February 2016

PhD Dissertation

A Study on Minimizing Association Delay in Machine-to-Machine Communications

Graduate School of Chosun University

Department of Information and Communication Engineering

Pranesh Sthapit

A Study on Minimizing Association Delay in Machine-to-Machine Communications

머신대 머신 통신 환경에서 연결 설정 최소화 연구

February 25, 2016

Graduate School of Chosun University

Department of Information and Communication Engineering

Pranesh Sthapit

A Study on Minimizing Association Delay in Machine-to-Machine Communications

Advisor: Prof. Jae-Young Pyun

A dissertation submitted in partial fulfillment of
the requirements for the degree of
Doctor of Philosophy

October 2015

Graduate School of Chosun University

Department of Information and Communication Engineering

Pranesh Sthapit

스타핏 프라네쉬의 박사학위논문을 인준함

위원장 조선대학교 교수 한승조 (인)

위 원 조선대학교 교수 권구락 (인)

위 원 조선대학교 교수 변재영 (인)

위 원 KETI 센터장 이정기 (인)

위 원 순천대학교 교수 강의성 (인)

2015 년 12 월

조선대학교 대학원

ABSTRACT

A Study on Minimizing Association Delay in Machine-to-Machine Communications

Pranesh Sthapit
Advisor: Prof. Jae-Young Pyun
Department of Information Communication Engineering
Graduate School of Chosun University

Machine to machine (M2M) is a technology that enables networked devices to exchange information and perform actions without the manual assistance of human. A M2M communication system is also known as a wireless sensor network (WSN). Depending on the application domain and the deployment environment, one or more communication solutions may be employed, including wireless personal area networks (WPANs) such as ZigBee, wireless local area networks (WLANs) like Wi-Fi, cellular networks like GSM, and even satellite links. In an infrastructure based wireless network such as WPAN and WLAN, devices communicate with each other through an access point (AP). AP or the coordinator bridges traffic between stations on the network. However, before a station or a node can send traffic through an AP, it must be associated with the AP. Therefore, association is a very important phase in any AP-based network. Since only after association data communication is possible, association should be as fast as possible.

In this dissertation, we present simple yet effective solutions for the fast association of stations with the AP in WPAN and WLAN. The first half of the dissertation is dedicated for WPAN. A novel fast association scheme for beacon-enabled IEEE 802.15.4 network is presented. Our proposed technique prevents nodes from scanning multiple channels. The single channel scanning scheme is able to decrease the association time of IEEE 802.15.4 operating in 2.4 GHz by 32 times. Furthermore, the proactive algorithm to anticipate the future link breakage and a method to increase the node connectivity time with its coordinator are presented for further enhancing the proposed scheme. Based on the theoretical and the simulation based analysis, we show the benefit of the proposed mechanism in terms of most relevant performance metrics.

The second half of the dissertation is dedicated for WLAN. IEEE 802.11ah is another wireless network where fast association is very important. One of the most important challenges in 802.11ah is how to support the large number of nodes (more than 8000) efficiently. The problem become worst when network resets and all stations try for authentication/association simultaneously. Since thousands of stations are simultaneously contending for association, it is obvious that it takes significant amount of time to associate all stations. In this dissertation, the authentication/association of IEEE 802.11ah is analyzed and two novel fast association methods are presented. IEEE 802.11ah employs authentication control mechanism which allows only a small group of stations for association in a beacon interval (BI). However, how to group stations and how to estimate the group size is undefined. In the proposed first method, we estimate an optimum group size for a BI and proposed an enhanced authentication control mechanism, which fully utilizes the BI giving the minimum association time. The results show that the proposed authentication control mechanism is able to minimize association delay significantly.

During network initialization, two types of stations co-exists: stations which are trying for association and those who have already got associated, but waiting for data transmission. Another open issue in IEEE 802.11ah is how to avoid collision of association requests and data traffic from already associated station. One very simple solution would be to bring the total association time of the whole network to less than 1 minute. We try to achieve same in our second method. In the proposed second method, the stations are divided into several groups, each having a group head. A group head is responsible for collecting all the association requests and sending an aggregated single block request to the AP. The proposed method is able to achieve simultaneous association in each group without interfering others. We developed both the mathematical model and the simulation model for the analysis. The detailed performance analysis is provided to demonstrate the performance gain achieved by the proposed scheme.

The schemes that we have presented in this dissertation are simple and can be implemented in any infrastructure based networks. We expect that our proposed methods will be beneficial in various M2M applications.

Index Terms: Machine-to-Machine Communications, IEEE 802.15.4, IEEE 802.11ah, Association, Analysis, Network simulator (ns-2)

초 록

머신대 머신 통신 환경에서 연결 설정 최소화 연구

스타핏 프라네쉬
지도교수: 변재영
정보통신공학과, 대학원, 조선대학교

기계와 기계간에 (Machine-to-Machine : M2M) 이루어지는 통신은 연결된 기기간의 정보를 교환하는 기술이고 인간의 도움없이 작업을 수행하는 기술이다. 또한, M2M 통신 시스템은 무선 센서 네트워크로 (Wireless sensor network : WSN) 알려져 있다. 어플리케이션 도메인과 배치 환경에 따라서, 지그비(zigbee)와 같은 무선 개인 영역 네트워크 (WPANs), 와이파이(Wi-Fi) 같은 무선 로컬 영역 네트워크 (WLANs), GSM등의 셀룰러 네트워크, 위성 링크까지를 포함한 하나 이상의 통신 솔루션이 사용 될 수 있다. WPAN 과 WLAN 같은 설비 기반의 무선 네트워크에서, 기기는 엑세스 포인트 (Access point : AP)를 통해서 서로 통신한다. AP 혹은 코디네이터는 네트워크상의 스테이션 간 트래픽을 중개한다. 그러나, 스테이션 혹은 노드가 AP를 통해 트래픽을 전송하기 전에 AP와 반드시 연결되어 있어야 한다. 따라서, 모든 AP 기반 네트워크에서 상호 연결은 매우 중요한 단계이다. 상호 연결 이후의 단계부터 데이터 통신이 가능하므로, 이는 가능한 신속하게 이루어져야 한다.

본 논문에서는 WPAN과 WLAN에서 AP와 스테이션의 빠른 연결을 위한 간단하면서도 효과적인 솔루션을 제시한다. 본 논문의 전반부는 WPAN에 대한 내용을 다루며, 비콘 기반 IEEE 802.15.4 네트워크에서의 새로운 고속의 상호 연결 방식을 소개하였다. 제안 기술은 노드의 다중 채널 탐색을 방지한다. 단일 채널 탐색 방식은 2.4GHz 대역에서 동작하는 IEEE 802.15.4의 상호 연결 시간을 32배 가량 단축할 수 있다. 뿐만 아니라, 제안 방식을 보다 향상시키기 위해 미래 연결 손실 예측을 위한 알고리즘과 코디네이터와의 노드 연결성 향상을 위한 방법을 선보였다. 이론과 모의실험 분석

을 기반으로, 대다수 관련 성능 지표 측면에서 제안 메커니즘의 이점을 나타내었다.

본 논문의 후반부에서는 WLAN에 대한 내용을 다루었다. IEEE 802.11.ah는 빠른 상호 연결이 매우 중요한 또 다른 무선 네트워크이다. 802.11ah에서 가장 중요한 문제 중 하나는 어떻게 효율적으로 8000개 이상의 다수 노드를 지원하는가에 있다. 문제는 네트워크가 리셋되거나 모든 노드가 동시에 인증 또는 연결하려고 할 때 가장 심각해진다. 수천 개의 스테이션들이 일제히 연결하기 위해 경쟁하면서, 모든 스테이션을 연결하는데 상당한 시간이 소요될 것은 명백하다. 본 논문에서는 IEEE의 802.11ah의 인증 및 연결을 분석하고 빠른 상호연결을 위한 두 가지 새로운 방법을 제안한다. IEEE 802.11ah는 비콘 주기(BI) 내에서의 상호 연결을 위해 작은 그룹의 스테이션들만의 연결을 허용하는 인증 제어 메커니즘을 사용한다. 그러나, 스테이션 그룹의 결정과 그룹의 크기를 예측하는 방법까지 정의하지는 않는다. 제안하는 첫 번째 방법에서, BI를 위한 최적의 그룹 사이즈를 추정하고, 최소 연결 시간을 제공하는 BI를 전적으로 활용하는 향상된 인증 제어 메커니즘을 제안한다. 실험 결과는 제안된 인증 제어 메커니즘이 상호 연결 지연을 최소화시킬 수 있음을 보이고 있다.

네트워크를 초기화하는 동안, 상호 연결을 얻고자 하는 스테이션과 이미 연결되어 있지만 데이터 송신 대기 중인 두 가지 형태의 스테이션이 공존한다. IEEE 802.11ah에서의 또 다른 문제는 이미 연결되어 있는 스테이션으로부터 연결 요청과 데이터 트래픽의 충돌을 회피하는 방법에 있다. 한 가지 매우 간단한 해결 방법은 주어지는 전체 네트워크의 총 연결 시간을 1분 이하로 설정하는 것이며, 두 번째 제안 방법에서 이와 동일한 방법을 적용한다. 두 번째 제안 방법에서, 스테이션은 각각의 그룹 헤드를 갖는 다수의 그룹으로 분할된다. 그룹 헤드는 모든 상호 연결 요청과 AP에 집계된 단일 블록 요청 전송을 담당한다. 제안 방법은 각각의 그룹에서 서로 간섭을 주지 않고 동시에 상호 연결을 이룰 수 있다. 본 연구에서는 분석을 위해 수학적 모델과 모의실험 모델이 함께 개발되었고, 제안 방법에 의해 달성한 성능 이득을 선보이기 위해 본 상세 성능 분석을 제공한다.

본 논문에서 선보인 방법들은 간단하면서 어떠한 기반 네트워크에서도 구현이 가능하므로, 본 논문의 제안 방법은 다양한 M2M 응용분야에서 유용할 것으로 판단된다.

Acronyms

AC	Access Category
ACK	Acknowledgement
ACT	Authentication Control Threshold
AID	Association Identifier
AP	Access Point
AIFS	Arbitration Inter-frame Space
BC	Beacon Channel
BEB	Binary Exponential Back-off
BI	Beacon Interval
BO	Beacon Order
BPSK	Binary Phase Shift Keying
BSS	Basic Service Set
CAP	Contention Access Period
CBR	Constant Bit Rate
CCA	Clear Channel Assessment
CCMP	Cipher-block chaining Message authentication code Protocol
CFP	Contention Free Period
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
CW	Contention Window
DBC	Dedicated Beacon Channel
DBPSK	Differential Binary Phase Shift Keying
DC	Data Channel
DCF	Distributed Coordination Function
DFS	Dynamic Frequency Selection
DIFS	Distributed Inter-frame Space
DLC	Detection of Loss of Connectivity
DLS	Direct Link Setup
DS	Distribution System
DSSS	Direct Sequence Spread Spectrum
DS-UWB	Direct-Sequence UWB
ED	Energy Detection
EDCA	Enhanced Distributed Channel Access
EIFS	Extended Inter-frame Space
ESS	Extended Service Set
ETST	European Telecommunications Standard Institute
FFD	Full Functional Device
FHSS	Frequency Hopping Spread Spectrum
GH	Group Head
GTS	Guaranteed Time Slots
HCCA	HCF Controlled Channel Access
HCF	Hybrid Coordination Function

HSPA	High Speed Packet Access
HTTP	Hypertext Transfer Protocol
HWSN	Healthcare Wireless Sensor Networks
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IDC	International Data Corporation
IoT	Internet of Things
IR	Infrared
ISM	Industrial, Scientific and Medical
ISO	International Organization for Standardization
LR-WPAN	Low Rate WPAN
LTE	Long Term Evolution
LQI	Link Quality Indication
M2M	Machine-to-Machine
MAC	Medium Access Control
MIMO	Multiple Input Multiple Output
MSDU	MAC Protocol Data Unit
NAV	Network Allocation Vector
NDP	Null DATA Packet
OFDM	Orthogonal Frequency Division Multiplexing
O-QPSK	Offset-Quadrature Shift Keying
PAN	Personal Area Network
PCF	Point Coordination Function
PDR	Packet Delivery Ratio
PHY	Physical Layer
PPDU	PHY Protocol Data Units
PRD	Proactive Re-association Decision
QoS	Quality of Service
RAW	Restricted Access Window
RF	Radio Frequency
RFD	Reduced Functional Device
RID	Response Indication Deferral
RSSI	Received Signal Strength Indicator
RTS	Request To Send
SIFS	Short Inter-frame Space
SD	Super-frame Duration
SNR	Signal-to-Noise Ratio
SO	Super-frame Order
STA	Station
STBC	Space-Time Block Coding
TCP	Transport Control Protocol
TG	Task Group
TIM	Traffic Indication Map
TKIP	Temporal Key Integrity Protocol
TP	Transmission Probability
TPC	transmit Power Control
TWT	Target Wake Time

TXOP	Transmission Opportunity
UDP	User Datagram Protocol
UWB	Ultra-Wideband
WBAN	Wireless Body Area Networks
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WG	Working Group
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Networks
WSN	Wireless Sensor Networks

Contents

List of Figures

List of Tables

Chapter 1

Introduction

With the advancement of wireless communications over the last few decades, and having been widely used, wireless communication is an eminent solution for the connectivity. Wireless communication form a base for internet, interconnects billions of devices without considering geographical limitations. Meanwhile, growth in quantity of various complex technologies was inevitable. From the very beginning, the internet has been a living entity, evolving and changing day by day with the introduction of new technologies and with the addition of more devices. They are becoming highly powerful with various embedded technologies [1, 2]. There is no limitation in the possibilities of wireless communication.

Enabling connectivity among diverse types of services and various devices such as computers, sensors, RFID tags, appliances, vehicles and etc., gives opportunity for a new paradigm called the internet of things (IoT) [2]. This new concept is driven by the expansion of Internet towards the future where everything are connected. Wireless are embedded in everything from small items such as gadgets, toys, mobile phones, home appliances, food carts to cars, bridges, roads, buildings, and even animals and people. To improve the quality of life, this omnipresence of computing will be of great help. Upon getting access to the huge amount of comprehensive data provided by sets of devices, the impact of utilizing this concept will ultimately emerge in professional, social and personal environments [3]. International data corporation (IDC) predicts the growth of IoT to 212 billion “thing” connected globally by the end of 2020 including over 30 billion installed autonomously connected smart devices serving various applications for smart systems, enterprisers and private consumers [4]. Indeed, to meet the requirements of IoT, it is very important to develop a new technologies. For enabling communications with devices via existing network infrastructures in the IoT, machine-to-machine (M2M) technology has recently emerged as a promising enabler for the development of new solutions in a plethora of IoT application [6]. Machine-to-Machine (M2M) communications is the information exchange among machines without any human interaction. The world has become more smarter and more efficient with the possibility to establish networks of automated devices without human intervention which facilitate the creation

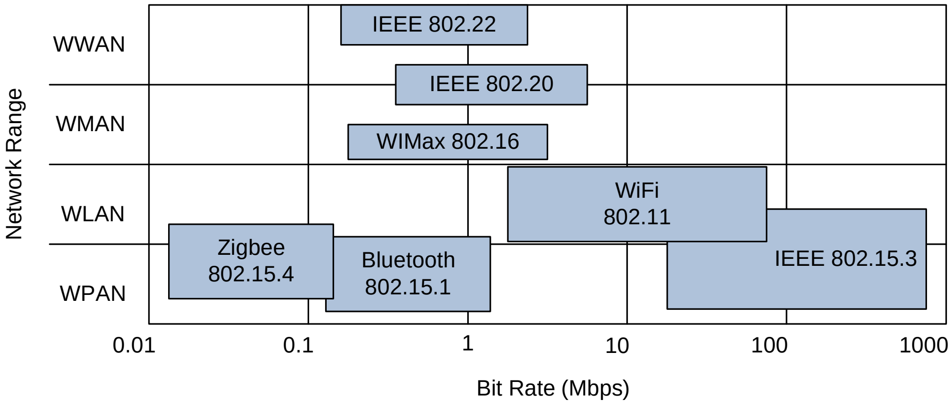


Figure 1.1: Wireless protocols overview.

of new applications. Smart buildings, smart cities, smart grids, e-Health, or automotive applications are some among many other examples [7]. M2M communications are characterized by low power, low cost, and low human intervention [8]. Due to the presence of large number of nodes in a typical M2M network, the efficient sharing of radio resources, maintaining sufficient quality-of-service (QoS) for reliable communications is vital and challenging requirement [9, 10]. One of the critical issues of M2M is how to deal with large number of accesses from large amount of machines while maintaining low power consumption with tolerable latency [11]. Moreover, applications such as the automotive applications, robotic networks, and e-health need support for mobility [12].

Some of the challenges in wireless networks are energy efficiency, scalability, routing, mobility, reliability, timeliness, security, clustering, localization and synchronization strategies. Wireless networks enable a wide range of new applications and usages like smart city, smart home, consumer electronics, industrial automation, environmental control and personal health care. There are a wide range of wireless communication protocol standards (Figure 1.1) for a wide range of applications, each one of them setting a compromise between bit rate and radio coverage, according to their target application scenarios (personal, local, metropolitan and wide).

There are various types of wireless technologies developed and being extensively used that can act as an infrastructure for developing new technologies like loT [5]. Wireless personal area networks (WPAN) covers short range (up to a few tens of meters) wireless communications, WLAN belongs to the middle range (a couple of hundred meters maximum) and cellular network communications to the long range (kilometers). Wireless technologies used in IoT are summarized as follows:

- IEEE 802.15.1/Bluetooth [13]: is a popular WPAN standard for interconnection of devices, such as mobile phones and different accessories associated with them (i.e. headset), PC accessories (i.e. keyboard and mouse), etc. However, it has not been used widely due to its high power consumption. This issue seems to be resolved with the latest low energy Bluetooth version (v4.0).

- IEEE 802.15.4 [14]: is also a WPAN standard which is suitable for very low energy consumption requirements. It is widely used for remote monitoring and home automation applications [18]. An UWB version is also available [17] achieving higher data rates.

- IEEE 802.11 [15]: is perhaps the most popular wireless interconnection interface, also known as WLAN (Wireless LAN). Already having an infrastructure for connectivity over Wi-Fi using IP, makes IEEE 802.11 a top choice for implementing IoT services. The most popular WLAN is the IEEE 802.11g offering data rates up to 54 Mbps and the latest one is the IEEE 802.11n, using multiple antenna interface (MIMO) achieving data rates up to 600 Mbps. Similarly, IEEE 802.11ah is new amendment for the support of IoT.

- Ultra-Wideband (UWB) [16]: is a WPAN technology implementation suitable for very high data rate (up to 480 Mbps) applications. The UWB technology which eventually dominated and currently exists is the Multiband Orthogonal Frequency Division Multiplexing (MB-OFDM) [16] supported by the WiMedia alliance. Another implementation attempted using Direct-Sequence UWB (DS-UWB) supported by UWB Forum [17].

- Others: DASH7 [19] and Z-Wave [20] are some other possible wireless technologies that can be used in IoT applications.

1.1 Selected Wireless Technologies in the Thesis

In this dissertation, two major wireless technologies used in M2M communications were studied. The short distance IEEE 802.15.4 standard and the long distance IEEE 802.11ah

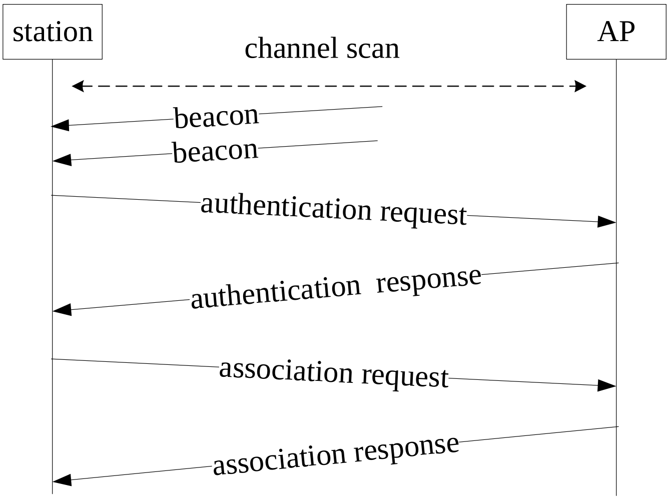


Figure 1.2: General association mechanism in wireless network.

standard were selected. The association process of both wireless technologies was extensively studied.

1.2 Research Objectives

In an AP based network such as IEEE 802.15.4 and IEEE 802.11ah, a device has to associate with AP before starting data communication. Association is the process of becoming the member of the network. Therefore, whenever a device is started or initialized, the device scans the standard defined radio channels and lists all APs which it can detect, and also signal strength indicated for each one received signal strength indicator (RSSI). It then chooses to associate itself with the AP of its choice. Only after the association is completed, the device can start data communication within the network. Figure 1.2 shows the general association mechanism in a wireless network. First, the station is authenticated and then is associated. The time spent by a station in the association plays the key role. Delay in association means delay in communication. Thus, the association should be done as soon as possible.

The major objective of this carried research is to study the association procedures in IEEE 802.15.4 and IEEE 802.11ah networks and to suggest some techniques and algorithms which can improve the association delay.

1.3 Contributions of Dissertation

This dissertation aims at contributing to the field of wireless networking. In particular, among the seven layers of the wireless networking protocol suite, the focus of this study is on the MAC sub-layer of the data link layer. In this dissertation, we present some innovative approaches that minimize the association time in a network.

The first contribution of this dissertation is dedicated to improvise the association time in IEEE 802.15.4. We observed that the amount of time required for the association process in IEEE 802.15.4 can be significantly reduced. We present a fast association technique for IEEE 802.15.4. In the proposed scheme, by scanning just a single channel, a node can learn about all the coordinators working in different channels. The single channel scanning scheme is able to decrease the association time of IEEE 802.15.4 operating in 2.4 GHz by 32 times. Furthermore, the proactive algorithm to anticipate the future link breakage and a method to increase the node connectivity time with its coordinator are proposed for the further enhancements. Experimental results have verified that our schemes work well also in the mobile sensor network environment. By virtue of rigorous performance analysis carried using computer simulations in ns-2 and through numerical analysis, we demonstrate that the new association scheme significantly outperforms the legacy method by decreasing the association time. Furthermore, rise in network throughput and decrease in packet transmission delay is observed because of prompt association and longer connectivity.

The next contribution is dedicated to improvise the association delay in upcoming IEEE 802.11ah standard. IEEE 802.11ah standard is developed to handle several thousand stations by a single AP. IEEE 802.11ah employs authentication control mechanisms allowing only a small group of stations for association in a BI. However, how to group stations and how to calculate the group size is undefined. To investigate the association procedure of IEEE 802.11ah, first the analytical model is derived. The analytical model showed several possible enhancement directions for the improvement of association delay. In this dissertation, we have proposed two novel methods for minimizing the association delay in 802.11ah. In our first method, we estimate an optimum group size for a BI and propose an enhanced association method, which fully utilizes the BI giving the minimum association time. By virtue of rigorous performance evaluation and the validated numerical results, we show that the proposed methods were able to minimize the total association time.

In IEEE 802.11ah networks, stations are divided into groups. But, the problem is that only one group can operate at a time. In the proposed second scheme, we try to eliminate this shortcoming. By electing a group head in each group and by using transmission power control to confine the transmission hearable only inside the group, the proposed method enable concurrent association in all groups at the same time. By virtue of the validated numerical results, we show that the proposed methods were able to decrease the total association time by several folds.

1.4 Organization of Dissertation

The remainder of this dissertation is organized as follows. Chapter 2 presents background information on IEEE 802.15.4 standard. Channel scanning and association procedure in IEEE 802.15.4 based WPAN are comprehensively discussed. Chapter 3 presents proposed association scheme for IEEE 802.15.4 along with numerical and simulation results. Chapter 4 presents background information on WLANs and the networking protocol suite for WLANs. Different standard MAC protocols for a typical IEEE 802.11 based WLAN are comprehensively discussed, and the new IEEE 802.11ah amendment is introduced. Chapter 5 presents the main features of 802.11ah. Association procedure in IEEE 802.11ah is discussed and the analytical model for the association process is derived. Chapter 6 estimates the optimum group size for association in IEEE 802.11ah and based on that a fast association method is presented. Experimental results are presented to show its superiority over its conventional counterpart. In Chapter 7, block association method is introduced and its performance is evaluated. Finally, Chapter 8 concludes the dissertation.

Chapter 2

IEEE 802.15.4

2.1 Introduction

M2M communication or also known as a wireless sensor network (WSN) is a network of self-organizing low-powered devices having sensing and communication capabilities [21, 22, 23]. The need for Low Rate Wireless Personal Area Networks (LR-WPANs) has been driven by the large number of emerging applications such as home automation, factory automation, health-care monitoring, and environmental surveillance [25]. IEEE 802.15.4 standard for LRWPAN has been widely accepted as the de facto standard for WSN that focuses on short-range wireless communications. The goal of the IEEE 802.15.4 LRWPAN is to support low data rate connectivity between wireless sensors with low complexity, cost and power consumption [14, 22, 24].

2.2 Overview of IEEE 802.15.4

The medium access control (MAC) sub-layer and the physical layer (PHY) for LR-WPANs is specified by the IEEE 802.15.4 protocol as shown in Figure 2.1 [14, 42, 43]. The IEEE 802.15.4 protocol is designed for low-data rate, low power consumption, and low cost wireless networks which fits the requirements of short range M2M applications. IEEE 802.15.4 is developed to complement the range of available wireless technologies in the lower end spectrum of data rates, power consumption, and cost. IEEE 802.15.4 has small coverage area. Coordinator covers a limited area, also called its personal area network (PAN). In IEEE 802.15.4, there are mainly two types of devices: full function device (FFD) and reduced function device (RFD). FFD can support all the network functions and can operate as a PAN coordinator or an end device. RFD can only be used as an end device. We use the term device or node interchangeably to represent the RFD. Similarly, coordinator and PAN coordinator are used interchangeably to represent the network coordinator. The IEEE 802.15.4 standard supports three kinds of topology: star, peer-to-peer, and cluster tree topologies, which can operate on the beacon and the non-beacon-enabled modes.

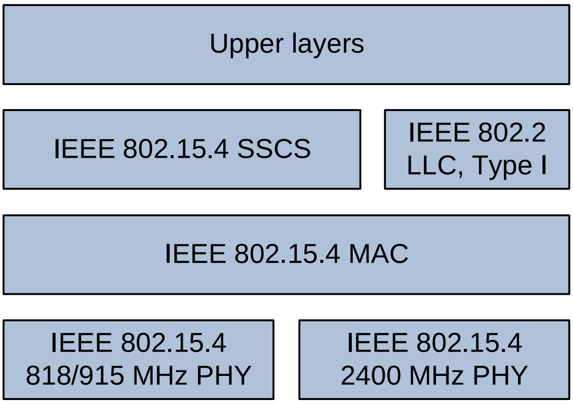


Figure 2.1: IEEE 802.15.4 Architecture.

2.3 Physical Layer (PHY)

The PHY layer consists of the data service and the management of the data service. The management part is the interface to the higher layers, and the data service part enables the transmission and reception of PHY protocol data units (PPDU) over the radio channel. The standard has two different modulation techniques, binary phase shift keying (BPSK) and offset-quadrature shift keying (O-QPSK), both used with direct sequence spread spectrum (DSSS) with a chip rate of 2 MChip/s on a 2 MHz wide frequency channel. The IEEE 802.15.4 standard operates in the unlicensed ISM bands, and the range is typically 5-75 m. The IEEE 802.15.4 offers three operational frequency bands: 2.4 GHz, 915 MHz, and 868 MHz. Three frequency bands have the following data rates: 250 kbps in the 2.4 GHz ISM band, 40 kbps in the 915 MHz ISM band and 20 kbps in the 868 MHz ISM band. O-QPSK modulation is used in the first case, and BPSK in the next two cases. Figure 2.2 shows the three operational frequency bands:

- 868-868.6 MHz: Europe, allows one communication channel.
- 902-928 MHz: North America, up to ten channels.
- 2400-2483.5 MHz: worldwide use, up to sixteen channels.

The protocol also allows dynamic channel selection, a channel scan function in search of a beacon, receiver energy detection, link quality indication, and channel switching. The physical layer of IEEE 802.15.4 is in charge of the following tasks:

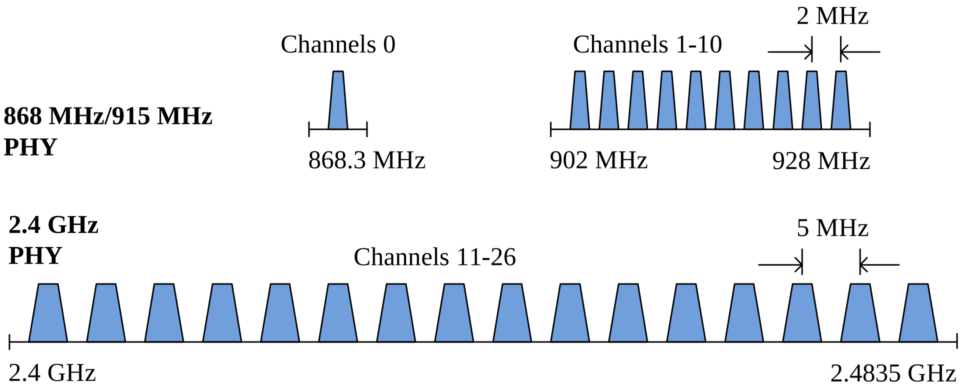


Figure 2.2: IEEE 802.15.4 PHY overview.

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

- **Energy Detection (ED):** ED is the estimation of the received signal strength within the bandwidth of an IEEE 802.15.4 channel. However, the received signal is not decoded. The energy detection time should be equal to 8 symbol periods. This measurement is typically used by the Network Layer as a part of channel selection algorithm or for the purpose of Clear Channel Assessment (CCA), to determine if the channel is idle or busy.

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

- **Clear Channel Assessment (CCA):** CCA is the evaluation of the medium activity state: idle or busy. The CCA is performed in three operational modes: (a) Energy Detection mode: the CCA reports a busy medium if the detected energy is above the ED threshold. (b) Carrier Sense mode: the CCA reports a busy medium only is it detects a signal with the modulation and the spreading characteristics of IEEE 802.15.4 and which may be higher or lower than the ED threshold. (c) Carrier Sense with Energy Detection mode: this is a combination of the aforementioned techniques.

- **Channel Frequency Selection:** The IEEE 802.15.4 defines 27 different wireless channels. Each network can support only part of the channel set. Hence, the physical layer should be able to tune its transceiver into a specific channel when requested by a higher layer.

2.4 Medium Access Control Sub-Layer (MAC)

The MAC protocol supports two operational modes, i.e., beacon and non-beacon-enabled modes.

- **The non Beacon-enabled Mode:** When the coordinator selects the non-beacon enabled mode, there is neither beacons nor superframe. Medium access is ruled by an unslotted CSMA/CA mechanism.

- **The Beacon-enabled Bode:** In the beacon-enabled mode, communication is synchronized and controlled by a PAN coordinator, which transmits periodic beacons. A beacon frame is transmitted in the beginning of a superframe. During the active part of superframe, frames are exchanged between different nodes in the PAN. Medium access is basically ruled by slotted CSMA/CA. However, the beacon-enabled mode also enables the allocation of contention free time slots, called guaranteed time slots (GTSs) for nodes requiring guaranteed bandwidth.

2.5 Superframe Structure

The superframe is defined between two beacon frames as shown in Figure 2.3. The structure of superframe is determined by coordinators using two parameters: superframe order (SO) and beacon order (BO). SO is used to determine the length of superframe duration, whereas BO defines the beacon interval. In beacon-enabled mode, each coordinator defines a superframe structure which is constructed based on:

- **The Beacon Interval (BI):** BI defines the time between two consecutive beacon frames.

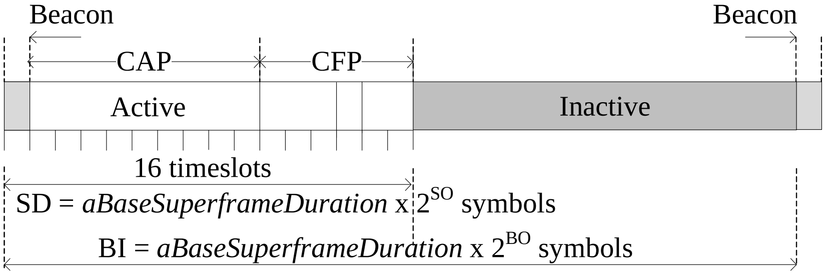

Beacon
Beacon
CAP
CFP
Active
Inactive
16 timeslots
SD = aBaseSuperframeDuration x 2^SO symbols
BI = aBaseSuperframeDuration x 2^BO symbols

Figure 2.3: The superframe structure of IEEE 802.15.4.

- **The Superframe Duration (SD):** SD defines the active portion in the BI and is divided into 16 equally-sized time slots, during which frame transmissions are allowed. Optionally, an inactive period is defined if BI $>$ SD. During the inactive period (if it exists), all nodes may enter in a sleep mode to save energy. BI and SD are determined as follows:

$$\left.\begin{aligned} BI &= aBaseSuperframeDuration \times 2^{BO} \\ SD &= aBaseSuperframeDuration \times 2^{SO} \end{aligned}\right\} \textit{for } 0 \leq SO \leq BO \leq 14$$

  aBaseSuperframeDuration = 15.36 ms (assuming 250 kbps in the 2.4 GHz frequency band) denotes the minimum duration of the superframe, corresponding to SO=0.

The superframe shown in Figure 2.3 may consist of active and inactive periods. The active portion of the superframe structure is composed of three parts, the beacon, the contention access period (CAP) and the contention free period (CFP):

- **Beacon:** The beacon frame is transmitted during beacon period at the beginning of the superframe. It contains the information on the addressing fields, the superframe specification, the GTS fields, the pending address fields and other PAN related information.

- **Contention Access Period (CAP):** The CAP starts immediately after the beacon period and ends before the beginning of the CFP, if it exists. Otherwise, the CAP ends at the end of the active part of the superframe. The minimum length of the CAP is fixed at aMinCAPLength = 440 symbols. All transmissions during the CAP are made using the slotted CSMA/CA mechanism. However, the ACK frames and any data that immediately follows the ACK of a data request command are transmitted without contention. If a transmission cannot be completed before the end of the CAP, it must be deferred until the next superframe.

- **Contention Free Period (CFP):** The CFP starts immediately after the end of the CAP and must complete before the end of the superframe. Transmissions are contention-free because they use GTS, which must be previously allocated by the PAN coordinator. All the GTSs that may be allocated by the PAN coordinator are located in the CFP and must occupy contiguous slots. The CFP can grow or shrink depending on the total length of all GTSs.

2.6 PAN Initialization, Channel Scan, and Association

Any FFD can be a PAN coordinator. FFD should perform the ED to detect the peak energy of a channel and choose an appropriate channel for communication. Then, FDD carries out an active scan to locate any coordinator transmitting beacon frames within its personal operating space (POS). Depending on the availability of a coordinator in the vicinity, the FDD can join the existing network or starts its own PAN. After a PAN has been initialized, it transmits periodic beacon. The other devices in the POS of the PAN can communicate with the coordinator and associate with this PAN. In order to start association, an end device needs to discover coordinators in the surrounding. In beacon-enabled IEEE 802.15.4, two types of channel scanning operations are performed by end devices. During the channel scans, nodes are deprived from data communication and must discard all data frames received. The association procedure takes place when a device wants to associate with a coordinator. This mechanism can be divided into three separate phases: (a) channel scan procedure; (b) selection of a possible coordinator; (c) association with the coordinator. IEEE 802.15.4 enables four types of channel scan procedures:

- **Energy Detection Scan** is performed to obtain a measure of the peak energy in each channel. The energy detect scan is used to determine which channels are the quietest. In each channel, ED scan is performed for the duration of t_{scan} symbols.

- **Active Scan** is performed to locates all coordinators transmitting beacon frames. This scan is performed on each channel by first transmitting a beacon request com-

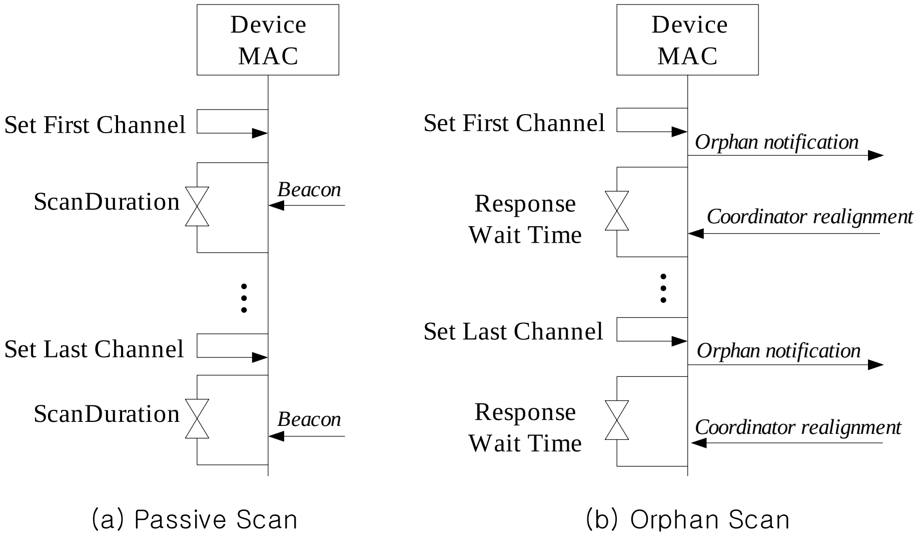


Figure 2.4: Channel scanning mechanism in beacon-enabled IEEE 802.15.4.

mand. During the active scanning, FDD first sends out a beacon request command and waits for the duration of t_{scan} symbols. If a beacon could not be detected during t_{scan}, the FFD can construct its own PAN by broadcasting its periodic beacons. During a active scan the MAC sub-layer must discard all frames received over the PHY data service that are not beacon frames.

- **Passive Scan** is performed for the coordinator discovery. As shown in Figure 2.4(a), during the passive scan, a device searches for beacon frame in each channel for the duration of t_{scan} symbols and records the beacon frames received in each channel. After the scanning is completed, the device may select any coordinator from the available pool for the association. If no beacon is detected, the device starts another passive scan after a period of time. During a passive scan the MAC sub-layer must discard all frames received over the PHY data service that are not beacon frames.

- **Orphan Scan** allows a device to attempt to relocate its coordinator following a loss of synchronization (missing of beacon more than *aMaxLostBeacons* times). The device shall first send the orphan notification command frame, and waits for coordinator realignment command frame for at most *macResponseWaitTime* symbols as shown in Figure 2.4(b). This procedure is repeated until it receives the coordinator realignment frame or all the available channels are scanned. If the orphan scan is unsuccessful, the device looks for a new parent by performing the passive scan. During an orphan scan, the MAC sub-layer shall discard all frames received over the PHY data service that are not coordinator realignment MAC command frames.

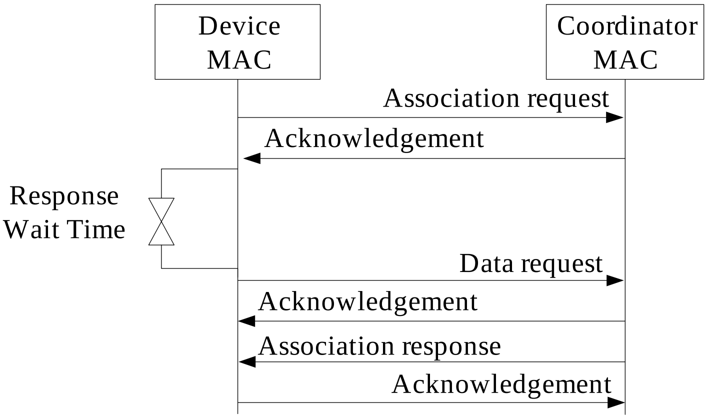


Figure 2.5: Association message exchange in IEEE 802.15.4.

In order to start association process, a node needs to know the PAN's physical channel, coordinator ID, addressing mode, and PAN ID. Nevertheless, as the channel on which the coordinator operates are unknown, nodes have to scan all available channels [34, 50, 35, 36, 37, 49]. Thus, the passive scan is performed for the coordinator discovery. IEEE 802.15.4 maintains a list called PANDescriptor that records all the beacons received. Based on the information collected during the scan, the device can choose the most suitable parent that permits associations. The IEEE 802.15.4 protocol standard does not specify in detail on coordinator selection. Nevertheless, one of the most relevant parameters to be considered is the LQI [25, 26]. Once the node selects the suitable coordinator, it starts association procedure by sending a request for the association as shown in Figure 2.5. Then, if the coordinator accepts the device, it adds it to its neighbor table as its child. In the case of a successful association, an association response command frame is sent to the device that contagions its short address. Otherwise, in the case of an unsuccessful association, the association response embeds the problem status information. The coordinator replies to the association command frame with an acknowledgment embedding the pending data control flag active, meaning that it has data ready to be transmitted to the device. The association procedure is completed when the device sends a data request command frame to the coordinator requesting the pending data. After a successful association, the device stores all the information about the new PAN by updating its MAC PAN information base (MAC PIB) and can start transmissions. Thus, a node association requires channel scanning followed by the association message exchange which is really a time consuming procedure [34, 54, 26, 47]. For a mobile node, association procedure is even worse because the mobile node has to go through the orphan scan first followed by the passive scan and then only can start the association message exchange [34, 54, 26, 38]. We use the term re-association to explicitly denote the association procedure used by the mobile node. We have observed from our study that if somehow this whole association duration be shortened to some tolerable level, IEEE 802.15.4 can be used in the mobile sensor network applications.

The disassociation from a coordinator is done via a disassociation request command. The disassociation can be initiated either by the device or by the coordinator. After the disassociation procedure, the device loses its short address and is not able to communicate. The coordinator updates the list of associated devices, but it can still keep the device information for a future re-association.

2.7 Guaranteed Time Slot Mechanism (GTS)

The GTS mechanism allows devices to access the medium without contention in the CFP. On request from the device, GTSs are allocated by the PAN coordinator and are used only for communications between the PAN coordinator and a device. Each GTS allocation may contain one or more time slots. The PAN coordinator may allocate up to seven GTSs in a superframe. Each GTS is only one direction: from the device to the coordinator or from the coordinator to the device. The GTS can be deallocated at any time at the discretion of the coordinator or the device that originally requested the GTS allocation. The PAN coordinator is responsible for performing the GTS management.

2.8 Concluding Remarks

In this chapter, we have provided a brief overview of IEEE 802.15.4 standard and its main features. The IEEE 802.15.4 is designed for static network and is an attractive choice for various short range WSN applications. However, its inability of mobility support makes it undesirable for mobile sensor network applications. We observed that the amount of time required for the association process is the key reason IEEE 802.15.4 is unable to handle mobility. In the next chapter, we will highlight long association delay problem of IEEE 802.15.4 and present our innovative solutions for the problem.

Chapter 3

Minimizing Association Delay in IEEE 802.15.4

In this chapter, we propose an interesting method to minimize the association delay in IEEE 802.15.4. Theoretical and simulation-based analysis are presented to show its superiority over its conventional counterpart.

3.1 Motivation

In many WSN applications, the sensor nodes need to be mobile. Wireless body area networks (WBANs) or healthcare wireless sensor networks (HWSNs) are such areas where node mobility is dominant [27, 31, 41]. The rapid growth in physiological sensors, low power integrated circuits, and wireless technology has enabled wireless body area networks in or on human body for continuous monitoring of vital signs such as heart-rate, temperature, blood pressure, etc. [27, 31]. A number of smart physiological sensors can be integrated into a wearable wireless network, which monitor vital body signs such as heart-rate, temperature, blood pressure, ECG, EEG, etc [32]. If an emergency is detected, the physicians will be immediately informed through the computer system by sending appropriate messages or alarms. Furthermore, WBAN (connected to the Cloud) can also be deployed in home environment which monitors not only human health but also human activities to provide low-cost, high-quality health care, and social network services to users [28][29]. WBANs used to monitor patients should offer mobility support of the sensor nodes carried by the patients. However, supporting mobility in IEEE 802.15.4 brings lots of new challenges and issues [45, 39, 41]. In IEEE 802.15.4, node mobility is expected to facilitate numerous applications, from home health-care and medical monitoring to target detection [45, 34, 39, 40].

IEEE 802.15.4 has small coverage area. Thus, large numbers of access points are deployed to cover large areas. Each access point covers a limited area, also called its PAN. Hereafter, we use the term PAN coordinator or just coordinator to refer an access point. The mobility of devices causes frequent loss of connection. To maintain the sensor connectivity, sensor node should frequently change their access point by performing a mechanism known as a handover. However, providing IP connectivity to mobile devices means that the devices need to be empowered with sophisticated mobility related IP protocols like MIPv6, HMIPv6 etc [30]. Thus, it is not feasible to run complex and sophisticated mobility protocol on a mobile node. Thus, in this work, we proposed light weighted handover mechanism that can be handled solely by IEEE 802.15.4. A mobile node loses its connectivity with the parent coordinator if it moves out of the coverage of its parent. To perform handover, the mobile node should first detect the loss of connectivity with its parent and then find a new parent for the new connection.

- **Detection of Loss of Connectivity**
  A node without a parent is considered as the orphan node. A node consider itself as orphan node if it cannot receive beacon from the parent coordinator for *aMaxLostBeacons* times. Orphan scan allows a device to attempt to relocate its coordinator following a loss of connectivity. If the orphan scan is unsuccessful, the device looks for a new parent by performing the passive scan. For a mobile node, the connection with coordinator can frequently break and the reassociation procedure is time consuming because the mobile node has to go through the orphan scan first followed by the passive scan and then the association message exchange. We use the term reassociation to explicitly denote the association procedure used by the mobile node. From our study, it is observed that IEEE 802.15.4 can be used in the mobile sensor network applications if somehow this whole reassociation duration is shortened to some tolerable level.

- **Coordinator Discovery**
  In order to start association, a sensor node needs to find a coordinator. The passive scan is performed for the coordinator discovery. During the passive scan, a device searches for beacon frame in each channel and records the beacon frames received in each channel. Once the node selects the suitable coordinator, it starts association procedure by sending a request for association. Once accepted by coordinator, the node is the member of the network.

The association is a time consuming procedure, where the required duration is proportional to the number of channels scanned. Furthermore, the connection is lost once the mobile node moves away from the transmission range of the coordinator. Therefore, the service continuation depends on how and which coordinator is selected in the mobile WSN environments. To support mobility, the association procedure should be modified in such a way that the node's loss of connectivity should be realized quickly, the channel scanning time should be minimized, and the coordinator connectivity time should be maximized.

This work focuses on the beacon-enabled network in 2.4 GHz band, where all coordinators have fixed positions, but the sensor nodes can be mobile. This type of topology applies to smart home and health care applications, where sensor nodes are attached to human. It is shown that a fast and energy efficient coordinator discovery and the long connectivity time with the coordinator cannot be achieved in this mobile WBAN without proper methods. Thus, the contribution of this work is three folds. The first algorithm tries to anticipate the link breakage by analyzing the LQI history. Thus, the algorithm decreases the time required by node to realize the link breakage from the coordinator. Second, we present a novel association scheme called dedicated beacon channel (DBC) that prevents a node from scanning multiple channels. The third algorithm increases the node connectivity time with a coordinator by performing handover to the coordinator that gives the longest connectivity time. The proposed association scheme provides support for mobility without the involvement of any higher layers. DBC scheme was presented in [34, 35]. DBC provides support for mobility while keeping intact the original features such as flexibility, scalability, adaptability, and low power consumption of typical IEEE 802.15.4.

3.2 Related Works

Node mobility degrades the performance of IEEE 802.15.4 based WPANs [26, 44, 45]. Also, mobility is highly dependent on network topology; network performance decreases with the number of mobile nodes or when nodes are moving fast. At higher speeds, nodes continuously lose their connectivity and fail to associate with coordinators [44]. There are some efforts done to minimize the association duration in IEEE 802.15.4. In IEEE 802.15.4e [46], optional fast association (FastA) is defined, which allows a device to associate in a reduced duration. However, most of the efforts are limited to mobility management, decreasing the duration of association message exchange [47], increasing connectivity [45] or coordinator discovery [26, 48, 49], whereas the channel scanning part has been left untouched. The authors in [50] have presented an interesting solution called greedy channel scan (GCS) scheme to decrease the channel scanning duration. In the GCS scheme, nodes are expected to use only 4 clear channels and those channels are scanned first. However, in GCS, if a node is unable to find the coordinator in all 4 channels, then it has to scan all remanding channels. Similarly, there are several works on multichannel solutions but are limited to throughput improvement or beacon collision avoidance [51, 52, 53].

In [47], Zhang et al. proposed an improved association scheme called Simple Association Process (SAP) that eliminates the redundant primitives, thus decreases the packet collisions and the association delay.

A fast association mechanism [54] is proposed for real-time WPAN applications. Delay caused by scanning multiple channels is reduced because the scanning process is stopped as soon as a beacon is received. Although this scheme prevents nodes from scanning all available channels, but nodes still need to scan multiple channels before finding a coordinator. Furthermore, the first beacon received may not always be the suitable coordinator.

Similarly, there are other works which focus on the neighbor discovery for quick association. In [48], algorithms are proposed for the optimized discovery of IEEE 802.15.4 static and mobile networks operating in multiple frequency bands and with different beacon intervals. In [45], a scheme to increase coordinator connectivity time with mobile nodes is presented for IEEE 802.15.4 beacon-enabled networks. Nodes use time-stamp of received beacons during the scan, along with link quality to determine the appropriate coordinator for association. Other mobility management schemes for cluster-tree based WPAN have been proposed by Chaabane et al. [55] and Bashir et al. [26]. These approaches use the speculative algorithm for node association based on LQI. Based on LQI value, the mobile node anticipates cell change based on LQI before the loss of connection and tries to associate with the next coordinator. However, in all the cases, nodes have to scan multiple channels to find coordinators.

3.3 Network Model

One obvious choice for IEEE 802.15.4 to cover a large areas is by using cluster tree topology. However, a cluster tree topology presents two major problems. First, the colli-

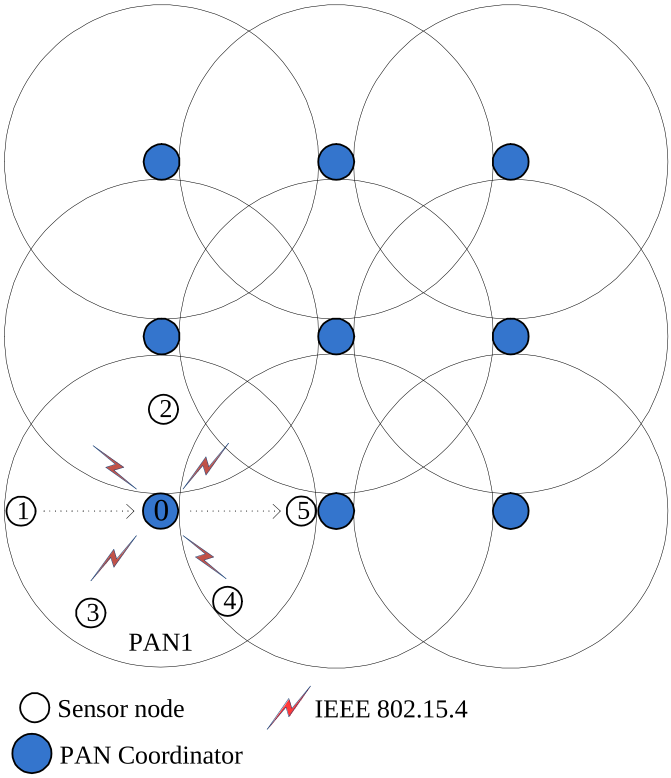


Figure 3.1: Network model.

sion probability is high since all nodes transmit on the same channel. Second, the IEEE 802.15.4 standard does not specify how to synchronize a cluster tree network [55]. Thus, we select the start topology to balance the network load. But, communication between different PAN coordinators is not possible unless they belong to the same channel, or if they define a common transmission channel. In this work, we consider that different wiredly connected PANs can form a unique heterogeneous network composed of star PANs. All PANs are assumed to be connected with the base station through the wired connection. Messages between nodes that do not belong to the same PAN Id can then be routed through the base station.

The basic network design is shown in Figure 3.1, which models a typical HWSN. The construction of a HWSN comprises three main elements, namely, a) a base station or gateway that acts as a bridge between the HWSN and Internet, b) PAN coordinator that support communication to/from the sensor nodes, and c) the sensor nodes themselves that collect body parameters and send them wirelessly over the network. Due to

Table 3.1: Network parameters and values.

Parameter	**Value**	**Parameter**	**Value**
Assumed power supply	3 V	Number of Channels	16
Reception power	56.5 mW	Transmission power	48 mW
Idle power	2.79 mW	Sleep power	30 μW
Transition time	192 μs	Transmission range	10 m
aMaxLostBeacons	4	LQI threshold	170
Frequency band	2.4 GHz	Radio data rate	250 kbps
Routing	AODV	Traffic	CBR
Data rate	2 kbps	Buffer size	10 packets
Packet size	50 B		

the limited coverage area of each PAN in indoor environments, several PAN coordinator are deployed to cover the monitored zone as shown in the figure. Furthermore, to prevent interference, each PAN may operate in a different transmission channel. Mobile node changes the point of attachment as it passes from a PAN to another in the network. For the maximum coverage of the area, the coordinators are assumed to be separated by the distance of transmission range. However, adjacent PAN does not interfere each other as they operate in different channels. In this work, LQI value is used to detect the movement of a sensor node. In IEEE 802.15.4, every MAC frame contains LQI value that ranges from 0 to 255. The LQI measurement is a characterization of the strength and/or quality of a received packet. However, the calculation of the LQI is not specified in the IEEE 802.15.4 standard. However, receiver ED, signal-to-noise ratio (SNR), or the combination of these methods can be used. In order to observe the change in LQI with respect to distance, mobility, and background traffic, we conducted a simple experiment. The simulation is done in NS-2 using parameters from Table 3.1 [90]. In PAN1 of Figure 3.1, node 1 is moved toward the node 5 at the speed of 1 m/s. Transmission range of PAN was set to 10 meters. The effect of interference is also accounted by introducing background traffic from nodes 2, 3, and 4. LQI values of beacon received from the coordinator as the node 1 moves are shown in Figure 3.2. In NS-2, the LQI is calculated based on the received signal strength and the signal to noise ratio. A packet is only received if its LQI is equal or greater than 128. Thus, LQI obtained ranges from 128 to 255 because the packets whose LQI is below 128 are dropped. Also, the LQI value of 255 is observed when the distance between node and coordinator is less than 7m and the

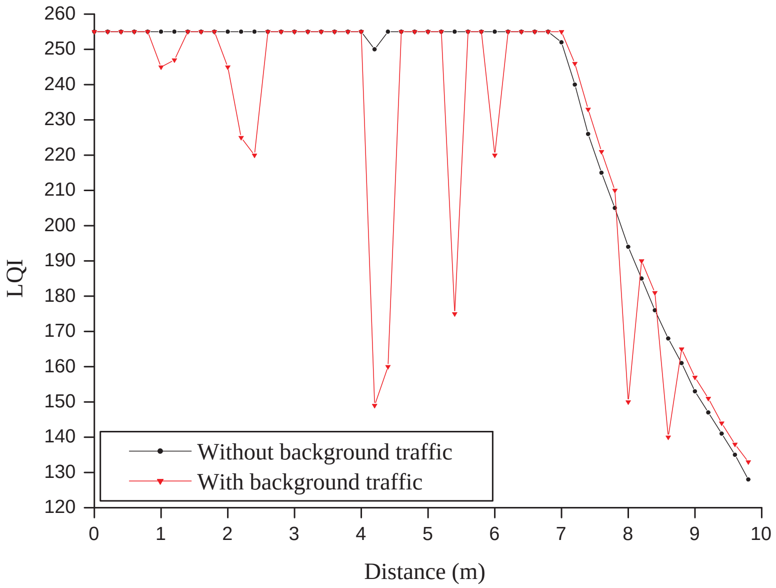


Figure 3.2: Change in LQI with distance and background traffic.

gradual decrease in LQI is observed once the distance from the coordinator exceeds 7m. With movement, some false LQI values are observed, and the LQI drops as the sensor node moves away from the coordinator. LQI is also affected by the background traffic because of interference and, especially, when the node is moving, where sudden drops in LQI values are observed. However, in this work, the normalized value of LQI is used to detect node movement. In [26] and [45], authors also obtained similar LQI result.

3.4 Proposed Scheme

Channel scanning is the most time consuming part of the association procedure. The time spent on association for various value of BO are shown in Figure 3.3. For each value of BO, the time required for association as the number of channels to scan varies from 1 to 16 is shown in the figure. The figure illustrates that the association time increases as the number of channel increases. From the detailed study of IEEE 802.15.4, it is observed that three updates can be possible to enable IEEE 802.15.4 efficiently handle mobility. The first update is the reduction of coordinator discovery time. The channel scanning for coordinator discovery is the most time consuming procedure. If somehow the nodes are prevented from scanning multiple channels, the mobility can be handled efficiently.

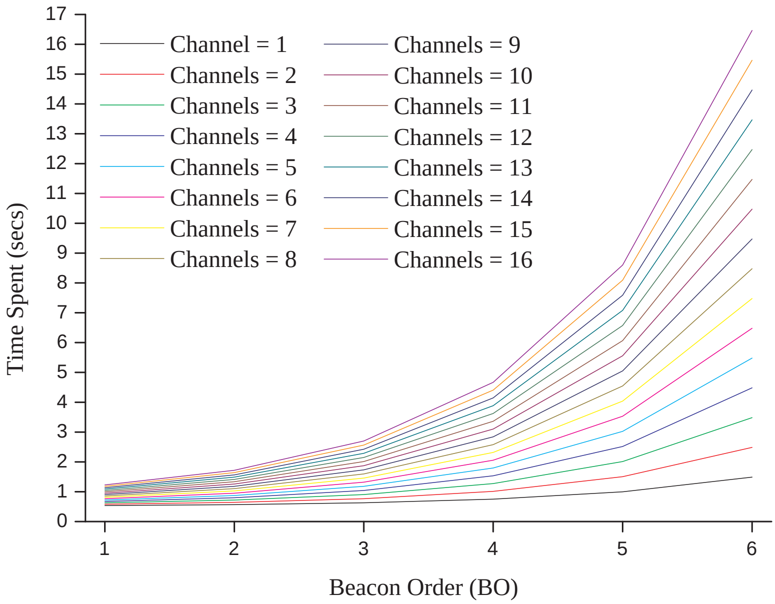


Figure 3.3: Time spent on association as BO and number of channels varies.

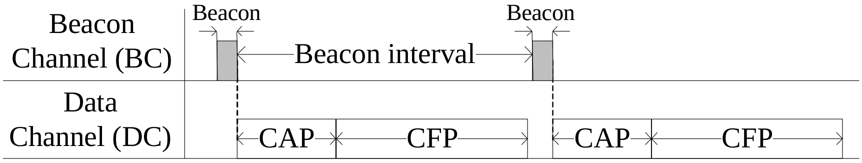


Figure 3.4: Channel switching mechanism of the proposed DBC scheme.

The second update is the early detection of loss of connectivity. The detection of loss of connectivity by counting loss of beacons for *aMaxLostBeacons* times is time consuming. A proactive method can significantly reduce the detection time of link breakage. And, the third one is to increase the connectivity time with the coordinator. In our proposed scheme, we implement all above mentioned updates to handle the mobility efficiently. Also, all the three updates are simple and can be easily implemented.

For the prompt coordinator discovery, the proposed DBC scheme exploits the channel switching capability of IEEE 802.15.4 radio hardware [56]. In DBC, we use two channels: beacon channel (BC) and data channel (DC). BC is used for the beacon frames, whereas the rest of the communication is done in the DC. A node switches its radio channel to the BC during its beacon period and then returns to its original DC at the end of

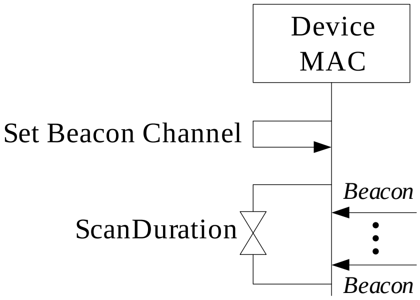


Figure 3.5: The passive scan in the proposed DBC scheme.

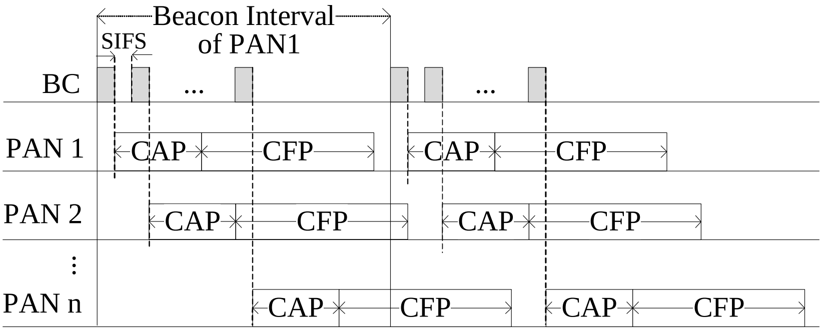


Figure 3.6: Scheduling of beacon in co-existence of multiple PANs.

the beacon period as shown in Figure 3.4. Thus, transmission and reception of the beacon frame are done in BC, whereas data communication is done in DC. With this small and simple modification in the original IEEE 802.15.4, now the nodes do not need to scan each and every channel for the association. The entire network information can be learned by just scanning the BC only as shown in Figure 3.5. The DC information is conveyed by piggybacking it in the beacon payload of the beacon frame. Furthermore, DBC scheme does not require separate channel scans such as ED scan, active scan, passive scan, and orphan scan. BC scan performs functions of all channel scans with minimal time.

3.4.1 Initialization of a PAN Coordinator

Unlike in original IEEE 802.15.4, nodes do not perform ED scan and active scan for initialization of a PAN coordinator. In the proposed scheme, when a FFD is initialized, it performs the passive scan in the BC only for the durations of t_{scan} (Figure 3.5). If

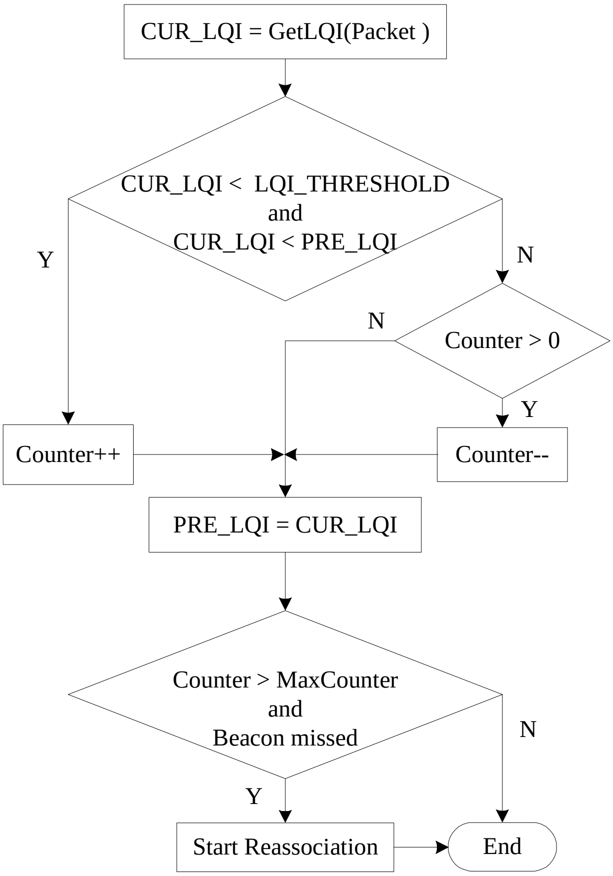


Figure 3.7: Flow chart of proactive reassociation decision.

beacons are received, FFD can join the suitable PAN. Otherwise, FFD can construct its own PAN by broadcasting its periodic beacons. The FFD is flexible to select its own non-overlapped DC, but it must broadcast its beacon in the BC. In the case where a number of PANs coexist in an adjacent area, (i.e., apartments or buildings having independent PAN), FFD schedules its beacon period with the minimum gap of the short inter frame space (SIFS) and chooses the unused DC as shown in Figure 3.6.

3.4.2 Proactive Re-association Decision

LQI is an important metric available in IEEE 802.15.4 for detection of link quality between two communicating nodes. Make-before-break approach requires either sensor node or coordinator to monitor the LQI for triggering the handover. However, the fre-

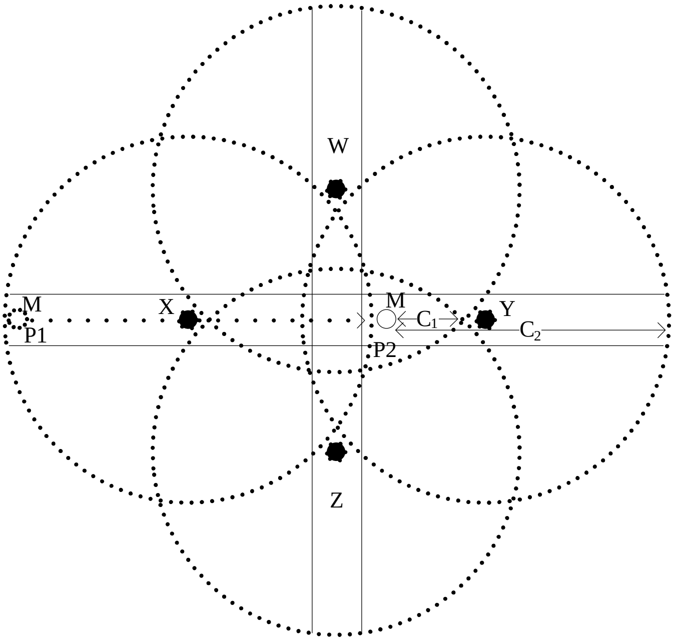


Figure 3.8: Selection of coordinator.

quency of beacons can be low or high depending on BO of the coordinator. At higher BO, beacons are received after longer intervals resulting in delayed detection of link quality. In our proactive re-association decision (PRD) scheme, sensor node monitors all packets from the coordinator and they used for analyzing the LQI. PRD algorithm shown in Figure 3.7 is used to take handover decision. The algorithm first observes the LQI value of each packet received from the coordinator. The node anticipates the link breakage by analyzing the LQI history and missing of a beacon. But, the link quality can be degraded due to increasing in distance, interference, and collision of packets. Thus, instantaneous LQI alone is not a reliable parameter for taking handover decision. Furthermore, observed LQI values can fluctuate at any instance of time. Therefore, successive LQI readings are considered. A counter shown in Figure 3.7 keeps track of how many times the LQI is less than previously recorded LQI. In addition to LQI drop, missing of beacon is used to ensure the link breakage. If LQI drops continuously for *MaxCounter* number of times followed by missing of a beacon, the reassociation decision is taken. The algorithm is designed in such a way that the fluctuation in the reading is compensated by decreasing the counter as shown in the flow chart.

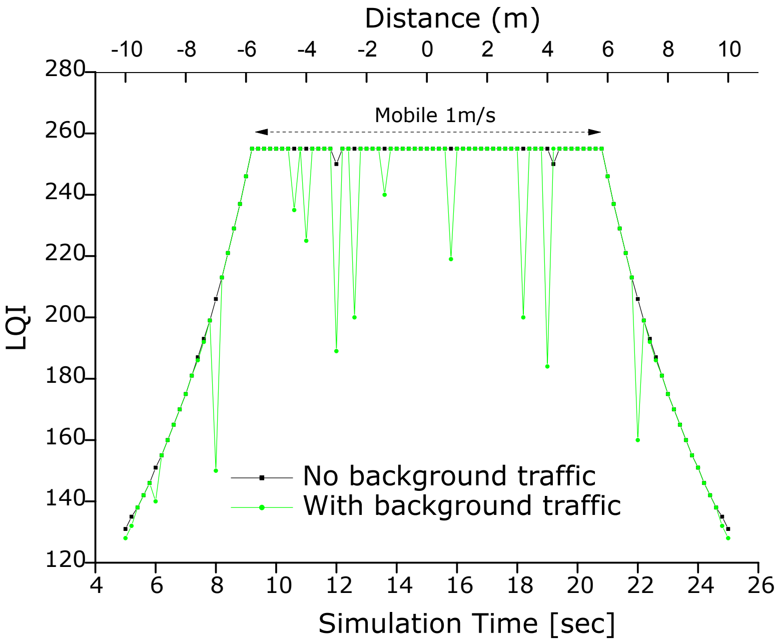


Figure 3.9: LQI received at node M as it passes through coordinator X.

3.4.3 Coordinator Selection and Association

A device that wants to associate with a PAN can be a new (just on) or an orphan device. Unlike in IEEE 802.15.4, an unassociated node always performs the passive scan in the BC for the duration of t_{scan} symbols. Let's see a coordinator selection process with an example. In Figure 3.8, the mobile node M (initially associated with X) moves toward coordinator Y at the speed of 1 m/s. The dotted region is the transmission range of a coordinator. IEEE 802.15.4 maintains a list called PANDescriptor that records all the beacons received. PANDescriptor contains fields such as PAN ID, coordinator address, logical channel, LQI (LQI of beacon received) and so on. Figure 3.9 shows simulation result of LQI of the beacon received from the coordinator X as the mobile node M moves from the position P1 to P2.

The simulation is done in NS-2 using parameters from Table 3.1. The figure shows that LQI increases as the node moves towards the coordinator, and vice versa. In IEEE 802.15.4, the multiple beacons received from the same coordinator is ignored. However, in DBC, we analyze LQI value of the multiple beacon from the same coordinator to anticipate the node's direction of movement. DBC adds 2 more fields in PANDescriptor

Table 3.2: Added fields of PANDescriptor in DBC.

Field	**Description**
LQI Previous	LQI value of last received beacon
Direction	Counter to detect increase or decrease in LQI

Table 3.3: PANDescriptor maintained by the mobile node M in DBC.

	Coordinator W/Z			**Coordinator Y**		
Time	**LQI Previous**	**LQI**	**Direction**	**LQI Previous**	**LQI**	**Direction**
T1	200	200	0	255	255	0
T2	197	193	-1	255	255	1
T3	192	187	-2	255	255	2
T4	187	181	-3	255	255	3

as shown in Table 3.2. At the point P2, M gets disassociated with X. Table 3.3 shows the instance of PANDescriptor maintained by M during the passive scan. If a beacon is received for the first time, LQI Previous and LQI are made same. If the beacon is received again from the same coordinator, calculations are done such that LQI holds the current LQI and LQI Previous field holds the average value of LQI of beacons received. Direction field (initially zero) is decreased if the current LQI is less than the previous LQI, and otherwise, it is increased. The positive value of Direction field indicates that the node is moving towards that coordinator and negative indicates that node is moving away. Based on these values, node uses Algorithm 1 to select the optimal coordinator for the association. In the current example, coordinator Y is selected because coordinator W and Z have negative values of Direction.

Algorithm 1 Coordinator selection from PANDescriptor.

```
1. Compare the Direction and LQI of every element
2. Select that coordinator which has positive Direction and lowest LQI (but LQI > $LQI_{threshold}$)
```

3.5 Numerical Analysis

Let *aBaseSuperFrameDuration* be the number of symbols forming a superframe when SO = 0. In IEEE 802.15.4, it takes equal duration to perform ED, active, and passive scan on a channel and is given by,

$$t_{scan} = aBaseSuperFrameDuration \times (2^{BO} + 1). \tag{3.1}$$

3.5.1 PAN Initialization

In IEEE 802.15.4, a PAN coordinator performs ED scan and active scan in all available *n* channels. But, in the case of DBC, only passive scan is performed in the BC for the duration of t_{scan}. Thus, the total initialization time of a PAN coordinator for IEEE 802.15.4 and DBC is,

$$PAN_{802.15.4\_init} = 2n \times t_{scan}, \tag{3.2}$$

$$PAN_{DBC\_init} = t_{scan}. \tag{3.3}$$

Thus, as compared (3.2) with (3.3), DBC decreases the initialization of PAN coordinator by the factor of *2n*.

3.5.2 Association

The total time spent for association is the sum of time spent in the channel scan and the time spent in the association message exchange ($Asso_{msg}$). A device desiring to associate with a PAN can be a new or orphan. IEEE 802.15.4 has separate procedures for the association of new and orphan devices. The total time spent for association by a newly joining node for both protocols are given by,

$$t_{802.15.4\_asso} = n \times t_{scan} + Asso_{msg}. \tag{3.4}$$

$$t_{DBC\_asso} = t_{scan} + Asso_{msg}. \tag{3.5}$$

From (3.4) and (3.5), DBC is able to decrease the association time of newly joining node by almost the factor of *n*.

3.5.3 Detection of Connectivity Loss

In IEEE 802.15.4, the beacon interval (BI) is given by the following equation.

$$BI = aBaseSuperFrameDuration \times 2^{BO}. \tag{3.6}$$

In IEEE 802.15.4, mobile node starts the orphan scan, if it misses the beacon for *aMaxLostBeacons* times. However, in the case of DBC, re-association is performed if the beacon is missed just once. Thus, the time required for the detection of loss of connectivity (DLC) can be calculated as,

$$DLC_{802.15.4} = BI \times aMaxLostBeacons, \tag{3.7}$$

$$DLC_{dbc} = BI. \tag{3.8}$$

3.5.4 Reassociation

In beacon-enabled IEEE 802.15.4, once a node realizes that it has lost connectivity with the PAN, orphan scanned is performed. an orphan node performs the orphan scan on each channel for duration of *macResponseWaitTime (32×aBaseSuperFrameDuration)* symbols until its parent is found or all *n* channels are scanned. Upon the failure of orphan scan, a new parent is searched through passive scan as mentioned above. Thus, the total time spent for re-association is given by,

$$t_{802.15.4\_reasso} = n \times macResponseWaitTime + t_{802.15.4\_asso}. \tag{3.9}$$

In the proposed scheme, (3.5) also gives the reassociation duration since there is no orphan scan. Thus, as compared (3.5) with (3.9), DBC decreases the re-association time of a node by many folds.

3.5.5 Connectivity Time

To evaluate the device connectivity time with its coordinator, we consider a four-way intersection, which models the corridor of a hospital as shown in Figure 3.8. We assume that fixed coordinators (black nodes) have the same transmission range and are uniformly spaced. The figure shows a situation in which the mobile node M can take any direction at the intersection. In this kind of situation, choosing the furthest coordinator will give the longest connectivity provided that the mobile node is moving toward it. Let C$_1$ be remaining distance in meter before the mobile node M moves out of the transmission range of coordinator W and Z. Similarly, C_2 be the remaining distance before M moves out of the transmission range of Y. Suppose the mobile node moves towards coordinator Y at the speed of *v* m/s. As can be seen from the figure, the connectivity time for the coordinators W or Z are C_1/v and for the coordinator Y is C_2/v s. Since $C_2 > C_1$, choosing C_2 will give the longest connectivity time. Algorithm 1 also select coordinator Y as explained before. Furthermore, whatever is the direction node M chooses to take at the intersection, Algorithm 1 selects that coordinator which gives the longest connectivity time.

3.6 Numerical Example

Assuming network parameters of Table 3.1, we get *aBaseSuperFrameDuration* of 15.36 ms and *macResponseWaitTime* and $Asso_{msg}$ of 0.49 s [14]. Thus, using these values and above equations and assuming BO = 3, the association time for both IEEE 802.15.4 and DBC is shown in Table 3.4. From the values obtained in the table, we can conclude that DBC reduces the association time of IEEE 802.15.4 by significant amount and makes association duration independent of the number of available channels. We observed theoretically how many times DBC can decrease the PAN initialization and re/association time of the original IEEE 802.15.4 for all values of BO (BO = SO), and the obtained graph is shown in Figure 3.10. Note that the graphs show the performance gain is not just in terms of percentage but in term of number of factors.

Table 3.4: Total time spent on association.

	PAN Initialization		**Association**		**Re-Association**	
Channels	**802.15.4**	**DBC**	**802.15.4**	**DBC**	**802.15.4**	**DBC**
3	0.82 s	0.14 s	0.90 s	0.63 s	2.37 s	0.63 s
10	2.76 s	0.14 s	1.87 s	0.63 s	6.77 s	0.63 s
16	4.42 s	0.14 s	2.70 s	0.63 s	10.54 s	0.63 s

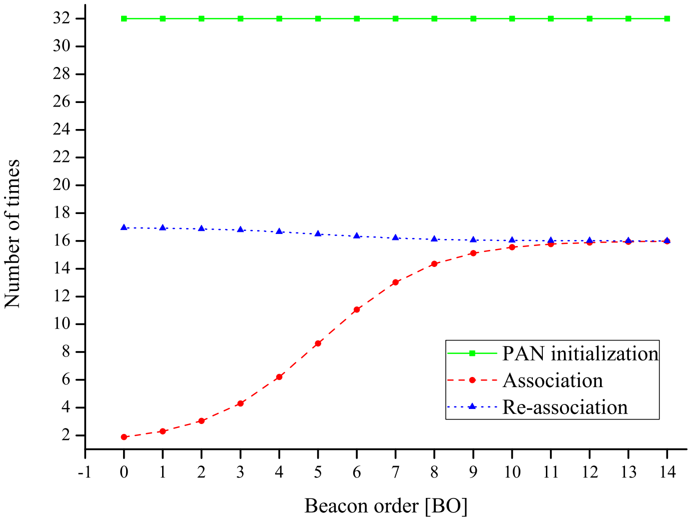
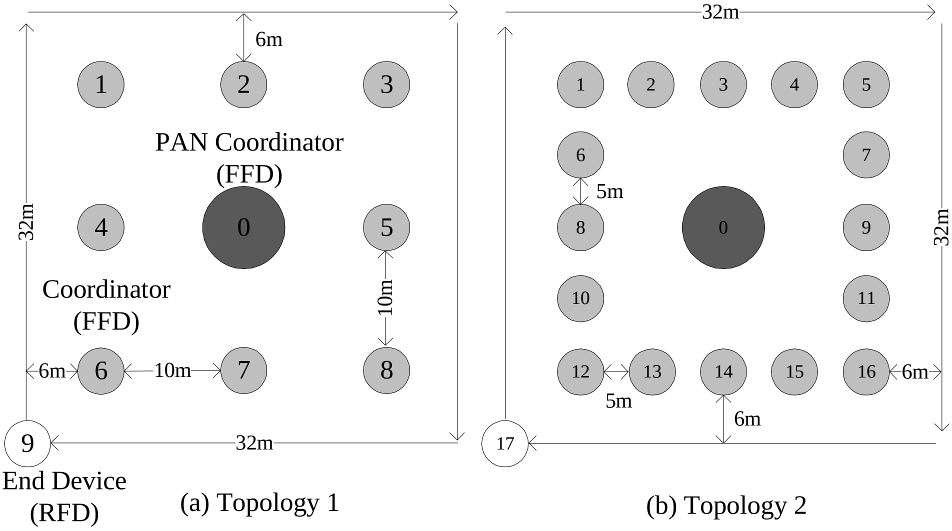


Figure 3.10: Number of times DBC outperforms the association duration of IEEE 802.15.4 in 2.4 GHz.

3.7 Performance Evaluation

For the simulation, nodes are deployed in a 50×50 m field with the PAN coordinator located at the center as shown in Figure 3.11, where arrow heads indicate the direction of movement of the mobile end device. Topology 1 and topology 2 are used to illustrate the performance of DBC in both thin and dense networks. Nodes are distanced by 10 m in topology 1 and by 5 m in topology 2. In both topologies, there is only one mobile node (node 9 and node 17 in each topology) and all others are coordinators. All coordinators broadcast beacon. Node performs reassociation if the beacon is lost more than *aMaxLost-Beacons* times. In the simulation time of 100 s, mobile node starts data transmission and moves at 110 s. The mobile node continuously moves while transmitting data to PAN coordinator. The simulation ends when the mobile node comes to its original position. In all the simulations, SO is the same as BO. The parameters of Table 3.1 are taken from CC2420 datasheet [56].



(a) Topology 1

(b) Topology 2

Figure 3.11: Network topologies used in the simulation.

3.7.1 Association Time

Figure 3.12 shows the time spent for PAN initialization and the node re/association in terms of various BOs obtained from numerical analysis and NS-2 simulations. In the NS-2 implementation of IEEE 802.15.4, the PAN coordinator performs only the active

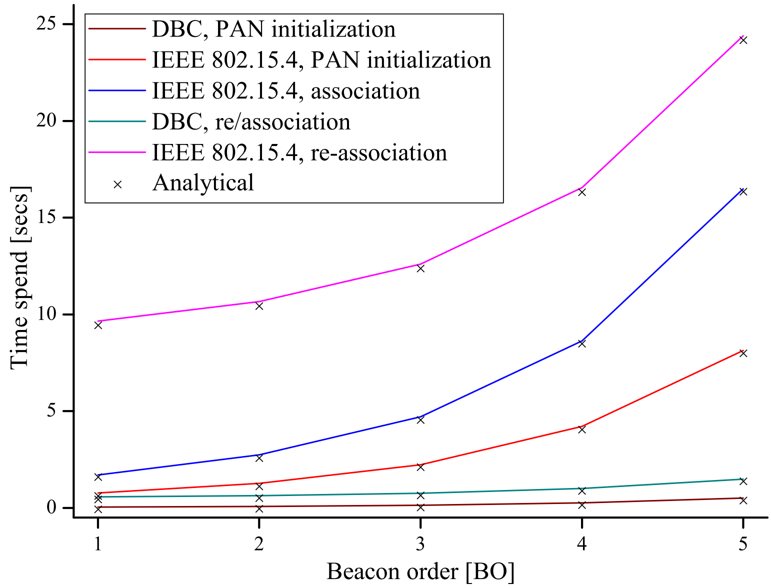


Figure 3.12: Total time spent for association at different beacon intervals.

scan for PAN initialization in the beacon-enabled mode. Thus, (3.2) can be updated to (3.10). In order to calculate the PAN initialization time, (3.1) is used to calculate t_{scan} for BO of 1 to 5. Then, (3.3) and (3.10) are used to calculate the PAN initialization times of IEEE 802.14.5 and DBC respectively for BO of 1 to 5. Similarly, for the assigned BO, nodes use BO + 1 internally to calculate t_{scan} except for the PAN coordinator. Thus, in order to calculate re/association time, (3.11) is used to calculate t_{scan} first. Then, (3.4) and (3.9) are used to calculate association and reassociation times respectively for IEEE 802.15.4. Since, DBC does not have separate orphan scan, (3.5) is used to calculate both association and reassociation times.

$$PAN_{802.15.4\_init} = n \times t_{scan}, \tag{3.10}$$

$$t_{scan} = aBaseSuperFrameDuration \times (2^{BO+1} + 1). \tag{3.11}$$

In all cases, the analytical results match well with the simulation results. As shown in the figure, the time required by DBC for re/association is much lower because only the BC is scanned for the association procedure. However, in the case of IEEE 802.15.4, it scans all available 16 channels spending significant amount of time and energy. At BO = 3, DBC is able to decrease the PAN initialization time by 15.92 times, the node association time by 6.19 times and the re-association time by 16.59 times, which is a great achievement

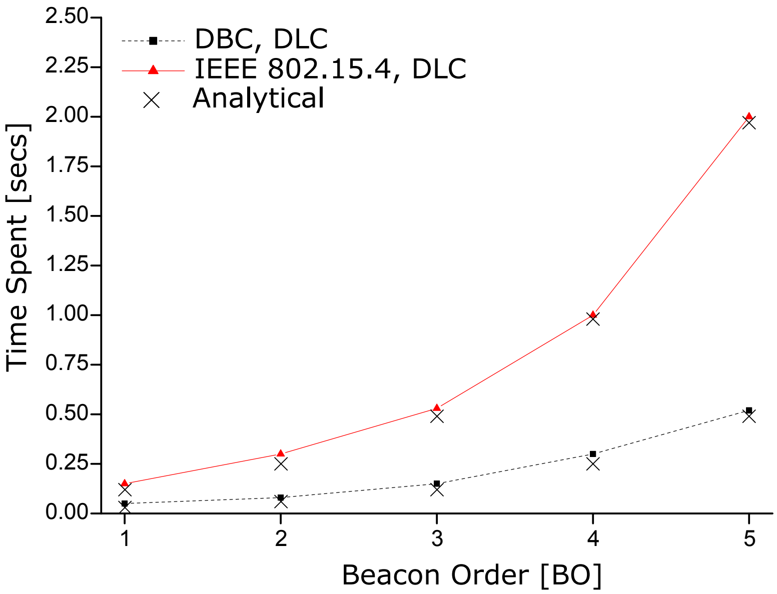


Figure 3.13: Total time spent for detection of lost of connectivity.

in itself. Similarly, the total time spent for DLC in the various values of BO is shown in Figure 3.13.

3.7.2 Association Success Rate and Packet Delivery Ratio

Success rate of association is calculated as the ratio of successful associations to the total number of possible associations. Topology 1 was used where there are total 8 associations possible before the mobile node comes to rest. BO was used same for all nodes. DBC increases the successful association rate of a mobile node by providing quick passive discovery of a coordinator. Percentage of successful associations at different BO(s) and node speeds are shown in Figure 3.14. We observed that even a slight mobility has a significant negative impact on association in the case of IEEE 802.15.4. At the human walking speed of 1.5 m/s, IEEE 802.15.4 had poor success rate of association even at the lower values of BO, and nodes were completely unable to associate at BO = 5. It is observed that the poor association ratio of IEEE 802.15.4 is due to the long duration required for reassociation (takes 12.5 s at BO=3). The time spent by the mobile node within the transmission range of a coordinator might not be enough to complete the association, which accounts for poor association rate. However, in the case of DBC (association takes 0.75 s at BO=3), association rate was 100% until BO = 4 and even at BO = 5, DBC could

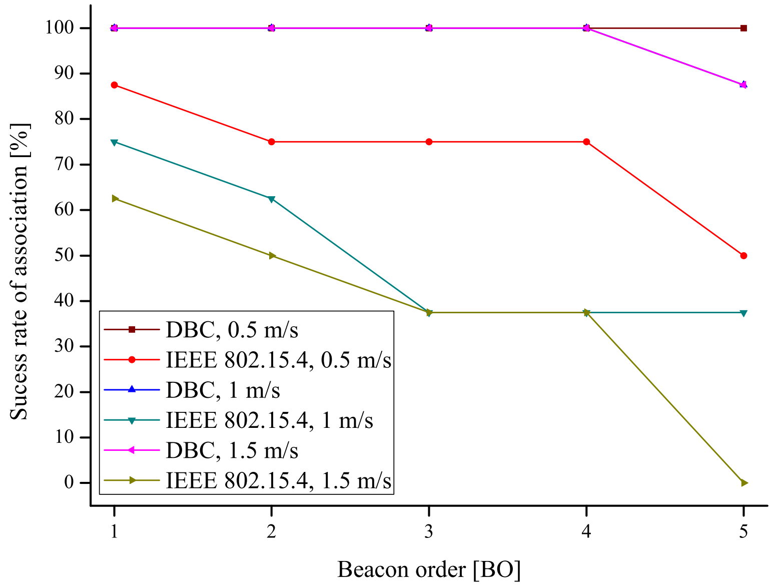


Figure 3.14: Association success rate at different beacon intervals using DBC and IEEE 802.15.4 at 0.5, 1, and 1.5 m/s.

successfully perform 7 associations out of 8. However, at node speed of 1.5 m/s, DBC was completely unable to associate at BO≥9. Figure 3.15 shows the throughput observed at the PAN coordinator in the packet delivery ratio (PDR). Due to IEEE 802.15.4 lengthy association time, most of the generated packets were dropped. As it can be seen from the graph, PDR was just 60% even at BO=1 and node speed of 0.5 m/s. However, the prompt re/association capability of DBC enabled mobile node to transmit most of the generated data to the coordinator increasing the overall throughput of the network. We can see in Figure 3.15 that PDR of DBC is much better than that of IEEE 802.15.4 for various node speeds, which corresponds to the better throughput achieved. At node speed of 1.5 m/s and BO = 5, the PDR of IEEE 802.15.4 was just 20% due to the fact that the mobile node 9 gets some opportunity to transmit data through node 6 before it starts to move and cannot associate then after. However, the PDR of DBC was of 82% for the same scenario.

3.7.3 Connectivity Time and Throughput

To illustrate how Algorithm 1 can enhance the connectivity time of a node, we used topology 2, where there are more than 1 coordinator to choose for association. In this

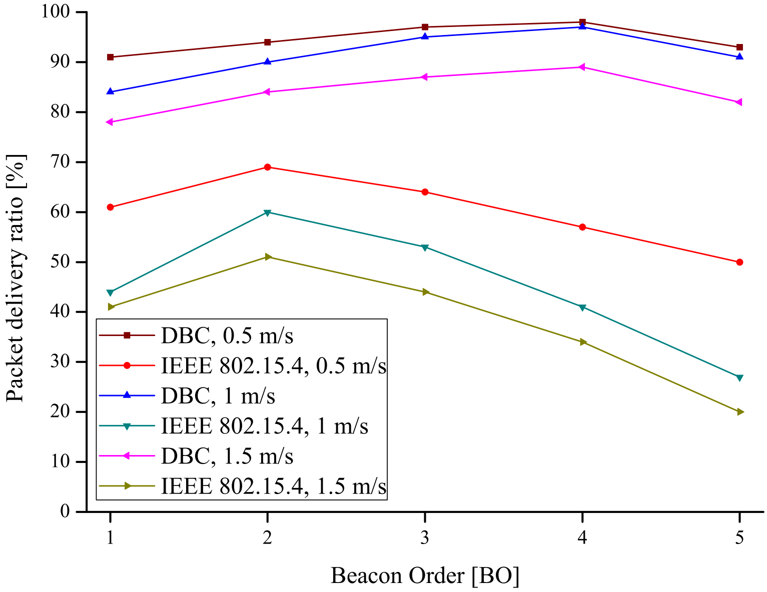


Figure 3.15: PDR at different beacon intervals using DBC and IEEE 802.15.4 at 0.5, 1, and 1.5 m/s.

Table 3.5: Performance enhanced by proper coordinator selection.

	Cell changes		**Connectivity (s)**		**PDR (%)**	
Protocols	**BO=3**	**BO=4**	**BO=3**	**BO=4**	**BO=3**	**BO=4**
IEEE 802.15.4	6	6	27	23	58	52
Enhanced 802.15.4	4	4	58	54	76	72
DBC	12	12	24	24	96	96
Enhanced DBC	8	8	37	36	98	98

simulation model, there were total 16 associations possible before the mobile node comes to rest. The fixed value of BO = 1 was assigned for all coordinators, whereas for the mobile node, it was varied. The performance enhancement after using Algorithm 1 in both IEEE 802.15.4 and DBC can be seen in Table 3.5. The table shows the total number of cell changes, average connectivity time, and the PDR. The average connectivity time is the average amount of time a node is connected with a coordinator before successfully getting associated with a new coordinator. The speed of the mobile node was of 0.5 m/s and the data rate of 2 Kbps. We use the term enhanced DBC and enhanced 802.15.4 to indicate that Algorithm 1 was implemented on them. The total cell changes were 6 and 12 for IEEE 802.15.4 and DBC respectively. As can be seen from Figure 3.12, at BO=3,

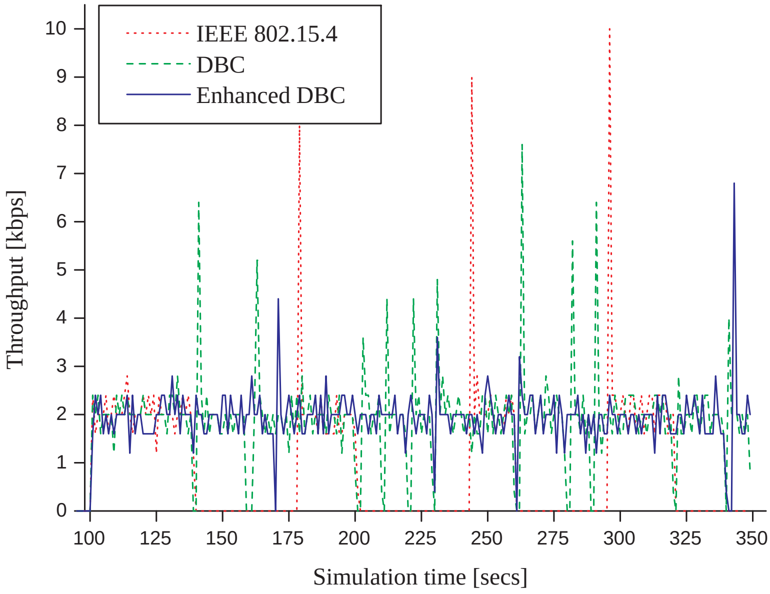


Figure 3.16: Throughput observed in the PAN coordinator at BO = 3, speed = 0.5 m/s, and data rate of 2 Kbps.

it takes 12.5 s and 0.75 s for IEEE 802.15.4 and DBC nodes respectively to reassociate with a new parent. Thus, even at the node speed of 0.5 m/s, the long reassociation time makes IEEE 802.15.4 to pass few adjacent coordinators before it successfully gets associated. However, nodes quickly get associated with a new coordinator and restart data transmission in DBC resulting for more cell changes and more PDR. However, frequent cell changes give less connectivity time in DBC as compared to IEEE 802.15.4. The connectivity time can be improved if the proper coordinator is selected as a new parent. As it can be seen in the table, the total cell change is reduced from 6 to 4 and 12 to 8 in IEEE 802.15.4 and DBC repressively after implementing Algorithm 1. Since the nodes choose the coordinator that gives the longest connectivity, we can see the decrease in cell changes along with the increase in PDR.

The effect of cell change on throughput observed at the PAN coordinator is shown in Figure 3.16. The mobile node is using beacon interval corresponding to BO = 3. The throughput of DBC drops while performing cell change because packets cannot be transmitted in the periods of passive discovery and association. However, nodes quickly get associated with a new coordinator and restart data transmission. Nodes can buffer packets. Therefore, buffered data are also transmitted after new association is completed, resulting into increased throughput immediately after the association. The performance of DBC was significantly improved by Algorithm 1 as can be seen in the figure. The total transferred rate was improved from 1554 kbps to 1900 kbps when Algorithm 1 was used. In some cell changes, throughput does not even drop to zero and regain its default value. However, in the case of IEEE 802.15.4, total transferred rate was just 539 kbps because nodes were unable to associate in every cell change resulting in poor performance.

3.8 Concluding Remarks

In this chapter, a new association scheme for IEEE 802.15.4 called DBC is presented that can decrease both time and energy required for the association. To achieve the above-mentioned advantages, the proposed DBC uses a dedicated channel for beacon transmission, preventing nodes from scanning all the available channels and looking for beacon. DBC scheme is further enhanced by two algorithms. The first algorithm (PRD) anticipates if the node is going to lose connectivity by analyzing the LQI history before it really happens. Thus, helps in early detection of future link breakage and handover decision. The second algorithm anticipates the nodes direction of movement with respect to the coordinator and selects that coordinator towards which the node is moving. Our analytical and simulation results demonstrated that our scheme is highly efficient in terms of both energy and time. With the implementation of our scheme, we give IEEE 802.15.4 the new ability to handle mobility. However, in this work, we assumed that there is no beacon collision. As future directions, we envision to study and provide a solution for beacon collision avoidance in a dense network.

Chapter 4

Wireless Local Area Networks

In this chapter, we provide a brief overview of wireless local area networks (WLANs) topology, WLAN protocol suite, some standardized WLAN MAC protocols and the standardization activities for WLAN that will facilitate the understanding of the contributions presented in this dissertation.

4.1 Overview of WLAN

WLAN is a flexible communication network which has emerged as a popular alternative for the wired network. IEEE 802.11 communication standard for WLAN has been designed and implemented to provide wireless connectivity for fixed, portable, and moving stations within a local area [57]. The IEEE 802.11 standard defines an over-the-air interface between a wireless station (STA) and a base (BS) station or access point (AP), or between two or more wireless stations.

WLANs are standardized by IEEE 802.11 Working Group (WG) which creates a set of standards for WLAN to operate in the unlicensed portion of the industrial, scientific, and medical (ISM) frequency band. Since the formation of the WG in 1990, there are series of IEEE 802.11 standards that have been produced, each with its own distinguishing characteristics, the popular amendments beng the IEEE 802.11 a, b, g, and n. Most of the commercial WLANs products available today are standardized with IEEE 802.11 standard and certified with Wi-Fi (for interpretability between WLANs products from different vendors, Wi-Fi Alliance have created certification program) [58]. The Wi-Fi technology is originally designed for human to human communication through wireless connection. Computers, smart phones and tablets are some of the most common devices using Wi-Fi technology. These devices can connect to the network, such as Internet via APs. The IEEE 802.11 specification only regulates the PHY and MAC layer of Wi-Fi technology, and the Wi-Fi network uses the same link layer protocol to connect with other local area networks, for example, Ethernet.

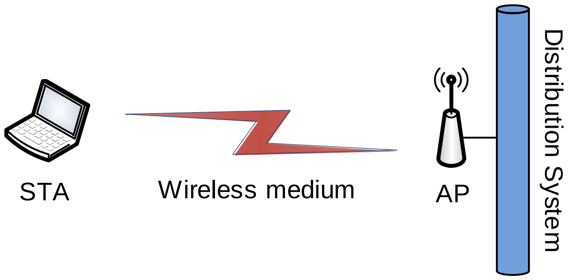


Figure 4.1: Basic components of 802.11 LANs.

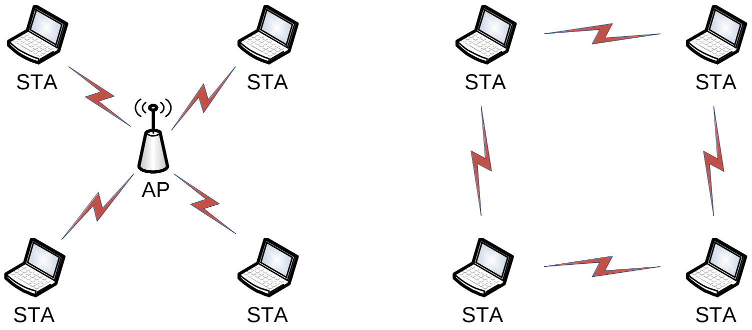
4.2 Basic Elements of 802.11 Networks

Wireless networks consist of various elements which enable data transfer. They also form the fundamental characteristics of the network. The basic components are being illustrated in Figure 4.1

- **Station (STA)**
  Stations in WLANs are addressable battery operated devices with wireless network interfaces (NIC) enabling them to connect to network. Portability is not a must though, because in some conditions wireless networking is being used to avoid excessive cabling [15]. Despite of being in the same network, stations may have different characteristics which distinguishes their unique functionalities. A network must have at least one STA to operate.

- **Access Point (AP)**
  A device that enables access of network to distribution system for its associated stations is called an access point. APs (as shown in Figure 4.1) are responsible to perform bridging functionalities between different types of mediums [15][33]. Having an AP in network, STAs are obliged to associate with and communicate through it. Therefore AP has the ability to control the network performance and data flow. All the messages generated by STAs to various destinations are sent via the AP.

- **Wireless Medium**
  Messages from different devices need to be transmitted over a medium and this is being met by various physical layers standards that have been developed [15]. They



(a) Basic service set (BSS).

(b) Independent basic service set (IBSS).

Figure 4.2: IEEE 802.11 network architecture.

can be categorized into radio frequency (RF) and infrared physical layer standards in IEEE 802.11 technologies whereas in the wired networks, twisted pairs, coaxial cables, and optical fibers are used.

WLANs have two basic modes of operation. WLAN has been popularly used either as infrastructure mode connection to the Internet or as an stand-alone ad hoc network.

- **The Basic Service Set (BSS)**
  BSS is the basic building block of an IEEE 802.11 network. In a typical BSS or infrastructure mode, stations can either connect itself to the Internet or to other stations only via AP. Furthermore, AP determines when a station can transmit or receive. Figure 4.2(a) shows a typical BSS.

- **The Independent Basic Service Set (IBSS)**
  IBSS enables two or more STAs to communicate directly and is usually established without preplanning, for as long as they are within the radio coverage of each other. This type of the AP-less ad hoc topology is often referred as independent basic service set (IBSS). Figure 4.2(b) shows an IBSS.

- **Distribution System (DS)**
  Interchanging data between several STAs connected to an AP and located in different wireless networks requires a type of backbone to enable APs to track and forward packets towards their final destination. This is made possible by implementing distribution system which is basically consists of a bridge and distribution

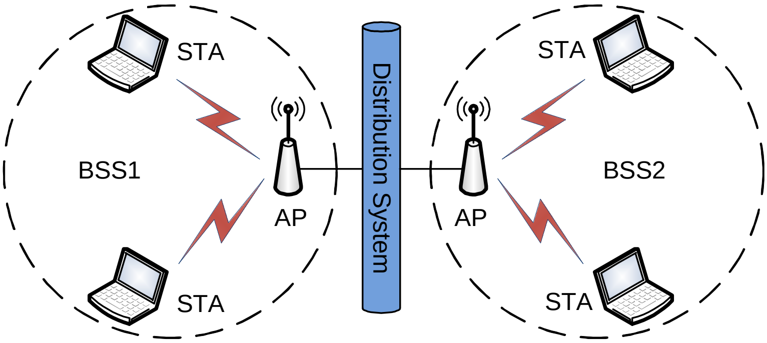


Figure 4.3: Distribution systems (DS).

system media. The DS is typically through a wired infrastructure (e.g. an Ethernet LAN). The DS or backbone can also be completely built wirelessly through the wireless distribution system (WDS).

- **Extended service set (ESS)**
  ESS is a set of one or more BSSS interconnected by a DS. The coverage of a WLAN can be increased using multiple BSSs interconnected via a DS as shown in Figure 4.3. Such multi BSS is known as extended service set (ESS). In ESS, the DS does not necessarily be a wired connection. In most practical ESSs, however, major portion of the DS is the wired ethernet [59]. All APs in the same ESS are set according to a common ESS Identification (ESSID) which identifies the network. A WDS can also be used for hard-to-wire locations or for extending the BSS's coverage area.

- **Relay**
  The coverage of AP can be extended by exchanging frames between STAs and an AP through relays. Also, relay improves reliability of data transmission in scenarios with obstructions. A Relay logically consists of two components: a relay station and a relay AP. A station associated with a relay AP operates almost in the same way as being associated with an actual AP. A basic schematic of a functioning network with relay entity is illustrated in Figure 4.4.

  Using relays, STAs are able to use higher data rates to transfer data and implement transmit opportunity (TXOP) sharing to access the channel. A TXOP is a period of time in which each STA can try to transmit as much packets as it can unless the

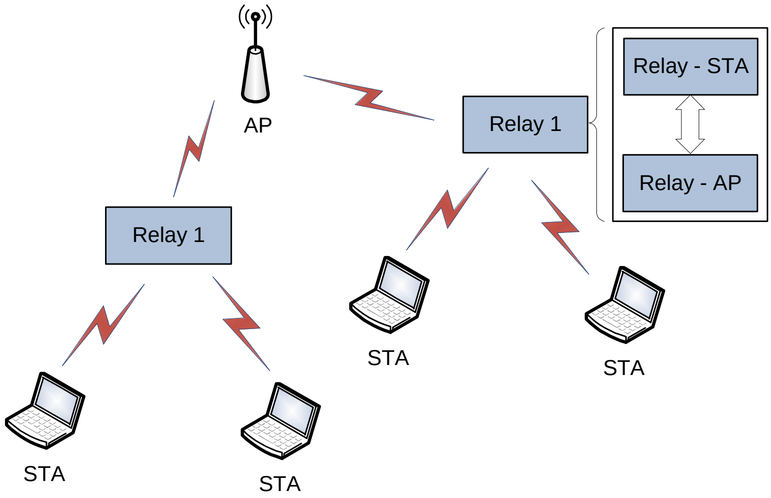


Figure 4.4: Structure of a relay entity in a network.

required time to transmit the whole packet exceeds this period. This improves the energy consumption by decreasing the required time a STA needs to be active [78].

4.3 WLANs Protocol Suite

Networking protocol suite is generally a set of communication protocols that describe rules and procedures for exchanging data among the network entities in any communication system. The implementation of such protocol suite is also known as a protocol stack. These two terms are often used interchangeably.

The protocol stack for WLANs is based on open system interconnection(ISO/OSI) reference model developed by international standard organization (ISO) [60]. The reference model is an idealized model with seven different layers (L1-L7), as shown in Figure 4.5. Each layer within a stack is responsible for a different facet of communications [61, 62]]. The lowest protocol always deals with physical interaction of the hardware. Every higher layer adds more features. User applications usually deal with the topmost layer.

In networking point of view, among seven layers, the four lower layers (L1-L4) are responsible for establishing efficient communication path. In particular, L4 and L3 are responsible for end to end flow control and routing functionalities, respectively, while the

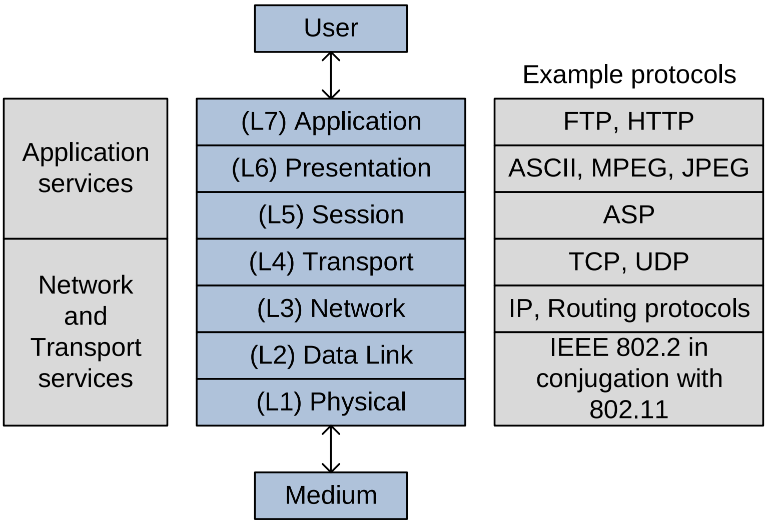


Figure 4.5: OSI reference model and some representative protocols.

L1 and L2 are responsible for establishing and managing the connection. The areas standardized by the IEEE 802.11 WG fall within the first and second layers of the networking protocol suite.

4.4 Services

The standard IEEE 802.11 defines the services that the DS and the STAs should implement. In this section, we briefly describe these services.

4.4.1 Distribution of Messages

Distribution of data messages between STAs is the primary service provided by an IEEE 802.11 network. It relies on the MAC protocol data unit (MSDU) delivery function present in all STAs.

The distribution of the message can be explained as follows: Suppose STA1 wants to send message to STA2 through DS. STA1 sends the message to its AP, the AP gives the message to the DS. It is the job of the DS to deliver this message to the appropriate destination. This operation may require the frame to be forwarded across different layer 2 technologies; the adaptation needed to deliver a frame to a non-802.11 network is carried out by the integration service, present in the APs. How the message is distributed within the DS is beyond the scope of the standard. However, IEEE 802.11 services are required to provide the DS with enough information to be able to forward the message towards the correct destination. This information is provided by the association related services.

4.4.2 Association Services

The STA first has to associate with an AP before it is allowed to send data frames via the AP. This operation provides a STA AP mapping that is used by the DS to accomplish its distribution service as described in the previous section. For this reason, a STA should be associated with no more than one AP, while an AP may be associated with many STAs at the same time.

In order to support BSS transition mobility, the DS also offers the reassociation service. AP mappings updated as the STAs move from BSS to BSS within an ESS. Both association and reassociation services are always initiated by the STA. The STA sends an association/reassociation request management frame to the selected AP, and the AP responds with an association/reassociation response.

Disassociation is used to terminate an existing association. As a consequence, the existing association information is removed. Unlike association and reassociation, a disassociation can be initiated either by STAs or by APs.

Scanning

When a STA in infrastructure mode is powered up, it needs to associate with an AP. The scanning process allows the STA to discover an AP, and hence the STA is able to choose the appropriate AP in range. AP broadcasts periodic beacon frame. Beacon frames contain information on the AP's capabilities and status that is useful for the association. STAs usually chose the best AP based on RSSI measurements of beacon frames. Scanning can be either active or passive. However, in the infrastructure based networks, passive scan is usually used for AP discovery.

Roaming

The DS has to support user inter-BSSS mobility within the ESS. When the STA perceives that the quality of the communication with its current AP degrades due to either its mobility or to the presence of interference, it tries to find a better AP candidate through a new scan. This is called roaming.

4.4.3 Security

Wired LANs assumes authentication is provided by the requirement of a physical connection to the media and confidentiality by the closed nature of the wire media. These assumptions are no longer valid for IEEE 802.11 WLANs due to their physically open medium nature. For this reason, the IEEE 802.11 standard defined two services in order to meet the aforementioned assumptions inherited from the wired LANs: authentication and data confidentiality at layer 2. This security is known as wired equivalent privacy (WEP).

Authentication is used to establish the STA's identities before the association process takes place. Two authentication methods are supported: Open System and Shared Key. Open system authentication simply consists of two communications. An authentication request by the client is followed by an authentication response from the AP containing a success or failure message. Shared key authentication relies on the fact that both stations taking part in the authentication process have the same shared key, which has been previously set on both STA and AP.

Data confidentiality protects the contents of messages. The current standard provides three cryptographic algorithms: WEP, temporal key integrity protocol (TKIP) and counter mode with Cipher-block chaining Message authentication code Protocol (CCMP). By default all messages are sent unprotected.

4.4.4 Spectrum Management

In order to satisfy requirements in different regulatory domains, specially for the operation of WLANs in the 5 GHz ISM band, a new amendment was released by 2003: the IEEE 802.11h [64]. Two services were specified: transmit power control (TPC) and dynamic frequency selection (DFS). The TPC service is intended to reduce interference with satellite devices, and DFS is used to avoid co-channel operation with radar systems as well as to ensure uniform utilization of available frequency channels.

4.5 Medium Access Control

IEEE 802.11 stations share a common wireless medium. The MAC Layer defines the rules that all STAs must follow in order to transmit to this medium. This is handled by using several access mechanisms. The IEEE 802.11 standards define two access methods: distributed coordination function (DCF) and point coordination function (PCF). Moreover, as of late 2005, the IEEE 802.11 task group ”E” released a new standard [63] that defines a set of quality of service (QoS) enhancements for the IEEE WLANs; it defines procedures for managing network QoS using classes of service. The extensions introduced inherit from the two previous access mechanisms (DCF and PCF). The new MAC protocol is called Hybrid Coordination Function (HCF).

Both PCF and HCF are provided through the services of DCF, which is the only mandatory access method. The fundamental access method used by the DCF based MAC is carrier sense multiple access with collision avoidance (CSMA/CA). This method is based on contention, whereas the PCF offers a contention free access. The three modes can be used alternately in time. The optional PCF mode is only allowed in the infrastructure BSS. In this case, the AP polls its associated STAs one after another by sending polling messages. Moreover, if the AP has data ready to be sent to a STA being polled, it can be included in the polling message. If the STA station has data to send to the AP, it is transmitted in the response message. In other words, PCF is a contention free protocol and enables stations to transmit data frames synchronously, with regular time delays between data frame transmissions. The contention free period takes priority over the regular DCF procedure. In this way, delay sensitive packets (e.g. voice or video) can have a higher priority. However, the 802.11 standard is vague in defining portions of the PCF protocol. As a result, APs implementing PCF are rare. Moreover, the Wi-Fi Alliance does not include PCF functionality in its interpretability standard. For all these reasons, in this section, we concentrate in the typical DCF mechanism and the carrier sense mechanism.

4.5.1 Carrier Sense mechanism

Physical and virtual carrier sense (CS) functions can be used to determine whether the wireless medium is idle or busy. Virtual carrier sense is also referred as the network allocation vector (NAV). The NAV maintains a prediction of future traffic on the medium

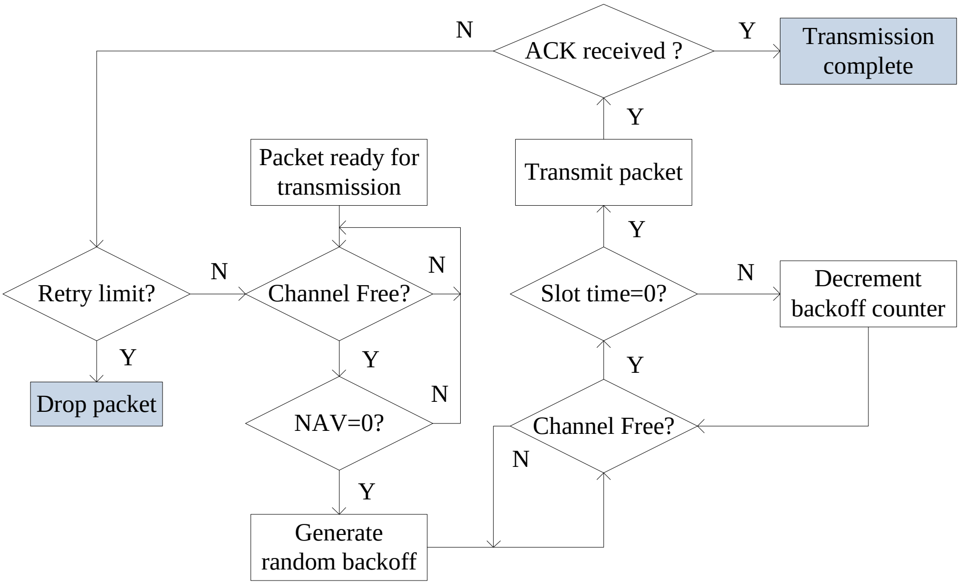


Figure 4.6: Channel access mechanism in DCF.

based on the duration information announced in some frames. The physical CS functions are provided by the PHY and logically depend on the PHY used. Basically, the physical layer provides a busy/idle medium recognition based on the detection of any energy above a given threshold.

4.5.2 Distributed Coordination Function

As mentioned before, the fundamental access method in IEEE 802.11 WLANs is a DCF based on CSMA/CA and a random backoff time following a busy medium condition. In addition, all unicast transmissions use positive Acknowledgment (ACK) frames. If no ACK is received, a retransmission is scheduled by the sender. Figure 4.6 shows the flow chart of channel access mechanism specified in DCF.

DCF is a contention-based MAC protocol. Each user in the network determines individually when to access the channel based on CSMA/CA protocol. DCF comes in two variants: the basic access mechanism and the Request-to-Send/Clear-to-Send (RTS/CTS) access mechanism. The principle to determine the transmission schedule is same regardless of the access mechanism.

The basic access mechanism requires each contending user to perform carrier sensing operation to determine the channel status. If the channel is found to be idle for a period of time equal to distributed inter frame space (DIFS), the user transmits its packet. If the channel is busy, STA waits until the channel becomes idle for DIFS period and then selects a random backoff time for which it should defer its transmission. The selected value is uniformly distributed in the interval [0, CW-1], where CW is the current contention window size. Once the channel has been found to be idle for DIFS, the backoff timer is decreased by one at the elapse of every idle slot until either the channel becomes busy again or the backoff timer reaches zero. If the timer has not reached zero and the channel becomes busy, the contending user freezes its timer. When the timer finally reaches zero, the STA transmits its packet. If receiver confirms the reception of the packet by sending a positive acknowledgement (ACK) after a short inter frame space (SIFS) time. If the sender does not receive the ACK within a certain timeout duration, it computes backoff time for retransmission according to binary exponential backoff (BEB) rules and follows the similar mechanism as in its failed transmission attempt until the packet is successfully transmitted or the maximum retransmission limit is reached [67].

The RTS/CTS based mechanism is an enhancement to the basic access mechanism. It reduces contention resolution overhead in terms of channel waste time due to packet collisions by reserving the channel using short RTS and CTS packets. A STA that has a packet to transmit follows the same process exactly as in the basic access mechanism, however, when the backoff counter reaches zero, it sends a special reservation packet called RTS packet. The intended receiver responds with CTS packet after SIFS interval. Other users who overhear RTS and CTS update their NAVs accordingly. Upon receiving the CTS, the source releases its data packets after SIFS interval. The rest of the other remaining process are identical to that of the basic access mechanism. Moreover, RTS/CTS help in resolving hidden node problems.

4.5.3 Enhanced Distributed Channel Access

Enhanced distributed channel access (EDCA) is a combination of DCF and PCF core functions, builds the foundation of the advanced HCF that includes the HCF controlled channel access (HCCA) method. An enhancement of HCF using contention-based channel access is going to be utilized in IEEE 802.11ah [78], called the enhanced distributed channel access, which has been applied in IEEE 802.11n [75] and IEEE 802.11ac [74]. EDCA classifies content into four access categories (ACs), including background, best effort, video, and voice traffic, with increasing access priority (background is the lowest

Table 4.1: List of several variants of IEEE 802.11 standard.

Series	Date	Description	Remark
802.11	1997	IEEE standard for WLAN MAC and PHY specifications	Initial standard
802.11a	1999	Higher Speed PHY extension in the 5 GHz band	54 Mbps, OFDM PHY
802.11b	1999	Higher Speed PHY extension in the 2.4 GHz band	11 Mbps, DSSS PHY
802.11g	2003	Further higher data rate extension in the 2.4 GHz	54 Mbps, OFDM PHY
802.11e	2005	MAC enhancements	Support for QoS
802.11n	2009	Enhancement for higher throughput	600 Mbps, MIMO PHY
802.11ac	2013	Very high throughput (below 6 GHz band)	Enhancements for greater than 1 Gbps throughput
802.11ah	Est. 2016	M2M communication (sub 1 GHz)	Support for IoT

access priority, voice is the highest access priority). The four access categories allow eight different content streams. For each of the ACs, an enhanced modification of DCF (EDCA) is used that allows transmission opportunity operations to enable QoS.

4.6 Standardization of WLAN

Several different WLAN technologies and standards have come and gone, for example, HiperLAN from European telecommunication standardization institute (ETSI) [62]. Today, there is one standard that is almost synonymous with the term WLAN, i.e IEEE 802.11 and its variants. Table 4.1 list several different IEEE standards that have already been approved or are in the process of being approved [66][78].

The first 802.11 standard was published in 1997. It covers the issues related to PHY and MAC layers of the networking protocol stack. It defines radio-based and Infrared (IR)-based Physical layer technologies that provide mechanisms for making wireless transmissions and receptions. Although IR-based PHY at 316-353 THz provides a basic data rate of 1 Mbps with an optional 2 Mbps mode, as in the case of the radio-based frequency hopping spread spectrum and direct sequence spread spectrum [65] at 2.4 GHz, the IR-based PHY implementations are not popular [66]. With a slight modification to

IEEE 802.3 Ethernet, IEEE 802.11 specifies a contention-based MAC protocol that operates according to a listen before-talk manner by employing CSMA/CA scheme. In addition to the contention-based MAC, it also specifies an optional contention-free polling-based MAC protocol which, however, is not adopted by WLAN product manufacturers. Those MAC protocols are comprehensively discussed in Section 4.5.

4.6.1 WLAN Amendments

The IEEE standard association updates the WLAN standard through amendments which define new features and concepts. Several representative amendments are listed to show the development of the WLAN technology as follows:

- **IEEE 802.11a:** The PHY layer technology, orthogonal frequency-division multiplexing, is first introduced to enhance the throughput. This amendment is now part of the standard. It defines an OFDM-based PHY offering 54 Mbps in the 5 GHz ISM band. This band offers much less potential for radio frequency interference than other PHYs (e.g., 802.11b and 802.11g) that utilize the 2.4 GHz band. On the other hand, a higher working frequency implies reduced coverage, since propagation loss is directly proportional to the frequency. It was ratified in 1999, although 802.11a-based products became available in late 2001.

- **IEEE 802.11e:** In 2005, an amendment IEEE 802.11e was introduced [63]. IEEE 802.11e as Quality of Service (QoS) extension of the former versions. Different new features in MAC layer were added by IEEE 802.11e. For example, service differentiation and prioritization scheme, TXOP sharing, and block acknowledgment.

- **IEEE 802.11n:** In 2009 a new amendment 11n was created, which employed MIMO techniques to raise the data rate significantly up to 600 Mbps [75]. This required a multiple antenna system in both the transmitter and the receiver. It works using one to four spatial streams with 40 MHz channel bandwidth. The 11n standard operates on both the 2.4 and the 5 GHz bands, but better performance is achieved on the 5 GHz band due to the availability of non-overlapping 40 MHz channels and less radio interference. It is backwards compatible with the 11a standard when operated in the Legacy format or the Mixed Mode format (11a and 11n).

But higher throughput can be achieved when operating in the Green Field format (11n only). The 11n also employed other techniques such as space-time block coding (STBC), and beam forming. The 11n products were available in the market before the completion of the standardization process.

- **IEEE 802.11ac:** The IEEE 802 Standards Committee created two new task groups 11ac and 11ad with the goal to enhance WLANs to reach the wired networks performance. The 11ac standard operates in the 5 GHz band (does not support the 2.4 GHz Band) [74]. It should theoretically enable a data rate of at least 1 Gbps. The new specifications are built on the 11n standard, by expanding the channel bandwidth to 80 MHz and optional 160 MHz channels, in addition to using MIMO with up to 8 spatial streams, higher order of modulation scheme (256-QAM) and other optional enhanced features like beam forming. It is approved in 2014.

- **IEEE 802.11ah:** IEEE 802.11ah is an amendment defined under the main IEEE 802.11 protocol to meet the needs for specific use cases in WLAN systems. IEEE 802.11ah TGah is working on new Wi-Fi standard to design a sub 1 GHz protocol which will allow up to 8191 devices attached to a single access point (AP) to get access for short-data transmissions [77]. IEEE 802.11ah wireless LAN standard group targets to support sensor networks, backhaul communications of sensor/meter data, and possibly M2M communications [78]. The standardization process is expected to complete by the end of 2016. IEEE 802.11ah is one of the main topics of this thesis and will be discussed more in upcoming sections.

4.7 Concluding Remarks

In this chapter, we have provided a brief overview of WLAN and some of its representative standardization activities. IEEE 802.11 has become de facto MAC for all commercially available WLAN products. In the subsequent chapters, we will highlight the most crucial problem of IEEE 802.11ah amendment, and present our innovative solutions to address the problem.

Chapter 5

IEEE 802.11AH

In this chapter, IEEE 802.11ah standard and its new features are discussed. In the latter sections, MAC and PHY layer architectures in the new 802.11ah amendment will be presented. The association problem in IEEE 802.11ah is then highlighted and the mathematical model for the association procedure is derived.

5.1 Introduction

The wide use of IEEE 802.11-based wireless networks in indoor and outdoor applications has crowded 2.4/5 GHz frequency bands. New technologies like smart grid applications, internet of things (IoT), and Machine-to-Machine(M2M) communication will further saturate the spectrum if same 2.4 GHz/5 GHz are used [77, 78].

IEEE 802.11ah is an amendment defined under the main IEEE 802.11 standard to meet the needs for specific use cases in WLAN systems. IEEE 802.11ah TGah is working on new Wi-Fi standard to design a sub 1 GHz protocol which will allow up to 8191 devices attached to a single access point (AP) to get access for short-data transmissions [77]. IEEE 802.11ah wireless LAN standard group targets to support sensor networks, backhaul communications of sensor/meter data, and possibly M2M communications [78].

5.2 Motivation for Development of 802.11ah

The market for WSN is increasing rapidly. However, the IEEE 802.11 standard was designed to be used by personal computers and not by WSN devices, this is what brings out the need for new amendments to fulfill new requirements.

IEEE 802.11ah standard in the M2M communications area was first introduced in 2010 and has been developed with very specific intentions: to deliver long range transmission above 1 Km and with data rates above 100 Kbps, but also to support a large number of nodes in the network while maintaining its operability with a very low power consumption policy.

IEEE 802.11ah will offer a very cost effective solution to WSN applications such as smart metering, plan automation, surveillance and also enabling operation in environment demanding scenarios such as natural or nuclear disasters. IEEE 802.11ah TGah wants to achieve them with the minimum changes respect to the widely adopted IEEE 802.11 standard. In fact, the proposed PHY and MAC layers are based on the IEEE 802.11ac amendment, trying to achieve an efficiency gain by reducing some control/management frames and the MAC header length. The benefits obtained by the standardization of sub-1GHz WLANs are many; very simple to use in outdoor environments in addition to excellent propagations characteristics at low frequencies in different levels of installation scenarios on ISM bands.

5.3 Use Cases

In this section, we analyze the potential use of the IEEE 802.11ah amendment for several scenarios. The task group for IEEE 802.11ah have classified the use cases under three main categories as sensors and meters, backhaul sensor and meter data, and extended range Wi-Fi [68, 71]. In the following sections, these use cases will be discussed to help understand the advantages of employing IEEE 802.11ah in various scenarios.

5.3.1 Sensor Networks

IEEE 802.11ah includes sensor networks as one of three adopted use cases. Sensors can be deployed to monitor physical or environmental conditions and to cooperatively pass their data through the network to a main location. Wireless controlled power distribution systems are also considered. Due to the increased penetration through walls at lower frequencies, a higher number of sensors can be covered in one-hop fashion. Considering tons of applicable areas for these kind of sensors and due to the elevated possibility of high density deployment of sensors, IEEE 802.11ah is going to be highly used among these sensor devices for communication purposes [68]. Most of the adopted use cases consider sensing applications can be [70],

- smart meters (gas, water and power consumption)
- smart grids
- environmental monitoring

- automation of industrial process
- health-care

5.3.2 Backhaul Networks for Sensors

Backhaul networks for sensors are the second use case adopted by the TGah. In a typical sensor network, IEEE 802.11ah can provide a wireless backhaul link to accommodate the aggregated traffic generated by the sensors and forward to remote control and data base [68, 72]. One of the main advantages of the IEEE 802.11ah is the long range coverage which allows simple networks design to link sub-1 GHz AP's together, for example as wireless mesh networks.

High speed and high bandwidth technologies such as high speed packet access (HSPA) and long term evolution (LTE) already exists. But simply increasing the speed may not always be economically effective, and the bandwidth provided by 4G may not be sufficient [73]. Because of this growing market the TGah has adopted this use case considering the technical requirements for a Wi-Fi based cellular traffic off-loading in this standard. Although other amendments of the IEEE 802.11 such as the IEEE 802.11n have been pointed to be a better solution to improve the off-loading because of its higher bandwidth characteristics, the long range coverage and low power consumption of the IEEE 802.11ah are key features to fulfill battery operated mobile devices requirements, and this is the main reason for this amendment to be chosen by the TGah.

5.3.3 Extended Wi-Fi Range

The third adopted use case considers technical requirements for a Wi-Fi based cellular traffic off-loading in IEEE 802.11ah. Both high throughput and long transmission ranges make 802.11ah attractive for extending hotspot range and for traffic offloading in mobile networks, which is a significant issue for operators and vendors because of mobile traffic explosion. Users are expecting to have access to high-speed internet connection anywhere and anytime. The caveat is that the performance should be at least comparable with the one from the cellular network.

5.4 PHY Layer

The PHY design of the IEEE 802.11ah is based on the PHY design of the IEEE 802.11ac which operates a 20 MHz, 40 MHz, 80 MHz and 160 MHz channel bandwidths [74]. IEEE 802.11ah's PHY is a ten times down-clocked version of IEEE 802.11ac, and operates in the 2 MHz, 4 MHz, 8 MHz and 16 MHz channel bandwidths, and an additional 1 MHz channel which has been intended to improve coverage. Multiple Input Multiple Output Orthogonal Frequency Division Multiplexing (MIMO-OFDM) multicarrier wireless system composed of a total of 64 tones will be used, which has been borrowed from the IEEE 802.11a to operate on the sub-1 GHz ISM bands.

5.4.1 Channelization

IEEE 802.11ah has defined the channelization based on the respective available wireless spectra in various countries. For example, for South Korea the ISM bands defined for its operation start 917.5 MHz ending at 923.5 MHz, a total of 6 MHz band is available. The 0.5 MHz offset is to avoid interference with wireless legacy systems at lower frequencies. Similarly, for Europe a total of 5 MHz band has been assigned, from 863 MHz to 868 MHz, assuming 600 KHz as a guard band. However, the United Stated of America is the country with the most bands available, a total of 26 MHz band has been adopted starting at 902 MHz and ending at 928 MHz, making it the only country able to operate with a bandwidth of 16 MHz.

5.4.2 Transmission Modes

Being available in all channelization across countries, the common channels adopted by the IEEE 802.11ah are 1 MHz and 2 MHz. Therefore, STAs and are obliged to support the reception in 1 MHz and 2 MHz channels. Similarly, there are two categories for PHY transmission modes: 1 MHz and greater or equal to 2 MHz. In the first case, the PHY layer designe is based on a ten times down-clocked version of IEEE 802.11ac; i.e. the PHY layer uses an OFDM waveform with a total of 64 tones/sub-carriers, which are spaced by 31.25 kHz. The supported modulations are BPSK, QPSK and 16 to 256 QAM. It also supports multi user MIMO and single user beam forming. For the second case, the tone spacing is maintained, but the waveform is formed with 32 tones, instead of 64 [77].

5.5 MAC Layer

MAC is an important technique that enables the successful operation of the network. In 802.11ah MAC layer design, some features are enhanced compared with the existing 802.11 MAC, including improvements related with support of large number of stations, power saving, improvised medium access mechanisms and throughput enhancements. The enhancements are presented in this sub chapter.

5.5.1 General MAC Improvements

The length of some fields in management frames in IEEE 802.11 standard must be increased to allow association of a large number of nodes. Once successfully associated with an AP, association identifier (AID) is assigned to a node. AID uniquely identifies the node in a network. AID is 14 bits long and ranges from 0 to 16383. However, all the values other than 1-2007 are reserved. Therefore, an AP can provide service for 2008 devices only. Another limitation is imposed by the traffic indication map (TIM) bitmap. TIM is a map that indicates the maps of STAs that the AP has buffered packets to be sent to and is used by power management schemes. The TIM field length is limited to 2008 bits.

As the IEEE 802.11ah is aimed to support more than 8000 STAs, the TGah has extended the range of AID numbers that can be used by a STA operating in IEEE 802.11ah networks to 0-8191. Similarly, the length for TIM has also increased to 8192 bits to be equally capable of supporting very high number of STAs.

5.5.2 Frame Shortening

One of the typical main problems in sensor networks is the overhead in transmissions. The overheads reduce the network throughput as well as the power efficiency. However, the use of aggregation and other IEEE 802.11 solutions are not applicable to many use cases. Therefore, in this section, the new ways to approach these issues by the work group for IEEE 802.11ah is discussed.

- **Short Headers**

  Header bits are always a part of sent frames and are highly valuable to induce information for routing, channel utilization and several other parameters.

Frame Control	Duration / ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	HT Control	Frame Body	FCS

Figure 5.1: The frame formate for IEEE 802.11.

Frame Control	Address 1	Address 2	Sequence Control	Address 3	Address 4	Frame Body	FCS

Figure 5.2: The frame formate for IEEE 802.11ah.

TGah has come up with the idea of defining a new short headers for data, management and control frames which is distinguishable from the legacy one by an indication in frame control field of both formats. A significant change that is imposed to frames by using short version, is that they do have the duration/ID field which is necessary for NAV operation in legacy IEEE 802.11 networks as shown in Figure 5.2. Therefore, the task group for IEEE 802.11ah are obliged to develop a new mechanism for channel access. The novel channel access mechanism, called response indication deferral (RID) will be discussed further in Section 5.5.3.

Frames using short MAC header can transmit frames between an AP and a STA directly using two address fields, while transmissions originated from a STA to another STA in the same BSS must use three address field because they use an AP to forward frames. Moreover, if the transmission is required to be done using multi-hop network, the use of four address field are necessary for transmitter, receiver, source and destination addresses.

- **NDP MAC Frames**

  In a network, apart from data, there exist several different types of frames for management and control purposes like CTS and ACK. Because these frames are mainly used for acknowledgement and do not carry a lot of useful information, aside form duration field used for setting NAV, TGah decided to take advantage from previously developed frames in IEEE 802.11ac networks called null data packet (NDP) and extend a new frame type called NDP MAC frames for IEEE 802.11ah networks.

  NDP frames has been used in IEEE 802.11ac as short frames for channel calibration required for beamforming. This process is done by scrutinizing the received

PHY header so the NDP frames does not need to carry any payload. TGah tends to use this frames and add just the sufficient amount of data to carry out the functionalities of the control frames.

- **Short Beacons**

  Beacons are another overhead in a networks. Beacons are sent periodically, and containing relatively large amount of information. They must be sent in the most robust modulation scheme to assure that they are received well even by the edge members. Since IEEE 802.11ah operates at lowest data rate that is a little bit more than 0.5 Mbps, transmission of even a few bytes in this mode will take significant amount of channel time and power in both transmitter and receiver.

  IEEE 802.11ah task group has developed two types of beacons, namely short and full. Short beacons are sent more frequently and contains the very essential information only. In contrast, full beacons are sent less frequently, but contain all the information which in the case of no change in network are unessential.

  Redundant information are omitted form the short beacons. When a STA is required to be notified about a change in the network, the AP changes a field in short beacon field to notify the STA about the update. Once the full beacon is received, STA can go to doze state for further power saving.

5.5.3 Channel Access

IEEE 802.11ah task group has developed several approaches for minimizing the drawback in legacy wireless networks in accessing the channel when very high number of devices are present. The main objective is to decrease the channel's wasted time by avoiding unnecessary collisions, interframe spaces, ACKs and overlapping transmission by STAs transmitting simultaneously.

Virtual Carrier Sensing

The legacy IEEE 802.11 standard uses virtual carrier sensing mechanism called network allocation vector (NAV) beside the physical carrier sensing to avoid collisions while transmissions. In other words, NAV is responsible for blocking all neighboring STAs in the receiver's area to access the channel during the period the STA is communicating.

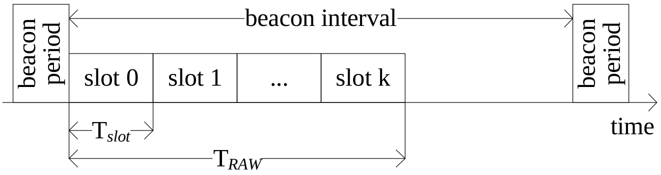


Figure 5.3: The superframe structure of IEEE 802.11ah.

As described previously, the NAV is disabled when using short frames. Thus, TGah developed a new virtual carrier sensing mechanism called RID.

Both RID and NAV are countdown timers. But, there are some differences which make these two CS mechanism usable for their respective standard. The main difference is that the NAV can be set after the complete and correct reception of the whole frame while RID can be set just right after the PHY header is received. This makes NAV very highly accuracy about the precise timings of the channel state changes, while RID tries estimating the duration of channel events based on the type of response with 2 bits length stored in response indication field in PHY header.

RID defines four types of responses named normal response, NDP response, no response and long response to distinguish different channel states. Information about these responses are included in PHY header which impose some advantages and disadvantages. Using no response, RID does not let a STA to waste channel time by waiting a very long time for an expected ACK when a collision may have occurred and an EIFS must be wasted using legacy DCF. In contrary, if a frame requires the use of Long Response, the channel is reserved for that STA and becomes busy for all others. It may happen that the STA needs less time than reserved for its transmission and it can use response indication field to inform the other STAs to update their RID and use the excess channel time. Here, the nodes that are hidden to the receiver can not get the updated information and their channel resource is wasted.

Restricted Access Window (RAW)

Figure 5.3 shows the superframe structure of IEEE 802.11ah. In order to provide the service to large number of stations, IEEE 802.11ah introduces RAW. The RAW mechanism enables fair channel access among the large number of stations. Right after the beacon period, there could be hundreds or thousands of stations trying to access the medium for data transmission. RAW mechanism restricts channel access to a small number of stations at a given time and distributes their access attempts over a much longer period of time. In this mechanism, the AP allocates a medium access period in the BI, called RAW, which is divided into several time slots of T_{slot} duration each as shown in Figure 5.3. The AP may assign a time slot inside the RAW to a group of stations during which only those certain stations are allowed to contend for medium access. RAW allocation information is broadcast in a beacon to notify whether a station is allowed to use RAW interval or not. The allocation information in the beacon also includes the start time and the duration of the RAW (T_{RAW}). If a station is allowed to access the channel within the RAW, it may contend for medium access at the start of its assigned time slot. However, stations should stop attempting to access the medium as soon as their assigned time slot is finished. It should be noted that there may be some stations, which are not allowed to use the RAW. During the channel time assigned to others, a station can go to sleep to save energy.

There is a parameter called cross slot boundary encapsulated in the beacon that defines the behavior of the RAW [79]. If the cross slot boundary is allowed, uplink transmissions can cross boundary of the allocated time slot. However, if it is not allowed, then the stations try to access the medium only if the remaining time in the allocated slot boundary is enough to complete the transmission. Otherwise, the station will not initiate a transmission even though the remaining slot duration is greater than zero.

Sectorization

One of the main mechanisms introduced to handle the complications in channel access is referred as sectorization. In simple context, it is the act of partitioning of the AP coverage area into sectors so that each of the sectors contain a subset of associated STAs. This can be done by using a set of omni-directional antennas or synthesized antenna beams in AP to perform the transmission and reception. The entire coverage area of an AP is assumed to be covered and every associated STA must belong to a sector. IEEE 802.11ah defines two types of sectorization, namely group sectorization and TXOP-based sectorization.

5.5.4 Power Saving

Power management and consumption is an important issue in wireless network. The main idea of numerous power management mechanisms used in IEEE 802.11 networks is based on alternating between awake and doze states. The communication is only possible in a awake state. By switching to the doze state the STA turns off its radio module and can not interact with network in anyway. The STA must inform its associated AP prior to switching states. The STA wakes up periodically for communication.

IEEE 802.11 has many power management features to enhance IEEE 802.11ah too but their efficiency is not high. Therefore, new procedures have been developed based on them to meet the requirements of IEEE 802.11ah network. Some of the newly developed approaches are discussed here.

Insufficient Doze Duration

In 802.11 networks, the duration of the doze state transmitted in 16 bits field is limited by max idle period, after which the AP de-associates the doze STA. The value of max idle period is 18.64 h [70]. However, some use cases require doze state duration much longer than 18h. To avoid being de-associated, they would need to send keep-alive messages, wasting energy. To reduce energy consumption, TGah develops 2 solutions modifying max idle period usage.

The first one is the use of two the most significant bits of the max idle period field as a scaling factor. Values 00, 01, 10, 11 represent scaling factors 1, 10, 1000, 10,000, respectively. This way maximal value of max idle period is 2500 times greater.

The second one allows the AP to set different max idle period for various stations. Moreover, a station can request specific max idle period in its association request.

Station Classification

Wireless network can have several devices in them. It is possible that they differ in requirements regarding QoS, packet size, duty cycle and etc. For addressing different STAs with their requirements, TGah has developed two different types of STAs named sensor and offloading stations. The idea is to tag stations, in order to be able to implement networks based on each group’s requirements.

Sensor stations are designed with limited power supply and may have limited capabilities. The limitations can be in their transmission and reception frequency and packet size. They may frequently go to doze mode and stay there for power saving.

On contrary, offloading stations require high traffic transmission such as video streaming. Laptops, wireless gadgets and cameras are classified as this type. Due to the high throughput required by the STAs of this kind, the number of devices associated to an AP can not be as high as the sensor type.

TGah specifies three different modes of BSS operation: sensor only BSS, non-sensor only BSS and mixed mode (contains both). The frequency to wake up is higher in sensor mode compared to non-sensor and mixed mode. Different types of BSSs can be separated spatially or can be assigned different channels to minimize the effect of sensors of two types on each other.

Target Wake Time (TWT)

This feature aims to efficiently put stations in doze mode for power saving. Here, the STAs are given a target wake time for their first interval start, minimum TWT, TWT interval, direction of packet flow for the first transmission, flow ID, channels on which the stations can transmit. The TWT are of types: implicit or explicit.

Since the protection for TWT separately increases overhead, TGah suggest the grouping of of TWT time meaning that to assign TWT grouped side by side in time. By this mechanism, the AP is allowed to create TWT groups and inform STAs about them. The STAs, then send requests to join to a TWT group and the AP will assign it to the appropriate group.

5.6 Association in IEEE 802.11ah

Figure 5.4 shows the association process. If a station is eligible for the association, it starts the association process. The association procedure starts by sending the authentication request to AP. After the station is authenticated, AP responses with authentication response frame and is acknowledged by the station. Once the station is authenticated, it will send an association request to the AP. The association request contains chosen encryption types if required and other compatible 802.11 capabilities. If the elements in the association request match with the capabilities of the AP, the AP will create an association ID for the station and respond with an association response message granting network access to the station. The association response is again acknowledged by the station. Once a station is associated with AP, it can start communication.

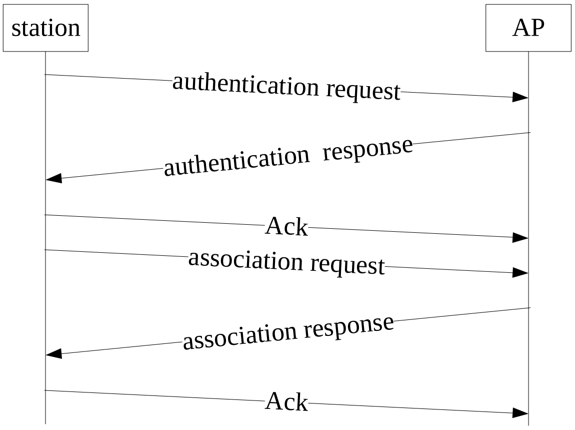


Figure 5.4: Authentication/association procedure in IEEE 802.11ah.

5.6.1 Authentication Control Mechanism (ACM)

One AP is responsible for handling 8000 stations. Heavy contentions is inevitable if all stations try for channel access simultaneously. However, IEEE 802.11ah has developed an authentication control mechanism (ACM) for limiting the contention. This feature aims to control the authentication process for large number of nodes by employing two methods namely centralized and distributed control mechanisms. In the first one the AP includes a threshold in each beacon that is determined by some rules in the implementation. Each STA, then generates a random number and the STAs that have their random values less than that threshold are eligible to authenticate in that beacon interval. The latter one is based on truncated exponential backoff. Each time there is an attempt for authentication, every STA generates two random numbers based on the number of whole slots in beacon interval and transmission interval. Centralized authentication control is studie discussed more below.

5.6.2 Centralized Authentication Control

In every beacon period, authentication control threshold (ACT) is selected according to some implementation dependent rules and is broadcasted in the beacon frame [78]. The AP may change this ACT dynamically. Similarly, in every beacon period, a station shall generate an authentication control number randomly from the interval [0, L]. Having received a beacon, the station tries to associate with the AP only if its authentication control number is less than the received ACT. Otherwise, it shall postpone association till the next BI.

5.7 Problem Statement

In IEEE 802.11ah network, thousands of stations are connected with a single AP. As the number of station increases, the network throughput and delay performances can be rapidly deteriorated due to the serious channel contention. While the contention becomes serious as the number of stations increases, one method to solve the problem is to limit the number of contending stations at a time by grouping. Same idea is adopted by IEEE 802.11ah. IEEE 802.11ah introduces a new mechanism called RAW. One or more RAWs can be allocated in a beacon interval (BI) and only designated stations can access the channel in a RAW using the prevalent distributed coordination function (DCF) or enhanced distributed channel access (EDCA) [15, 79].

IEEE 802.11ah is mainly designed for low data traffic, thus, even the large number of stations can be fairly serviced by RAW. RAW performs only after the stations are associated. Thus, even though RAW limits the number of associated stations contending for the channel, it cannot improve channel usage efficiency at the stage of network initialization. Network can reset due to various reasons, such as power failure, AP reboot, system crash, and so on. Once AP restarts, stations try to associate. (ACM) is used for limiting the contention during network initialization. However, it takes significantly long duration for all the stations to get associated with an AP.

5.7.1 Co-existence of Data and Association Frames

As mentioned above, during association ACM is used, whereas RAW is used for data communication. Even though both ACM and RAW are used to limit the number of contending stations, they come into picture at different network stages. However, they may co-exist during network initialization stage. During network initialization, there will be two types of stations, one using ACM and another using RAW. However, how these two types of stations co-exist and how to manage the traffic from these two types of stations is unanswered in the draft of 802.11ah. An open issue is how to avoid collisions of authentication requests and traffic of already associated stations. So, these questions can be topics for future research. Therefore, during the network initialization, how to avoid collisions of authentication requests and traffic of already associated stations is a big question [70].

To demonstrate our point, an analytical model of the authentication/association process is developed to analyze and evaluate the performance of IEEE 802.11ah networks. Since it may take up to several minutes for all stations to get associated, the obtained results clearly indicate that the traffic from stations contending for network association can collide with the traffic from stations contending for data transmission. Therefore, a new method to handle data and association traffic is necessary [82].

The main contribution of this chapter is to emphasize the need of a new method to handle data and association traffic simultaneously in IEEE 802.11ah. This further strengthens the prospects of IEEE 802.11ah as one of the key enabling technologies in massive M2M communication deployments and associated IoT applications in the future.

5.8 Numerical Analysis

In this section, we derive the analytical model of the association procedure in IEEE 802.11ah.

5.8.1 System Model and Analysis

We consider a network consisting of N stations and an AP at the center. The stations are completely connected in the network, i.e., there is no hidden terminal in the network. Moreover, an ideal channel condition is assumed, wherein there are no communication errors and there is no capture effect. Initially, stations are unassociated with the AP. A batch of g stations participate in the association process at a time. Once all g stations get associated, the next batch of g stations start association process. Once associated, stations remain idle.

5.8.2 Analysis

In order to model the association process, we observe it from the viewpoint of queuing theory. Figure 5.5 illustrates the proposed queuing network model (4-stage tandem network). Each station has to pass through four stages before it gets successfully associated. Each stage is represented by a queue. At a time, g stations enter the queue system and no new station is allowed to enter the system until all g stations are out of queue system. At each queue, the customers stay until it is served and travel to the next queue. Each successful transmission moves a customer into the next stage. Let d_k and μ_k represent

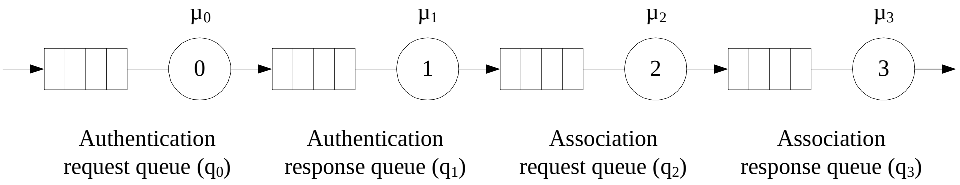

μ0
μ1
μ2
μ3
0
1
2
3
Authentication request queue (q0)
Authentication response queue (q1)
Association request queue (q2)
Association response queue (q3)

Figure 5.5: The Queuing network model for association in IEEE 802.11ah.

the average delay and average service time of queue q_k, respectively. By Little's theorem, the average number of stations in queue *k*, n_k, is

$$n_k = \frac{d_k}{\mu_k}. \tag{5.1}$$

The total number of stations in the system gradually decreases until all *g* station are out of the system. Therefore, the average number of station in a queue, n_k is *g/2*. Now, the average waiting time in a queue can be calculated, once the average service time is known.

The transmission behavior of the devices in IEEE 802.11ah can be approximated by that of IEEE 802.11 stations [84]. The group of *g* stations contend for access to the network. The stations access the channel using distributed coordination function. That is, station senses the channel if it is idle for one DIFS. Then, the station chooses a random backoff time uniformly distributed from [0, CW], where CW is the backoff window size. The CW is doubled in the range from CW$_{min}$ to CW$_{max}$, whenever there is a collision. Also, it can reset to CW$_{min}$, whenever a frame is acknowledged by the receiver or dropped. When a device succeeds in channel access, it sends a corresponding association frame. Except for the ACK frame, other frames are transmitted using DCF. Therefore, the probability τ that a station transmits a frame in a randomly chosen slot time is expressed as

$$\tau = \frac{2(1-2p)}{(1-2p)(CW_{min}+1)+pCW_{min}(1-(2p)^m)}, \tag{5.2}$$

where *m* is the maximum backoff stage and *p* is the conditional collision probability that a transmitted frame encounters a collision. The *p* is given by

$$p = 1-(1-\tau)^{g/2-1}, \tag{5.3}$$

where *g/2* is the mean number of stations [86][84]. Equations (5.2) and (5.3) represent a non-linear system with two unknown τ and *p*, which can be solved using numerical methods and has a unique solution. The discrete-time markov chain of our model is same with the markov chain employed in [85]. For the complete derivations of τ and *p*, please refer to [85]. Similarly, same model is used in [84, 86, 87, 89] and many more for the analysis of DCF in IEEE 802.11ah.

The probability P_{tr} that there is at least one transmission in the considered slot time and the probability P_s that a channel access attempt is successful is derived as

$$P_{tr} = 1 - (1-\tau)^{g/2}, \; P_s = \frac{g\tau(1-\tau)^{g/2-1}}{2P_{tr}}. \tag{5.4}$$

The average amount of time, *E[slot]*, spent on the channel for successful transmission is equal to

$$E[slot] = \frac{(1-P_{tr})}{P_{tr}P_s}\sigma + T_s + \frac{(1-P_s)}{P_s}T_c, \tag{5.5}$$

where σ is the backoff slot duration, T_s is the average transmission time, and T_c is the average collision time due to two or more simultaneous frame transmissions. The channel occupancy time due to successful transmissions and collisions of individual association frames are given by

$$\begin{cases} T_s^{at\_req} = AT_{req} + DIFS + \delta \\ T_c^{at\_req} = AT_{req} + DIFS + \delta, \end{cases} \tag{5.6}$$

$$\begin{cases} T_s^{at\_res} = AT_{res} + \delta + SIFS + ACK + DIFS + \delta \\ T_c^{at\_res} = AT_{res} + DIFS + \delta, \end{cases} \tag{5.7}$$

$$\begin{cases} T_s^{as\_req} = AS_{req} + DIFS + \delta \\ T_c^{as\_req} = AS_{req} + DIFS + \delta, \end{cases} \tag{5.8}$$

$$\begin{cases} T_s^{as\_res} = AS_{res} + \delta + SIFS + ACK + DIFS + \delta \\ T_c^{as\_res} = AS_{res} + DIFS + \delta, \end{cases} \tag{5.9}$$

where δ is the propagation delay. AT_{req}, AT_{res}, AS_{req}, AS_{res}, and *ACK* represent the channel occupancy times of respective association frames. Note that the authentication response and association response contain an ACK because these two frames are acknowledged by the stations. Substituting the transmission and collision duration from Equation (5.6) into (5.5), we obtain $E[slot]_{at\_req}$, which is the average time spent by the authentication request frame. Similarly, we obtain $E[slot]_{at\_res}$, $E[slot]_{as\_req}$, and $E[slot]_{as\_res}$.

Now going back to the queue theory, we have μ_0=$E[slot]_{at\_req}$, μ_1=$E[slot]_{at\_res}$, μ_2=$E[slot]_{as\_req}$, and μ_3=$E[slot]_{as\_res}$, which are the respective service time for each queue. Using (5.1), the average total time required by a station for successfully getting associated is the summation of the average time spent on each queue and given by

$$\begin{aligned} E[AD] = \frac{g}{2}(E[slot]_{at\_req} + E[slot]_{at\_res} \\ +E[slot]_{as\_req} + E[slot]_{as\_res}). \end{aligned} \tag{5.10}$$

When there are g competing stations, the total number of stations successfully associated in a given BI among g stations can be evaluated as

$$X_{bi} = \frac{BI - BP}{E[AD]}, \tag{5.11}$$

where *BP* represents the duration of beacon period.

Now, the total association time (T_{asso}) required by N stations for association can be obtained as

$$T_{asso} = \begin{cases} \left\lceil \dfrac{N}{g} \right\rceil \times BI, & \text{if } X_{bi} \geq g \\ \left\lceil \dfrac{N}{X_{bi}} \right\rceil \times BI, & \text{otherwise.} \end{cases} \tag{5.12}$$

Above equation as can explained as follows. If $X_{bi} \geq g$, then all g stations can successfully get associated with in a BI, with the unused portion left in the BI. In addition, the next g stations have to wait until the following BI. However, if all the g stations are unable to association in the BI, following BI is used.

Table 5.1: Network parameters and values for analysis and simulation.

Parameter	**Value**	**Parameter**	**Value**
Physical rate	650Kbps	Beacon interval	500 ms
Physical header	240 μs	MAC header	14 bytes
Association request	28 Bytes	Association response	30 Bytes
Authentication request	34 Bytes	Authentication response	34 Bytes
ACK	Physical header	SIFS	160 μs
DIFS	264 μs	Back-off slot	52 μs
Propagation delay	1 μs	CWmin	15
CWmax	1023	L	1024

5.9 Experimental Results and Analysis

5.9.1 Experimental Setup

The overall purpose of our study is to see how long stations spend for association in a large network. The transmission behavior of the devices in IEEE 802.11ah can be approximated by that of IEEE 802.11 stations [84]. Therefore, the default implementation of IEEE 802.11 that is readily available in ns-2 is used to study the behavior of IEEE 802.11ah. The problem in ns-2 is that it cannot simulate thousands of stations. However, IEEE 802.11ah implements authentication control mechanism that allows only limited number of station to contend for channel access at a time. Therefore, even though we are assuming a large network with N stations, we assume only certain number of stations are active at a time. All simulations are performed under ns-2.34. Table 5.1 depicts the

Table 5.2: Average time required by a station for association.

Stations	**Average time**	**Average time**
(g)	($E[AD]$)	(Simulation)
10	0.03 secs	0.03 secs
20	0.06 secs	0.06 secs
30	0.09 secs	0.09 secs
40	0.13 secs	0.14 secs
50	0.16 secs	0.17 secs

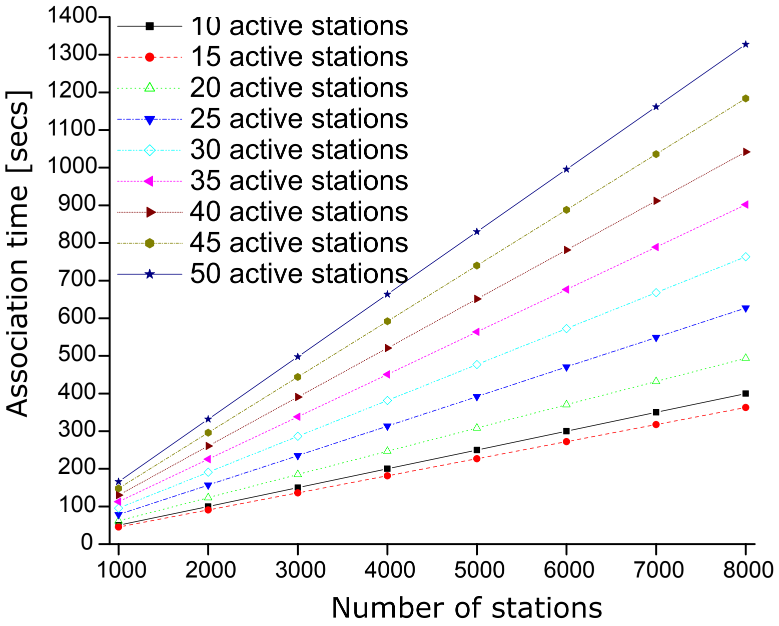


Figure 5.6: Total association time for various network size.

parameters used for simulation. However, we consider only the unassociated state of the network. An AP is deployed at the center of the network. All stations try to associate with the AP. Once the stations are associated, they stay idle. To simulate the behavior of IEEE 802.11ah, in our simulation, we varied the number of stations from 10 to 50 and evaluated the average time taken by each station for the association. From the trace file, we first observed the total time taken for association by all stations. Then, the average time is calculated by dividing total time by the number of stations. Table 5.2 shows the average time *E[asso]* taken by (g) stations for successfully getting associated with AP obtained from analysis and simulation and have close match. Note that average association time do not depend on BI and is always fixed for g stations in a network [79]-[86].

5.9.2 Experimental Results And Discussions

The results presented have been obtained by using above-derived equations. Unless specified, the default value used for the total number of stations is 8000 and for BI is 0.5 sec.

The total association time experienced by IEEE 802.11ah stations for various network sizes is plotted in Figure 5.6. At 50 active stations in a BI, it takes 1327 secs for all 8000 stations to associate with AP. Note that this time is calculated in the absence of data

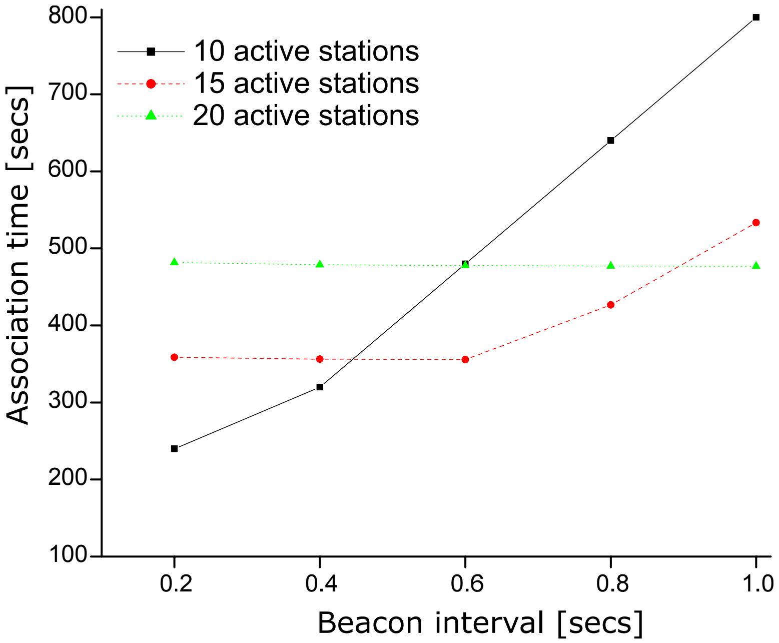


Figure 5.7: Total association time for varying no. of active stations and BI.

traffic. However, in the real situation, there shall be a heavy collision between data traffic and association frames and the association time can be much larger than shown above. Also, channel error may also prolong the delay. Another interesting result that can be seen from the figure is that the total association time for 10 stations is greater than for 15 stations. Therefore, another important observation from the figure is that less active stations do not always means less association time.

Figure 5.7 shows the total association time experienced by IEEE 802.11ah stations when fixed number of stations are allowed to contend under various BI. The results can be interpreted as follows. Let us take the case of g=20 active stations. As the number of contending station is always fixed, the average time taken by a station to associated is also fixed for a BI. Therefore, for a given number of g active stations, as long as $g \geq X_{bi}$, the total time taken for the association of all stations is almost same regardless of the BI duration. However, once $g < X_{bi}$, then the association duration increases because of the unused portion of BI. Therefore, the important conclusion from this experiment is that it is not possible to decrease the total association duration by changing BI.

To see how varying the number of active stations effect the association time for a BI, another experiment was performed. Figure 5.8 shows the total association time experi-

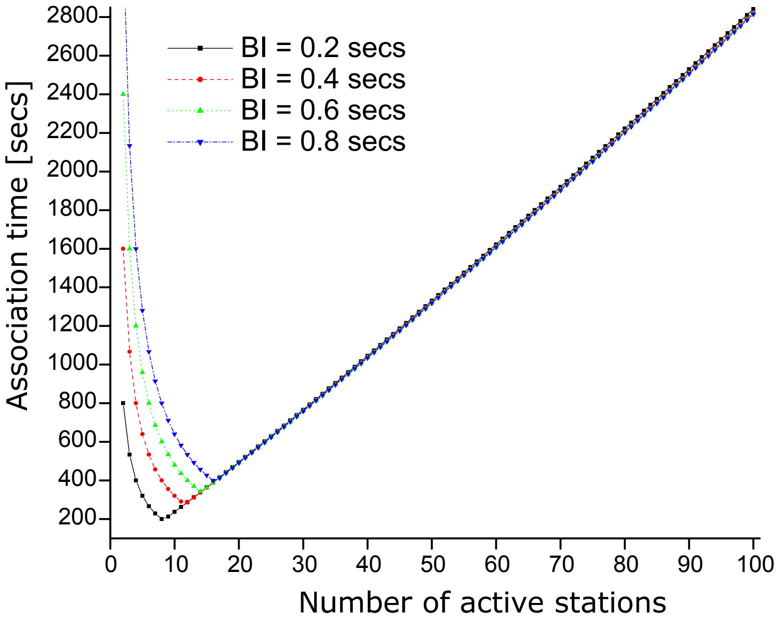


Figure 5.8: Total association time for varying no. of active stations and BI.

enced by IEEE 802.11ah stations when the number of active stations are varied. It can be seen from the figure that changing the number of active stations changes the association time for a given BI. Also, it can be seen from the figure that for any given BI, there exist a number that gives the least association time. For example, for BI=0.2, 8 active stations gave the least association time whereas, for BI=0.8, 16 active stations gave the least association time. Therefore, authentication control mechanism should limit the number of active stations to the optimum number that gives the least association time. The important observation from the figure is that for a given BI, there is an optimum number of active stations that gives the lowest association time.

5.10 Concluding Remarks

In this chapter, we have provided a brief overview of 802.11ah and some of its representative amendments followed by the association problem in IEEE 802.11ah. IEEE 802.11ah has introduced RAW strategy to address heavy channel contention for large network size. However, RAW cannot improve channel access at the stage of network initialization. Therefore, in the case of network reset or during network initialization, every station tries for association and network suffer from heavy contention. In this chapter, the association process of IEEE 802.11ah is analyzed. Our analysis and results demonstrate that during network reset, stations experience heavy contention and long association delay. Also during network initialization phase, there exist two types of stations. One which are already associated (using RAW) and another which are trying to get associated (using ACT). However, no mechanism has been proposed in the draft of IEEE 802.11ah to handle the collision of authentication requests and traffic from already associated stations. Minimizing the association time as lower as possible can reduce the collision to some extend. However, a new mechanism to avoid collision of frames from above mentioned two different types of stations is necessary.

Our analysis and results show that here is an optimum number of active stations for a BI that gives the least association delay. This motivates future work to develop an efficient algorithm that calculates an optimum number of active stations for a BI and used that number for minimizing the association delay.

Chapter 6

Authentication Control in 802.11ah

The analytical results from Chapter 5 demonstrated that there exist an optimum group size for a BI. In this chapter, we present our first scheme to minimize the association delay in IEEE 802.11ah. The second scheme will be presented in the next chapter. In this chapter, we extend our mathematical mode from Chapter 5 to calculate the optimum group size. Also, an enhanced association method is proposed. Rigorous simulation analysis is presented to support the suitability of the proposed scheme.

6.1 Motivation

Since IEEE 802.11ah WLAN supports the connections of more than 8,000 stations, the network throughput may rapidly deteriorate owing to channel contention [69, 81, 82]. When power outage occurs at stations or network initialization, a large number of stations may try to authenticate/associate with the AP simultaneously, leading to severe collision and authentication/association failure. IEEE 802.11ah employs ACM that only allow a small group of stations for association in a BI. We use the term *group size* to denote the number of stations in a group. However, methods for grouping and calculating the group size is undefined. In the previous chapter, we showed that for a given BI, there exists the optimum group size that gives the minimum association delay. In this chapter, we will extend our previous derived mathematical model to calculate the optimum group size for a given BI. Also, an enhanced association method is proposed, which uses the calculated optimum group size for minimizing the total association time.

6.2 Related Works

There has been limited work on deceasing the association time in IEEE 802.11ah. In [80], its is shown that association delay can be decreased by the authentication control mechanism. Similarly, [82] showed that there exist an optimum group size for a BI that gives the minimum association time. However, how to calculate the optimum group size is not showed. A new association scheme for IEEE 802.11ah is proposed in [81] to minimize the authentication delay. However, the authors proposed to change the standard association procedure of IEEE 802.11ah by dedicating a BI for authentication request frame only and postpone rest of the association frames until the next BI.

6.3 System Model Used for Analysis

We consider a network consisting of *N* stations and an AP at the center. The stations are completely connected in the network, i.e., there is no hidden terminal in the network. Moreover, an ideal channel condition is assumed, wherein there are no communication errors and there is no capture effect.

Initially, stations are unassociated with the AP. For making associations, stations generate a random number in the interval [0, L] and listen to a beacon frame including the ACT. From *N* total stations, only a group consisting of *g* stations participate in the association process in a BI. This implies that *g* stations generated a random number less than the ACT value. Moreover, the entire BI is used for the association. Once the stations are associated, they remain idle.

When a station is eligible to participate in the association process, it access the channel using DCF. The station senses the channel if it is idle for one DIFS. Then, the station chooses a random backoff time uniformly distributed from [0, CW], where CW is the backoff window size. The backoff window size is doubled in the range CW$_{min}$ to CW$_{max}$ whenever there is a collision, and it is reset to CW$_{min}$ whenever a frame is acknowledged by the receiver or dropped. When a device succeeds in channel access, it sends a corresponding association frame. Except for the ACK frame, other frames are transmitted using DCF.

6.4 Numerical Analysis

In the previous chapter, we used queue theory to calculate the total association time. However, in this chapter, we used methods used in [85, 87, 86] to calculate the average delay. The calculated delay by both methods were exactly same.

The transmission behavior of the devices in IEEE 802.11ah can be approximated by that of IEEE 802.11 stations [84]. Each time the ACT is broadcast, the group size of *g* stations contend for access to the network. The number of contending station gradually decreases until all *g* stations are associated. The probability τ that a station transmits a frame in a randomly chosen slot time is expressed as

$$\tau = \frac{2(1-2p)}{(1-2p)(CW_{min}+1)+pCW_{min}(1-(2p)^m)}, \tag{6.1}$$

where *m* is the maximum backoff stage, and *p* is the conditional collision probability that a transmitted frame encounters a collision and is given by

$$p = 1-(1-\tau)^{g_a-1}. \tag{6.2}$$

There are *g* active stations at a time. However, as each station gets associated, the number of stations contending for association gradually decreases until all stations in the group are associated. Therefore, the mean number of stations, i.e., g_a=*g/2* is used for the analysis. The probability P_{tr} that there is at least one transmission in the considered slot time is derived as

$$P_{tr} = 1-(1-\tau)^{g_a}. \tag{6.3}$$

Moreover, the probability P_s that a channel access attempt is successful is derived as

$$P_s = \frac{g_a\tau(1-\tau)^{g_a-1}}{P_{tr}}. \tag{6.4}$$

The average amount of time, *E[slot]*, spent on the channel for successful transmission is equal to

$$E[slot] = (1-P_{tr})\sigma + P_{tr}P_sT_s + P_{tr}(1-P_s)T_c, \tag{6.5}$$

where σ is the backoff slot duration, T_s is the average transmission time, and T_c is the average collision time due to two or more simultaneous frame transmissions. The channel occupancy time due to successful transmissions and collisions of individual association frames are given by

$$\begin{cases} T_s^{at\_req} = AT_{req} + DIFS + \delta \\ T_c^{at\_req} = AT_{req} + DIFS + \delta \end{cases} \tag{6.6}$$

$$\begin{cases} T_s^{at\_res} = AT_{res} + \delta + SIFS + ACK + DIFS + \delta \\ T_c^{at\_res} = AT_{res} + DIFS + \delta \end{cases} \tag{6.7}$$

$$\begin{cases} T_s^{as\_req} = AS_{req} + DIFS + \delta \\ T_c^{as\_req} = AS_{req} + DIFS + \delta \end{cases} \tag{6.8}$$

$$\begin{cases} T_s^{as\_res} = AS_{res} + \delta + SIFS + ACK + DIFS + \delta \\ T_c^{as\_res} = AS_{res} + DIFS + \delta, \end{cases} \tag{6.9}$$

where δ is the propagation delay, and AT_{req}, AT_{res}, AS_{req}, AS_{res}, and *ACK* represent the channel occupancy times of the authentication request, authentication response, association request, association response, and ACK frames, respectively. Note that the authentication response and association response contain an ACK because these two frames are acknowledged by the stations.

Equation (6.5) is a generalized equation of the average amount of time spent by a frame. Substituting the transmission and collision duration from equation (6.6) into (6.5), we obtain $E[slot]_{at\_req}$, which is the average amount of time spent by the authentication request frame. Similarly, we obtain $E[slot]_{at\_res}$, $E[slot]_{as\_req}$, and $E[slot]_{as\_res}$, which are the average amount of time spent by the authentication response, association request, and association response frames, respectively.

We calculates the average delay *E[D]* for a successfully transmitted packet. Packet delay is defined to be the time interval from the time a packet is at the head of its MAC queue ready for transmission, until its successful reception in the destination. *E[D]* is given by [86]

$$E[D] = E[X] \times E[slot], \tag{6.10}$$

where *E[X]* is the average number of slot required for a successful packet transmission and is given by

$$E[X] = \frac{(1-2p)(CW_{min}+1) + pCW_{min}(1-(2p)^m)}{2(1-2p)(1-p)}. \tag{6.11}$$

The total time required by a station for successfully exchanging all the association frames is given by

$$\begin{aligned} E[Asso] = E[slot]_{at\_req} + E[slot]_{at\_res} \\ +E[slot]_{as\_req} + E[slot]_{as\_res}, \end{aligned} \tag{6.12}$$

Association delay *E[AD]* is defined as the time interval from the start of the association process to the time a station successfully gets associated with the AP and is evaluated as,

$$E[AD] = E[X] \times E[Asso]. \tag{6.13}$$

When there are *g* competing stations, the total number of stations successfully associated in a given BI among *g* stations can be evaluated as

$$X_{bi} = \frac{BI - BP}{E[AD]}. \tag{6.14}$$

where *BP* represents the duration of beacon period.

If $X_{bi} \geq g$, then all *g* stations can be successfully associated in a BI, with the remaining duration in the BI left unused. In addition, the next *g* stations have to wait until the next BI. Therefore, the total association time (T_{asso}) required by *N* stations for association can be obtained as

$$T_{asso} = \begin{cases} \left\lceil \dfrac{N}{g} \right\rceil \times BI, & \text{if } X_{bi} \geq g \\ \left\lceil \dfrac{N}{X_{bi}} \right\rceil \times BI, & \text{otherwise.} \end{cases} \tag{6.15}$$

T_{asso} has a minimum value when X_{bi} = *g*, i.e., when all *g* stations are successfully associated without any time left in the BI. Now substituting X_{bi} = *g* in (6.14), we obtain,

$$g = \frac{BI - BP}{E[AD]}. \tag{6.16}$$

Equations (6.1), (6.2), and (6.16) represent a nonlinear system with three unknowns τ, *p*, and *g* that can be solved using numerical techniques. Let us denote this solution of *g* as X_{gbi}. Therefore, X_{gbi} is the optimum group size or the number of stations that can be successfully associated in a given BI. Once X_{gbi} is known, we can easily map X_{gbi} to ACT.

$$ACT_{bi} = \frac{X_{gbi} \times L}{N_{left}}. \tag{6.17}$$

Now, by broadcasting ACT_{bi} in a beacon, approximately X_{gbi} stations will participate in the association process in a BI.

6.5 Proposed Association Mechanism

In our algorithm, we analytically find the optimum group size, i.e. X_{gbi}. Using X_{gbi}, we adjust the ACT value (to ACT_{bi}) such that the number of new stations participating in a BI is X_{gbi} stations. In every BI, the AP counts the total number of stations sending authentication requests and store in $Count_{asso}$. If $Count_{asso}$ ¿ 2×X_{gbi} stations, the next beacon ACT value is changed to ACT$_{min}$ to notify that the AP is not accepting any new authentication requests. However, once the number of stations sending authentication requests reach below *X_{gbi}/2*, *ACT_{bi}* is adjusted such that the AP can accept X_{gbi} number of stations in the next BI.

Algorithm 2 Proposed association algorithm.

```
1. Find the optimum number of stations ($X_{gbi}$) that can be successfully associated in the given BI
2. Find the corresponding value of ACT ($ACT_{bi}$) using $X_{gbi}$ and broadcast it in the beacon.
3. Count the number of stations sending authentication requests in every BI and compare it with $X_{gbi}$
4. If the counter exceeds $2 \times X_{gbi}$, stop accepting new requests
5. If the counter is below $X_{gbi}/2$, adjust the ACT to accept $X_{gbi}$ stations
```

We have assumed two cases for estimating the *ACT_{bi}*. In the first case, we assume that the total number of stations is unknown. This is the case when the network is initializing for the first time. In this case, assuming that stations generate a random number in the range[0 to L] and there are 8000 stations, we estimate the initial value of *ACT_{bi}* as *ACT_{bi} = X_{gbi}×(L / 8000).* From the next BI, following equation is used to estimate new ACT when respective conditions are satisfied.

$$ACT_{bi} = \begin{cases} min\{2 \times Last(ACT_{bi}), L\}, & \text{if } Count_{asso} < \frac{X_{gbi}}{2}, \\ ACT_{min}, & \text{if } Count_{asso} > 2 \times X_{gbi}. \end{cases} \tag{6.18}$$

where *Last(ACT_{bi})* is the last value of *ACT_{bi}* broadcast which is not *ACT_{min}*. The value of *ACT* is doubled every time the *$Count_{asso}$* ¡ *X_{gbi}/2.*

In the second case, we assume that AP remembers how many station were there in the network. AP can save the number of stations in a network so that it can be used for the next association process due to network reset or power failure. Assuming AP knows total number of stations (N_{left}) waiting for the association process, following equation is used to estimate new ACT.

$$ACT_{bi} = \begin{cases} \frac{X_{gbi} \times L}{N_{left}}, & \text{if } Count_{asso} < \frac{X_{gbi}}{2}, \\ ACT_{min}, & \text{if } Count_{asso} > 2 \times X_{gbi}. \end{cases} \tag{6.19}$$

In either cases, either AP knows or does not know about the number of stations, Algorithm 2 ensures that on an average approximately X_{gbi} stations participate in the association process in a BI.

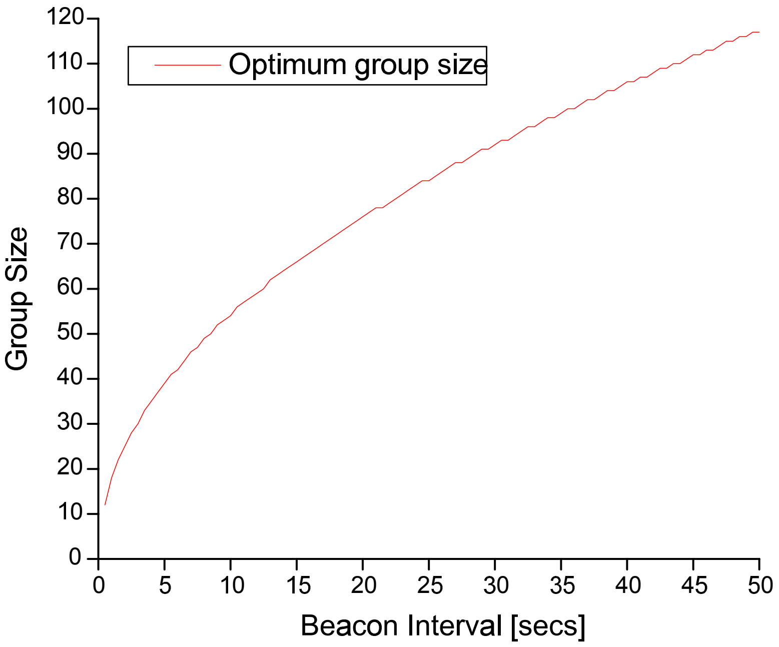


Figure 6.1: Optimum group size for varying BI.

6.6 Experimental Results

The results have been obtained from a simulation and analytical framework. Table 5.1 lists the parameters used for the analysis and simulation. The simulation was conducted in ns-2.34. In the case of IEEE 802.11ah, it is assumed that a group of g stations attempt association in every BI. For BI = 0.5 s, in both the analysis and the simulation, we observed that a total of X_{gbi} = 12 successful associations are possible. Therefore, in the case of the proposed algorithm, the group size was set to 12 stations. Similarly, Table 6.1 lists the optimum group sizes for various BIs. Similarly, the optimum group size for various values of BI is shown in Figure 6.1

Table 6.1: Optimum group size for various BIs.

BI (s)	0.2	0.4	0.6	0.8	1.0
$\mathbf{X}_{gbi}$	8	11	14	16	18

The total association time taken by stations under various network sizes is plotted in Figure 6.2. The results are obtained from both simulation and analysis. However, because of the limitation with ns-2 simulation, only up to 1000 stations are shown. Figure 6.2

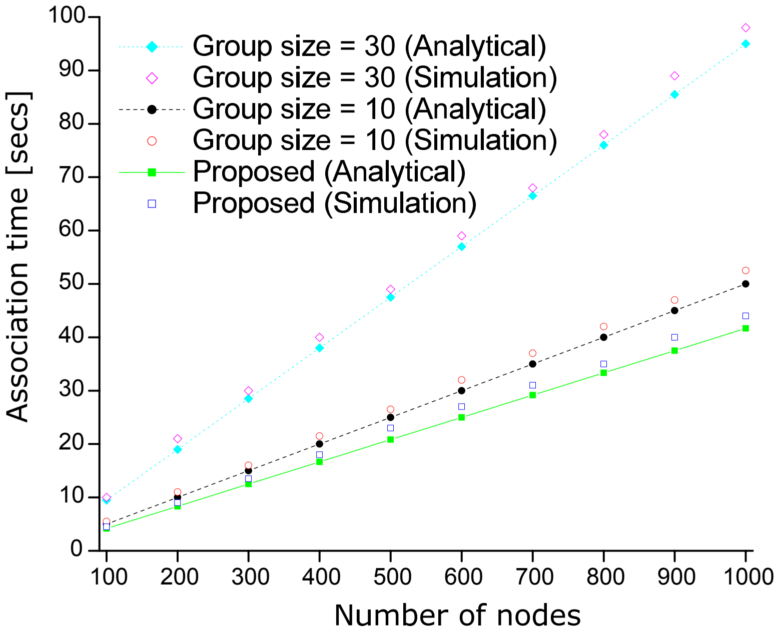


Figure 6.2: Association time for varying number of stations.

shows that the results of our analytical model are in good agreement with the simulation results, thus validating our results. We made a comparison with the proposed algorithm: two group sizes were selected for IEEE 802.11ah. The first group size, g=10, had a low number of contending stations, whereas the second group size, g=30, had a high number of contending stations. In the case of g=30, the contention was high, resulting in more collisions and delays. As all 50 stations were unable to get associated in a single BI, more than one BI was adopted. However, in the case of g=10, all 10 stations were successfully associated with a significant amount of unused time in the BI. The next group had to wait until the next BI. This inefficient use of BI results in more delay as compared with the delay in the proposed method. However, in the case of the proposed algorithm, the total number of stations contending in a BI is controlled and is maintained at a fixed optimum size. The proposed algorithm completely unitized the entire BI without wastage, keeping contention to the minimum. From the figure, it can be clearly seen that the proposed method has the least association time and is successful in decreasing the total association time by a large extent.

Figure 6.3 shows the association time for up to 8,000 stations. For g=30 stations, it took 760 s for all 8,000 stations to associate with the AP. Similarly, for g=10 stations,

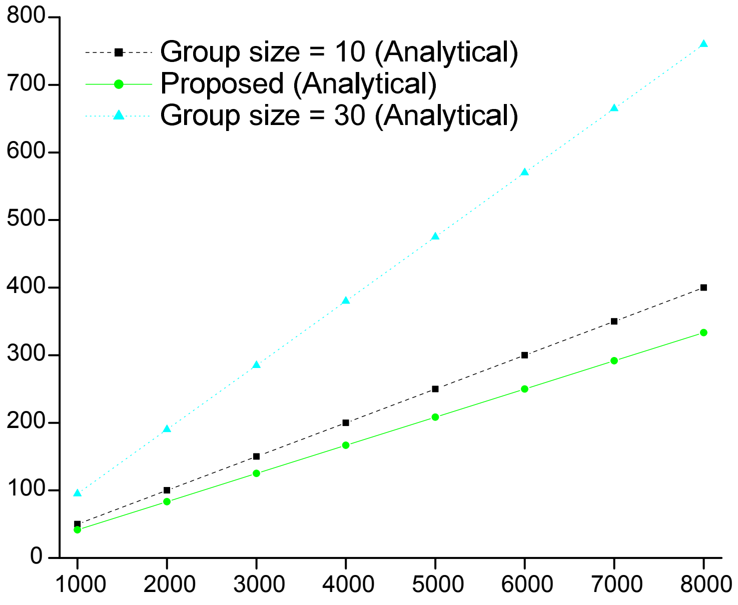


Figure 6.3: Association time for varying number of stations.

the total time taken was 400 s for associating 8,000 stations. However, with the proposed algorithm, it took only 333 s for associating all 8,000 stations. It was observed that the proposed method was able to decrease the total association time by factors of 2.28 and 1.2 as compared to the case of *g*=30 and *g*=10, respectively. From this analysis, it can be concluded that the proposed algorithm is able to decrease the association time of IEEE 802.11ah by a large extent.

6.7 Concluding Remarks

In this chapter, the analytical model of an authentication/association process is extended. Based on the analytical model, the optimum number of stations (group size) that could be successfully associated in a given BI was derived and estimated. The analytical results demonstrated that optimum group size give the minimum association delay. Therefore, an enhanced association algorithm was proposed, allowing only an optimum number of stations to contend in a BI. The experimental results verified that the proposed algorithm yields the minimum association delay as compared with other group sizes.

Chapter 7

Block Association for 802.11ah

In this chapter, we present our second scheme for minimizing the association delay in IEEE 802.11ah. The second scheme is based on block association. The proposed block association method is able to decrease the total association time of IEEE 802.11ah by several folds. Rigorous simulation analysis is presented to support the suitability of the proposed scheme.

7.1 Motivation

As explained in Chapter 6, authentication control limits the number of stations that can participate for association in a BI. Hereafter, we use the term *active stations* to denote the number of stations eligible for the association. At BI = 0.5 secs, the total association time experienced by IEEE 802.11ah stations for various network sizes is plotted in Figure 7.1. When only the optimum number of active stations is allowed in a BI, it takes 333.33 secs for all 8000 stations to associate with AP, which is about 6 minutes. Note that this time is calculated in the absence of data traffic and in the absence of channel error. As the number of active stations goes higher, the total time taken for the association is even higher. At just 30 active stations in a BI, it takes 760.01 secs for all 8000 stations to associate with AP, which is about 13 minutes. Similarly, for 100 active stations, it takes 26 minutes for all 8000 stations to associate with AP.

As mentioned above, during association ACM is used, whereas RAW is used for data communication. Even though both ACM and RAW are used to limit the number of contending stations, they come into the picture at different network stages. However, they may co-exist during network initialization stage. However, when these two types of stations co-exists, how to manage the traffic from these two types of stations is unanswered in the draft of 802.11ah. An open research challenge is how to prevent collisions of authentication requests and traffic of already associated stations. So, these questions are the motivation for our proposed scheme. Our goal is to bring the total association time to minimum level such that ACM completes before RAW even comes into the pictures.

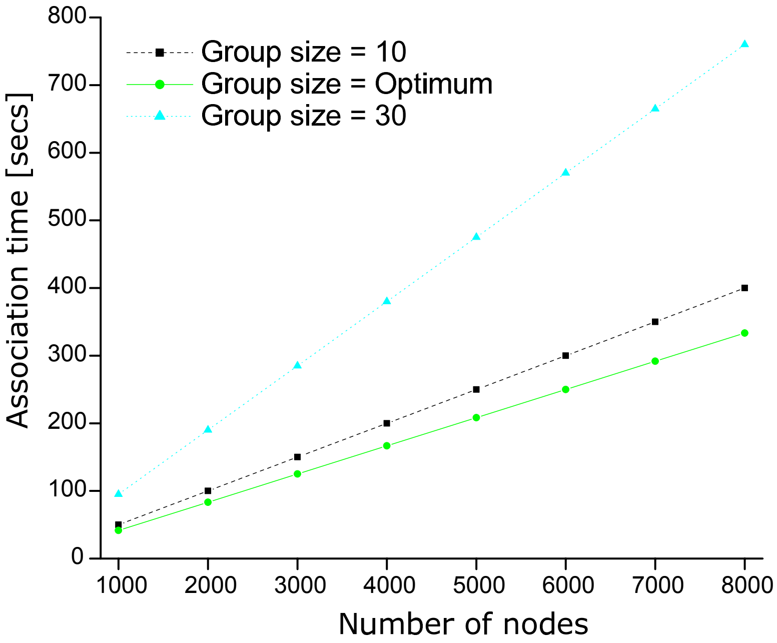


Figure 7.1: Total time spent in association.

7.2 Network Model and Assumptions

In this section, we describe our network scenario model shown in Figure 7.2. The assumptions made regarding the network is provided in the following:

- The network is assumed to be a circular geographic area of radius *R* with the AP positioned at the center.
- Several thousand of stations (black dots) are uniformly deployed in the network.
- Each station can directly communicate with AP in a single hop.
- Stations can adjust the transmission power and can switch between different channels.
- An ideal channel condition is assumed, and there is no capture effect.

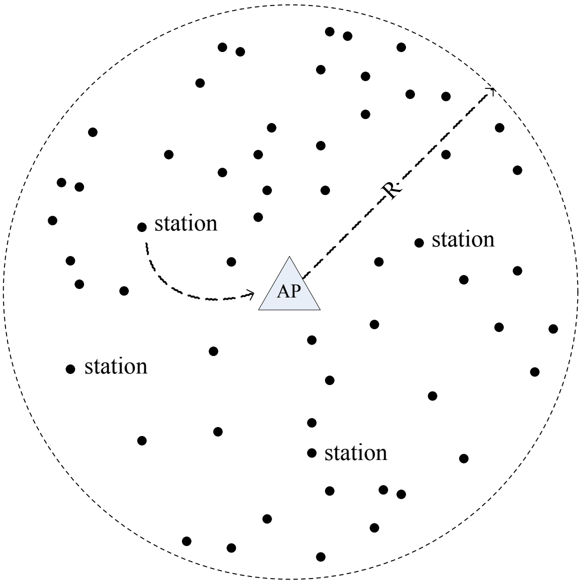


Figure 7.2: Network scenario model.

7.3 Proposed Block Association Scheme

In this section, the proposed block association scheme is explained. In the proposed scheme, the total networking is divided into *k* number of groups, with each group having its own group head (GH). GH are especial nodes which can also function as an AP. A relay node can be a GH. During the network initialization, GH broadcast beacon such that only the stations in the group can hear it (explained more in Section 7.3.2). GH behaves as a temporary AP of the group, and all stations in the group associate with the GH at first. Once all the stations in the group are associated with GH, GH sends block association request to the main AP. AP analyze the request and then in return sends block association response which contains AID of all stations. Once the stations are associated with the main AP, now they can start direct communication with the AP. The key intention of the proposed scheme is to minimize association as minimum as possible.

The proposed block association scheme can be divided into three phases: GH selection, association, and communication.

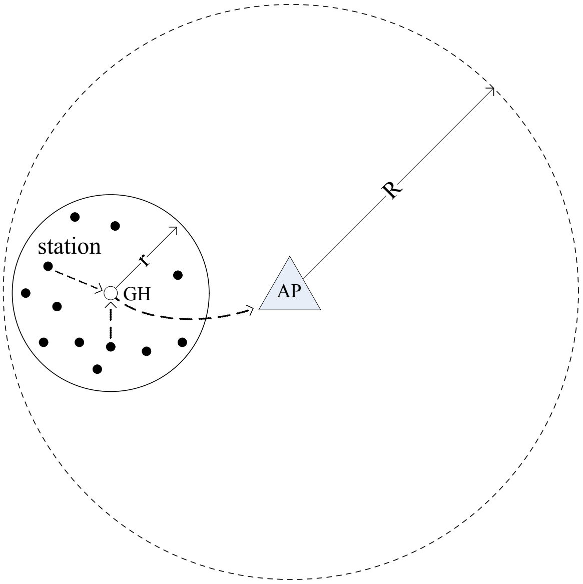


Figure 7.3: Grouping in proposed method.

7.3.1 Phase I: GH Selection

Since GH has special capability of being temporary AP, it is assumed that the number of such stations are uniformly deployed to cover entire network. From the pool of special capable stations, *k* number of GHs are selected such that the GHs are uniformly distributed and covers entire network. GH selection is a one-time process and once done, the station remembers it. GH can be selected in two methods: manual selection and automatic selection.

- **Manual selection:** Since we are talking about the large network covering the area of 1 km diameter, the GHs can be properly planned and selected. For example, in the case of smart meter and smart grid, GH can be carefully planned and selected manually. However, the problem with manual selection is that they are not flexible.
- **Automatic selection:** GH selection has been already extensively studied. Various GH selection scheme such as LEACH has been already discussed in various literature [88]. We assume one of them are used to select the GH.

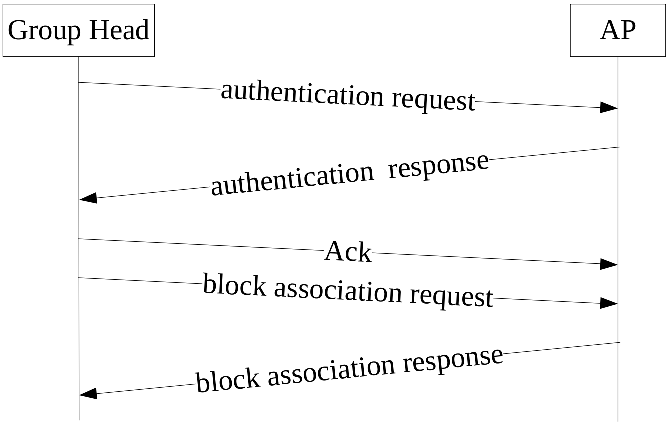


Figure 7.4: Proposed block association scheme.

7.3.2 Phase II: Association

Figure 7.3 shows the grouping of the network. Let A_n be the area of the whole network and A_g be the area of a group. Owing to the uniform deployment strategy, we can compute an approximation for the group radius, *r* :

$$\begin{aligned} k \times A_g &= A_n \\ \Rightarrow k \times \pi r^2 &= \pi R^2 \\ \Rightarrow r &= R/\sqrt{k} \end{aligned} \tag{7.1}$$

During the association phase, GH becomes a temporary AP and take control of the group. GH starts association process by transmitting the periodic beacon. However, GH sets their transmission range to *r* such that only the stations in its group can hear it. All the stations in the group associate with GH following the standard association procedure of IEEE 802.11ah (Figure 5.4). GHs used authentication control mechanism for fair channel access among a large number of stations in a group. Since there are *k* groups in the network, all groups can perform the association simultaneously as the groups don't interfere with each other.

Once the GH does not get any more association request from the stations, it performs block association with the main AP. Before performing the block association, GH changes its transmission range to its default range. Figure 7.4 shows the proposed block association scheme. First the GH authenticate itself with the AP. Once it is authenticated, it then sends the block association request. The block association request contains as-

MAC header					Frame body		
2	2	2	6	2	Variable	Variable	4
Frame Control	DA	SA	BSS ID	Seq-ctrl	STAA	Other Fields	FCS

Figure 7.5: Proposed block association request frame.

MAC header					Frame body			
2	2	2	6	2	Variable	Variable	Variable	4
Frame Control	DA	SA	BSS ID	Seq-ctrl	STAA	AID	Other Fields	FCS

Figure 7.6: Proposed block association response frame.

sociation request of all the station in the group. Figure 7.5 shows the proposed block association request frame. The frame consists of a new field of variable length called STAA, which is basically the two bytes address of all the stations requesting the association. The other fields in the frame indicate other things such as capability info, supported rates, listen intervals and so on. Since associating stations are IEEE 802.11ah stations of similar types, these stations are assumed to have similar requirements. However, in case the stations have different requirements in the other fields, those stations having similar request are bundled into one block association request. The AP analyze the block association request from the GH and if they are valid, then it response with the block association response frame. Figure 7.6 shows the proposed block association response frame. The block association response contains two new fields, STAA, and AID. These two fields are of variable length. Each two bytes in STAA is the address of the associating station. Similarly, each two bytes of AID is the corresponding association ID of the stations. That means first two bytes of AID is the association ID of the station whose address is the first two bytes of STAA and the pattern continues. The block association response frame broadcast by the AP can be received by all the stations. By analyzing this received block association response frame, the intended stations can decode its AID. Once the station receives its AID, it is now ready for data transfer.

7.3.3 Phase II: Communication

Once the station has its AID, now it is ready for data communication. We do not propose any changes in data communication. Thus, data communication is done exactly as proposed in original IEEE 802.11ah. Stations directly upload its data to AP in a single hop.

7.4 Numerical Analysis

The numerical model of association of stations with AP has been already derived in previous chapters. The analytical model from Chapter 5 model is used here. For the ease of readability, some equations are rewritten.

The total number of *N* stations in the network is divided into equal size of *k* groups. The total number of stations in each group, G_s, is given by

$$G_s = \frac{N}{k}, \tag{7.2}$$

Each station in a group tries to associate with the GH first. When multiple stations try to access at the same slot, they contend via the random backoff procedure. Therefore, the probability τ that a station transmits a frame in a randomly chosen slot time is expressed as above

$$\tau = \frac{2(1-2p)}{(1-2p)(CW_{min}+1)+pCW_{min}(1-(2p)^m)}, \tag{7.3}$$

where *m* is the maximum backoff stage. The conditional collision probability, *p*, that a transmitted frame encounters a collision and is expressed as

$$p = 1-(1-\tau)^{g/2-1}. \tag{7.4}$$

Because of ACM, only *g* stations can participate in association at a time. However, as each station gets associated, the number of stations contending for association gradually decreases until all stations in the group are associated. Therefore, the average number of stations, i.e., *g/2* is used for the analysis. The probability P_{tr} that there is at least one transmission in the considered slot time is derived as

$$P_{tr} = 1-(1-\tau)^{g/2}. \tag{7.5}$$

Moreover, the probability P_s that a channel access attempt is successful is derived as

$$P_s = \frac{g\tau(1-\tau)^{g/2-1}}{2P_{tr}}. \tag{7.6}$$

The average amount of time, *E[slot]*, spent on the channel for successful transmission is equal to

$$E[slot] = \frac{(1-P_{tr})}{P_{tr}P_s}\sigma + T_s + \frac{(1-P_s)}{P_s}T_c, \tag{7.7}$$

where σ is the backoff slot duration, T_s is the average transmission time, and T_c is the average collision time due to two or more simultaneous frame transmissions. The channel occupancy time due to successful transmissions and collisions of individual association frames are given by

$$\begin{cases} T_s^{at\_req} = AT_{req} + DIFS + \delta \\ T_c^{at\_req} = AT_{req} + DIFS + \delta \end{cases} \tag{7.8}$$

$$\begin{cases} T_s^{at\_res} = AT_{res} + \delta + SIFS + ACK + DIFS + \delta \\ T_c^{at\_res} = AT_{res} + DIFS + \delta \end{cases} \tag{7.9}$$

$$\begin{cases} T_s^{as\_req} = AS_{req} + DIFS + \delta \\ T_c^{as\_req} = AS_{req} + DIFS + \delta \end{cases} \tag{7.10}$$

$$\begin{cases} T_s^{as\_res} = AS_{res} + \delta + SIFS + ACK + DIFS + \delta \\ T_c^{as\_res} = AS_{res} + DIFS + \delta, \end{cases} \tag{7.11}$$

where δ is the propagation delay, and AT_{req}, AT_{res}, AS_{req}, AS_{res}, and *ACK* represent the channel occupancy times of the authentication request, authentication response, association request, association response, and ACK frames, respectively. Note that the authentication response and association response contain an ACK because these two frames are acknowledged by the stations.

Substituting the transmission and collision duration from equation (7.8) into (7.7), we obtain $E[slot]_{at\_req}$. Similarly, $E[slot]_{at\_res}$, $E[slot]_{as\_req}$, and $E[slot]_{as\_res}$ are obtained.

The total time required by a station for successfully exchanging all the association frames is given by

$$\begin{aligned} E[Asso] = E[slot]_{at\_req} + E[slot]_{at\_res} \\ + E[slot]_{as\_req} + E[slot]_{as\_res}, \end{aligned} \tag{7.12}$$

Association delay *E[AD]* is defined as the time interval from the start of the association process to the time a station successfully gets associated with the AP and is evaluated as,

$$E[AD] = \frac{g}{2} \times E[Asso]. \tag{7.13}$$

If there are *g* competing stations, it may not be possible to associate all *g* stations in a BI. The total number of stations, X_{bi}, that can be successfully associated in a given BI among *g* contending stations can be evaluated as

$$X_{bi} = \frac{BI - BP}{E[AD]}. \tag{7.14}$$

There are G_s stations in a group. The total association time (GT_{asso}) required by G_s stations for association can be obtained as

$$GT_{asso} = \begin{cases} \dfrac{G_s \times BI}{g}, & \text{if } X_{bi} \geq g \\ \dfrac{G_s \times BI}{X_{bi}}, & \text{otherwise.} \end{cases} \tag{7.15}$$

Once the total time take for association within a group is found, the time taken by GHs for the association with AP is calculated. Same equations through 7.3 to 7.13 are used for calculationg the association delay of GHs. However, *k* (number of GHs) is used as the total number of contending station. Let *Exreq* be the extra bytes required for each station in block association request frame, *sn* be the number of stations included in the block association request frame, and *brate* be the bit rate. Then the channel occupancy time due to successful or collision of block association request frame are given by,

$$\begin{cases} T_s^{bas\_req} = AS_{req} + \frac{Exreq \times sn}{brate} + DIFS + \delta, \\ \\ T_c^{bas\_req} = AS_{req} + \frac{Exreq \times sn}{brate} + DIFS + \delta. \end{cases} \tag{7.16}$$

Similarly, assuming *Exres* be the extra bytes required for each station in block association response frame, the channel occupancy time due to successful or collision of block association response frame are given by,

$$\begin{cases} T_s^{bas\_res} = AS_{res} + \frac{Exres \times sn}{brate} + DIFS + \delta, \\ \\ T_c^{bas\_res} = AS_{res} + \frac{Exres \times sn}{brate} + DIFS + \delta. \end{cases} \tag{7.17}$$

Now, substituting the transmission and collision duration from equation (7.16) into (7.7), we obtain *E[slot]*$_{bas\_req}$, which is the average amount of time spent by the block association request. Note that, *k* is used as the total number of contending station while calculating various probabilities in (7.7). Similarly, we obtain *E[slot]*$_{bas\_res}$, which is the average amount of time spent by the block association response frame.

Let *E[GHAsso]* be the total association time required by a GH to successfully get associated with the AP. The total time required by a GH for successfully exchanging all the association frames is given by

$$\begin{aligned} E[GHAsso] = E[slot]_{at\_req} + E[slot]_{at\_res} \\ +E[slot]_{bas\_req} + E[slot]_{bas\_res}. \end{aligned} \tag{7.18}$$

Association delay (*E[GAD]*) or the average amount of time a GH has to wait before it can successfully gets associated with the AP is calculated as

$$E[GAD] = \frac{k}{2} \times E[GHAsso]. \tag{7.19}$$

The total association time is the time required by all stations to be successfully get associated with the AP. Therefore, the total association time, *E[TAD]*, is summation of time required by stations to associate with GH and the time required by all GHs to successfully associate with the AP and is derived as

$$E[TAD] = kE[GAD] + GT_{asso} + BI. \tag{7.20}$$

Even though there are *k* groups, all groups can simultaneously associate with their GHs without interfering with other groups. Therefore, only one GT_{asso} is added in the total time. Each GH starts association with AP if there in no association request in a BI. Therefore, BI is added.

Table 7.1: Network parameters and values for analysis and simulation.

Parameter	**Value**	**Parameter**	**Value**
Physical rate (brate)	650Kbps	Beacon interval	500 ms
Physical header	240 μs	MAC header	14 bytes
Association request	28 Bytes	Association response	30 Bytes
Authentication request	34 Bytes	Authentication response	34 Bytes
ACK	240 μs	SIFS	160 μs
DIFS	264 μs	Back-off slot	52 μs
Exreq	6 bytes	Exres	2 bytes
sn	G_s	CWmin	15
CWmax	1023	L	1024

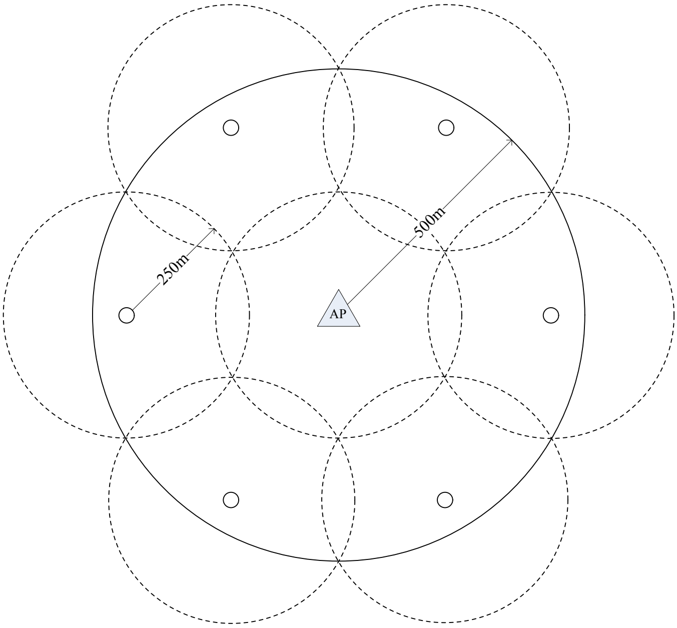


Figure 7.7: GHs selected to cover the whole network area.

7.5 Experimental Results

The results have been obtained from a simulation and analytical framework. Table 7.1 lists the parameters used for the analysis and simulation. The simulation was conducted in ns-2.34. The available standard IEEE 802.11 code was modified to reflect the IEEE 802.11ah and the proposed block association scheme. In both cases, ACT is implemented to allows only *g* stations to association in every BI. Unless specified *g*=30 was used.

For the simulation, a circular region of radius 500m was taken with AP at the center. The stations were uniformly distributed within this region. 7 GHs were selected including the AP as one of the GH. To cover the circular region with radius of 500m with 7 circles, the required radius of small circle is 250m [83]. Thus, the transmission range of all GH, including the AP was set to 250m at the beginning of the simulation. Figure 7.7 shows the coverage of the whole network by 7 GHs.

The total time taken for association in IEEE 802.11ah and with block association scheme under various network sizes is plotted in Figure 7.8. The results are obtained from both simulation and analysis. However, because of the limitation with ns-2 simulation, only up to 1000 stations are shown. Figure 7.8 shows that the results of our analytical model are in good agreement with the simulation results, thus validating our

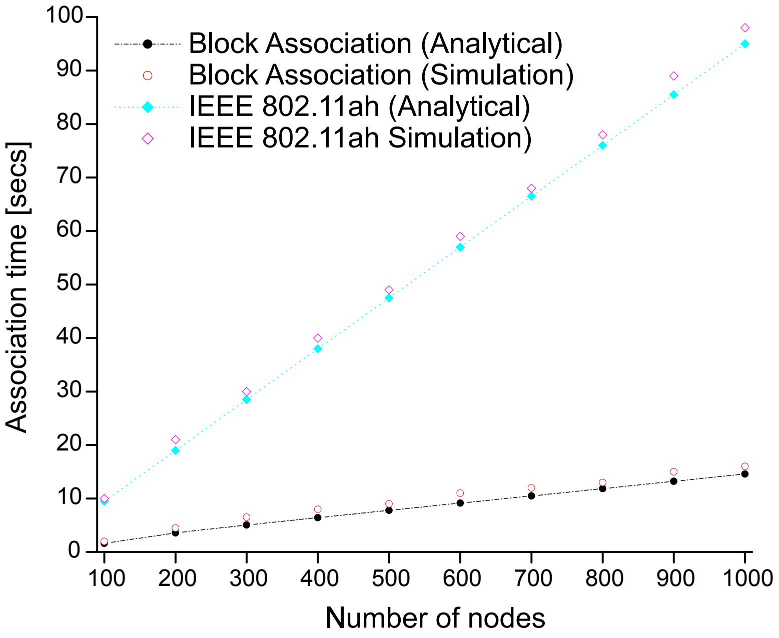


Figure 7.8: Total association time for various network size.

results. Similarly, the total time taken for association in IEEE 802.11ah and with block association scheme for up to 8000 stations is plotted in Figure 7.9. In the case of block association method, it can be viewed as 7 independent APs associating stations simultaneously at the same time. Therefore, the results obtained in both figures shows that the block association method is able to decrease the total association time roughly by 7 times. Therefore, intuitively it can be understood that the block association method is able to decrease the total association time by total number of GH times. However, below we will show that this is not true.

The total time taken for association in IEEE 802.11ah and with block association scheme under various network sizes when the number of active stations is varied is plotted in Figure 7.9. As expected, the association time is minimum when the optimum number of active stations are allowed to contend.

To see how the number of GHs effect the overall association time, another experiment was performed. In this experiment, the number of active stations was set to the optimum group size for all values of BI. The total number of stations was set to 8000. The obtained results are shown in Figure 7.10. As can be seen in the figure, the total association time decreases exponentially as the number of GHs is increased by 1. However, as we keep on

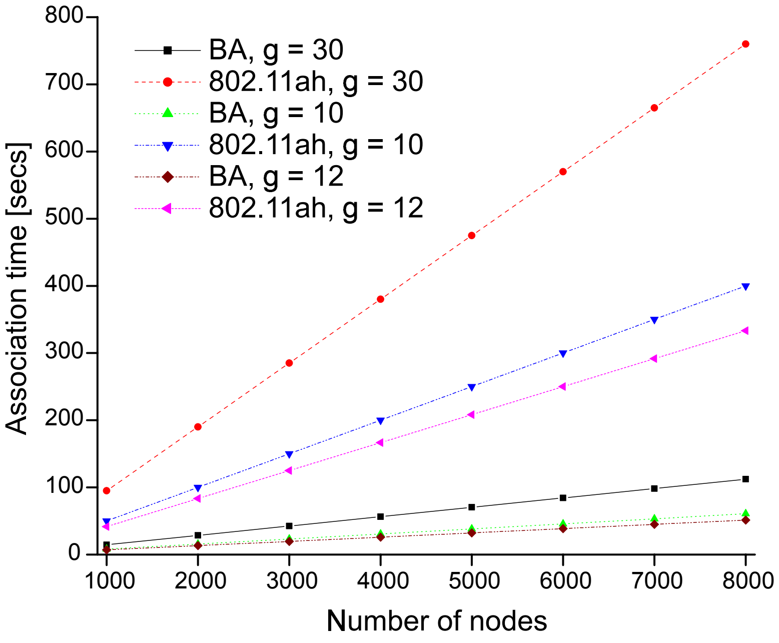


Figure 7.9: Total association time for varying number of group and network sizes.

increasing the GHs, after exceeding a certain limit, the decrease in the total association time is minimum. The red dot in the graph shows the association time for GHs = 10 in the case of BI = 0.5. As the number of GHs, increase beyond 10, no significant performance improvement is noticed. Table 7.2 shows the total time spent for association by 8000 stations for various values of BI. The important conclusion from this experiment is that just keeping the number of GHs to 10 or less is enough to bring the total association time to less than a minutes. Since, GHs is an expensive resource, results show that large number of GHs is not required to keep the association time to the acceptable minimum level. The graph also shows that there is a limit on GHs that gives the minimum time. However, increasing the number of GHs beyond this value instead increases the total association time.

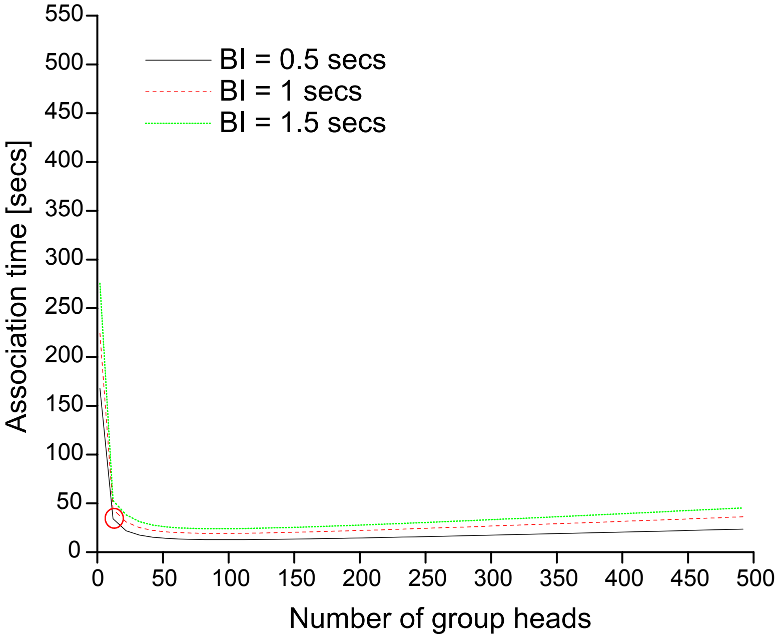


Figure 7.10: Total association time for various group heads.

Table 7.2: Total time required for association of 8000 stations.

No. GHs	**Association time in secs** ($E[TAD]$)		
(***k***)	**BI =0.5 secs**	**BI = 1 sec**	**BI =1.5 secs**
1	333	444	545
2	167	224	275
3	112	150	184
4	85	113	139
5	69	92	112
6	58	77	95
7	51	67	82
8	45	60	73
9	41	54	66
10	38	50	60

7.6 Concluding Remarks

One of the most challenging issues in IEEE 802.11ah is supporting a large number of stations efficiently. To reduce heavy channel contention in IEEE 802.11ah networks, stations are divided into groups and each group of stations are allowed to access in only the designated channel access period. Even though, grouping strategy enables fair channel access among the large number of stations, they cannot operate simultaneously. Only one group can operate at a time. In the proposed scheme, we try to eliminate this shortcoming of legacy grouping strategy. By electing a group head in each group and by using transmission power control to confine the transmission hearable only inside the group, the proposed method enable concurrent association in all groups at the same time. This strategy brings drastic fall in the total association time. Our experimental results verify that our block association method decreases the total association time by many folds. However, the performance gain is achieved with extra cost of special node, i.e., group head.

Chapter 8

Conclusions

In this dissertation, we have presented some innovative approaches to improve the association delay in IEEE 802.15.4 and IEEE 802.11ah networks. The remarkable attributes of the proposed improvised approaches are that they are simple and easy to implement. Such attributes make the proposed approaches attractive for practical implementation in the real-world M2M applications. In what follows, we summarize those approaches in the order they have appeared in the dissertation.

In Chapter 3, a new fast association technique called DBC for IEEE 802.15.4 is presented. We showed through analysis and simulation that channel scanning is the key reason for long association delay in IEEE 802.15.4. The proposed DBC scheme prevents nodes from scanning multiple channels, thus, minimizing the association delay. Early detection of link breakage and once associated, retaining the connectivity with coordinator are also crucial. Thus, a method for the early detection of link breakage and the method to increase the node connectivity time with its coordinator in IEEE 802.15.4 beacon-enabled mode are also presented. Our approach results in significant improvement by reducing the number of times the moving node switches coordinators. Experimental results have verified that our schemes work well.

IEEE 802.11ah is another wireless network where fast association is very important. During network initialization, thousands of stations are simultaneously contending for association. Therefore, if no proper measure is taken, network suffers from serious congestion. In Chapter 5, the analytical model for authentication/association of IEEE 802.11ah is derived. IEEE 802.11ah has proposed some methods on decreasing the association delay. However, our study shows that the proposed methods can be improved and enhanced. Therefore, we have proposed new and enhanced methods.

IEEE 802.11ah employs authentication control mechanism allowing only a small group of stations for association in a BI. However, how to group stations and how to calculate the group size is undefined. In Chapter 6, we presented the first method that estimates the optimum group size for a BI and then proposed an enhanced association method that fully utilizes the BI giving the minimum association time. The results show that the proposed authentication control mechanism is able to minimize association delay significantly.

Finally, in Chapter 7, the second fast association method for IEEE 802.11ah is presented. In the second method, the stations are divided into several groups each having a group head. A group head is responsible for collecting all the association requests and sending an aggregated one block request to AP. By electing a group head in each group and by using transmission power control to confine the transmission hearable only inside the group, the proposed method enable concurrent association in all groups at the same time. This strategy brings drastic fall in the total association time. The experimental results show that our proposed methods can decrease the total association time by many folds as compared to the original protocol. Despite of the fact that the proposed method needs the group head, the introduced performance enhancement makes it a fruitful solution.

Our fast association methods are simple and can be implemented in any infrastructure based network. We expect that our proposed methods will be beneficial in various M2M applications.

Bibliography

[1] N. Bari, G. Mani, and S. Berkovich, “Internet of Things as a Methodological Concept,” in Computing for Geospatial Research and Application (COM.Geo), 2013 Fourth International Conference, pp. 48-55, Jul. 2013.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Generation Computer Systems, vol. 27, no. 7, pp. 1645-1660, 2013.

[3] L. Coetzee and J. Eksteen, “Internet of Things - promise fo the future? An Intorduction,” IST-Africa Conference Preceeding, pp. 1-9, May 2011.

[4] D. Lund, C. MacGillivray, V. Turner, and M. Morales, “Worldwide and Regional Internet of Things (IoT) 2014-2020 Forecast: A Virtuous Circle of Proven Value and Demand,” pp. 1-27, May 2014.

[5] V. Gazis, K. Sasloglou, N. Frangiadakis, and P. Kikiras, “Wireless Sensor Networking, Automation Technologies and Machine to Machine Developments on the Path to the Internet of Things,” In Informatics (PCI), 2012 16th Panhellenic Conference, pp. 276-282, 2012.

[6] L. Foschini, T. Taleb, A. Corradi, and D. Bottazzi, “M2M-based metropolitan platform for IMS-enabled road traffic management in IoT,” IEEE Communications Magazine, vol. 49, no. 11, pp. 50-57, 2011.

[7] Y. Liu, C. Yuen, J. Chen, and X. Cao, “A Scalable Hybrid MAC Protocol for Massive M2M Networks,” arXiv preprint arXiv:1301.4315, 2013.

[8] G. Botter, J. Alonso-Zarate, L. Alonso, F. Granelli, and C. Verikoukis, “Extending the lifetime of M2M wireless networks through cooperation,” Communications (ICC), 2012 IEEE International Conference, 2012.

[9] Y. Zhang, R. Yu, S. Xie, W. Yao, Y. Xiao, and M. Guizani, “Home M2M networks: architectures, standards, and QoS improvement,” IEEE Communications Magazine, vol. 49, no. 4, pp. 44-52, 2011.

[10] Z.M. Fadlullah, M.M. Zubair, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, “Toward Intelligent Machine-to-Machine Communications in Smart Grid,” IEEE Communications Magazine, vol. 49, no.4, pp. 60-65, 2011.

[11] T. Adame, A. Bel, B. Bellalta, J. Barcelo, and M. Oliver, “IEEE 802.11AH: the WiFi approach for M2M communications,” IEEE Wireless Communications, vol. 21, no. 6, pp. 144152, Dec. 2014.

[12] B.H. Lee and S.L. Kim, “Mobility Control for Machine-to-Machine LTE Systems,” Wireless Conference 2011-Sustainable Wireless Technologies (European Wireless), 11th European VDE, pp. 1-5, 2011.

[13] IEEE WPAN Task Group 1, 2012, http://www.ieee802.org/15/pub/TG1.html.

[14] IEEE 802.15.4, “Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs),” IEEE, Sep. 2006.

[15] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: IEEE 802.11 Wireless Network Management, IEEE Std. 802.11v, 2011.

[16] K. Siwiak and D. McKeown, “Ultra-Wideband Radio Technology,” John Wiley & Sons Ltd., 2004.

[17] “Freescale, motorola pull out of uwb Forum, ” http://www.eetimes.com/electronics-news/4059719/Freescale-Motorola-pull-out-of-UWB-Forum

[18] M. Kohvakka, M. Kuorilehto, M. Hannikainen, and T. D. Hamaalainen, “Performance analysis of ieee 802.15.4 and zigbee for large-scale wireless sensor network applications,” PE-WASUN ’06, pp. 48-57, USA, 2006.

[19] “Dash7, ” http://www.dash7.org

[20] “OpenZwave. (n.d.). Retrieved June 2013, from openzwave, ” https://code.google.com/p/openzwave

[21] P. Sthapit and J.Y. Pyun, “Medium reservation based sensor MAC protocol for low latency and high energy efficiency,” Telecommun. Syst., vol. 47, no. 3-4, Aug. 2011.

[22] Y.T. Park, P. Sthapit, and J.Y. Pyun, “ Smart digital door lock for the home automation,” In TENCON 2009-2009 IEEE Region 10 Conference, pp. 1-6, 2009.

[23] P. Sthapit and J.Y. Pyun, “Intelligent network synchronization for energy saving in low duty cycle MAC protocols,” In WoWMoM 2009, pp. 1-6, 2009.

[24] Y.T. Park, P. Sthapit, and J.Y. Pyun, “ Energy Efficient Data Fragmentation for Ubiquitous Computing,” The Computer Journal, 2013.

[25] K. Zen, D. Habibi, and I. Ahmad, “Improving Mobile Sensor Connectivity Time in the IEEE 802.15.4 Networks,” Proc. of Telecommunication Networks and Applications Conference (ATNAC), pp. 317-320, 2008.

[26] F. Bashir, W.S. Baek, P. Sthapit, D. Pandey, and J.Y. Pyun, “Coordinator Assisted Passive Discovery for Mobile End Devices in IEEE 802.15.4,” Proc. of IEEE CCNC, pp. 601-604, Jan. 2013.

[27] J. Caldeira, J. Rodrigues, and P. Lorenz, “Intra-Mobility Support Solutions for Healthcare Wireless Sensor Networks-Handover Issues,” Sensor Journal, vol. 33, pp. 4339-4348, Jun. 2012.

[28] L. X. Hung, et al., “Secured WSN-integrated cloud computing for u-life care,” Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE, 2010.

[29] J. J. Jung, “Knowledge Distribution via Shared Context between Blog-based Knowledge Management Systems: a Case Study of Collaborative Tagging,” Expert Systems with Applications, vol. 36, no. 7, pp. 10627-10633, 2009.

[30] B. Gargi, et al., “Network assisted mobility support for 6LoWPAN.,” Consumer Communications and Networking Conference, 2009 CCNC 6th IEEE, 2009.

[31] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, K.S. Kwak, “A comprehensive survey of wireless body area networks: On PHY, MAC, and Network Layers Solutions,” J. Med. Syst, vol. 36, pp. 1065-1094, Jun. 2012.

[32] X. Liang and I. Balasingham, “Performance analysis of the IEEE 802.15.4 based ECG monitoring network,” in Proc. of the 7th IASTED WOC, Canada, pp. 99-104, May 2007.

[33] M.S. Gast, “802.11 Wireless Networks: The Definitive Guide,”, 2nd Edition . O’Reilly Media, Apr. 2005.

[34] P. Sthapit, Y.S. Choi, G.R. Kwon, S.S. Hwang, and J.Y. Pyun, “A Fast Association Scheme over IEEE 802.15.4 based Mobile Sensor Network,” Proc. of ICWMC 2013, Jul. 2013.

[35] P. Sthapit and J.Y. Pyun, “Mobility Support in IEEE 802.15. 4 Based Mobile Sensor Network,” IEICE Transactions on Communications, vol. 97, no. 3, pp. 555-563, 2014.

[36] A. Willig, N. Karowski, and J.H. Hauer, “Passive discovery of IEEE 802.15.4-based body sensor networks,” Ad Hoc Networks 8, no. 7, pp. 742-754, 2010.

[37] N. Karowski, A.C. Viana, and A. Wolisz, “Optimized asynchronous multichannel discovery of IEEE 802.15.4-based wireless personal area networks,” Mobile Computing, IEEE Transactions on, vol. 12, no. 10, pp. 1972-1985, 2013.

[38] C. Chaabane, A. Pegatoquet, M. Auguin, and M.B. Jemaa, “Energy optimization for mobile nodes in a cluster tree IEEE 802.15.4/ZigBee network,” In Computing, Communications and Applications Conference (ComComAp), pp. 328-333, 2012.

[39] N. F. Timmons and W. G. Scanlon, “Analysis of the performance of IEEE 802.15.4 for medical sensor body area networking,” Proc. of IEEE SECON, pp. 16-24, Oct. 2004.

[40] P. Sthapit and J.Y. Pyun, “Passive synchronization based energy-efficient MAC protocol over M2M wireless networks,” International Journal of Distributed Sensor Networks, 2013.

[41] N. F. Timmons and W.G. Scanlon,“An adaptive energy efficient MAC protocol for the medical body area networks,” Proc. of IEEE Wireless VITAE, pp. 587-593, May 2009.

[42] Y. Huang, A. Pang, and H. Hung, “A Comprehensive Analysis of Low-Power Operation for Beacon-Enabled IEEE 802.15.4 Wireless Networks,” IEEE Trans. on Wireless Communications, vol. 8, no. 11, pp. 5601-5611, 2009.

[43] S. A. Gopalan, and J.T. Park, “Energy-efficient MAC protocols for wireless body area networks: Survey,” Proc. ICUMT, pp. 739-744, Oct. 2010.

[44] F. Silva, C. Branquinho, and M. Assumpcao, “Mobility Impact on IEEE 802.15.4 Network through a Simulation Platform,” IEEE Latin America Transactions, vol. 9, no. 5, pp. 655-652, 2011.

[45] K. Zen, D. Habibi, A. Rassau, and I. Ahmad, “Performance evaluation of IEEE 802.15.4 for mobile sensor networks,” Proc. of the 5th IEEE WOCN ’08, India, pp. 1-5, May 2008.

[46] IEEE P802.15.4e-2012, “Part 15.4: Low-Rate Wireless Personal Area Networks (WPANs), Amendment 1: MAC sub-layer,” Feb. 2012.

[47] F. Zhang, F. Wang, B. Dai, and Y. Li, “Performance Evaluation of IEEE 802.15.4 Beacon-enabled Association Process,” In Advanced Information Networking and Applications Workshops, pp. 541-546, Mar. 2008.

[48] N. Karowski, A.C. Viana, and A. Wolisz, “Optimized Asychronous Multi-channel Neighbor Discovery,” Proc. of Infocom, pp. 536-540, 2011.

[49] N. Karowski, A.C. Viana, and A. Wolisz, “Optimized asynchronous multi-channel neighbor discovery,” In INFOCOM, 2011 Proceedings IEEE, pp. 536-540, 2011.

[50] P. Sthapit and J.Y. Pyun, “Handover Strategies in Beacon-Enabled Mobile Sensor Network,” International Journal of Distributed Sensor Networks, 2014.

[51] F. Osterlind and A. Dunkels, “Approaching the maximum 802.15.4 multi-hop throughput,” Proc. of 5th ACM Workshop Embedded Netw. Sens., pp. 1-6, June 2008.

[52] E. Toscano and L.L. Bello, “Multiplechannel Superframe Scheduling for IEEE 802.15.4 Industrial Wireless Sensor Networks,” IEEE Trans. on Industiral Informatics., vol. 8, no. 2, pp. 337-350, May 2012.

[53] B.Y. Shih, C.J. Chang, A.W. Chen, and C.Y. Chen, “Enhanced MAC channel selection to improve performance of IEEE 802.15.4,” International Journal of Innovative Computing, Information and Control, vol.6, no.12, pp.5511-5526, 2010.

[54] F. Meng and Y. Han, “A New Association Scheme of IEEE 802.15.4 for Real-time Applications,” Proc. of Wireless Communications, Networking and Mobile Computing, pp. 1-5, 2009.

[55] C. Chaabane, C. Pegatoquet, M. Auguin, and M. D. Jemaa, “Energy optimization for mobile nodes in a cluster tree IEEE 802.15.4/ZigBee network,” Proc. of IEEE Computing, Communications and Applications Conference (ComComAp), pp. 328-333, 2012.

[56] Texas Instrument, CC2420 Data Sheet,
http://www.ti.com/lit/ds/symlink/cc2420.pdf.

[57] J. Berg, “The IEEE 802.11 Standardization, its History, Specifications, Implementations and Future,” Graduate Program in Telecommunications, Gorge Mason University, Vermont, USA

[58] Wi-Fi Alliance. Online: http://www.wi-fi.org/

[59] P. Roshan and J. Leary, “802.11 Wireless LAN Fundamentals Cisco Press,” 2003.

[60] J.D. Day, and H. Zimmermann, “The OSI Reference Model,” Proceedings of the IEEE, vol. 71, no. 12, pp. 1334-1340, 1983.

[61] W. R. Stevens, “TCP/IP Illustrated, Volume 1: The Protocols,” Addison-Wesley, 1994.

[62] G. A. Halls, “HIPERLAN-the Mbit/s Radio LAN,” in Proc. Radio LANs and MANs, pp. 1-8, Apr. 1995.

[63] Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements. ANSI/IEEE Std 802.11e-2005, IEEE, Nov. 2005.

[64] Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 5: Spectrum and Transmit Power Man-

agement Extensions in the 5 GHz band in Europe. ANSI/IEEE Std 802.11h-2003, IEEE, Oct. 2003.

[65] V. Vermeer, “Wireless LANs: Why IEEE 802.11 DSSS,” in Proc. Wescon, pp. 172-178, Nov. 1997

[66] G. R. Hiertz, D. Denteneer, L. Stibor, Y. Zang, X. P. Costa, and B. Walke, “The IEEE 802.11 Universe,” IEEE Communications Magazine, vol. 48, no. 1, pp. 62-70, Jan. 2010.

[67] B. J. Kwak, N. O. Song, and L. E. MillerPerformance Analysis of Exponential Backoff,” IEEE/ACM Trans. Netw., vol. 13, no. 2, pp. 343-355, Apr. 2005.

[68] S. Aust, R. V. Prasad, and I. G. Niemegeers, “IEEE 802.11 ah: Advantages in standards and further challenges for sub 1 GHz Wi-Fi,” In Communications (ICC), 2012 IEEE International Conference, pp. 6885-6889, Jun. 2012.

[69] Y. Zhou, H. Wang, S. Zheng, and Z.Z. Lei, “Advances in IEEE 802.11 ah standardization for machine-type communications in sub-1GHz WLAN,” In Communications Workshops (ICC), 2013 IEEE International Conference, pp. 1269-1273, Jun. 2013.

[70] E. Khorov, A. Lyakhov, A. Krotov, and A. Guschin, “ A survey on IEEE 802.11 ah: An enabling networking technology for smart cities,” Computer Communications, vol. 58, pp. 53-69, 2015.

[71] R.D. Vegt, “Potential compromise for IEEE 802.11ah use case document,” IEEE 802.11-11/0457r0, Mar. 2011.

[72] X. Liu, “On the Deployment of Wireless Data Back-haul Networks,” University of California, Davis, CA.

[73] S. Dimatteo, P. Hui, B. Han, O. K. Li. Victor, “Cellular Traffic Offloading through Wi-Fi Networks,” IEEE 8th International Conference on Mobile Ad-Hoc and Sensor Systems, MASS 2011, Valencia, Spain, Oct. 2011.

[74] “802.11ac: The Fifth Generation of Wi-Fi, Technical White Paper,” CISCO Systems, Inc., San Jose, 2014.

[75] IEEE Std 802.11n -2009 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancement for Higher Throughput, 2009.

[76] W. Sun, M. Choi, and S. Choi, “IEEE 802.11ah: A long range 802.11 waln at sub 1 ghz,” in Journal of ICT Standardization , vol. 1, pp. 83-107, May 2013.

[77] T. Adame, A. Bel, B. Bellalta, J. Barcelo, J. Gonzalez, and M. Oliver, “Capacity analysis of IEEE 802.11 ah WLANs for M2M communications,” In Multiple Access Communcations, pp. 139-155. Springer International Publishing, 2013.

[78] IEEE P802.11ah Draft Ver.1.2, IEEE Std. 802.11 TGah, 2014

[79] L. Zheng, L. Cai, J. Pan, and M. Ni, “Performance Analysis of Grouping Strategy for Dense IEEE 802.11 Networks,” Proc. of IEEE GLOBECOM’13, pp. 1-6, 2013.

[80] “Supporting of the Authentication/Association for Large Number of Stations,” https://mentor.ieee.org/802.11/dcn/12/11-12-0112-04-00ah-supporting-of-the-authentication-association-for-large-number-ofstations.pptx

[81] D. Bankov, E.E. Khorov, and L. Andrey , “The Study of the Centralized Control Method to Hasten Link Set-up in IEEE 802.11 ah Networks,” 21th European Wireless Conference, VDE, pp. 1-6, 2015.

[82] P. Sthapit, S. Subedi, G.R. Kwon, S.S. Hwang, and J.Y. Pyun, “Performance Analysis of Association Procedure in IEEE 802.11ah,” ICSNC 2015 : The Tenth International Conference on Systems and Networks Communications, pp. 70-73, Nov. 2015.

[83] G. F. Toth, “Thinnest covering of a circle by eight, nine, or ten congruent circles.,” Combinatorial and computational geometry , vol. 52, pp. 361-376, 2005.

[84] C. W. Park, D. Hwang, and T.J. Lee,“Enhancement of IEEE 802.11 ah MAC for M2M Communications,” IEEE Communications Letters, vol. 18, no. 7, pp. 1151-1154, 2014.

[85] G. Bianchi, “Performance analysis of the IEEE 802.11 distributed coordination function,” IEEE Journal on Selected Areas in Communication, vol. 18, no. 3, pp. 535-547, 2000.

[86] P. Chatzimisios, A.C. Boucouvalas, and V. Vitsas , “Packet delay analysis of IEEE 802.11 MAC protocol,” Electronics Letters, vol. 39, no. 18, pp. 1358-1359, 2003.

[87] H. Wu, Y. Peng, K. Long, S. Cheng, and J. Ma, “Performance of reliable transport protocol over IEEE 802.11 wireless LAN: analysis and enhancement,”In INFOCOM 2002, pp. 599-607, 2002.

[88] M. J. Handy, M. Haase, and D. Timmermann, “Low energy adaptive clustering hierarchy with deterministic cluster-head selection,’ In Mobile and Wireless Communications Network, 2002. 4th International Workshop, pp. 368-372, 2002.

[89] P. Chatzimisios, A.C. Boucouvalas, and V. Vitsas , “Influence of channel BER on IEEE 802.11 DCF,” Electronics Letter, vol. 39, no. 23, pp. 1687-1689, 2003.

[90] NS2: http://nsnam.isi.edu/nsnam/index.php/main page.

Acknowledgement

The completion of this thesis owes a great deal to the help of the people around me. I would like to express my sincere gratitude to my advisor, Prof. Jae-Young Pyun for his invaluable support, encouragement, supervision, personal guidance, and useful suggestions throughout the course of my research. Working with Prof. Pyun for the last seven years has been a great learning experience which I believe would be very useful to take the future career assignments in a very confident way. I am also thankful to all the Professors of Information and Communication Engineering Department from whom I have learnt great deal of knowledge.

My sincere thanks to committee members, Prof. Goo-Rak-Kwon, Prof. Seung-Jo Han, Prof. Euisung Kang, Sunchon National University, and Dr. Jeong-Gi Lee, KETI research center, for their detail review, constructive criticism and excellent advice during the preparation of this thesis. Likewise, I would like to thank all anonymous reviewers at different leading international conferences and reputed journals for their time and efforts they spend in giving valuable feedbacks for the manuscripts that I have submitted for possible publication. Their suggestions have certainly raised the quality of those manuscripts, which are the foundation of this dissertation.

Furthermore, I would like to express my gratitude to all my lab mates of Wireless and Mobile Communication System and to all the friends in Korea for their warm friendship, cooperation and support and making my stay memorable.

I am as ever, especially indebted to my parents and family for their love, support, and encouragement in every moment of my life. I also wish to thank them for their understanding during my study.

The financial support of Korean Government, Ministry of Education, Korean Government Scholarship Program (KGSP), and Chosun University is greatly acknowledged.