of houses instead of apartment buildings or row houses resulting in lower density of remote terminal units (RTU). The total suburb is divided in to clusters as shown in Figure 20. Each cluster dimension roughly about 150m*150m and constitute around 25 smart meters. There are about 30 of such clusters in the area that is contained in space 2.5 km*1.5 km. Therefore the expected number of AMR RTUs to be 750 units in the whole area. The RTUs are randomly placed inside every cluster at the start of the each simulation run. The purpose of the random placement is to let the AMR units to be placed in various locations, not dictated by municipal planning as is usually in real environments. For simulation purpose, it is assumed that each house has one RTU that is connected with an LTE-network eNodeB.

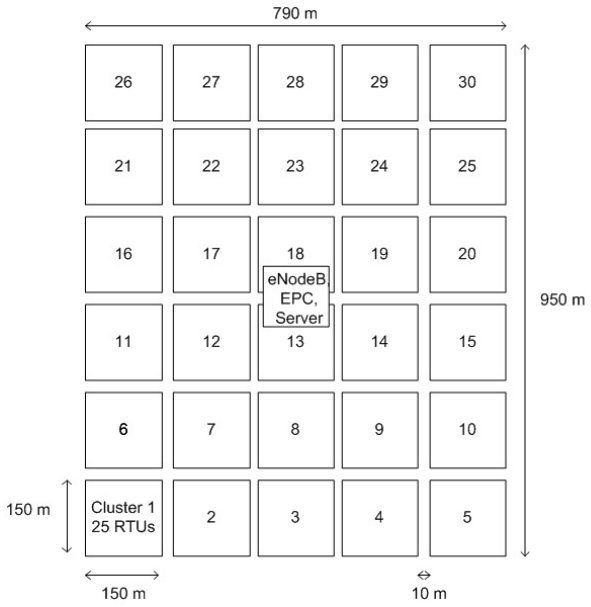

Figure 20. LTE simulation topology.

It is envisioned that a single LTE cell, using 1805-1880 MHz frequency band, could entirely cover Jääli area. The assumption is that all of the RTUs are serviced by a

single LTE carrier. The RF environment chosen will be mostly free space, light trees, and houses being the main obstructions for communications. The simulations are performed independently using LTE. The propagation model for LTE is detailed in Section 5.1.2

The key parameters selected for RTU and eNodeB in LTE simulations are tabulated in Table 4.

Table 4. LTE UE and eNodeB parameters [44]

Parameter	RTU	eNodeB
Tx Antenna gain	-2 dBi	16.5 dBi
Bandwidth	10 MHZ(UL)	10 MHZ(DL)
Transmission power	0.2 W	39.8 W
Receiver sensitivity	-106.5 dBm	-120.7 dBm
Antenna Height	1.5 m	30 m
Base frequency	1800 MHZ	1990 MHZ
QOS class identifier	9(non-GBR)	
RLC mode	Acknowledged	
Maximum number of transmissions	4	
Scheduling mode	Link adapatation and channel dependent scheduling	
Pathloss	Suburban macrocell terrain type C pathloss from obstacles -6 dB *(0,1,2)	

RTUs will take measurements on various sub-bands and calculate separate modulation and coding scheme (MCS) indexes for each subband shown as link adaptation and channel dependent scheduling mode. The eNodeB will try to match the RTUs to their preferred sub-bands, perform link adaptation and create wideband MCS index. If the eNodeB can put the RTU in one of its preferred sub-bands, and if the MCS index of that sub-band is higher than the wideband MCS index, the eNodeB will use the sub-band MCS index and optimise frame resources. The pathloss due to the propagation channel is detailed in Section 5.1.2.

5.1.2. Propagation model

In typical suburban environment pathloss occurs when signal propagates from transmitter to receiver. Radio channel modeling [45] is done in order to evaluate propagation effects. Radio channel modeling can be classified in to narrowband, wideband, and spatial.

In narrowband modeling the radio channel does not consider the delay domain, all the signal components are combined in to single time variant signal. The narrowband models are further classified in to empirical, semi-deterministic and deterministic models. Empirical models are based on measurement data, simple parameters using statistical properties. Commonly known empirical models [46] are Okumura-Hata, and COST231-Hata model for urban and suburban regions. Semi-deterministic narrowband models are based on both empirical and deterministic aspects. Determin-

istic models are site specific and they require enormous amount of geometry and geographical site information e.g., Allsebrrok-parsons, Walfish-Bertoni, and COST231-Walfish/Ikegami models [45].

In wideband modeling each received signal component is separated with respect to delay domain. Each delayed domain constitute single propagation path. The received signal is the sum of the delayed paths. In wideband modeling delay spread, and coherence bandwidth, coherence time are taken in to consideration.

In spatial channel modeling there are more than one transmit and receive antennas. The channel is analyzed for multiple input multiple output (MIMO). The propagation channel model is a matrix with n_t transmit and r_m receive pairs [45].

The channel model for smart meters when deployed in suburban environment is a combination of outdoor propagation loss, indoor propagation loss, and building penetration loss [47]. While considering indoor propagation, the loss can be due to different kinds of obstacles. The respective losses incurred due to common obstructions during indoor propagation can be found from [48]. To model all the incurred losses due to indoor and outdoor propagation can be complicated. So in simulation the modeling of outdoor and indoor propagation is done using predefined channel model [49] and losses caused by external walls during the signal propagation with 6 dB [50] for each wall. The simulations are performed in such a way that radio wave signal can enter a maximum of 3 walls before reaching the end device.

5.1.2.1. LTE propagation model

LTE uses simultaneous data transmission through low rate parallel orthogonal channels. The advantage of using LTE is that all the orthogonal channels face narrow band fading i.e., frequency variable channel appears flat over the narrow band of OFDM subcarrier, eliminating the need of complex equalisation. Hence narrow band radio channel modeling can be used for evaluating the channel propagation effects. One such narrowband empirical model that can be used for evaluating suburban scenarios is suburban macrocell model developed by 3GPP [51] which uses modified COST231 HATA model [49].

The simulator chosen is opnet modeler v16.0, LTE specialized model. Opnet modeler supports the following path loss models for LTE: free space model, suburban fixed, outdoor to indoor, pedestrian Environment, suburban macro cell, urban micro and macro cell. The relevant pathloss model that is chosen in the opnet modeler for simulations is suburban macrocell model. The suburban macrocell model takes in to consideration of outdoor and indoor propagation.The pathloss for the macrocell suburban model [51] is given by:

$$\begin{aligned} PL[dB] &= (44{,}9 - 6{,}55\log10(hbs))log10(d/1000) \\ &\quad +45{,}5 + (35{,}46 - 1{,}1hms)log10(fc) \\ &\quad -13{,}82log10(hbs) + 0{,}7hms + C, \end{aligned} \tag{5.1}$$

where *hbs* is the base station(BS) antenna height in meters, *hms* is the mobile station(MS) antenna height in meters, f_c is the carrier frequency in MHz, *d* is the distance between BS and MS in meters and *C* is a constant factor. The terrain category 'c' is

chosen for the simulations. Pathloss is influenced by the terrain contours. They are three different kinds of terrains contours categorised in suburban environment. They are categories A, B, and C. The category A is the maximum pathloss contour with hilly terrain consisting of moderate to heavy tree densities. The category B is the flat terrain with moderate to heavy tree densities or hilly terrain with light tree densities. The category C is minimum pathloss contour having flat terrain with light tree densities.

5.1.3. Simulation scenarios

The simulation scenarios of LTE simulations consist of:

- Normal AMR traffic generation.
- Background LTE traffic generation.
- Two way normal AMR traffic with LTE background traffic generation.

5.1.3.1. Normal AMR traffic generation scenario

In this simulation scenario, all 750 RTUs transmit AMR traffic to a server located somewhere beyond the evolved packet core (EPC). AMR traffic generation. With total of 750 RTUs, the time taken for one-hour simulation would be excessively high due to the amount of signaling and command traffic. For this reason, only one RTU as shown in Figure 20 is transmitting AMR traffic to server. The volume of traffic is however, the same, as 25 RTUs would generate in total. The Table 5 shows the traffic generation parameters in normal traffic generation scenario.

Table 5. Normal traffic generation parameters

Data type	start time	Interval	Payload	Simulation
AMR data	random 5-20 min	15 min	250 B	1hr

The Figure 21 shows the load of AMR traffic with respect to time. The plot shows the averaged values over 10 simulation runs. The Figure 22 shows the average network delay in ms. Network delay constitutes processing, queueing, transmission and propagation delay. It is found that, throughout the simulations the averaged network delay is below 20 ms without considering background traffic. From the graphs it can be deduced that smart metering traffic has very little effect on eNodeB, and it can be stated that average network delay and traffic load parameters for smart metering are well satisfied according to the NIST requirements [9].

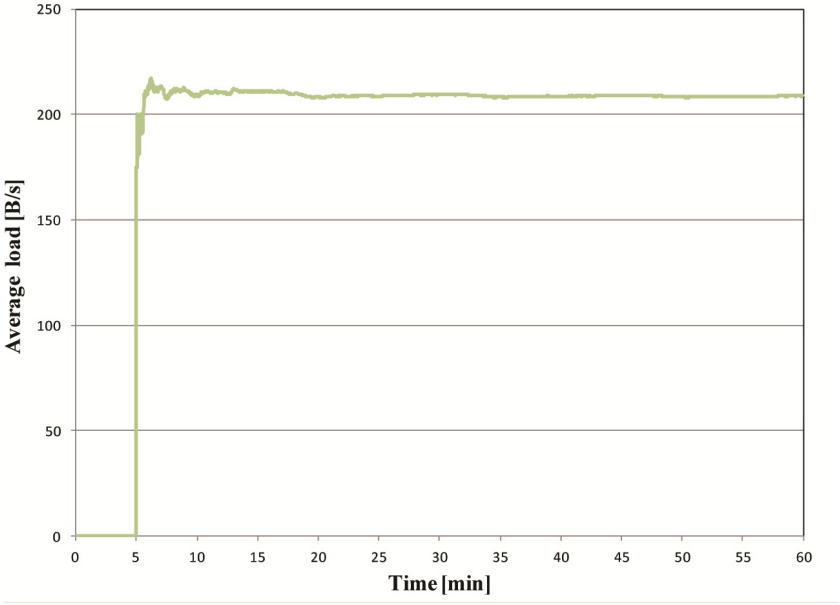

Figure 21. Average load of AMR normal traffic.

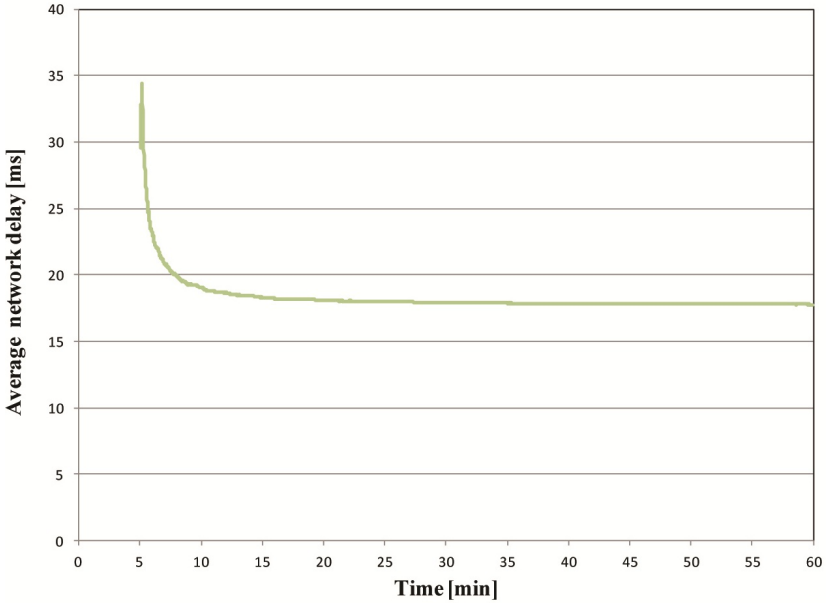

Figure 22. Average delay of AMR normal traffic.

5.1.3.2. Background traffic generation scenario

The typical traffic present in LTE is known as background traffic (BG). The background applications that generate background traffic in LTE constitute voice, video, streaming, web, file transfer protocol (FTP) and data usage [14]. For simulations, the applications are chosen with parameters specified in Table 6

Table 6. LTE background traffic generation parameters

Parameter (per subscriber)	Session Length/size	Simulation time
Voice	2.5 min	
Video	0.05 min	Total time
Streaming	1 min	60 min with
Web	2 pages	5 min network
FTP	2914 kB	initialization
Data usage	5 MB/hr	

The average network load and network delay for the chosen background applications in LTE are shown in the subsequent graph plots. These application types are selected such that the amount of the traffic corresponds to 55 min simulation time because five first minutes of the simulation is reserved for the network initialization, i.e., during the five first minutes there is not any BG traffic generation.

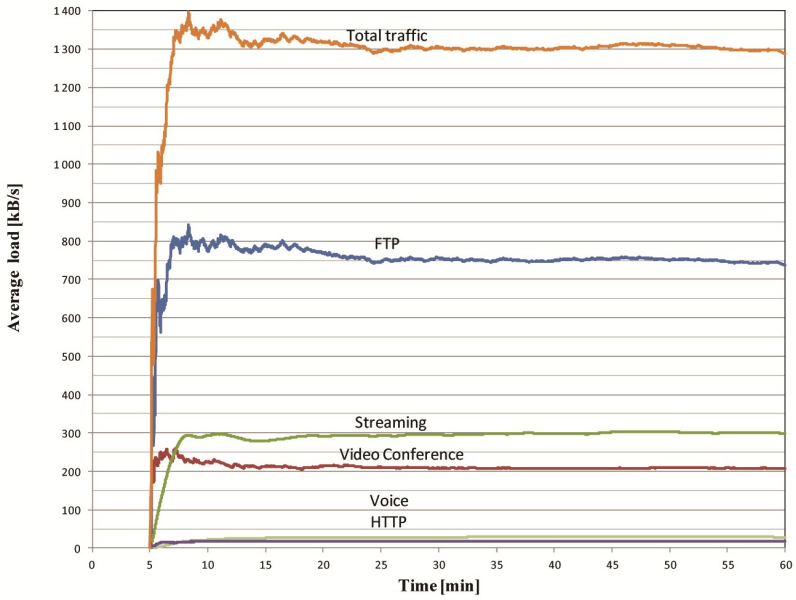

Figure 23. Average load of LTE background traffic generation scenario.

The Figure 23 shows the average load of the BG traffic applications in LTE as a function of time. FTP produces the maximum traffic of 750 kB/s, streaming produces 300 kB/s, Voice with 30 kB/s and hypertext transfer protocol (HTTP) bit less than 20 kB/s. The Figure 24 signify the average network delay caused in the network as a function of time. The network delay for FTP is exponentially increasing to 100 seconds while delay due to voice and video conference equals 0.1 s. The background applications in LTE can be mainly classified in to two main categories. They are guaranteed bit rate (GBR) and Non-GBR. The requirements for the GBR and Non-GBR are specified in the Table 7.

Table 7. LTE background traffic application requirements [20]

Categories	Delay Budget	Application
GBR	100 ms 300 ms	Voice Streaming
Non-GBR	300 ms	FTP, Web, and data usage

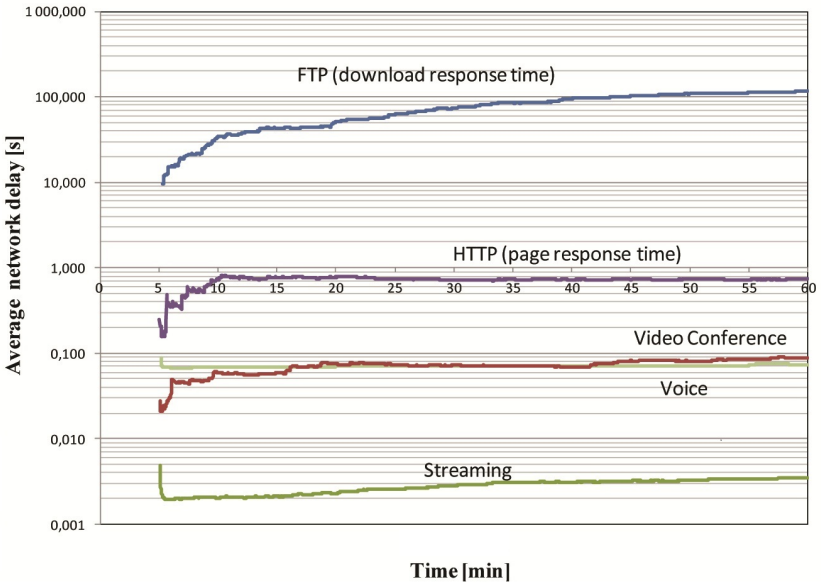

Figure 24. Average delay of LTE background traffic generation scenario.

5.1.3.3. Two way normal AMR traffic with LTE background traffic generation scenario

The scenario includes DL AMR component to normal and background traffic scenario. The server generates AMR data (Tarif updates, reconfiguration, etc.) in downlink direction. Traffic generation parameters for the simulation scenario. The server generates 750 packets evenly between the clusters, i.e., 1 packet is generated for each RTU with a repeating cycle. The downlink packet generation is evenly distributed throughout the generation time interval so as to not burden the network with unnecessary large simultaneous generation of data packets.

Table 8. AMR traffic generation parameters in uplink and downlink

Data type	start time	Interval	Payload	Simulation
AMR data (uplink)	random 5-20 min	15 min	250 B	1hr
AMR data (downlink)	5 min	4.3 s	250 B	1hr

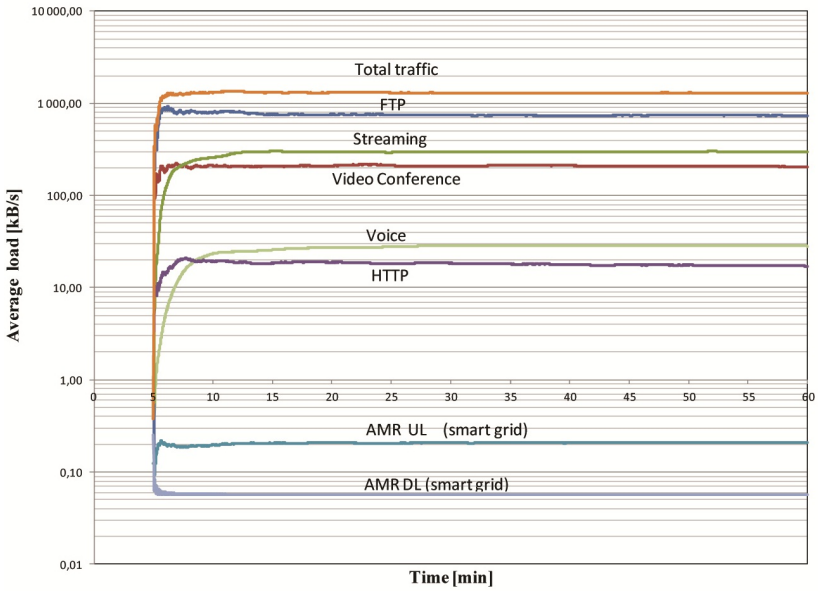

Figure 25. Average load of two way normal AMR traffic with LTE background traffic generation scenario.

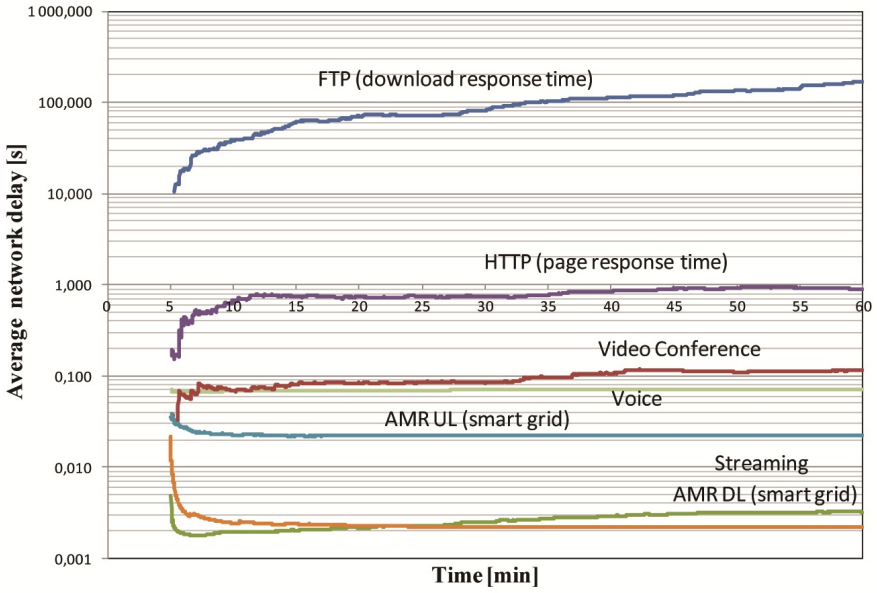

Figure 26. Average delay of two way normal AMR traffic with LTE background traffic generation scenario.

The Table 8 shows the traffic generation parameters. The average generated uplink and downlink traffic along with the AMR component is shown in the Figure 25. The Figure 26 shows the average network delay as a function of time. The DL AMR traffic is shown in this plot is less compared to previous BG and normal scenario. The delay for DL AMR is found to be bit more than 2 ms. The obtained results are compared with the NIST [9] smart metering requirements in Table 11.

5.2. Sensor Network

We have seen that AMR data produced in the LTE network does not effect the load and delay performance of the network. In this section we use sensor nodes instead of LTE devices. The chosen sensor network model for performing the simulations is based on [52].

5.2.1. Topology description

The sensor network simulations are done on suburban environment, as depicted in Figure 20. The topology stated in the LTE network model is used for sensor network simulations. The parameters used for simulating sensor nodes are described in Table 9.

Table 9. Simulation parameters of WSN in smart meters

Physical layer parameters	
Data rate	250 Kbps
Bandwidth	2000 Khz
Frequency	2401 Mhz
Noise figure	1 dB
MAC layer parameters	
Beacon order	7
Superframe order	7
Number of retransmissions	4
CSMA backoff number	5
CSMA backoff exponent	3
Beacon enabled	yes
Application layer parameters	
Traffic generated	Best effort traffic
Packet inter arrival time	600 s
Packet size	2000 bits

5.2.2. Propagation model

The sensor node in the simulations use free space pathloss model for evaluating pathloss during propagation. The free space pathloss [48] is given by:

$$PL_f = A + 10\gamma log_{10}(d_{pl}/d_{pl0}) + s; \quad d \leq d_0 \tag{5.2}$$

where A is the free space path loss constant, s is shadow fading component, d_{pl} is the distance separation between the transmitter and receiver, d_{pl0} is the reference distance

which is equal to 100 meters, λ is wavelength in meters, and γ_{pl} is a gaussain random of the chosen terrain category known as pathloss component.

$$\begin{aligned} A &= 20log_{10}(4\pi d_{pl0}/\lambda) \\ \gamma &= (a - bh_b + c/h_b) + x\sigma \\ s &= y\sigma \\ \sigma &= \mu_\sigma + z\sigma_\sigma \end{aligned} \tag{5.3}$$

where a, b, c, and σ_y are data driven constants, σ is standard deviation of shadow fading, μ_σ is the mean of σ, h_b is the height of the base station antenna in meters, y and z are zero mean Gaussian random variable of unit standard deviation N[0,1]. The 6 dB loss incurred by walls during signal propagation as in suburban environment of LTE propagation model in section 5.1.2.1 is also considered in sensor network propagation model.

5.2.3. Simulation scenarios

The simulation scenarios of sensor network standard IEEE 802.15.4 consist of normal AMR traffic. The traffic generation parameters in LTE scenarios are used in sensor network simulations. The Table 10 details the traffic components as a function of time. The average network load,delay and packet delivery ratio are the main parameters used

Table 10. AMR traffic generation parameters.

Data type	start time	Generation interval	Payload data	Simulation
AMR data	random 5-20 min	15 min	250 B	1hr

for evaluating the ability of the technology to handle generated traffic. Average network load denotes the number of bits that can be transferred per second to destination from the source. The End to end delay is the time taken for the packet to reach the destination from the source. The end to end delay and packet delivery ratio can be evaluated using Eq (5.4) and Eq (5.5). Packet delivery ratio is the proportion to the total amount of packets reached the receiver to the amount of the packets sent by the source.

$$\text{End to end delay (ms)} = \frac{\sum \text{(Delay of each entities data packet)}}{\text{(Total number of delivered data packets)}} \tag{5.4}$$

$$\text{Packet delivery ratio (\%)} = \frac{\text{(Number of packets successfully delivered)}}{\text{(Number of packets generated by source)}} \tag{5.5}$$

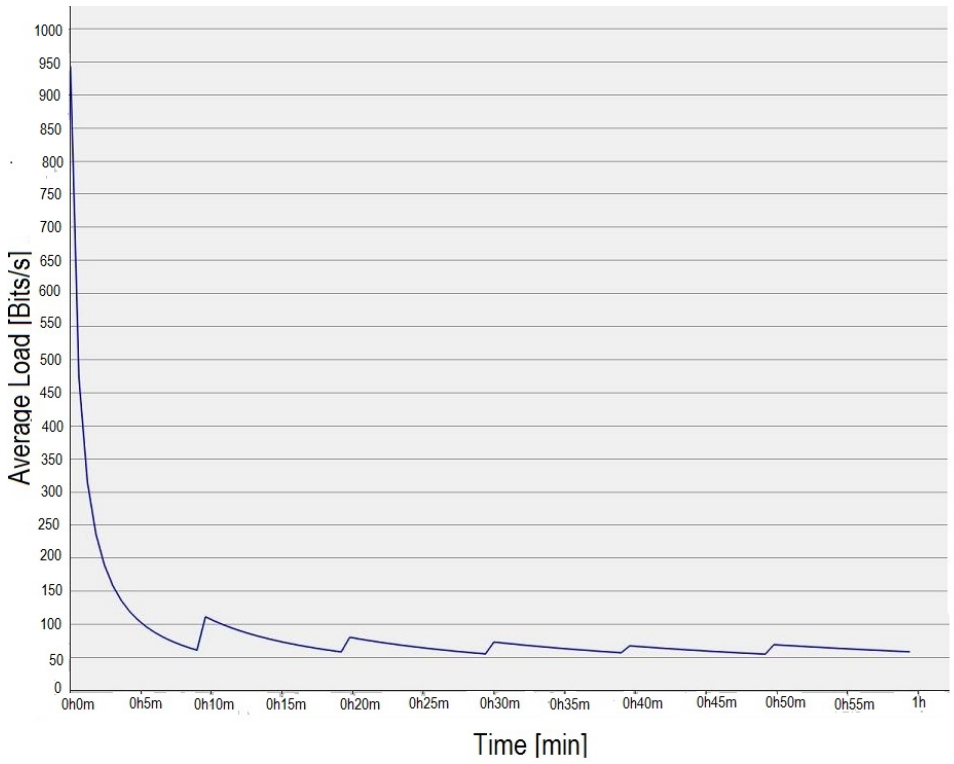

Figure 27. Average load of normal AMR traffic in WSN.

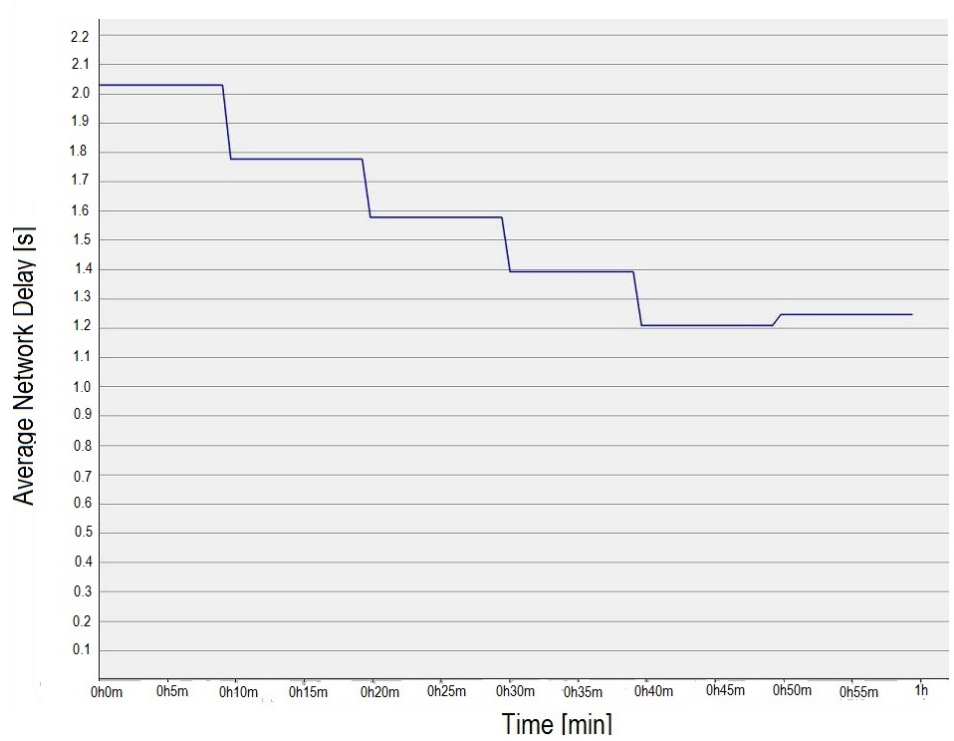

Figure 28. Average network delay of normal AMR traffic in WSN.

The Figure 27 visualizes the average network load of AMR traffic using WSN. The communication of data with the coordinator from 25 nodes show a exponential decrease from 900 to 60 Kbps. The average load is found to be 80 Kbps with payload of 250 Bytes. The Figure 28 shows the network end to end delay with normal traffic components as function of time. The average end to end delay is found to be 1.6 seconds. To summarise the Figures 27 and 28 the traffic load and the network end to end delay values are below the tolerable level specified by NIST [9] requirements for smart metering. The Table 11 summarise the LTE and WSN simulation output results detailed in the Section 5.3.

5.3. Discussion

The main aspect of the simulation study detailed in Sections 5.2.3, and 5.1.3 is to understand the feasibility of LTE and WSN communication techonologies for smart meters. The feasibility study compares the results of LTE and WSN with the requirements by NIST [9] as shown in Table 11. The data aggregation point (DAP) to smart meter is considered as downlink and smart meter to DAP as uplink communication.

Table 11. Feasibility study of LTE and WSN in smart meters

NIST [9] requirements for smart metering		
Parameter	Value	
Average delay (seconds)	<10	
Average payload (Bytes)	200 to 1600	
Use cases (specific to NIST [9])	MR-14, MR-16, MR-26, MR-27, MR-35	
Reliability	99%	
Smart meters using LTE technology		
Parameter	Uplink	Downlink
Average delay (seconds)	3E-02	3E-03
Average payload (Bytes)	250	250
Data rate (bits/sec)	0.3k	0.08k
Smart meters using WSN technology		
Parameter	Downlink	
Average delay (seconds)	1.6	
Average payload (Bytes)	250	
Data rate (bits/sec)	50	

The simulation results validate the feasibility of LTE and WSN communications in smart meters with respect to NIST [9] requirements. The average delay according to the NIST [9] smart metering requirements is less than 10 seconds for a payload ranging from 200 to 1600 Bytes of packet data. The simulations are performed for payload packet data of 250 Bytes for both LTE and WSN in suburban environment. The delay due to smart metering traffic is found to $3 \times 10^{-03} s$ for LTE communication technology and $1{,}6s$ for WSN communication technology.

6. FRAGMENTATION ANALYSIS IN THE MAC LAYER OF IEEE 802.15.4K STANDARD

6.1. Introduction

In this chapter the suitable size for handling smart meter traffic in WSN is evaluated using fragmentation scheme. Each fragment has a error control code to mitigate the errors that occur in the wireless communication channel. The WSN uses CRC code in the MAC layer. CRC codes are error detecting codes which are used in digital communication networks for link reliability and in storage devices to protect the data. CRC code was invented by W. Wesley Peterson [53] in the year 1961.

In LECIM draft (i.e., IEEE 802.15.4k [10] which can be used for smart metering applications in sensor node devices) the frames in the MAC layer are fragmented. The whole MAC frame of IEEE 802.15.4 [12] is divided in to equal sized fragments. Now, each fragment requires separate CRC code attached for the reliability of the fragment data received. In this chapter the appropriate fragment and CRC checksum size for each fragment of divided MAC frame in the IEEE 802.15.4k standard is evaluated using undetected error probability. The generator polynomials used for different CRC checksums (i.e, 8, 16, 24, and 32 bits) are shown in 6.1 [12], 6.2 [12], 6.3 [54], and 6.4 [27].

8 bit polynomial:

$$x^8 + x^7 + x^4 + x^3 + x + 1 \tag{6.1}$$

16 bit polynomial:

$$x^{16} + x^{12} + x^5 + 1 \tag{6.2}$$

24 bit polynomial:

$$x^{24} + x^{23} + x^6 + x^5 + x + 1 \tag{6.3}$$

32 bit polynomial:

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x^1 + 1 \tag{6.4}$$

The 8 bit CRC generator polynomial was proposed by Comité consultatif international téléphonique et télégraphique (CCITT) now renamed as international telecommunication union - telecommunication standardization sector (ITU-T) [55]. The 8 bit generator polynomial is also used in asynchronous transfer mode (ATM), a switching technique used in computer networks and in integrated services digital network (ISDN) a communication standard used for transmission of voice, data and other network services. The IEEE 802.15.4 standard [12] specifies the generator polynomials for 16 and 32 bit. The 24 bit polynomial was proposed by Nokia to 3GPP [54].

6.2. Error performance analysis

The performance evaluation of linear block code (e.g., CRC code) depends on the probability of undetected error [56] at the decoder. Errors at the decoder can be categorized to detected or undetected errors. The detected errors can be corrected using

error recovery techniques (e.g., ARQ, FEC). For undetected errors, the error probability is evaluated which can provide the performance criteria of the used error detection code. The theoretical undetected error probability for CRC code of particular checksum length [56] is given in 6.5.

$$P_{ue}(C,\epsilon) = \sum_{i=1}^{n} A_i \epsilon^i (1-\epsilon)^{n-i}, \tag{6.5}$$

where A_i is the number of codewords of weight *i* in (*n,k,d*) linear block code *C*, and ϵ is the bit error rate of the channel ($\epsilon \in [0,0{,}5]$).

Alternatively, the probability of undetected error can be evaluated by 6.6.

$$P_{ue}(C,\epsilon) = 2^{-m} \sum_{i=0}^{n} B_i (1-2\epsilon)^i - (1-\epsilon)^n, \tag{6.6}$$

where B_i is the number of codewords of weight i in (n, k, d) linear block dual code C^T, $m = n - k$. The weight distributions A_i, B_i in Eq (6.5) and Eq (6.6) are

$$A(z) = A_0 + A_1 z + A_2 z + \cdots + A_n z\cdot \tag{6.7}$$

$$B(z) = B_0 + B_1 z + B_2 z + \cdots + B_n z\cdot \tag{6.8}$$

The weight distributions of the A_i and B_i are needed for evaluating undetected error probabilities. Different methods for the evaluation of weight distributions of A_i and B_i are proposed in [57–59]. The calculation of weight distributions using the proposed methods is complex and cumbersome. The easiest way to evaluate the weight distributions is by assuming the weight distributions to a previously known distribution. To understand the complexity of determining weight distributions, let us take a linear block code of (1040,1024) for example where $n = 1040$ bits and $k = 1024$ bits. The calculation of weight distribution of A_i for the block code (1040,1024) is obtained by evaluating all the codewords of weights equal to 2^{1024} (i.e., $1.8* 10^{308}$), whereas the calculation of weight distribution of B_i is evaluated using dual code. Dual code is the scalar product of the original code. Hence, the weight distribution of B_i result to 2^m codewords (i.e., $2^{16} = 65536$ codewords). But, to derive the dual code weight distribution B_i can be much more tedious than the weight distribution A_i. To evaluate the weight distribution of A_i in this thesis, binomial distribution can be assumed as detailed in [60]. Then the equation to evaluate probability of undetected error probability is given by

$$P_{ue}(\epsilon) = \sum_{i=d_{min}}^{d_{max}} \binom{n}{i} / 2^m * (\epsilon^i (1-\epsilon)^{n-i})\cdot \tag{6.9}$$

The theoretical upper bound of the undetected error for different polynomials is given by 2^{-m} [61] where *m* is the redundancy of the code or the length of the parity code. Hence, the theoretical upper bound values for 8, 16, 24, 32 bits are $3.9*10^{-03}$, $1.52*10^{-05}$, $5.9*10^{-08}$, and $2.32*10^{-10}$ respectively.

6.3. Fragmentation scheme in IEEE 802.15.4k standard

In low energy, critical infrastructure monitoring (LECIM) networks, requires dividing the whole data frame to several frames for higher reliability. The fragmentation is done in the MAC layer before sending it to the physical layer. The objective for fragmenting MAC frame to several smaller fragments is to avoid interference caused by low PHY operating modes [10] and also to reduce retransmission costs for longer frames. The fragmentation scheme of MAC service data unit (MSDU) in to several fragments is shown in the Figure 29. The MSDU is fragmented into several fragments form the physical layer protocol data unit (PPDU). Each PPDU now consist of new header and validity check sequence.

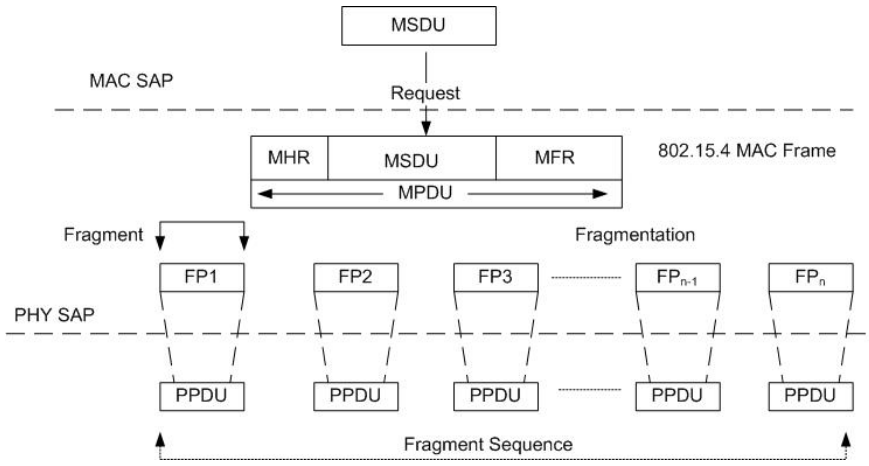

Figure 29. Fragmentation in IEEE 802.15.4k [10].

The validity check sequence is the CRC checksum obtained through polynomial division as detailed in Section 4.1.1. The different polynomials chosen for evaluating the checksum are specified in Section 6.1. Different fragment lengths where the MAC frame can be fragmented are considered. The sizes considered are shown in table 12. The size of MSDU according the IEEE 802.15.4 standard [12] is 127 bytes which is 1016 binary bits.

The MSDU frame format according the IEEE 802.15.4 standard [12] is shown in the Figure 30.

Figure 30. MAC Frame format [12] of IEEE 802.15.4 Standard.

MHR (24 bits)	MSDU (1016 bits)	FCS (32 bits)

The MAC layer frame shown in Figure 30 is divided in to many fragments. The fragmented frame consist of fields shown in Figure 31. The fragmented frame is composed of the fragment header which can be 1 to 3 bytes variable depending the PHY profile [12], the fragment payload data and the validity check sequence (i.e., frame check sequence (FCS)).

If the frame cannot be divided exactly in to chosen fragment sizes (i.e., 2,4,8,$\cdots$, 1024) then bit stuffing is performed. In bit stuffing, MAC frame is appended with zeros

Figure 31. Fragmented frame format.

Fragment Header (variable)	Fragment Data (variable)	FCS (variable)

to adjust to the chosen fragmented length. The fragment length for each polynomial is shown in Table 12.

Table 12. Variable fragment data size with different FCS lengths

	Fragmented frame length of different CRC lengths (bits)			
Fragment data (bits)	CRC-8	CRC-16	CRC-24	CRC-32
2	18	26	34	42
4	20	28	36	44
8	24	32	40	48
16	32	40	48	56
32	48	56	64	72
64	80	88	96	104
128	144	152	160	168
256	272	280	288	296
512	528	536	544	552
1024	1040	1048	1056	1064

6.3.0.1. Fragmentation scheme.

The evaluation of undetected error probabilities using fragmentation scheme is shown in the Figure 32. The fragments are transmitted to the receiver. While transmission, random error is added with the transmitted packet. If the fragment CRC is valid after addition of random error, then the undetected error probability is evaluated using the Eq (6.9). Once all the fragments are received, then the reassembly takes place. The packet CRC is checked and if the packet CRC is valid the packet is accepted and undetected error probability for each packet is evaluated.

If the fragment CRC is invalid, then the respective fragment is retransmitted. The max number of retransmission tries for a single fragment is 4 (i.e., *macMaxFrameRetries)* [12]). If the fragment retransmission fails, then the packet is fragmented again with newly generated random MAC data frame (i.e., MPDU). If the packet CRC fails the whole packet is retransmitted. In order to obtain the probabilities statistically correct, each simulation is run for 10^5 times. The energy consumption for each packet is calculated once the fragment and packet undetected error probabilities are derived.

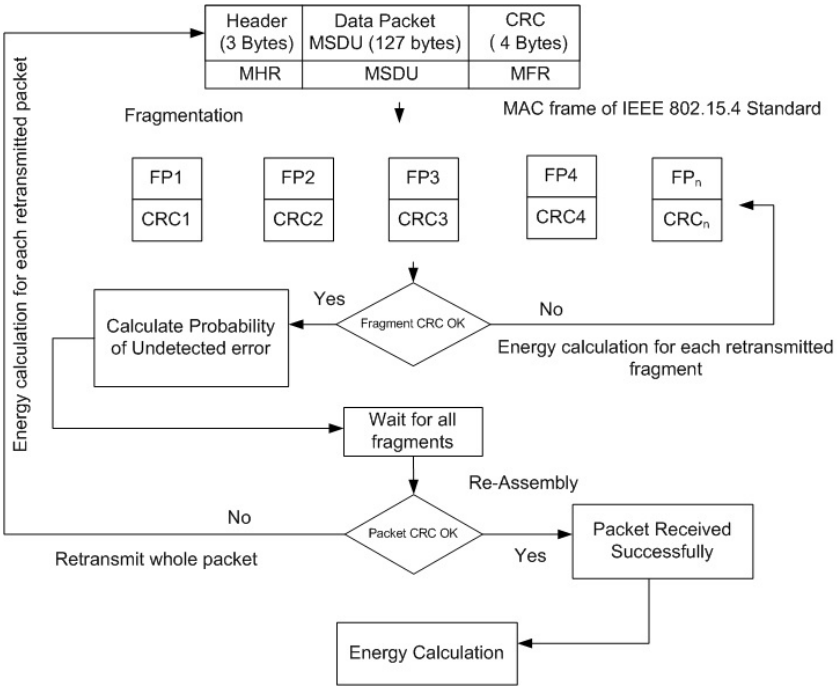

Figure 32. Fragmentation Algorithm

6.3.0.2. Simulation results.

The simulation results obtained from the fragmentation scheme are the total fragment and packet undetected error probability for chosen polynomials in Section 6.1.A three dimensional surface with fragment length in bits, BER, and the undetected error probability is plotted in order to evaluate the performance of chosen 8 bit, 16 bit, 24 bit, and 32 bit polynomials. The Table 13 provides the sum of the fragment undetected error probabilities for different BER's ranging from 10^{-06} to 10^{-02} for different fragment bit lengths.

Table 13. Fragment undetected error probabilities of 8, 16, 24 and 32 bit polynomials

Fragment data (bits)	CRC-8	CRC-16	CRC-24	CRC-32
2	0,010182	0,00010187	$1{,}0478 \times 10^{-7}$	$2{,}1623 \times 10^{-9}$
4	0,010881	0,00010897	$1{,}2262 \times 10^{-7}$	$1{,}1056 \times 10^{-9}$
8	0,016395	0,00015865	$2{,}3209 \times 10^{-7}$	$1{,}5660 \times 10^{-9}$
16	0,011695	0,00011703	$1{,}4233 \times 10^{-7}$	$1{,}1951 \times 10^{-9}$
32	0,026378	0,00018934	$2{,}7171 \times 10^{-7}$	$1{,}8921 \times 10^{-9}$
64	0,019552	0,00018020	$2{,}6859 \times 10^{-7}$	$1{,}6977 \times 10^{-9}$
128	0,029947	0,00015945	$2{,}0878 \times 10^{-7}$	$1{,}9331 \times 10^{-9}$
256	0,042887	0,00010034	$1{,}0046 \times 10^{-7}$	$2{,}1275 \times 10^{-9}$
512	0,040932	0,00010000	$1{,}0000 \times 10^{-7}$	$1{,}0226 \times 10^{-9*}$
1024	0,010912	0,00010000	$1{,}0000 \times 10^{-7}$	$1{,}4993 \times 10^{-9}$

The Figure 33 show the 8, 16, 24 and 32 bit polynomial fragment undetected error probabilities over different BER's and with different fragment lengths.

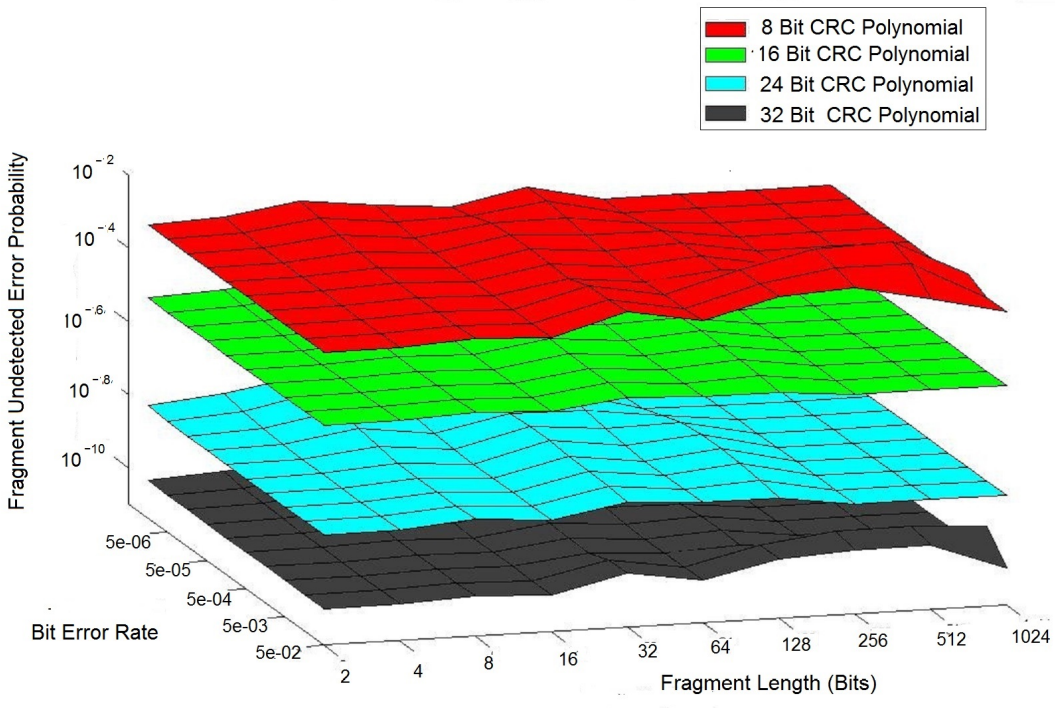

Figure 33. Surface plot of fragment undetected error probability of 8, 16, 24 and 32 bit CRC polynomials.

The Figure 34 shows the comparison of 8, 16, 24 and 32 bit CRC generator polynomials with respect to undetected error probabilites, fragment length in bits and BER's. The 8 bit generator polynomial has the least packet undetected error probability compared to 16, 24, and 32 bit polynomials. The Packet undetected error probabilities are calculated statistically running simulations for 10^5 iterations. The Table 14 gives the sum of the packet undetected error probabilities for different BER's ranging from 10^{-06} to 10^{-02} for different fragment bit lengths. The packet undetected error probabilities are derived using the Eq (6.9) as in fragment undetected error probability. Based on the evaluation of fragment and packet undetected error probabilities we can evaluate the average number of undetected error bits that can occur in the suburban environment described in Section 5.1.1. The Table 15 shows the number of undetected error bits that can occur in a duration of 1 month using different fragmentation lengths.

$*$ Red value indicates the least value in the table.

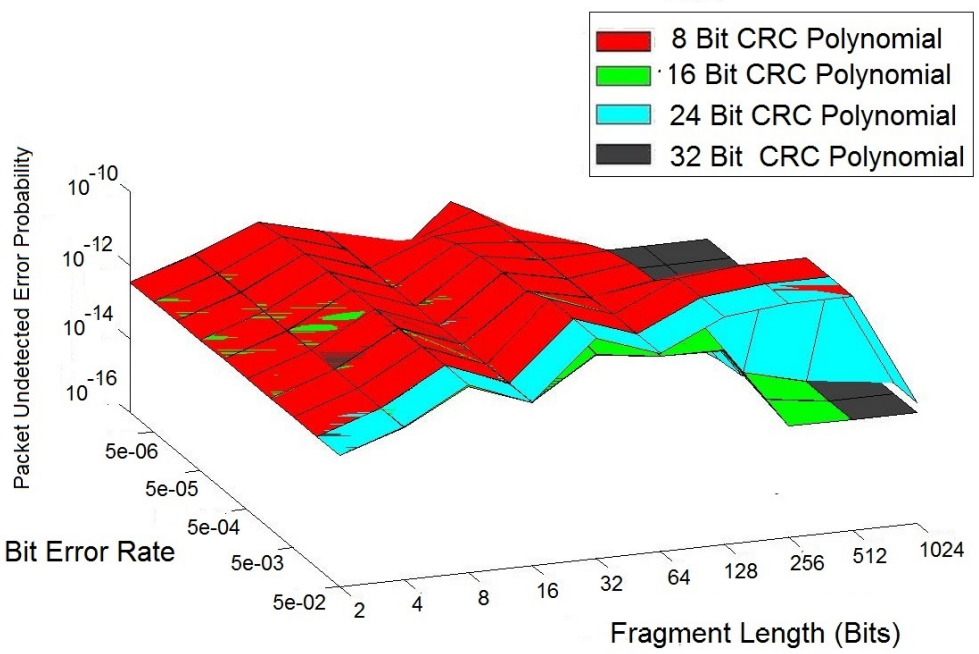

Figure 34. Surface plot of packet undetected error probability of 8, 16, 24 and 32 bit CRC polynomials.

Table 14. Packet undetected error probabilities of 8, 16, 24 and 32 bit polynomials

Fragment data (bits)	CRC-8	CRC-16	CRC-24	CRC-32
2	$3{,}5605 \times 10^{-12}$	$3{,}5572 \times 10^{-12}$	$3{,}5538 \times 10^{-12}$	$3{,}5549 \times 10^{-12}$
4	$1{,}3610 \times 10^{-11}$	$1{,}3531 \times 10^{-11}$	$1{,}3446 \times 10^{-11}$	$1{,}3472 \times 10^{-11}$
8	$1{,}0901 \times 10^{-10}$	$1{,}0313 \times 10^{-10}$	$9{,}9640 \times 10^{-11}$	$9{,}9872 \times 10^{-11}$
16	$2{,}5749 \times 10^{-11}$	$2{,}5445 \times 10^{-11}$	$2{,}5138 \times 10^{-11}$	$2{,}5231 \times 10^{-11}$
32	$4{,}7174 \times 10^{-10}$	$2{,}8306 \times 10^{-10}$	$3{,}6718 \times 10^{-10}$	$2{,}6093 \times 10^{-11}$
64	$1{,}8830 \times 10^{-10}$	$1{,}6980 \times 10^{-10}$	$1{,}6513 \times 10^{-10}$	$1{,}6223 \times 10^{-11}$
128	$5{,}7806 \times 10^{-10}$	$1{,}8333 \times 10^{-10}$	$4{,}1426 \times 10^{-10}$	$1{,}6319 \times 10^{-11}$
256	$6{,}9572 \times 10^{-10}$	$1{,}5377 \times 10^{-12}$	$4{,}6504 \times 10^{-10}$	$1{,}3816 \times 10^{-12}$
512	$6{,}9830 \times 10^{-10}$	$1{,}5200 \times 10^{-12}$	$4{,}6665 \times 10^{-10}$	$1{,}6800 \times 10^{-12}$
1024	$1{,}2702 \times 10^{-12}$	$1{,}8900 \times 10^{-12}$	$1{,}2802 \times 10^{-12}$	$1{,}2600 \times 10^{-12*}$

The Table 14 shows the sum probabilities of packet undetected errors. From the Table 14 the packet undetected error probabilities are found to be the least for 2 and 1024 bits with values ranging to 10^{-12} for all the CRC Polynomials. It can also be seen that 16, and 32 bit CRC polynomials showing a similar profile while 8, and 24 bit exhibiting a similar packet undetected error profile. If we consider the 8 bit and 24 bit CRC polynomials for the packet undetected error values, as the fragment size increases the undetected error probability increases and decreases until 16 bit fragment length and remains constant till 512 bit fragment length and decreases for 1024

$*$ Red value indicates the least value in the table.

bits. The reason behind this fluctuating error probabilities might be due to the length of the payload and CRC for each packet. If we consider the 16, and 32 bit polynomial, the undetected error probabilities also increase until 128 bit fragment length and decrease as the fragment length increases. It can inferred from the result that 16 bit and 32 bit polynomials are better compared to 8 and 24 bit Polynomial with respect to packet undetected error probabilities. Based on the fragment and packet undetected error probabilities we can derive the average number of possible undetected error bits in particular duration of time (i.e., 30 days) as shown in Table 15. As the packet error probabilities and fragment error probabilities are least for 2 and 1024 bit fragment lengths, the occurence of undetected error bits are also the least. The undetected error bits (i.e., 1,2609) is found to be the least for 512 bit fragment length with CRC polynomial of 32 bit length. The probability of undetected error bits are evaluated using Table 5. The AMR traffic is generated every 15 min with packet size of 250 Bytes. Hence the total number of packets for 30 days is evaluated. The packet undetected error probabilities are multiplied with the number of packets to determine the number of bits which can be undetected at the receiver in a duration of 30 days.

Table 15. Average undetected error bits of 8, 16, 24 and 32 bit polynomials

Fragment data (bits)	CRC-8	CRC-16	CRC-24	CRC-32
2	1,2660	1,2618	1,2616	1,2680
4	1,5162	1,5542	1,5621	1,5658
8	1,8895	1,8956	1,5061	1,5156
16	1,5172	1,5041	1,545	1,5074
32	1,8155	1,8758	1,8111	1,8520
64	1,7742	1,7818	1,8836	1,8477
128	1,8367	1,7388	1,8802	1,8595
256	1,8600	1,2768	1,8008	1,2895
512	1,8282	1,2681	1,8322	1,2609*
1024	1,2703	1,2611	1,2630	1,2772

6.4. Energy evaluation analysis

WSNs consist of a set of small devices with limited energy resources, reduced processing capabilities and a radio frequency communication unit with limited transmission power. Power consumption models [62] in sensor nodes take both transceiver and startup power consumption along with an accurate model of the amplifier as shown in Figure 35. The power consumption energy per bit e_b [63] can be given as

$$e_b = e_{tx} + e_{rx} + E_{dec}/\imath, \tag{6.10}$$

where e_{tx} and e_{rx} are the transmitter and receiver power energy consumption per bit, respectively, E_{dec} is the energy required for decoding a packet, and $\imath$ is the payload length in bits. The e_{tx} from Eq (6.10) can be given by

* Red value indicates the least value in the table.

$$e_{tx} = e_{te} + e_{ta}d^{\alpha}, \tag{6.11}$$

where e_{te} is the energy consumption of the transmitter electronics per bit, e_{ta} is the energy consumption of the transmit amplifier per bit over a distance of 1 meter, d is the transmission distance, and α is the pathloss component. The expression for evaluating the transmit amplifier per bit over a distance of 1 meter [64] can be given by

$$e_{ta} = \frac{(S/N)_r(NF_{Rx})(N_0)(BW)(4\pi/\lambda)^{\alpha}}{(G_{ant})(\eta_{amp})(R_{bit})} \tag{6.12}$$

where $(S/N)_r$, is the desired signal to noise ratio at the receiver demodulator, NF_{Rx} is the receiver noise figure, N_0 is the thermal noise floor for 1 Hz bandwidth, BW is the channel noise bandwidth, λ is the wavelength in meters, G_{ant} is the antenna gain,η_{amp} is the transmitter efficiency, R_{bit} is the raw channel rate in bits per second.The Eq (6.10) takes into account the energy needed to transmit a frame from a transmitter to a receiver over single hop. The Figure 35 shows the transmitter and receiver energy consumption components when k bits are transmitted to the receiver.

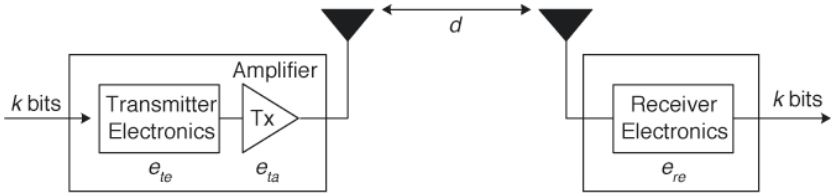

Figure 35. Typical radio energy consumption model where k bits are transmitted, e_{te} and e_{ta} are the transmitter electronics and amplifier energy consumption per bit, respectively. The transmission distance is d and the k bits are received by the receiver, consuming e_{rx} energy per bit [62].

The parameters used for determining the energy consumption values of the transmitter and receiver are shown in Table 16.

Table 16. Radio parameters of sensor node

Parameter	Value
Transmitter circuitry (e_{te})	1.066 $\mu J/bit$
Receiver circuitry (e_{rx})	0.533 $\mu J/bit$
Receiver noise figure (NF_{rx})	10 dB
Thermal noise floor (N_0)	4.17*10^{-21}J
Bandwidth (BW)	40000 Hz
Frequency (f)	900 MHz
Wavelength (λ)	0.333 m
Path loss exponent (α)	2.5
Antenna gain (G_{ant})	0 dB
Transmitter efficiency (η_{amp})	0.2
Signal to Noise Ratio $(S/N)_r$	10 dB
Raw bit rate (R_{bit})	37500 bps

The PHY profile of the 802.15.4 [12] standard can employ different modulation schemes as stated in chapter 2. Different modulation schemes results in different signal to noise ratios (SNR). In order to understand the energy consumption per bit, we assume that sensor node is IEEE 802.15.4 [10] with the respective parameters shown in Table 16. The energy consumption per bit in joules per each fragment when transmitted using different fragment lengths, BER, and polynomials is evaluated. The respective surface plot is shown in Figure 36. The surfaces shows the consumed energy per each polynomial while using the parameters from the Table 16.

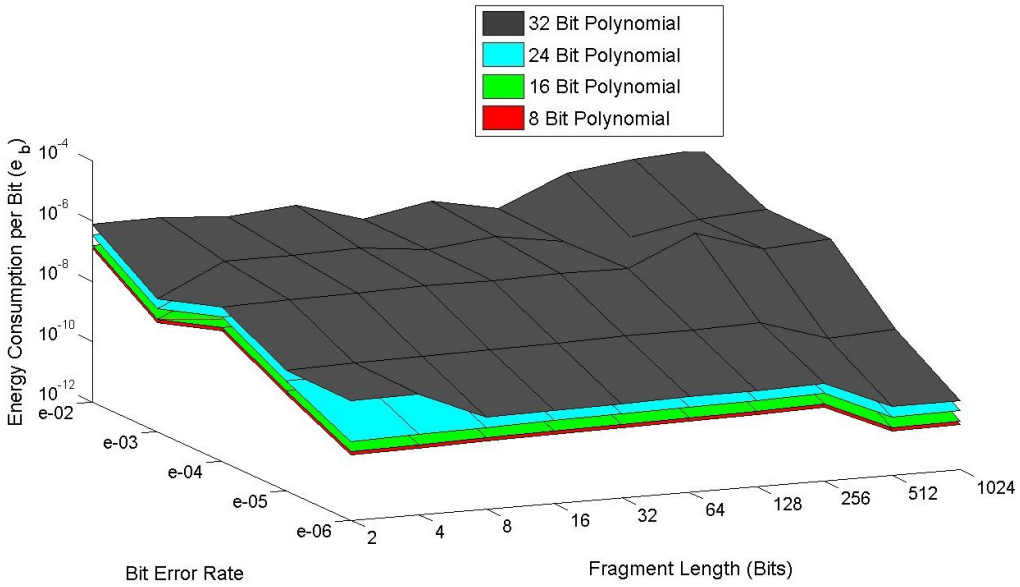

Figure 36. Surface plot of energy consumption of 8, 16, 24 and 32 bit CRC polynomials.

The Figure 36 represent the energy consumption per bit while transmitting fragment lengths shown in Table 12. The graph shows the energy consumption per payload bit for each polynomial when transmitting a 1024 bit payload using fragment sizes between 2 and 1024 and taking into account overhead of fragmentation and CRC. The algorithm considers the retransmission of each fragment with retransmission which equals to 4, if the CRC fails. Even after retransmission if the packet is not received, the packet is discarded and new packet is sent. From the fragmentation algorithm shown in Figure 32 transmitted and retransmitted packets are evaluated. Using the transmitted and retransmitted packets, the delivery ratios are evaluated. The delivery ratios and energy consumption per bit shown in Eq (6.10) is used to evaluate the energy consumption of each packet for a particular fragment length, CRC polynomial and BER. The energy consumptions of the polynomials are determined statistically for 10^5 simulation iterations. The energy consumption for different BER's (i.e., 10^{-2} to 10^{-6}) using CRC-8, 16, 24, and 32 is shown in Table 17, 18, 19, 20, and 21.

Table 17. Energy consumption of 8, 16, 24 and 32 bit polynomials for BER 10^{-2}

Fragment data (bits)	CRC-8	CRC-16	CRC-24	CRC-32
2	$1{,}2350 \times 10^{-7}$	$1{,}5719 \times 10^{-7}$	$3{,}4581 \times 10^{-7}$	$7{,}6425 \times 10^{-7}$
4	$1{,}3264 \times 10^{-7}$	$6{,}6881 \times 10^{-7}$	$3{,}7138 \times 10^{-7}$	$8{,}2075 \times 10^{-7}$
8	$1{,}0367 \times 10^{-7*}$	$1{,}2010 \times 10^{-7}$	$2{,}6423 \times 10^{-7}$	$5{,}8394 \times 10^{-7}$
16	$1{,}5322 \times 10^{-7}$	$1{,}9501 \times 10^{-7}$	$7{,}2902 \times 10^{-7}$	$9{,}1310 \times 10^{-7}$
32	$3{,}4116 \times 10^{-7}$	$4{,}3420 \times 10^{-7}$	$3{,}2325 \times 10^{-7}$	$2{,}1111 \times 10^{-7}$
64	$8{,}6141 \times 10^{-7}$	$1{,}0963 \times 10^{-7}$	$2{,}4119 \times 10^{-7}$	$5{,}3304 \times 10^{-7}$
128	$3{,}2529 \times 10^{-7}$	$4{,}1401 \times 10^{-7}$	$3{,}1082 \times 10^{-7}$	$2{,}0129 \times 10^{-7}$
256	$3{,}0565 \times 10^{-7}$	$3{,}8901 \times 10^{-7}$	$2{,}5583 \times 10^{-7}$	$1{,}8914 \times 10^{-6}$
512	$5{,}9478 \times 10^{-6}$	$3{,}5699 \times 10^{-7}$	$1{,}6654 \times 10^{-6}$	$3{,}6805 \times 10^{-6}$
1024	$8{,}0093 \times 10^{-6}$	$1{,}0194 \times 10^{-6}$	$2{,}2426 \times 10^{-6}$	$4{,}9561 \times 10^{-6}$

Table 18. Energy consumption of 8, 16, 24 and 32 bit polynomials for BER 10^{-3}

Fragment data (bits)	CRC-8	CRC-16	CRC-24	CRC-32
2	$4{,}1425 \times 10^{-9}$	$5{,}2722 \times 10^{-9}$	$1{,}1599 \times 10^{-8}$	$2{,}5634 \times 10^{-8}$
4	$4{,}6165 \times 10^{-8}$	$5{,}8755 \times 10^{-8}$	$1{,}2926 \times 10^{-8}$	$2{,}8567 \times 10^{-8}$
8	$4{,}6407 \times 10^{-8}$	$1{,}9064 \times 10^{-9*}$	$1{,}2994 \times 10^{-7}$	$2{,}8717 \times 10^{-7}$
16	$5{,}5751 \times 10^{-8}$	$3{,}0956 \times 10^{-8}$	$1{,}5610 \times 10^{-7}$	$3{,}4499 \times 10^{-7}$
32	$3{,}2506 \times 10^{-8}$	$4{,}1371 \times 10^{-8}$	$9{,}1017 \times 10^{-7}$	$2{,}0115 \times 10^{-7}$
64	$5{,}4713 \times 10^{-8}$	$6{,}9635 \times 10^{-7}$	$1{,}5320 \times 10^{-7}$	$3{,}3857 \times 10^{-7}$
128	$2{,}4635 \times 10^{-8}$	$3{,}1354 \times 10^{-7}$	$6{,}8979 \times 10^{-7}$	$1{,}5244 \times 10^{-7}$
256	$2{,}3246 \times 10^{-8}$	$2{,}9586 \times 10^{-8}$	$6{,}5090 \times 10^{-7}$	$1{,}4385 \times 10^{-7}$
512	$5{,}4303 \times 10^{-7}$	$7{,}5477 \times 10^{-7}$	$1{,}6605 \times 10^{-7}$	$3{,}6697 \times 10^{-7}$
1024	$4{,}0065 \times 10^{-7}$	$1{,}0190 \times 10^{-7}$	$2{,}2418 \times 10^{-7}$	$4{,}9544 \times 10^{-7}$

Table 19. Energy consumption of 8, 16, 24 and 32 bit polynomials for BER 10^{-4}

Fragment data (bits)	CRC-8	CRC-16	CRC-24	CRC-32
2	$2{,}0763 \times 10^{-8}$	$2{,}6425 \times 10^{-8}$	$5{,}8136 \times 10^{-8}$	$1{,}2848 \times 10^{-7}$
4	$2{,}3324 \times 10^{-8}$	$2{,}9685 \times 10^{-8}$	$6{,}5307 \times 10^{-8}$	$1{,}4433 \times 10^{-7}$
8	$2{,}5511 \times 10^{-8}$	$3{,}2469 \times 10^{-8}$	$7{,}1431 \times 10^{-8}$	$1{,}5786 \times 10^{-7}$
16	$2{,}8454 \times 10^{-8}$	$3{,}6214 \times 10^{-8}$	$7{,}9670 \times 10^{-8}$	$1{,}7607 \times 10^{-7}$
32	$2{,}7169 \times 10^{-8}$	$1{,}4579 \times 10^{-8*}$	$7{,}6073 \times 10^{-8}$	$1{,}6812 \times 10^{-7}$
64	$3{,}2613 \times 10^{-8}$	$4{,}1508 \times 10^{-8}$	$9{,}1317 \times 10^{-8}$	$2{,}0181 \times 10^{-7}$
128	$2{,}9433 \times 10^{-8}$	$3{,}7460 \times 10^{-8}$	$8{,}2413 \times 10^{-8}$	$1{,}8213 \times 10^{-7}$
256	$2{,}9940 \times 10^{-7}$	$3{,}8106 \times 10^{-7}$	$8{,}3832 \times 10^{-7}$	$1{,}8527 \times 10^{-6}$
512	$5{,}8864 \times 10^{-8}$	$7{,}4918 \times 10^{-8}$	$1{,}6482 \times 10^{-7}$	$3{,}6425 \times 10^{-7}$
1024	$8{,}0013 \times 10^{-8}$	$1{,}0184 \times 10^{-7}$	$2{,}2404 \times 10^{-7}$	$4{,}9512 \times 10^{-7}$

$*$ Red value indicates the least value in the table.

Table 20. Energy consumption of 8, 16, 24 and 32 bit polynomials for BER 10^{-5}

Fragment data (bits)	CRC-8	CRC-16	CRC-24	CRC-32
2	$1{,}5582 \times 10^{-9}$	$1{,}9831 \times 10^{-9}$	$4{,}3629 \times 10^{-9}$	$9{,}6420 \times 10^{-9}$
4	$1{,}7528 \times 10^{-9}$	$2{,}2308 \times 10^{-9}$	$4{,}9079 \times 10^{-9}$	$1{,}0846 \times 10^{-9}$
8	$1{,}9457 \times 10^{-9}$	$2{,}4764 \times 10^{-9}$	$5{,}4480 \times 10^{-9}$	$1{,}2040 \times 10^{-9}$
16	$2{,}1421 \times 10^{-9}$	$2{,}7263 \times 10^{-9}$	$5{,}9978 \times 10^{-9}$	$1{,}3255 \times 10^{-9}$
32	$2{,}3104 \times 10^{-9}$	$2{,}9405 \times 10^{-9}$	$6{,}4692 \times 10^{-9}$	$1{,}4297 \times 10^{-9}$
64	$2{,}5265 \times 10^{-9}$	$3{,}2155 \times 10^{-9}$	$7{,}0741 \times 10^{-9}$	$1{,}5634 \times 10^{-9}$
128	$2{,}6657 \times 10^{-9}$	$3{,}3928 \times 10^{-9}$	$7{,}4641 \times 10^{-9}$	$1{,}6496 \times 10^{-9}$
256	$2{,}9382 \times 10^{-9}$	$3{,}7396 \times 10^{-9}$	$8{,}2270 \times 10^{-9}$	$1{,}8182 \times 10^{-9}$
512	$5{,}8350 \times 10^{-10}$	$1{,}0263 \times 10^{-10*}$	$8{,}6338 \times 10^{-10}$	$3{,}6107 \times 10^{-9}$
1024	$7{,}6994 \times 10^{-10}$	$1{,}9181 \times 10^{-10}$	$8{,}9398 \times 10^{-10}$	$4{,}9501 \times 10^{-10}$

Table 21. Energy consumption of 8, 16, 24 and 32 bit polynomials for BER 10^{-6}

Fragment data (bits)	CRC-8	CRC-16	CRC-24	CRC-32
2	$1{,}4337 \times 10^{-10}$	$1{,}8247 \times 10^{-10}$	$4{,}0143 \times 10^{-10}$	$8{,}8717 \times 10^{-9}$
4	$1{,}6129 \times 10^{-10}$	$2{,}0528 \times 10^{-10}$	$4{,}5161 \times 10^{-10}$	$9{,}9806 \times 10^{-9}$
8	$1{,}7921 \times 10^{-10}$	$2{,}2809 \times 10^{-10}$	$5{,}0179 \times 10^{-10}$	$1{,}1090 \times 10^{-9}$
16	$1{,}9713 \times 10^{-10}$	$2{,}5090 \times 10^{-10}$	$5{,}5197 \times 10^{-10}$	$1{,}2199 \times 10^{-9}$
32	$2{,}1505 \times 10^{-10}$	$2{,}7370 \times 10^{-10}$	$6{,}0215 \times 10^{-10}$	$1{,}3307 \times 10^{-9}$
64	$2{,}3297 \times 10^{-10}$	$2{,}9651 \times 10^{-10}$	$6{,}5233 \times 10^{-10}$	$1{,}4416 \times 10^{-9}$
128	$2{,}5090 \times 10^{-10}$	$3{,}1932 \times 10^{-10}$	$7{,}0251 \times 10^{-10}$	$1{,}5525 \times 10^{-9}$
256	$2{,}8674 \times 10^{-10}$	$3{,}6494 \times 10^{-10}$	$8{,}0287 \times 10^{-10}$	$1{,}7743 \times 10^{-10}$
512	$3{,}0735 \times 10^{-11*}$	$3{,}9117 \times 10^{-11}$	$8{,}6057 \times 10^{-11}$	$1{,}9019 \times 10^{-10}$
1024	$3{,}2885 \times 10^{-11}$	$4{,}1854 \times 10^{-11}$	$9{,}2079 \times 10^{-11}$	$2{,}0349 \times 10^{-10}$

From the Table 17, it is evident that the energy consumption values are lower for lower fragment lengths and vice versa. The best performance of each polynomial can be seen in 2, 4, and 8 bit fragment length signifying the suitability of lower sizes for higher BERs. Similar profile for the four polynomials is seen in Table 18 with BER $10^{-}3$. As the BER deceases from Table 17 to Table 21 energy consumption values are proportional directly and hence decrease. This decrease can be clearly seen in the Figure 36. In Figure 36 the CRC 8 bit polynomial has the best performance representing the lower surface. The better performance is seen for 16 bit and consecutively. The CRC polynomial of length 32 bit uses the maximum energy per bit compared to the other polynomials. It is also seen that higher fragment lengths are suitable with low BER. From the Table 21 it is seen that 512 bit fragment length showing the best performance with 8 bit CRC polynomial to signify the adaptability of higher fragment lengths in low BER channel conditions.

$*$ Red value indicates the least value in the table.

6.5. Discussion

The simulation results signify the importance of considering the fragmentation in the MAC layer of IEEE 802.15.4k [10] standard. To consider the proposed fragmentation scheme, this thesis focusses mainly on the fragment and packet undetected error probabilities, probability of undetected error bits, and the energy consumption per bit. From the fragment undetected error probability values, fragment length of 512 bits and CRC polynomial of length 32 bits has the least fragment undetected error probability of $1{,}0226 \times 10^{-9}$. The surface plot in Figure 33 shows the 8 bit polynomial surface on the top signifying the maximum of undetected error probabilities. It can be concluded that the higher the length of the CRC polynomial the higher is the reliability of the system with less undetected errors. The fragment undetected error probability simulation results show the fragment length of 512 bits has the least undetected error probability while using CRC polynomial of length 32 bits. But while considering the whole packet undetected error probability, fragment length of 1024 bits with CRC polynomial of 32 bits has the least probability of $1{,}2600 \times 10^{-12}$. The next aspect to be considered is the occurrence of undetected error bits. The Table 15 shows the average number of undetected error bits that can occur in a particular duration of time (e.g., 30 days). The CRC polynomial of length 32 bit and the fragment payload of 512 bits length is found to have the least undetected error bits (i.e., $1{,}2609$). To summarise the results, the fragmentation scheme reduce the probability of undetected errors and the occurrence of undetected error bits. Hence, the MAC layer packet with fragmentation has the least fragment and packet undetected error probability with least number of undetected error bits in a particular duration of time.

If we consider energy consumption per bit for the proposed fragmentation scheme, the Table 21, 20, 19, 18, and 17 show the energy consumption per bit for different BER (i.e., 10^{-06} to 10^{-02}). For BER 10^{-02} in Table 17, the 8 bit CRC polynomial has the least energy consumption for 8 bits (i.e., $1{,}0367 \times 10^{-7}$), the least energy consumption for 16 bit CRC is $6{,}6881 \times 10^{-7}$ for 4 bit fragment length, and for 24 bit CRC, the least energy consumption is $7{,}2902 \times 10^{-7}$ for 16 bit fragment length and for 32 bit CRC polynomial the least energy consumption is $8{,}2075 \times 10^{-7}$ for 4 bit fragment length. It can be inferred from these results collectively that the lower fragment lengths are more suitable at higher bit error rate. If we consider BER 10^{-03} in Table 18, the increase in fragment length is directly proportional to an increase in energy consumed in transmission, reception, and decoding is higher. For BER 10^{-03}, the least energy consumption per bit is found to be $1{,}9064 \times 10^{-9}$ for fragment length of 8 bit and CRC polynomial of length 16 bit. For BER 10^{-04}, the same bit polynomial with fragment length of 32 bit is found have the least energy consumption with $1{,}4579 \times 10^{-8}$. For BER 10^{-05} the least energy consumption is $1{,}0263 \times 10^{-10}$ and for BER 10^{-06} the 512 bit with bit CRC polynomial have the least consumptions $3{,}0735 \times 10^{-11}$. To summarise the energy consumption per bit aspect, the 512 bit fragment length and CRC polynomial with bit length of 8 bit has the least value (i.e., $3{,}0735 \times 10^{-11}$) . Hence it can be concluded that, for different BER's different fragment lengths are found to be effective. But the energy consumption of 8 bit CRC polynomial with fragment length of 512 bit is relatively superior when compared to 16, 24, and 32 bit CRC polynomials.

7. CONCLUSION

The simulation parameters, scenarios and results of smart meters using LTE and WSN communication technologies were studied in this thesis. The first part of the thesis problem was to identify whether smart meter traffic effects LTE and WSN traffic. The feasibility study was performed by evaluating end to end delay and average load of smart meters using LTE and WSN. The results of the end to end delays and average load values posed by smart meter traffic were compared with the NIST [9] requirements. The results validate that the values are well below the requirements specified by NIST. The usage of LTE in smart meter for smart metering can be a option but higher spectrum utilization results in smaller cell sizes and other technologies (i.e., WSN) can also become competitive alternatives.

In the second part of the thesis the required frame length for handling smart meter traffic was discussed. A new fragmentation scheme was proposed. Fragmentation is required in WSN [12] devices reduce the channel coherence time as the present medium access control (MAC) design suffers from collisions [65] during carrier sense multiple access (CSMA) algorithm in high contention environments. In order to avoid collisions in the MAC layer during CSMA algorithm so as to confront the required higher data rates in physical layer of IEEE 802.15.4 [12] standard. The whole packet is divided in to equal length fragments. Fragment lengths were assumed to be 2, 4, $\cdots$, 1024 bits. The fragments were reconstructed again to form the complete packet at the receiver. The surface plot of fragment and packet undetected error probability was derived. It is found that the CRC polynomial of length 32 bit with fragment length of 512 bits showing the least fragment undetected error probability. The packet undetected error probabilities were calculated after reconstructing the packet the receiver. The packet undetected error probabilities shows that the same CRC polynomial of length 32 bit has the least packet undetected error probability. But the fragment length of 1024 bit for each packet has the least probability. This shows that fragment undetected probability and packet undetected error probability result in different error performance. It was also seen that as the packet size increases packet undetected error probability decreases while fragment undetected error probability is vice versa. It can be inferred from these results that if the WSN device opts to use fragmentation then the best suitable length is fragment length of 512 bits with CRC polynomial of 32 bit length while without fragmentation the packet size of 1024 bits have the best performance. If the fragment, and packet undetected error probabilities can be derived, the occurrence of undetected error bits can also be evaluated. The results obtained in this thesis show that the least number of undetected error bits occur for fragment length of 512 bits with CRC polynomial 32 bit.

The energy consumption per bit for the fragmented sizes and the chosen polynomials (i.e., 8, 16, 24, and 32 bits) show that for different BERs different fragment lengths were found to be effective. The least energy consumption profile was seen for 8 bit CRC polynomial. The higher the length of the polynomial the higher was the energy consumption with higher reliability. The energy consumption results signify that fragment length of 512 bit with CRC polynomial of length 8 bit signifying the best performance compared to other fragment sizes and polynomials.

8. REFERENCES

[1] Massoud Amin S. & Wollenberg B. (2005) Toward a smart grid: power delivery for the 21st century. Power and Energy Magazine, IEEE 3, pp. 34 – 41.

[2] Momoh J. (2012) Smart Grid: Fundamentals of Design and Analysis. IEEE Press Series on Power Engineering, Wiley. URL: http://books.google.nl/books?id=j8IFx-6vMloC.

[3] Rafiei M., Elmi S. & Zare A. (2012) Wireless communication protocols for smart metering applications in power distribution networks. In: Electrical Power Distribution Networks (EPDC), 2012 Proceedings of 17th Conference on, pp. 1 –5.

[4] Depuru S., Wang L., Devabhaktuni V. & Gudi N. (2011) Smart meters for power grid; challenges, issues, advantages and status. In: Power Systems Conference and Exposition (PSCE), 2011 IEEE/PES, pp. 1 –7.

[5] IEEE draft standard for a convergent digital home network for heterogeneous technologies. IEEE P1905.1/D06, September 2012 , pp. 1 –125.

[6] Cuvelier P.K. & Sommereyns P. (2009) Proof of concept smart metering. In: Electricity Distribution - Part 1, 2009. CIRED 2009. 20th International Conference and Exhibition on, pp. 1 –4.

[7] Koay B., Cheah S., Sng Y., Chong P., Shum P., Tong Y., Wang X., Zuo Y. & Kuek H. (2003) Design and implementation of bluetooth energy meter. In: Information, Communications and Signal Processing, 2003 and Fourth Pacific Rim Conference on Multimedia. Proceedings of the 2003 Joint Conference of the Fourth International Conference on, pp. 1474 – 1477.

[8] Rusitschka S., Gerdes C. & Eger K. (2009) A low-cost alternative to smart metering infrastructure based on peer-to-peer technologies. In: Energy Market, 2009. EEM 2009. 6th International Conference on the European, pp. 1 –6.

[9] JoeHughes (2010), Smart metering requirements ,pap02objective1 (accessed on 01 Sep,2012)). URL: {http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP02Objective1/}.

[10] IEEE draft for local and metropolitan area networks-part 15.4: Low-rate wireless personal area networks (wpans) amendment physical layer specifications for low energy, critical infrastructure monitoring networks. IEEE D802.15.4k-2012 (Amendment to IEEE Std 802.15.4-2011) .

[11] 3GPP,LTE overview (accessed on 08 oct 2012). URL: {http://www.3gpp.com/LTE}.

[12] IEEE standard for local and metropolitan area networks–part 15.4: Low-rate wireless personal area networks (LR-WPANs). IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006) , pp. 1 –314.

[13] Sauter M. (2010) From GSM to LTE: An Introduction to Mobile Networks and Mobile Broadband. Wiley Online Library: Books, Wiley. URL: http://books.google.nl/books?id=uso-6LN2YjsC.

[14] Holma H. & Toskala A. (2009) LTE for UMTS: OFDMA and SC-FDMA based radio access. Wiley. URL: http://books.google.fi/books?id=AHr43Lh-roQC.

[15] 3GPP TS 33.401, "Digital cellular telecommunications system (phase 2+); universal mobile telecommunications system (umts); 3GPP system architecture evolution (sae); security architecture (release 8)". URL: http://www.etsi.org/deliver/etsi_ts/133400_133499/133401/08.01.01_60/ts_133401v080101p.pdf.

[16] Poikselkä M. (2006) The IMS: IP multimedia concepts and services. J. Wiley & Sons. URL: http://books.google.fi/books?id=lBMfAQAAIAAJ.

[17] Mobile WiMAX part 1: A technical overview and performance evaluation, WiMAX forum, white paper, august 2006, (accessed on 18 sept 2012). URL: {http://www.ictregulationtoolkit.org/en/Publication.2952.html}.

[18] Digital video broadcasting (DVB): Framing structure, channel coding and modulation for digital terrestrial television, etsi, ets en 300 744 v 1.1.2.

[19] Chang R.W. (1966) [duplicate] Synthesis of Band-Limited Orthogonal Signals for Multichannel Data Transmission. Bell Systems Technical Journal 45, pp. 1775–1796.

[20] Khan F. (2009) LTE for 4G Mobile Broadband: Air Interface Technologies and Performance. Cambridge University Press, New York, NY, USA, 1st ed.

[21] Dahlman E. (2008) 3G Evolution: HSPA and LTE for Mobile Broadband. Academic Press, Academic. URL: http://books.google.fi/books?id=cmMgp4j23D0C.

[22] Myung H. & Goodman D. (2008) Single Carrier Fdma: A New Air Interface for Long Term Evolution. Wireless Communications and Mobile Computing, John Wiley & Sons. URL: http://books.google.fi/books?id=Dotsv0dfH7kC.

[23] Mao R. & Julka V. (2011) Wireless broadband architecture supporting advanced metering infrastructure. In: Vehicular Technology Conference (VTC Spring), 2011 IEEE 73rd, pp. 1 –13.

[24] Wong K. (2004) Physical layer considerations for wireless sensor networks. In: Networking, Sensing and Control, 2004 IEEE International Conference on, vol. 2, vol. 2, pp. 1201 – 1206 Vol.2.

[25] IEEE standard for local and metropolitan area networks–part 15.4: Low-rate wireless personal area networks (LR-WPANs) amendment 1: Mac sublayer. IEEE Std 802.15.4e-2012 (Amendment to IEEE Std 802.15.4-2011) , pp. 1 –225.

[26] Choi S. & Shin K. (2001) A class of adaptive hybrid arq schemes for wireless links. Vehicular Technology, IEEE Transactions on 50, pp. 777 –790.

[27] Shu L. & Shu Lin D. Error Control Coding. Pearson Education India.

[28] Lee K.H., Hwang G.H. & Cho D.H. (2004) Type ii hybrid arq scheme based on qos and ldpc code. In: Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th, vol. 4, vol. 4, pp. 2630 – 2634 Vol. 4.

[29] Kallel S. & Haccoun D. (1990) Generalized type ii hybrid arq scheme using punctured convolutional coding. Communications, IEEE Transactions on 38, pp. 1938 –1946.

[30] Benedetto S. & Biglieri E. (1999) Principles of Digital Transmission: With Wireless Applications. Information Technology: Transmission, Processing, and Storage, Kluwer Academic/Plenum Press.

[31] Reed I.S. & Solomon G. (1960) Polynomial codes over certain finite fields. Journal of the Society for Industrial and Applied Mathematics 8, pp. 300–304. URL: http://www.jstor.org/stable/2098968.

[32] Geisel W. (1990), Tutorial on reed-solomon error correction coding, NASA technical memorandum 102162.

[33] Neubauer A., Freudenberger J. & Kuhn V. (2007) Coding Theory: Algorithms, Architectures and Applications. John Wiley & Sons. URL: http://books.google.nl/books?id=dPmdMQEACAAJ.

[34] Greenberg S., Feldblum N. & Melamed G. (2004) Implementation of the berlekamp-massey algorithm using a dsp. In: Electronics, Circuits and Systems, 2004. ICECS 2004. Proceedings of the 2004 11th IEEE International Conference on, pp. 358 – 361.

[35] Wu Y. (2012) Novel burst error correction algorithms for reed-solomon codes. Information Theory, IEEE Transactions on 58, pp. 519 –529.

[36] Komo J. & Joiner L. (1995) Fast error magnitude evaluations for reed-solomon codes. In: Information Theory, 1995. Proceedings., 1995 IEEE International Symposium on, p. 416.

[37] P.Elias "coding for noisy channels" , 1955 ire international convention record (part4) also reprinted, e.r berlekamp,ed., key papers in the development of coding theory, new york, : Ieee press ,1974 , pp. 39-47.

[38] Agarwal R., Popovici E., De Feo O. & O'Flynn B. (2007) Energy driven choice of error recovery protocols in embedded sensor network systems. In: Sensor Technologies and Applications, 2007. SensorComm 2007. International Conference on, pp. 560 –565.

[39] Balakrishnan G., Yang M., Jiang Y. & Kim Y. (2007) Performance analysis of error control codes for wireless sensor networks. In: Information Technology, 2007. ITNG '07. Fourth International Conference on, pp. 876 –879.

[40] Howard S.L., Schlegel C. & Iniewski K. (2006) Error control coding in low-power wireless sensor networks: when is ecc energy-efficient? EURASIP J. Wirel. Commun. Netw. 2006, pp. 29–29. URL: http://dx.doi.org/10.1155/WCN/2006/74812.

[41] Abughalieh N., Steenhaut K. & Nowe´ and A. (2010) Low power channel coding for wireless sensor networks. In: Communications and Vehicular Technology in the Benelux (SCVT), 2010 17th IEEE Symposium on, pp. 1 –5.

[42] Zorzi M. (1998) Performance of fec and arq error control in bursty channels under delay constraints. In: Vehicular Technology Conference, 1998. VTC 98. 48th IEEE, vol. 2, vol. 2, pp. 1390 –1394 vol.2.

[43] Opnet technologies (2011) opnet modeler version 16.1.,(accessed on 30 oct 2012). URL: {http://www.opnet.com}.

[44] 3GPP TR 36.888 v2.0.0 (2012-06) 3rd generation partnership project; technical specification group radio access network; study on provision of low-cost mtc ues based on lte; (release 11).

[45] Saunders S. & Aragón-Zavala A. (2007) Antennas And Propagation for Wireless Communication Systems. J. Wiley & Sons.

[46] Goldsmith A. (2005) Wireless Communications. Cambridge University Press.

[47] Project C.A.., European Commission. DGXIII "Telecommunications Information Society I.M. & Research" E. (1999) Digital mobile radio towards future generation systems: final report. Directorate General Telecommunications, Information Society, Information Market, and Exploitation Research.

[48] Rappaport T. (1991) The wireless revolution. Communications Magazine, IEEE 29, pp. 52 –71.

[49] Sarkar T., Ji Z., Kim K., Medouri A. & Salazar-Palma M. (2003) A survey of various propagation models for mobile communication. Antennas and Propagation Magazine, IEEE 45, pp. 51 – 82.

[50] Maxstream, "indoor path loss", technical report xstan005a-indoor, sept. 2003 (accessed on 10, july 2012). URL: http://digilander.libero.it/windflow/eng/Usage/RFIDSensor/Indoor%20Path%20Loss.pdf.

[51] Etsi TR 125.996,v8.0.0 - universal mobile telecommunications system (UMTS) spatial channel model for multiple input multiple output (MIMO) simulations. European Telecommunications 2009 1, pp. 0–41.

[52] Koubaa A., Alves M. & Tovar E. (2006) A comprehensive simulation study of slotted csma/ca for IEEE 802.15.4 wireless sensor networks. In: Factory Communication Systems, 2006 IEEE International Workshop on, pp. 183 –192.

[53] Peterson W. & Brown D. (1961) Cyclic codes for error detection. Proceedings of the IRE 49, pp. 228 –235.

[54] Nokia (1999), 3GPP TSG RAN WG1 proposal to add 24 bit crc polynomial (accessed on 10 august,2012). URL: //http://www.3gpp.org/ftp/tsg_ran/wg1_rl1/TSGR1_07/Docs/Pdfs/R1-99b47.pdf.

[55] ITU telecommunication standardization sector (ITU-T). URL: {http://www.itu.int/net/ITU-T/info/Default.aspx}.

[56] Lin R.D. & Chen W.S. (2005) Fast calculation algorithm of the undetected errors probability of crc codes. In: Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference on, vol. 2, vol. 2, pp. 480 – 483.

[57] Fujiwara T., Kasami T., Kitai A. & Lin S. (1985) On the undetected error probability for shortened hamming codes. Communications, IEEE Transactions on 33, pp. 570 – 574.

[58] Castagnoli G., Brauer S. & Herrmann M. (1993) Optimization of cyclic redundancy-check codes with 24 and 32 parity bits. Communications, IEEE Transactions on 41, pp. 883 –892.

[59] Chun D. & Wolf J. (1994) Special hardware for computing the probability of undetected error for certain binary crc codes and test results. Communications, IEEE Transactions on 42, pp. 2769 –2772.

[60] Kasami T. & Lin S. (1984) On the probability of undetected error for the maximum distance separable codes. Communications, IEEE Transactions on 32, pp. 998 – 1006.

[61] Wolf J., Michelson A. & Levesque A. (1982) On the probability of undetected error for linear block codes. Communications, IEEE Transactions on 30, pp. 317 – 325.

[62] Haapola J., Shelby Z., Pomalaza-Ráez C. & Mähönen P. (2005) Multihop medium access control for WSNs: an energy analysis model. EURASIP J. Wirel. Commun. Netw. 2005, pp. 523–540. URL: http://dx.doi.org/10.1155/WCN.2005.523.

[63] Sankarasubramaniam Y., Akyildiz I. & McLaughlin S. (2003) Energy efficiency based packet size optimization in wireless sensor networks. In: Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on, pp. 1 – 8.

[64] Chen P., O'Dea B. & Callaway E. (2002) Energy efficient system design with optimum transmission range for wireless ad hoc networks. In: Communications, 2002. ICC 2002, pp. 945–952, Vol.2.

[65] Yoon J., Kim H. & Ko J.G. (2007) Data fragmentation scheme in ieee 802.15.4 wireless sensor networks. In: Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th, pp. 26 –30.