공학박사 학위논문

A study for the construction of large-scale, low-power wireless sensor networks

대규모 저전력 무선 센서 네트워크를 구축하는 방법에 관한 연구

2023 년 8 월

서울대학교 대학원

전기·정보공학부

방 재 석

A study for the construction of large-scale, low-power wireless sensor networks

대규모 저전력 무선 센서 네트워크를 구축하는 방법에 관한 연구

지도교수 심 병 효

이 논문을 공학박사 학위논문으로 제출함

2023 년 8 월

서울대학교 대학원

전기·정보공학부

방 재 석

방재석의 공학박사 학위논문을 인준함

2023 년 8 월

위 원 장	박 세 웅	(인)
부위원장	심 병 효	(인)
위 원	이 용 환	(인)
위 원	신 요 안	(인)
위 원	최 지 웅	(인)

Abstract

The arrival of the Internet of Things (IoT) era has opened a new way of living by connecting the physical and the virtual domains as a single domain. Wireless sensor networks (WSNs) may play a key role for combining the two domains in a very efficient manner. A number of technologies have been developed for the deployment of WSNs, in consideration of IoT services in various operation environments. The primary concern on WSN operation is the provision of connectivity that can provide reliable and seamless communications among devices. ZigBee and Bluetooth Low Energy (BLE), low-power connectivity technologies, have widely been applied to IoT services. However, they may not provide desired performance when applied to large-scale IoT service environments. It is of great concern to develop wireless connectivity technologies that can provide desired performance in commercial IoT service environments.

In this dissertation, we consider low-power connectivity technologies in large-scale IoT service environments. We first investigate the connectivity problem of legacy ZigBee in a multi-hop tree-structured networking configuration that may not provide full connectivity in large-scale environments. We may improve the connectivity problem by focusing on device selection and resource allocation for routers. We make devices join the network as an end device in the first stage. Then, parent devices convert some of their child end devices to their child router devices in consideration of geographical network expansion. The resource is allocated to routers in consideration of data traffic and addressing parameters, improving the throughput and latency performance, while preserving the network scalability.

We also investigate the connectivity of BLE with adaptive frequency hopping in the presence of co-channel interference (CCI). We consider the reduction of time for the detection of CCI by means of channel grouping, where devices operate using a single channel group in the normal operation. Upon the detection of severe CCI, the devices may operate using multiple channel groups to find a channel group least affected by CCI. By fast detecting severe CCI and fast investigating the frequency band, the proposed scheme may maintain connectivity even in presence of rapidly time-varying CCI.

Finally, we verify the proposed schemes by means of extensive computer simulation and hardware implementation. The proposed schemes can significantly enhance the connectivity of ZigBee and BLE, improving the scalability, latency, memory footprint and power consumption.

Keywords: Internet of Things, large-scale low-power wireless sensor networking, network self-configuration, interference avoidance, ZigBee, Bluetooth low-energy

Student number: 2014-31069

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Recent advances in sensors, actuators, communications and semiconductor technologies have made the deployment of Internet of Things (IoT) services quite feasible in various application environments [1-3]. These IoT services may need to employ *open* and *generic* networking technologies that can accommodate various devices in various interface specifications. Wireless sensor networks (WSNs) may play a key role for IoT services by bridging the physical and the virtual domains, with lower deployment complexity and higher scalability than wired networks [3]. The deployment of commercial IoT services may need WSN technologies that can reliably provide networking performance, such as the connectivity, data transmission reliability, power consumption and deployment/operation cost, even in large-scale operation environments [4]. It has been a long-time challenge to develop WSN technologies that can provide reliable networking performance for IoT services.

The deployment and operation of commercial IoT services should consider the return-on-investment (RoI). Many of IoT services consider the use of unlicensed frequency bands for the networking to reduce the cost for deployment and operation. The operation in unlicensed frequency bands may require networking technologies that can provide reliable connectivity and communications among devices even in the presence of co-channel interference (CCI). Power consumption may be of another great concern especially when the IoT service needs battery-based operation. As these issues are closely related to each other, technical challenges may become even harder when operating in power-, complexity- and capacity-limited environments. ZigBee and Bluetooth Low Energy (BLE) technologies have widely been applied to IoT services in the past decade [5, 6]. They may quite be suitable in battery-powered operation environments with the use of low-duty cycle operation. However, they may not provide desired performance when applied to large-scale WSN environments.

ZigBee may not guarantee the full-node connectivity in large-scale service environments. Its first-come, first-serve (FCFS) strategy for the selection of routers may make the network configuration proceed to a certain direction, referred to biased networking problem [7, 8]. Previous studies on the router selection strategy have focused on the enhancement of link quality, rather than the improvement of the connectivity [9-11]. Furthermore, ZigBee provides no practical guidelines for resource allocation to routers [5, 12]. Since the resource allocation may directly affect the data transmission performance, it is of great concern to allocate orthogonal resources to routers to avoid so-called beacon collision problem and to adequately allocate the amount of resources according to the data traffic [13]. Although numerous studies have been conducted on the resource allocation for ZigBee [13-17], they did neither consider spatial reuse of communication resources [13, 14] nor distributed networking [15-17], making them impractical for application to large-scale WSNs. To the author's best knowledge, no practical solution has been proposed in consideration of selection and resource allocation for routers, especially in large-scale WSN environments. In practice, ZigBee is applicable to small-scale WSN environments [7, 18].

BLE, quite applicable to small-scale personal-area network environments [19-21], demonstrates potential for application to large-scale networking [22-26]. It may employ a frequency-hopping time-division multiple access (FH-TDMA) technique in the connection mode and an ALOHA technique in the connectionless mode. The connectionless mode (e.g., BLE Mesh) has been applied to large-scale networking environments [22- 24]. However, it may not provide desired networking performance mainly due to the use of ALOHA technology that may suffer from random access and hidden node collision [27]. In practice, BLE with the connectionless mode may not be suitable for large-scale, low-power networking environments. BLE with the connection mode [25, 26] may also suffer from unstable networking (e.g., link disruption), especially in the presence of CCI when applied to large-scale networking environments [28]. Since the occurrence of a single link disruption may seriously affect the entire network operation, the effect of link disruptions may seriously be of great concern as the network size increases. Numerous studies have considered the avoidance of interference in Classic Bluetooth systems by means of adaptive frequency hopping (AFH) [28-34]. However, they may not be applicable to BLE whose operation frequency is quite lower than Classic Bluetooth. AFH schemes reliant on channel quality measurements on each channel have been developed for BLE [35-38]. However, they may take a long-time making the measurement. In presence of rapidly time-varying CCI, they may suffer from the link disruption problem as well as sub-optimal performance due to the outdated information.

In this dissertation, we consider the networking in large-scale low-power WSN environments. We investigate the biased networking and the beacon collision problem of ZigBee and the link disruption problem of BLE in large-scale low-power WSN environments. We design practical and implementable solutions that may provide desired connectivity performance.

We consider the biased networking and the beacon collision problem in legacy ZigBee when applied to large-scale network environments. We may alleviate the biased networking problem by making the parent node pick routers that have potential to expand the networking area. We also consider the resource allocation to routers to reduce the beacon collision. We determine the length and the time-offset of resource according to data traffic to improve the throughput while reducing the latency, without sacrificing scalability.

We also consider the link disruption problem in BLE with the connection mode in the presence of CCI. We propose fast detection of CCI to handle rapidly time-varying CCI. The fast detection of CCI may suffer from potential detection errors due to infrequent operation of BLE in the connection mode. We may reduce the detection error by making devices use a group of adjacent channels and gather channel quality statistics on the group in the normal operation. Upon the detection of severe CCI, we make devices use multiple channel groups to find a channel group least affected by CCI. We further consider the improvement of connectivity even in the presence of transmission failure of AFH command frames. The operation in a channel-group basis may require minimal memory for the collection of channel quality statistics and reduce the computational overhead for the AFH operation, while providing desired connectivity performance.

Following Introduction, Chapter 2 describes the system model in consideration. Chapter 3 proposes a network construction scheme for ZigBee, quite applicable to large-scale WSN environments. Chapter 4 describes a frequency hopping scheme for BLE that can fast detect and avoid the CCI. Finally, conclusions and further works are summarized in Chapter 5.

Chapter 2

System model

2.1. Multi-hop cluster-tree structured networks

We consider a cluster-tree structured network comprising a coordinator, routers and end devices, as illustrated in Fig. 2-1. The coordinator may work as a sink when the data is collected and a gateway to outside network. For a pair of devices connected directly, a device that has a network depth (i.e., the number of hops between the device and the coordinator) less than the other is defined as a parent device, and the other is defined as a child device. Router may have their child devices. For example, the coordinator operates only as a parent, an end device operates only as a child device and a router may operate as both a parent and a child device. The coordinator and routers can be a cluster head of clusters consisting of them and their child devices. The clusters are connected in a tree structure, yielding a cluster-tree structured network.

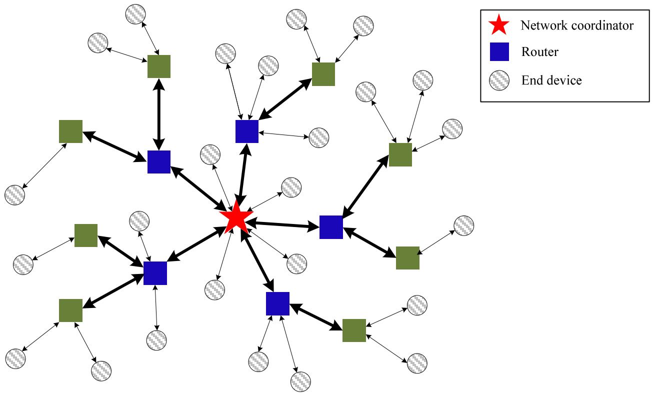


Fig. 2-1. Cluster-tree structure

2.2. Co-channel interference

Low-power WSNs operating in unlicensed frequency band may noticeably be affected by the presence of CCI like IEEE 802.11x wireless local area network (WLAN) traffic [39-43]. The channel occupancy ratio (COR) of WLAN signal, defined by the portion of time that WLAN signal presents, may significantly vary over the time even in a time scale of minutes [44]. It may be desirable for low-power WSNs to employ a transmission scheme that can effectively avoid major interference [34, 42, 43]. We may design such a transmission scheme by exploiting the COR of WLAN signal.

The WLAN traffic workload can be characterized by so-called sessions that represent WLAN users, the number of traffic flows generated by a session and the inter-arrival time between the traffic flows [45]. The arrival of sessions can be represented by a time-varying Poisson process and the traffic flow arrival by a bi-Pareto distribution [45]. It may well characterize large-scale behavior of WLAN channel occupancy, but it may not well characterize the inter-arrival time of WLAN signal since it does not consider the medium access control (MAC) of WLAN.

The WLAN channel occupancy can be represented using a single-layer semi-Markovian process in consideration of WLAN MAC [46, 47], where the transition between the states is deterministic and depends on the data size, as illustrated in Fig. 2-2. The medium may be in an idle state when WLAN devices are in a back-off state to avoid collision or has no data to transmit, referred to free-time (FT).

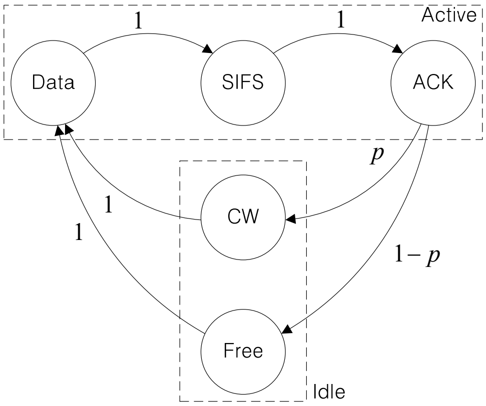


Fig. 2-2. Semi-Markovian channel occupancy model [46, 47]

The probability density function (pdf) of the sojourn time in the idle state can be represented as [46]

$$f_I(\tau) = pf_C(\tau) + (1-p) f_F(\tau) \tag{2.1}$$

where $p \in [0,1]$ is a mixture variable, $f_C(\tau)$ denotes the pdf of the contention window for random back-off that follows uniform distribution, and $f_F(\tau)$ denotes the pdf of FT. Here, $f_C(\tau)$ follows an uniform distribution due to selection of CW of WLAN. Considering the transmission characteristics of WLAN signal, $f_F(\tau)$ can be represented using a heavy-tailed pdf which has longer tail than the exponential distribution (ED) (e.g., GPD) as [46]

$$f_F(\tau) = \frac{1}{\sigma}\left(1 + \xi \frac{\tau}{\sigma}\right)^{-1-1/\xi} \tag{2.2}$$

where the shape parameter ξ and the scale parameter σ depends on WLAN traffic. It was shown that the semi-Markovian modeling of WLAN channel occupancy is effective for statistical characterization of WLAN signal [46, 48]. However, the semi-Markovian modeling may not effectively characterize time-varying nature of WLAN signal due to the use of fixed shape and scale parameters.

Based on characterization of WLAN users [49], we may assume that the usage pattern of WLAN users is similar to each other and that the COR of WLAN signal is a function of the number of WLAN users, which solely depends on the arrival/departure of WLAN users. We may characterize the inter-arrival time by an ED parametrized by the time-varying COR of WLAN signal, achieving heavy-tail characteristics. The memoryless property of ED makes it easy to analyze and simulate the WLAN signal.

We may represent the WLAN channel occupancy in a two-layer process as illustrated in Fig. 2-3, where the upper and the lower layer process represent the arrival/departure of WLAN users and the generation of WLAN signal, respectively. The arrival and departure of WLAN users can be represented by a Poisson process since WLAN users may come in and out independently of each other. The number of WLAN users at time t, denoted by n_t, can be represented by an M/M/m/m queueing process with parameters λ_A and μ_D, representing the arrival rate and the departure rate of WLAN users, respectively. Letting $N_C^{\max}$ be the maximum number of WLAN users, it can be shown that the average number of WLAN users can be represented as [50]

$$\bar{N}_C = \frac{\sum_{n=0}^{N_C^{\max}} n\left(\lambda_A/\mu_D\right)^n / n!}{\sum_{n=0}^{N_C^{\max}} \left(\lambda_A/\mu_D\right)^n / n!}. \tag{2.3}$$

Letting $\rho_t = \xi(n_t)$ be the COR of WLAN signal at time t and $\xi(n) = \rho_C n$, the average COR of WLAN signal in the steady state can be represented as $\bar{\rho} = \rho_C \bar{N}_C$.

The lower layer process can be represented as a two-state semi-Markovian process where the state "Active" represents Data, SIFS and ACK, and the state "Idle" represents CW and FT [47]. Since WLAN signal is present only in Active state, the duration of Active state depends on the size of WLAN packets [45]. Provided that the sojourn time of Active state does not significantly vary in time, the sojourn time of Idle state (i.e., the inter-arrival time of WLAN signal) can be represented by an ED with mean $\lambda_I^{-1}(t)$. Letting $\overline{T}_A$ be the average time duration of Active state, the COR of WLAN signal at time t can be represented as

$$\begin{aligned}\rho(t) &= \rho_C n_C(t) \\ &= \frac{\overline{T}_A}{\overline{T}_A + \lambda_I^{-1}(t)}\end{aligned} \tag{2.4}$$

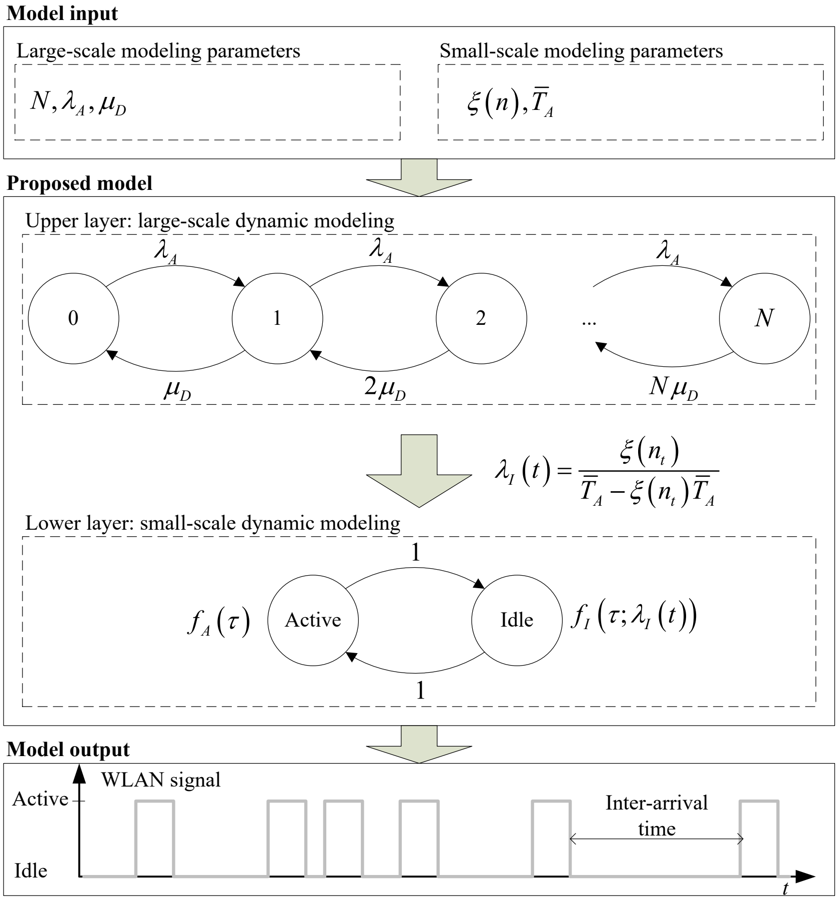
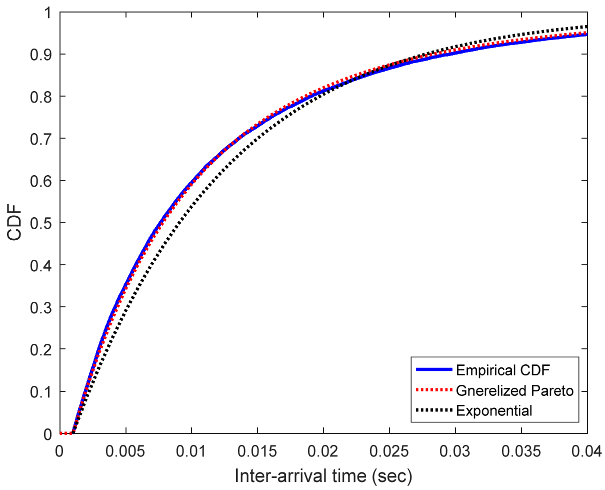


Fig. 2-3. Proposed time-varying WLAN traffic model

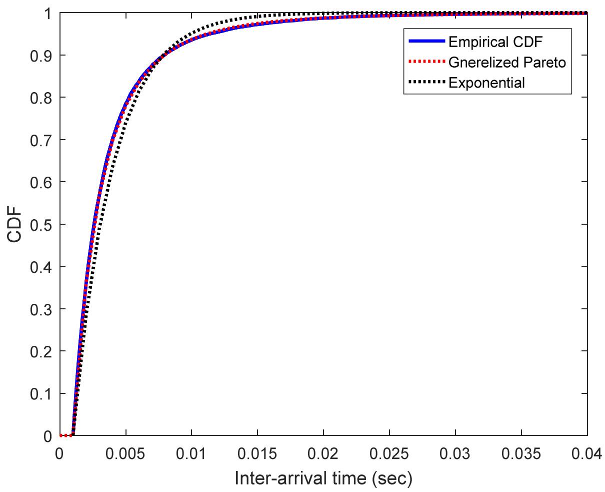
We evaluate the validity of the proposed model by computer simulation. Table I summarizes parameters of the proposed model for the evaluation, where we assume that the arrival rate is once a 30-second, which may represent a highly dynamic operation scenario. We generate the WLAN signal for an interval of 104 seconds. To verify the validity of the proposed model, we perform Kolmogorov-Smirnov test on the empirical distribution of inter-arrival time of WLAN signal and the GPD fitting [51].

Fig. 2-4 depicts the empirical CDF when $\bar{\rho} = 0.1$ and $\bar{\rho} = 0.3$. The fitting parameters and its goodness-of-fit of GPD are summarized in Table 2. It can be seen that the empirical distribution is well approximated by a GPD. It can also be seen that the GPD fitting works well when $\bar{\rho} = 0.3$ because the variance of COR of WLAN signal increases as $\bar{\rho}$ increases, which agrees well with the result in [48].

Fig. 2-5 and Fig. 2-6 depict WLAN signal generated by the proposed model and the single-layer semi-Markovian model [47], respectively, where (a) depicts the COR of WLAN signal measured in one-second bins, and (b) and (c) depict the presence of WLAN signal when the measured COR of WLAN signal is the highest and the lowest, respectively. It can be seen that the inter-arrival time of WLAN signal generated by the two models may well be approximated by a GPD in a long-time interval. It can also be seen that the proposed model generates WLAN signal showing time-varying nature of COR of WLAN signal, while the single-layer semi-Markovian model does not.



(a) $\bar{\rho} = 0.1$



(b) $\bar{\rho} = 0.3$

Fig. 2-4. Empirical CDF of inter-arrival time of WLAN signals and its generalized Pareto and exponential fits

Table 2-1. Fitting parameters for GPD over the distribution of inter-arrival time of WLAN signal

$\bar{\rho}$	0.1	0.2	0.3
Fitted parameters of generalized Pareto distribution			
ξ	0.2256	0.2609	0.3024
σ	0.0091	0.0036	0.0021
Goodness-of-fit under Kolmogorov-Sminorv test			
p-value	0.0040	0.2873	0.7165
D-value	0.0134	0.0073	0.0050

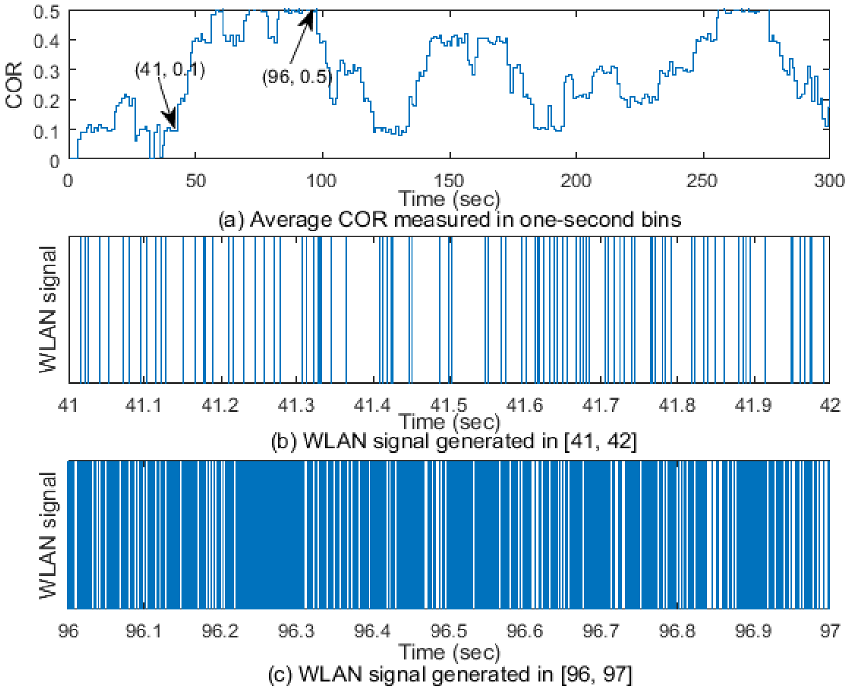


Fig. 2-5. WLAN signal generated by the proposed model with $\bar{\rho} = 0.3$

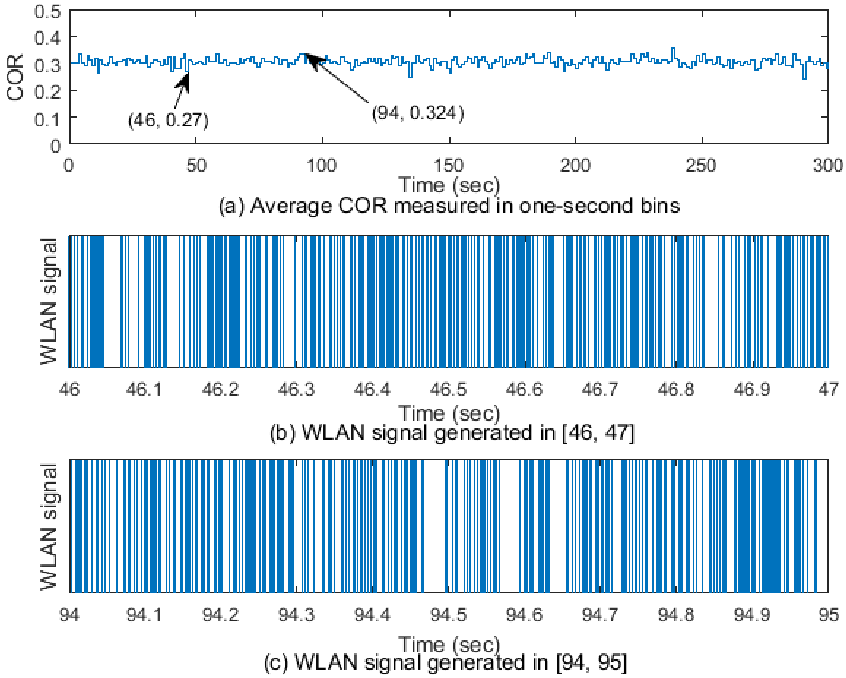


Fig. 2-6. WLAN signal generated by [47] with $\bar{\rho} = 0.3$

Chapter 3

Construction of large-scale low-power wireless sensor networks

In this chapter, we consider the biased networking and the beacon collision problem of ZigBee employing IEEE 802.15.4 beacon-enabled mode [12]. Legacy ZigBee may have a tendency of network construction to a certain direction, referred to biased networking, hampering full node connection and networking expansion. We also consider the collision among super-fames in multi-hop tree-structured networking environments.

We may alleviate the biased networking problem by making devices join the network as an end device and then making the parent node select routers among its child end devices that has a potential to geographically expand the network, referred to scalable child router selection (SCRS). We may also alleviate the beacon collision problem by orthogonally allocating the super-frame of clusters in the time/frequency domain in consideration of data traffic, referred to traffic-aware super-frame scheduling (TASS). The TASS exploits the super-frame schedule of two-hop neighboring clusters to reduce collision among the super-frames of clusters that have the same network depth. It determines the length and the time offset of the super-frame in consideration of data traffic and addressing parameters to increase the throughput with low latency, while preserving the scalability. The router selection and the resource allocation procedures are organized into a single on-line algorithm that may be executed in a distributed manner, making it suitable for real-world implementations.

3.1. ZigBee over IEEE 802.15.4

ZigBee can construct a large-scale network of up to 65,535 devices as a single network by means of multi-hop cluster-tree structured networking protocols [5, 12]. ZigBee can operate with the IEEE 802.15.4 technology that can operate in beacon-enabled or non-beacon-enabled mode. The beacon-enabled mode allows devices to make communications only in the active period, saving the power consumption by putting the device in an idle status in the inactive period. It can employ a time division multiple access (TDMA) technique to improve the throughput performance, while supporting bounded latency in a multi-hop cluster-tree structured network [52-54]. The non-beacon-enabled mode does not make use of duty-cycling, requiring routers powered in all time. It may suffer from so-called hidden-node and random-access collision [27], yielding poorer throughput performance than the beacon-enabled mode.

As illustrated in Fig. 3-1, a cluster head r can make synchronized communications with its child devices by means of periodic transmission of beacon frames. After transmitting a beacon frame, it can communicate with its child devices during its super-frame. The duration of the beacon interval and the super-frame of cluster head r can be represented as, respectively,

$$T_{BI,r} = aBSD \times 2^{BO_r} t_{sym} \tag{3.1}$$

$$T_{SD,r} = aBSD \times 2^{SO_r} t_{sym} \tag{3.2}$$

where $aBSD$ denotes a base super-frame duration, BO_r and SO_r respectively denotes the beacon order (BO) and the super-frame order (SO) of the beacon interval and the super-frame of cluster head r.

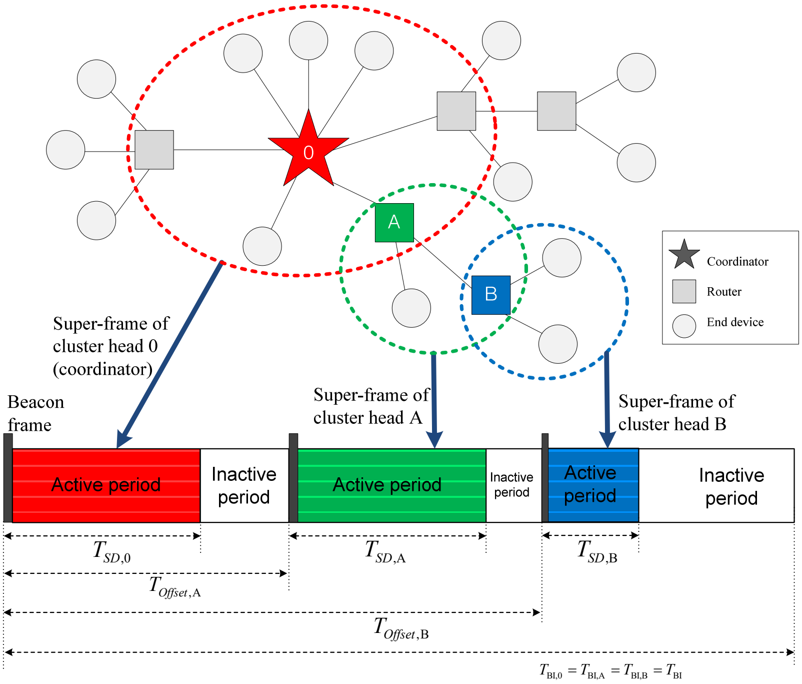


Fig. 3-1. An example of a cluster-tree structured network using IEEE 802.15.4 beacon-enabled mode

3.2. Previous works

A number of studies have been conducted to construct large-scale networks by using ZigBee in the IEEE 802.15.4 beacon-enabled mode [7, 8, 55-59]. Few works have considered the scalability issue of ZigBee in IEEE 802.15.4 beacon-enabled mode.

ZigBee can construct a cluster-tree structured network by using a distributed address allocation mechanism (DAAM) [5]. DAAM introduces a trade-off between the breadth and depth of a cluster-tree structured network, imposing limitation on the number of child devices that a parent device may adopt [55, 56]. As DAAM makes a parent device select those limited number of child devices in an FCFS manner, the selected child devices may not be evenly distributed. This may make the cluster-tree structure network predominantly expand in a specific geographical direction, referred to the biased networking problem [8, 9]. A stochastic address allocation mechanism (SAAM) may alleviate the biased networking problem by making parent devices randomly assign the network addresses to their child devices, eliminating the restriction on the maximum number of child devices [5]. However, SAAM may require to verify the uniqueness of assigned addresses by means of broadcasting, resulting in significant increase of signaling overhead, referred to broadcast storm problem [57, 58]. It also requires a routing algorithm like the Ad Hoc on Demand Distance Vector (AODV), further increasing the signaling overhead. As an alternative approach, 6LoWPAN employs a Duplicate Address Detection (DAD) technique [59]. The DAD makes a parent device assign random network addresses to its child devices and makes a network coordinator verify the uniqueness of the allocated address, requiring two-way multi-hop communications. However, it may require considerable signaling overhead verifying the uniqueness of allocated addresses and necessitates the use of complex routing mechanisms such as AODV. In practice, SAAM and DAD have not been applied to large-scale WSN environments.

Multi-step DAAM (M-DAAM) is an improvement of DAAM that may effectively mitigate the trade-off between the breadth and the depth of cluster-tree structured networks by adjusting the addressing parameters of DAAM in a multi-step manner [7]. The approach proposed in [7] further introduced a child selection scheme where the parent device chooses child devices with the fewest potential parents as their child routers. However, in high-density network environments, child devices may have the same number of potential parents, regardless of whether they are in the propagating position (i.e., located farther away from the parent device in the coordinator's view) or not. In such environment, the child selection scheme may lead to waste of network depth, failing to achieve the full-node connectivity.

ZigBee simply suggests the use of IEEE 802.15.4 beacon-enabled mode for unique allocation of a super frame to each cluster in cluster-tree structured network environments [5]. The IEEE 802.15.4b amendment introduces the concept of beacon-only period (BOP) for application of the beacon-enabled mode to large-scale networking environments. Beacon frames from multiple clusters can be transmitted in the BOP [14]. However, the IEEE 802.15.4b amendment does not specify how to set key parameters.

A time division beacon scheduling (TDBS) scheme may alleviate the beacon collision problem by means of setting the time offset of super frames using a pinwheel algorithm, enabling an individual super-frame configuration for each cluster [13, 60]. However, TDBS does not consider spatial reuse of time and frequency resource and data traffic, making it unsuitable for large-scale WSN environments. A two-way beacon scheduling (TWBS) scheme may take account of the data traffic, focusing on the latency of uplink and downlink data traffic [15]. TWBS enables each cluster to have two active periods, namely an uplink active period and a downlink active period, in a single beacon interval. The time offset of these active periods is set to minimize end-to-end latency. However, TWBS did not consider the amount of the data traffic. Both TDBS and TWBS operate in a centralized manner, yielding large signaling and computational overhead.

3.2. Proposed self-configuration scheme

The aforementioned scalability issues, namely the biased networking and the beacon collision problem, may not be solved individually, as a selection of a router and resource allocation for a router may not be independently executed. In this section, we consider a self-configuration procedure comprising the proposed SCRS and TASS, as illustrated in Fig. 3-2.

A network-joining device k scans communication channels to find nearby cluster head. During the scanning, it collects a set of super-frame schedules of nearby clusters, denoted by $\mathbf{B}_k$, and a set of potential parents, denoted by $\mathbf{P}_k$. Then, it selects a device in $\mathbf{P}_k$ as a potential parent device, say r. It initiates the network joining by transmitting an association request message to the potential parent r, with $\mathbf{B}_k$ for TASS and with $|\mathbf{P}_k|$ and $I_{revert,k}$ for SCRS. Here, $|\mathbf{P}_k|$ denotes the cardinality of $\mathbf{P}_k$ and $I_{revert,k}$ denotes the reversion tree construction flag indicating that device k may be located closer to the coordinator than the potential parent r. $I_{revert,k} = 1$ implies that the selection of device k as a router may not be effective for the expansion of tree structure. Receiving the association request, device r can accept device k as an end device by allocating an network address to it.

We assume device r, being a cluster head, collects the super-frame schedules of nearby clusters before adopting child devices. The super-frame schedule may be collected periodically or just before the child adoption. Device r waits for other association requests until $|C_r|$ does not grow. Using SCRS and TASS algorithm, device r selects its child devices satisfying following criteria.

- The child device should be in a propagating position (i.e. $I_{revert,k} = 0$)
- A new super frame is schedulable for the child device

Then device r sends an association response messages to these new router devices with new network addresses (i.e., router addresses) and the super-frames schedule. The new routers begin to operate as cluster heads.

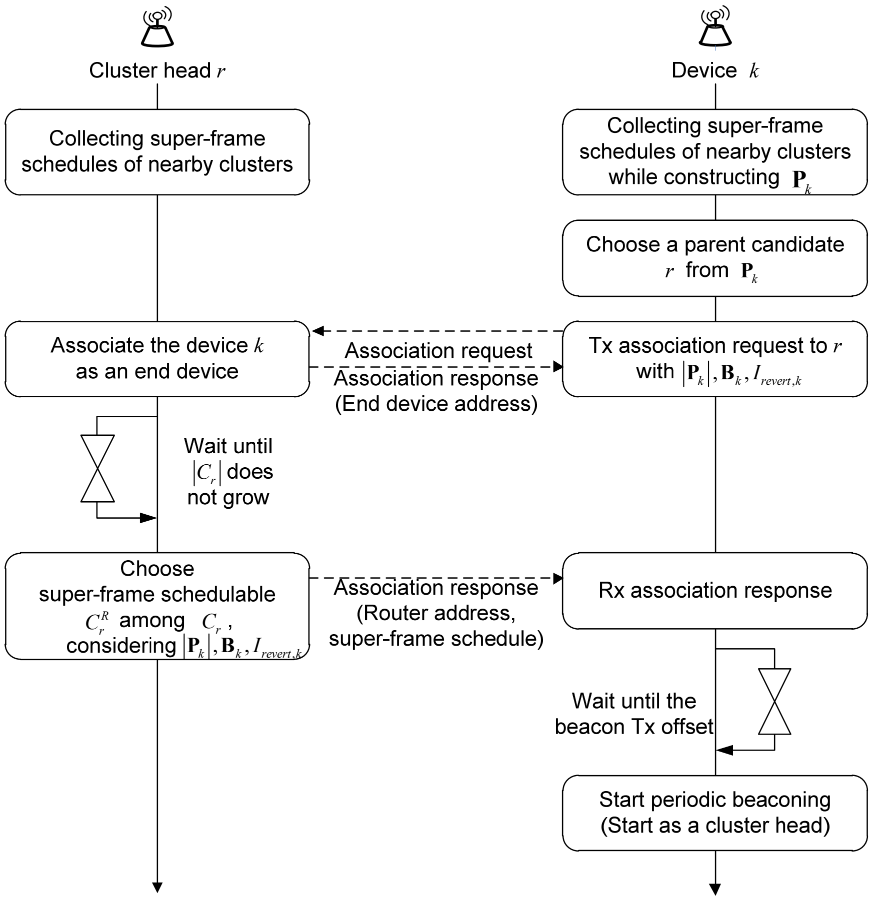


Fig. 3-2. Distributed self-configuration procedure

3.2.1. Scalable child router selection

The biased networking problem can be alleviated by selecting nodes with a minimum number of potential parents as child routers (i.e. selecting devices in the area where the routers are most sparsely located) [7]. However, it may not be efficient when devices are densely located. In this section, we delineate the proposed SCRS.

The SCRS first make cluster head r accept all devices as end devices and then switches some of them as routers later. It makes cluster head r keep receiving association requests for better selection of child routers until $|C_r|$ does not increase, i.e., $|C_r| = Cm(l) - Rm(l)$ or $|C_r|$ remains unchanged for a time interval.

The SCRS makes cluster head r select outermost end devices as routers, as shown in Algorithm 3-1. Cluster head r selects a set of end devices whose reversion tree construction flag is unset, $\tilde{C}_r^{ED}$. To this end, a device $c \in \tilde{C}_r^{ED}$ is expected to be located farther away from the coordinator than the cluster head r. The SCRC selects one with the minimum number of potential parents in $\tilde{C}_r^{ED}$ as a router candidate, say $\hat{c}$. Since $\hat{c}$ is located in an area where the routers are most sparsely located, it may effectively handle devices to be networked. Finally, the SCRC verifies the availability of a new super-frame for $\hat{c}$, which can be processed by the proposed super-frame scheduling algorithm described in Section 3.2.2. If a new super-frame is schedulable for $\hat{c}$, cluster head r selects device $\hat{c}$ as an its child router. Then $\hat{c}$ is removed from $\tilde{C}_r^{ED}$. Then cluster head r sends an association response to device $c \in C_r^R$ with super-frame scheduling information. The SCRS can allow cluster head r to select child devices located outermost as routers using only local information, easily expanding the hierarchical structure of a network in a distributed manner.

Algorithm 3-1. Scalable child router selection (SCRS)
Initialize
$\tilde{C}_r^{ED} \leftarrow \{c \mid c \in C_r,\ I_{revert,c} = 0\}$
$C_r^R \leftarrow \varnothing$
while $\lvert C_r^R \rvert < Rm(l)$ **and** $\lvert \tilde{C}_r^{ED} \rvert > 0$
$\hat{c} = \arg\min_{c \in \tilde{C}_r^{ED}} \lvert \mathbf{P}_c \rvert$
if $\mathrm{TASS}(\hat{c}) \neq$ **FALSE**
$C_r^R \leftarrow C_r^R \cup \{\hat{c}\}$
end if
$\tilde{C}_r^{ED} \leftarrow \tilde{C}_r^{ED} - \{\hat{c}\}$
end while
return C_r^R

3.2.2. Proposed super-frame scheduling

The TASS may reduce the super-frame collision. It partitions the time domain into a number of dedicated intervals and allocates cluster heads with the same network depth to a dedicated interval, eliminating super-frame collision among cluster heads with different network depth. The super-frame collision among cluster heads with the same network depth can be reduced by exchange of bitmaps indicating super-frame schedules of cluster heads nearby. TASS arranges the dedicated intervals according to the network depth, reducing the transmission latency. It determines the length of super-frame in consideration of data traffic and addressing parameters to increase the throughput and energy efficiency as well.

A. Scanning procedure

The TASS schedules the super-frame of child routers in consideration of super-frame schedule of neighboring clusters. To notify other device of the super-frame schedule, cluster heads in the network broadcast their time-offset on which their beacon frames are transmitted, on their beacon frames. For example, cluster head r may quantize its beacon Tx offset $T_{Offset,r}$ by

$$T^{Q}_{Offset,r} = \left\lfloor \frac{T_{Offset,r}}{aBSD \times 2^{SO_{\min}} t_{sym}} \right\rfloor \tag{3.3}$$

where $SO_{\min}$ is the minimum SO to be shared by all devices.

A device k (a cluster head or a device to join the network) may scan each operation channel for T_{BI} to get the super-frame schedule of neighboring clusters. It may store the schedule in the form of a $N_{ch} \times 2^{BO-SO_{\min}}$ bitmap B_k. Let $B_k(i,j)$

be the bit representing the i-th channel and the j-th time slot. When device k receives the beacon frame transmitted from cluster head r through channel h, it may update its bitmap B_k as

$$B_k\left(h, j\right) = 1, \text{ where } T^{Q}_{Offset,r} \leq j < T^{Q}_{Offset,r} + 2^{SO_r - SO_{\min}}. \tag{3.4}$$

Fig. 3-3 depicts an example of bitmap, where the grey part represents the updated bitmap when $h = 1$, $T^{Q}_{Offset,r} = 32$, $SO_r = 3$, $BO = 8$ and $SO_{\min} = 1$. The bitmap may be sent to the cluster head with an association request message. Thus, the cluster head may avoid super-frame collision by using the 2-hop super-frame schedule.

B. Dedicated interval

The TASS partitions the beacon interval into a number of dedicated intervals to avoid super-frame collision and reduce the end-to-end packet transmission latency. It schedules the super-frames of clusters with the same network depth in each dedicated interval.

Let $\mathbf{T}_l$ denote the dedicated interval for super-frames of clusters of network depth l. To avoid super-frame collision between clusters with different network depth, the TASS determines dedicated intervals so that

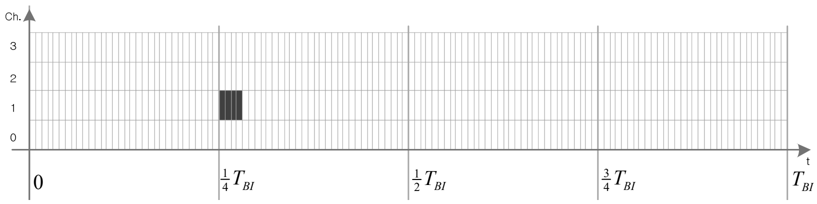


Fig. 3-3. An example of bitmap ($N_{ch} = 4, BO - SO_{\min} = 7$)

$$\mathbf{T}_l \cap \mathbf{T}_{l+m} = \varnothing \tag{3.5}$$

where $m = 1,2$. (3.5) implies that the TASS reuses the time domain resource by allowing clusters with different network depth of at least 3 to use the same time interval. Super-frame collision between clusters with the same network depth can be resolved by exchanging the super-frame schedule of clusters nearby.

To reduce the end-to-end packet transmission latency, it is required to set the relative time offset of super-frames in the routing paths. This is mainly due to that devices should hold data packets and wait for the super-frame of the next-hop router in the IEEE 802.15.4 beacon-enabled mode. It is critical to reduce the waiting time between the super-frames in the routing paths. To measure the minimum end-to-end delay inherently imposed by the super-frame structure, we define the *traversing time* by the summation of waiting durations between beacon Tx offsets in the routing path. The traversing time can be represented as

$$D(r) = \sum_{i=0}^{Lm-1} d\left(p_i(r)\right) \tag{3.6}$$

where $p_i(r)$ is the i-th hop parent of cluster head r (i.e., $p_0(r) \equiv r$ and $p_i(0) \equiv 0$). Here, $d(x)$ is the waiting duration from the super-frame of device x to the super-frame of the parent of device x and can be represented as

$$d(x) = \left(T_{Offset,p(x)} - T_{Offset,x}\right) \bmod T_{BI} \tag{3.7}$$

where "mod" denotes the modulo operation. The maximum traversing time $T_{tr}^{\max}$ can be represented as

$$T_{tr}^{\max} = \max_{r \in \mathbf{P}} \left\{D(r)\right\}. \tag{3.8}$$

When the coordinator periodically transmits its beacon frame at time $t = nT_{BI}$ ($n \in \mathbb{Z}$), $\mathbf{T}_l$ ($l = 0,1,\cdots,Lm-1$) can be represented as

$$\mathbf{T}_l = \left[nT_{BI} + \alpha_l, nT_{BI} + \alpha_l + \beta_l \right] \tag{3.9}$$

where $0 \le \alpha_l$ and $0 < \beta_l$. It can be seen that $T_{tr}^{\max}$ is bounded by

$$T_{tr}^{\max} \le \sum_{l=0}^{Lm-1} \left\{ \left(\alpha_l - \alpha_{l+1} \right) \operatorname{mod} T_{BI} \right\}. \tag{3.10}$$

To reduce the traversing time of uplink data traffic, the TASS determines the dedicated interval so that $\mathbf{T}_{l+1}$ precedes $\mathbf{T}_l$ for $l = 0,1,\cdots,Lm-2$ in the time domain, minimizing $\left(\alpha_l - \alpha_{l+1} \right) \operatorname{mod} T_{BI}$ of (3.10).

We may easily handle the super-frame collision between clusters with different network depth using the concept of dedicated intervals. Furthermore, the super-frames may be scheduled in a sub-optimal way so that the traversing time may be reduced. We may obtain the optimal solution that minimizes $T_{tr}^{\max}$ of (3.10) under the assumption that all parent nodes have knowledge of the entire network structure and the location of all nodes in the network, which is very complicated for the processing.

C. Heuristic design of dedicated intervals

The TASS is aware of traffic bottleneck problem in the vicinity of the sink. Thus, it differentiates the super-frame length, *SO*, according to the network depth. Let $SO(l)$ be the *SO* of the super-frame of depth l cluster.

In the uplink scenario, whole data traffic gathers at the super-frame of the coordinator. The SO of the coordinator can be calculated as

$$SO(0) = \min\left\{n \mid \tilde{\tau} aBSD \times 2^{n} \geq r_{UL} aBSD \times 2^{BO}\right\}$$
$$= BO - \left\lfloor \log_2 \frac{\tilde{\tau}}{r_{UL}} \right\rfloor \tag{3.11}$$

where r_{UL} denotes the data generation rate of the entire network and $\tilde{\tau}$ denotes the expected throughput in the super-frame. We use $\tilde{\tau}$ instead of the actual throughput because the throughput of hybrid MAC using CSMA/CA and TDMA has not been obtained in a closed form [61, 62]. Heuristically, $\tilde{\tau}$ is approximately 60 Kbps when IEEE 802.15.4 PHY uses direct sequence spread spectrum (DSSS) at a data rate of 250 Kbps.

The cluster heads with network depth $l \geq 1$ may use smaller super-frame than their parent. Assuming that the tree structure is evenly distributed under depth $l-1$ cluster head, the sufficient condition for successful data collection may be represented as

$$\tilde{\tau} Rm(l-1) aBSD \times 2^{SO(l)} \leq \tilde{\tau} aBSD \times 2^{SO(l-1)}. \tag{3.12}$$

Thus, $SO(l)$ ($l = 1, 2, \cdots, Lm-1$) may be conditioned as

$$SO(l) \leq SO(l-1) - \log_2 Rm(l-1). \tag{3.13}$$

In practice, the cluster-tree structured networks may not be constructed in a balanced tree structure form. We may calculate $SO(l)$ with some margin as

$$SO(l) = \max\left\{SO_{\min},\ SO(l-1) - \left\lfloor \log_2 Rm(l-1) \right\rfloor\right\},\ l = 1, 2, \cdots, Lm-1. \tag{3.14}$$

$\mathbf{T}_1$ is the dedicated interval in which the super-frames of coordinator's child routers are scheduled. The coordinator must allocate super-frames of depth-1 routers that are orthogonal to each other unless it knows the complete knowledge of whether or not a signal transmitted form a router can reach another router. As such knowledge may not be easily obtained, the duration of $\mathbf{T}_1$ in a beacon interval, denoted by β_1, must satisfy

$$N_{ch}\beta_1 \geq Rm(0)aBSD \times 2^{SO(1)} t_{sym} . \tag{3.15}$$

When $SO(1)$ follows (3.14) and $\beta_1 = \frac{1}{4}T_{BI}$, it can be seen that

$$N_{ch} \geq \frac{Rm(0)}{2^{\lfloor \log_2 Rm(0) \rfloor}} \frac{T_{SD,0}}{1/4\,T_{BI}} . \tag{3.16}$$

The right-hand side of (3.16) is bounded as

$$\frac{Rm(0)}{2^{\lfloor \log_2 Rm(0) \rfloor}} \frac{T_{SD,0}}{1/4\,T_{BI}} \leq 2^{\log_2 Rm(0) - \lfloor \log_2 Rm(0) \rfloor} \frac{1/2\,T_{BI}}{1/4\,T_{BI}} < 4 \tag{3.17}$$

since $T_{SD,0} \leq \frac{1}{2}T_{BI}$ and $x - \lfloor x \rfloor < 1$ for $\forall x \in \mathbf{R}$. We may claim that it may be sufficient to schedule depth-1 routers with values of $\beta_1 = \frac{1}{4}T_{BI}$ and $N_{ch} = 4$ regardless of addressing parameter, provided that $SO(1)$ follows (3.14).

We may also claim the value $\beta_2 = \frac{1}{4}T_{BI}$ may be sufficient for depth-2 routers alongside with (3.14), based upon following observations: We may successfully construct a connected tree that 16 clusters of the same depth are schedulable in a radius of two hops. For addressing parameters that can successfully construct a connected tree, (3.14) implies that $SO(2) \leq SO(0) - 3$. For $N_{ch} \geq 4$, the above observations imply that the super-frame of depth-2 cluster is schedulable with an aid of spatial reuse resources by means of bitmaps exchange (refer to Section 3.2.2-B).

We may apply the same claim as $\mathbf{T}_2$ to $\mathbf{T}_3, \mathbf{T}_4, \cdots, \mathbf{T}_{Lm-1}$ that $\frac{1}{4}T_{BI}$ may be sufficient as the duration in a single beacon interval. For simplicity, we may determine $\mathbf{T}_3, \mathbf{T}_4, \cdots, \mathbf{T}_{Lm-1}$ by

$$\mathbf{T}_l = \mathbf{T}_{l \bmod 3}, \; l = 3, 4, \cdots, Lm-1 . \tag{3.18}$$

To reduce the traversing time of uplink data traffic, the TASS determines $\mathbf{T}_0, \mathbf{T}_1$ and $\mathbf{T}_2$ so that they circulate as $\mathbf{T}_2 \rightarrow \mathbf{T}_1 \rightarrow \mathbf{T}_0 \rightarrow \mathbf{T}_2 \rightarrow \mathbf{T}_1 \cdots$. It can easily be seen that $T_{tr}^{\max} \le \frac{1}{2}T_{BI}$ in this heuristic design for $Lm = 3$. Fig. 3-4 illustrates the super-frame scheduled in $\mathbf{T}_0$, $\mathbf{T}_1$ and $\mathbf{T}_2$.

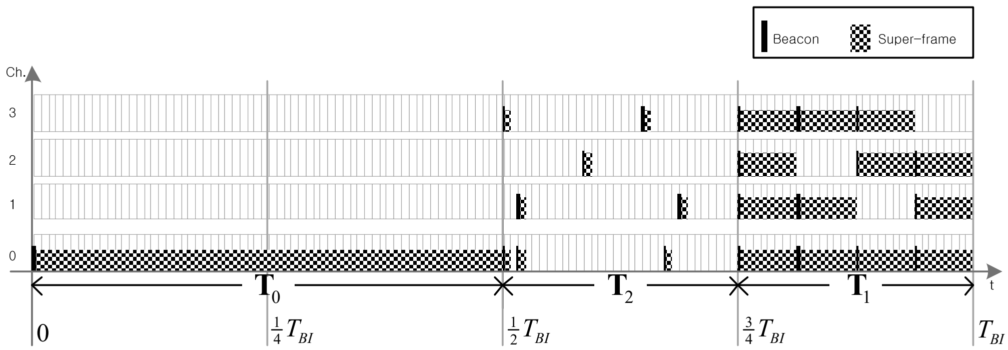


Fig. 3-4. Dedicated interval and example of super-frame schedule ($N_{ch} = 4, BO - SO_{\min} = 7$)

D. Super-frame scheduling

As the heuristic design of the dedicated intervals (i.e., $\mathbf{T}_1, \mathbf{T}_2, \cdots \mathbf{T}_{Lm-1}$) does not require on-line observations, the dedicated intervals may be pre-implemented. Then the super-frame of child router candidate $\hat{c}$ can be scheduled using Algorithm 3-2. Device r calculates the *SO* of $\hat{c}$ by (3.14) and merges the super-frame schedule of itself and $\hat{c}$ to avoid super-frame collision. If a super-frame schedule is available in $\mathbf{T}_{l+1}$, the available resource is assigned to child router candidate $\hat{c}$, where l is the depth of cluster head r. If not, cluster head r needs to initiate another selection process.

Algorithm 3-2. Traffic-aware energy-efficient super-frame scheduling (TASS)

(Super-frame scheduling for child router candidate $\hat{c}$)
Calculate $SO_{\hat{c}}$ using equation (3.14)
Merge nearby super-frame schedules of cluster head r and the candidate $\hat{c}$
if time/frequency is available in $\mathbf{T}_{l+1}$ for super-frame of $SO_{\hat{c}}$
   $h_{\hat{c}} \leftarrow$ channel of available resource
   $T_{Offset,\hat{c}} \leftarrow$ beacon Tx offset of available resource
   Update nearby super-frame schedule of cluster head r
   return $\left(SO_{\hat{c}}, h_{\hat{c}}, T_{Offset,\hat{c}}\right)$
else
   return FALSE (initiate another selection process)
end if

3.3. Performance evaluation

We verify the performance of the proposed self-configuration schemes in terms of the scalability, traversing time and energy consumption by computer simulation. The simulation parameters are summarized in Table 3-1. For comparison, we also evaluate the performance of ZigBee with two configurations; configuration 1 uses the same *Rm* at network depth zero as the proposed scheme and configuration 2 maximally utilizes the addressing space, where *Rm* is a relatively larger number. We assume that ZigBee operates with collision-free super-frame scheduling, where the collision of super-frames among two-hop neighbor clusters is avoided. We also evaluate the performance of M-DAAM which selects child nodes with the smallest number of potential parents as routers to verify the benefit of SCRS.

A. Connectivity

Fig. 3-5 depicts snapshots of self-configuration of ZigBee (config.1 and config. 2), M-DAAM and the proposed scheme. The links connecting cluster heads and their child end-devices are omitted in the graphs for the visibility. It is shown that all those schemes connect the network when $|\mathbf{K}| = 100$, since the addressing space is enough for 100 devices. However, in the tree structure formed by ZigBee, the branches go back and forth due to FCFS router selection. MDAAM places routers in better positions than ZigBee since it places routers in the router-sparsest area. Comparing M-DAAM and the proposed scheme, it can be seen that depth-1 routers are located farther in the proposed scheme, since the proposed scheme

Table 3-1. Simulation parameters

<table>
<tr><th rowspan="2" colspan="2">Parameters</th><th colspan="2">Value</th></tr>
<tr><th>ZigBee</th><th>Proposed scheme</th></tr>
<tr><td colspan="2">Deployment area</td><td colspan="2">81.2 x 81.2 m^2</td></tr>
<tr><td colspan="2">Number of devices ($|\mathbf{K}|$)</td><td colspan="2">100, 500, 1000</td></tr>
<tr><td colspan="2">Maximum network depth</td><td colspan="2">3</td></tr>
<tr><td colspan="2">Beacon order (BI)</td><td colspan="2">8 (3932.16 ms)</td></tr>
<tr><td rowspan="3">Super-frame order (SD)</td><td>Coordinator</td><td rowspan="3">2 (61.44 ms)</td><td>4 (245.76 ms)</td></tr>
<tr><td>Depth-1 router</td><td>1 (30.72 ms)</td></tr>
<tr><td>Depth 2 router</td><td>1 (30.72 ms)</td></tr>
<tr><td colspan="2">Number of operating channels (N_{ch})</td><td>1</td><td>4</td></tr>
<tr><td colspan="2">Transmit power</td><td colspan="2">-10 dBm</td></tr>
<tr><td colspan="2">Maximum data rate</td><td colspan="2">250 kbps (IEEE 802.15.4 PHY)</td></tr>
<tr><td colspan="2">Data packet size</td><td colspan="2">19 + 20 bytes (header + payload)</td></tr>
<tr><td colspan="2">Offered traffic load (payload only)</td><td colspan="2">0.5 ~ 15 kbps</td></tr>
<tr><td colspan="2">Traffic type</td><td colspan="2">Uplink/downlink</td></tr>
<tr><td colspan="2">ZigBee Config. 1 (Cm, Rm, Lm)</td><td colspan="2">64, 14, 3 (18% of addressing space)</td></tr>
<tr><td colspan="2">ZigBee Config. 2 (Cm, Rm, Lm)</td><td colspan="2">64, 31, 3 (97% of addressing space)</td></tr>
<tr><td colspan="2">M-DAAM, Proposed scheme ($Cm_1, Cm_2, Rm_1, Rm_2, L_1, Lm$)</td><td colspan="2">64, 64, 14, 7, 1, 3 (5% of addressing space)</td></tr>
</table>

avoids the branches to come back by placing routers who seem to be in propagating positions.

Although ZigBee and M-DAAM achieved 100% connectivity in $|\mathbf{K}|=100$ scenario, the aforementioned benefits of the proposed scheme can be clearly seen in large-scale networks. Fig. 3-6 depicts snapshots of self-configuration when

$|\mathbf{K}| = 1000$. As the network become denser, ZigBee and M-DAAM suffer from connectivity problem, especially in the edge region of the deployment area. It can be seen that ZigBee tree goes back and forth of the network, not in one direction, limiting the scalability. One may expect that ZigBee config.2 has more opportunity of expanding the tree, since it has much larger Rm than ZigBee config.1. But it can be seen that they suffer from almost the same problem, since the number of routers saturates at 64 and does not increase. This is because in this scenario only 64 (2^{BO-SO}) super-frame is schedulable, witnessing the cross-layer scalability problem. Although M-DAAM shows better performance than ZigBee, it occasionally forms a wriggling tree. It is mainly due to that the number of potential parents may not so different between exterior children and interior children in a dense environment. The proposed scheme, however, by locating depth-1 router farther and by utilizing the revert tree flag, guarantees 100% connectivity even in a densely deployed environment.

To evaluate the scalability, we evaluated the above schemes in terms of self-configuration success rate[1] as the number of devices increases in the same area. We also measured the traversing time to evaluate the structural lower bound of the end-to-end data transmission latency.

---

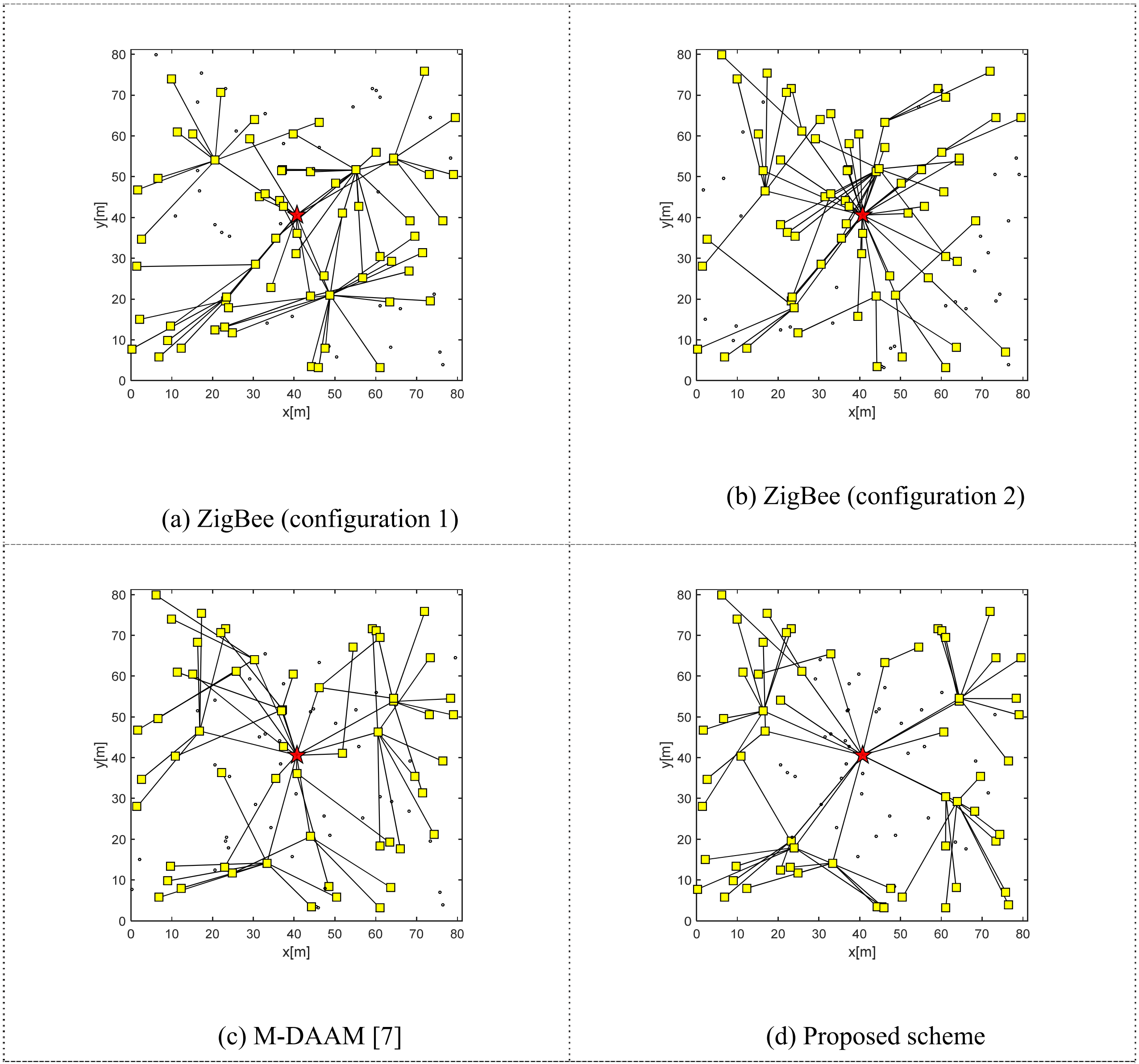
[1] The self-configuration is defined to be successful only if all the devices have successfully joined the network.

Fig. 3-7 depicts the success probability of self-configuration according to the number of nodes. It can be seen that ZigBee may be successful for the connection when the number of nodes is less than 100, but it fails as the density of nodes increases. It is mainly due to the fact that the tree may not properly be expanded. The proposed scheme guarantees full connectivity regardless of the node density.

Fig. 3-8 depicts the average and the maximum traversing time according to the number of nodes. Since ZigBee does not consider the arrangement of super-frames, the traversing time may increase near $2T_{BI}$, which is the upper-bound of traversing time when $Lm = 3$. ZigBee data transmission may suffer larger latency due to the use of super-frame structure. The proposed scheme with TASS can guarantee the traversing time being less than $\frac{1}{2}T_{BI}$. Table 3-2 summarizes the average and the maximum traversing time of ZigBee, the proposed scheme and the optimal solution found using a brute-force algorithm[2]. It can be seen that the performance of the proposed scheme approaches the optimal performance as the network size increases. This is mainly because more routers are created as the network size increases, making it possible to allocate super-frames in a compact manner, reducing the gaps among the super-frames.

---

[2] The bure-force algorithm searches all possible super-frame schedules for given network configurations, finding a super-frame schedule with the minimum end-to-end traversing time.



(a) ZigBee (configuration 1)

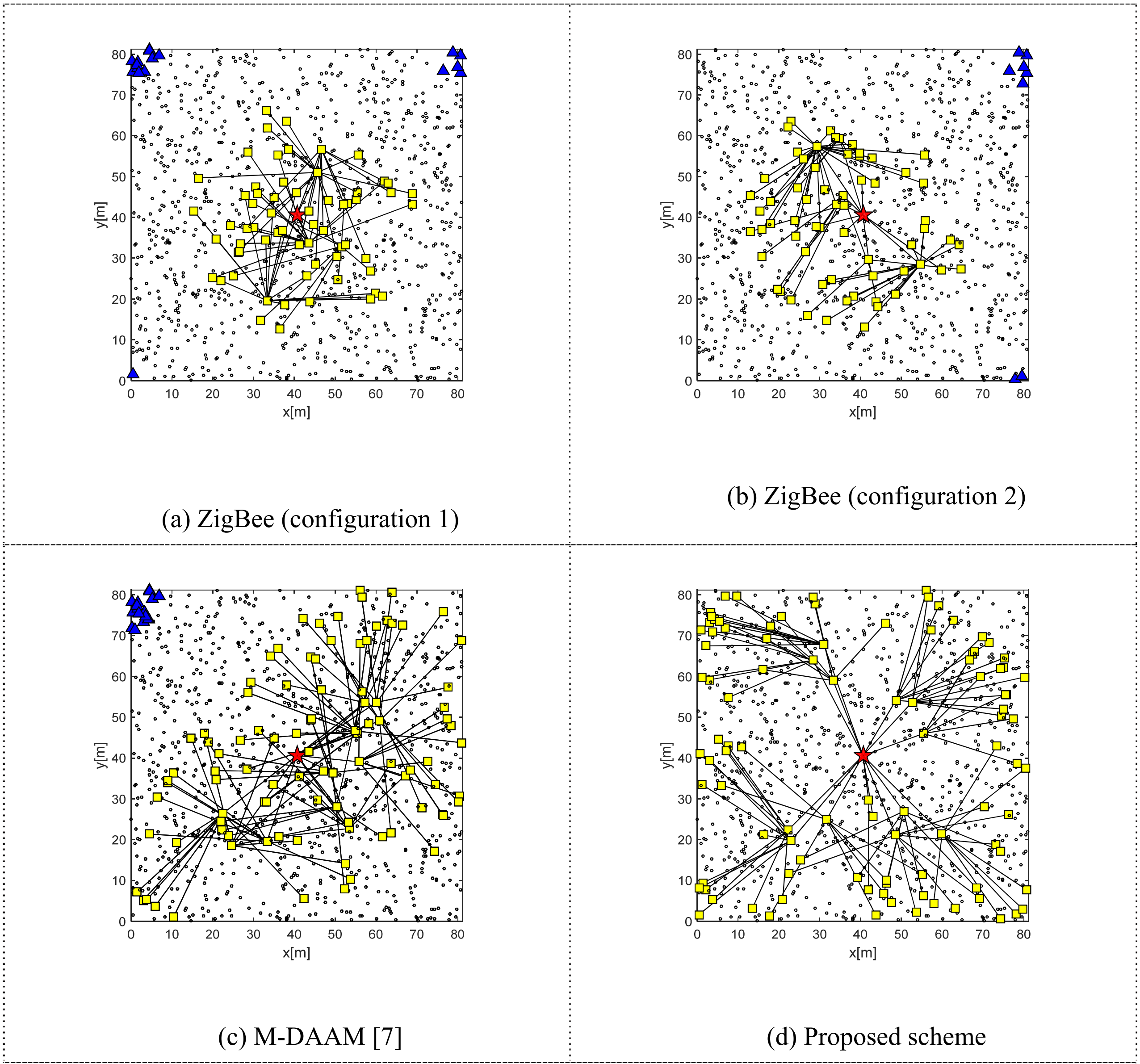
(b) ZigBee (configuration 2)

(c) M-DAAM [7]

(d) Proposed scheme

Fig. 3-5. Snapshots of self-configuration

($|\mathbf{K}| = 100$, red star: coordinator, yellow square: router, dot: end device)



(a) ZigBee (configuration 1)

(b) ZigBee (configuration 2)

(c) M-DAAM [7]

(d) Proposed scheme

Fig. 3-6. Snapshots of self-configuration

($\left|\mathbf{K}\right| = 1000$, red star: coordinator, yellow square: router, dot: end device, blue triangle: orphan device)

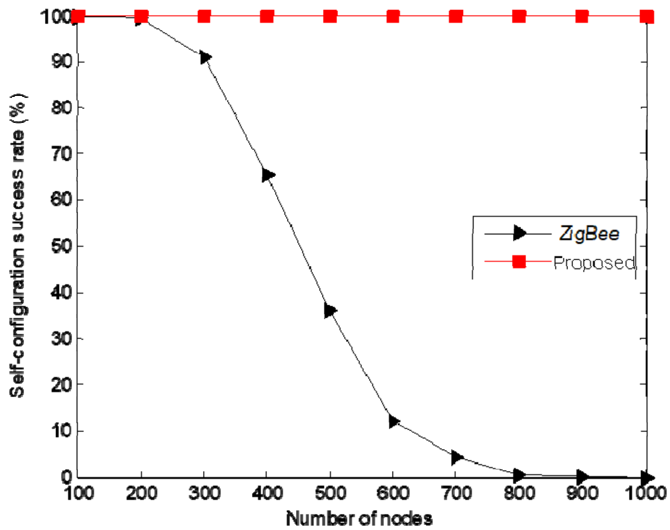


Fig. 3-7. Self-configuration success rate.

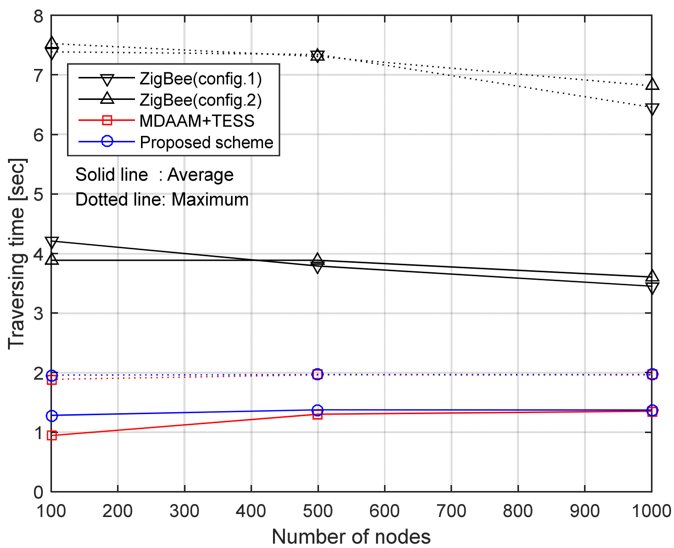


Fig. 3-8. Traversing time according to the number of nodes

Table 3-2. End-to-end traversing time (unit: sec, denoted as 'average/maximum')

Technology	$\lvert\mathbf{K}\rvert = 100$	$\lvert\mathbf{K}\rvert = 500$	$\lvert\mathbf{K}\rvert = 1000$
ZigBee	4.2/7.4	3.8/7.3	3.5/6.5
Proposed scheme	1.3/2.0	1.4/2.0	1.4/2.0
Optimal solution	1.1/1.5	1.2/1.7	1.3/1.9

B. Data transmission performacne

Fig. 3-9, Fig. 3-10 and Fig. 3-11 respectively depict the throughput, the average end-to-end latency and the energy efficiency due to offered uplink data traffic. It can be seen that the proposed scheme may adjust the length of the super-frames according to offered traffic load, significantly improving the throughput performance than legacy ZigBee. It can also be seen that the average end-to-end latency of the proposed scheme is bounded by 2 BI, taking benefit of the bounded end-to-end traversing time, as already summarized in Table 3-2. Furthermore, the proposed scheme may also significantly improve the energy efficiency in terms of J/bit, i.e., energy consumed to transmit data, by adjusting the length of super-frames according to the offerered traffic load.

The proposed scheme may further be improved by applying a proper interference management scheme. Fig. 3-12 depicts the snapshot of throughput of the proposed scheme adopting the interference management scheme introduced in [40] and that of ZigBee. We considered 1 WLAN AP and 4 non-overlapping WLAN AP in Fig. 3-12 (a) and Fig. 3-12 (b), respectively. We turned the WLAN AP(s) on at 50 sec and turned the WLAN AP(s) off at 150 sec. We offered 4 kbps of the data traffic. In can be seen that ZigBee may not handle the data traffic but only provides 1 kbps of throughput. The throughput performance of legacy ZigBee is further degraded when WLAN AP(s) are turned on. On the other hand, the proposed scheme, calculating the super-frame duration using $\tilde{\tau}$ in consideration of WLAN load (i.e., CORI), may yield reliable data transmission even in presence of severe CCI.

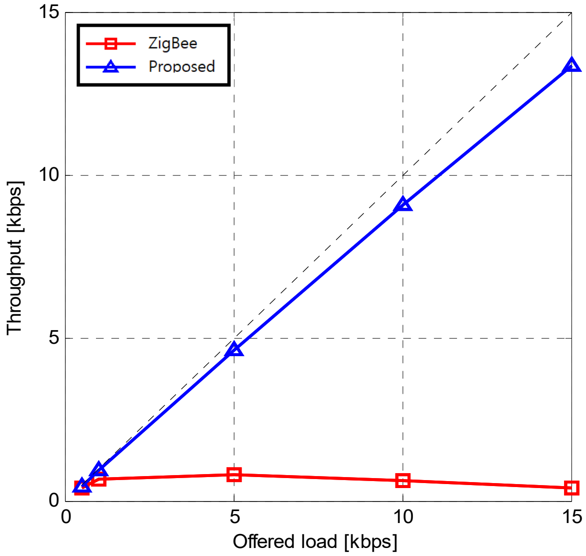


Fig. 3-9. Throughput according to the offered load (uplink)

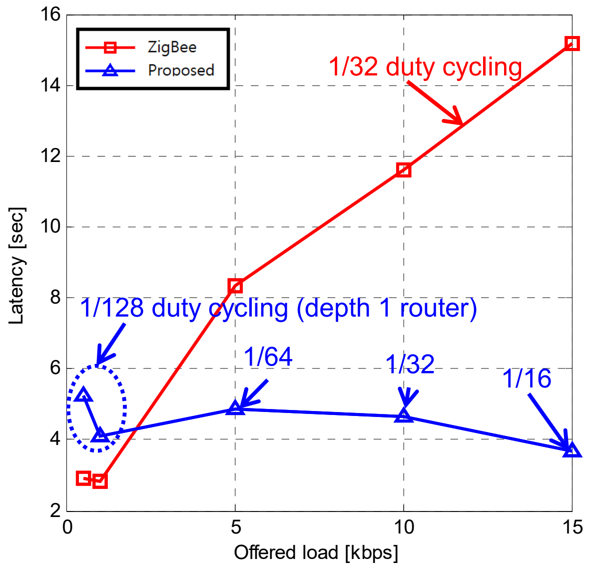


Fig. 3-10. End-to-end latency according to the offered load (uplink)

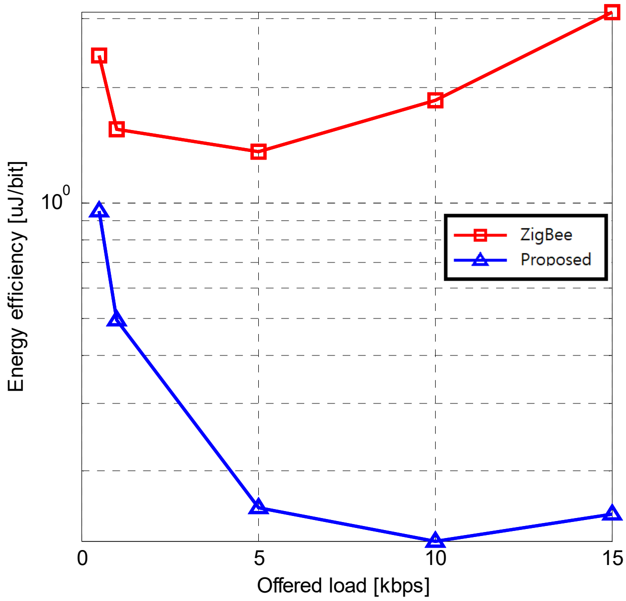
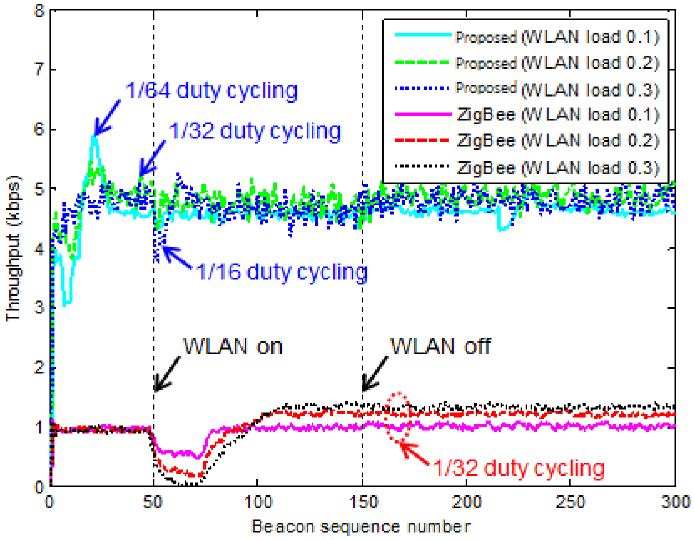
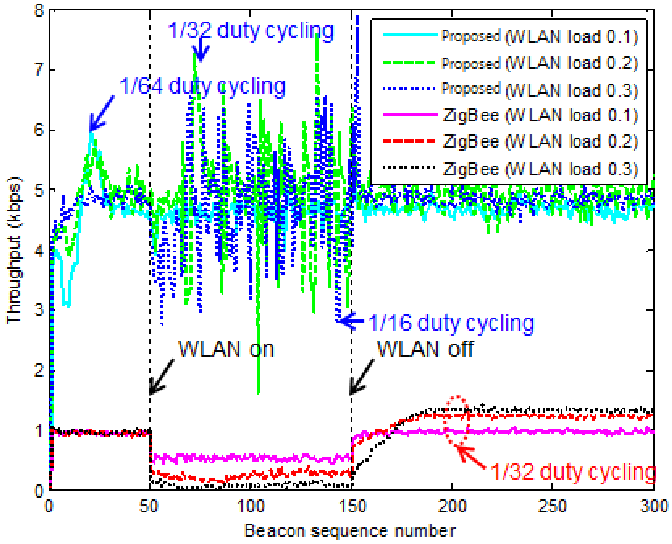


Fig. 3-11. Energy efficiency according to the offered load (uplink)



(a) 1 WLAN AP



(b) 4 Non overlapping WLAN AP

Fig. 3-12. Snapshot of throughput in time (uplink)

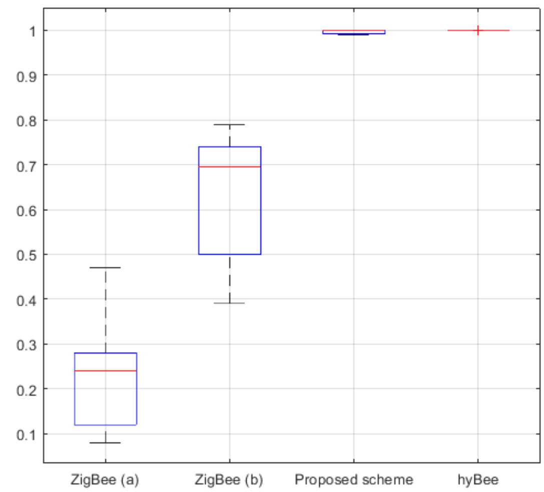
C. Hardware implementation

We implemented the legacy ZigBee and the proposed scheme using HB2200 SoC of *hy*Bee Inc. We further implemented the proposed scheme alongside with the interference management scheme introduced in [40], denoted as hyBee. Table 3-3 summarizes the memory footprint of the hardware implementation. It can be seen that the proposed scheme may be implemented using minimal additional RAM.

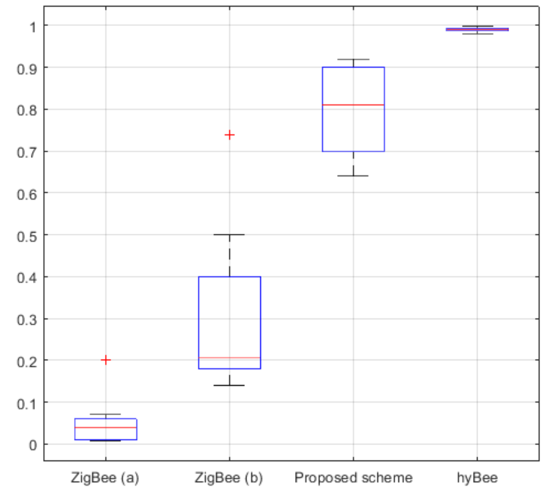
Fig. 3-13 and Fig. 3-14 respectively depict the end-to-end reliability and latency. Here, the duty-cycle of ZigBee (a) is the same as depth-1 routers of the proposed scheme. The duty-cycle of ZigBee (b) is 1/16, which is the maximum duty-cycle allowed under multi-channel usage. It can be seen that the proposed scheme significantly increases the data transmission performance of legacy ZigBee. It can be further seen that the implementation of the proposed scheme and a proper interference management scheme may yield the data transmission performance suitable for commercial IoT service environments.

Table 3-3. Memory footprint of hardware implementation

	ZigBee	Proposed scheme	Proposed scheme and [40]
ROM (program)	**Coordinator:** 26,638 bytes **Terminal device:** 27,070 bytes	**Coordinator:** +3,012 bytes (11%) **Terminal device:** +2,928 bytes (11%)	**Coordinator:** +4,352 bytes (16%) **Terminal device:** +3,616 bytes (13%)
RAM (data)	**Coordinator:** 1,334 bytes **Terminal device:** 1,450 bytes	**Coordinator:** +60 bytes (4.4%) **Terminal device:** +32 bytes (2.2%)	**Coordinator:** +108 bytes (8.1%) **Terminal device:** +74 bytes (5.10%)

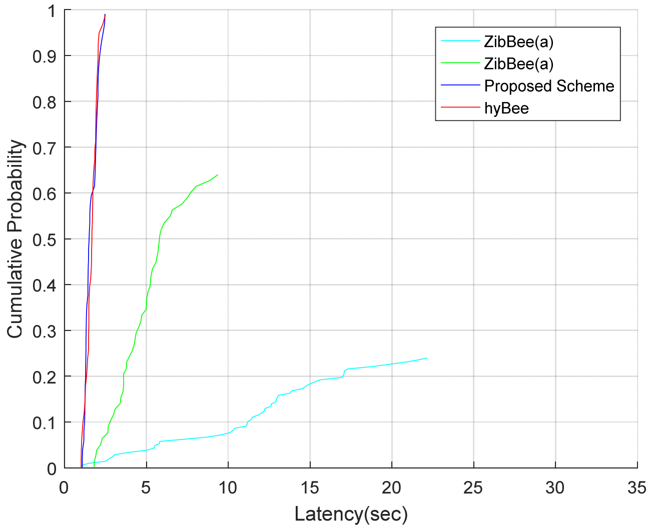


(a) No WLAN AP

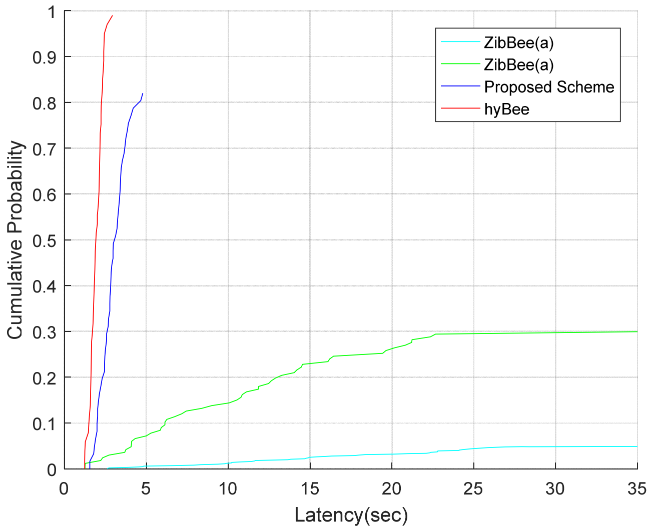


(b) 4 Non overlapping WLAN AP (CORI of 0.3)

Fig. 3-13. End-to-end reliability (hardware implementation)



(a) No WLAN AP



(b) 4 Non overlapping WLAN AP (CORI of 0.3)

Fig. 3-14. End-to-end latency (hardware implementation)

Chapter 4

Network connectivity in presence of co-channel interference

As illustrated in Fig. 4-1, BLE operates in the 2.4 GHz Industrial, Scientific and Medical (ISM) band shared with other wireless communication technologies such as Classic Bluetooth, ZigBee, Z-Wave and Wireless LAN (WLAN) [6]. Employing frequency hopping spread spectrum (FHSS), BLE may be robust to the presence of multi-path fading and narrow-band interference signal [63]. However, FHSS is quite susceptible to the presence of wide-band interference signal like WLAN [64].

A communication system using FHSS may employ an adaptive frequency hopping (AFH) scheme to avoid CCI [65]. Defining a set of channels selected for frequency-hopping as a channel map, AFH detects 'bad' channels more affected by interference signal than others and excludes them from the channel map, referred to blacklisting. It also performs whitelisting operation that restores presumably 'good' channels among the blacklisted ones to the channel map.

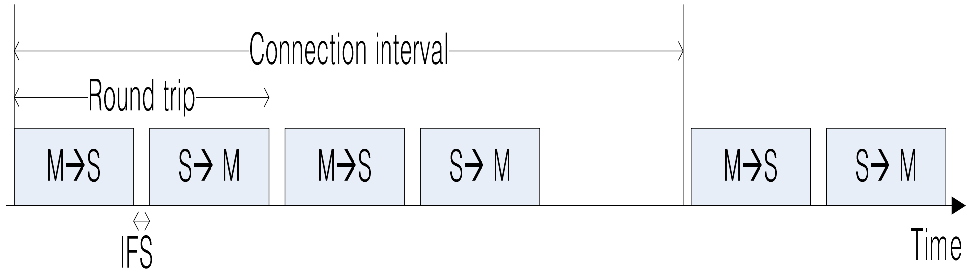


Fig. 4-1. Channel usage of BLE and WLAN in 2.4 GHz ISM band

Both BLE and Classic Bluetooth may employ AFH but do not precisely suggest how to employ it. Classic Bluetooth effectively employ an AFH technique [28-34], BLE not. For example, neither Zephyr and Mynewt, popular open-source real-time operating systems (RTOSs) employing BLE, do not utilize any AFH technique nor does Raspberry Pi 3 [35, 66]. It may be desirable for the employment of AFH to carefully consider the following issues.

Interference detection: Upon blacklisting, it may need for AFH to fast detect whether an undesirable level of CCI exists in a channel of the channel map. Since the CORI fast changes in time [44], delay in interference detection may cause ‘good’ channels to be blacklisted.

Whitelisting: A ‘bad’ channel may not be bad forever. Whitelisting is a testing process whether the condition of channels excluded from the channel map is in a good condition (i.e., the CORI has been decreased). If the whitelisting is performed in a late manner, it may not be easy to update the channel map due to increased packet error ratio (PER) of channels in the channel map. On the other hand, hasty whitelisting may not well utilize the benefit of blacklisting. This issue will further be discussed in Section 4.3.

Channel map update: Unless a pair of devices use the same channel map, they may not encounter each other, yielding a link disruption. When the CORI dynamically changes, it may be required to frequently update the channel map. A pair of devices need to exchange commands to update the channel map following the standardization [6], which may cause latency problem due to increase of signaling overhead.

Energy consumption: When BLE is applied to battery-based operation environments, it is of great concern to reduce the energy consumption for other than communications. It may not be desirable to estimate the CORI using energy detection for low power operation [67].

Memory footprint: Advances in semiconductor technologies allows the use of system-on-chips (SoCs) with large memory while lowering the power consumption. It may be possible to use a cheap SoC with hundreds of Kilobytes of random-access memory (RAM) [68, 69]. Nevertheless, however, it may not be practical to estimate the statistics of all channels in low-cost implementation environments.

In this section, we investigate the performance of BLE in presence of CCI. We then design a channel-group-wise, detection-and-whitelisting AFH (GDW-AFH) scheme. The GDW-AFH operates using a group of adjacent channels and collects channel quality statistics on the group in the normal operation, reducing the time to detect the presence of severe CCI. Upon detection of severe CCI, in contrast to existing AFH schemes that performs blacklisting channels, it utilizes multiple channel groups to find a channel group least affected by CCI. The GDW-AFH further introduces a rendezvous algorithm to maintain connection even in the presence of transmission failure of AFH command frames. The channel-group basis operation of the GDW-AFH does not need extra energy consumption and occupies minimal memory for the implementation.

4.1. Bluetooth low-energy (BLE)

BLE uses one of 40 channels in the 2.4 GHz ISM band (2402 + 2k MHz, k=0, ..., 39). The channels of k=0, 12, and 39 are used as advertising channels and the rest of channels are used as data channels. The slave device sends a subscription request message, referred to ADV_IND, through the advertising channels and receives a subscription permission message, referred to CONNECT_IND, from a master device, establishing ‘connection’. Then the slave device periodically communicates with the master device at a period of connection interval (CI) through a data channel, referred to connection event.

As illustrated in Fig. 4-2, the connection event begins with packet transmission by the master device. Receiving a packet, the slave device transmits a packet after an inter-frame spacing (IFS) of 150 μs. The master or the slave device transmits an empty packet for no data to be transmitted. We refer this process to round-trip. The next round-trip begins when at least one packet of the previous round-trip sets the more data (MD) flag in the packet header. The connection event may be terminated in the presence of following cases; no data to be transmitted, cyclic redundancy check (CRC) errors in two consecutive round-trips, transmission errors in the access address field and no preamble detection. The connection event may be treated as a failure in the case of no preamble reception or transmission errors in the access address field. Consecutive connection event failure during s*upervisionTimeout* leads to a link disruption where the master and the slave stop making communications.

Packet transmission error(s) in the previous round trip may be recovered by means of stop-and-wait flow control using sequence number (SN) and next expected sequence number (NESN) flags in the packet header. The SN is toggled when a new packet is transmitted and the NESN is toggled after successful packet reception. A device re-transmits the last transmitted packet if it receives a packet with the NESN equal to that of the previously received packet.

The initial channel map is contained in the CONNECT_IND transmitted by the master device. The master device may change the channel map using LL_CHANNEL_MAP_IND command frame that contains the new channel map and the time when the new channel map will be used, referred to a channel map update instance.

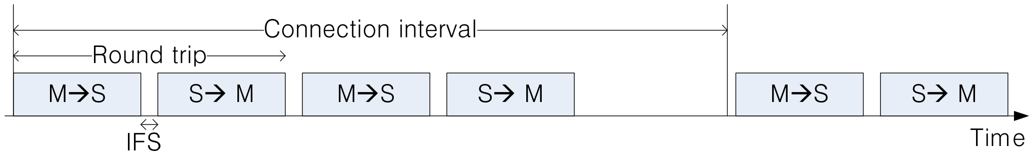


Fig. 4-2. An example of connection events

4.2. Performance of BLE in the presence of CCI

In this section, we analyze the average of data transmission delay of BLE. The number of packets remaining in the buffer in each connection cycle can be calculated using a Markov chain according to the result of data transmission/reception between the master and the slave device in consideration of packet error rate and data traffic generation in the presence of CCI.

We consider unidirectional data communications, which transfers data from the master device to a slave device. We assume that there is no link disruption due to consecutive connection event failure. We also assume the CORI of all BLE channels are the same.

When a new data packet is generated, it will be transmitted after the transmission of data packets stored in the data buffer. When a data packet occurs, it may wait for $T_{CI}/2$ on the average until the next connection event starts, where

T_{CI} is the connection interval. We can represent the average transmission delay from the generation of data packet to the delivery to destination $\bar{L}$ as

$$\bar{L} = \frac{1}{2}T_{CI} + \sum_{n=1}^{B} n\bar{l}_0 p_n \tag{5.1}$$

where B is the maximum number of data packets that can be stored in the buffer, p_n is the probability that n data packets are stored in the connection event immediately after the generation of a new data packet and $\bar{l}_0$ the time taken for transmission of a data packet from the beginning of a connection event.

In the case of two CRC errors or a access address error, the connection event is terminated and data transmission must be retried after T_{CI}. $\bar{l}_0$ can be represented as

$$\bar{l}_0 = \sum_{n=0}^{\infty}\left[\left\{1-\left(\Gamma+\Omega\Gamma\right)\right\}^n \left\{\Gamma\left(nT_{CI}+T_{RT}\right)+\Omega\Gamma\left(nT_{CI}+2T_{RT}\right)\right\}\right] \tag{5.2}$$

where T_{RT} is the round-trip time. When IFS is denoted by T_{IFS}, T_{RT} can be represented as

$$T_{RT} = \left(L_{Data}+L_{Ack}\right)/R + 2T_{IFS}\,. \tag{5.3}$$

Let Γ be the probability that one round trip will succeed (i.e., the probability to successfully transmit both data packets and ACK), and Ω be the probability that only a CRC error occurs without an access address error in a round trip. Γ and Ω can be represented as, respectively,

$$\Gamma = \Gamma_{Data}\Gamma_{Ack} \tag{5.4}$$

$$\Omega = \Gamma_{Data}\Omega_{Ack} + \Omega_{Data}\Gamma_{Ack} + \Omega_{Data}\Omega_{Ack}\,. \tag{5.5}$$

We may assume that $\lambda_I(t)$ of Section 2.3 is a constant (i.e., $\lambda_I(t)=\lambda$) and the bit error rate in the absence of CCI is p_b. Then the probability Γ_{Data} and Γ_{Ack} that the data packet and the ACK are successfully transmitted, respectively, can be represented as, respectively,

$$\Gamma_{Data}=(1-\rho)(1-p_b)^{L_{Data}}\,e^{-\lambda L_{Data}/R} \tag{5.6}$$

$$\Gamma_{Ack}=(1-\rho)(1-p_b)^{L_{Ack}}\,e^{-\lambda L_{Ack}/R}. \tag{5.7}$$

The probability Ω_{Data} and Ω_{Ack} that respectively only the CRC error will occur without error in the access address of the data packet and the ACK can be represented as, respectively,

$$\begin{aligned}\Omega_{Data}&=(1-\rho)(1-p_b)^{L_{AA}}\,e^{-\lambda L_{AA}/R}\\&\cdot\left\{1-(1-p_b)^{L_{Data}-L_{AA}}+(1-p_b)^{L_{Data}-L_{AA}}\left(1-e^{-\lambda(L_{Data}-L_{AA})/R}\right)\right\}\end{aligned} \tag{5.8}$$

$$\begin{aligned}\Omega_{Ack}&=(1-\rho)(1-p_b)^{L_{AA}}\,e^{-\lambda L_{AA}/R}\\&\cdot\left\{1-(1-p_b)^{L_{Ack}-L_{AA}}+(1-p_b)^{L_{Ack}-L_{Ack}}\left(1-e^{-\lambda(L_{Ack}-L_{AA})/R}\right)\right\}.\end{aligned} \tag{5.9}$$

Here L_{Data}, L_{Ack}, L_{AA} and R denote the data packet length, ACK length, access address length, and data transmission rate, respectively.

Let S_n be the state that n data packets exist in the buffer at the beginning of each connection event. The probability of changing the state to S_m in the next connection event depends only on S_n, which can be represented as a Markov chain. The state transition probability can be represented as

$$P\left(S_m \mid S_n\right)=\begin{cases}\sum_{i=0}^{N_{\max}} P(i \mid n) Q(m-n-i), & m<B \\ \sum_{i=0}^{N_{\max}} P(i \mid n) \sum_{k=m-n-i}^{\infty} Q(k), & m=B\end{cases} \tag{5.10}$$

where $N_{\max}$ $\left(=\left\lfloor T_{CE}/T_{RT}\right\rfloor\right)$ denotes the maximum number of packets that can be transmitted in a connection event, $P(i \mid n)$ is the probability of successful transmission of i of n data packets in a connection event and $Q(x)$ denotes the probability of occurrence of n data packets during T_{CI}. Assuming that data packets are generated as a Poisson process with a mean of r packets/sec, we can represent $Q(x)$ as

$$Q(x)=\begin{cases}\left(rT_{CI}\right)^{x} e^{-rT_{CI}} / x!, & 0 \leq x \\ 0, & o/w\end{cases} . \tag{5.11}$$

Letting $p(i \mid k)$ be the probability that i round trips are successful after k round trips, it can be represented as

$$P(i \mid n)=\sum_{k=i}^{n} p(i \mid k) . \tag{5.12}$$

Let $\Phi(i,k)$ be the number of cases that i round trips are successful after k round trips (i.e., the number of cases where two consecutive CRC errors occur only at the end, or two consecutive CRC errors do not occur). Letting $P_{cl}(k)$ be the probability that the connection events ends after k round trips, $p(i \mid k)$ can be represented as

$$p(i \mid k)=\Gamma^{i} \Omega^{k-i} \Phi(i,k) P_{cl}(k) . \tag{5.13}$$

It can be shown that [70]

$$\Phi(i,k)=\binom{i+1}{k-i}+\left\{2\binom{i}{k-i-2}+(k-3)\binom{i-1}{k-i-2}\right\}P_1 \tag{5.14}$$

$$P_{cl}(k)=\begin{cases}2\Omega_{AA}+\Omega_{Data}^2+\Omega_{Ack}^2, & 0\le k\le N_{\max}-2\\ 2\Omega_{AA}, & k=N_{\max}-1\\ 1, & k=N_{\max}\end{cases} \tag{5.15}$$

where P_1 is the probability that two failed round trips do not terminate the connection event and can be represented as

$$P_1=\frac{2\Omega_{Data}\Omega_{Ack}\left(1-\Omega_{Data}\right)\left(1-\Omega_{Ack}\right)}{\left(\Omega_{Data}+\Omega_{Ack}\right)^2}. \tag{5.16}$$

From (5.11)-(5.16), we can calculate the steady state probability that n data packets is in the buffer when the connection event is initiated. From (5.1) and (5.2), we can also calculate the average of data transmission delay.

We perform computer simulation in the operation environment summarized in Table 4-1 to measure the average transmission delay according to the data generation rate and the interference load. We generate data by the Poisson process of (5.11). Each experiment runs for 10,000 connection events and the simulation data is collected after 2,000th connection event. Each experiment is repeated 100 times.

Fig. 4-3 depicts the average of transmission delay according to the data generation rate, where the symbol indicates the simulation results and the solid line indicates the analysis result. It can be seen that the simulation result agrees well with the analysis. In the presence of no interference signal, the average data transmission delay is about 50 msec, which is the waiting time until the next connection event starts after the data packet occurs, whereas the connection event termination occurs due to a packet error as the interference load increases. As a result, there is increase of the transmission delay at least by about 40%. It can also be seen that the transmission delay increases as the packets accumulated in the buffer increases when the data generation period is short. This effect increases as the interference load increases.

Table 4-1. Simulation parameters for data transmission delay analysis

Parameters	Value
L_{Data}, L_{Ack}, L_{AA}	37, 10, 4 bytes
T_{CI}	100 msec
T_{CE}	10 msec
B	10 pkts
R	1 Mbps
p_b	10^{-6}
T_W	1 msec
ρ	0 – 0.3

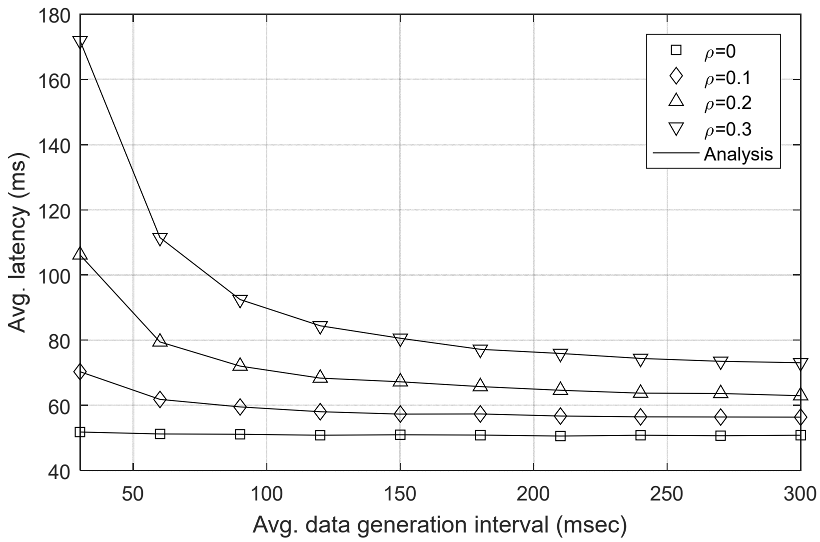


Fig. 4-3. Average data transmission delay due to data generation interval

4.3. Previous works

A number of AFH schemes have been proposed for Classic Bluetooth. Packet loss rate (PLR)[3], defined by 1 - (number of successfully received packets) / (number of transmitted packets), has widely been applied to the measure of channel quality for AFH schemes because no additional power consumption or signaling overhead is required. However, we may need a very large number of samples to accurately estimate the PLR [30]. Assuming that packet losses occur independently of each other, the number of samples, K, to guarantee that the absolute estimation error of PLR does not exceed $\varepsilon_{abs}^{\max}$ with a confidence level of ν can be represented as [67]

$$K \geq 2\left(\frac{\mathrm{erf}^{-1}(\nu)}{\varepsilon_{abs}^{\max}}\right)^2 \Psi(1-\Psi) \tag{5.17}$$

where $\mathrm{erf}(\cdot)$ denotes the error function and Ψ denotes the PLR. For example, more than 57 samples are needed when $\Psi = 0.3$ with $\varepsilon_{abs}^{\max} = 0.1$ and moderately relaxed confidence level of $\nu = 0.9$.

[3] Since a master-slave pair of BLE devices transmits packets every connection interval, it can be judged as a preamble error if the preamble is not received in the connection event (on the other hand, preamble error is difficult to measure when a random-access technology such as CSMA is used). Unlike the packet error rate (PER), PLR can measure the channel quality even if the preamble is not received.

For fast detection of CCI, previous works designed AFH schemes blacklisting channel groups with the use of estimated PLR of each channel group [28-31]. However, they do not consider whitelisting [29, 30] or simply reset the channel map (include all channel groups in the channel map) in a fixed time interval [28, 31], making it impossible to frequently probe blacklisted channels. For continuous monitoring of all channels, some works designed AFH schemes that lower the frequency of visit of a 'bad' channel, rather than complete blacklisting [32-34]. However, they may slowly estimate the PLR and require a non-standard channel selection algorithm (CSA).

Table I summarizes previous works for the design of AFH for BLE. A previous work blacklists the channel when the estimated PLR is below a threshold, where the PLR is estimated by means of moving average [36]. When the size of channel map becomes below a threshold, it may reset the entire channel map. [37] designed a simple method for the estimation of PLR in a certain time interval and whitelisting a channel after a time interval after the channel is blacklisted and further optimized those time intervals. In [38], a short-term PLR is used for blacklisting and a long-term PLR is used for calculating a timeout for whitelisting. CI of BLE (7.5 ms ~ 4 sec) is more than ten times longer than that of Classic Bluetooth (625 μs). However, in contrast to fast estimation schemes (e.g., [28-31]), these algorithms do not consider the reduction of PLR estimation time. Another AFH scheme for BLE that adjust the frequency of visit of each channel has been proposed in [35]. In addition to sharing the same shortcomings of [32-34],

Table 4-2. AFH schemes for BLE

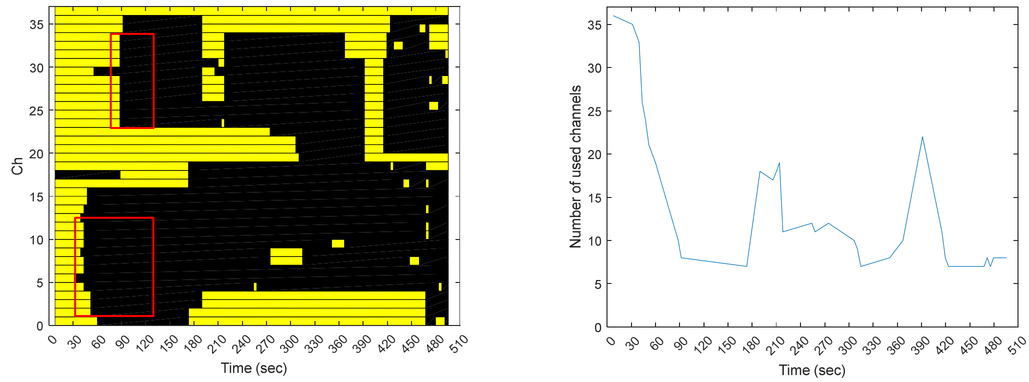
	Blacklisting criteria	Whitelisting criteria	Channel map update	CSA
Spork’20 [36]	PLR (moving average)	When channel map size is below a threshold	Standard	Standard
Mast’21 [37]	PLR during a fixed time interval	Timeout (a fixed time interval)	Standard	Standard
Poirot’21 [38]	Short-term PLR	Timeout calculated using long-term PLR	Standard	Standard
Pang’21 [35]	Single connection failure	Single connection success	Standard	Proprietary

it also requires significant signaling overhead because it updates the channel map even after a single connection failure.

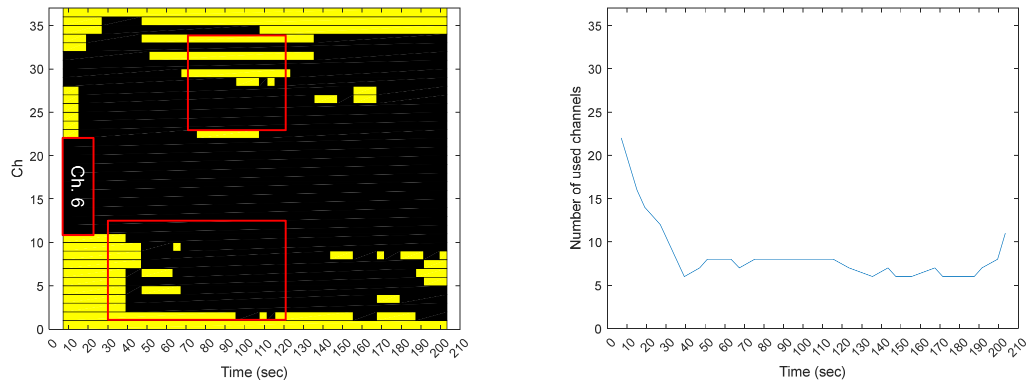
We analyzed the AFH of Broadcom BCM43012 BLE-WLAN combo chipset implemented on a smart phone. As shown in Fig. 4-4, BCM43012 uses all 37 data channels at the first time, and when the smart phone is connected to a WLAN AP, BLE channels inside the frequency band of the WLAN AP is blacklisted. It can be seen that the channel map update is performed every 4 seconds, regardless of the number of channels being used. The adaptation time to the change in the interference environment was slower than that, and after 20 seconds or more since the WLAN was turned on, the channel map update was performed as the channel overlapping the WLAN band was blacklisted. When a channel is blacklisted due to the presence of WLAN interference, it can be whitelisted after a certain time interval of between 100 and 400 seconds. The number of channels in use in Fig. 4-4 (a) and (b) do not exceed 6. This shows that the minimum number of channels threshold that is higher than the BLE standard (at least 2 channels). When the channel is blacklisted and the available channels were less than the threshold (i.e., 6), The channel is whitelisted by selecting some of the channels from the blacklisted channel (420 to 450 seconds in Fig. 4-4 (a), 70 to 120 seconds in Fig. 4-4 (b)).

The AFH algorithm of BCM43012 generalized through the above-described measurement is summarized in Fig. 4-5 and Fig. 4-6, where N_{fail} denotes the number of consecutive connection event failures and τ_{SH} is the maximum number of connection event failures. The BLE determines that the connection is broken if the connection event is not successfully executed during *supervisionTimeout*. For the connection interval of T_{CI}, τ_{SH} can be represented as

$$\tau_{SH} = \left\lfloor \frac{supervisionTimeout}{T_{CI}} \right\rfloor. \tag{5.18}$$



(a) 30sec: WLAN Ch.2 ON, 70 sec: WLAN Ch. 11 ON, 120 sec: WLAN OFF (all).



(b) 30sec: WLAN Ch.2 ON, 70 sec: WLAN Ch. 11 ON, 120 sec: WLAN OFF (all).
(The device is connected to WLAN Ch. 6)

Fig. 4-4. Real-world experiment of Broadcom BCM43012
(left: channel map in use, right: Number of channels in use)

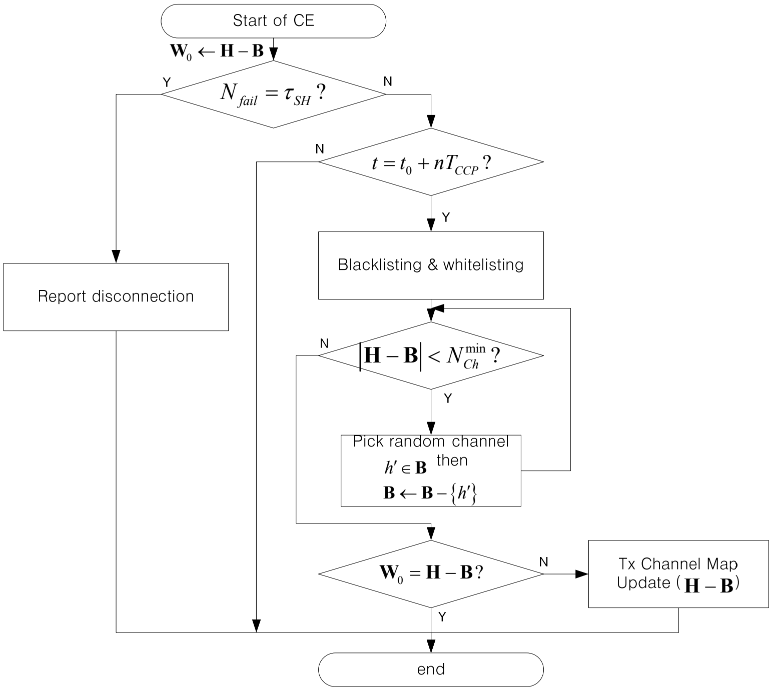


Fig. 4-5. AFH algorithm of Broadcom BCM43012

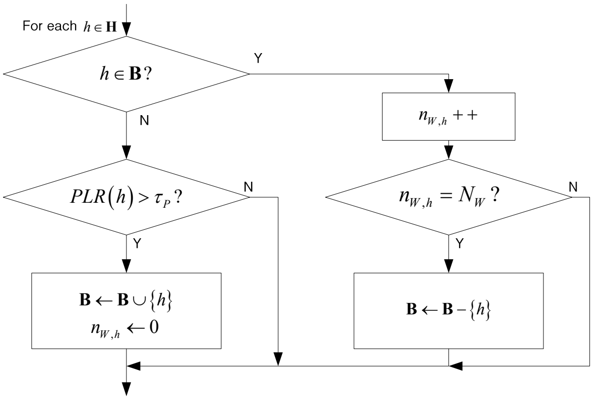


Fig. 4-6. Blacklisting/whitelisting of Broadcom BCM43012

Letting t_0 be the initial connection establishment time, the conventional BLE updates the blacklist $\mathbf{B}$ among the entire channel map $\mathbf{H}$ by driving the blacklisting and whitelisting algorithm of Fig. 4-6 for each channel classification period T_{CCP}. If the number of available channels $|\mathbf{H}-\mathbf{B}|$, is less than the minimum number of channels $N_{Ch}^{\min}$, any blacklisted channels are deleted from the blacklist. The update of channel map is notified by sending LL_CHANNEL_MAP_IND.

It may be assumed that the channel is classified using the recommendations of the BLE standard (packet loss ratio (PLR), received signal strength (RSS), etc.). If the PLR of a channel measured for a certain time is greater than or equal to a threshold (δ_{PLR}), the channel is blacklisted, and the blacklisted channel is whitelisted after a certain time ($N_W T_{CCP}$).

Using the AFH algorithm of Fig. 4-5 and Fig. 4-6, the connectivity and the effective CORI (CORI averaged over channels in use) are examined by computer simulation, where the simulation parameters are summarized in Table 4-3. Note that N_W is configured so that the effective CORI may be minimized.

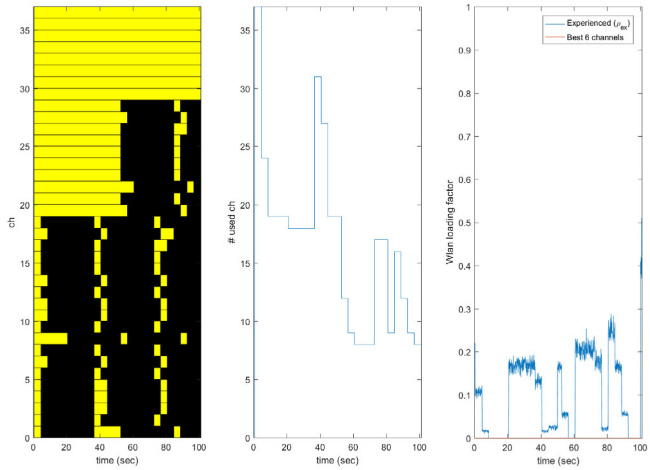
Fig. 4-7 depicts snapshots of the operation of conventional BLE AFH algorithm, where the graph on the left displays the channel map in use as yellow color, the graph in the middle displays the number of channels in use, and the graph on the right displays the effective CORI. The average CORI of six channels with the lowest CORI among 37 data channels is further displayed in orange color.

Table 4-3. Simulation parameters for the conventional AFH algorithm

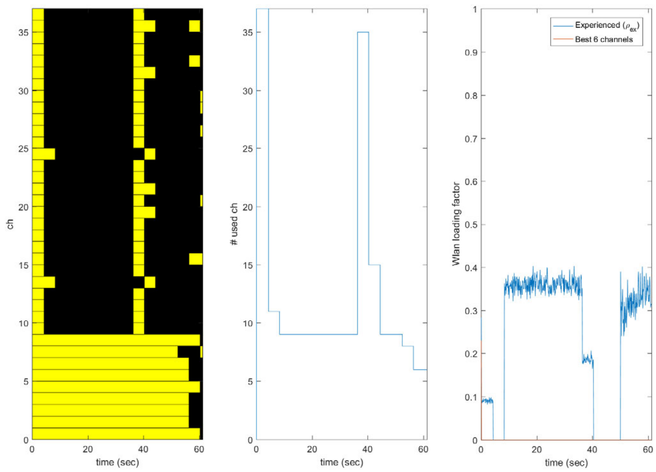
Parameter	Value
Average CORI	0.3
WLAN AP	WLAN Ch. 1, 5, 9, 13
Topology	One-to-one
Connection interval (T_{CI})	50 ms
Channel classification period (T_{CCP})	4 sec
PLR threshold (δ_{PLR})	0.15
Whitelisting interval (N_W)	8 (in T_{CCP})
Minimum number of channels ($N_{Ch}^{\min}$)	6
Connection failure threshold (τ_{SH})	6

In Fig. 4-7 (a), it can be seen that the connection is disconnected when the number of used channel decreases, as it may be hard to make a channel map update when CORI of the small number of the used channels increases. In Fig. 4-7 (b), the existing BLE AFH algorithm recognizes the change in the interference environment and attempts to update the channel map. If the number of available channels is less than a threshold after the blacklisting/whitelisting, some of blacklisted channels are whitelisted again. In this way, it may not be easy to find a channel with less CORI, and it can be seen that the connection is lost after several channel map updates.

In either case, the connection is lost even though there exist channels with low CORI, as the average CORI of six channels with the lowest CORI (depicted in orange lines) shows. To make an AFH scheme applicable to BLE, it may be desirable to swiftly make decision of a channel map update (i.e., detect severe CCI) before the CORI of the used channels becomes too high. It may also be desirable to conduct more frequent investigations across the entire frequency bands to identify channels less affected by CCI.



(a)



(b)

Fig. 4-7. Broadcom BCM43012 operation snapshot (simulation)
(left: channel map, middle: the number of utilized channels, right: effective CORI)

4.4. Proposed adaptive frequency hopping scheme

It may take a long time to accurately estimate the channel quality statistics for BLE, making it impractical in presence of rapidly time-varying CCI. It may be desirable to use an AFH scheme that can quickly gather channel quality statistics and take appropriate actions, although it may have some degree of inaccuracy. Moreover, the AFH technique may have the capability that can correct decision associated with erroneous channel quality statistics, ensuring reliable operation even in dynamic interference environments.

The proposed GDW-AFH collects statistics of a set of channels, a channel group. It normally operates on a single channel group, making the detection of CCI fast. We consider immediate whitelisting that makes use of multiple channel groups after the detection of CCI. This strategy not only reduces the impact of CCI but also may mitigate erroneous interference detection by further investigating the previously utilized single channel group. The GDW-AFH makes devices use the multiple channel groups after a pre-determined number of consecutive connection event failure, maintaining connections even in the failure of transmission of channel map update.

4.4.1. Interference detection

The GDW-AFH normally operates using a single channel group, referred to single channel group operation (SGO) mode. Each channel group consists of adjacent channels whose channel quality (CORI) may be similar to each other, assuming that the major interference source has a bandwidth significantly larger than that of BLE.

In the SGO mode, when experienced n_f failures during the last W_{SCO} connection events, the master device makes a whitelisting by means of transition to multiple channel group operation (MGO) mode. It update the channel map, where multiple channel groups will be used $N_{update,S2M}$ connection events after the current connection event. Grouping channels eliminates the need to collect statistics of individual channels. Instead, the channel status can be monitored with the use of less momory.

Fig. 4-8 depicts the CDF of the number of connection events taken for the interference detection, where the solid and the dotted line respectively denote the CDF when CORI is 0.3 and 0.1, representing the presence of severe and moderate levels of CCI, respectively. By decreasing n_f and increasing W_{SCO}, it can be inferred that the transition to the MGO mode occurs more rapidly in the presence of severe CCI. However, this may also lead to frequent transitions to the MGO mode when the CORI is low, which may not be desirable. This is because remaining in the SGO mode could offer better performance when the CORI in other channel groups is higher. It may be not easy to accurately estimate the interference level before transition to the MGO mode since the measurement of interference level of other channel groups is not feasible. It may be desirable to handle incorrect transition due to estimation inaccuracy of interference level.

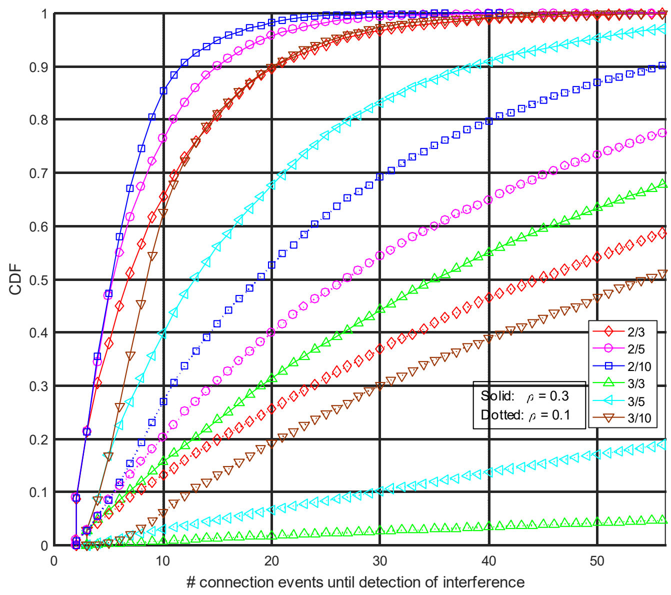


Fig. 4-8. CDF of the number of connection events until detection of interference (parameters are denoted as n_f/W_{SCO})

4.4.2. Whitelisting & blacklisting

The GDW-AFH makes transition to the MGO mode, which is basically whitelisting, after the detection of severe CCI. It may be desirable to select channel groups that are sufficiently spaced apart considering the signal bandwidth of CCI.

Let K_M be the number of channel groups utilized in the MGO mode. The master device collects channel statistics, including the failure rate of connection events for an interval of $K_M W_{MCO}$ connection events. Letting e_g be the failure rate of connection events of channel group g, the channel group with the lowest e_g is selected for the next transition to the SGO mode and other channel groups are blacklisted. The master device updates the channel map that will be used for an interval of $N_{update,M2S}$ connection events. It may require for $K_M W_{MCO}$ bits of memory to get the channel statistics.

4.4.3. Channel map update

BLE utilizes the LL_CHANNEL_MAP_IND command frame for the update of channel maps. However, multiple connection events may be required to transmit this command frame in high CORI environments, yielding data transmission delay. This delay becomes significant in rapidly changing CORI environments, leading to degradation of transmission performance.

The GDW-AFH can work with the use of BLE standard command frames, but it may further enhance the transmission performance by avoiding transmitting command frames. It can piggyback the channel group and channel map information on data packets. Thus, it can improve the transmission performance without the need of additional command framing overhead. Assume that the total number of channel groups within 12 and the timing for the channel map update is within 15 connection events. Then, the channel group index and the update timing can be represented in a form of 4 bits, respectively, as shown in Table 4-4. It may reduce the transmission delay associated with the update of channel map at a small expense of throughput. When applied to WSN environments with small data, this trade-off is quite acceptable.

Table 4-4. An example of piggybacked information for a channel map update

<table>
<tr><th>Operation</th><th>Channel group index</th><th>Channel map update instance</th></tr>
<tr><td>SGO mode</td><td>0x0D</td><td>Don’t care</td></tr>
<tr><td>MGO mode</td><td>0x0E</td><td>Don’t care</td></tr>
<tr><td>Transition from SGO to MGO mode</td><td>0x0F</td><td rowspan="2">Lower 4-bit of the connection event count when the updated channel map will be used</td></tr>
<tr><td>Transition from MGO to SGO mode</td><td>The index of the selected channel group</td></tr>
</table>

To avoid disconnection due to missing channel map update in the SGO mode, the master or the slave device can make immediate transition to the MGO mode after $W_{SCO} + N_{update,S2M}$ consecutive connection failures. This may ensure continuous operation and avoid disruption by disconnection, improving the reliability of communication link.

4.4.3. Optimal design of the proposed scheme

In this section, we consider the implementation of the proposed scheme in terms of the CORI. Letting $\rho(h(t),t)$ be the CORI of channel $h(t)$ at time t, we can make decision for the transition of operation mode to minimize $\lim_{t\to\infty}\frac{1}{t}\int_0^t \rho(h(\tau),\tau)d\tau$. It may not be practical to accurately estimate the CORI. To this end, we may utilize a partially observable Markov decision process (POMDP) for the decision of transition. However, since the dimension of the state of POMDP exponentially increases as the number of channels increase, it may be extremely hard to enumerate.

We can assume that, if a device decides to switch to the MGO mode, it dwells in a SGO mode for T_S, in a MGO mode for T_M and in a new SGO mode for another T_S. We can also assume that the SGO is affected by independent WLAN APs. By using the WLAN model of Chapter 2, we may to switch to the MGO mode if

$$\int_{t}^{t+2T_S+T_M} m_c(\tau)\,d\tau > \int_{t}^{t+T_S} m_c(\tau)\,d\tau + \int_{t+T_S}^{t+T_S+T_M} \frac{1}{N_{MCS}} \sum_{i=0}^{N_{MCS}-1} m_i(\tau)d\tau + \int_{t+T_S+T_M}^{t+2T_S+T_M} m_{c'}(\tau)\,d\tau \quad (5.19)$$

where c and c' respectively denote currently used and newly selected single channel group (SG)and $m_c(t)$ denotes the number of WLAN clients affecting the SG c at time t.

The device must rely only on $m_c(t)$ to decide the change of operation mode. Using the WLAN model of Chapter 2, it can be shown that

$$\begin{aligned} L(m',m,\tau) &= \Pr[m' \text{ clients at } t=\tau+t_0 \mid m' \text{ clients at } t=t_0] \\ &= \sum_{k=\max(0,m+m'-N_C)}^{\min(m,m')} \binom{m}{k} (1-\psi_L)^k \psi_L^{m-k} \binom{N_C-m}{m'-k} (1-\psi_A)^{N_C-m-m'+k} \psi_A^{m'-k}\,. \end{aligned} \quad (5.20)$$

Here the probability of an active client at time t_0 to be idle after τ, ψ_L and the probability of an idle client at time t_0 to be active after τ, ψ_A can respectively be represented as

$$\psi_L = (1-\beta)\left(1-e^{-(\lambda+\mu)\tau}\right) \text{ and} \quad (5.21)$$

$$\psi_A = \beta\left(1-e^{-(\lambda+\mu)\tau}\right) \quad (5.22)$$

where $\beta = \lambda/(\mu+\lambda)$. Without loss of generality, let $t=0$. Taking the expectation of both side of (5.19), we may optimally switch to the MGO mode if

$$M\left(T_S+T_M,T_S,m_c\left(0\right)\right)>\frac{1}{N_{MCS}}E\left\{\sum_{i=0}^{N_{MCS}-1}M\left(T_M,0,m_i\left(T_S\right)\right)\right\}+E\left\{M\left(T_S,T_M,m_{c'}\left(T_S\right)\right)\right\} \quad (5.23)$$

where

$$M\left(T,t_0,m_0\right)\triangleq\int_{t_0}^{t_0+T}\sum_{m=0}^{N_C}mL\left(m,m_0,\tau\right)d\tau\ . \quad (5.24)$$

The first term of the right-hand side of (5.23) takes the expectation over $m_i\left(T_S\right)$ ($i=0,\cdots,N_{MCS}-1$) since $\Pr\left[m_c\left(T_S\right)=m\right]=L\left(m,m_c\left(0\right),T_S\right)$. For other SGs, the device does not have prior knowledge on the number of WLAN clients. It can be seen that ψ_A and ψ_L converge to β and $(1-\beta)$ as the time increases, respectively. When the decisions epochs are sufficiently separated in time, it can be shown that

$$p_{M_i}\left(m\right)=\Pr\left[m_i\left(T_S\right)=m\right]=\begin{cases}L\left(m,m_i\left(0\right),T_S\right), & i=c\\ \binom{N_C}{m}\beta^m\left(1-\beta\right)^{N_C-m}, & i\neq c\end{cases}. \quad (5.25)$$

The second term of the right-hand side of (5.23) takes the expectation over $m_{c'}\left(T_S\right)$. The proposed scheme makes $m_{c'}\left(T_S\right)=\min_{i=0,\cdots,N_{MCS}-1}m_i\left(T_S\right)$ and the distribution of $m_{c'}\left(T_S\right)$ can be calculated by (5.25).

The device may not acquire perfect information on the number of the WLAN clients due to detection error. When the CORI is ρ in a certain channel, the distribution of the measured CORI $\hat{\rho}$ can be represented as [65]

$$\Pr\left[\hat{\rho}=\frac{d}{W}\right]=\binom{W}{d}\rho^d\left(1-\rho\right)^{W-d}\ \text{for}\ d=0,1,\cdots,W\ . \quad (5.26)$$

Let $d_0 = 0 \le d_1 \le \cdots \le d_{N_C} \le d_{N_C+1} = W$ be thresholds. Assume that the device detect $\hat{m}$ WLAN clients when $d_{\hat{m}} \le d \le d_{\hat{m}+1}$. The distribution of measured WLAN clients can be represented as

$$\begin{aligned} p_{\hat{M}|M}\left(\hat{m} \mid m\right) &= \sum_{d=d_{\hat{m}}}^{d_{\hat{m}+1}} \binom{W}{d} \rho^d \left(1-\rho\right)^{W-d} \\ &= \sum_{d=d_{\hat{m}}}^{d_{\hat{m}+1}} \binom{W}{d} \left(\rho_C m\right)^d \left(1-\rho_C m\right)^{W-d} \end{aligned}, \tag{5.27}$$

where $\hat{m} = 0,1,\cdots,N_C$ and $m = 0,1,\cdots,N_C$. Using the Bayes' theorem, it can be shown that

$$p_{M_i|\hat{M}_i}\left(m \mid \hat{m}\right) = \frac{p_{\hat{M}|M}\left(\hat{m} \mid m\right) p_{M_i}\left(m\right)}{\sum_{m=0}^{N_C} p_{\hat{M}|M}\left(\hat{m} \mid m\right) p_{M_i}\left(m\right)} \tag{5.28}$$

and

$$p_{\hat{M}_i}\left(\hat{m}\right) = \Pr\left[\hat{m}_i\left(T_S\right) = \hat{m}\right] = \sum_{m=0}^{N_C} p_{\hat{M}|M}\left(\hat{m} \mid m\right) p_{M_i}\left(m\right). \tag{5.29}$$

The cost of staying in the SGO mode (i.e., the left-hand side of (5.23)) can be re-arranged as

$$C_{SCS} = \sum_{m=0}^{N_C} M\left(T_S + T_M, T_S, m\right) p_{M_c|\hat{M}_c}\left(m \mid \hat{m}_c\left(0\right)\right). \tag{5.30}$$

Calculating the cost of switching to the MGO mode, it is worth notifying that the first term of the right-hand side of (5.23) is independent of the detection error. The distribution of $m_{c'}\left(T_S\right)$ is required to calculate the second term of (5.23). There may be chances to choose an SG with high CORI due to the detection error in the MGO mode. Using the Bayes' theorem, it can be shown that, for $i = 0,\cdots,N_{MCS}-1$,

$$\Pr\left[m_{c'}\left(T_s\right)=m \mid \text{Selecting } c' \text{ in MCS}\right]=$$
$$\frac{\Pr\left[\hat{m}_{c'}\left(T_S\right)\le \hat{m}_i\left(T_S\right) \mid m_{c'}\left(T_s\right)=m\right]p_{M_{c'}}\left(m\right)}{\sum_{k=0}^{N_C}\Pr\left[\hat{m}_{c'}\left(T_S\right)\le \hat{m}_i\left(T_S\right) \mid m_{c'}\left(T_s\right)=k\right]p_{M_{c'}}\left(k\right)} \tag{5.31}$$

where

$$\Pr\left[\hat{m}_{c'}\left(T_S\right)\le \hat{m}_i\left(T_S\right) \text{ for } i=0,\cdots,N_{MCS}-1 \mid m_{c'}\left(T_s\right)=m\right]=$$
$$\sum_{\hat{m}=0}^{W} p_{\hat{M}|M}\left(\hat{m}\mid m\right)\prod_{i=0}^{N_{MCS}-1}\sum_{\hat{m}_i=\hat{m}}^{W} p_{M_i}\left(\hat{m}_i\right). \tag{5.32}$$

From (5.31), the cost of switching to the MGO mode can be represented as

$$C_{MCS}=\frac{1}{N_{MCS}}\underset{\substack{m_i(T_S)\\(i=0,\cdots N_{MS})}}{E}\left\{\sum_{i=0}^{N_{MCS}-1}M\left(T_M,0,m_i\left(T_S\right)\right)\right\}+\underset{m_{c'}(T_S)}{E}\left\{M\left(T_S,T_M,m_{c'}\left(T_S\right)\right)\right\}. \tag{5.33}$$

C_{SCS} and C_{MCS} due to $\hat{m}_c\left(0\right)$ may be calculated before the deployment of BLE network. The threshold for the transition to the MGO mode can be determined by the smallest value of $\hat{m}_c\left(0\right)$, where C_{MCS} is less than C_{SCS}.

4.5. Performance evaluation

As summarized in Table 4-5, we perform performance experiments with a pair of parents-child devices using the CCI model of Chapter 2 where the average CORI is 0.3 in all bands. After randomly generating and storing 1000 interference occurrence scenarios for 500 seconds, performance experiments were performed using each interference scenario. Table 4-6 summarizes AFH parameters for the performance evaluations. Legacy BLE used the Broadcom algorithm of Chapter 4.3. We consider the use of whitelisting of 8 and 2 cycles for legacy BLE the proposed scheme, respectively.

Table 4-5. Simulation parameters for performance evaluations

Parameter	Value
Average CORI	0.3
WLAN AP	WLAN Ch. 1, 5, 9, 13
Topology	Star
Connection interval (T_{CI})	250 msec
Simulation time per iteration	500 sec (2,000 connection events)

Table 4-6. AFH parameters

Parameter	Legacy BLE	Proposed scheme
Channel classification period (T_{CCP})	4 sec	-
PLR measurement window (W)	-	8
PLR threshold (δ_{PLR})	0.15	0.15
Whitelisting interval (N_W)	8 T_{CCP}	-
Minimum number of channels ($N_{Ch}^{\min}$)	6	2
supervisionTimeout	1.5 sec ($6T_{CI}$)	-
Channel map update time (N_{Update})	-	7
Self-healing threshold ($\tau_{SH}^{SCS}, \tau_{SH}^{MCS}$)	-	(6,20)
Number of channels in an SG(K)	-	4
Number of SGs in the MGO mode (K_M)	-	4
Spacing between SGs in the MGO mode	-	8 MHz

4.5.1. Connectivity and effective CORI

Fig. 4-9 depicts the empirical cumulative distribution function (CDF) for the number of connection events that represents the connection maintenance time, i.e., the time taken from the connection establishment to the connection loss. Fig. 4-10 depicts the average of effective CORI as an empirical distribution function. Here 'Legacy-Legacy' represents the case when a pair of legacy BLE devices is connected, 'Legacy-Proposed' represents the case when a legacy BLE child device is connected to a parent device with the proposed scheme, and 'Proposed-Proposed' represents the case when a pair of devices with the proposed scheme.

When a pair of legacy BLE devices are connected, the connection is lost for about 2,000 connection events on the average, which means that the connection is lost once every 8 minutes. As seen in 4.3, legacy BLE has a low channel classification speed and does not actively perform whitelisting when the number of available channels is small. When a legacy BLE device is connected to a parent device with the proposed scheme, it can be seen the improvement of connectivity compared to a pair of legacy BLE devices. It can be seen that the connection is well kept for a duration of about 50,000 connection events (i.e., 200 minutes). This is mainly because the parent device normally operates in SGO mode comprising a small number of channels and it can quickly find an empty band using the MGO mode. It was observed that the connection loss is very rarely occurred (i.e., once in 3,200 experiments) with use the proposed algorithm. This is mainly due to that the proposed algorithm can make child devices to be synchronized with the parent device even in the transmission failure of channel map information. It can be seen from Fig. 4-10 that the proposed scheme has a low effective CORI by quickly avoiding the interference signal.

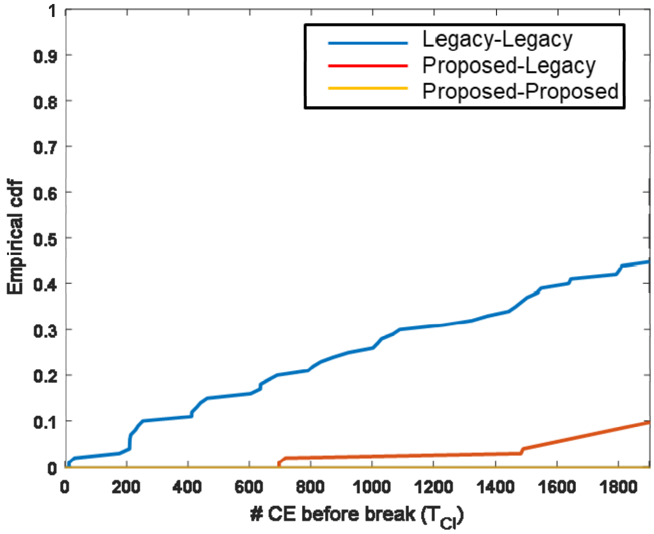


Fig. 4-9. Empirical CDF of connection maintenance

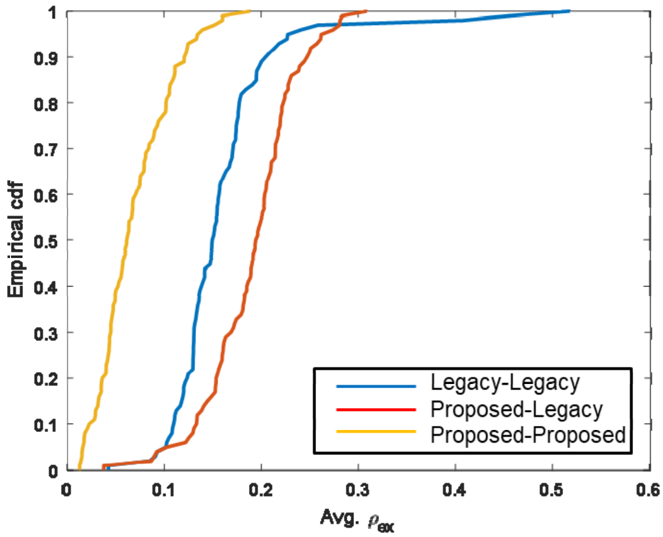


Fig. 4-10. Empirical CDF of effective CORI

4.5.2. Design of channel sets

Fig. 4-11 depicts the average of effective CORI according to the channel set configuration, when the interval between channel groups utilized in the MGO mode is 8~24 MHz and the number of channels in a channel group, K, is 3~6. Here, black indicates K = 3, and red, green and blue indicate K = 4, K = 5, and K = 6, respectively. The square indicates the case when the number of channel groups utilized in the MGO mode, N_m, is 2, the inverted triangle, and the triangles N_m = 3 and N_m = 4, respectively. It can be seen that the larger N_m, the lower the effective CORI factor regardless of K. This is mainly because the probability of finding an empty band increases due to N_m. When K = 4, the effective CORI is the lowest.

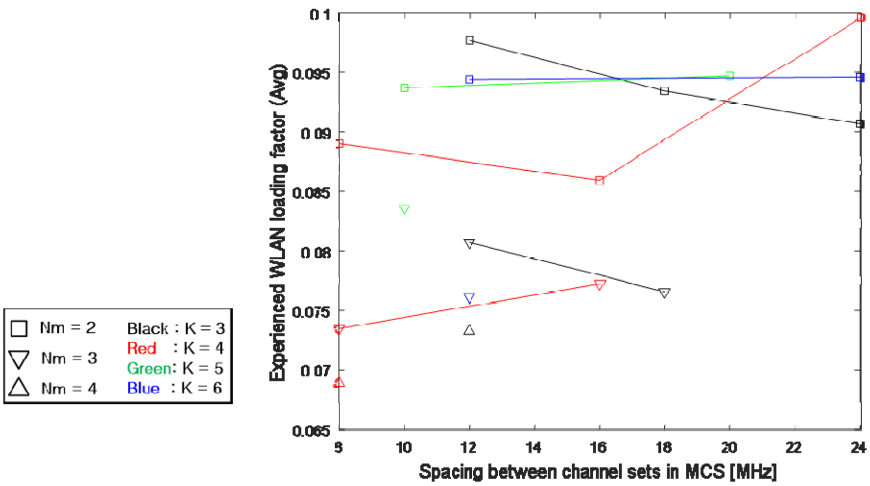


Fig. 4-11. Effective CORI due to channel group configuration

4.5.3. Hardware implementation

We implemented the proposed scheme on nRF52840 SoC [68], using mynewt RTOS [66]. Table 4-7 summarizes the memory footprint implementing the proposed scheme. It can be seen that the proposed scheme may be implemented using only 0.4 KB of RAM, which corresponds to 0.7% additional memory overhead.

During 24 hours of evaluation under the average CORI of 0.3 using four non-overlapping WLAN APs, the proposed scheme experienced link disruptions after 4000 connection events in average, yielding 99.95% of connectivity. Fig. 4-12 depicts the empirical CDF of latency. It can be seen that 99% of data is delivered in two connection intervals, showing that the proposed scheme effectively finds frequency band with low CORI.

Table 4-7. Memory footprint of hardware implementation

Parameter	Mynewt	Proposed scheme
ROM (program)	148.6 KB	+8.2 KB (+5.5%)
RAM (data)	56.3 KB	+0.4 KB (+0.7%)

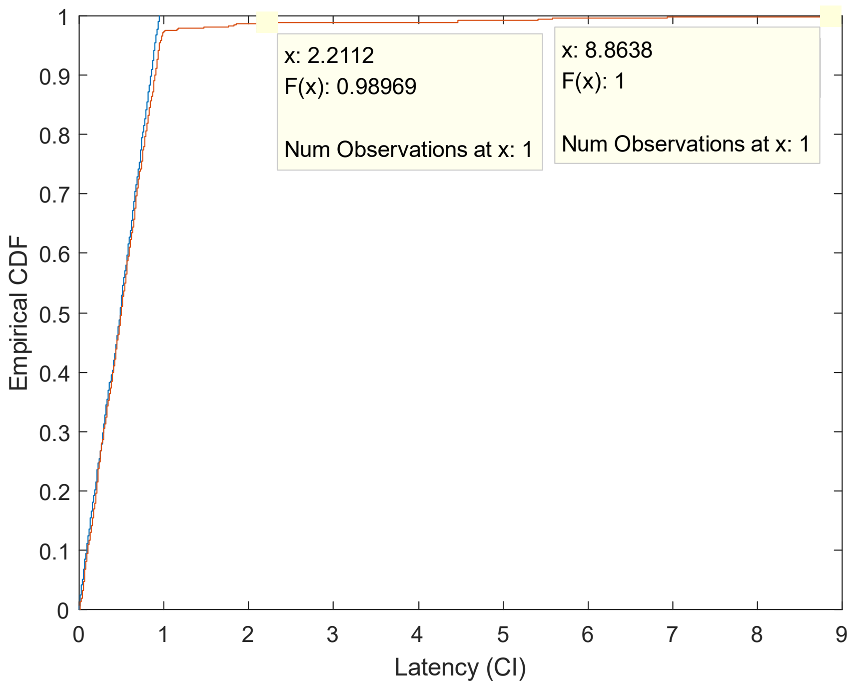


Fig. 4-12. Empirical CDF of latency (blue: CORI of 0, red: CORI of 0.3)

Chapter 5

Conclusions

In this dissertation, we have considered construction and management of large-scale low-power WSNs. We first have considered a multi-hop cluster-tree structured self-configuration scheme that guarantees the successful configuration of large-scale low-power networks while providing the backward compatibility with legacy ZigBee. We have also considered network management to mitigate inherent problems of cluster-tree structured networks, namely inflexible network structure and unbalanced power consumption.

We have considered the scalability problem of ZigBee with IEEE 802.15.4 beacon-enabled mode. The proposed scheme can guarantee full node connectivity in large-scale wireless sensor networks by placing routers in appropriate positions. The proposed scheme allows efficient data transaction since the super-frames are allocated considering data traffic. The computer simulation showed that the proposed scheme can support the construction of large-scale WSNs of up to a thousand nodes with much lower end-to-end latency and power consumption than legacy ZigBee.

We have considered interference management for BLE networks, which can fast detect and avoid the CCI. The proposed scheme may significantly reduce interference recognition time by dividing the entire band into a number of channel groups and operating by using a single channel group. Detecting the interference, it uses a union of several channel groups to the find best channel group, while keeping the connectivity. The computer simulation results showed that the proposed scheme can greatly increase the connectivity by switching the channel groups.

We summarize some interesting future researches regarding the connectivity problem of WSNs below.

- **Self-healing**: Multi-hop cluster-tree structured WSNs are quite susceptible for a link disruption of a router. This is mainly because devices reside in the sub-tree of the router also lose connection with the network, referred to the single point of failure problem [71]. Re-connecting those disconnected devices to the network, so-called self-healing, may lead to extra energy consumption as well as degradation of data transmission performance. It may be desirable to design a 'sustainable' self-healing scheme that may preserve the networking structure so that multiple self-healing procedures may be effectively handled for the entire network lifetime.
- **Role-switching**: Multi-hop cluster-tree structured WSNs may be limited in their network lifetime when operating using batteries because routers consumes 3-10

times more energy than end devices in a large/multi-hop network. It is of great concern for multi-hop cluster-tree structured WSNs to equalize of power consumption of devices. It may be desirable to design a role-switching scheme that switches role of routers and end-devices, while preserving the normal operation.

References

[1] Stankovic, J.A., "Research directions for the Internet of Things," *Internet of Things Journal*, IEEE, vol.1, no.1, pp.3,9, Feb. 2014.

[2] A. Zanella, *et al*., "Internet of Things for smart cities," *Internet of Things Journal*, IEEE,vol. 1, no.1, pp. 22-32, Feb. 2014.

[3] S. Chen, *et al*., "A vision of IoT: applications, challenges, and opportunities with China perspective," *Internet of Things Journal*, IEEE, vol.1, no.4, pp. 349-359, Aug. 2014.

[4] Jin-Seok Han, "Low-power wireless sensor networking in interference environments," Seoul National University, Feb. 2017.

[5] ZigBee Alliance. 2012. ZigBee specification r20.

[6] Bluetooth SIG. 2016. Bluetooth Standard 5.0.

[7] H.-S. Kim, J.-S. Bang, and Y.-H. Lee, "Distributed network configuration in large-scale low power wireless networks," *Computer Networks*, vol. 70, pp. 288-301, Sept. 2014.

[8] M.S. Pan, C.H. Tsai, Y.C. Tseng, "The orphan problem in ZigBee wireless networks," *IEEE Trans. Mobile Comput.*, vol. 8, issue 11, pp. 1573-1594, Nov. 2009.

[9] H.-S. Kim, J.-S. Han and Y.-H. Lee, “Scalable network joining mechanism in wireless sensor network,” in *Proc. IEEE WiSNet’12*, pp. 45-48, Jan. 2012.

[10] S. B. Attia, A. Cunha, A. Koubaa, and M. Alves, “Fault-tolerance mechanisms for ZigBee wireless sensor networks,” in *Proc. ECRTS*, July 2007.

[11] J. H. Lee, E. S. Lee, and D. S. Kim, “Network joining algorithm for mobile nodes in ubiquitous sensor networks,” in *Proc. IEEE ICCIT*, Dec. 2010.

[12] IEEE Std. 802.15.4-2006: IEEE standard for wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs), 2006.

[13] A. Koubaa, A. Cunha, M. Alves and E. Tovar, “TDBS: a time division beacon scheduling mechanism for ZigBee cluster-tree wireless sensor networks,” *Real-Time Syst. J.*, vol. 40, no. 3, pp. 321–354, Oct. 2008.

[14] P802.15.4/D6, Apr 2006 - Approved Draft Revision for IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 15.4b: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs) (Amendment of IEEE Std 802.15.4-2003).

[15] L. Yeh and M. Pan, "Beacon scheduling for broadcast and convergecast in ZigBee wireless sensor networks," *Computer Communications*, vol. 38, pp.1-12, Feb. 2014.

[16] IEEE std. 802.15.4e, Part. 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendament 1: MAC sublayer, IEEE standard for Information Technology, April 2012.

[17] W. Lee, K. Hwang, Y. Jeon and S. Choi, "Distributed fast beacon scheduling for mesh Networks," in *Proc. Mobile Adhoc and Sensor Systems (MASS)*, 2011, pp.727-732, Oct. 2011.

[18] ZigBee Alliance. 2014. ZigBee PRO Stack User Guide v2.5.

[19] A. Gupta, I. Mohammed, "Bluetooth low energy (BLE) fundamentals," *embedded*, Oct. 2016.

[20] M. Siekkinen, M. Hiienkari, J. Nurminen, "How low energy is Bluetooth low energy? Comparative measurements with ZigBee/802.15.4," in *Proc. IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, pp. 234-237, April 2012.

[21] Raul Rondon, Mikael Gidlund, Krister and Landernas, "Evaluating Bluetooth low energy suitability for time-critical industrial applications," *Int. J. Wireless Inf. Networks*, vol. 24, pp.278-290, May. 2017.

[22] Bluetooth Special Interest Group, "Mesh Profile v1.0," Jul, 2017.

[23] ERICSSON, "Bluetooth mesh networking," White paper, July, 2017.

[24] L. Leonardi, G. Patti and L. Lo Bello, “Multi-hop real-time communications over Bluetooth low energy industrial wireless mesh networks,” *IEEE Access*, vol. 6, pp. 26505-26519, May 2018.

[25] Z. Guo, I. G. Harris, L. Tsaur and X. Chen, “An on-demand scatternet formation and multi-hop routing protocol for BLE-based wireless sensor networks,” in *Proc. 2015 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1590-1595, March 2015.

[26] T. Lee, M. Lee, H. Kim and S. Bahk, “A synergistic architecture for RPL over BLE,” in *Proc. 2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pp. 1-9, June 2016.

[27] Pei Huang and Li Xiao, “The evolution of MAC protocols in wireless sensor networks: a survey,” *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, First Quarter, 2013.

[28] P. Popovski, H. Yomo and R. Prasad, “Dynamic adaptive frequency hopping for mutually interfering wireless personal area networks,” *IEEE Trans. on Mobile Computing*, vol. 5, no. 8, pp. 991-1003, Aug. 2006.

[29] H. Yomo, P. Popovski, H. C. Nguyen and R. Prasad, “Adaptive frequency rolling for coexistence in the unlicensed band,” *IEEE Trans. on Wireless Commun.*, vol. 6, no. 2, pp. 598-608, Feb. 2007.

[30] Q. Pang and V. C. M. Leung, “Channel clustering and probabilistic channel visiting techniques for WLAN interference mitigation in Bluetooth devices,"

IEEE Trans. on Electromagnetic Compatibility, vol. 49, no. 4, pp. 914-923, Nov. 2007.

[31] T. M. Taher, K. Rele and D. Roberson, “Development and quantitative analysis of an adaptive scheme for Bluetooth and Wi-Fi co-existence,” in *Proc. 2009 6th IEEE Consumer Communications and Networking Conference*, pp. 1-2, Jan. 2009.

[32] L. Stabellini, L. Shi, A. A. Rifai, J. Espino and V. Magoula, “A new probabilistic approach for adaptive frequency hopping,” in *Proc. 2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 2147-2151, Sept. 2009.

[33] K. –J. Park, et al., “Design of robust adaptive frequency hopping for wireless medical telemetry systems,” *IET Communications*, vol. 4, issue 2, pp. 178-191, Jan. 2010.

[34] S. Ben Cheikh, T. Esemann and H. Hellbrück, “SAFH - smooth adaptive frequency hopping,” in *Proc. 2011 Third International Workshop on Cross Layer Design*, pp. 1-5, Dec. 2011.

[35] B. Pang, et al., “Bluetooth low energy interference awareness scheme and improved channel selection algorithm for connection robustness,” *Sensors*, vol. 21, no. 7, p. 2257, March 2021.

[36] M. Spörk, et al., "Improving the reliability of Bluetooth low energy connections", in *Proc. Int. Conf. Embedded Wireless Systems and Networks*, pp. 144-155, Feb. 2020.

[37] J. Mast, T. Hänel and N. Aschenbruck, "Enhancing adaptive frequency hopping for Bluetooth low energy," *2021 IEEE 46th Conference on Local Computer Networks (LCN)*, pp. 447-454, October 2021.

[38] V. Poirot and O. Landsiedel. "eAFH: informed exploration for adaptive frequency hopping in Bluetooth low energy," arXiv preprint arXiv:2112.03046, Dec. 2021.

[39] J.-S. Han, H.-S. Kim, J.-S. Bang and Y.-H. Lee, "Interference mitigation in IEEE 802.15.4 networks," in *Proc. IEEE Global Commun. Conf.*, pp. 1-5, Dec. 2011.

[40] J.-S. Han, T.-H. Kim and Y.-H. Lee, "Robust transmission of the IEEE 802.15.4 signal in the presence of co-channel interference," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC),* Apr. 2013.

[41] A. Ancans et al., "Bluetooth low energy throughput in densely deployed radio environment," in *Proc. 2019 23rd International Conference Electronics*, pp. 1-5, June 2019.

[42] Wha Sook Jeon and Dong Geun Jeong, "Enhanced channel access for connection state of Bluetooth low energy networks," *IEEE Trans. on Vehicular Technology*, vol. 66, issue 9, pp. 8469-8481, Sept. 2017.

[43] C.-J. M. Liang, N. B. Priyantha, J. Liu and A. Terzis, “Surviving Wi-Fi interference in low power ZigBee networks,” in *Proc. ACM SenSys,* pp. 309-322, Nov. 2010.

[44] M. Sha, G. Hackmann and C. Lu, “Real-world empirical studies on multi-channel reliability and spectrum usage for home-area sensor networks,” *IEEE Trans. on Network and Service Management*, vol. 10, no. 1, pp. 56-69, Mar. 2013.

[45] Felix Hernandez-Campos et al., “Spatio-temporal modeling of traffic workload in a campus WLAN,” in *Proc. WICON '06: the 2nd annual international workshop on Wireless internet*, pp. 1-12, August 2006.

[46] Stefan Geirhofer and Lang Tong, “Dynamic spectrum access in WLAN channels: empirical model and its stochastic analysis,” in *Proc. TAPAS '06: the first international workshop on Technology and policy for accessing spectrum*, pp. 14-23, August 2006.

[47] Stefan Geirhofer, Lang Tong and Brian M. Sadler, “Cognitive medium access: constraining interference based on experimental models,” *IEEE J. on Selected Areas in Communications*, vol. 26, no. 1, pp.95-105, January 2008.

[48] I. Glaropoulos, et al., “Closing the gap between traffic workload and channel occupancy models for 802.11 networks,” *Ad Hoc Networks 21*, pp.60-83, May 2014.

[49] A. Paramonov, A. Vikulov and S. Scherbakov, “Practical results of WLAN traffic analysis,” *Lecture Notes in Computer Science*, vol. 10531, pp. 721-733, Sept. 2017.

[50] L. Kleinrock, Queueing Systems. Volume I: Theory, Hoboken, NJ, USA: Wiley, 1975.

[51] F. J. Massey Jr., "The Kolmogorov-Smirnov test for goodness of fit," *J. of American statistical Association*, vol. 46, no. 253, pp. 68-78, Mar. 1951.

[52] C. Na *et al.*, “An optimal GTS scheduling algorithm for time-sensitive transactions in IEEE 802.15.4 networks,” *Computer Networks*, vol. 52, no. 13, pp. 2543-2557, Sept. 2008.

[53] H. Cao *et al.*, “Employing IEEE 802.15.4 for quality of service provisioning in wireless body area sensor networks,” in *Proc. IEEE Advanced Information Networking and Applications (AINA)’10*, pp. 902-909, April 2010.

[54] A. Koubaa, M, Alves and E. Tovar, “GTS allocation analysis in IEEE 802.15.4 for real-time wireless sensor networks,” in *Proc. Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International*, pp. 25-29, April 2006

[55] Y. Wong et al., “Hybrid address configuration for tree-based wireless sensor networks,” *IEEE Commun. Lett.*, vol. 12, issue 6, pp. 414-416, June 2008.

[56] L. Yen, W. Tsai, “The room shortage problem of tree-based ZigBee/IEEE 802.15.4 wireless networks,” *ACM J. Comput. Commun.*, vol. 33, issue 4, pp. 454-462, March 2010.

[57] F. Wang, J. Liu, “Duty-cycle-aware broadcast in wireless sensor networks,” *in Proc. IEEE INFOCOM’09*, pp. 468–476, April 2009.

[58] E. Talipov *et al.*, “A lightweight stateful address autoconfiguration for 6LoWPAN,” *ACM J. Wireless Netw.*, vol. 17, issue. 1, pp. 183-197, Jan. 2011.

[59] Z. Shelby, S. Chakrabarti, and E. Nordmark, “Neighbor discovery optimization for low power and lossy networks (6LoWPAN),” *Work in progress, IETF draft-ietf-6lowpan-nd-18,* 2011.

[60] R. Holte, A. Mok, L. Rosier, I. Tulchinsky, and D. Varvel, “The pinwheel: a real-time scheduling problem,” in *Proc. the 22nd Hawaii International Conference on System Science*, vol.2, pp. 693-702, Jan. 1989.

[61] S. Pollin, et al., “Performance Analysis of Slotted Carrier Sense IEEE 802.15.4 Medium Access Layer,” *IEEE Trans. Wireless Communications,* vol.7, no.9, pp.3359-3371, Sep. 2008.

[62] P. Park, C. Fischione and K. Johansson, “Performance Analysis of GTS Allocation in Beacon Enabled IEEE 802.15.4,” in *Proc. IEEE SECON’09*, vol., no., pp.1,9, 22-26 June 2009.

[63] E. McCune, “DSSS vs. FHSS narrowband interference performance issues,” *RF Design Mag.*, pp. 90-104, Sept. 2000.

[64] J. Lansford, A. Stephens, and R. Nevo, “Wi-Fi (802.11b) and Bluetooth: enabling coexistence,” *IEEE Network*, vol. 15, no. 5, pp. 1024-31, Sept. 2001.

[65] Seung-Hwan Lee and Yong-Hwan Lee, "Adaptive frequency hopping and power control based on spectrum characteristic of error sources in Bluetooth systems," *Computers & Electrical Engineering*, vol. 36, issue 2, pp. 341-351, March 2010.

[66] Apache, Apache Mynewt, [online] Available: https://mynewt.apache.org, accessed: 2023-01-23.

[67] M. López-Benítez and J. Lehtomäki, "On the sensing sample size for the estimation of primary channel occupancy rate in cognitive radio," in *Proc. 2016 IEEE Wireless Communications and Networking Conference*, April 2016.

[68] Nordic Semiconductors. nRF52840 Specifications, 2018.

[69] M. Afaneh, "17 most popular Bluetooth low energy chipsets compared," June 2022, [online] Available: https://novelbits.io/17-most-popular-bluetooth-low-energy-chipsets-compared, accessed: 2023-01-23.

[70] C. Gomez, I. Demirkol and J. Paradells, "Modeling the maximum throughput of Bluetooth low energy in an error-prone link," *IEEE Commun. Lett.*, vol. 15, no. 11, pp.1187-1189, Nov. 2011.

[71] W. Qiu, P. Hao, and R. J. Evans, "An efficient self-healing process for ZigBee sensor networks," in *Proc. IEEE ISCIT*, Oct. 2007.

Korean Abstract

사물인터넷 (IoT)의 도래로, 물리적인 영역과 가상적인 영역을 하나로 연결하는 새로운 패러다임을 이끌어내고 있다. 무선 센서 네트워크(WSN)는 이 두 가지 영역을 매우 효율적으로 결합하는 데 중요한 역할을 할 수 있다. 이러한 역할 때문에, WSN 은 다양한 IoT 서비스 운용 환경에서 연결성, 즉, 기기 간 안정적이고 원활한 통신을 제공할 수 있어야 한다. ZigBee 와 Bluetooth Low Energy (BLE) 같은 저전력 연결 기술들이 널리 IoT 서비스에 적용되어 왔지만, 대규모 IoT 서비스 환경에서 상용화 가능한 수준의 연결성을 제공하지 못하고 있다.

본 논문은 대규모, 저전력 무선 센서 네트워크에서의 원활한 연결성을 제공하는 네트워킹 기술을 다룬다. 우선, 대규모 네트워크에서 완전한 연결성을 제공하기 어려운, 기존 ZigBee 의 다중 홉 트리 구조의 네트워킹 기술을 자녀 선택과 라우터에 대한 자원 할당에 초점을 맞추어 개선한다. 제안 기술은 우선적으로 기기들을 종단 기기로 네트워크에 가입시킨 후, 네트워크를 확장하기에 적합한 일부의 기기를 선택하여 라우터로 전환한다. 또한 데이터 트래픽과 주소 파라미터를 고려하여 라우터에 자원을 할당함으로써 쓰루풋(throughput)과 전송 지연 성능을 개선하는 한편, 네트워크의 확장성은 유지한다.

본 논문은 동일 채널 간섭이 존재하는 환경에서 적응적 주파수 도약(adaptive frequency hopping)을 사용한 BLE 의 연결성 문제도 고려한다. 제안 기술은 채널 그룹화를 통해 간섭 신호 감지 시간을 단축시킨다. 기기들은 일반 운용(normal operation) 시 하나의 채널 그룹만 사용하여 동작하고, 심한 간섭 신호가 검출되면, 여러 개의 채널 그룹을 사용함으로써 간섭 신호가 더 적은 채널 그룹을 찾을 수 있다. 간섭 신호를 빠르게 검출하고 검출 즉시 전 주파수 대역을 조사함으로써, 제안 기술은 빠르게 시변(時變)하는 간섭 신호가 존재하는 환경에서도 연결성을 유지할 수 있다.

본 논문은 컴퓨터 시뮬레이션과 하드웨어 구현을 통해 제안 기술을 검증한다. 제안 기술은 메모리 사용량 및 전력 소비를 철저히 고려하여 실제 구현이 가능하게끔 설계되었으며, ZigBee 와 BLE 의 연결성을 현저하게 향상시킬 수 있다.

주요어: 사물 인터넷, 대규모 저전력 무선 센서 네트워킹, 망 자가구축, 간섭 회피, 지그비, 저전력 블루투스.

학번: 2014-31069