OULUN YLIOPISTO
UNIVERSITY of OULU

DEGREE PROGRAM IN WIRELESS COMMUNICATIONS ENGINEERING

IMPLEMENTATION AND EVALUATION OF IEEE 802.15.4K PRIORITY CHANNEL ACCESS

Author ____________________________________
Berhane Gebremedhin

Supervisor ____________________________________
Jussi Haapola

Second supervisor ____________________________________
Prof. Jari Iinatti

Accepted _____ /_____ 2013

Grade ____________________________________

Gebremedhin G. (2013) Implementation and Evaluation of IEEE 802.15.4k Priority Channel Access. Master's Degree Programme in Wireless Communications Engineering, Department of Communications Engineering, University of Oulu, Oulu, Finland. Master's thesis, 86 p.

ABSTRACT

Critical infrastructures are assets whose disruption or malfunction poses a serious effect on the functioning of a society and its economy. Monitoring these infrastructures ensures their safety, reduces outage and maintenance costs, and speeds up restoration of interrupted services. Hence, the tendency of using wireless sensor networks (WSN) for low-energy critical infrastructure monitoring (LECIM) applications has been growing rapidly. LECIM networks aim at collecting scheduled and event-driven (high priority) data from a large number of endpoints spread over a wide area. LECIM applications require simple, low cost, and commissioned communication environment supporting long deployment time, large coverage area, low data-rate, asymmetrical data flow, multipoint-to-point communication, etc. However, the existing WSN standards and many other wireless technologies are unfit for LECIM networks for one or more of the following reasons: high power consumption, high cost, infrastructure complexity, low capacity, transmission range, and large payload etc. So, a new standard designed to serve mainly LECIM applications was necessary.

Recently, the Institute of Electrical and Electronics Engineers (IEEE) published the 802.15.4k standard to facilitate communication for LECIM devices. While it appears to have promising medium access control (MAC) layer and physical (PHY) layer specifications for LECIM devices, its suitability must be carefully evaluated. In this thesis work, the performance of LECIM direct sequence spread spectrum (DSSS) PHY layer with priority channel access (PCA) is evaluated. A star network topology supporting 750 endpoints and a collector is implemented in OPNET modeler. The model utilizes slotted Aloha with PCA algorithm. In addition, Rayleigh fading and Hata pathloss model for suburban area is used to model the channel. Due to the broadness of the standard, its fragmentation part is not included in this thesis. Instead, a payload size, which meets the PHY layer specification is used. For different network settings, the performance of LECIM DSSS PHY with PCA is analyzed and evaluated in terms of packet delivery ratio, success probability, delay, and throughput for varying number of retransmissions. Also, a Markov model for the same protocol is developed to analyze the network delay and throughput.

The results show that while user priority access brings a superior performance for high priority data, increasing the number of PCAs in the contention access period (CAP) has the opposite effect on the same data. Besides, the protocol is observed to offer low delay, low throughput, and poor performance in last gasp messaging applications where all network nodes attempt to access the channel simultaneously.

Keywords: LECIM, MAC, WPAN, critical infrastructure, priority access.

TABLE OF CONTENTS

PREFACE

This Master's thesis has been done at the Centre for Wireless Communications (CWC), University of Oulu under the project Smart Grids and Energy Markets (SGEM). I am so grateful to the SGEM project for providing me with the necessary mentorship and fund for this thesis work. I would like to express my utmost gratitude to my supervisor Jussi Haapola (Dr. Tech), who is the SGEM project manager, for supervising the thesis. His inspiration, insight, expert attitude, and friendly approach towards the research work was very encouraging. I would like to sincerely thank Professor Jari Iinatti for being my second supervisor and providing me his expert opinion and excellent feedback of the thesis work, and for being around me whenever I needed his help. I am also thankful to Juho Markkula and Tuomas Paso for their technical support, advice, and for providing me the necessary materials for this work.

November 27, 2013
Berhane Gebremedhin

LIST OF SYMBOLS AND ABBREVIATIONS

ACK	acknowledgment
AMCA	asynchronous multi-channel adaptation
BE	backoff exponent
BER	bit error rate
BI	beacon interval
BMA	bit-map-assisted
BO	beacon order
BPSK	binary phase shift keying
CAP	contention access period
CCA	clear channel assesment
CFP	contention free period
CH	cluster head
CSMA	carrier sense multiple access
CSMA/p	p-persistent CSMA protocol
CSMA-CA	carrier sense multiple access with collision avoidance
CTS	clear to send
CW	contention window
CWC	center for wireless communications
DEMAC	distributed energy aware MAC
DEV	device
DLL	data link layer
DMAC	data gathering MAC protocol
DSME	deterministic and synchronous multi-channel extension
DSN	data sequence number
DSSS	direct sequence spread spectrum
EA-TDMA	Energy efficient adaptive TDMA
E-BMA	energy efficient bit-map-assisted
ED	energy detection
FCF	fragment context frame
FCS	frame check sequence
FEC	forward error correction
FFD	full function device
FHSS	frequency hopping spread spectrum
FSK	frequency shift keying
FSM	finite state machine
FVS	fragment validation sequence
GFSK	gaussian FSK
GTS	guaranteed time slot
HR-WPAN	high rate WPAN
I-ACK	fragment incremental acknowledgement
ID	identification
IE	information element
IEEE	institute of electrical and electronics engineers
ISM	industrial, scientific, and medical
LCD	liquid crystal display

LECIM	low energy critical infrastructure monitoring
LIFS	long interframe spacing
LLC	logical link control
LLDN	low latency deterministic network
LR-WPAN	low rate WPAN
MAC	medium access control
MATLAB	MATrix LABoratory
MBWA	mobile broadband wireless access
MFR	MAC Footer
MHR	MAC header
MPDU	MAC protocol data unit
MSDU	MAC service data unit
NACK	not acknowledged
nData	n consecutive data frames
np-CSMA	non-persistent CSMA
OPNET	optimized network engineering tool
O-QPSK	offset quadrature phase shift keying
PACT	power aware cluster TDMA
PAN	personal area network
PC	personal computer
PCA	priority channel access
PDA	personal digital assistant
P-FSK	position-based FSK
P-GFSK	position-based GFSK
PHR	PHY header
PHY	physical layer
PIB	PAN information base
PNC	piconet coordinator
POS	personal operating space
PPDU	PHY protocol data unit
ppm	parts per million
PSDU	PHY service data unit
QoS	quality of service
RF	radio frequency
RFD	reduced function devuce
RFID	radio frequency identification
RTS	request to send
S-Aloha	slotted aloha
SAP	service access point
SCADA	supervisory control and data acquisition
SD	superframe duration
SFD	start-of-frame delimiter
SHR	synchronization header
S-MAC	sensor-MAC protocol
SO	superframe order
Std	standard
STEM	sparse topology and energy management

SUN	smart utility network
TB	total backoff
TDMA	time division multiple access
TG	task group
THz	tera Hertz
TID	transaction identifier
T-MAC	time-out MAC protocol
TRLE	time-slot relaying based link extension
TSCH	time slotted channel hopping
UWB	ultrawide band
VPAN	VLC personal area networks
WBANs	wireless body area networks
WiseMAC	wireless MAC protocol
WLAN	wireless local area network
WMAN	wireless metropolitan area network
WPAN	wireless personal area network
WRAN	wireless regional area network
WSN	wireless sensor network
WWAN	wireless wide area network
Z-MAC	hybrid MAC

B	number of busy time slots
$b(t)$	a random process representing the backoff counter of a given user
$b_{i,k}$	stationary prob of the (i,k) state
b_{I}	stationary distribution of the idle state
$ChanCenterFreq$	channel center frequency in MHz
D	MAC delay
$D_{\mathrm{e2e\_emerg}}$	average end-to-end delay of emergency packets
$D_{\mathrm{e2e\_normal}}$	average end-to-end delay of normal packets
D_{e2e_i}	end-to-end delay of the i^{th} packet
D_{e2e}	average end-to-end delay
D_i	sum of all delay times experience in i backoff stages
$D_{\mathrm{MAC\_emerg}}$	MAC delay of emergency packets
$D_{\mathrm{MAC\_normal}}$	MAC delay of normal packets
D_{MAC_i}	MAC-to-MAC delay of the i^{th} packet
D_{MAC}	average MAC-to-MAC delay
$D_{\mathrm{Q\_emerg}}$	queueing delay of emergency packets
$D_{\mathrm{Q\_normal}}$	queueing delay of normal packets
h_{b}	base station antenna height
h_{m}	sensor node antenna height
I	number of idle time-slots
m	number of PCAs in one CAP period
N	number of users in the network
n	packet service time in slots
$p_{\mathrm{col_e}}$	probability of collision for emergency packets

p_{col}	probability of collision
p_{E}	probability of emergency packet transmitted
p_{e}	probability of error
$p_{\text{emerg\_gen}}$	probability of emergency packet generation in the non-PCA period
$p_{i,k}$	transition probability of the $(i{,}k)$ state
p_i	probability of packet transmission from backoff stage i
p_l	probability of generating emergency packet during $E[D_{normal}]$
p_{PCA}	probability of the next time-slot lies in one of the allocated PCAs
p_{q_e}	probability of emergency queue not empty
p_{q}	probability of queue not empty
p_{R}	probability of normal packet transmitted
p_{s_e}	probability of success for emergency packets
P_{s}	success probability
p_{s}	probability of success
p_{suc_e}	conditional probability of success for emergency packets
p_{suc_o}	overall conditional probability of success
p_{suc}	conditional probability of success for normal packets
p_{t_e}	prob. of transmitting at least one emergency packet in a give time-slot
p_{t_o}	overall prob. of transmitting at least one packet in a give time-slot
p_{t}	probability of transmitting at least one packet in a give time-slot
PDR	packet delivery ratio
$Pkt_{\text{generated}}$	total generated packets
Pkt_{received}	total received packets
Pkt_{sent}	total sent packets
S	throughput
$s(t)$	a random process representing the size of a contention window
T_{ACK}	ACK duration
T_{AckWait}	ACK waiting time
T_{BP}	the duration of *aUnitBackoffPeriod*
T_{c}	time wasted when a transmitted packet collides
T_{IAT}	total number of slots in one expected packet inter-arrival time
$T_{\text{MAC\_HEADER}}$	MAC header fields duration
T_{minLIFS}	the minimum duration of an LIFS period
$T_{\text{PAY\_LOAD}}$	payload bits duration
T_{PCA}	duration of one PCA
$T_{\text{PHY\_HEADER}}$	PHY header fields duration
T_{s}	time taken to successfully transmit a packet
T_{slot}	duration of one time-slot
$T_{\text{superframe}}$	SD in seconds
T_{TAT}	maximum turnaround time from RX-to-TX mode or vice-versa
U	number of useful time-slots
W_i	contention window at backoff stage i

α	probability of packet arrival in one time slot
α_{e}	probability of emergency packet arrival in one time-slot
γ	pathloss exponent
λ	packet arrival rate
τ_{E}	probability of a node transmitting an emergency packet in a given time-slot
τ_{p}	propagation delay
τ_{R}	probability of a node transmitting a normal packet in a given time-slot

$\lceil\;\rceil$	closest integer greater than or equal to the argument
$\lfloor\;\rfloor$	closest integer less than or equal to the argument
$E[\;]$	the expected value of

1. INTRODUCTION

Consider the heating system, internet connection, electric supply, water supply, the gas supply we use in our houses, or the connectivity to our mobile phones. We use these services in our day-to-day life without thinking about the infrastructures enabling them. What if something goes wrong with these critical infrastructures, how difficult our life would it be? Fortunately, service disruption or malfunction happens very rarely. However, due to manmade [1] or natural causes, the services we get from such facilities can be interrupted. Not only that, much of the good life that the developed countries enjoy heavily depend on the functioning of a number of interdependent critical infrastructures. If one of them fails, it may result in a disastrous effect by cascading throughout the infrastructures network. Therefore, they have to be protected; they have to function 24 hrs a day, 7 days a week. For this, monitoring them is of high importance. Monitoring these infrastructures ensures their safety, reduces outage and maintenance cost, and speeds up restoration of interrupted services.

One of the technologies that have to be used to monitor critical infrastructures are wireless sensor networks (WSN) [2]. This is because WSNs can provide simple, cost-effective, and easy-to-deploy monitoring networks. However, due to many reasons which will be explained in next sections, the existing WSN standards are not suitable for critical infrastructures monitoring. Recently, the Institute of Electrical and Electronics Engineers (IEEE) adopted IEEE 802.15.4k standard [3] as communication protocol for low energy critical infrastructure monitoring (LECIM) networks. While it appears to have promising medium access control (MAC) layer and physical layer (PHY) specifications for LECIM networks, its suitability must be carefully evaluated.

In this thesis work, the performance of LECIM direct sequence spread spectrum (DSSS) PHY with priority channel access (PCA) is evaluated. While using a slotted Aloha (S-Aloha) with PCA channel access mechanism, a star network topology supporting 750 endpoints and a collector is implemented in OPNET modeler [4]. Besides, a numerical analysis for the same system is developed.

The thesis is structured as follows: Chapter 2 introduces wireless sensor networks (WSN) and different medium access control (MAC) protocols. It discusses the characteristics and requirements of WSNs used in structural and wide area monitoring, and presents a survey of MAC protocols for structural and wide area monitoring applications. In Chapter 3, Wireless personal area network (WPAN) and low energy critical infrastructure monitoring (LECIM) are explained, the role of WPAN in LECIM applications discussed, and existing wireless technologies reviewed. Chapter 4 describes the IEEE 802.15.4k standard with more emphasis on the MAC layer and physical layer (PHY) specifications relevant for the thesis. In Chapter 5, the system simulation and analytical models are discussed. Chapter 6 presents the simulation parameters used in the simulator, performance metrics, the results of different simulation scenarios and their detailed discussion. Finally, a summary of the thesis is explained in Chapter 7. Also, a derivation to some of the equations in the thesis are provided in the appendix.

2. WIRELESS SENSOR NETWORKS FOR STRUCTURAL AND WIDE AREAS MONITORING

This chapter focuses on WSNs MAC protocols proposed for structural and wide areas monitoring applications. Sections 2.1 and 2.2 present an overview and applications of WSNs. While Section 2.3 discusses the major sources of energy waste in WSN MACs, Section 2.4 discusses design requirements of an efficient protocol. Finally, a survey of different MAC protocols is presented in Section 2.5.

2.1. Overview

In recent years wireless sensor networking has become an appealing research area due to its wide range of applications. A common architecture of an WSN consists of many miniaturized, small battery-powered sensing devices which are distributed in the sensor field, collaborating to accomplish a common task, i.e. probing the environment and transmitting the collected information wirelessly to a mains-powered central node, the coordinator. Unlike conventional wireless networks, the wireless means of communication (it can be between sensor nodes or between a sensor node and the coordinator) liberates such networks from the constraints of wires enabling them to be deployed in locations which are appropriate for the intended application. As a result, WSN have become ideal for applications such as in disaster management, target detection and tracking, wide area environmental monitoring, industrial process monitoring, medical systems, and home automation. For example, in structural health monitoring, we can deploy such systems to effectively monitor bridges, tunnels, and highways enabling civil engineers to remotely monitor the status of the structures. They can also be deployed to monitor office buildings, hospitals, airports, factories, power plants, airports and, other utilities. [2, 5, 6]

However, WSN systems also have their own constraints which have to be considered during the system design. The sensor nodes are deployed in an unattended setup. The lifetime of a node in the network is highly dependent on the batteries. In such networks it is generally hard or not practical replacing or charging exhausted batteries. Therefore, energy conservation is a critical design issue of the system. In the past, this has motivated a lot of researchers to develop many energy-aware protocols in all the layers of the communication stack [7–10]. Given the fact that the radio unit is a most power consuming part of a sensor node, a large energy conservation gain can be obtained at the MAC layer where the MAC protocol takes care of the radio link utilization [11, 12]. As a result, with the ultimate goal of energy minimization and thereby increasing the lifetime of the network, several MAC protocols for wireless sensor networks have been proposed in the literature. Many other MAC schemes with different objectives are also utilized in sensor networks [13, 14].

While other networks try to achieve Quality of Service (QoS) provisions and bandwidth efficiency, the primary objective of most of WSN MAC protocols is prolonging the lifetime of the network, leaving the other system performance metrics as secondary objectives [15–17].

Like in all shared networks, the MAC layer in sensor networks takes an important role in improving the overall performance of the system. In such systems, the protocol should support diverse applications, and variable but highly correlated and dominantly periodic traffic along with high level QoS. Some WSNs follow a query-based data collecting mechanism; others follow event-driven communication mechanism. In query-based data collection mechanism, the endpoints send their messages only when they receive a request from the sink; whereas in the event-driven communication scheme, the endpoints send a message when they detect the event in target. Regardless of the type of application or the type of the sensor network, every MAC protocol has the following fundamental tasks. The first is sharing the resources of the network fairly and efficiently among the sensor nodes. This helps them to avoid collisions by preventing simultaneous transmissions of interfering nodes while maintaining minimum latency, maximum throughput, reliable communication, and efficient utilization of energy. The second goal of a MAC layer is creating the network infrastructure, and thus establishing a communication link for data transfer between concerned nodes [2].

2.2. Application of WSNs

WSNs can be used to monitor wide areas or different types of structures. The sensor fields of such networks are deployed in unattended and critical regions. The sensor nodes and the monitoring center are then linked wirelessly. According to the requirement of the application, the WSNs consist of one or more sink nodes and large number of sensors which are distributed in the target area. Sensor nodes are typically battery-powered, and these batteries are not easily replaceable. Therefore in monitoring WSNs, energy saving is a major issue during communication among the devices so that the batteries do not drain quickly. Sensor nodes send gathered data to the base station (sink). Sinks are mains-powered, have more advanced transmitting and data processing capabilities, and more memory-size than the sensors. Depending on the employed network topology, the sensor nodes can use a single-hop or multi-hop paths for data transmissions. [18]

WSNs can operate in two monitoring models: a regular continuous model and an event-driven model. In a regular continuous monitoring model, sensor nodes either periodically transmit data to the sink or only transmit collected data on request. This type of model is used in applications where a continuous or regular report of the event is needed. Whereas in an event-driven model, sensors transmit critical-event messages to the sink when the target event occurs. In most event-driven monitoring applications, the target events are very rare. During most of the monitoring time sensor nodes are idle; in the meantime they either forward keep-alive messages to the sink or wait for request messages from the sink. The traffic flow, in this case, is very low and a regular continuous model is applied. When the target event is detected, sensors alert the sink by sending a report of the event simultaneously, thereby creating a burst data transmission in the medium. In such moments, the network should apply an event-driven model to handle the high traffic flow. [19]

In general, WSNs engaged in monitoring applications experience fluctuating data traffic and should be capable of handing the extreme scenarios. In the literature several studies are made on event-driven models. For example, in soil moisture estimation and wetland monitoring [20], sensors are used to monitor soil moisture level; in a volcanic event monitoring system [21], sensors are used to monitor volcanic activities; in a coffee factory application [22], sensors are employed to monitor water quality, humidity, air temperature, etc in different parts of the factory; in surveillance applications [23]; and in other environmental monitoring applications [24].

2.3. Sources of energy waste

As stated above, the sensor nodes are battery-powered, and thus energy is a critical resource that has to be utilized efficiently. However, there are different sources of energy waste [18, 25]: collision of packets, overhearing, idle-listening, control packet overhead, overmitting and frequent switching of modes.

Packet collision - whenever two or more nodes transmit simultaneously, the packets collide, even when they coincide partially. In some cases due to the capture effect phenomenon one of the packets is recovered otherwise the packets are corrupted and they have to be retransmitted. Packet collision is the most dominant source of energy waste. *Overhearing* occurs when nodes unnecessarily try to hear packets which are destined to other nodes, this effect is worst in dense networks and/or when the data traffic is high. Transmitting and receiving a packet consumes much more energy than when a node is either in a sleep or idle mode. But when the node listens the channel excessively thinking that a packet will arrive also causes a significant amount of energy loss. This is called *Idle-listening*, and to avoid it the receiver should be turned off during the idle state. However, in some cases too *frequent switching of modes* of the sensor node becomes more energy consuming than leaving the transceiver in the idle state. When the node switches from a sleep mode to an active mode, a significant amount of energy is lost.

For a reliable data transmission control packets are used. However, as these packets do not carry any data information, the MAC layer should use minimum number of them. The energy wasted to transmit or receive these packets is termed as *Control packet overhead*. *Overmitting* in sensor networks results in when a packet is transmitted while the receiver is not ready, sleeping, dead, or out of range. So it should be avoided to minimize energy consumption. According to [26], *Traffic fluctuation* is also a cause of energy waste in WSNs. In some applications the traffic generation varies with time, which at times results in peak offered loads that may derive the system into congestion, and thereby causing huge packet collisions. The overall effect is wasting much time and energy of the system in the back-off procedure.

2.4. WSN MAC protocol design requirements

Because of the resource constraints and application requirements of sensor networks, an efficient MAC protocol design is very crucial for a longer lifetime, performance, and better failure, and mobility management. For all the design constraints, a good MAC protocol is expected to consider a set of performance attributes and make trade-offs among them [16, 27, 28]. As a general rule, the design of a good MAC protocol has to consider that nodes have limited energy sources and processing capabilities, are prone to failures, are large in number and densely deployed, and network size and topology may change.

- **Energy efficiency**: The lifetime of battery-powered nodes depends on how efficiently they use their limited energy resource. Once the batteries are exhausted, it may not be easy to replace or recharge them. As explained earlier, MAC layer controls the shared medium and the radio is the major power consumer, especially when the receiver is kept on all the time. So, the prime design attribute of MAC protocols in WSNs is energy optimization especially under low traffic loads. Such protocols are designed by considering the possible causes of energy wastes described in Section 2.3.

- **Scalability**: The number of sensing nodes can change over time. This can be due to the limited node lifetime or due to the nature of the application. This fluctuation in network size can affect the way resources i.e. time and bandwidth, are shared among the nodes. In some cases also it can impose a restriction on the type of MAC protocol to be used. Therefore, a scalable protocol which adapts for such node density variation is crucial for a fair resource allocation and excessive packet collisions prevention.

- **Adaptability**: In some applications, node mobility can change the network topology. In other applications like in structural monitoring and surveillance applications, the traffic density may not be uniform all the time. For example, a sensor network installed on a certain infrastructure to monitor fire detection behaves differently. During normal conditions the nodes send periodic data, which may be a low traffic to the central node, and therefore does not affect the operation of the network. However, whenever fire is detected it is likely that all the nodes report the event-driven messages simultaneously; this leads to a high traffic flow. So, a well-designed MAC protocol has adaptation schemes to node mobility, node failure, and traffic density variation without sacrificing much energy efficiency especially with low traffic loads.

- **Delay predictability**: In sensor networks, latency is application dependent. Some applications require delay-bounded data delivery, to others it may not be even a performance attribute. The delay experienced during a packet transmission is a contribution of all the delays occurring in various layers of the communication stack. Unless special routing techniques are employed in network layer, long queuing delay, for example, has a significant effect on the end-to-end delay [29, 30]. However, the majority of the end-to-end delay is contributed by the MAC layer. A well-designed MAC protocol tries to avoid packet collisions and thus maximizes the network performance by applying a careful packet scheduling technique for medium arbitration. If some packets or services need prioritizing or a special way of handling, the MAC scheme handles it. The employed packet scheduling strategy affects the rate at which packets in the buffer get serviced. The amount of delay experienced at the MAC layer is a trade-off with the other performance attributes like reliability, energy consumption, and throughput.

- **Reliability**: Reliability is a measure of how many of the packets generated by the sensors in the sensor field are successfully received by the sink within a predefined delay bound. In sensor networks especially in systems engaged in critical-event monitoring, a reliable packet delivery can be ensured by applying control traffic overhead, sending redundant reports, carefully selecting error free links, or by applying different error detection and correction mechanisms. However, guaranteed packet delivery with the application of control traffic overheads, for example, is achieved at the cost of increased energy consumption, increased end-to-end delay, a lower effective link bandwidth, and system complexity.

In monitoring WSN applications, even though the performance attributes and the trade-offs they make among them are application dependent, the above design requirements are common to all MAC protocols. Others like throughput, bandwidth efficiency and fairness are of secondary importance. In event-driven monitoring applications latency, reliability and energy efficiency are critical requirements of the MAC protocols.

2.5. Survey of MAC protocols

A wide range of MAC layer protocols have been proposed in the literature for different WSN applications. MAC protocols can be classified in many ways: based on channel access method, based on power saving method, etc. Based on the channel access method, [18] divides WSN MAC protocols into two major groups: solitary MAC protocols and cross-layer MAC protocols. Each group is again subdivided into scheduled (or contention-free), contention-based (or random), and hybrid protocols. Solitary protocols are specific to the MAC layer, and they are designed by considering only the constraints set by layers from below and above; whereas cross-layer protocols are designed by considering two or more layers. In this thesis, the MAC protocols are grouped into contention-based, scheduled, and hybrid protocols. Accordingly, a summary of the existing MAC protocols in their respective group is given in [18].

In scheduled MAC protocols, the communication between sensor nodes is made in an ordered way, and the scheduling is mostly based on the TDMA scheme, where each node is allocated at least one slot in a time frame. These types of protocols are inherently energy conserving as they reduce wastage due to collisions, idle listening, and over-hearing, and this is obtained at the cost of synchronization and previous knowledge of network topology. Unscheduled MAC protocols use different mechanisms to access the shared medium and to conserve energy by letting the sensor nodes to operate independently and with minimum complexity. Examples include Aloha, S-Aloha, carrier sense multiple access (CSMA), and others. In random protocols though there is energy loss due to collisions and idle listening, synchronization nor topology knowledge is not mandatory. These protocols are scalable and good for large-scale networks. Hybrid MAC protocols are aimed at combining the strengths of scheduled and random protocols while compensating their weakness to design an efficient MAC protocol. These protocols try to optimize different parameters to obtain the required network performance. The major advantage of these protocols comes from its simple and rapid adaptability to data traffic. This behavior enables them to save a large amount of energy. In this section, only MAC protocols which have relevance in the areas of structural and wide area monitoring will be reviewed.

2.5.1. Contention-based MAC protocols

Contention-based MAC protocols use different channel access techniques to minimize collision. Some of these protocols include Aloha, CSMA or their variants. If we take CSMA, for example, it is used in many WSNs because it does not require much infrastructure support; no previous knowledge of topology is required; and has better scalability and adaptability to topology changes without strict synchronization requirement. However, the above benefits are obtained at the expense of access collisions. Even though collisions among one hop nodes can be greatly minimized by carrier sensing, it does not work beyond one hop. So, contention-based protocols have hidden/exposed terminal problem. One way of tackling this problem is by using collision avoidance schemes like RTS/CTS handshaking.

Contention based protocols, in general, have the following advantages: they assign resource on-demand; at low traffic loads which is typical of WSNs, they offer low latency with good throughput property; they have better scalability to topology changes and better adaptability to changing traffic loads than scheduled protocols. The major disadvantages of unscheduled protocols are resource allocation unfairness and energy inefficiency. In this subsection, some representative contention-based protocols will be discussed.

Duty-cycled MAC protocols

MAC protocols like Sensor MAC (S-MAC) [17], Time-out MAC (T-MAC) [31], and Optimized MAC protocol [32] are duty-cycled contention-based protocols. They are synchronized protocols. They conserve energy by making the nodes to periodically go into a listen/sleep cycle, enabling the nodes to use their radio transceiver at low duty cycles. The protocols divide the time into frames. Nodes which have data for transmission wake up at the beginning of each frame and compete for channel access.

S-MAC is designed for low power operation in WSNs. The low power operation is obtained by employing a fixed low duty cycling. Its basic operation is based on the carrier sense multiple access with collision avoidance (CSMA-CA) principle. Neighboring nodes build virtual clusters to set up the common sleep schedule. In a virtual cluster, nodes have the same schedule. Neighboring nodes which reside in more than one virtual cluster take multiple schedules and wake-up during the active periods of all clusters. To synchronize with its neighbors, a node periodically broadcasts SYNC packets to exchange the schedule. Consequently, nodes periodically sleep in a coordinated manner. Messages enqueued during the relatively large sleep time are then transmitted in the next short active period. Furthermore, S-MAC applies the RTS/CTS mechanism for channel arbitration and hidden terminal avoidance. An important feature of this protocol is it provides message fragmentation for efficiently transferring bulk data in a burst, achieving energy savings by minimizing control packets at the expense of unfairness in channel access. S-MAC reduces energy waste due to idle listening, over-hearing, collision, and control packet overhead by using the listen/sleep scheme, in-channel signaling to let each node sleep when its neighbor communicates with another node, synchronization mechanism, and the RTS/CTS channel arbitration scheme respectively. However, these benefits are obtained at the cost of reduced throughput and higher latency.

Because of the fixed duty cycle it uses, S-MAC is not a suitable protocol for varying traffic load networks. For example, in structural and wide area monitoring applications an event can occur randomly; and if we use S-MAC for this purpose, then the node will waste most of its energy in the idle state. If we set the duty cycle for higher traffic load and the network experiences low traffic, then the node wastes energy in idle listening. Alternatively, if we set the duty cycle for low traffic condition and high traffic is experienced, then the latency increases which leads to a low QoS. Therefore, the protocol is suitable only for normal traffic conditions.

T-MAC is proposed to overcome the shortcomings of S-MAC. It inherits most of the features and working principle of S-MAC. Unlike the fixed duty cycle in S-MAC, T-MAC is designed to enhance adaptive duty cycling so that it solves the poor performance observed in S-MAC when the traffic load varies. The active period in T-MAC ends when no event is detected for a time interval of *Time-Out*, the node goes to sleep to save energy even if the active period is not over yet . On the other hand, if the node detects an event or when there is high traffic load, the node communicates continuously without going to a sleep mode and starts a new *Time-Out* when that communication is over.

In T-MAC, nodes send their queued packets in bursts at the beginning of each frame which increases the traffic load. Besides, nodes exchange RTS/CTS packets to avoid collision, and an ACK to achieve a reliable transmission. In addition to saving energy, adaptive duty-cycling enables nodes to adapt fluctuating traffic conditions. T-MAC has an early sleep problem i.e. a node sleeps even if a neighboring node has a message to send. As a result, T-MAC has higher latency than S-MAC. To avoid early sleeping problem, a node uses the *future request to send* (FRTS) control packet to inform the next hop that it has a future packet to send. T-MAC outperforms S-MAC in fluctuating traffic conditions. With a careful selection of *Time-Out*, T-MAC can be used for wide area monitoring applications.

Optimized MAC is also an improved and optimized version of S-MAC. It tries to adjust the sensor node duty cycle based on the system traffic conditions. For high data traffic the node's duty cycle increases, and for low traffic the duty cycle decreases. The traffic status is determined based on the number of queued packets in a specific node. Simulation results in [33] show that Optimized-MAC achieves a high energy efficiency under wide range of traffic loads and is able to improve the network delay performance by automatically adjusting its duty cycle in high traffic load situations. This indicates that it can be a good candidate protocol for event-driven WSN applications.

NanoMAC protocol [18, 34] is proposed for a fully distributed WSN, and uses CSMA-CA (*p*-nonpersistent) algorithm for channel access. It shares many features with S-MAC. For data communication, it follows RTS/CTS/nData/ACK operation cycle. Supporting broadcast messages, reduced overhearing, low overhead, virtual and physical carrier sensing capability, and applying frame train structure with block ACK/NACK are some of its features. When a sensor has a packet to transmit, the packet is first divided into $35-$bytes fragments. After applying carrier sensing using *p*-nonpersistent CSMA-CA, the sensor applies the RTS/CTS/nData/ACK cycle, i.e. after the RTS/CTS, the first n fragments are transmitted consecutively as a train, followed by a single ACK frame which consists of ACK/NACK for each data frame. NanoMAC can support large number of users and it operates at low data-rate, which are both good features for monitoring applications.

Next, suitability of duty-cycled protocols for wide area monitoring is summarized. S-MAC and NanoMAC are suitable only for scheduled data monitoring, whereas T-MAC and Optimized MAC are adaptive to traffic changes, and thus they can be used in scheduled or in event-driven monitoring WSNs. Duty-cycled protocols are suitable only for one-hop networks. If applied in multi-hop networks, high delay and hidden terminal problem reduces the network performance.

Event-driven MAC protocols

Unlike the MAC protocols used in regular continuous monitoring model, which are more concerned with energy efficiency, the protocols used in event-driven monitoring model must comply with the latency and reliability requirements of applications while minimizing the energy consumption, because latency and reliability are also critical. WSNs engaged in monitoring applications have very low traffic most of the time, but experiences very high traffic when the target event occurs. So event-driven protocols are designed with a notion of the network characteristics. SIFT [35], Alert MAC [36], Sparse Topology and Energy Management protocol (STEM) [37], and *p*-persistent CSMA Protocol (CSMA/p) [38] are some of the contention-based protocols proposed for this application.

When an event is detected, SIFT considers that the first R of M potential reports sufficiently represents the alert and tries to deliver it with low latency and less collision. To meet this objective, it employs a slotted fixed-size contention window and a non-uniform probability distribution of transmitting in each slot. If a slot is sensed idle, then in the next slot the transmission probability of each node increases exponentially assuming that the number of nodes is small. SIFT offers very low latency for many traffic sources, which is good for emergency messaging, has good adaptivity to changes. SIFT is adaptive to changes. It trades off between latency and energy efficiency. The protocol suffers from increased idle listening and overhearing, which reduce its energy efficiency. Also, system-wide time synchronization increases its system complexity.

Alert MAC is used to collect event-driven emergency messages from the sensing nodes with minimum delay and without any cooperation or pre-scheduling among any of the nodes. It uses a combination of time and frequency multiplexing to reduce channel contention among the nodes. The protocol divides the time into slots, which is large enough to make a message-ACK pair transmissions. The benefits of using an Alert MAC are many: it reduces the message collecting delay; the fact that it is a non-carrier sense protocol eliminates the hidden terminal problem; the dynamic frequency shifting offers robustness against interferences; and the adaptive nature enables operation without the knowledge of the number of users.

Event-driven protocols are suitable for wide area monitoring because they offer low latency with a reasonable energy consumption, and they have good adaptivity to traffic changes.

Preamble sampling MAC protocols

Preamble sampling or channel polling protocols have unsynchronized duty-cycles. In preamble sampling technique, data transmission is preceded by preambles to alert the receiving node. To reduce power consumption, sensor nodes sleep most of the time and periodically probe the channel to synchronize themselves with their neighbors. Once the nodes know that each one is awake, they start communicating. Berkeley MAC (B-MAC) [39], Wireless sensor MAC (WiseMAC) [40], and Aloha with preamble sampling [41] are examples of preamble sampling protocols.

B-MAC uses periodic channel sampling and very long preambles to achieve low power communication in monitoring applications. The sensor nodes can follow their sleeping schedule independently. In B-MAC, the source node sends a preamble long enough that the receiver, which wakes up at every check-for-preamble interval and samples the channel, has enough time to wake up and detect the preamble. Sensor nodes that sense the preamble remain active to receive the data following the preamble. After reception of a data or if no preamble is detected, the receiver returns to sleep. The channel sampling interval and thus the length of the preamble are important design parameters of the protocol.

WiseMAC is a low power, single channel contention protocol which combines nonpersistent-CSMA (np-CSMA) technique with preamble sampling to mitigate idle listening. All nodes periodically sample the medium to check for activity. To reduce the power consumption incurred due to the fixed-length preamble, the novel idea wiseMAC offers is to dynamically determine the preamble length based on the information of the sampling schedule table of its neighbors. Neighboring nodes learn and update their sleep schedules by ACK packets during every data transfer. Transmissions are scheduled in such a way that receiving nodes sample the channel at the middle of the sender's preambles. The decentralized sleep/work scheduling results in different sleep and wake-up times, and hidden terminal problem are its main drawbacks. Additionally, WiseMAC functions in one-hop WSNs.

Aloha with preamble sampling combines an Aloha protocol with preamble sampling technique to achieve low power sporadic communication in an ad hoc WSN. The goal is to have the sensor nodes in their sleep mode most of the time, and to wake up periodically to listen a preamble. This protocol is designed for low traffic WSN. The author analytically derived throughput, delay and power consumption of the protocol, and compares its delay, power consumption, and life-time performance with Aolha, CSMA, and np-CSMA.

Aloha with preamble sampling and B-MAC are optimized for light traffic networks, they have good energy efficiency in regular continuous monitoring WSNs. Besides, WiseMAC is scalable and adaptive to varying traffic loads while providing comparable energy efficiency at low and high traffic loads. So, they can be used in wide area monitoring WSNs. However, performance limitation under dynamic traffic loads is also observed in many preamble sampling protocols.

2.5.2. Scheduled MAC protocols

Scheduled protocols, which use some form of TDMA [25], minimize energy consumption by making all the sensor nodes to follow a common schedule. TDMA divides the shared channel into frames; each frame is subdivided into slots. Each node is assigned a time slot in each frame and that node can send or receive packets only in its own slot. When there is no activity the node turns off its transceiver to save power [42]. The coordinator stays on all the time to coordinate the network. As a result, packet collision, idle-listening, and over-hearing are avoided. In scheduled protocols synchronization is very crucial to maintain the schedule. Any clock drift results in a serious problem. Node mobility, node redeployment, and node death complicates the schedule and hence they are not scalable or adaptive protocols. Such node activities result in unnecessary delays due to the unused time slots, and packet drop.

In TDMA-based protocols, nodes form clusters in which each cluster has its own coordinator. The coordinator allocates time slots to the nodes, and coordinates all activities in the cluster. Communication is limited only between nodes and the coordinator. The coordinator collects all data from the nodes and forwards the aggregated and compressed data to the base station. This hierarchical organization complicates their usage in multi-hop ad-hoc networks where peer-to-peer communication is supported; nodes are equal and have limited resources. Some of the TDMA-based MAC protocols are discussed as follows.

Distributed energy aware MAC (DEMAC) protocol [43] employs the TDMA scheme for channel access. In a normal operation mode, a node can switch off its radio and go into a sleep mode only if it is in its pre-assigned slot and has no task to do. During the time slots assigned to its neighbors, the node stays awake and is set in the receive mode, even when they do not have packets to send. In DEMAC, to accomplish load balancing, weak nodes are used less frequently in a routing; rather they let to sleep more than the other neighboring nodes. This helps them to conserve energy. DEMAC is optimized for light traffic applications

Power aware cluster TDMA (PACT) protocol [44] is designed mainly to be used in large multi-hop WSNs, networks with high density of sensor nodes and engaged in battlefield surveillance, space exploration, and condition-based monitoring applications. The protocol adopts the duty cycle to the user traffic to decrease energy consumption. The radio is turned off if a node has no activity. PACT uses passive clustering to take advantage of the redundant dense topology and prolong the lifetime of the entire network even further. In passive clustering, only a subset of the network nodes participate in data communication at a time. In such networks, PACT offers better performance over the existing protocols in that it uses adaptive duty cycles based on the current traffic to save energy; it uses passive clustering to minimize message delays and to save energy even further; and it supports any network topology. PACT is a suitable MAC protocol for large-scale monitoring WSNs.

Bit-map-assisted (BMA) [45,46] is a cluster-based TDMA MAC protocol proposed to reduce energy waste due to collisions and idle listening while maintaining low delay performance. The new feature in BMA is in the absence of data, all the sensors including the cluster head (CH) turn off their radio till the next round; or if some of the sensors have data, following a TDMA scheme they send their data to the CH, after which the CH turns off its radio till the next round. So, there is no need for the CH to turn on its radio all the time. BMA is designed for large-scale event-driven monitoring applications. It has superior energy efficiency and delay performance in low and medium traffic networks, i.e. in relatively few sensor nodes per cluster.

Energy efficient adaptive TDMA (EA-TDMA) [47] is another cluster-based protocol originally designed for railway monitoring applications. All sensors and the CH are placed in the train wagons. In EA-TDMA, each node wakes up in its pre-assigned slot but turns off its transceiver immediately if it has no data in the buffer, otherwise the sensor sends its data to the CH. After receiving all the data from sensors, the CH aggregates the data and forwards it to the base station. In addition to railway monitoring, EA-TDMA is a suitable protocol for monitoring WSNs which have medium to high traffic loads. EA-TDMA does not support sensors mobility.

Energy efficient BMA (E-BMA) protocol [48] is a cluster-based TDMA scheme proposed for railway wagon health monitoring system, but it can also be used for other monitoring WSNs. E-BMA is developed to further improve the energy efficiency obtained in BMA. In BMA, sensors request a slot immediately when data is available in their buffers and then CH approves the request. Whereas, in E-BMA sensors wait for one more frame time to check if more data is coming and then slot reservation is made by piggybacking. During transmission, if a sensor has consecutive data, the first transmitted packet conveys that information by piggybacking. This method enables E-BMA to achieve better energy efficiency than MBA in low and medium traffic WSNs.

In general, TDMA-based protocols offer collision free communication for WSNs. Cluster-based TDMA schemes are suitable for wide area monitoring as they are capable of extending the network size by forming clusters while providing comparable latency and energy efficiency performance. These protocols lack scalability to topology changes and adaptability to traffic changes. They cannot be used in event-driven monitoring networks. Instead, they are suitable for scheduled data monitoring applications, in which the traffic density remains constant.

2.5.3. Hybrid MAC protocols

The characteristics of MAC protocols discussed above have their own strengths and weaknesses in different WSN scenarios. So to further solve the key problems of specific applications like event-driven monitoring, combining the good features of those protocols is crucial. Hybrid protocols adjust the behavior of MAC protocols between CSMA and TDMA to make them more energy efficient and more adaptive to changes in the data traffic.

Zebra-MAC (Z-MAC) [49] exploits the good features of CSMA and TDMA schemes to adapt the data traffic in the network, i.e. under low traffic it behaves like CSMA, and under high traffic like TDMA. It uses CSMA as the default contention resolution method. Time slots are allocated during deployment and each node reuses its own slot periodically. Unlike in TDMA, a node can transmit in any slot in Z-MAC. The fact is that before a node starts transmitting in a certain slot, it always performs carrier sensing and proceeds if the channel is sensed idle. However, channel access priority is always given to the owner of the slot, non-owner nodes can use it only when the owner node does not have a packet to transmit. The idea of giving earlier chances to owner nodes to transmit a packet and getting channel access on carrier sensing basis has the effect of switching between TDMA and CSMA methods based on the data traffic. Z-MAC easily and rapidly adapts itself to traffic conditions to minimize energy consumption. This property makes it a suitable protocol for event-driven monitoring WSNs.

Data gathering MAC (D-MAC) is designed and optimized for a tree-based data gathering with the aim of achieving low latency while still being energy efficient [50]. In S-MAC and T-MAC protocols, nodes which are on the path to the sink but more than one hops away from the sink do not have a knowledge of the ongoing traffic, and hence packet forwarding may stop after few hops. Consequently, a high delay occurs in the packet delivery. DMAC is a suitable protocol for such scenarios. DMAC maintains a fair and predictable packet arrival at the sink by staggering the listen/sleep periods of all child and/or grandchild nodes based on their distance from the sink i.e during the receive period of a node, all the child nodes are made to have transmit periods and compete for the receive period in the sink. Low latency is, therefore, achieved by allocating subsequent slots to the nodes that are successive in the same transmission path. While having good delay and energy saving performance, DMAC has few drawbacks. It does not employ collision avoidance mechanism, hence when more than one nodes have the same schedule and all send packets to a common sink, then collision occurs. This is a common phenomenon in event-driven WSN applications. An ACK packet and packet retransmission are used to ensure packet delivery. The other drawback is data transmission paths might not be estimated in advance, which affects the data gathering tree formation. Despite these drawbacks, DMAC supports multi-hop communication, and this makes it a suitable protocol for wide area monitoring applications.

2.5.4. Conclusion

In this section, a survey of different MAC protocols with respect to energy efficiency and their advantages and disadvantages in structural and wide area monitoring is made. They are broadly classified into scheduled, unscheduled and hybrid protocols. Each of them use different medium access techniques to maximize energy efficiency and QoS while minimizing latency. Although there are many protocols proposed for this application, there is no protocol accepted as a standard. Many of the existing protocols are developed with specific assumptions in mind and for specific applications.

Comparing the existing protocols, it is observed that contention-based MAC protocols have better network scalability and are robust to a variety of network malfunctions. They do not require strict synchronization. On the contrary, contention-free protocols are power efficient, have better bandwidth utilization, and work well even in dense networks but suffer from synchronization sensitivity. The selection of MAC protocols for monitoring WSNs is application-dependent. Contention-based protocols are best suited for event-oriented monitoring applications, in which the occurrence of events is unpredictable. On the other side, stable networks with periodical or on-demand data gathering requirements are better suited for contention-free protocols. These protocols can also be used in networks where monitoring with non-critical data is supported.i.e sensor nodes gather data for a long time, they wake up and send it to the central node.

Table 1 summarizes the characteristics of various MAC protocols proposed for monitoring applications. From the survey above, it is observed that the selection of one protocol for a specific application does not fully implement its requirements. Each protocol has its own strengths and drawbacks. Therefore, to improve the network performance and thus to prolong the network lifetime, using hybrid protocols or new mechanisms is crucial.

Table 1. Summary of some of MAC protocols used in WSN monitoring applications

Protocols	MAC Approach/ Basic Operation	Time Synchronization	Advantages	Disadvantages	Comments
S-MAC	CSMA/ duty-cycling	NO	Simplicity, high latency, time synchronization overhead may be prevented due to sleep schedules	Low throughput,overhearing and collision may cause if the packet is not destined to listening node	Good for light traffic applications
T-MAC	CSMA/ duty-cycling	NO	Packets are sent in burst, better delay, gives better result under variable load	Suffers from early sleeping problems	Good adaptability to changes in traffic conditions
DMAC	CSMA/ Scheduling	NO	Good delay performance, energy efficient	Collision avoidance are not used,leading to collisions	Good for low delay applications
Optimized MAC	CSMA/ duty-cycling	NO	High energy efficiency, good delay performance in high traffic loads	-	Good for wide-range traffic aplications
DEMAC	TDMA/ Scheduling	YES	Offers collision free communication between nodes	low energy efficiency, low QoS, and high latency in dense networks	Good for light traffic applications
PACT	TDMA/ Passive clustering	YES	Low overhead, prolonged network lifetime	High traffic overhead and idle listening, lacks support for dynamic network	Good for normal traffic applications
SIFT	CSMA	NO	Low overhead, prolonged network lifetime, low latency	Suffers from Idle listening, overhearing, and system-wide synchronization	Optimized for event reporting
EA-TDMA	TDMA / clustering	YES	Energy efficiency, contention free	Lacks scalability and adaptability,	Optimized for medium to high traffic WSN
E-BMA	TDMA / clustering	YES	Energy efficiency, contention free	Lacks scalability and adaptability,	Optimized for low to medium traffic WSN
Alert MAC	CSMA	NO	low latency, eliminates hidden terminal problem, robust to interference	affected by the traffic patterns	Good for normal traffic applications
B-MAC	CSMA	NO	Simplicity,good packet delivery rate, high throughput	Long preamble increases power consumption,	Good for normal traffic applications
WiseMAC	np-CSMA/ Listening	NO	Mobility support, scalable and adaptive to traffic load	Decentralized sleep/listen scheduling results in different sleep and wake-up times	Good for normal traffic applications
Z-MAC	CSMA/ Listening	YES	Robust to timing failures, slot assignment failures, and to topology changes	periodical rerun of the slot allocation algorithm reduces its energy efficiency	Adaptive to different traffic loads

3. IEEE STANDARD 802.15.4 FAMILY OF PROTOCOLS AND ITS APPLICATIONS IN LOW ENERGY INFRASTRUCTURE MONITORING NETWORKS

The chapter is organized as follows: Section 3.1 presents an overview of wireless personal area networks (WPANs) family protocols. Section 3.2 discusses critical infrastructures. Finally, Section 3.3 presents the suitability of IEEE Std. 802.15.4 for LECIM applications.

3.1. IEEE standard 802.15.4 WPAN family

The realization of a battery and wireless communication enabled the creation of electronic devices like personal digital assistants (PDAs), cell phones, cameras, pagers, etc. In a similar way, with the successful implementation of wireless local area network (WLAN), a lot of researches have been made on enhancing WLAN capabilities and developing new solutions to meet the ever growing demand of applications requiring wireless devices. Furthermore, there was a tendency of developing standardized protocols, and new applications with dynamic wireless connectivity often based on proprietary technologies. As a result of the above reasons, the idea of wireless personal area network (WPAN) was born. WPAN is a person-centered short-range wireless network that enables communication among any type of personal electronic devices.

Infrared was the first among the WPAN technologies. In march 1999 [51] Task Group 1 (TG1), under the IEEE 802 Working Group 15 [52], was formed to begin the development of the first WPAN standard IEEE 802.15.1, in which it was standardized into Bluetooth 1.1 soon. In the following years, IEEE formed Task Group 2 (TG2), Task Group 3 (TG3), and Task Group 4 (TG4) aiming at developing IEEE 802.15.2, IEEE 802.15.3, and IEEE 802.15.4 standards respectively. The WPAN standards are proposed to operate in the unlicensed 2.4 GHz industrial, scientific, and medical (ISM) band, which is the same operational band used by the other IEEE 802 wireless devices. In addition, they are proposed with the common goals of cable replacement of existing devices, low power consumption, self-configuring networks, device interoperability, and using little or no infrastructure. This allows small, power-efficient, inexpensive solutions to be implemented for a wide range of devices. WPANs use star, mesh, and cluster tree network topologies, and have two types of component devices: full function device (FFD), and reduced function device (RFD). On top of the aforementioned ones, IEEE also released IEEE 802.15.5, IEEE 802.15.6, and IEEE 802.15.7 WPAN standards in the following years.

The coverage area of WPANs as compared to other wireless networks is illustrated in Figure 1. Next to WBANs, WPANs have the smallest coverage area. The MAC and PHY layers of WPANs are defined to provide a robust short-range wireless connectivity for portable personal devices within a personal operating space (POS). A POS is a space with a person at center that extends up to a distance of 10 m in all directions. The fact that it is very energy-efficient makes it suitable to be used in small personal devices. Example applications for each wireless network are also seen in the same figure.

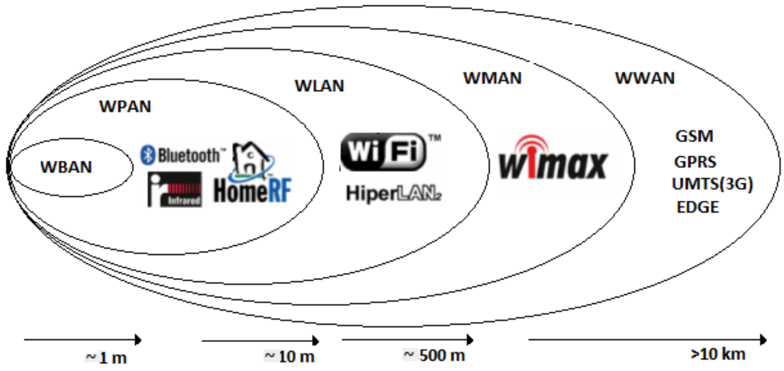


Figure 1. Coverage area comparison between WPANs and other wireless networks.

WSN applications like home automation, industrial, agriculture, and others need a different set of requirements. They do not require high data rate or high throughput. Because of complexity, power consumption, and high cost, existing standards are not suitable for such applications. The IEEE 802.15 TG4 [53] is focused to define a new standard with PHY and MAC layer specifications aiming at providing ultra low complexity, ultra low cost, ultra low power consumption, and low data rate wireless connectivity among inexpensive fixed or portable devices typically operating in the POS of 10m. The low rate WPAN (LR-WPAN) standard or IEEE 802.15.4-2003 standard is later revised to become IEEE 802.15.4-2006 which was included by the Zigbee Alliance. IEEE 802.15.4 and Zigbee Alliance work together. i.e., IEEE 802.15.4 takes care of PHY and MAC layers and Zigbee handles tasks in the higher layers like routing, security and control. Then the standard is used in many monitoring applications.

The standard PHY can operate in one of the three ISM frequency bands (i.e. 868-868.6 MHz, 902-928 MHz, or 2400-2483.5 MHz) and chooses from a total of 27 channels. It provides data rates of 20 kbps at 686 MHz band, 40 kbps at 915 MHz band, and 250 kbps at 2.4 GHz band. The PHY has the following key functions: activation and deactivation of the radio transceiver, energy detection (ED) within the current channel, clear channel assesment (CCA) for CSMA-CA, channel frequency selection, and data transmission and reception. The MAC layer also handles the following tasks: generating network beacons if the device is a coordinator, synchronizing to the beacons, employing the CSMA-CA mechanism for channel access, supporting PAN association and disassociation, supporting device security and others. Two types of devices are defined in this standard: an FFD and an RFD. The FFD can be a PAN coordinator, a coordinator or a device. It can talk to any device whereas an RFD can talk only to an FFD. LR-WPAN supports a star and a peer-to-peer network topologies. A special form of the peer-to-peer topology is a cluster tree, in which a node may only talk to its parent and its children. A peer-to-peer topology allows more complex network implementations like ad-hoc and self-configuring networks. The standard also uses 16-bit short and 64 bit IEEE addressing, and power management mechanism. As a result LR-WPAN has a multi-month to multi-year battery life, which makes it good for monitoring applications.

Through the time, a lot of PHY and MAC layer amendments have been made on the original IEEE 802.15.4 [54]. Some of them are mentioned below.

- IEEE 802.15 WPAN TG4a - a PHY amendment to create an alternative PHYs.

- IEEE 802.15 WPAN TG4b - specific enhancements and clarifications to the IEEE 802.15.4-2003 standard.
- IEEE 802.15 WPAN TG4c - a PHY amendment for China.
- IEEE 802.15 WPAN TG4d - PHY and MAC Amendment for Japan on the IEEE 802.15.4-2006 standard.
- IEEE 802.15 WPAN TG4e - MAC amendment on 802.15.4-2006 for industrial applications.
- IEEE 802.15 WPAN TG4f - PHY and MAC amendment for active RFID.
- IEEE 802.15 WPAN TG4g - PHY amendment for smart utility network.

Other WPAN standards are also developed for different applications. The IEEE 802.15.5 standard [55] is developed for LR-WPAN and HR-WPAN mesh networks with the aim of (1) extending network coverage without increasing the transmit power or the receiver sensitivity; (2) enhanced reliability via route redundancy; (3) easier network configuration; and (4) better device battery life. IEEE 802.15 Task Group 6 (TG6) [56] developed IEEE 802.15.6 for wireless body area network (WBAN) applications. The standard provides a low power, very short-range, and highly reliable wireless connectivity for WBAN devices in medical or personal entertainment applications. By employing a star topology, it offers up to 10 Mbps data rates. IEEE 802.15 also developed IEEE 802.15.7 [57], which is called visible light communication WPAN (VPAN), for a short-range optical wireless communications using visible light. VPAN has data rates high enough to support multimedia data exchanges, and a MAC layer that accommodates visible links, and mobility of the visible link. A summary of different WPAN standards with their sample applications is given in Table 2.

3.2. Critical infrastructures

3.2.1. Concept of a critical infrastructure

There are many definitions for the term critical infrastructure. For example, according to the European Commission [1], "Critical Infrastructures consist of those physical and information technology facilities, networks, services, and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security, or economic well-being of citizens or the effective functioning of governments in the Member States. Critical Infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply, and communications, as well as key government services". It also states that not all critical elements in these sectors are ’infrastructure’, but rather networks or supply chains that support the delivery of an essential product or service. Some applications associated with the term are:

- Energy installations and networks (e.g., electrical power, oil and gas production, storage facilities and refineries, transmission and distribution system)

Table 2. Summary of IEEE 802.15 WPAN Standards

IEEE standard	Name	Data rate	Example applications	QoS Requirement
802.15.1	Bluetooth	1 Mbps	Cell phones, laptops, printers, PDAs, microphones, speakers, headsets, pagers, sensors, etc.	QoS suitable for voice applications
802.15.2	Coexistence of WPAN and WLAN	N/A	N/A	N/A
802.15.3	High-rate WPAN (HR-WPAN)	>20 Mbps	Home theater, PC to LCD projector, interactive video gaming, personal home storage	Very high QoS
802.15.4	Low-rate WPAN	<0.25 Mbps	Industrial, Agricultural, vehicular, residential, medical, and other low power, low cost requiring WSN applications	QoS and data rates are not primary requirements
802.15.5	WPAN mesh	>20 Mbps HR-WPAN, <0.25 Mbps LR-WPAN	In application areas where HR-WPAN and LR-WPAN respectively are required	High QoS for HR-WPAN mesh, relaxed QoS for LR-WPAN mesh
802.15.6	WBAN	<10 Mbps	medical applications	High QoS for high-priority medical applications
802.15.7	VPAN	Hundreds of Mbps	Public data broadcasting, traffic communications, indoor broadband broadcasting in office, home access network and military communications	QoS suitable for broadband communications

- Communications and Information Technology (e.g., telecommunications, broadcasting systems, software, hardware and networks including the Internet)
- Financial services (e.g., banking, securities and investment)
- Agriculture, food production, and distribution
- Water services (e.g., dams, storage, treatment and networks, waste water/sewage)
- Health care (e.g., hospitals, ambulances, blood supply facilities, pharmacies, rescue services)
- Transportation (e.g., fuel supply, railway network, airports, harbors and traffic control systems)
- Security services (e.g., police, military)
- Production, storage and transport of dangerous goods (e.g., chemical, biological, radiological and nuclear materials)
- Government (e.g., critical services, information networks, assets and key national sites and monuments)

For the functioning of a society and its economy, these facilities are very essential that they are expected to be available 7 days a week, 24 hours a day. However, a sudden failure of and/or an intentional attacks on them results in service interruptions. So critical infrastructures need protection. An effective protection requires employing some monitoring mechanisms on them and can be done by using WSNs. Monitoring critical infrastructures enables us to detect failures and attacks as early as possible. It ensures safety by providing protection mechanisms from catastrophic failures, environmental damages, hazardous leaks; it increases reliability and thus reduces outage and speeds up restoration of services; it helps to do preventive maintenance; and it significantly reduces the overall cost through improved operations and efficiency.

3.2.2. Use case examples

The following use cases exemplify LECIM applications.

Oil and gas pipeline monitoring

Oil and gas pipelines are of high importance for oil and gas transportation [58]. They are deployed in cities, suburban, and very remote areas over the surface or underground. Pipeline monitoring benefits compliance, environmental protection (less spilling), protection from damage and theft, redemption cost reduction, and reliability. It also provides an easier way of detecting corrosion, pressure, leakage, vibration etc; and locating the incident in the pipes. The key application requirements are long range over non-accessible terrain coverage, non-mains based infrastructure, low to no maintenance, and simple and easy deployment. The sensors installed on the pipes report scheduled or event-driven short data messages to the control system.

Water leak detection

Globally there is shortage of fresh water. Water is a scarce natural resource and often found far away from where it is used. It requires transporting from the supply to consumers using water pipes. Conventional leak detection methods take time and resources. Besides, underground leak detection is not easy. A good solution for the above problem is to remotely monitor logging systems which are installed underground. The key requirements of the WSN-based monitoring system are long range and ability to penetrate underground vaults; large number of sensors deployed underground; low installation and maintenance costs; and battery based sensors. Battery life is very critical as the network should serve for multiple-years. Sensors inform the control system about the pipe status by sending short data messages once per day; or by sending alarm messages in case a leak is detected.

Bridge monitoring

Bridges are part of the national road networks. Also, it is known that these networks are the backbone of a national economy. In other words, maintaining bridges at high performance level induces public safety, economic productivity, and growth. Therefore, bridges need regular inspection for early detection of stress cracks or fractures. Traditional methods of bridge monitoring are done by visual inspections which have many drawbacks. Effective bridge health monitoring can be done using WSNs. Sensors installed on critical parts of the bridge are used to report measurement or state information over long periods. Whenever a damage or a fracture occurs in the bridge, all the sensors which detect the incident simultaneously send emergency messages to the control system so that correction actions are taken on time. Battery life, low duty cycle, low installation, and low maintenance costs are some of the basic requirements of such monitoring systems.

3.2.3. LECIM characteristics

LECIM networks require ultra-low energy, long deployment lifetime, scalability, reliability, robustness, and security. The low energy requirement is due to the fact that sensor nodes used in such networks are located at very remote places where mains power is not available. The sensors work in a highly challenging propagation environments including cities, rural areas, forests, mountains, underground monitoring places; and they are expected to work for multiple-years without human contacts. Periodic, event-driven, or query-based monitoring methods are used. Sensor nodes report measurement or state information in several minutes to several hours interval. Some events or state changes detected in the system maybe time-sensitive and the detecting sensors report them with emergency. The main LECIM characteristics with their brief descriptions are listed below [3].

1. Extreme difference between network devices: the PAN coordinator (collector) and endpoints (sensors) are network devices proposed for LECIM. The coordinator has by far higher performing capabilities and a larger energy supply than the sensors. No mobility for sensors while the coordinator has limited portability.

2. Minimal infrastructure: the network uses a star topology to support one to multipoint direct communication. Except for the PAN coordinator, all sensor nodes are non-mains powered. Endpoints cannot communicate with each other; and they can communicate with the coordinator either directly or through the time-slot relaying based link extension (TRLE) PAN relay if TRLE is enabled.

3. Commissioned network: the network does not have ad-hoc nature. The network devices are configured for the specific network before deployment. Besides, the devices are preconfigured with parameters which avoid unnecessary configuration information messaging.

4. Large coverage area: LECIM is set primarily for outdoor environments. The sensors are widely dispersed that the range may vary from a few meters to several kilometers. Therefore, LECIM is tolerant to high data latency (may be in seconds); has high receiver sensitivity and interference robustness; and provides a reliable communication in a dramatically changing propagation medium.

5. Low energy: once deployed the network should work for multiple-years without replacing the batteries of sensors or performing any maintenance. Sensors must

be able to conserve their limited energy. To achieve this, LECIM utilizes different energy saving mechanisms. e.g. short and infrequent messages and low duty cycle.

6. Low data rate: LECIM aims to collect scheduled and event-driven data, which are often infrequent, from the sensors. Hence, the application data rate is limited to less than 40 kbps.
7. Low cost: LECIM systems require low operational cost (unlicensed or lightly licensed spectrum), low installation cost, and low infrastructure and maintenance cost.
8. Asymmetrical data flow: the uplink communication dominates data flow with limited downlink data needs.
9. Addressing: LECIM networks can address supporting thousands of connected sensor nodes.
10. Worldwide use: such networks are required to operate in all regulatory domains, and transmit power is low and complying with international regulations.

LECIM applications, in general, require large number of endpoints, broadcast/multicast capability, very low energy operation, low or light infrastructure, low receiver sensitivity, and a simple low-cost communication environment.

3.2.4. Existing technologies

Many of the afore-mentioned applications are not well served by any of the existing technologies. This is because of the unique features mentioned in section 3.2.3. The main reasons why the existing architectures do not support LECIM systems are briefly explained below.

Satellite links are characterized by having high power, high cost and incur subscriber fees. Cellular networks have high power, short range and incur subscriber fees. Wireless supervisory control and data acquisition (SCADA) has high unit and installation cost, limited capacity, high power, and is proprietary. All the above techniques require heavy infrastructures. The IEEE 802.11 networks are also unfit for LECIMs because they are optimized for computing applications which require high data rate, high duty-cycle, and high performance. They are limited to hot spots and consume a lot of power. As mentioned in Section 3.1, WPANs have good features which fulfill many of the LECIM requirements. Nevertheless, they are not suitable for LECIM devices as they are because they are not designed to support large networks, long-range communications, and to work in harsh channels. In addition, some of them are proposed for multimedia applications. IEEE 802.16 [59] wireless metropolitan area network (WMAN) and IEEE 802.20 [60] mobile broadband wireless access (MBWA) are designed mainly for broadband wireless applications. Also, because of high data rate, complex architecture, high cost, very high power consumption, and medium capacity, IEEE 802.22 [61] wireless regional area network (WRAN) standard is not suitable for LECIM networks.

Despite the above facts, the IEEE 802.15 family is, relatively, the right group to investigate for a new standard for LECIM systems for the following reasons: they have good fit for the applications space; less architecture complexity; and no overlap with existing or planned PHY standards.

3.3. IEEE standard 802.15.4 suitability for LECIM

Unlike the previous WPAN standards, IEEE 802.1.5.4 (LR-WPAN) and its amendments have low complexity, low power consumption, simple infrastructures, and support low-rate applications. However, they do not satisfy all LECIM requirements. Having short ranges, low node density, and the requirement of either powered network infrastructure, mesh or no mechanisms to extend the range are their drawbacks. Also, they are not designed for outdoor propagation environment. To use them in large networks while operating in long range and challenging environments, they need MAC layer and PHY layer modifications.

It is known that the main identifying feature of IEEE 802.15.4 among WPANs is its capability to achieve extremely low power consumption, low installation, manufacturing and operation costs, and infrastructure simplicity. It is defined for applications which require relatively low data rates and low quality of services. However, as already mentioned above even including its latest versions they are not sufficient for LECIM. To enhance more features or to expand its application areas, a lot of MAC layer and PHY amendments have been made to the 802.15.4 standard. Among many of them, IEEE 802.15.4e and IEEE 802.15.4g are potential candidates for LECIM.

IEEE 802.15.4e defines a MAC amendment to the 802.15.4-2011 standard. To address all the industrial/commercial applications requirements (e.g., low latency, robustness in the harsh industrial RF environment, and determinism), it necessitates to have a wide range of MAC behaviors. The two main MAC enhancements added are [62]:

- behaviors to support specific application domains such as process automation, factory automation
- general functional improvements not specifically tied to application domains

The MAC amendments specific to a particular application domain mode are time-slotted channel hopping (TSCH), low latency deterministic networks (LLDN), deterministic and synchronous multi-channel extension (DSME), radio frequency identification blink (RFID), and asynchronous multi-channel adaptation (AMCA). Example application domains of the MACs are:

- TSCH - process automation (to mitigate the effects of multipath fading and interferences)
- LLDN - factory automation (to support the very low latency requirements)
- DSME - for compatibility with modifications proposed within the Chinese WPAN (to improve network performances)
- RFID - item and people identification, location, and tracking (e.g. to communicate device ID)

- AMCA - for large infrastructure applications

MAC enhancements not specific to a particular application domain mode include low-energy protocol to allow very low duty cycle devices functioning; information elements to provide extensible MAC data transfers; enhanced beacons and enhanced beacon requests to send beacons; a multipurpose MAC frame to facilitate scalability and extensibility. Unlike its good features in the industrial/commerial applications, the standard does not support LECIM for the following reasons. First, TSCH uses TDMA protocol which is not an appropriate one when the number of endpoints is large. Besides, in TSCH the sensors follow a common schedule which is good for point-to-point connections. Second, DSME is good for periodic traffic, whereas LECIM often entertains both periodic and event-driven traffic. Third, this standard has slot ownership concept which degrades the network performance because of the multi-thousand endpoints.

IEEE 802.15.4g [63] is a PHY amendment for smart metering utility networks. It defines a global standard for very large scale process control applications like the utility smart-grid networks. These networks cover wide areas containing very large number of fixed endpoints while using minimum infrastructure. The devices in this standard are designed to be capable of supporting large scale, low power applications (and often using the maximum available power) to facilitate a long range, point-to-point communications. Besides, they use either a mesh or a peer-to-peer multihop method to communicate with the access point. However when it comes to LECIM, this standard also does not satisfy all the application requirements. The observed problems are higher data rate per node, higher power consumption, uses large payload size, supports neighborhood area range, uses a multihop technique to extend the range, and the system trade-offs assume mains power availability for endpoints.

It is observed that given the application requirements, no IEEE standard or any wireless technology serves LECIMs very well. Consequently, it was understood that a new IEEE standard with a new MAC layer and PHY specifications optimized for LECIMs was necessary. In May 2011, the IEEE working group issued a call for proposals [64], by taking the IEEE 802.15 objectives, to develop IEEE 802.15.4k as an amendment to the IEEE 802.15.4. The next chapter discusses this new standard.

4. THE IEEE 802.15.4K STANDARD

4.1. Introduction

The IEEE 802.15.4k standard is an evolution of the IEEE 802.15.4-2011 being developed to facilitate LECIM applications. The draft standard is defined for wide-area networks, where there are widely dispersed multi-thousand endpoints, long distance links (up to 20 km) and large propagation path-loss (up to 120 dB) can be expected while operating in any of the available licensed, unlicensed, or special purpose frequency bands. It attempts to complement other WPAN technologies by providing features like minimal network infrastructure, very low energy operation necessary for multi-years battery life, data rates of less than 40 kbps, tolerant to data latency, and reliable operation in changing environments, thus enabling applications that were previously impractical or less properly served.

The amendment proposes a star network topology consisting of two types of network devices: a PAN coordinator (collector) and the endpoints (sensors), thus enabling a point-to-multipoint communication. Endpoints cannot communicate between each other. There is extreme difference in performance and capabilities between the coordinator and endpoints. The standard supports an asymmetric data flow, i.e. in the uplink case the coordinator collects scheduled and event-driven data from the endpoints, and in the downlink case there is much lower management and/or maintenance data flow from the coordinator to the endpoints. To conserve energy, the standard uses short and infrequent messages. The PAN coordinator often monitors the channel, in the mean time a sensor node spends most of its time sleeping, unless it has a message to send.

4.2. The MAC layer description

According to the IEEE 802 project, the data link layer (DLL) is divided into the MAC and logical link control (LLC) sublayers. The LLC, once standardized for the IEEE 802.2, is a common standard for all IEEE 802 standards. LECIM networks are large in size and scalability is very essential. Energy consumption and lifetime are critical design parameters of the MAC layer. In this section, the MAC layer proposed for IEEE Std 802.15.4k will be discussed.

The IEEE Std 802.15.4k MAC layer uses contention based MAC mechanism. This is because this MAC mechanism has low energy consumption. Its major problem is packet collision. However, in LECIM networks the daily scheduled data transmission is very low and thus there is almost no collision. Other benefits of using asynchronous MAC mechanism are:

- endpoints can send high priority messages immediately. This produces very low latency.
- it enables endpoints to join or leave the network very easily with minimum interruptions to the existing communications. No need of slot redistribution.

Like IEEE Std 802.15.4-2011, IEEE Std 802.15.4k allows an optional use of a superframe structure. An illustration of a superframe structure is shown Figure 2. The

MAC layer can operate either in non-beacon or beacon-enabled mode. In a beacon-enabled mode, the PAN coordinator periodically sends network beacons. The time duration bounded between consecutively transmitted beacon frames is termed as the superframe. The format of the superframe is defined by the PAN coordinator. The beacon interval (BI) defines the duration of the superframe and consists of an active period and, optionally, an inactive period. During the inactive period, if it exists, all nodes enter into a sleep mode to save energy. The active period is divided into 16 equal time slots, and includes a contention access period (CAP) and, optionally, a contention-free period (CFP). The CFP period is allocated (on demand), and the time slots assigned for this portion are called guaranteed time slots (GTSs). A unique feature of this draft is that it, optionally, adds PCA in the CAP period of the superframe. These PCA slots are allocated to facilitate high priority frame transactions, and more will be said on it in the next section. If a PAN coordinator does not wish to use a superframe structure, it will turn off the beacon transmissions, and thus operates in the non-beacon mode.

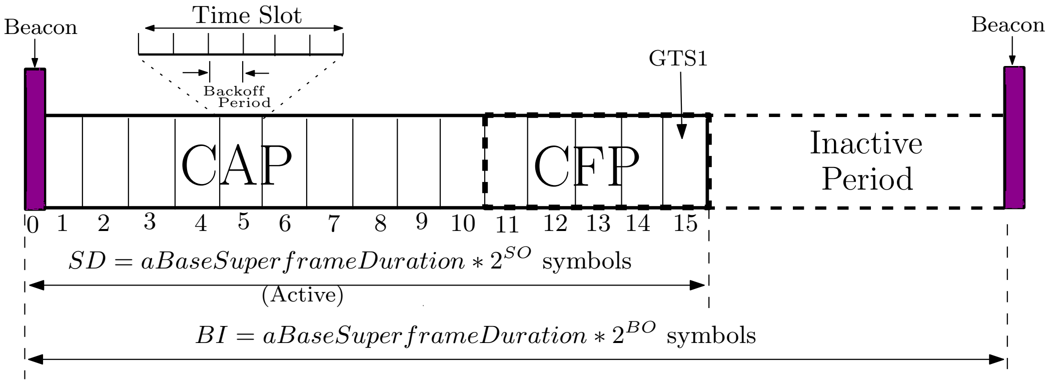


Figure 2. Schematic view of superframe structure.

4.2.1. Channel access

One of the main tasks of the MAC layer is creating a conducive channel access mechanism. For this purpose, IEEE 802.15.4 utilizes a slotted and unslotted versions of CSMA-CA algorithm for beacon-enabled and non-beacon enabled PANs respectively. In both cases, the algorithm is implemented using units of time called backoff periods, where one backoff period equals to *aUnitBackoffPeriod*. The MAC layer constant, *aUnitBackoffPeriod*, defines the number of symbols forming the basic time period used by the MAC algorithm. The working principle of these two algorithms can be referred in IEEE Std 802.15.4 [53].

Unlike IEEE 802.15.4, the emerging standard allows the use of CSMA-CA and Aloha algorithms for channel access, with each one having slotted and unslotted versions to support beacon-enabled and non-beacon enabled PANs respectively. Moreover, in LECIM networks there are two types of data frames whose medium access requirement is different: the scheduled data frames and the high priority data frames used to report critical events. Depending on the network configuration, the former ones use normal access (using CSMA-CA or Aloha algorithm), whereas the latter ones use priority access. The PCA can be implemented using CSMA-CA used with PCA or Aloha used with PCA algorithm. Next, the two priority access schemes will be discussed based on [3].

CSMA-CA with PCA

When PCA is enabled and when a critical event occurs, CSMA-CA with PCA backoff algorithm is employed before the transmission of the high priority message. The PCA backoff algorithm, on average, provides a shorter backoff delay for priority access than for normal access. Furthermore, the PCA conducts a clear channel assessment (CCA) at regular intervals even if the channel is assessed to be busy, so as to gain immediate access to the channel once it is assessed to be idle.

In a beacon-enabled PAN, the slotted version of CSMA-CA with PCA backoff algorithm is used for priority frame transmissions in the CAP of the superframe. In this mode of operation, a fixed-size CAP time slots are dedicated for PCA; and the information about the PCA allocations in the CAP is included in the PCA allocation specification payload information element (IE) of the enhanced beacon frames and is broadcast to the endpoints. An IE is a formatted data entity which has an ID, a length, and a data payload used to pass data between layers. High priority frames always apply PCA backoff algorithm; and can start accessing the channel in any one of the time slots in the CAP and continue through the duration of the CAP. Whereas, normal frames always use CSMA-CA algorithm and are restricted from accessing the channel during the allocated PCAs.

Conversely, the unslotted versions of CSMA-CA with PCA backoff algorithm is used in non-beacon enabled PANs. In this case, a critical event message transmission can be initiated at any time, and the PCA backoff algorithm is used for priority access. The slotted and unslotted CSMA-CA with PCA backoff algorithm finite state machines are shown in Figures 3 [65] and Figure 4 [65], respectively. The PCA backoff algorithms of each version are also indicated within the dashed line rectangles of each figure.

In PCA backoff algorithm, prior to the first transmission attempt, the backoff exponent (BE) is set to the maximum value of either *macMinBE* -1 or 1, and it remains constant for subsequent retransmissions. *Total Backoffs* (TB) is one of the MAC layer variables which is used to indicate the number of remaining backoff periods since the start of the CSMA-CA with PCA backoff algorithm. TB is initialized to a random value from the interval $[0,\ 2^{BE}-1]$. As seen in Figures 3 and 4, the PCA backoff algorithm follows a persistent CSMA mechanism so as to gain an immediate access once the channel is assessed to be idle.

In beacon-enabled mode, MAC layer ensures that, after the persistent random backoff, the remaining CSMA-CA steps and the entire transaction is completed before the end of the CAP. If TB is greater than the remaining number of backoff periods in the CAP, The MAC layer pauses the TB countdown at the end of the CAP and is resumed at the start of the CAP of the next superframe, otherwise it applies the PCA backoff algorithm one CCA attempt further and then checks if there is enough time to proceed. The MAC layer proceeds if the remaining CSMA-CA steps and the entire transaction can be completed before the end of the CAP. Otherwise, the process is paused and continued in the CAP of the next superframe.

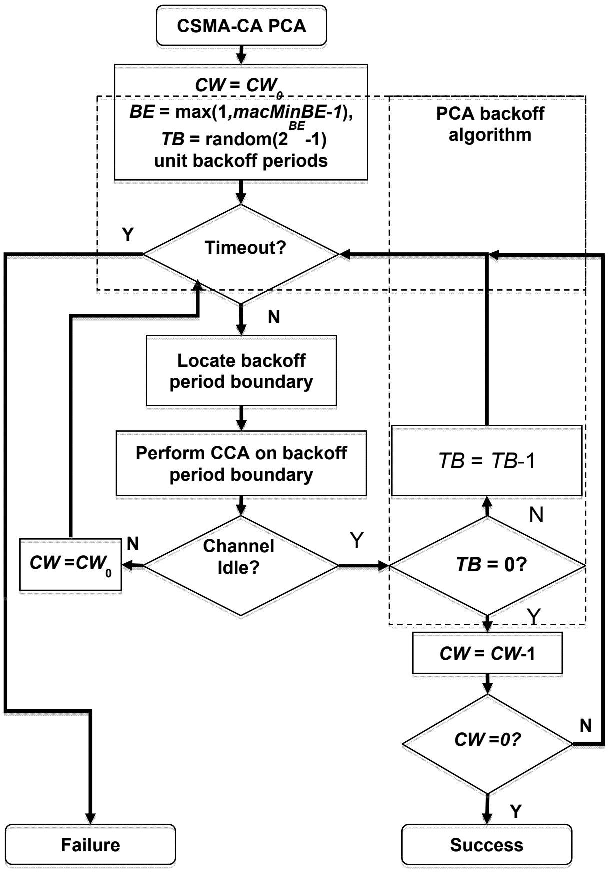


Figure 3. Algorithm for slotted CSMA-CA with PCA.

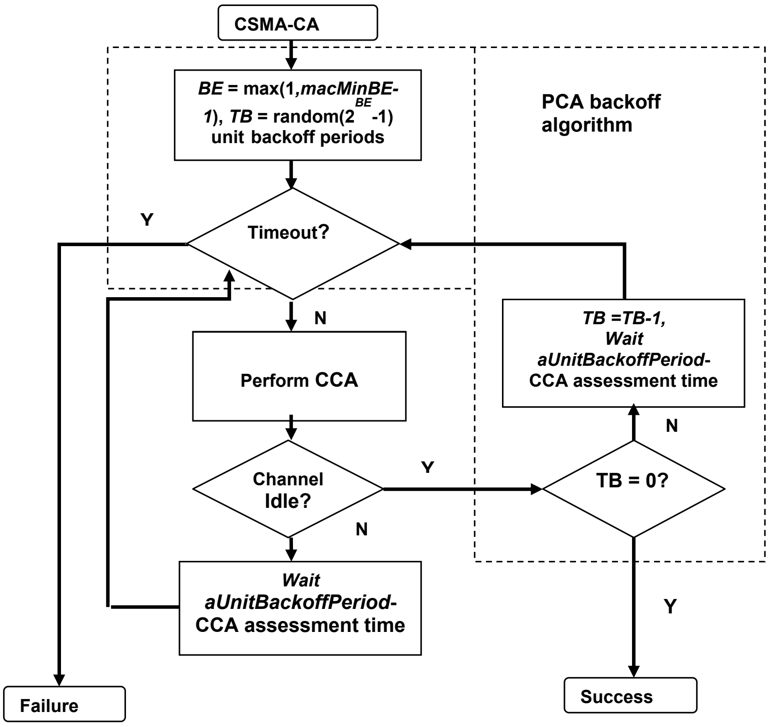

CSMA-CA
BE = max(1,macMinBE-1), TB = random(2^BE -1)
unit backoff periods
PCA backoff algorithm
Timeout?
Y
N
Perform CCA
TB =TB-1, Wait aUnitBackoffPeriod-CCA assessment time
N
Channel Idle?
Y
TB = 0?
N
Wait aUnitBackoffPeriod-CCA assessment time
Y
Failure
Success

Figure 4. Algorithm for unslotted CSMA-CA with PCA.

The length of PCA allocation in a beacon-enabled mode should be at least 880 symbols duration. The number of PCA allocations per superframe is defined using the MAC PAN information base (PIB) attributes *macPCAAllocationSuperRate*, *macPCAAllocationRate*, and *macCritMsgDelayTol* and is determined as seen in Table 3 [3]. A PCA allocation shall not occur if the CAP duration is less than *aMinCAPLength* plus the time required for one PCA allocation, where *aMinCAPLength* is a MAC layer constant which represents the minimum number of symbols required to for a CAP. If there are multiple PCA allocations in a superfarme, the first one is placed at the start of the CAP; and the remaining ones are allocated by uniformly distributing them throughout the CAP as shown in Figure 5. [3]

Table 3. Determination of number of PCA allocations per superframe

Value of *macPCAAllocationSuperRate*	Superframe duration (SD)	*macPCAAllocationRate*
FALSE	$SD \leq \frac{macCritMsgDelayTol}{3}$	Maximum value $\lfloor \frac{macCritMsgDelayTol}{3\times SD} \rfloor$
TRUE	$\frac{macCritMsgDelayTol}{3} < SD \leq$ *macCritMsgDelayTol*	Minimum value 1
TRUE	$SD >$ *macCritMsgDelayTol*	Minimum value $\lceil \frac{SD}{macCritMsgDelayTol} \rceil$

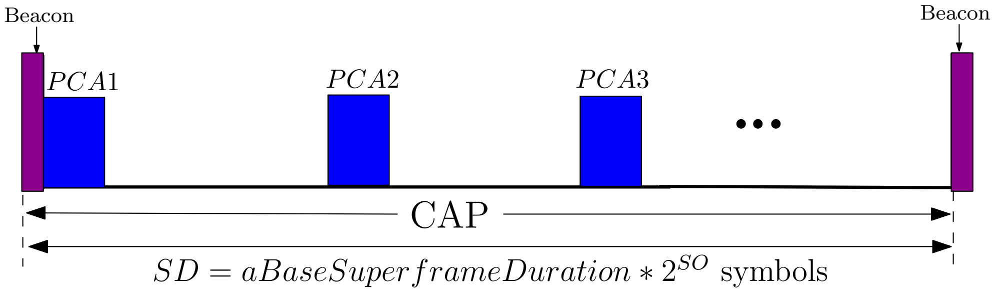


Figure 5. An illustration of how allocated PCAs are distributed in the CAP period.

Aloha with PCA

There are slotted and unslotted versions of Aloha with PCA algorithms. In a PCA-enabled mode of operation, the PCA backoff algorithm is implemented using a modified version of the Figures 3 and 4. In this algorithm, one backoff period is equal to *macLECIMAlohaUnitBackoffPeriod* and should be long enough to accommodate the entire frame transaction. A S-Aloha with PCA backoff algorithm is obtained from Figure 3 with the following modifications: CW is initialized to 1 and the CCA step is skipped, i.e., the algorithm advances directly from the state "Locate backoff period boundary" to the state "TB = 0?". Whereas, in an unslotted Aloha with PCA backoff algorithm is obtained from Figure 4 with the following changes: when the state "Timeout?" returns "N", the algorithm advances directly to the state "TB = 0?". [3]

When PCA is in use, each PCA allocation should have at least four consecutive *macLECIMAlohaUnitBackoffPeriod* in duration. A PCA allocation cannot occur if the

CAP duration is less than *aMinCAPLength* plus the time required for one PCA. The number of PCA allocations per superframe is determined using Table 3. [3]

4.2.2. MPDU fragmentation

Devices which operate with LECIM DSSS PHY shall support MAC protocol data unit (MPDU) fragmentation; other PHYs use it optionally. Normally, the MPDU frame is constructed based on the IEEE 802.15.4 MAC frame format. When IEEE 802.15.4 MAC frame at LECIM data rates is applied, the over-the-air duration of the frame increases, and leads to the following problems: increased interference, and susceptibility to channel variations during the duration of the frame transmission. A long packet duration also incurs a large cost during retransmission (in terms of energy and interference). These problems occur because the existing MACs and protocols, especially that of IEEE Std 802.15.4, and LECIM DSSS PHY operating modes do not fit.

When fragmentation is enabled, it operates on the MAC header (MHR) and MAC service data unit (MSDU) parts of the MPDU; converts them into a sequence of fragments to adapt the MAC frame structure to the specific PHY layer and PHY layer operating mode. The MPDU fragmentation process is summarized in Figure 6. In this process, to reduce over-the-air overhead, MHR is sent once by establishing a fragment sequence context or suppressed; and the MSDU is fragmented into a sequence of fragmentation cells that each fit into the size supported by the current PHY configuration. Therefore, each fragment has minimum overhead and carries an incremental validity check sequence for error detection. No MAC footer (MFR) is transmitted with a fragment. At the receiver side, each fragment is identified with the help of the fragment sequence context and the information in the fragment. Each fragment is validated and

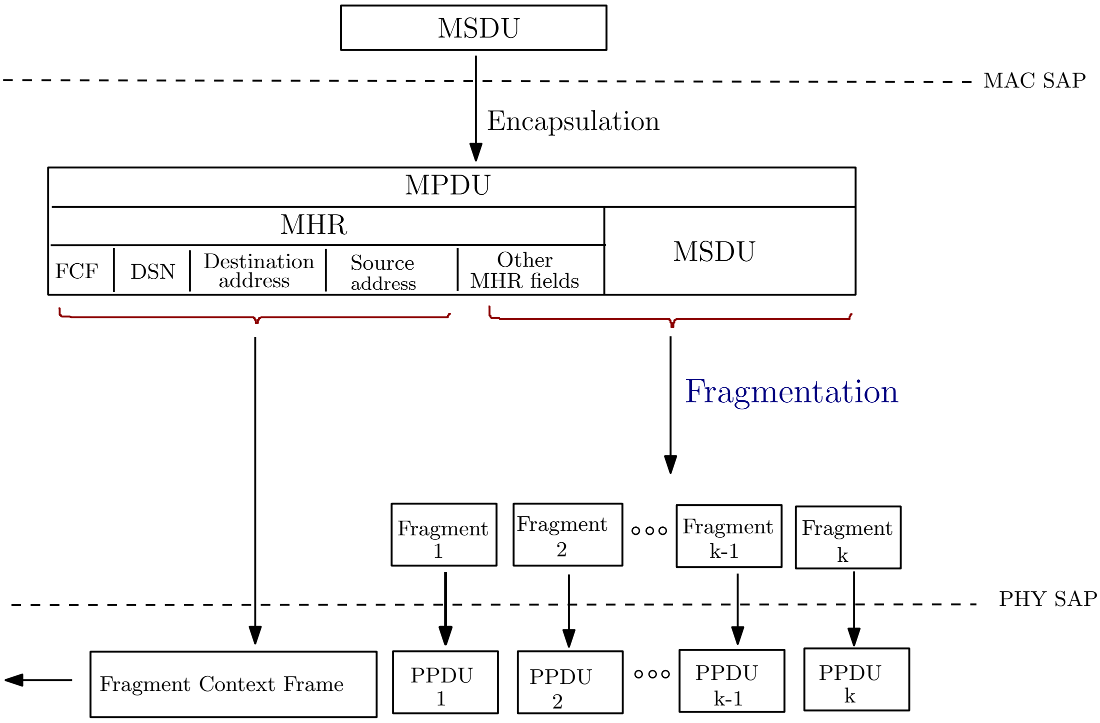


Figure 6. An illustration of MPDU fragmentation.

optionally acknowledged individually. If a certain fragment is not acknowledged, only that fragment is retransmitted. When all the fragments are received, the MPDU (the whole fragment sequence) is reassembled and, optionally, acknowledged.

The fragments obtained by the fragmentation process are of the same length except the last one. Each fragment is packaged into a PHY protocol data unit (PPDU) for transmission. A typical fragment format is shown in Table 4 [3]. The frame type field indicates if the frame is fragmented or unfragmented; the transaction identifier (TID) field contains the value that uniquely identifies the fragment sequence; the Fragment Number field identifies the position of each fragment within the fragment sequence; the fragment data represents the part of the fragmented MPDU indicated by the fragment number field; and the fragment validation sequence (FVS) field is used to validate the received fragment.

Table 4. Fragment format

Octets: 2			variable	2/4
Bits: 0-2	3-9	10-15		
Frame Type	TID0-TID6	Fragment Number	Fragment Data	FVS
Fragment header				

Fragment transmission is initiated by the transmission of a fragment context frame. Following the successful transmission of the fragment context frame, the fragments are transmitted beginning with fragment 1 and ending with fragment k. Upon a successful transmission, each fragment is, optionally, acknowledged. There are two levels of fragment acknowledgments: the fragment incremental acknowledgment (I-ACK), which acknowledges each fragment and provides progress reports; and acknowledgement of the reassembled MPDU.

Fragmentation creates adaptability to a variety of PHY layers and data rates, improves reliability of the medium, mitigates interference, reduces over-the-air overhead, leverages IEEE 802.15.4 MAC frame structures and capabilities, and fits other PHY characteristics for LECIM. An optimum use of fragmentation depends on the interference environment, channel performance, and characteristics of the PHY selected (e.g., data rate and maximum PSDU size).

4.3. The PHY layer description

Two PHYs are proposed to support LECIM applications: the DSSS and frequency shift keying (FSK). The two PHYs have different operating characteristics and frequency ranges.

4.3.1. LECIM DSSS PHY

This is a multi-regional, DSSS PHY operating with frequency ranges 433-434.57 MHz, 470-510 MHz, 779-787 MHz, 863-870 MHz, 902-928 MHz, 915-928 MHz, 917.1-923.5 MHz, 920-928 MHz, 921-928 MHz, and 2400-2483.5 MHz. Each frequency range can use binary phase shift keying (BPSK) or offset quadrature phase shift keying (O-QPSK) modulation methods and different chip rates.

The channel center frequency for all LECIM DSSS PHY frequency bands is calculated as follows.

$$\begin{aligned} ChanCenterFreq &= FreqBandEdge + FreqOffset \\ &\quad + (phyCurrentChannel - 1) \times ChanSpacing \end{aligned} \tag{1}$$

where *ChanCenterFreq* is the center frequency in MHz, *FreqBandEdge* is the band edge for the frequency band in use in MHz, *FreqOffset* is the frequency offset for each band in MHz, *phyCurrentChannel* is a channel identifier number with values from 1 to n, and *ChanSpacing* is the gap between adjacent channels in MHz.

The values of the above parameters and the range of valid channel numbers of each frequency band can be referred from [3], Table 68I.

The LECIM DSSS PHY PPDU format is made up of synchronization header (SHR) and the PSDU as shown in Table 5 [3]. The PSDU field contains the data of PPDU and is set to one of the *phyLECIMDSSSPSDUSize* values (a PHY PIB that determines the LECIM DSSS PSDU size). The SHR, if present, is used for obtaining frequency, symbol and frame synchronization. The Preamble field is used to obtain symbol timing and frequency offset. Bit transmission begins from the left side of the PPDU format and continues with the right most bits transmitted last.

Table 5. Format of the LECIM DSSS PHY

Octets		
0/2/4	0/1	16/24/32
Preamble	SFD	PSDU
SHR		PHY payload

In DSSS PHY data rate depends on the frequency band in use, the spreading factor, the modulation rate, and the type of modulation being in use, and is computed as

$$DataRate = \frac{1}{2} \times \frac{(t \times ChipPerSymbol)}{phyLECIMDSSSPSDUSpreadingFactor}\ kbps \tag{2}$$

where t = *phyLECIMDSSSPPDUModulationRate*, *ChipPerSymbol* = 1 when BPSK modulation is used, and *ChipPerSymbol* = 2 when O-QPSK modulation is used. The multiplying factor $\frac{1}{2}$ represents the forward error correction (FEC) $\frac{1}{2}$ coding. According to (2), the data rate of a DSSS PHY never exceeds 40 kbps.

DSSS PHY relies on convolutional encoding, interleaving and differential encoding. Gold code sequences are used to generate pseudo-random sequences. In addition, its radio frequency tolerance should be ± 2.5 ppm; its channel switching time should be 500 μs; it has a receiver sensitivity which varies from -108 dBm to -148 dBm depending on the spreading factor and modulation rate used; and it has 10 dB and 30 dB minimum receiver adjacent channel rejection and alternate channel rejection requirements, respectively. The transmitter power prescribed for DSSS PHY is -3 dBm.

Compared to DSSS devices in other standards, LECIM DSSS devices have better processing gain that can enable them to receive messages with very low or negative carrier-to-noise ratios. High processing gain also has an indirect effect in reducing the possibility of collisions. LECIM DSSS PHY has many options that enable it to best address the applications throughout a diverse or changing set of regulatory environments. Some options can have restrictions in some regulatory domains, others may comply with local regulations.

4.3.2. LECIM FSK PHY

LECIM FSK PHY is narrow bandwidth (hence with low data-rate), multi-regional PHY intended to operate with characteristics that allow LECIM applications. The narrow bandwidth characteristics in FSK PHY devices promotes higher sensitivity, and an increased number of channels in each band, which minimizes packet collision. It operates in one of the frequency bands 169.4 - 169.475 MHz, 433.050-434.790 MHz, 470-510 MHz, 779-787 MHz, 863-870 MHz, 902-928 MHz, 915-928 MHz, 917.1-923.5 MHz, 920-928, and 921-928 MHz by using one of the following modulation techniques: FSK, Gaussian FSK (GFSK), position-based FSK (P-FSK), or position-based GFSK (P-GFSK). The data-rate of the FSK PHY is always less than 40 kbps.

The FSK PPDU format is shown in Table 6. It comprises of SHR, PHY header (PHR), and the PSDU. The order of bit transmission follows the same rule like that of the DSSS PHY.

Table 6. Format of the LECIM FSK PHY

Octets			
Variable	3	2	variable
Preamble	SFD	PHR	PSDU
SHR		PHR	PHY payload

FSK PHY is characterized by having a radio frequency tolerance of ±10 ppm; channel switch time of 500 μs; receiver sensitivity of -97 dBm; and a transmission power of -3 dB. To improve the receiver sensitivity, it applies convolutional encoding, robust interleaving, a better spreading capability, and optionally data whitening. Furthermore, the transmitted signal has a constant-envelope nature which allows for low cost implementation and good transmit power efficiency.

5. THE SYSTEM MODEL

The chapter is organized into two major sections. The first section focuses on the general issues about the implemented simulation model; and the second section explains the development of Markov model of the system.

5.1. The simulation model

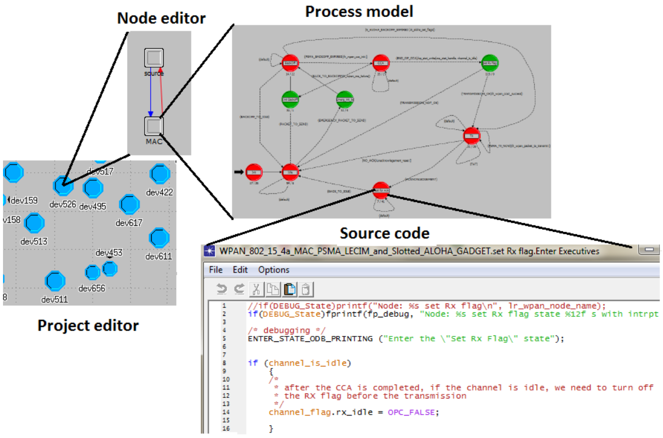
The IEEE 802.15.4k recently became a communication standard for LECIM applications. While it appears to have a promising solution for WSNs in these application areas, its performance must be evaluated carefully. As described earlier, the standard supports non-beacon or beacon-enabled modes of operations with CSMA-CA or Aloha MAC protocols. In the simulation work of this thesis, the objective is to study the performance limits of LECIM with PCA over the DSSS PHY while applying an S-Aloha MAC algorithm in the beacon-enabled mode. The choice of a beacon-enabled mode is because it is flexible; uses a superframe structure that guarantees dedicated bandwidth for low latency requiring applications; and gives to networks the option to work under a controllable duty cycle to achieve a low power consumption compared to the non-beacon enabled mode. The choice of a S-Aloha protocol is because in low traffic conditions it has better performance than CSMA-CA protocol. Besides CSMA-CA, which uses carrier sensing mechanism, is not suitable always in LECIM networks due to the wide coverage and large number of nodes (near-far problem, deep fades, hidden nodes, etc).

To implement and evaluate the IEEE 802.15.4k with DSSS PHY and priority channel access, OPNET modeler is used as the simulation tool. The simulation model focuses on the MAC and PHY layers of the new standard. Initially, the simulator was an implementation of the IEEE 802.15.4 MAC layer and IEEE 802.15.4 UWB PHY specifications which was developed by the Center for Wireless Communications (CWC) for a different research work. For this thesis work, it was mandatory to modify it based on the MAC and DSSS PHY layer specifications of the new standard. Therefore, the modified simulator mainly implements the S-Aloha protocol with and without PCA for priority access and normal access, respectively; non-saturated traffic sources generating normal and high priority data frames; non-ideal channel conditions and different pathloss models. Unfortunately, owing to its broadness to be part of the thesis, MPDU fragmentation is not included in the simulation model.

5.1.1. IEEE 802.15.4k DSSS PHY PCA model in OPNET

The simulation are performed using OPNET modeler version 15.0. OPNET is a packet oriented software that incorporates tools for network model design, simulation, and data collection and analysis. Originally, it was built to model and simulate fixed networks. Consequently, it possesses an extensive library of accurate models of commercially available fixed network hardware and protocols. Nowadays, OPNET also contains broad range of tools for wireless modeling. Although its potential for wireless networks is huge, it does not support the most recent wireless systems. Compared to signal-based simulation tools like MATLAB [66], OPNET has more difficulty in modeling and realizing some wireless communication effects like fading, pathloss, and shadowing. OPNET modeling for new technologies requires significant work.

OPNET modeler has three main hierarchical levels: network domain, node domain and process domain. The network domain specifies the overall scope of the network to be modeled. The project editor is used to create and edit network models, collect statistics directly from each network object or from the whole network, to execute a simulation, and to view results. The network model defines the objects in the system, their physical coordinates, interconnections, and configurations. The node domain defines the individual network nodes. The node editor provides operations to create and edit node models in the network. The node model defines the operational behavior of a network node. Nodes can be fixed or mobile type. The process editor creates process models that control the underlying functionalities of the node models. Process models are represented by finite state machines (FSM) which consist of states with transitions and conditions between them. The states describe the operations performed by a process model using C and C++ languages and OPNET specific built-in functions. A schematic overview of OPNET modeler is shown in Figure 7.



```
//if(DEBUG_State)printf("Node: %s set Rx flag\n", lr_wpan_node_name);
if(DEBUG_State)fprintf(fp_debug, "Node: %s set Rx flag state %12f s with intrpt

/* debugging */
ENTER_STATE_ODB_PRINTING ("Enter the \"Set Rx Flag\" state");


if (channel_is_idle)
    {
    /*
     * after the CCA is completed, if the channel is idle, we need to turn off
     * the RX flag before the transmission
     */
    channel_flag.rx_idle = OPC_FALSE;

    }
```

Figure 7. Hierarchy overview in OPNET modeler.

5.1.2. Description of the simulator

In this thesis, an OPNET simulator implementing a beacon-enabled PAN using the S-Aloha algorithm for LECIM DSSS PHY with PCA is developed. The WSN considered in this model has a star topology; covers a surface area of $790\,\mathrm{m} \times 950\,\mathrm{m}$ as shown in Figure 8. It contains a PAN coordinator and 750 identical, randomly distributed sensor nodes. Besides, a virtual node called channel node is used as part of the implementation. The sensor nodes' main task is generating data and reporting to the PAN coordinator, whereas the PAN coordinator is responsible for collecting reports from the nodes, coordinating the PAN, defining and then informing the superframe structure to the nodes. On the other hand, the channel node is used to model the channel so that the simulation will work properly.

The PAN coordinator periodically transmits enhanced beacon frames to the PAN; informing the sensors about the details of the superframe structure such as the beacon

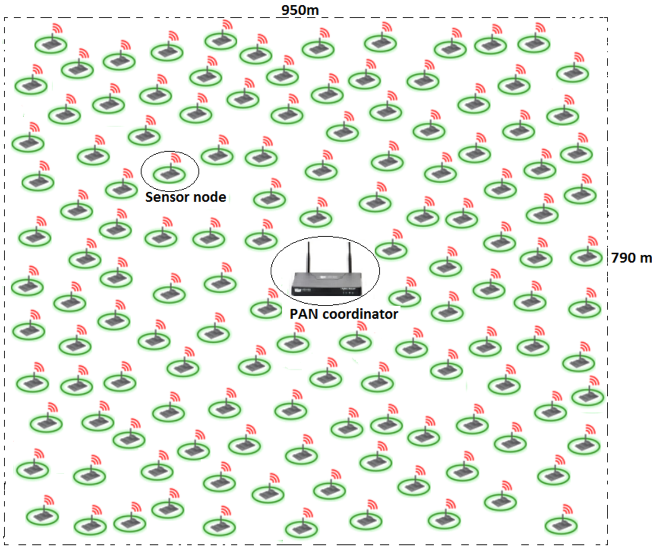


Figure 8. Network model (PAN coordinator, 750 sensor nodes and a channel node.)

interval, slot duration, and PCA allocation rate in the CAP if PCA allocation is enabled. Hence, the sensors are able to communicate in a slotted environment with the coordinator through a contended shared channel. Throughout the simulation, a 100 % duty-cycle is assumed (i.e. $SO = BO$). No sleeping nor a GTS period is considered.

In a beacon enabled mode PAN, the channel is discretized into backoff periods, and the duration of a backoff period should be long enough to accommodate the entire frame transaction. The sensors are informed, through the enhanced beacons, about the backoff period boundaries. Should any one of them send a data message, the transmission must be completed within one backoff period. The duration of one backoff period is determined as

$$\begin{aligned} T_{\mathrm{BP}} \quad &= \quad 2 \times \tau_{\mathrm{p}} + T_{\mathrm{PHY\_HEADER}} + T_{\mathrm{MAC\_HEADER}} + T_{\mathrm{PAY\_LOAD}} \\ &\quad\quad + T_{\mathrm{AckWait}} + T_{\mathrm{minLIFS}} \end{aligned} \tag{3}$$

where T_{BP} is the duration of *aUnitBackoffPeriod*, τ_{p} is packet propagation delay, $T_{\mathrm{PHY\_HEADER}}$ is the PHY header fields duration, $T_{\mathrm{MAC\_HEADER}}$ is the MAC header fields duration, $T_{\mathrm{PAY\_LOAD}}$ is the payload bits duration, T_{AckWait} is the ACK waiting time, T_{minLIFS} represents the minimum duration of a long interframe spacing(LIFS) period.

The coordinator and sensors have a common node model. Their functionalities are differentiated by their address codes and the attributes they use. In this simulator, the communication stack is divided into three major sections: the application layer, where it is modeled by the traffic module; the MAC layer, where it is modeled by the MAC module; and the PHY layer, where it is modeled by the channel node and thus by the channel module. Each module has a process model that defines its functionality.

The traffic module generates acknowledged data frames in the case of sensors or collects data frames forwarded from the lower layers in a coordinator. The sensors generate two types of data frames: status reporting frames which have a constant traffic distribution and generated hourly, daily, or weekly etc; and event-driven (emergency) frames which have a poisson traffic distribution. The latter ones occur very rarely and randomly. In the last gasp scenario, all the sensors transmit emergency messages in burst to the coordinator when they detect the occurrence of a critical event. Example of critical events include fire, short circuit, critical battery, blackout etc. Regardless of the frame type, it is assumed that all sensors generate equal size data frames.

Process models use states and transitions to determine what actions the module can take in response to an event. A state represents the condition of a module, and can be a forced (green) or unforced (red) state. In a forced state, the simulation control is transitioned to the next state right after all the tasks in that state are executed. In unforced state, after executing the state enter executive (tasks), the control is returned to the simulation kernel, and stays there until the next event comes. On the other hand, transitions represent change of a state following to an event. A transition can have a transition executive (a code that is executed in response to a specific event). If a transition is conditional (has transition executive, and represented by a dashed line), then the condition must evaluate to true to pass the simulation control from the source state to the destination state. If a transition is unconditional (solid line), then the control passes from the source state to the destination state immediately.

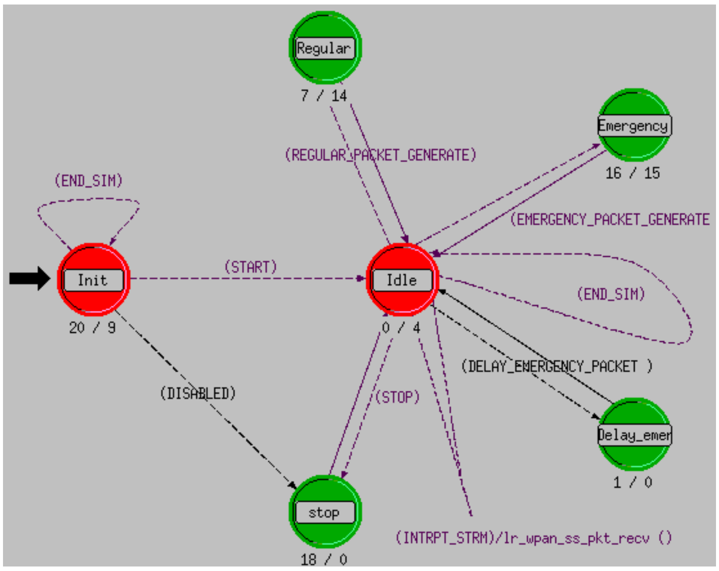


Figure 9. Sensor node data source process model.

The source process model is shown in Figure 9. It starts by initializing the source node at the Init state and it goes to the Idle state if the START condition evaluates to true, or it goes to the stop state if DISABLE evaluates to true. Once in the Idle state, the process model waits for the next event. If the next event represents a 'packet generate' command, then the simulation control goes to the Regular state if REGULAR_PACKET_GENERATE is true, generates a regular packet, passes the packet to the MAC layer, and goes back to the Idle state; or it goes to the Emergency state if EMERGENCY_PACKET_GENERATE is true, generates an emergency packet, passes the packet to the MAC layer, and goes back to the Idle state. If the generated emergency packet requires some delay, then DELAY_EMERGENCY_PACKET becomes true and the packet spends the required amount of time in the Delay_emerg state before it is forwarded to the MAC layer. If the event at the Idle state represents a packet arrival from a MAC layer (applies to a coordinator node), then the INTRPT_STRM transition becomes true, the received packet is collected, statistics updated, and finally destroyed by executing the lr_wpan_ss_pkt_recv() function. When simulation finishes, i.e. END_SIM evaluates to true, then the process model cancels any packet generating schedules, updates statistics and goes to the Stop state to stay in a silent mode. The Delay state is used in the last cast scenario and adds some random internal delay for emergency packets, after their generation, so that they have different forwarding times to the MAC layer and thus level of packet collision is minimized.

The main task of the MAC module is providing channel access to the users. When PCA is enabled, it allocates the calculated PCAs in the CAP; with the first one allocated next to the enhanced beacon frame, and the others are distributed uniformly in the CAP. During the time periods allocated for PCA, only emergency frames access the channel using S-Aloha with PCA algorithm as described in section 4.2.1; and during the non-PCA time periods, both emergency and normal frames access the channel using S-Aloha with PCA and S-Aloha algorithms respectively. In this simulator, each node has separate queues for normal and emergency packets. Generated packets stay in their respective queue until they get channel access. To transmit a packet, the MAC layer always checks the emergency queue first, finishes transmitting all the emergency packets if any. Then the normal packets' queue is checked, and transmits a packet if any. This process repeats every time the MAC tries to transmit a packet. Giving priority to emergency packets enables sensors to deliver alarm messages to the coordinator with very low delay. The MAC module also receives packets from the physical layer, acknowledges them, updates statistics, and sends them to the higher layer.

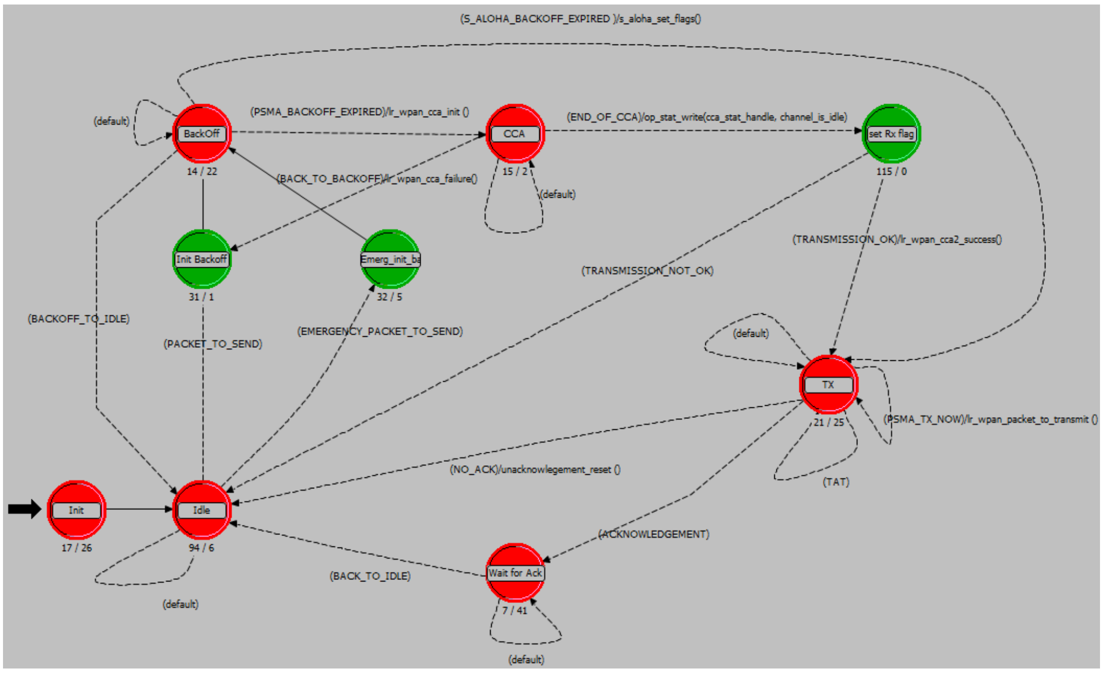

(S_ALOHA_BACKOFF_EXPIRED)/s_aloha_set_flags()
(default)
BackOff
14 / 22
(PSMA_BACKOFF_EXPIRED)/lr_wpan_cca_init ()
CCA
15 / 2
(default)
(END_OF_CCA)/op_stat_write(cca_stat_handle, channel_is_idle)
set Rx flag
115 / 0
(BACK_TO_BACKOFF)/lr_wpan_cca_failure()
Init Backoff
31 / 1
Emerg_init_ba
32 / 5
(TRANSMISSION_OK)/lr_wpan_cca2_success()
(TRANSMISSION_NOT_OK)
(BACKOFF_TO_IDLE)
(PACKET_TO_SEND)
(EMERGENCY_PACKET_TO_SEND)
(default)
TX
21 / 25
(PSMA_TX_NOW)/lr_wpan_packet_to_transmit ()
(TAT)
(NO_ACK)/unacknowlegement_reset ()
Init
17 / 26
Idle
94 / 6
(default)
(ACKNOWLEDGEMENT)
(BACK_TO_IDLE)
Wait for Ack
7 / 41
(default)

Figure 10. Senor node MAC process model.

The MAC module functionality is defined by the MAC process model shown in Figure 10. Once initialized, the process model stays in the Idle state until a packet arrives from a higher layer. When a packet arrives at the MAC layer, its priority and the access period is checked. If the packet is an emergency packet and the current time-slot lies in the CAP period, then EMERGENCY_PACKET_TO_SEND becomes true and the packet is forwarded immediately to the Emerg_init_backoff state to start the PCA backoff algorithm. Next, the simulation control goes immediately to the

Backoff state to perform the random backoff delay. If the packet is a normal packet and the current time-slot lies in a non-PCA but CAP period, then PACKET_TO_SEND becomes true, the process control goes to the Init_backoff state and then to the Backoff state to start applying the random backoff delay; otherwise the process control stays in the Idle state until the current PCA period is over. If there is not enough backoff periods in the CAP to complete the backoff delay or to transmit the packet, BACKOFF_TO_IDLE becomes true and the process returns to the Idle state. In the next beacon interval, the process completes the remaining steps by following the same procedure. When the backoff delay is over and there is enough time to transmit the packet, S_ALOHA_BACKOFF_EXPIRED evaluates to true, the process advances to the Tx state and transmits the packet immediately. Then the process transits to the Wait_for_Ack state if ACKNOWLEDGEMENT is true and waits for an acknowledgement, or the process advances to the Idle state if NO_ACK is true. From the Wait_for_Ack state, the control goes back to the Idle state either on receiving an acknowledgement or when the acknowledgement times out.

The channel node used in the simulator models a basic WPAN channel. It serves to compute bit error rate (BER), the propagation and transmission delays of packets; and to model and realize some prominent wireless communication effects like fading, pathloss, and shadowing. The simulator provides the option AWGN, Nakagami, or Rayleigh fading channel to choose from to model the characteristics of the actual propagation medium, out of which Rayleigh fading channel [67] is used in the simulations. Furthermore, it provides Hata pathloss model [67] for different propagation environments from which suburban area is used in the simulation.

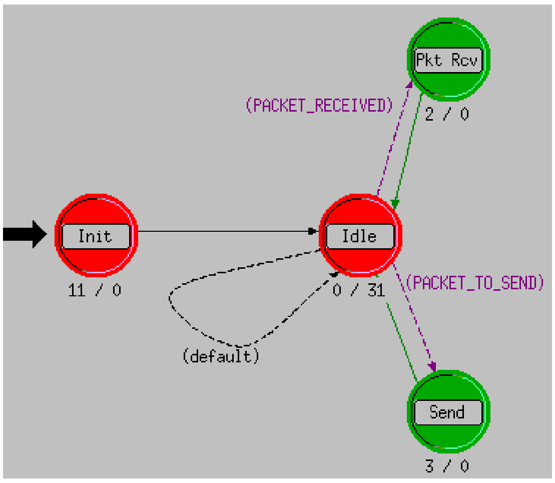


Figure 11. Channel node process model.

The channel process model shown in Figure 11 starts by initializing the channel parameters at the Init state, the process stays at the Idle state until an internal interrupt occurs. If a packet is received from the sensors, then PACKET_RECEIVED becomes true and the process goes to the Pkt_Rcv state. In the Pkt_Rcv state, the process computes packet transmission and propagation times; computes BER by considering a non-ideal channel; and checks for a packet collision in the channel. If the event at the Idle state enables the PACKET_TO_SEND condition, the process goes to the Send state and transmits the packet according to the destination address.

5.2. System Markov model

In this section, a Markov model that characterizes the behavior of the MAC protocol over LECIM DSSS PHY with PCA in non-saturated traffic conditions is proposed. In doing so, it is assumed that an S-Aloha protocol is used, data exchange follows a 2-way handshaking technique, the transmission channel is prone to errors, and the number of sensors, N, is finite.

To reduce probability of packet collision, the MAC protocol performs a random backoff delay before a transmission is made. Let $b(t)$ be a random process representing the backoff counter of a given user. In performing the backoff delay, $b(t)$ decrements in unitary steps in every time slot and when it reaches zero, the user transmits a packet and $b(t)$ takes a new value. The new value of $b(t)$ relies on the size of the contention window from which it is randomly drawn. Let $s(t)$ be a second random process that determines the size of a contention window from which $b(t)$ is drawn. i.e., $s(t) = i$, where i represents the number of transmission attempts (backoff stages). Let W_o be the minimum contention window size corresponding to the first transmission attempt, $i = 0$ and W_i be a contention window size at backoff stage i, where $W_i = 2^i W_o$. The backoff counter at stage i is, therefore, set to a value from the range $[0,W_i - 1]$ following a uniform distribution. A transmitted packet is considered successful when the transmitter receives the corresponding ACK, otherwise it is unsuccessful. Packet transmission can fail either due to collision or due to erroneous reception. In such a case, the transmitter contends again for access by doubling its contention window (i.e, i increments by one) until maximum window size is reached. It repeats this process until either the packet is successfully transmitted or dropped after a total of $m+1$ transmission attempts. Therefore, the processes $(s(t),b(t))$ define a 2-dimensional Markov model of the system. A transmitted packet can be received in error with a probability of p_e, or it can collide with other packets with a probability of p_{col}. Note that p_{col} and p_e are assumed as statistically independent events.

In LECIM networks, there are normal and emergency packets. In this Markov modeling, the packet priorities are treated differently as they have different channel access mechanisms. The corresponding Markov chains for normal packets and for emergency packets are shown in Figures 12 and 13 respectively.

5.2.1. Throughput analysis

Throughput computation for normal packets

The Markov chain in Figure 12 shows different states, including the one labeled *I* (idle). State *I* is used to account the non-saturated data traffic in LECIM networks and models the following cases:

- after a successful transmission, the user has no packet in its queue, or
- the user is in an idle state, no packet in its queue and waits for one to arrive, or
- $m + 1$ transmission attempts failed, the packet is dropped and the user has no other packets in its queue.

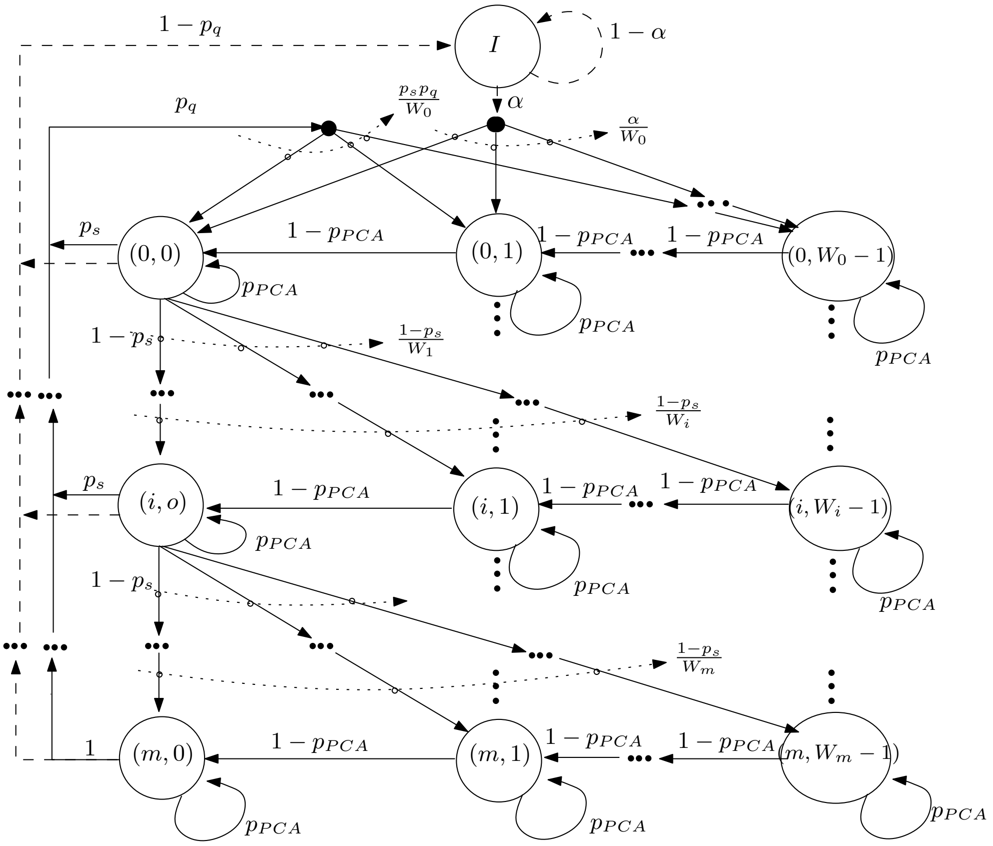


Figure 12. Markov model for normal packets for an S-Aloha protocol based system considering the scenario PCA allocation enabled, non-saturated traffic conditions, a two-way handshaking scheme and non-ideal channel.

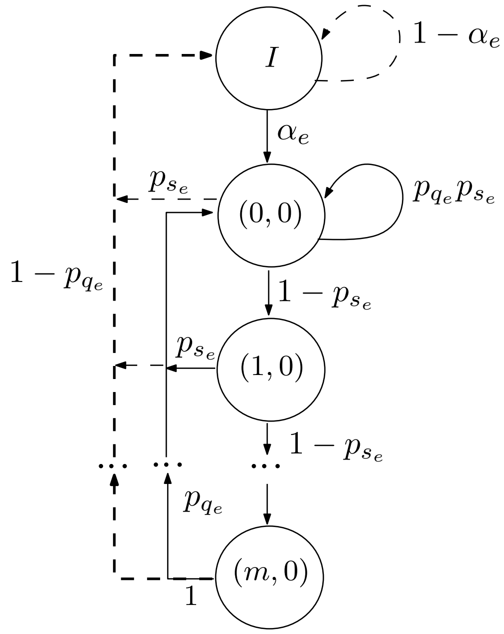


Figure 13. Markov model for high priority packets for an S-Aloha protocol based system considering the scenario PCA allocation enabled, non-saturated traffic conditions, a two-way handshaking scheme and non-ideal channel.

It can also be noticed that the model contains $m + 1$ different backoff stages. This implies a failed packet transmission can make up to m number of retransmissions before it is dropped. Regardless of the current backoff stage, a packet transmission is made only in the $(i{,}0)$ states. If a transmission attempt on the $(i{,}0)$ states is successful, then the transmitter goes back to one of the $(0{,}k)$ states with probability $\frac{p_{\mathrm{s}}p_{\mathrm{q}}}{W_{\mathrm{o}}}$ if at least one packet is present in its queue, where p_{q} is the probability of having at least one packet in the queue and p_{s} is the probability of a successful transmission, otherwise the device advances to the *I* state to wait for new packet to arrive. Otherwise, the backoff stage is incremented by one and the new state will be $(i+1{,}k)$ with probability $\frac{1-p_{\mathrm{s}}}{W_{i+1}}$. Note that a uniform distribution between the states in the same backoff stage is assumed.

The following transition probabilities can be drawn from the Markov model depicted in Figure 12. For $p_{i,k} = Pr\{s(t) = i{,}b(t) = k\}$, we have

$$\begin{array}{lll}
p_{i,k/i,k+1} = & 1 - p_{\mathrm{PCA}}, & k\,\epsilon\,[0{,}W_i - 1],\, i\,\epsilon\,[0{,}m] \\
p_{0,k/i,0} = & \dfrac{p_{\mathrm{q}}p_{\mathrm{s}}}{W_0}, & k\,\epsilon\,[0{,}W_i - 1],\, i\,\epsilon\,[0{,}m-1] \\
p_{0,k/m,0} = & \dfrac{p_{\mathrm{q}}}{W_0}, & k\,\epsilon\,[0{,}W_i - 1],\, i = m \\
p_{i,k/i-1,0} = & \dfrac{1 - p_{\mathrm{s}}}{W_i}, & k\,\epsilon\,[0{,}W_i - 1],\, i\,\epsilon\,[1{,}m] \\
p_{\mathrm{I}/i,0} = & (1 - p_{\mathrm{q}})p_{\mathrm{s}},. & i\,\epsilon\,[0{,}m-1] \\
p_{\mathrm{I}/m,0} = & 1 - p_q,. & i = m \\
p_{\mathrm{I}/\mathrm{I}} = & 1 - \alpha & \\
p_{0,k/\mathrm{I}} = & \dfrac{\alpha}{W_0} &
\end{array} \tag{4}$$

where α is the probability of packet arrival in one time slot and p_{PCA} is the probability of the next time slot lies in one of the allocated PCAs and is given by

$$p_{\mathrm{PCA}} = \frac{mT_{\mathrm{PCA}}}{T_{\mathrm{superframe}}} \tag{5}$$

where T_{PCA} is duration of one PCA in seconds, $T_{\mathrm{superframe}}$ is SD in seconds, and m is the number of PCAs allocated in the CAP period.

The different equations in (4) can be explained as follows. The first one describes that at the beginning of each time slot, the backoff counter decrements by one if the time slot does not lie in one of the PCA periods. The second equation explains that after a successful packet transmission and when there is at least one packet in the queue, a new packet transmission starts in the first backoff stage. Equation three, in addition to what is said in equation two, accounts the fact following $m + 1$ unsuccessful transmissions. The user drops that packet and plans to transmit a new one, if any. The fourth equation explains the need for a new contention window following an unsuccessful transmission. The fifth and sixth equations state that the user transits to the *I* sate after a successful transmission or after $m + 1$ unsuccessful transmissions, $i = m$, and when there is no packet waiting for transmission. Finally, equation seven deals with the situation that the sensor has no packet to transmit, and thus stays in the

I state until a packet arrives. When a packet arrives at the *I* state with a probability of α, as modeled by the last equation, the user schedules a new backoff time in backoff stage 0.

Now, it is time to determine the stationary probabilities of each state, i.e., the probability of a user occupying a given state at any time slot. Let,

$$b_{i,k} = \lim_{t\to\infty} Pr\{s(t) = i,b(t) = k\} \qquad \forall k \,\epsilon\, [0,W_i - 1], \forall i \,\epsilon\, [0,m]. \tag{6}$$

Therefore, for the $(i,0)$ states

$$b_{i,0} = (1 - p_{\mathrm{s}})b_{i-1,0} + b_{i,0}p_{\mathrm{PCA}} = \left(\frac{1 - p_s}{1 - p_{\mathrm{PCA}}}\right)^i b_{0,0}, \quad \forall i \,\epsilon\, [1,m] \tag{7}$$

For the idle state, let its stationary probability be b_I, given by

$$\begin{aligned} b_I &= (1 - p_{\mathrm{q}})p_{\mathrm{s}} \sum_{i=0}^{m} b_{i,0} + (1 - \alpha)b_{\mathrm{I}} + (1 - p_{\mathrm{q}})(1 - p_{\mathrm{s}})b_{m,0} \\ &= \frac{1}{\alpha}\left[(1 - p_{\mathrm{q}})p_{\mathrm{s}} \sum_{i=0}^{m} b_{i,0} + (1 - p_{\mathrm{q}})(1 - p_{\mathrm{s}})b_{m,0}\right]. \end{aligned} \tag{8}$$

The other stationary distributions, $b_{i,k}$, are determined as follows. For backoff stage 0, $b_{0,k}$ is given by

$$b_{0,k} = \frac{W_0 - k}{W_0(1 - p_{\mathrm{PCA}})}\left[p_{\mathrm{q}}p_{\mathrm{s}} \sum_{i=0}^{m} b_{i,0} + p_{\mathrm{q}}(1 - p_{\mathrm{s}})b_{m,0} + \alpha b_{\mathrm{I}}\right]. \tag{9}$$

Upon substitution of (8) in (9), we have

$$b_{0,k} = \frac{W_0 - k}{W_0(1 - p_{\mathrm{PCA}})}\left[p_{\mathrm{s}} \sum_{i=0}^{m} b_{i,0} + (1 - p_{\mathrm{s}})b_{m,0}\right]. \tag{10}$$

Similarly, $b_{i,k}$ for $i \,\epsilon\, [1,m]$ is given by

$$b_{i,k} = \frac{W_i - k}{W_i(1 - p_{\mathrm{PCA}})}(1 - p_s)b_{i-1,0}. \tag{11}$$

Substituting (7) in (11)

$$b_{i,k} = \left(\frac{W_i - k}{W_i}\right)\left(\frac{1 - p_{\mathrm{s}}}{1 - p_{\mathrm{PCA}}}\right)^i b_{0,0}. \tag{12}$$

The value of $b_{0,0}$ can be obtained from the fact that the sum of all stationary probabilities in Figure 12 must add up to give 1. i.e.,

$$\begin{aligned} 1 &= \sum_{i=0}^{m} \sum_{k=0}^{W_i-1} b_{i,k} + b_{\mathrm{I}} \\ &= \sum_{k=0}^{W_0-1} b_{0,k} + \sum_{i=1}^{m} \sum_{k=0}^{W_i-1} b_{i,k} + b_{\mathrm{I}}. \end{aligned} \tag{13}$$

Upon substitution of (8), (10), and (12) in (13), and approximating $b_{m,0}$ to zero gives:

$$b_{0,0} = \frac{(2p_{\mathrm{s}} - p_{\mathrm{PCA}} - 1)(p_{\mathrm{s}} - p_{\mathrm{PCA}})}{a + b + c + d} \tag{14}$$

where $a = \frac{W_0}{2}(1 - p_{\mathrm{PCA}})(p_{\mathrm{s}} - p_{\mathrm{PCA}})(1 - (2e)^{m+1})$
$b = (2p_{\mathrm{s}} - p_{\mathrm{PCA}} - 1)(p_{\mathrm{s}} - p_{\mathrm{PCA}})\left(\frac{W_0+1}{2}\right)$
$c = \frac{1}{2}(1 - p_{\mathrm{PCA}})(2p_{\mathrm{s}} - p_{\mathrm{PCA}} - 1)(1 - e^{m+1})$
$d = p_{\mathrm{s}}(1 - p_{\mathrm{PCA}})(2p_{\mathrm{s}} - p_{\mathrm{PCA}} - 1)(1 - e^{m+1})(\frac{W_0+1}{2(1-p_{PCA})} + \frac{1-p_{\mathrm{q}}}{\alpha})$
$e = \frac{1-p_{\mathrm{s}}}{1-p_{\mathrm{PCA}}}$.

It is known that packet transmission occurs from the $(i{,}0)$ states, and thus the total probability that a sensor transmits in any random time slot, τ_{R}, is computed as

$$\tau_{\mathrm{R}} = \sum_{i=0}^{m} b_{i,0} = \sum_{i=1}^{m} b_{i,0} + b_{0,0}. \tag{15}$$

Substitution of (7) in (15) produces

$$\tau_{\mathrm{R}} = \sum_{i=1}^{m} \left(\frac{1 - p_s}{1 - p_{\mathrm{PCA}}}\right)^{i} b_{0,0} + b_{0,0}. \tag{16}$$

For $\frac{1-p_{\mathrm{s}}}{1-p_{\mathrm{PCA}}} < 1$, and using the geometric series approximation in (16), τ_R becomes

$$\tau_{\mathrm{R}} = \left(\frac{1 - p_{\mathrm{PCA}}}{p_{\mathrm{s}} - p_{\mathrm{PCA}}}\right)\left[1 - \left(\frac{1 - p_{\mathrm{s}}}{1 - p_{PCA}}\right)^{m+1}\right] b_{0,0}. \tag{17}$$

Substituting the expressions of $b_{0,0}$, a,b, c,d and e from (67) in (17), τ_R becomes

$$\tau_{\mathrm{R}} = \frac{(1 - p_{\mathrm{PCA}})(2p_{\mathrm{s}} - p_{\mathrm{PCA}} - 1)(1 - e^{m+1})}{a + b + c + d}. \tag{18}$$

To compute the system throughput, the different probabilities such as p_{col}, p_{s}, p_{q},α, and the probability of transmitting at least one packet in a given time slot (p_{t}), should be first determined. The system model assumes N sensors contending for medium access, each one transmitting with probability τ_{R}.

A transmitting sensor experiences packet collision when at least one of the $N - 1$ sensors transmits another packet during the same time slot. Hence, p_{col} is given by

$$p_{\mathrm{col}} = 1 - (1 - \tau_{\mathrm{R}})^{N-1}. \tag{19}$$

In a given time slot, each of the N sensors has a transmitting probability of τ_{R}; and thus the value of p_{t} is computed by

$$p_t = 1 - (1 - \tau_{\mathrm{R}})^{N}. \tag{20}$$

A packet is successfully delivered only if it neither collides nor faces a channel error. Hence, p_{s} is given by

$$\begin{aligned} p_{\mathrm{s}} &= (1 - p_{\mathrm{col}})(1 - p_{\mathrm{e}}) \\ &= (1 - \tau_{\mathrm{R}})^{N-1}(1 - p_{\mathrm{e}}). \end{aligned} \tag{21}$$

p_{suc} is the probability that exactly one sensor transmits on the considered time slot given that at least one of the N sensors transmits

$$p_{\text{suc}} = \frac{N\tau_{\text{R}}\left(1-\tau_{\text{R}}\right)^{N-1}}{1-\left(1-\tau_{\text{R}}\right)^{N}}. \tag{22}$$

Also α, the probability of packet arrival in one time slot, for a single device is calculated as

$$\alpha = \frac{1}{T_{\text{IAT}}} \tag{23}$$

where T_{IAT} represents the total number of slots in one packet inter-arrival time.

The last term, p_{q}, is calculated as the probability of at least one packet is available in the buffer in a service time of n time-slots.

$$p_{\text{q}} = 1-(1-\alpha)^{n}. \tag{24}$$

Now that all the necessary analysis is made, the final step is to compute the system throughput (S). Throughput is defined as the fraction of time the channel is used to successfully transmit a packet payload. For S-Aloha protocol, S is calculated as

$$S = p_{\text{t}}p_{\text{suc}}(1-p_{\text{e}})E[payload] \tag{25}$$

where $p_{\text{t}}p_{\text{suc}}(1-p_{\text{e}})$ is the probability of only one node transmits in the considered time-slot and the channel does not introduce an error; and $E[payload]$ is the average packet payload size expressed in time slots. Upon substitution of (20) and (22) in (25) gives

$$S = N\tau_{\text{R}}\left(1-\tau_{\text{R}}\right)^{N-1}(1-p_{\text{e}})E[payload]. \tag{26}$$

Throughput computation for emergency packets

In this case, the Markov chain model shown in Figure 13 is used. The working principle of this model and the one shown in Figure 12 are similar except that the following changes are specific to the former one. The first difference is as far as the time slots are in the CAP period, the emergency packets have no restrictions for transmission. In other words, the backoff counter always decrements with a probability of one. The second difference is once a packet transmission fails, the backoff stage is incremented by one as usual, but the contention window remains the same, i.e., all backoff stages have the same contention window. Consequently, the Markov chain model for emergency packets is obtained by applying the modifications to the Markov chain model given in Figure 12. Since the procedure in all backoff stages is the same, the Markov chain is collapsed and the simplified model for emergency packets is indicated in Figure 13. The transition probabilities of the new model are, therefore, given

$$\begin{aligned}
p_{0,0/i,0} &= p_{\text{q}_{\text{e}}}p_{\text{s}_{\text{e}}}, && i\,\epsilon\,[0,m-1]\\
p_{0,0/m,0} &= p_{\text{q}_{\text{e}}}, && i=m\\
p_{i,0/i-1,0} &= 1-p_{\text{s}_{\text{e}}}, && i\,\epsilon\,[1,m]\\
p_{\text{I}/i,0} &= (1-p_{\text{q}_{\text{e}}})p_{\text{s}_{\text{e}}}. && i\,\epsilon\,[0,m-1]\\
p_{\text{I}/m,0} &= 1-p_{\text{q}_{\text{e}}}, && i=m\\
p_{\text{I}/\text{I}} &= 1-\alpha_{\text{e}}\\
p_{0,0/\text{I}} &= \alpha_{\text{e}}
\end{aligned} \tag{27}$$

where p_{q_e} is probability of emergency queue not empty, p_{s_e} is probability of success for emergency packets, and α_e is probability of emergency packet arrival in one time slot.

The first and second equations in (27) describe that after the current packet transmission and if there is a packet in the buffer, a new transmission starts at the $(0,0)$ state. The third one explains the need for a packet retransmission following an unsuccessful transmission. The fourth and fifth equations deal with the situation following the current packet transmission and when there is no packet in the buffer. Equations six and seven explain the situation related with a packet arrival.

In this model there are $m + 2$ states, and the corresponding stationary distributions are computed as

$$b_{i,0} = (1 - p_{\mathrm{s_e}})b_{i-1,0} = (1 - p_{\mathrm{s_e}})^i b_{0,0}, \qquad i \,\epsilon\, [1,m]. \tag{28}$$

The expression for b_I is given by (8). To calculate $b_{0,0}$, the logic discussed previously is used

$$1 = \sum_{i=0}^{m} b_{i,0} + b_{\mathrm{I}}. \tag{29}$$

Substituting (28) and the expression of e in (29), and rearranging the terms results in

$$b_{0,0} = \frac{\alpha_{\mathrm{e}}(1 - e)}{(1 - e^{m+1})(\alpha_e + (1 - p_{\mathrm{q_e}})p_{\mathrm{s_e}})}. \tag{30}$$

The probability of a sensor transmitting an emergency packet in a given time slot, τ_E, is calculated as

$$\tau_{\mathrm{E}} = \sum_{i=0}^{m} b_{i,0}. \tag{31}$$

By using (28) for $b_{i,0}$ and then (30) for $b_{0,0}$ in (31) gives

$$\tau_E = \frac{\alpha_{\mathrm{e}}}{\alpha_e + (1 - p_{\mathrm{q_e}})p_{\mathrm{s_e}}}. \tag{32}$$

In this model, the packets have exponential inter-arrival times. For a single device, the value of α_e is approximated by

$$\alpha_{\mathrm{e}} = \frac{1}{E[T_{\mathrm{IAT}}]} \tag{33}$$

where $E[T_{\mathrm{IAT}}]$ is expected number of time-slots in one packet inter-arrival time of emergency packets.

The other terms such as probability of collision for emergency packets $(p_{\mathrm{col_e}})$, probability of transmitting at least one emergency packet in a give time slot $(p_{\mathrm{t_e}})$, $p_{\mathrm{s_e}}$, the conditional probability of success for emergency packet $(p_{\mathrm{suc_e}})$, and $p_{\mathrm{q_e}}$ are determined as in (19), (20), (21), (22), and (24) respectively, where τ_R is substituted by τ_E. As a result, S for this model is determined using

$$S = N\tau_E \left(1 - \tau_{\mathrm{E}}\right)^{N-1} (1 - p_{\mathrm{e}})E[payload]. \tag{34}$$

Overall system throughput

Regardless of the traffic type, the overall system throughput is computed next. Owing to the existence of the two traffic types, the new expressions for $p_{\mathrm{suc_e}}$ and $p_{\mathrm{t_e}}$ are given as

$$p_{\mathrm{suc_o}} = \frac{N\tau_{\mathrm{R}}(1-\tau_{\mathrm{R}})^{N-1}p_{\mathrm{R}} + N\tau_{\mathrm{E}}(1-\tau_{\mathrm{E}})^{N-1}p_{\mathrm{E}}}{1-[(1-\tau_{\mathrm{R}})^{N}p_{\mathrm{R}} + (1-\tau_{\mathrm{E}})^{N}p_{\mathrm{E}}]} \tag{35}$$

$$p_{\mathrm{t_o}} = 1 - \left[(1-\tau_{\mathrm{R}})^{N}p_{\mathrm{R}} + (1-\tau_{\mathrm{E}})^{N}p_{\mathrm{E}}\right] \tag{36}$$

where $p_{\mathrm{suc_o}}$ is overall conditional probability of success, $p_{\mathrm{t_o}}$ is overall probability of transmitting at least one packet in a give time slot, p_{R} is the probability of a normal packet transmitted, and p_{E} is the probability of an emergency packet transmitted. They are defined as

$$p_{\mathrm{R}} = \frac{\tau_{\mathrm{R}}}{\tau_{\mathrm{R}}+\tau_{\mathrm{E}}} \tag{37}$$

$$p_{\mathrm{E}} = \frac{\tau_{\mathrm{E}}}{\tau_{\mathrm{R}}+\tau_{\mathrm{E}}}. \tag{38}$$

Now, the overall system throughput can be computed as

$$S = p_{\mathrm{suc_o}}p_{\mathrm{t_o}}(1-p_{\mathrm{e}})E[payload]. \tag{39}$$

Substituting (35) and (36) in (39) and using the expressions for p_{R} and p_{E} results in

$$S = \frac{\left(N\tau_{\mathrm{R}}^{2}\left(1-\tau_{\mathrm{R}}\right)^{N-1} + N\tau_{\mathrm{E}}^{2}\left(1-\tau_{\mathrm{E}}\right)^{N-1}\right)(1-p_{\mathrm{e}})E[payload]}{\tau_{\mathrm{R}}+\tau_{\mathrm{E}}}. \tag{40}$$

5.2.2. Delay analysis

In this section two types of packet delays will be analyzed: MAC delay and end-to-end delay for both packet types. MAC delay covers the time interval from the time a packet is at the head of its MAC queue ready for transmission until the corresponding ACK is received, whereas end-to-end delay covers the time interval from packet generation up to the successful reception of the packet by the destination device. End-to-end delay is the sum of MAC delay and the queueing delay of a given packet. In both cases, the delay analysis accounts the average delays of only successfully transmitted packets, dropped packets are not considered.

MAC delay for normal packets

Let $E[D_i]$ be the average delay of a successfully transmitted packet, transmitted from the i^{th} backoff stage. The delay D_i is the sum of all delay times experienced in the previous i backoff stages. Hence, $E[D_i]$ is calculated as

$$E[D_i] = T_{\mathrm{s}} + iT_{\mathrm{c}} + E[T_{\mathrm{slot}}]\sum_{l=0}^{i}E[D_l], \qquad 0 \leq i \leq m \tag{41}$$

where T_s is the time taken to successfully transmit a packet from stage i; T_c is the time taken for a collided packet which was transmitted from the $i-1$ backoff stage; iT_c is the duration of i collisions occurred before it succeeds in the i^{th} backoff stage; $E[T_\mathrm{slot}]$ is the average slot duration; and $E[D_l]$ is the average number of time-slots that the sensor backs off in a given backoff stage. Note that T_s, T_c and $E[T_\mathrm{slot}]$ have all equal values which is one time-slot when an S-Aloha protocol is used.

$E[D_l]$ for a normal packet can be estimated as

$$E[D_l] = \sum_{k=0}^{W_l-1} \frac{k}{W_l} \left(1 + 4p_\mathrm{PCA} + p_\mathrm{emerg\_gen} E[D_\mathrm{MAC\_emerg}]\right) \tag{42}$$

where $p_\mathrm{emerg\_gen}$ is probability of emergency packet generation in the non-PCA period, and $1 + 4p_\mathrm{PCA} + p_\mathrm{emerg\_gen}E[D_\mathrm{MAC\_emerg}]$ is the total number of time-slots a normal packet may spend in one of the (i,k) states. It is approximated that only one emergency packet maybe generated during the $W_l - 1$ contention period. $p_\mathrm{emerg\_gen}$ is given by

$$p_\mathrm{emerg\_gen} = \lambda e^{-\lambda}(1 - p_\mathrm{PCA}). \tag{43}$$

where λ is packet arrival rate. So, the final expression for $E[D_l]$ is

$$E[D_l] = \sum_{k=0}^{W_l-1} \frac{k}{W_l} \left(1 + 4p_\mathrm{PCA} + \lambda e^{-\lambda}(1 - p_\mathrm{PCA})E[D_\mathrm{MAC\_emerg}]\right). \tag{44}$$

Let p_i be the probability that a successfully transmitted packet is transmitted from the i^{th} backoff stage, and is defined as

$$p_i = \frac{p_\mathrm{s}(1-p_\mathrm{s})^i}{1-(1-p_\mathrm{s})^{m+1}}, \qquad 0 \le i \le m. \tag{45}$$

In (45), it is clear to see that the packet reaches the i^{th} stage with a probability of $(1-p_\mathrm{s})^i$ and is successfully transmitted from the i^{th} backoff stage provided that it is not dropped, $1-(1-p_\mathrm{s})^{m+1}$.

The final step is to determine the average MAC delay $(E[D_\mathrm{MAC\_normal}])$ and it is computed as

$$E[D_\mathrm{MAC\_normal}] = \sum_{i=0}^{m} p_i E[D_i]. \tag{46}$$

Substituting the expressions of $E[D_i]$ and p_i in (46) results in

$$E[D_\mathrm{MAC\_normal}] = \sum_{i=0}^{m} \left(\frac{p_\mathrm{s}(1-p_\mathrm{s})^i}{1-(1-p_\mathrm{s})^{m+1}}\right) \left(T_\mathrm{s} + iT_\mathrm{c} + E[T_\mathrm{slot}] \sum_{l=0}^{i} E[D_l]\right) \tag{47}$$

where p_s and $E[D_l]$ are given in (21) and (44) respectively.

End-to-end delay for normal packets

The queueing delay of a normal packet is the time spent in the queue while waiting until high priority packets or previously arrived normal packets get service. Queueing delay for normal packets can be calculated as

$$D_{\text{Q\_normal}} = \sum_{i=1}^{\infty} p_l^i E[D_{\text{MAC\_emerg}}] \tag{48}$$

where p_l is the probability of a node generating an emergency packet in $E[D_{\text{MAC\_normal}}]$ time and $(E[D_{\text{MAC\_emerg}}])$ is given in (53). p_l is determined by

$$p_l = \frac{E[D_{\text{MAC\_normal}}]}{E[T_{\text{IAT}}]}. \tag{49}$$

Upon substitution of (49) in (48), $D_{\text{Q\_normal}}$ becomes

$$D_{\text{Q\_normal}} = \sum_{i=1}^{\infty} \left(\frac{E[D_{\text{MAC\_normal}}]}{E[T_{\text{IAT}}]} \right)^i E[D_{\text{MAC\_emerg}}]. \tag{50}$$

Once $D_{\text{Q\_normal}}$ and $E[D_{\text{MAC\_normal}}]$ are found, the average end-to-end delay of normal packets $(D_{\text{e2e\_normal}})$ can be given by

$$D_{\text{e2e\_normal}} = D_{\text{Q\_normal}} + E[D_{\text{MAC\_normal}}]. \tag{51}$$

MAC delay for emergency packets

For such packets, $E[D_i]$ is given using (41) with the exception that $P_{\text{PCA}} = 0$, and thus $E[D_l]$ is approximated by

$$E[D_l] = \frac{W_l - 1}{2}, \qquad l \, \epsilon \, [0,i]. \tag{52}$$

Therefore, the average MAC delay of emergency packets $(E[D_{\text{MAC\_emerg}}])$ is obtained by inserting (52) in (47) (in time-slots)

$$E[D_{\text{MAC\_emerg}}] = \sum_{i=0}^{m} \left(\frac{p_{\text{s}_\text{e}}(1-p_{\text{s}_\text{e}})^i}{1-(1-p_{\text{s}_\text{e}})^{m+1}} \right) \left(T_\text{s} + iT_\text{c} + E[T_{\text{slot}}] \sum_{l=0}^{i} \frac{W_l - 1}{2} \right) \tag{53}$$

where p_{s_e} is given in (21) after replacing τ_R by τ_E.

End-to-end delay for emergency packets

When PCA allocation is enabled, emergency packets have almost zero queueing delay. The queueing delay of emergency packets $(D_{\text{Q\_emerg}})$ is approximated by

$$\begin{aligned} D_{\text{Q\_emerg}} &= \sum_{i=2}^{\infty} p_l^i E[D_{\text{MAC\_emerg}}] \\ &= \sum_{i=2}^{\infty} \left(\frac{E[D_{\text{MAC\_normal}}]}{E[T_{\text{IAT}}]} \right)^i E[D_{\text{MAC\_emerg}}]. \end{aligned} \tag{54}$$

Therefore, the average end-to-end delay of emergency packets ($D_{\text{e2e\_emerg}}$) is expected to be much shorter than that of the normal packets and is obtained as

$$D_{\text{e2e\_emerg}} = D_{\text{Q\_emerg}} + E[D_{\text{MAC\_emerg}}]. \tag{55}$$

6. RESULTS AND DISCUSSION

In this section, the configuration and parameter settings of the IEEE 802.15.4k DSSS PHY with PCA model in OPNET and the performance metrics used are presented. The simulation scenarios considered and the corresponding results are presented and discussed. Also, simulation and analytical results are compared and discussed.

6.1. Simulation settings

The simulation parameters used to model the WSN are classified into three groups: general, MAC layer related, and PHY layer related simulation parameters. The parameters are summarized in Tables 7, 8, and 9, respectively. Other parameters which are not described in these tables are set to their default values as specified by the standard [3]. The general and PHY layer related parameters are common to all simulated scenarios, whereas a few of the MAC layer related parameter values may change in some scenarios and they will be explained in more detail.

Table 7. General simulation parameters

Parameter	Value / Type	Remark
normal packet interarrival time	10 min	Normal packets' interarrival time (constant traffic distribution)
emergency packet interarrival time	4 hrs	Emergency packets interarrival time (Poisson traffic distribution)
payload size	23 octets	Payload size
Topology type	star	
N	750	number of sensor nodes in the network
Synchronization type	beacon-enabled	MAC mode of operation
Protocol type	S-Aloha with PCA	MAC protocol used for LECIM

Table 8. MAC layer related simulation parameters

Parameter	Value / Type	Remark
SO	10	Superframe order
BO	10	Beacon order
ACK	40 bits	Acknowledgement frame
symbol	10 μs	One symbol duration
aMinMPDUOverhead	9 octets	MAC minimum overhead length
macAckWaitDuration	92 symbols	Maximum time to wait for an ACK
aTurnaroundTime	12 symbols	Turn around time
aMinLISFPeriod	40 symbols	Minimum LIFS length
aBaseSlotDuration	526 symbols	Minimum slot duration
Allocation rate	3	number of PCAs allocated per superframe
macMinBE	3	Minimum backoff exponent
T_{slot}	16.9 ms	One *macLECIMAlohaUnitBackoffPeriod* duration
PCA duration	4 backoff periods	Nb of *macLECIMAlohaUnitBackoffPeriod* per CAP
delay tolerance	15 s	Critical message delay tolerance

The model is set up to support 750 identical and randomly distributed sensor nodes. The sensor nodes are set to generate equal-sized normal and emergency data packets. A smaller payload size is used because the model does not implement MPDU fragmentation and, therefore, the unfragmented MPDU packet size should meet the maximum

Table 9. PHY layer related simulation parameters

Parameter	Value / Type	Remark
PHY payload	32 octets	PHY layer payload size
aMaxPHYPacketSize	32 octets	Maximum PPDU packet size
data rate	31 kbps	Data rate
channel	865.125 MHz	Center frequency
bandwidth	200 kHz	Bandwidth
power	0.1 W	Transmit power
h_m	2 m	Sensor node antenna height (used in Hata model)
h_b	10 m	Collector node antenna height (used in Hata model)
modulation type	BPSK	Modulation technique used to compute data-rate
channel type	Rayleigh fading	Varying propagation environment
Hata pathloss model	Suburban	Pathloss model used
k	40.54	Hata model constant
γ	free space	Pathloss exponent
τ_p	3 ms	Propagation time
carrier sense sensitivity	-120 dBm	Receiver sensitivity
transmission range	10 km	Coverage range

PPDU packet size requirements. The packet inter-arrival time and the traffic distribution used in each packet type are specified in Table 7. In actual LECIM networks, sensor nodes periodically send operational/normal packets to the coordinator, and thus they are modeled by a constant traffic distribution; whereas emergency packets are modeled by Poisson traffic distribution to imply their random generation. The packet inter-arrival time for each packet type can be much greater than the ones given here, but the selection of these parameter values is intended to study the system performance under low traffic conditions.

In all the simulation scenarios, a 100% active superframe $(SO = BO)$ duty-cycle is used, meaning that if *SO* changes, *BO* also changes; the entire packet transaction completes in one *macLECIMAlohaUnitBackoffDuration* duration, T_{slot}. To materialize the statistical significance of the simulation results, for every simulation with the same input parameters, OPNET simulations are made with multiple random seeds, from which the mean value is computed for each performance metric. In most cases, the simulation time used is limited to 24 hours because the network supports large number of endpoints and, therefore, the simulator takes a long time to complete the entire simulation. The larger the number of endpoints in the network, the longer the simulation duration. Otherwise, the network size could be extended if required.

6.2. Performance metrics

The performance of the LECIM DSSS PHY with PCA is evaluated in terms of MAC-to-MAC and end-to-end communication performance metrics; and they are packet delivery ratio, success probability, average packet delay, and throughput. All simulation scenarios are simulated over a varying number of retransmissions. The number of retransmissions varies from 2 to 8 per each packet transmission attempt.

Packet delivery ratio *(PDR)* is an end-to-end reliability measure of the network. It evaluates how many of the generated packets have successfully been received at the destination, and it is computed as

$$PDR = \frac{Pkt_{\text{received}}}{Pkt_{\text{generated}}} \tag{56}$$

where Pkt_{received} is the total number of successfully received packets and $Pkt_{\text{generated}}$ is the total number of generated data packets in the application layer.

Similarly, network reliability can be evaluated in terms of individual transmission attempt success probability (P_{s}) as

$$P_s = \frac{Pkt_{\text{received}}}{Pkt_{\text{sent}}} \tag{57}$$

where Pkt_{sent} is the total number of packets sent. The value of P_{s} reflects the level of failure each first transmission attempt experiences before it succeeds, and its maximum value is 1 which implies that all first transmission attempts are successful.

Another network performance metric is the average delay experienced by a successfully received packet during transmission. Packet delay can be expressed in terms of an end-to-end delay (D_{e2e}) or in terms of a MAC delay (D_{MAC}). D_{e2e} represents the average delay from source to sink, and is formulated as

$$D_{\text{e2e}} = \frac{\sum_i D_{e2e_i}}{Pkt_{\text{received}}} \tag{58}$$

where D_{e2e_i} is the end-to-end delay of a single packet. Similarly, D_{MAC} is the average MAC delay of a packet and is given as

$$D_{\text{MAC}} = \frac{\sum_i D_{MAC_i}}{Pkt_{\text{received}}} \tag{59}$$

where D_{MAC_i} represents the MAC delay of a single packet. D_{e2e} is the sum of D_{MAC} and the average queueing delay of each packet.

The fourth performance metric is network throughput (S). It measures how much of the total time is used to transmit useful information, and is computed as [68]

$$S = \frac{U}{B + I} \tag{60}$$

where U is the number of useful time slots, B is the number of busy time slots, and I is the number of idle time slots during the entire simulation time.

6.3. Simulation results under different settings

In this section, the simulation results for LECIM DSSS PHY with PCA which are obtained by considering different scenarios will be presented.

6.3.1. Scenario 1: Impact of PCA allocation

The goal of the first simulation scenario is to study the network performance when PCA is enabled. For comparison purpose, three different network configurations are setup: with PCA-enabled, with PCA-disabled, and with emergency packets generation disabled. All the simulation parameters described in Tables 7, 8, and 9 are applied. Consequently, for $SO = 10$ the superframe duration *(SD)* has a value of $31.711\,s$. The PCA-enabled configuration has three PCA allocation rates, each one with four backoff periods duration and distributed in the CAP with $10.566\,s$ interval among them.

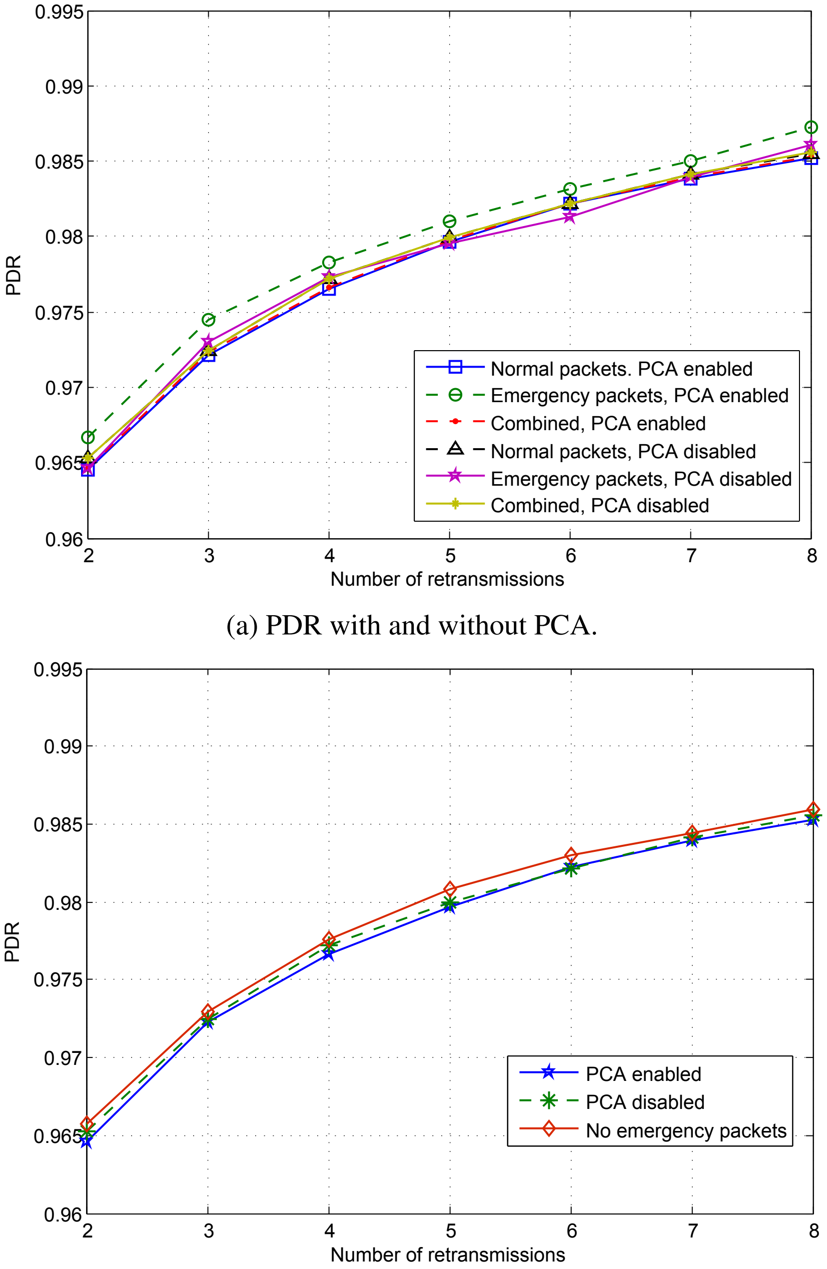
Emergency packets can be transmitted on any random backoff period within the CAP period, whereas normal packets can be transmitted only during the non-PCA periods. In such a network, if a normal packet is in a backoff state or if it has finished its backoff period and is ready for transmission, and if the next time-slot lies in one of the allocated PCAs, then all normal packet activities are paused for the next four consecutive time-slots. In the mean time, emergency packets get channel access by contending among themselves. Once the PCA period is over, the normal packet activities are resumed. Emergency and normal packets equally compete for access.

For channel access, whether PCA is enabled or disabled, normal packets use the normal S-Aloha protocol whereas emergency packets use PCA backoff algorithm. The latter one offers minimum random backoff periods. In the third configuration, which does not generate emergency packets, the network supports less traffic and thus less contention is expected. In all the three simulation settings, four random seeds are applied; the simulator models a 24 hr monitoring time of a real LECIM network, i.e., the simulation time is 24 hrs.

A comparison of the different simulation settings for system reliability in terms of PDR for varying number of retransmissions is shown Figure 14. As can be seen from the curves, each configuration has a reliability of greater than $96\,\%$ for all number of retransmissions. As expected, the network reliability improves as the number of retransmissions increases. Figure 14a compares PDR when PCA is enabled versus when PCA is disabled. PCA enabling has improved the PDR performance of emergency packets. This is clearly depicted by comparing the PDR of emergency packets in the PCA-disabled configuration. In both cases, it is also observed that the application of PCA backoff mechanism by the emergency packets enables them to have better PDR than the normal packets.

The comparison of the overall PDRs for the three cases is illustrated in Figure 14b. The result shows that priority access affects the PDR of normal packets; and thereby the overall PDR of the system reduces. This is because the priority access has an indirect effect of increasing the contention in the non-PCA periods. This results in more packet collisions and retransmissions.

Figure 15 presents the average MAC and end-to-end delays for normal and emergency packets. It is interesting to observe that even for higher number of retransmissions, all the three configurations offer low MAC and end-to-end delays for both packet types. The possible reasons for the low latency are the low traffic load in the network; and the duty cycle applied. As the number of retransmissions increases, the average delays for emergency packets remain almost constant, which implies that most of the packets are successfully delivered in the first few transmission attempts; whereas for normal packets the MAC and end-to-end delays increase.

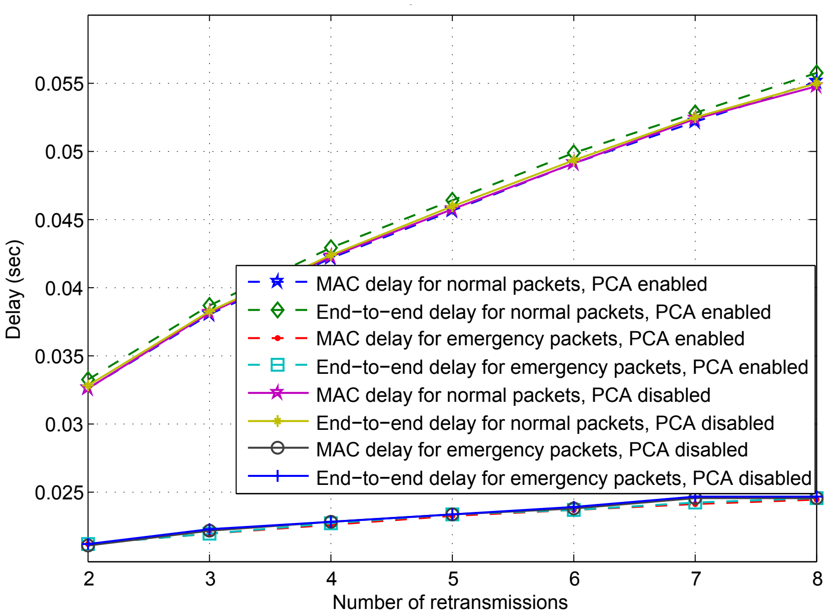


(a) PDR with and without PCA.

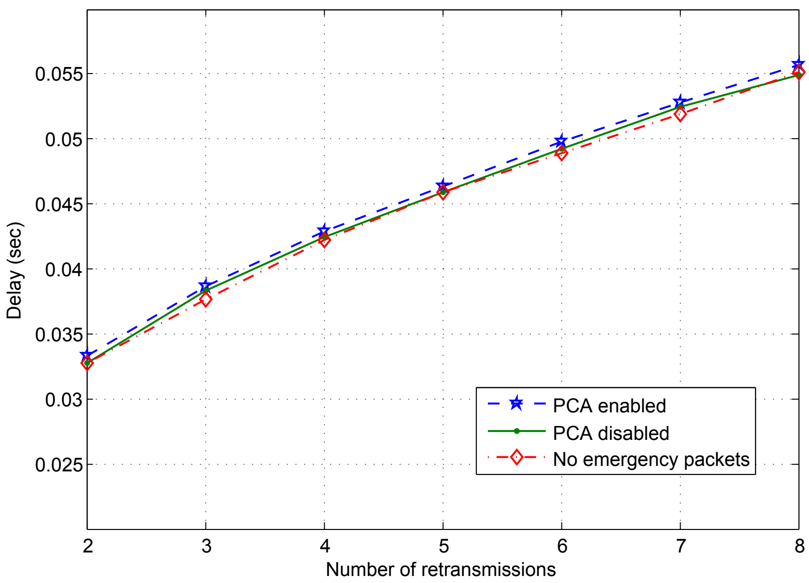
(b) Overall PDR.

Figure 14. Packet delivery ratio as a function of number of retransmissions (a) with and without PCA (b) when PCA is enabled, when PC is disabled, and when no emergency packets are generated.

As seen from the similarity of delay for normal packets in Figures 15a and 15b, the queuing delay is negligible for both packet types. This is obvious as the traffic load is low. Expectedly, the curves depict that the MAC and end-to-end delays of emergency packets are much lower than the corresponding values of the normal packets. Much of the low delay performance in emergency packets is a contribution of the PCA backoff mechanism used; with a small contribution also gained from the short-duration allocated PCAs. The impact of priority access on the average delay of normal packets



(a) MAC and end-to-end-delays.



(b) End-to-end delay of normal packets.

Figure 15. Average MAC and end-to-end delays as a function of number of retransmissions (a) with and without PCA (b) end-to-end delay of normal packets.

is seen in Figure 15b. The normal packets in the PCA-enabled configuration have relatively the highest average end-to-end delay.

The success probability of the three experiments is illustrated in Figure 16. The result shows that packet collision and/or channel error causes packet retransmissions, and this reduces success probability of the network. The overall success probabilities of the three configurations are almost the same. Compared to the two packet types, emergency packets have lower success probability than normal packets. This is because emergency packets are few in number and any retransmission easily affects the value of the success probability. The result also shows that in the PCA-disabled configuration, emergency packets are facing higher contention and, therefore, some of them are retransmitted multiple times, which ultimately reduces the success probability.

Based on the nature of the traffic density in the three networks, one can intuitively expect a very low throughput. The measured result shown in Figure 17 confirms the expectation; only a very small fraction of the total monitoring time is used by the channel to successfully deliver messages to the coordinator. Increasing the number of retransmissions does not have much effect on the throughput of the three networks.

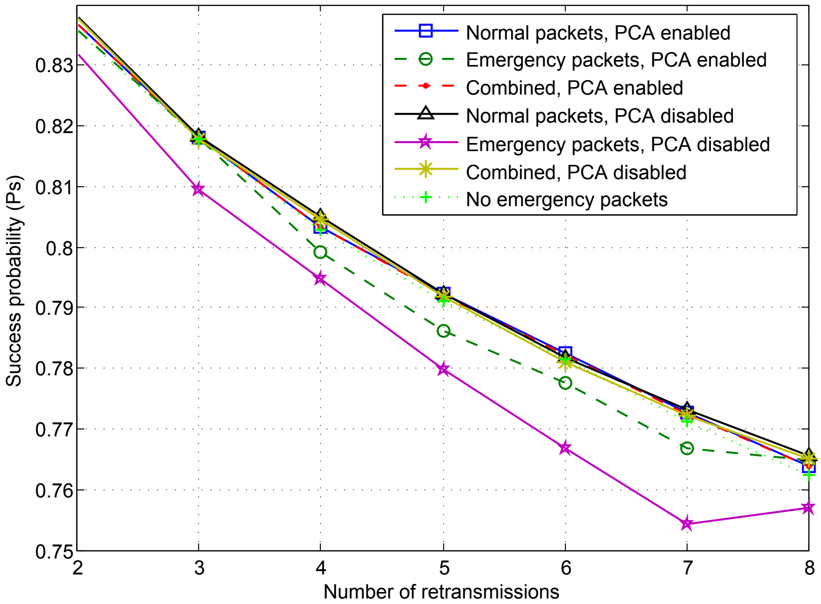


Figure 16. Success probability as a function of number of retransmissions for PCA-enabled, PCA-disabled, and emergency packets generation disabled networks.

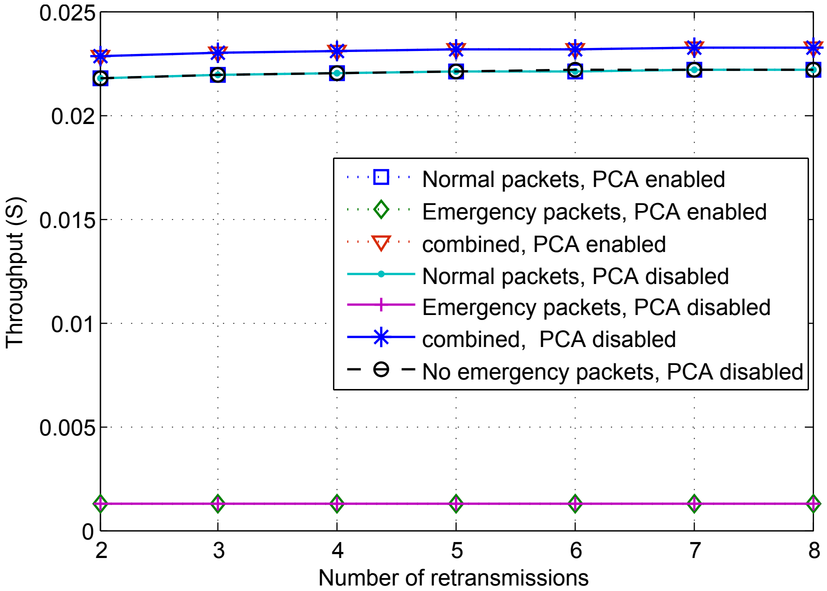


Figure 17. Throughput as a function of number of retransmissions for PCA-enabled, PCA-disabled, and emergency packets generation disabled networks.

6.3.2. Scenario 2: Impact of varying PCA allocation rate per CAP

In the previous section, the performance benefits of PCA allocation was investigated by considering different network configurations. In this section, the performance of LECIM DSSS PHY with PCA for varying number of PCAs per CAP will be studied. The scenario can be described as follows: there are three simulation settings. The first one is set to $SO = 10$; the second one is set to $SO = 11$; and the third one is set to $SO = 12$, which is equivalent to setting each one to an SD value of $31.711\,s$, $63.422\,s$, and $126.844\,s$ respectively. With the help of Table 3, in the above order there are 3 PCAs, 5 PCAs, and 9 PCAs allocated per CAP. The duration of one PCA is set to four backoff periods for all cases. Based on this calculation, the set of PCAs in a given configuration are uniformly distributed in the CAP, and there is $10.566\,s$, $12.687\,s$, and $14.0955\,s$ interval among them respectively. The fact one can observe here is as SD increases, the number of allocated PCAs and the interval among them also increase. Apart from the change in SO values, all the parameter values described in Tables 7, 8, and 9 are used in all the experiments. Finally, different simulations are made, each one with four seeds and for varying number of retransmissions. Figures 18, 19, 20, and 21 present the measured PDR, average delay, success probability, and throughput respectively as a function of varying number of retransmissions.

Figure 18 depicts the measured PDR of the three configurations. As expected, PDR of the system improves when unsuccessful packets are retransmitted. Emergency packets have better PDR than the normal packets do. PDR performance comparison of the three configurations for emergency packets indicates that the first configuration has better PDR over the others; with the third configuration performing the least. In other words, the PDR of emergency packets is decreasing as the PCA allocation rate increases. This is because as PCA allocation rate increases, the interval between consecutive PCAs also increases, making it more difficult for the emergency packets to get priority access. The indirect impact of increasing PCAs in the CAP is gradually converting a PCA-enabled network into a PCA-disabled network. In other words, the percentile proportion of the PCAs decrease when more of them are allocated in the CAP. On the other hand, the overall system PDR (also the PDR of normal packets which is not included in the curves) shows that there is an indication of PDR improvement as the number of PCAs increases. This is the consequence of priority access reduction as PCA allocation increases.

The average end-to-end delay of this scenario is illustrated in Figure 19. If one closely looks at the result, the normal packets of the first configuration have the highest average end-to-end delay. This is because the priority access in the first configuration has the highest impact on the normal packets. Therefore, it is possible to say that increasing the PCAs in the CAP slightly increases the average delay of normal packets. On the other hand, the end-to-end delays of emergency packets of the three cases are almost the same; and slowly increase as the number of retransmissions increases.

The success probability shown in Figure 20 confirms the impact observed in Figure 18 that longer PCA interval reduces emergency packet transmission success rate. Comparing the success probabilities of the three configurations of emergency packets, the third one has the lowest result; followed by the second one. The reason is emergency packets experience the highest contention in the third configuration, followed by the second case. More contention implies more retransmissions, which ultimately reduces

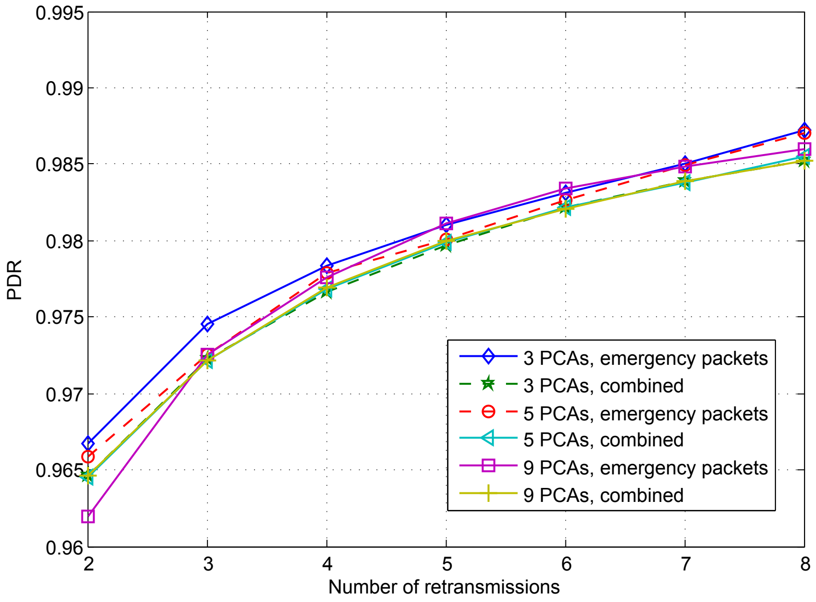


Figure 18. PDR as a function of number of retransmissions for varying number of PCA allocation rates.

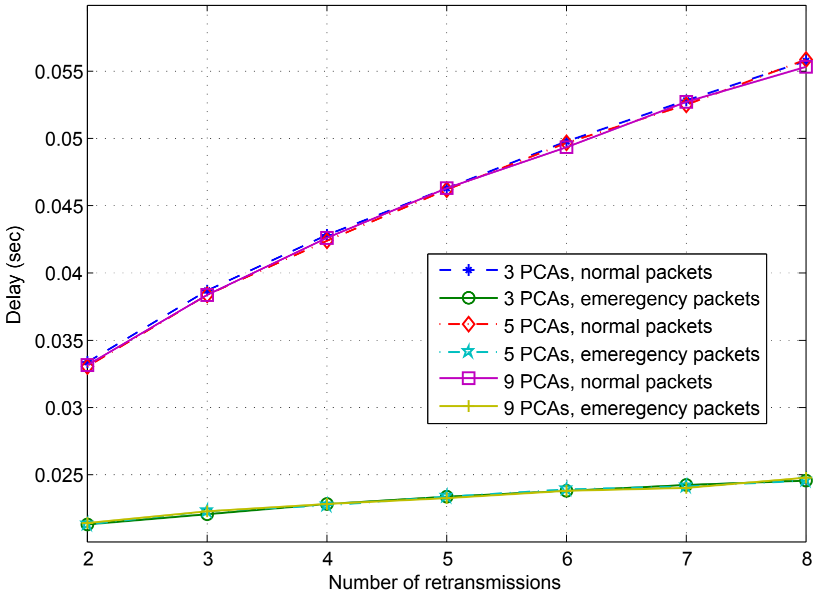


Figure 19. Average end-to-end delay as a function of number of retransmissions for varying number of PCA allocation rates.

the success probability. The result also shows that the overall success probability is almost the same for all cases; and the success probability of emergency packets is lower than the overall success probability. The latter one implies that insufficient emergency packets are generated, and thus any transmission failure has more effect on the success probability than in the case of normal packets.

Figure 21 depicts the measured throughputs of the three simulation settings. Generally speaking, very low network throughputs are obtained. As PCAs increase, no performance change is observed either in the overall throughput nor in the throughput of emergency packets. This could be because of the low traffic load in the network.

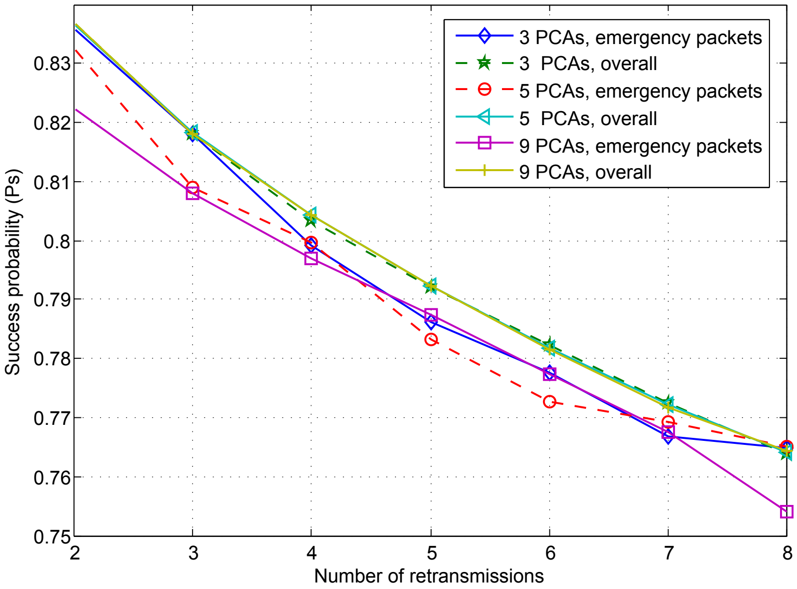


Figure 20. Success probability as a function of number of retransmissions for varying number of PCA allocation rates.

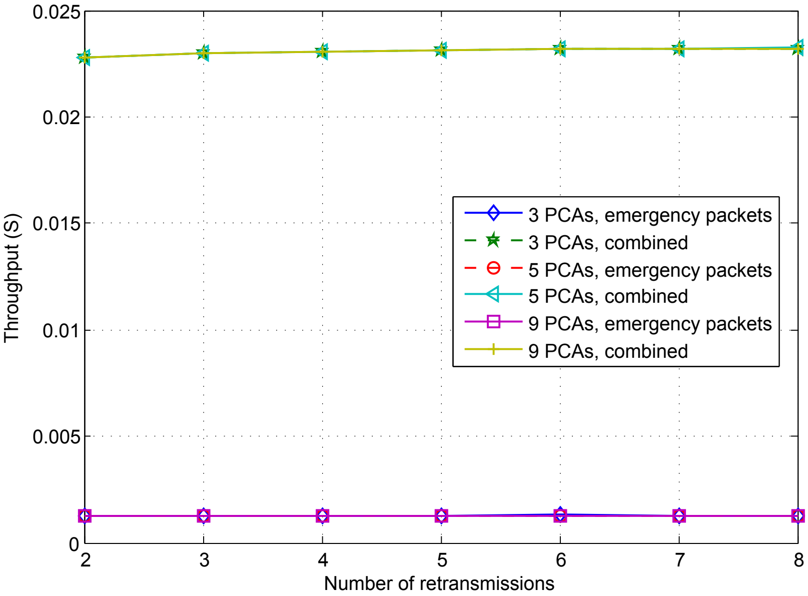


Figure 21. Throughput as a function of number of retransmissions for varying number of PCA allocation rates.

6.3.3. Scenario 3: Last gasp messaging

The last gasp messaging is the worst case communication scenario in an LECIM network. In a monitored critical infrastructure, an accident may happen to it, or a blackout may occur, or any sort of phenomenon that disrupts the critical infrastructure's normal functioning may occur. The situation must be reported to the monitoring center so that correcting actions may be taken timely. In such a scenario, there is a possibility that a large number of the sensor nodes in the LECIM network detect the critical event and all send alarm messages to the PAN coordinator nearly simultaneously. This is termed as the last gasp messaging, a moment of large amount of emergency messages transmission from the sensor nodes. So, can the network handle such events, i.e., can all these messages be delivered reliably and within a reasonable time delay?

In this section, the performance of LECIM DSSS PHY with PCA on last gasp scenario is evaluated. It is obvious that when all the sensor nodes transmit emergency packets at the same time, there will be significant packet collisions; none of them may even deliver their emergency packets. The mechanism used to minimize packet collisions in such phenomena is to apply some reasonable random waiting time (delay) to the packets right after their generation so that the channel accessing time will be somehow distributed and thereby avoiding any potential collisions. The random delay is assigned to each packet on a uniform distribution basis. For this purpose, three configurations with different delays are selected: configuration 1 is set to 0 s delay; configuration 2 is set to 20 s delay; and configuration 3 is set to 40 s delay. These are the delays out of which the random delays of each packet are withdrawn on a uniform distribution basis. In this simulation scenario, it is assumed that before or after the last gasp moment, no emergency packets are generated, only normal packets. Based on these settings, the results obtained from the simulator for PDR, average end-to-end delay, and success probability are given in Figures 22, 23, and 24 respectively.

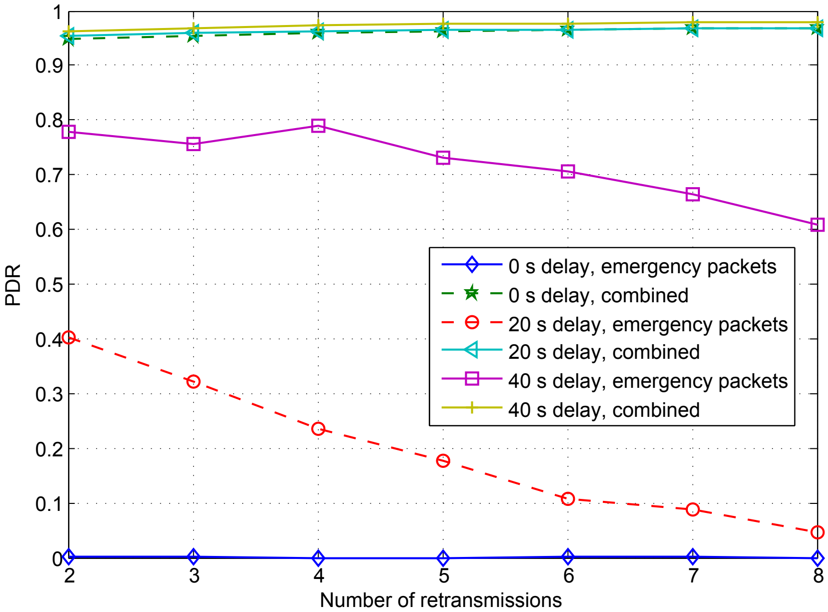


Figure 22. The network PDR as a function of number of retransmissions for last gasp scenario.

The overall system PDR and that of emergency packets of the three configurations as a function of number of retransmissions are given in Figure 22. For each setting, the overall system PDR, which is usually dominated by the PDR of the normal packets, is very high; slowly and steadily increasing as more retransmissions are made. In addition, the overall PDR slightly improves as the applied delay increases. On the other hand, the PDR of emergency packets for configuration 1 is zero, which implies no packet has been delivered successfully. This is the consequence of collisions that result from the zero waiting time before accessing the channel. It can be observed that applying a random delay has improved the PDRs of configurations 2 and 3 though each value is much lower than the expected PDR, which is 99 % and above for this scenario. Besides, it can be seen that the PDR of emergency packets decreases as the

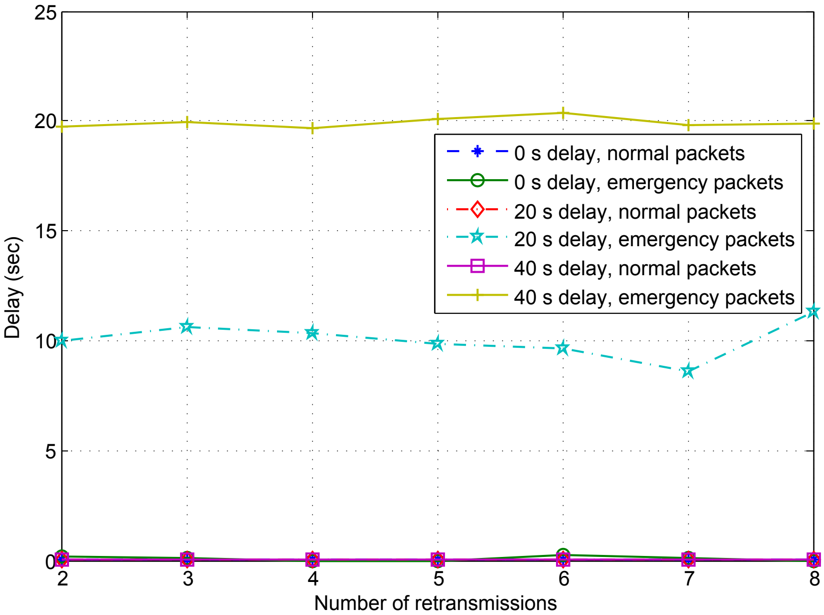


Figure 23. Average end-to-end delay as a function of number of retransmissions for last gasp scenario.

number of retransmissions increases. This is because retransmitting the unsuccessful packets discourages the successful transmission of newly arriving emergency packets, i.e. while both sets of packets (new arrivals and the unsuccessful ones) access the channel simultaneously, more collisions occur. So, retransmission is not improving the PDR of emergency packets.

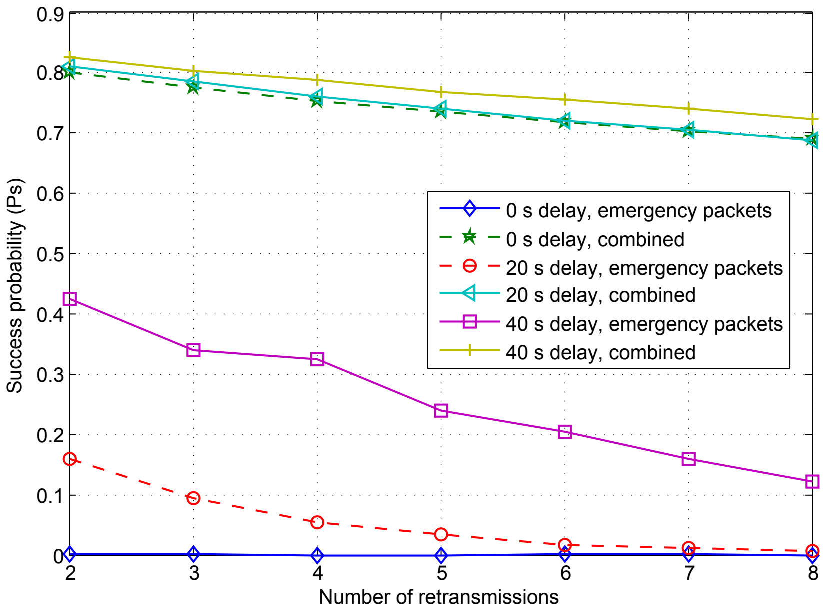


Figure 24. Success probability as a function of number of retransmissions for last gasp scenario.

Figure 23 presents the average end-to-end delays of emergency and normal packets. The end-to-end delay of normal packets is very low, around 27 ms; and it is almost the same for all retransmissions. However, the average end-to-end delays of emergency packets for the three configurations are different: configuration 1 has no delay as no packets have succeeded transmission; configurations 2 and 3 have approximately 10 s and 20 s delays respectively. The latter two delays are too high but within the delay tolerance of the standard smart grid monitoring for last gasp scenario, which is 30 s.

Similarly, the success probability is displayed in Figure 24. In general, success probability increases as the applied random delay increases. Normal packets have good success probability and decreases as more retransmissions are made. On the other hand, the performance of emergency packets for all configurations is very low, being zero for configuration 1.

In general, the simulation results show that PDR and success probability performance of the system in the last gasp scenario is very low. Consequently, LECIM DSSS PHY with PCA does not support last gasp messaging using only a single channel link.

6.4. Analytical vs. simulation results

This section focuses on comparing the results of simulation and analytical models for an LECIM DSSS PHY with PCA network. The Markov chain model developed in a previous section will be validated by simulation results. In the mathematical analysis of the system, expressions for network throughput and average delay for both packet types have been developed. The results obtained from these expressions will be compared with the corresponding simulation results of the PCA-enabled configuration of scenario 1. In doing so, the simulation results and the equations are kept independent. However, MAC layer and PHY layer specification values of the standard and some simulation parameters are used as inputs to the equations.

The throughput and average delay properties of the Markov chain model for a large-scale network, $N = 750$, are shown in Figures 25 and 26 respectively. One can draw a conclusion that the analytical and simulated results mismatch completely. This is because the S-Aloha becomes unstable when the network size goes large. In [68], it explains that an Aloha system which supports very large number of users cannot be stable for a retransmission mechanism of unsuccessful packets that does not consider the system state. To stabilize the system, the packet retransmission policy must (somehow) adapt the state of the system.

In this Markov model, a large N value results in an extremely low p_s value, which in turn forces the network throughput to zero. The analytical results of Figure 25 confirm the situation. When the network throughput is very low, the number of backlogged users in the system steadily grows, which ultimately drives the system into instability. As illustrated in Figure 26, the average delay of normal packets becomes very high as more retransmissions are made.

To verify if the developed Markov model works in a small-sized network, a test network with $N = 50$ is taken for analysis and the corresponding results are shown in Figures 27 and 28. The result in Figure 27 indicates that the analytical and simulated throughputs are almost matching. Both models prove that the system throughput is low. Figure 28 also shows the average delays of the two models. One can see that the theoretical delays are a bit overestimated. Except for the minor difference between the corresponding average delays, both models indicate that the network offers very low average delay. Also, the queueing delay is negligible. To sum up, the delay and

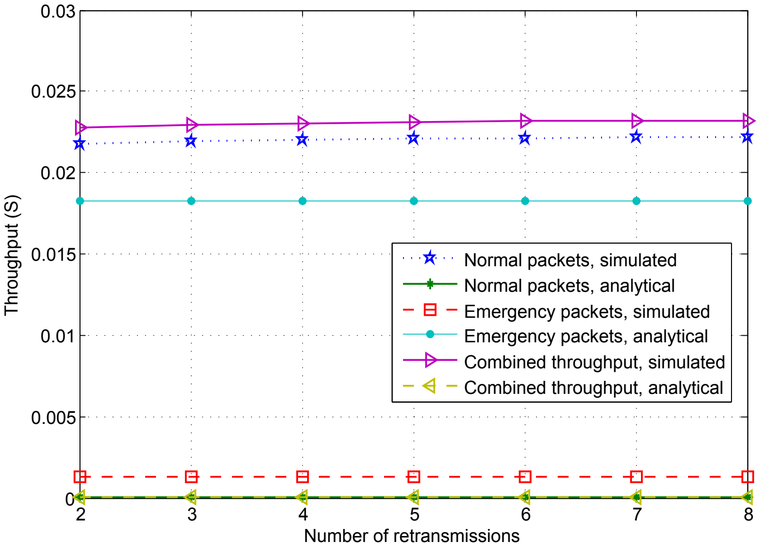


Figure 25. Analytical and simulated throughput of emergency and normal packets as a function of number of retransmissions, $N = 750$.

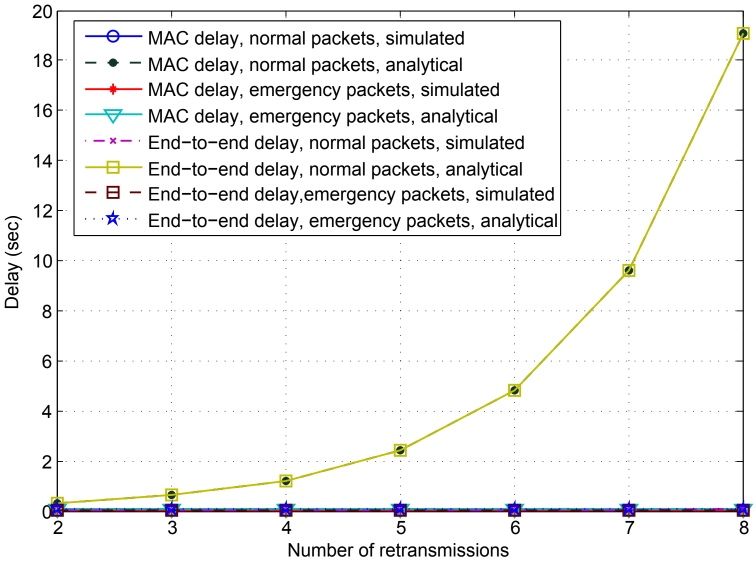


Figure 26. Analytical and simulated average MAC and end-to-end delays of emergency and normal packets as a function of number of retransmissions, $N = 750$.

throughput performances discussed above confirm the validity of the model for small-scale networks.

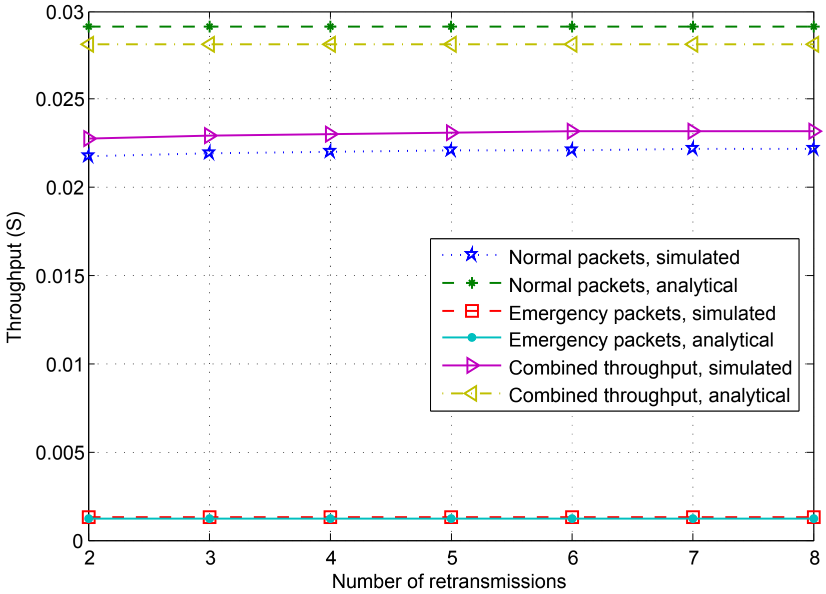


Figure 27. Analytical and simulated throughput of emergency and normal packets as a function of number of retransmissions, $N = 50$.

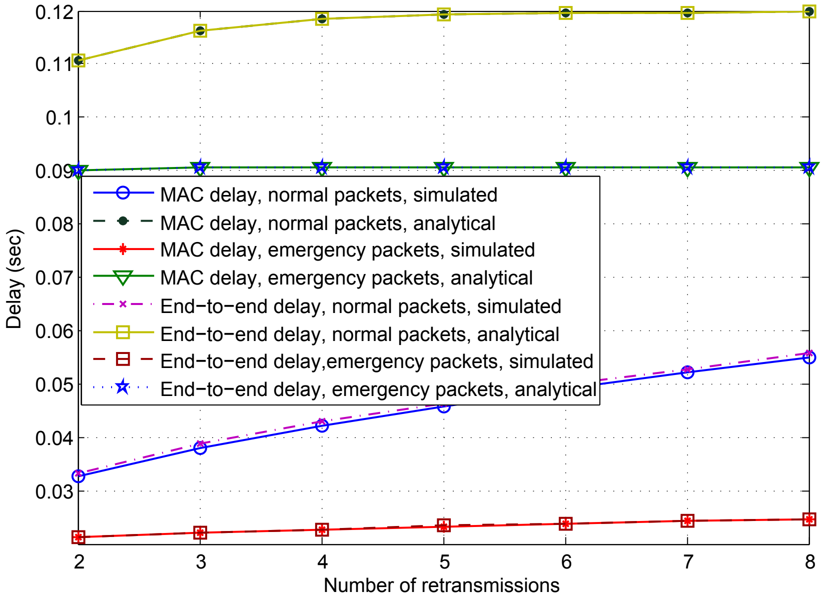


Figure 28. Analytical and simulated average MAC and end-to-end delays of emergency and normal packets as a function of number of retransmissions, $N = 50$.

6.5. Discussion

As explained earlier, the goal of this thesis is to implement IEEE Std. 802.15.4k priority channel access and to assess its performance on emergency and normal packets. Accordingly, the LECIM DSSS PHY with PCA is implemented using OPNET modeler and its performance evaluated by considering different scenarios.

The first part of the study focuses on validating the importance of priority access for high priority messages (or emergency packets). For this purpose, a performance comparison among a PCA-enabled configuration, a PCA-disabled configuration, and a third configuration that does not support emergency packets is made based on reliability (PDR and success probability) and network delay. In the PCA-enabled configuration, the results show that priority access improves the reliability and delay of emergency packets. Priority access guarantees emergency packets less channel contention and better backoff mechanism. Therefore, they have better PDR and delay performance over the normal packets. The fact that emergency packets have low traffic density causes their success probability to be less than that of the normal packets, but this does not mean they do not manage to reach the destination. It implies that few of them have to make multiple retransmissions before they succeed. The performance gain in emergency packets is obtained at cost of performance loss of the normal packets and the overall system. The overall system performance, which is often dominated by the network performance of normal packets, is reduced by the applied priority access scheme.

In the case of the PCA-disabled network, there is no priority access; emergency packets get channel access on competition basis. As a result, there is not much difference in the reliability performance between the two packet types except for the low delay in emergency packets, which is an attribute of the backoff mechanism they use. The absence of priority access has improved the PDR, success probability, and delay of normal packets; so do the combined PDR and success probability of the network.

So, when the performances of the two configurations are compared, the emergency packets in the PCA-enabled configuration have better PDR, success probability and delay than the emergency packets in the PCA-disabled configuration. This proves the advantage of a priority access. Due to the absence of priority access, normal packets in the PCA-disabled network have better PDR, success probability, and delay than the normal packets in the PCA-enabled network; so is true with the combined PDR and success probability. The three configurations are also compared for delay, PDR, and success probability. The fact that the third configuration has relatively the least traffic load indicates that there is less contention in the channel. Consequently, it has, to some extent, better delay and PDR performance than the others.

The other part of the study is evaluating the impact of increasing the number of PCAs in the CAP period on the performance of the network. All PCAs are made to have the same duration. The results of the different configurations show that as the number of the PCAs increase, the effect of a priority access reduces. This is because of the widening in the SD as SO goes higher to produce more PCAs. So, as PCAs increases in the CAP, the performance of the network in PDR, delay, and success probability for emergency packets deteriorates; whereas for normal packets and the overall system performance improves.

The last gasp scenario is taken as a case study to assess how the network behaves to rare and critical events, like a blackout. In such events, the network is flooded with emergency packets, and very high packet collision is observed. Unless a collision avoidance mechanisms is applied, no matter how many times the sensors retransmit their emergency packet, none of them succeeds. So, the network cannot handle a last gasp scenario by using a single channel link. Considering a multi-channel link utilization would be a potential solution to improve its performance.

As part of the performance study, a Markov model is developed to evaluate the delay and throughput performance of the network, and its results compared with the simulator results. It is found out that the Markov model of a large-scale network which applies an Aloha protocol cannot be stable. This is mainly because the retransmission policy of failed packets does not consider the system state. This drives the model into instability; the throughput is almost zero, and the delay is extremely high. However, comparison of the results of the simulator and the Markov model for a small-scale network proves the validity of the Markov model.

In conclusion, the study of the different experiments on LECIM DSSS PHY with PCA shows that the network delay is low for both traffic types; the queuing delay is negligible; the network throughput is very low and this is because of the low monitoring data flow; and considering the number of users and the channel characteristics, the network has acceptable reliability.

In my future work, I plan to implement MPDU fragmentation on the existing simulator so that I can make a complete performance study of LECIM DSSS PHY with PCAs. Also, I would like to implement multi-channel MAC layer that will improve the performance of last gasp messaging.

7. SUMMARY

Recently, the concept of critical infrastructure emerged into the field of wireless sensor networking. Critical infrastructures consist of physical facilities, assets, and services which if interrupted or destroyed would have a serious impact on the health, safety, security, or economy of a society or a nation. Therefore, monitoring these infrastructures is essential for their safety, reliability, preventative maintenance, and cost reduction through improved operations and efficiency.

With the successful implementation of many WSN applications, there was a tendency to develop and use a wireless application to monitor critical infrastructures. This was how the concept of LECIM was born. Large coverage area, minimal infrastructure, commissioned network, low energy, low data-rate, low cost, asymmetrical data flow, and supporting point-to-multi-point direct communication are some of the main characteristics/requirements of an LECIM network. However, many of the existing WSN MAC protocols, IEEE 802 family, and other wireless technologies are unsuitable for LECIM networks for one or more of the following reasons: high power consumption, high cost, infrastructure complexity, high QoS requirement, number of users supported is small, transmission range, high data-rate requirement, low link margin for challenging environments, maintenance requirement, large payload, and network topology. After realizing this problem, IEEE proposed IEEE Std. 802.15.4k to facilitate communication in LECIM devices.

IEEE Std. 802.15.4k uses a star network topology consisting of a PAN coordinator and sensor nodes. The standard has MAC layer and PHY layer specifications which enable the collection of periodic and event-driven (high priority) messages from a large number of sensor nodes that are widely dispersed, or are in challenging environments. The MAC layer defines Aloha and CSMA-CA channel access algorithms, each one with slotted and unslotted versions, and the PHY layer defines LECIM DSSS PHY and LECIM FSK PHY. The MAC layer supports new features like MPDU fragmentation and priority access scheme. So, Aloha with PCA and CSMA-CA with PCA are priority access mechanisms dedicated only for high priority messages.

The aim of the thesis was to implement LECIM DSSS PHY with PCA and to evaluate its performance with simulations carried out in OPNET modeler. Therefore, a star network topology supporting 750 sensor nodes and that uses S-Aloha with PCA algorithm was implemented. In addition, Rayleigh fading and Hata pathloss model for suburban area was used to model the propagation medium. Due to the broadness of the topic, fragmentation is not included in this thesis. Instead, a payload size which meets the PHY layer specification was used. Accordingly, simulations for different scenarios were carried out, each one for varying number of retransmissions; the results are analyzed; and the network performance evaluated in terms of PDR, success probability, delay, and throughput. Also, a Markov chain model is developed for the same system focusing on delay and network throughput.

The simulation results show that user priority access brings a superior performance for the high priority messages; increasing the PCAs in the CAP decreases their percentile proportion and, therefore, does not improve the high priority messages performance. Other features of the system observed from the results are given below.

1. Low delay (though the standard has good delay tolerance).

2. Low throughput (which is a typical characteristics of a monitoring WSN).
3. Despite the large network size and channel characteristics, it has good reliability.
4. It has less than required performance in smart grid last gasp messaging.
5. The system Markov model for large number of users is unstable; whereas for small number of users, it has comparable delay and throughput properties with simulation.

8. REFERENCES

[1] Commission of the European Communities. Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the Fight Against Terrorism, COM (2004) 702 final, Brussels, 20 October 2004". [Last accessed: 10 Aug. 2013].

[2] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002) Wireless sensor networks: a survey. Computer Networks, Vol. 38, pp. 393–422.

[3] (2013) IEEE Standard for Local and metropolitan area networksPart 15.4: Low-Rate Wireless Personal Area Networks (WPANs) Amendment 5: Physical Layer Specifications for Low Energy, Critical Infrastructure Monitoring Networks. IEEE P802.15.4k, June, 2013.

[4] http://www.opnet.com/, [Last accessed: 13 Oct. 2013].

[5] Estrin, D., Govindan, R., Heidemann, J., & Kumar, S. (1999) Next century challenges: scalable coordination in sensor networks. In: Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, MobiCom '99, pp. 263–270. Seattle, Washington, USA.

[6] Corke, P., Wark, T., Jurdak, R., Hu, W., Valencia, P., & Moore, D. (2010) Environmental Wireless Sensor Networks. Proceedings of the IEEE, Vol. 98, No. 11, pp. 1903–1917.

[7] Bohm, A. (2007) State of the art on energy-efficient and latency constrained networking protocols for wireless sensor networks. Tech. Rep. IDE0749.

[8] Ye, W. & Heidemann, J. Medium Access Control in Wireless Sensor Networks, [Last accessed: 18 July 2013] URL = http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.4.8290. Tech. rep.

[9] Melodia, T., Vuran, M.C., & Pompili, D. (2006) The state of the art in cross-layer design for wireless sensor networks. In: Proceedings of the Second international conference on Wireless Systems and Network Architectures in Next Generation Internet, EURO-NGI'05, pp. 78–92. Villa Vigoni, Italy.

[10] Pantazis, N., Nikolidakis, S., & Vergados, D. (2013) Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey. Communications Surveys Tutorials, IEEE, Vol. 15, No. 2, pp. 551–591.

[11] Raghunathan, V., Schurgers, C., Park, S., & Srivastava, M. (2002) Energy-aware wireless microsensor networks. Signal Processing Magazine, IEEE, Vol. 19, No. 2, pp. 40–50.

[12] E. Shih, e.a. (April 2001) Energy-Efficient Link Layer for Wireless Microsensor Networks. In: the Proceedings of the IEEE Computer Society Workshop on VLSI 2001 (WVLSI '01). Orlando, FL.

[13] Liu, Y., Elhanany, I., & Qi, H. (2005) An energy-efficient QoS-aware media access control protocol for wireless sensor networks. In: Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on, pp. 3 pp.–191.

[14] Iyer, R. & Kleinrock, L. (2003) QoS control for sensor networks. In: Communications, 2003. ICC '03. IEEE International Conference on, Vol. 1, pp. 517–521 vol.1.

[15] Al Ameen, M., Riazul Islam, S.M., & Kwak, K. (2013) Energy Saving Mechanisms for MAC Protocols in Wireless Sensor Networks. International Journal of Distributed Sensor Networks, Vol. 2010, No. 163413.

[16] Yahya, B. & Ben-Othman, J. (2009) Towards a classification of energy aware MAC protocols for wireless sensor networks. Wireless Communications and Mobile Computing, Vol. 9, No. 12, pp. 1572–1607.

[17] Ye, W., Heidemann, J., & Estrin, D. (2002) An energy-efficient MAC protocol for wireless sensor networks. In: INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, Vol. 3, pp. 1567–1576.

[18] Haapola, J. (2010) Evaluating medium access control protocols for wireless sensor networks, Ph.D, Thesis, Center for Wireless Communications, University of Oulu, Finland.

[19] Kottapalli, V.A., Kiremidjian, A.S., Lynch, J.P., Carryer, E., Kenny, T.W., Law, K.H., & Lei, Y. (2003) Two-tiered wireless sensor network architecture for structural health monitoring. In: Proceedings of the SPIE, Vol. 5057, pp. 8–19. San Diego, CA.

[20] Villegas, M.A.E., Tang, S.Y., & Qian, Y. Wireless Sensor Network Communication Architecture for Wide-Area Large Scale Soil Moisture Estimation and Wetlands Monitoring, [Last accessed:15 Sep., 2013] URL = http://users.cis.fiu.edu/ meraz001/TR-NCIG-0501.

[21] Werner-Allen, G., Lorincz, K., Ruiz, M., Marcillo, O., Johnson, J., Lees, J., & Welsh, M. (2006) Deploying a wireless sensor network on an active volcano. Internet Computing, IEEE, Vol. 10, No. 2, pp. 18–25.

[22] Valverde, J., Rosello, V., Mujica, G., Portilla, J., Uriarte, A., & Riesgo, T. (2011) Wireless Sensor Network for Environmental Monitoring: Application in a Coffee Factory. International Journal of Distributed Sensor Networks, Vol. 2012, No. 638067.

[23] Ali, M., Bohm, A., & Jonsson, M. (2008) Wireless Sensor Networks for Surveillance Applications - A Comparative Survey of MAC Protocols. In: Wireless and Mobile Communications, 2008. ICWMC '08. The Fourth International Conference on, pp. 399–403. Athens, Greece.

[24] Corke, P., Wark, T., Jurdak, R., Hu, W., Valencia, P., & Moore, D. (2010) Environmental Wireless Sensor Networks. Proceedings of the IEEE, Vol. 98, No. 11, pp. 1903–1917.

[25] Demirkol, I., Ersoy, C., & Alagoz, F. (2006) MAC protocols for wireless sensor networks: a Survey. Communications Magazine, IEEE, Vol. 44, No. 4, pp. 115–121.

[26] Czapski, P. (2006) A Survey: MAC Protocols For Applications Of Wireless Sensor Networks. In: TENCON 2006. 2006 IEEE Region 10 Conference, pp. 1–4. Washington, D.C.

[27] Younis, M. & Nadeem, T. (2004) Energy Efficient MAC Protocols for Wireless Sensor Networks. Tech. rep., University of Maryland baltimore County.

[28] LU Zheng, L.j. Study of MAC Protocol for Event-Driven Wireless Sensor Networks. Tech. rep., School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876.

[29] Akkaya, K. & Younis, M. (2004) Energy-aware delay-constrained routing in wireless sensor networks. Journal of Communication Systems, special issue on QoS support and service differentiation in wireless networks, Vol. 17, pp. 663–687.

[30] Akkaya, K. & Younis, M. (2005) A survey on routing protocols for wireless sensor networks. Ad Hoc Networks, Vol. 3, pp. 325–349.

[31] Van Dam, T. & Langendoen, K. (2003) An adaptive energy-efficient MAC protocol for wireless sensor networks. In: Proceedings of the 1st international conference on Embedded networked sensor systems, SenSys '03, pp. 171–180. New York, NY, USA.

[32] Yadav, R., Varma, S., & Malaviya, N. (2008) Optimized Medium Access Control for Wireless Sensor Network. International Journal of Computer Science and Network Security (IJCSNS), Vol. 8, No. 2.

[33] Yadav, R., Varma, S., & Malaviya, N. (2010) Performance Analysis of Optimized Medium Access Control for Wireless Sensor Network. Sensors Journal, IEEE, Vol. 10, No. 12, pp. 1863–1868.

[34] Haapola, J. (2002) Low-power wireless measurement system for physics sensors, Master's thesis, Department of Physical Sciences, University of Oulu, Oulu, Finland.

[35] Jamieson, K., Balakrishnan, H., & Tay, Y.C. Sift: A MAC Protocol for Event-Driven Wireless Sensor Networks, [Last accessed:05 Aug., 2013] URL = http://publications.csail.mit.edu/lcs/pubs/pdf/MIT-LCS-TR-894.pdf.

[36] Namboodiri, V. & Keshavarzian, A. (2008) Alert: An Adaptive Low-Latency Event-Driven MAC Protocol for Wireless Sensor Networks. In: Proceedings of the 7th international conference on Information processing in sensor networks, pp. 159 –170. Washington, DC, USA.

[37] Schurgers, C., Tsiatsis, V., Ganeriwal, S., & Srivastava, M. (2002) Optimizing sensor networks in the energy-latency-density design space. Mobile Computing, IEEE Transactions on, Vol. 1, No. 1, pp. 70 –80.

[38] Tay, Y., Jamieson, K., & Balakrishnan, H. (2004) Collision-Minimizing CSMA and its Applications to Wireless Sensor Networks. IEEE Journal on Selected Areas in Communications, Vol. 22, pp. 1048 –1057.

[39] Polastre, J., Hill, J., & Culler, D. (2004) Versatile low power media access for wireless sensor networks. In: Proceedings of the 2nd international conference on Embedded networked sensor systems, SenSys '04, pp. 95 –107. San Diego, CA.

[40] Enz, C., El-Hoiydi, A., Decotignie, J.D., & Peiris, V. (2004) WiseNET: an ultralow-power wireless sensor network solution. Computer, Vol. 37, No. 8, pp. 62 –70.

[41] El-Hoiydi, A. (2002) Aloha with preamble sampling for sporadic traffic in ad hoc wireless sensor networks. In: Communications, 2002. ICC 2002. IEEE International Conference on, Vol. 5, pp. 3418–3423 vol.5. New York, NY, USA.

[42] Cionca, V., Newe, T., & Dadarlat, V. (2008) TDMA Protocol Requirements for Wireless Sensor Networks. In: Sensor Technologies and Applications, 2008. SENSORCOMM '08. Second International Conference on, pp. 30–35.

[43] Kalidindi, R., Ray, L., Kannan, R., & Iyengar, S. (2003) Distributed energy aware mac layer protocol for wireless sensor networks. In: International conference on Wireless Networks, pp. 282–286. Las Vegas, Nevada.

[44] Pei, G. & Chien, C. (2001) Low power TDMA in large wireless sensor networks. In: Military Communications Conference, 2001. MILCOM 2001, IEEE, Vol. 1, pp. 347–351 vol.1.

[45] Li, J. (2004) A bit-map-assisted energy-efficient MAC scheme for wireless sensor networks, Master's thesis, Electrical Engineering, Mississippi State University.

[46] Li, J. & Lazarou, G. (2004) A bit-map-assisted energy-efficient MAC scheme for wireless sensor networks. In: Information Processing in Sensor Networks, 2004. IPSN 2004. Third International Symposium on, pp. 55–60. Berkeley.

[47] Shafiullah, G.M., Thompson, A., Wolfs, P., & Ali, S. (2008) Energy-efficient TDMA MAC protocol for wireless sensor networks applications. In: Computer and Information Technology, 2008. ICCIT 2008. 11th International Conference on, pp. 85–90. Khulna, Bangladesh.

[48] Shafiullah, G., Azad, S., & Ali, A. (2013) Energy-Efficient Wireless MAC Protocols for Railway Monitoring Applications. Intelligent Transportation Systems, IEEE Transactions on, Vol. 14, No. 2, pp. 649–659.

[49] Rhee, I., Warrier, A., Aia, M., Min, J., & Sichitiu, M. (2008) Z-MAC: A Hybrid MAC for Wireless Sensor Networks. Networking, IEEE/ACM Transactions on, Vol. 16, No. 3, pp. 511–524.

[50] Lu, G., Krishnamachari, B., & Raghavendra, C. (2004) An adaptive energy-efficient and low-latency MAC for data gathering in wireless sensor networks. In: Parallel and Distributed Processing Symposium, 2004. Proceedings. 18th International.

[51] Working Group 15: Wireless Personal Area Networks, [Last accessed: 04 July 2013] URL = http://grouper.ieee.org/groups/802/15/pub/2003/Jan03/03053r0P802-15_PC-Overview-of-WG15-and-Task-Groups.ppt.

[52] IEEE 802.15: Wireless Personal Area Networks (WPANs), [Last accessed: 20 July 2013] URL = http://standards.ieee.org/getieee802/802.15.html.

[53] (2011) IEEE Draft Standard for Local and metropolitan area networks - Part 15.4: Low-Rate Wireless Personal Area Networks (WPANs). Draft IEEE P802.15.4REVi/D09, April 2011 (Revision of IEEE Std 802.15.4-2006), pp. 1–311.

[54] IEEE 802.15 Working Group for WPAN, [Last accessed: 02 Sep. 2013] URL = http://ieee802.org/15/index.html.

[55] (2009) IEEE Recommended Practice for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 15.5: Mesh Topology Capability in Wireless Personal Area Networks (WPANs). IEEE Std 802.15.5-2009, pp. 1–166.

[56] IEEE 802.15 WPAN Task Group 6 (TG6) Body Area Networks, [Last accessed: 14 Sep. 2013] URL = http://ieee802.org/15/pub/TG6.html.

[57] (2011) IEEE Standard for Local and Metropolitan Area Networks–Part 15.7: Short-Range Wireless Optical Communication Using Visible Light. IEEE Std 802.15.7-2011, pp. 1–309.

[58] Ullah, N., Chowdhury, M.S., Khan, P., & Kwak, K.S. (2012) Multi-hop medium access control protocol for low energy critical infrastructure monitoring networks using wake-up radio. International Journal of Communication Systems. ISSN 1099-1131.

[59] (2009) IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems. IEEE Std 802.16-2009 (Revision of IEEE Std 802.16-2004), pp. 1–2080.

[60] (2008) IEEE Standard for Local and Metropolitan Area Networks Part 20: Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobilityphysical and Media Access Control Layer Specification. IEEE Std 802.20-2008, pp. 1–1039.

[61] (2011) IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 22: Cognitive Wireless RAN Medium

Access Control (MAC) and Physical Layer (PHY) specifications: Policies and procedures for operation in the TV Bands. IEEE Std 802.22-2011, pp. 1–680.

[62] (2012) 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.

[63] (2012) IEEE Standard for Local and metropolitan area networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 3: Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks. IEEE Std 802.15.4g-2012 (Amendment to IEEE Std 802.15.4-2011), pp. 1–252.

[64] https://mentor.ieee.org/802.15/dcn/11/15-11-0147-02-004k-lecim-call-for-proposals.docx, [Last accessed: 10 Sep. 2013].

[65] Haapola, J. d3P802.15.4k Section 5.1.1.4.5 Comment Resolution, [Last accessed: 13 Oct. 2013] URL = https://mentor.ieee.org/802.15/documents, https://mentor.ieee.org/802.15/documents,.

[66] http://www.mathworks.se/products/matlab/, [Last accessed: 10 Oct. 2013].

[67] Goldsmith, A. (2005) Wireless Communications. Cambridge University Press, New York, 42-60 pages.

[68] Rom, R. & Sidi, M. (1990) Multiple Access Protocols: Performance and Analysis. Springer Verlag, New York, 47-73 pages.

9. APPENDICES

Appendix 1: Mathematical derivation

The value of $b_{0,0}$ in Figure 12 can be obtained from the fact that the sum of all the stationary probabilities in the Markov chain model is 1. i.e,

$$\begin{aligned} 1 &= \sum_{i=0}^{m} \sum_{k=0}^{W_i-1} b_{i,k} + b_{\mathrm{I}} \\ &= \sum_{k=0}^{W_0-1} b_{0,k} + \sum_{i=1}^{m} \sum_{k=0}^{W_i-1} b_{i,k} + b_{\mathrm{I}} \end{aligned} \tag{61}$$

The three terms in (61) can be derived separately as follows.

$$\begin{aligned} b_{0,k} &= \frac{W_0 - k}{W_0(1-p_{\mathrm{PCA}})} \left[p_{\mathrm{s}} \sum_{i=0}^{m} b_{i,0} + (1-p_{\mathrm{s}}) b_{m,0} \right] \\ &= \frac{W_0 - k}{W_0(1-p_{\mathrm{PCA}})} \left[\frac{p_{\mathrm{s}}(1-e^{m+1})}{1-e} b_{0,0} + (1-p_{\mathrm{s}}) b_{m,0} \right] \end{aligned} \tag{62}$$

where $e = \frac{1-p_{\mathrm{s}}}{1-p_{\mathrm{PCA}}}$

$$\begin{aligned} \sum_{k=0}^{W_0-1} b_{0,k} &= \sum_{k=0}^{W_0-1} \frac{W_0 - k}{W_0(1-p_{\mathrm{PCA}})} \left[\frac{p_{\mathrm{s}(}1-e^{m+1})}{1-e} b_{0,0} + (1-p_{\mathrm{s}}) b_{m,0} \right] \\ &= \left[\frac{W_0 + 1}{2(1-p_{\mathrm{PCA}})} \right] \left[\frac{p_{\mathrm{s}}(1-e^{m+1})}{1-e} b_{0,0} + (1-p_{\mathrm{s}}) b_{m,0} \right] \end{aligned} \tag{63}$$

$$\begin{aligned} \sum_{i=1}^{m} \sum_{k=0}^{W_i-1} b_{i,k} &= \sum_{i=1}^{m} \sum_{k=0}^{W_i-1} \left(\frac{W_i - k}{W_i} \right) \left(\frac{1-p_{\mathrm{s}}}{1-p_{\mathrm{PCA}}} \right)^{i} b_{0,0} \\ &= \sum_{i=1}^{m} \left(\frac{1-p_{\mathrm{s}}}{1-p_{\mathrm{PCA}}} \right)^{i} \sum_{k=0}^{W_i-1} \left(\frac{W_i - k}{W_i} \right) b_{0,0} \\ &= b_{0,0} \sum_{i=1}^{m} \left(\frac{1-p_{\mathrm{s}}}{1-p_{\mathrm{PCA}}} \right)^{i} \left(\frac{W_i + 1}{2} \right) \end{aligned} \tag{64}$$

Substituting $\frac{2^i W_0+1}{2}$ for $\frac{W_i+1}{2}$ in (64) gives:

$$\begin{aligned}
&= \frac{b_{0,0}W_0}{2}\sum_{i=1}^{m}\left(2\frac{1-p_{\mathrm{s}}}{1-p_{\mathrm{PCA}}}\right)^i + \frac{b_{0,0}}{2}\sum_{i=1}^{m}\left(\frac{1-p_{\mathrm{s}}}{1-p_{\mathrm{PCA}}}\right)^i \\
&= \frac{b_{0,0}W_0}{2}\sum_{i=0}^{m}\left(2\frac{1-p_{\mathrm{s}}}{1-p_{\mathrm{PCA}}}\right)^i - \frac{b_{0,0}W_0}{2} + \frac{b_{0,0}}{2}\sum_{i=0}^{m}\left(\frac{1-p_s}{1-p_{\mathrm{PCA}}}\right)^i - \frac{b_{0,0}}{2} \\
&= \frac{W_0}{2}\left[\frac{1-p_{\mathrm{PCA}}}{2p_{\mathrm{s}}-p_{\mathrm{PCA}}-1}\right]\left[1-(2e)^{m+1}\right]b_{0,0} - \frac{(W_0+1)}{2}b_{0,0} \\
&\quad + \frac{1}{2}\left[\frac{1-p_{\mathrm{PCA}}}{p_{\mathrm{s}}-p_{\mathrm{PCA}}}\right]\left[1-e^{m+1}\right]b_{0,0} \\
&= \left(y\left[1-(2e)^{m+1}\right] - \frac{(W_0+1)}{2} + \frac{1}{2}\left[\frac{1-p_{\mathrm{PCA}}}{p_{\mathrm{s}}-p_{\mathrm{PCA}}}\right]\left[1-e^{m+1}\right]\right)b_{0,0}
\end{aligned} \tag{65}$$

where $y = \frac{W_0}{2}\left[\frac{1-p_{\mathrm{PCA}}}{2p_{\mathrm{s}}-p_{\mathrm{PCA}}-1}\right]$.

Also

$$\begin{aligned}
b_{\mathrm{I}} &= \frac{1}{\alpha}\left[(1-p_{\mathrm{q}})p_{\mathrm{s}}\sum_{i=0}^{m}b_{i,0} + (1-p_{\mathrm{q}})(1-p_{\mathrm{s}})b_{m,0}\right] \\
&= \frac{1}{\alpha}\left[\frac{p_{\mathrm{s}}(1-p_{\mathrm{q}})(1-e^{m+1})}{1-e}b_{0,0} + (1-p_{\mathrm{q}})(1-p_{\mathrm{s}})b_{m,0}\right]
\end{aligned} \tag{66}$$

Now, by substituting (63), (65) and (66) in (61), and by rearranging the terms gives the final expression for $b_{0,0}$ as:

$$b_{0,0} = \frac{(2p_{\mathrm{s}}-p_{\mathrm{PCA}}-1)(p_{\mathrm{s}}-p_{\mathrm{PCA}})}{a+b+c+d} \tag{67}$$

where
$a = \frac{W_0}{2}(1-p_{\mathrm{PCA}})(p_{\mathrm{s}}-p_{\mathrm{PCA}})(1-(2e)^{m+1})$
$b = (2p_{\mathrm{s}}-p_{\mathrm{PCA}}-1)(p_{\mathrm{s}}-p_{\mathrm{PCA}})\left(\frac{W_0+1}{2}\right)$
$c = \frac{1}{2}(1-p_{\mathrm{PCA}})(2p_{\mathrm{s}}-p_{\mathrm{PCA}}-1)(1-e^{m+1})$
$d = p_{\mathrm{s}}(1-p_{\mathrm{PCA}})(2p_{\mathrm{s}}-p_{\mathrm{PCA}}-1)(1-e^{m+1})(\frac{W_0+1}{2(1-p_{\mathrm{PCA}})} + \frac{1-p_{\mathrm{q}}}{\alpha})$