ZigBee Wireless Sensor Networks and Their Applications

Meng-Shiuan Pan and Yu-Chee Tseng
Department of Computer Science
National Chiao Tung University
Hsin-Chu, 30010, Taiwan
E-mail: mspan@csie.nctu.edu.tw and yctseng@cs.nctu.edu.tw

1 Introduction

The rapid progress of wireless communication and embedded micro-sensing microelectromechanical systems (MEMS) technologies has made wireless sensor networks (WSN) possible. A WSN consists of many inexpensive wireless sensors, which are capable of collecting, storing, processing environmental information, and communicating with neighboring nodes. In the past, sensors are connected by wirelines. With the development of *ad hoc* networking technologies, tiny sensors can communicate through wireless links in a more convenient manner (Pottie and Kaiser, 2000; Sohrabi et al., 2000).

A lot of applications of WSN have been proposed. For example, wildlife monitoring applications are discussed in (FireBug 2004; GreatDuckIsland 2004) and mobile object tracking issues are addressed in (Lin and Tseng, 2004; Tseng et al., 2003). How to ensure network coverage/connectivity is discussed in (Huang et al., 2005; Yan et al., 2003). Guiding applications based on wireless sensor networks are presented in (Li et al, 2003; Tseng et al., 2006). Applications of mobile sensors are presented in (Tseng et al., 2005).

Many WSN platforms have been developed, such as MICA2, MICAz, TelosB MOTE (Xbow, 2005), and Dust Network (DustNetworks, 2005). To allow different systems to work together, standards are needed. ZigBee/IEEE 802.15.4 protocols are developed for this purpose. ZigBee/IEEE 802.15.4 is a global hardware and software standard designed for WSN requiring high reliability, low cost, low power, scalability, and low data rate. Table x.1 compares ZigBee/IEEE 802.15.4 against several other wireless technologies. The ZigBee alliance (ZigBee, 2004) is to work on the interoperability issues of ZigBee/IEEE 802.15.4 protocol stacks. The IEEE 802.15 WPAN Task Group 4 (IEEE Std 802.15.4, 2003) specifies physical and data link layer protocols for ZigBee/IEEE 802.15.4. The relationship of ZigBee and IEEE 802.15.4 is shown in Fig. x.1. In the current development, IEEE 802.15 WPAN working group creates two task groups 15.4a and 15.4b. The former is to specify an alternate physical layer, the ultra wide band (UWB) technologies. The latter is to enhance the IEEE 802.15.4 MAC protocol so that it can tightly couple with the network layer functionalities specified by ZigBee. ZigBee alliance published the version 1.0 standard in Dec. 2004.

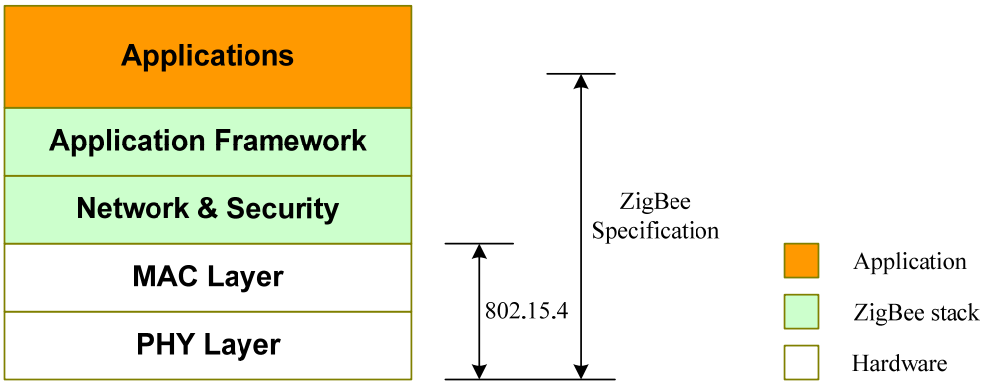

Fig. x.1. The ZigBee/IEEE 802.15.4 protocol stack.

Table x.1. Comparison of different wireless technologies (ZigBee, 2004).

Standard	ZigBee/IEEE 802.15.4	Bluetooth	UWB	IEEE 802.11 b/g
Working frequency	868/915 MHz, 2.4GHz	2.4 GHz	3.1 - 10.6 GHz	2.4 GHz
Range (m)	30 – 75+	10 – 30	~10	30 – 100 +
Data rate	20/40/250 kbps	1 Mbps	100+ Mbps	2 – 54 Mbps
Devices	255 – 65k	8		50 – 200
Power consumption	~1 mW	~40 – 100 mW	~80 – 300 mW	~160 mW – 600W
Cost ($US)	~2 – 5	~4 – 5	~5 – 10	~20 – 50

Companies such as Chipcon (Chipcon, 2005), Ember (Ember, 2005), and Freescale (Freescale, 2005) provide system-on-chip solutions of ZigBee/IEEE 802.15.4. For home networking, ZigBee/IEEE 802.15.4 can be used for light control, heating ventilation air conditioning (HVAC), security monitoring, and emergency event detection. For health case, ZigBee/IEEE 802.15.4 can integrate with sphygmomanometers or electronic thermometers to monitor patients' statuses. For industrial control, ZigBee/IEEE 802.15.4 devices can be used to improve the current manufacturing control systems, detect unstable situations, control production pipelines, and so on.

In the rest of this chapter, we will review IEEE 802.15.4 and ZigBee network layer protocols in Section 2 and Section 3, respectively. Section 4 discusses the beacon scheduling issue in a ZigBee tree network. Section 5 introduces the broadcast procedures in ZigBee. Some application examples of WSN are introduced in Section 6. Finally, we conclude this chapter in Section 7.

2 IEEE 802.15.4 Basics

IEEE 802.15.4 specifies the physical layer and data link layer protocols for low-rate wireless personal area networks (LR-WPAN), which emphasize on simple, low-cost applications. Devices in such networks normally have less communication capabilities and limited power, but are expected to operate for a longer period of time. As a result,

energy-saving is a critical design issue. In IEEE 802.15.4, there are two basic types of network topologies, the star topology and the peer-to-peer topology. Devices in a LR-WPAN and can be classified as *full function devices (FFDs)* and *reduced function devices (RFDs)*. One device is designated as the *PAN coordinator*, which is responsible for maintaining the network and managing other devices. A FFD has the capability of becoming a PAN coordinator or associating with an existing PAN coordinator. A RFD can only send or receive data from a PAN coordinator that it associates with. Each device in IEEE 802.15.4 has a unique 64-bit *long address*. After associating to a coordinator, a device will be assigned a 16-bit *short address*. Then packet exchanges between the coordinator and devices will use short addresses. In the following, the IEEE 802.15.4 physical layer and data link layer protocols are introduced.

2.1 Physical Layer (PHY)

In IEEE 802.15.4 PHY, there are three operating frequency bands with 27 radio channels. These bands are 868 MHz, 915 MHz, and 2.4 GHz. The channel arrangement is shown in Fig. x.2. Channel 0 is in the frequency 868.0~868.6 MHz, which provides a data rate of 20 kbps. Channels 1 to 10 work in frequency 902.0~928.0 MHz and each channel provides a data rate of 40 kbps. Channels 11~26 are located in frequency 2.4~2.4835 GHz and each channel provides a data rate of 250 kbps.

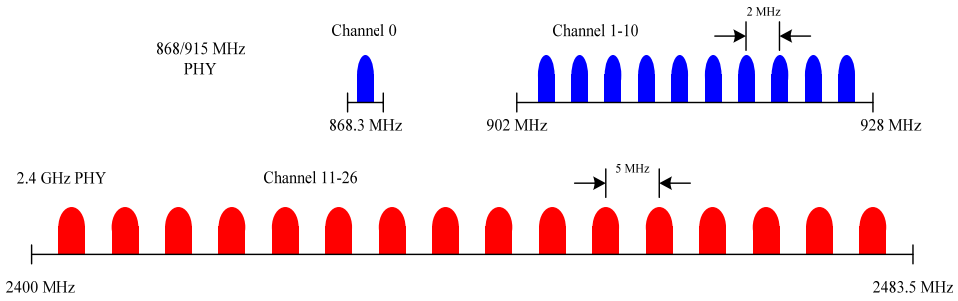

Fig. x.2. Arrangement of channels in IEEE 802.15.4.

Channels 0 to 10 use the binary phase shift keying (BPSK) as their modulation scheme, and channels 11 to 26 use the offset quadrature phase shift keying (O-QPSK) as their modulation scheme. The required receiver sensitivity should be larger than -92 dBm for channels 0 to 10, and larger than -85 dBm for channels 11 to 26. The transmit power should be at least -3 dBm (0.5 mW). The transmission radius may range from 10 meters to 75 meters. Targeting at low-rate communication systems, in IEEE 802.15.4, the payload length of a PHY packet is limited to 127 bytes.

2.2 Data Link Layer

In all IEEE 802 specifications, the data link layer is divided into two sublayers: *logical link control (LLC)* sublayer and *medium access control (MAC)* sublayer. The LLC sublayer in IEEE 802.15.4 follows the IEEE 802.2 standard. The MAC sublayer manages superframes, controls channel access, validates frames, and sends acknowledgements. The IEEE 802.15.4 MAC sublayer also supports low power operations and security mechanisms. In the following subsections, we introduce the MAC layer protocols in IEEE 802.15.4.

2.2.1 Superframe Structure

In IEEE 802.15.4, the superframe structure of a network is defined by its coordinator. The length of a superframe is equal to the time interval of two adjacent beacons sent by a coordinator. A superframe can be divided into an active portion and an inactive portion. An active portion consists of 16 equal-length slots and can be further partitioned into a *contention access period (CAP)* and a *contention free period (CFP)*. The CAP may contain i slots, i = 1, 2, …, 16, and the CFP, which follows the CAP, may contain 16-i slots. The coordinator and network devices can exchange packets during the active portion and go to sleep during the inactive portion. The superframe structure is shown in Fig. x.3.

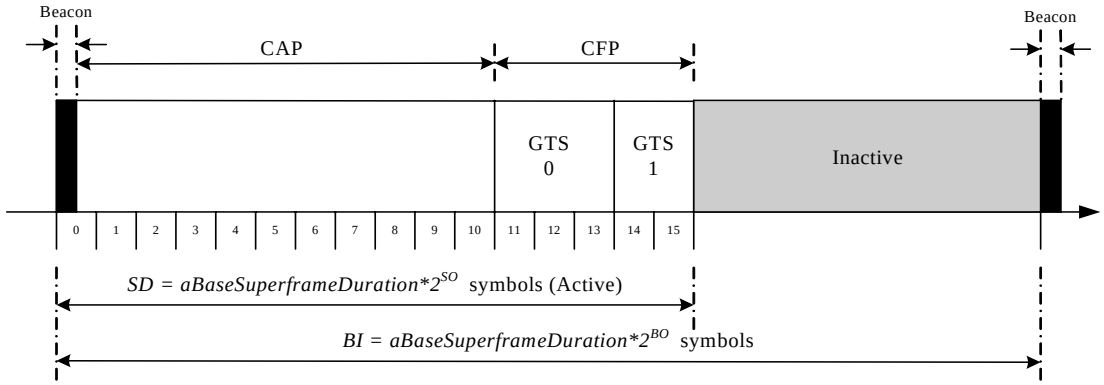

Fig. x.3. The superframe structure in IEEE 802.15.4.

Beacons are used for starting superframes, synchronizing with other devices, announcing the existence of a PAN, and informing pending data in coordinators. In a beacon-enabled network, devices use the slotted CAMA/CA mechanism to contend for the usage of channels. FFDs which require fixed rates of transmissions can ask for *guarantee time slots (GTS)* from the coordinator. A CFP can include multiple GTSs, and each GTS may contain multiple slots. For example, in Fig. x.3, GTS 0 uses three slots and GTS 1 uses two slots. A coordinator can allocate at most seven GTSs for network devices.

In IEEE 802.15.4, the structure of superframes is controlled by two parameters: *beacon order (BO)* and *superframe order (SO)*, which decide the length of a superframe and its active potion, respectively. For a beacon-enabled network, the setting of BO and SO should satisfy the relationship $0 \leqq SO \leqq BO \leqq 14$. For channels 11 to 26, the length of a superframe can range from 15.36 *ms* to 215.7 *s*, so can an

active potion. Specifically, the length of a superframe is

$$BI = aBaseSuperframeDuration \times 2^{BO} \text{ symbols,}$$

where each symbol is 1/62.5 *ms* and *aBaseSuperframDuration* = 960 symbols. Note that the length of a symbol is different for channels 0 to 10. The length of each active portion is

$$SD = aBaseSuperframeDuration \times 2^{SO} \text{ symbols.}$$

Therefore, each device will be active for $2^{-(BO-SO)}$ portion of the time, and sleep for $1-2^{-(BO-SO)}$ portion of the time. Change the value of (BO-SO) allows us to adjust the on-duty time of devices, and thus estimate the network lifetime. Table x.2 shows the relationship between (BO-SO) and duty cycle of network devices. When the value of (BO-SO) becomes larger, the duty cycle of network devices will reduce. For a non-beacon-enabled network, the values of both BO and SO will be set to 15 to indicate that superframes do not exist. Devices in a non-beacon-enabled network always use the unslotted CSMA/CA to access the channels. Since there is no superframe structure, devices can not go to sleep to save energy.

Table x.2: The relationship between (BO-SO) and the duty cycle of network devices.

BO-SO	0	1	2	3	4	5	6	7	8	9	≧10
Duty cycle (%)	100	50	25	12	6.25	3.125	1.56	0.78	0.39	0.195	< 0.1

2.2.2 Data Transfer Models

IEEE 802.15.4 defines three data transfer models: 1) data transmission to a coordinator, 2) data transmission from a coordinator, and 3) data transmission between peers. The first two models are for star networks and the last one is for peer-to-peer networks. In the following, we introduce these three data transfer models.

1. *Data transmission to a coordinator*: In a beacon-enabled network, devices that have data to send use the slotted CSMA/CA mechanism to contend for channels after receiving beacons. In a non-beacon-enabled network, devices contend for channels using the unslotted CSMA/CA mechanism. In both kinds of networks, after successfully obtaining a channel, a device can send data to its coordinator directly. A coordinator that receives a data frame from a device may reply an acknowledgement (optional). Fig. X.4 shows the procedures of data transfer to a coordinator.
2. *Data transmission from a coordinator*: Data transmission from a coordinator is based on requests from devices. In a beacon-enabled network, a coordinator should notify devices that it has buffered packets by its beacons, instead of directly sending data frames to devices. A device that receives a beacon first checks whether its ID appears in the *pending data fields* in the beacon. If so, this device sends a data request command to the coordinator. The coordinator, after receiving the data request, will reply an acknowledgement and forward the data frame to that device. On the other hand, in a non-beacon-enabled network, a

device should periodically send data request frames to query the coordinator if there are buffered packets for itself. The coordinator, on receipt of a data request frame, should check if there are frames for the sender. If so, the coordinator will reply an acknowledgement and then send a data frame to the corresponding device. The procedures of data transmission from a coordinator are shown in Fig. x.5.

3. *Data transmission between peers*: In a beacon-enabled network, peers cannot send data to each other directly. However, peers can directly transmit data to each other in a non-beacon-enabled network. The unslotted CSMA/CA mechanism is used to contend for channels.

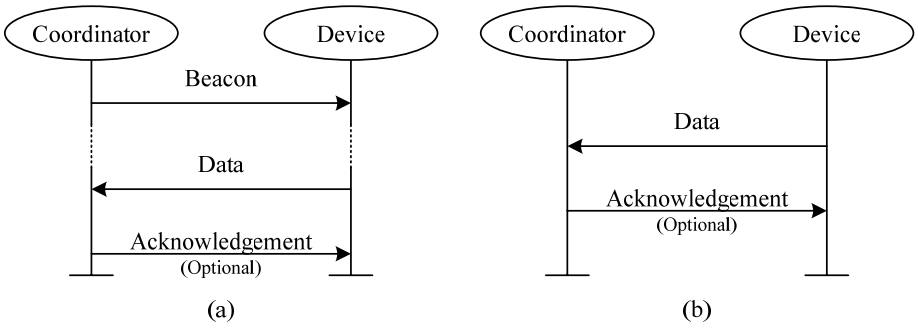

Fig. X.4. (a) Data transmission to a coordinator in a beacon-enabled network. (b) Data transmission to a coordinator in a non-beacon-enable network.

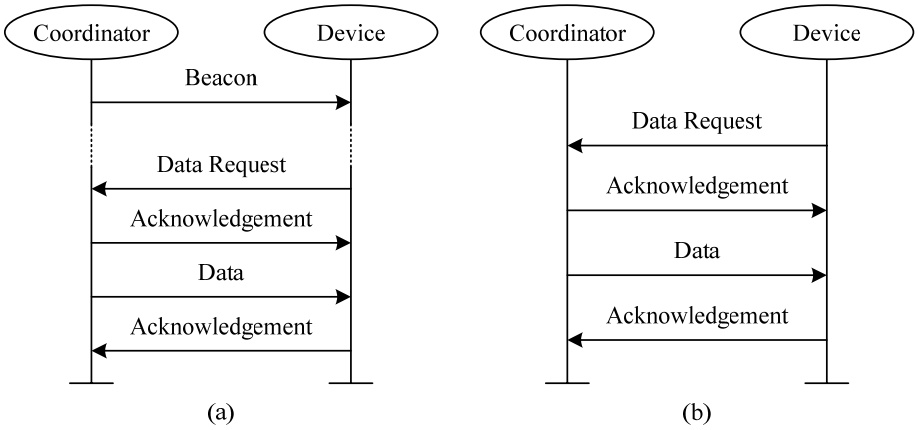

Fig. x.5. (a) Data transmission from a coordinator in a beacon-enabled network. (b) Data transmission from a coordinator in a non-beacon-enable network.

2.2.3. CSMA/CA Mechanisms

There are two channel access mechanisms in IEEE 802.15.4. One is unslotted CSMA/CA and the other is slotted CSMA/CA. The operations of unslotted CSMA/CA are similar to the ones in IEEE 802.11 CSMA/CA. A device that has a data

or command frame to send will randomly backoff a period of time. If the medium is idle when the backoff expires, this device can transmit its frame. On the other hand, if the medium is busy, this device will increase its backoff window and waits for another period of time.

The slotted CSMA/CA works differently from unslotted CSMA/CA. In the slotted CSMA/CA mechanism, the superframe structure is needed. A superframe can be further divided into smaller slots called backoff periods, each of length 20 symbols[1]. The start of the first backoff period in a superframe is aligned to the start of beacon transmission. Before transmission, a device first calculates a random number of backoff periods. After timeout, the device should perform *clear channel assessment (CCA)* twice in the upcoming two backoff periods. If the channel is found to be clear in two CCAs, the device can start to transmit a frame to the coordinator. If the channel is found to be busy in any of the two CCAs, the device should double its contention window and perform another random backoff. Fig. x.6 shows the procedures of the slotted CSMA/CA mechanism in IEEE 802.15.4.

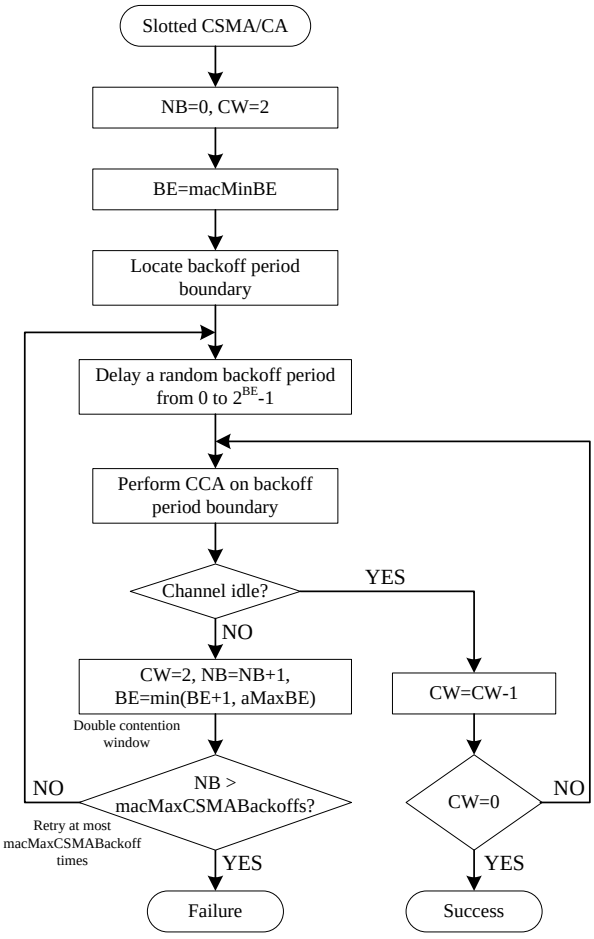

Fig. x.6. The basic slotted CSMA mechanism in IEEE 802.15.4.

[1] The time required to transmit a symbol varies according to working bands of PHY. For example, in the 2.4 GHz band, the length of a symbol is 16 us; hence, in the 2.4 GHz band, a unit backoff period is 320 us.

2.2.4. Association and Disassociation Procedures

A device becomes a member of a PAN by associating with its coordinator. At the beginning, a device should scan channels to find potential coordinators. After choosing a coordinator, the device should locate the coordinator's beacons and transmit an association request command to the coordinator. In a beacon-enabled network, the association request is sent in the CAP of a superframe. In a non-beacon-enabled network, the request is sent by the unslotted CSMA/CA mechanism. On receipt of the association request, the coordinator will reply an ACK. Note that correctly receiving an ACK does not mean that device has successfully associated to the coordinator; the device still has to wait for an association decision from the coordinator. The coordinator will check its resource to determine whether to accept this association request or not. In IEEE 802.15.4, association results are announced in an indirect fashion. A coordinator responds to association requests by appending devices' long addresses in beacon frames to indicate that the association results are available. If a device finds that its address is appended in a beacon, it will send a data request to the coordinator to acquire the association result. Then the coordinator can transmit the association result to the device. The association procedure is summarized in Fig. x. 7.

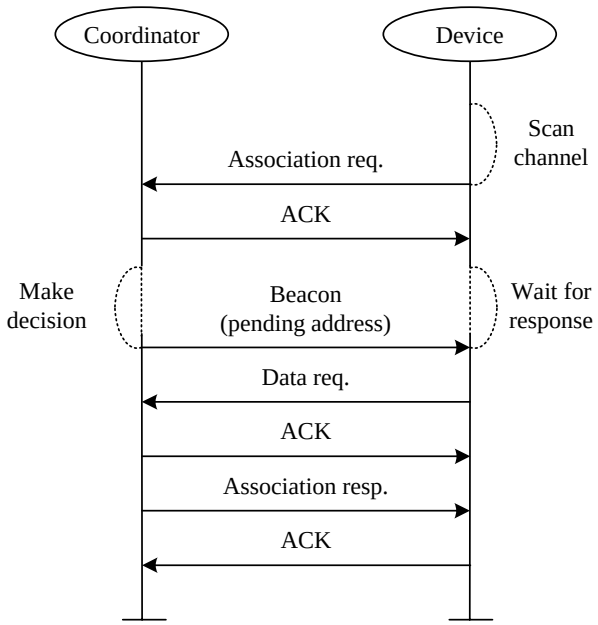

Fig. x. 7. The association procedure in IEEE 802.15.4.

When a coordinator would like an associated device to leave its PAN, it can send a disassociation notification command to the device. After receiving this command, the device will reply an ACK. If the ACK is not correctly received, the coordinator will still consider that the device has been disassociated. When an associated device wants to leave a PAN, it also sends a disassociation notification command to the coordinator. On receipt of the command, the coordinator will reply an ACK and

remove the records of the correspond device. Similar to the above case, the device considers itself disassociated even if it does not receive an ACK from the coordinator.

2.3. Summary of IEEE 802.15.4

IEEE 802.15.4 specifies the physical layer and data link layer protocol for low-rate wireless personal area networks. However, this specification only concerns communications between devices that are within each other's transmission range. For larger sensor networks, the support of network layer protocols is needed. In the next section, we will introduce a developing standard, ZigBee, which supports protocols above the data link layer for connecting IEEE 802.15.4 devices together.

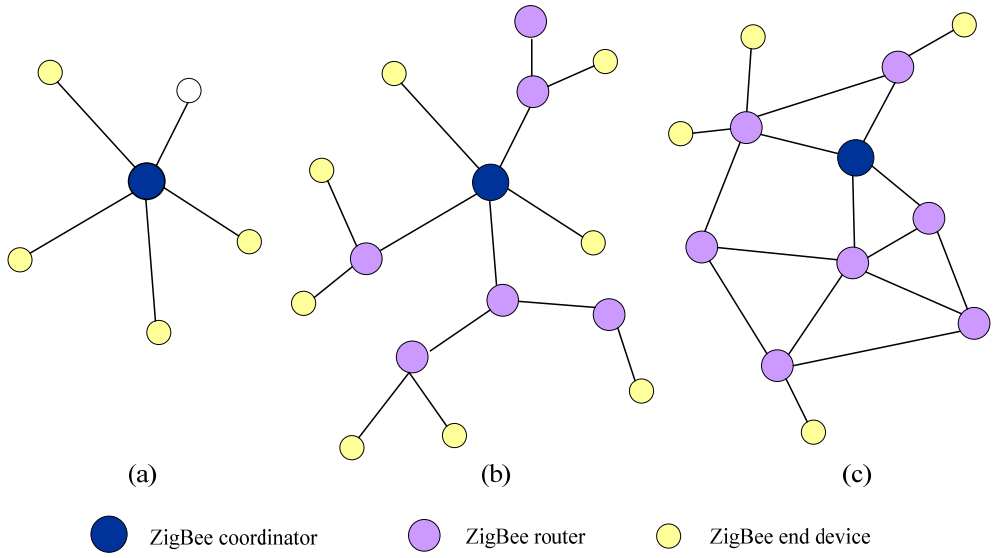

Fig. x. 8. Zigbee network topologies: (a) star, (b) tree, and (c) mesh.

3 ZigBee Network Layer

In ZigBee, the network layer provides reliable and secure transmissions among devices. Three kinds of networks are supported, namely star, tree, and mesh networks. A ZigBee coordinator is responsible for initializing, maintaining, and controlling the network. A star network has a coordinator with devices directly connecting to the coordinator. For tree and mesh networks, devices can communicate with each other in a multihop fashion. The network backbone is formed by one ZigBee coordinator and multiple ZigBee routers. RFDs can join the network as end devices by associating with the ZigBee coordinator or ZigBee routers. In a tree network, the coordinator and routers can announce beacons. However, in a mesh network, regular beacons are not allowed. Devices in a mesh network can only communicate with each other by peer-to-peer transmissions specified in IEEE 802.15.4. Some example of ZigBee network topologies are shown in Fig. x. 8.

3.1 Network Formation

Devices that are coordinator-capable and do not currently join a network can be candidates of ZigBee coordinators. A device that desires to be a coordinator will scan all channels to find a suitable one. After selecting a channel, this device broadcasts a beacon containing a PAN identifier to initialize a PAN. A device that hears beacons of an existing network can join this network by performing the association procedures and specifying its role, as a ZigBee router or as an end device. The beacon sender will determine whether to accept this device or not by considering its current capacity and its permitted association duration. Then the association response can be carried by its beacons. If a device is successfully associated, the association response will contain a short 16-bit address for the request sender. This short address will be the network address for that device.

3.2 Address Assignment in a ZigBee Network

In a ZigBee network, network addresses are assigned to devices by a distributed address assignment scheme. After forming a network, the ZigBee coordinator determines the maximum number of children (*Cm*) of a ZigBee router, the maximum number of child routers (*Rm*) of a parent node, and the depth of the network (*Lm*). Note that $Cm \geqq Rm$ and a parent can have (*Cm*-*Rm*) end devices as its children. In this algorithm, addresses of devices are assigned by their parents. For the coordinator, the whole address space is logically partitioned into *Rm*+1 blocks. The first *Rm* blocks are to be assigned to the coordinator's child routers and the last block is reversed for the coordinator's own child end devices. In this scheme, a parent device utilizes *Cm*, *Rm*, and *Lm* to compute a parameter called *Cskip*, which is used to compute the starting addresses of its children's address pools. The *Cskip* for the ZigBee coordinator or a router in depth *d* is defined as:

$$Cskip(d) = \begin{cases} 1 + Cm \cdot (Lm - d - 1), & \text{if } Rm = 1 \quad \Lambda\,\Lambda\,\Lambda\,\Lambda \text{ (a)} \\ \dfrac{1 + Cm - Rm - Cm \cdot Rm^{Lm-d-1}}{1 - Rm}, & \text{Otherwise} \quad \Lambda\,\Lambda\,\Lambda\,\Lambda \text{ (b)} \end{cases} \tag{1}$$

The coordinator is said to be at depth 0; a node which is a child of another node at depth *d* is said to be at depth *d*+1. Consider any node *x* at depth *d*, and any node *y* which is a child of *x*. The value of *Cskip(d)* indicates the maximum number of nodes in the subtree rooted at *y* (including *y* itself). For example, in Fig. x. 9, since the *Cskip* value of B is 1, the subtree of C will contain no more than 1 node; since the *Cskip* value A is 7, the subtree of B will contain no more than 7 nodes. To understand the formulation, consider again the nodes *x* and *y* mentioned above. Node *y* itself counts for one node. There are at most *Cm* children of *y*. Among all children of *y*, there are at most *Rm* routers. So there are at most *CmRm* grandchildren of *y*. It is not hard to see that there are at most $CmRm^2$ great grandchildren of *y*. So the size of the subtree rooted at *y* is bounded by

$$Cskip(d) = 1 + Cm + CmRm + CmRm^2 + \ldots\ldots + CmRm^{Lm-d-2}, \tag{2}$$

since the depth of the subtree is at most *Lm-d-1*. We can derive that

$$\text{Eq. 2} = 1+Cm(1+Rm+Rm^2+ \ldots\ldots + Rm^{Lm-d-2})$$

$$= 1+Cm(1- Rm^{Lm-d-1})/(1-Rm)$$

$$= \text{Eq. 1(b)}$$

Address assignment begins from the ZigBee coordinator by assigning address 0 to itself and depth d=0. If a parent node at depth d has an address A_{parent}, the nth child router is assigned to address $A_{parent}+(n-1)\times Cskip(d)+1$ and nth child end device is assigned to address $A_{parent}+Rm\times Cskip(d)+n$. An example of the ZigBee address assignment is shown in Fig. x. 9. The *Cskip* of the ZigBee coordinator is obtained from Eq. 1 by setting d=0, Cm=6, Rm=4, and Lm=3. Then the 1st, 2nd, and 3rd child routers of the coordinator will be assigned to addresses 0+(1-1)×31+1=1, 0+(2-1)×31+1=32, and 0+(3-1)×31+1=63, respectively. And the two child end devices' addresses are 0+4×31+1=125 and 0+4×31+2=126.

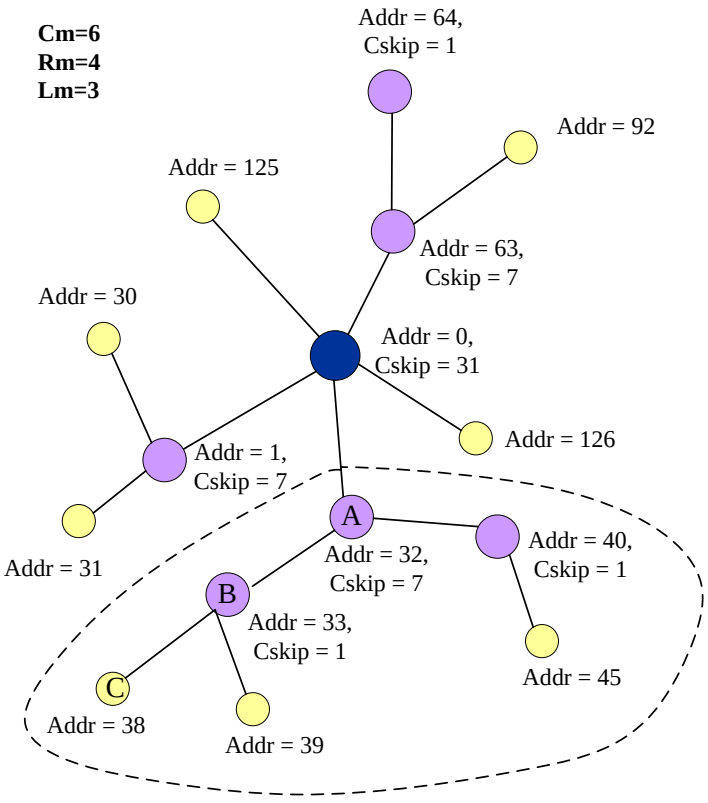

Fig. x. 9. An address assignment example in a ZigBee network.

3.3 Routing Protocols

In a tree network, the ZigBee coordinator and routers transmit packets along the tree. When a device receives a packet, it first checks if it is the destination or one of its child end devices is the destination. If so, this device will accept the packet or forward

this packet to the designated child. Otherwise, it will relay packet along the tree. Assume that the depth of this device is *d* and its address is *A*. This packet is for one of its descendants if the destination address A_{dest} satisfies $A < A_{dest} < A + Cskip(d\text{-}1)$, and this packet will be relayed to the child router with address

$$A_r = A + 1 + \left\lfloor \frac{A_{dest} - (A+1)}{Cskip(d)} \right\rfloor \times Cskip(d) .$$

If the destination is not a descendant of this device, this packet will be forwarded to its parent.

In a mesh network, ZigBee coordinators and routers are said to have *routing capacity* if they have routing table capacities and route discovery table capacities. Devices that are routing-capable can initiate routing discovery procedures and directly transmit packets to relay nodes. Otherwise, they can only transmit packets through tree links. In the latter case, when receiving a packet, a device will perform the same routing operations as described in tree networks. When a node needs to relay a received packet, it will first check whether it is routing-capable. If it is routing-capable, the packet will be unicast to the next hop. Otherwise, the packet will be relayed along the tree.

A device that has routing capacity will initiate route discovery if there is no proper route entry to the requested destination in its routing table. The route discovery in a ZigBee network is similar to the AODV routing protocol (Perkins et al., 2003). Links with lower cost will be chosen into the routing path. The cost of link *l* is defined based on the packet delivery probability on link *l*. However, how to calculate the packet delivery probability is not explicitly stated in the ZigBee specification.

At the beginning of a route discovery, the source broadcasts a route request packet. A ZigBee router that receives a route request packet first computes the link cost. If this device has routing capacity, it will rebroadcast this request if it does not receive this request before or the link cost recorded in route request plus the cost it just computed is lower than the former received request. Otherwise, it will discard this request. For the case that a ZigBee router that is not routing capable receives a route request, it also determines whether to resend this request based on the same comparison. If this device determines to resend this route request, it will check the destination address and unicast this route request to its parent or to one of its children (in the tree network). An example is shown in Fig. x. 10. In Fig. x. 10, device S broadcasts a route request for destination T and devices A and D receive this packet. Since device A has no routing capacity, it will check the address of destination T and unicast this request to device C. Since device D has routing capacity, it will rebroadcast this request. A device that has resent a route request packet will record the request sender in its route discovery table. This information will be discarded if this device does not receive a route reply within a time interval.

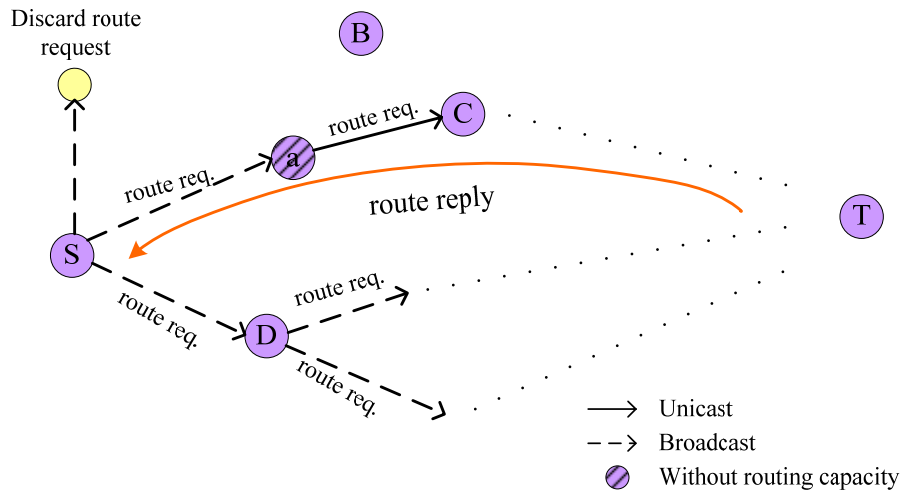

Fig. x. 10. An example of route request dissemination in a ZigBee network.

When the destination receives route request packets from multiple paths, it will choose the routing path with the lowest cost and send a route reply packet to the source. The route reply packet will be sent by unicast. An intermediate node that receives the route reply packet checks its route discovery table and sends the route reply to the request sender. After the source node successfully receives the route reply, it can send data packets to the destination node along the discovered route.

The ZigBee network layer also specifies route maintenance mechanisms for mesh and tree networks. In a mesh network, route failure is detected by a failure counter. If the counter of a ZigBee router exceeds a threshold, the router can start the route maintenance procedure. For those routers that have routing capacity, they can flood route request packets to find destinations. For routers that do not have routing capacity, they will unicast route request packets to their parents or children according to the destination addresses. However, in a tree network, a router does not broadcast route request packets when it loses its parent. Instead, it disassociates with its parent and tries to re-associate with a new parent. After re-association, it will receive a new short 16-bit network address and can transmit packets to its new parent. Note that a device that re-associates to a new parent will disconnect all its children. Those children that lose their parents will also try to find new parents. On the other hand, when a router cannot send packets to a child, it will directly drop this packet and send a route error message to the packet originator. Then this router will send a disassociation notification command to the child. The disassociated child may reconnect to the same parent or find a new parent depending on its new scan result.

3.4 Summary of the ZigBee Network Layer

ZigBee is designed to support low-cost network layer. It supports three kinds of network topologies, which are star, tree, and mesh networks. Network developers can choose a suitable network topology for their applications. The pros and cons of these three topologies are summarized in Table x. 3.

Table x. 3. Pros and cons of different kinds of ZigBee network topologies.

	Pros	Cons
Star	1. Easy to synchronize 2. Support low power operation 3. Low latency	1. Small scale
Tree	1. Low routing cost 2. Can form superframes to support sleep mode 3. Allow multihop communication	1. Route reconstruction is costly 2. Latency may be quite long
Mesh	1. Robust multihop communication 2. Network is more flexible 3. Lower latency	1. Cannot form superframes (and thus cannot support sleep mode) 2. Route discovery is costly 3. Needs storage for routing table

4 Beacon Scheduling in ZigBee Tree Networks

In a tree network, the ZigBee coordinator and routers can transmit beacons. Sending beacons facilitates devices to synchronize with their parents and thus can support devices to go to sleep and save energy. Recall that after forming a network, the network coordinator will determine the beacon order (BO) and superframe order (SO). When BO is larger than SO, devices can go to sleep during the inactive portions of superframes. In the ZigBee network specification version 1.0, a superframe can be divided into 2^{BO-SO} non-overlapping time slots. A router can choose a slot to announce its beacon. The start time of its beacons is also the start time of superframes of that router. Therefore, routers' superframes will be shifted away from those of the coordinator's by multiples of SD.

To avoid collisions, a device should not arbitrarily choose a slot to transmit its beacons. A device should avoid using the same beacon transmit slots as its neighbors' and its parent's; otherwise, its children may lose beacons due to collisions. Beacon collisions may occur in two ways: *direct beacon conflict* between two neighbors (refer to Fig. x. 11(a)) and *indirect beacon conflict* between non-neighbors (refer to Fig. x. 11(b)). In Fig. x. 11(b), since A and B are not neighbors, the conflict is more difficult to detect. The ZigBee network specification version 1.0 does not provide an explicit solution to this problem. In the current specification, a device should keep the beacon transmission schedules of its neighbors and its neighbor's parents. In other words, beacon transmission schedules of nodes within two hops should be maintained. The same slots should be avoided. When sending beacons, a device will add the time offset between its beacon transmission time and its parent's in the beacon payload. This will help a device to choose a conflict-free slot.

In a tree network, a device decides its beacon transmission time when joining the network. During the joining procedure, a device listens to the beacons from its parent and its neighbors for a period of time. Then the device calculates an empty slot as its beacon transmission slot. If there is no available slot, this device will join this network as an end device. After deciding beacon transmission time, the network layer will inform the MAC layer the time difference between its beacon transmission time and

its associated parent's beacon transmission time.

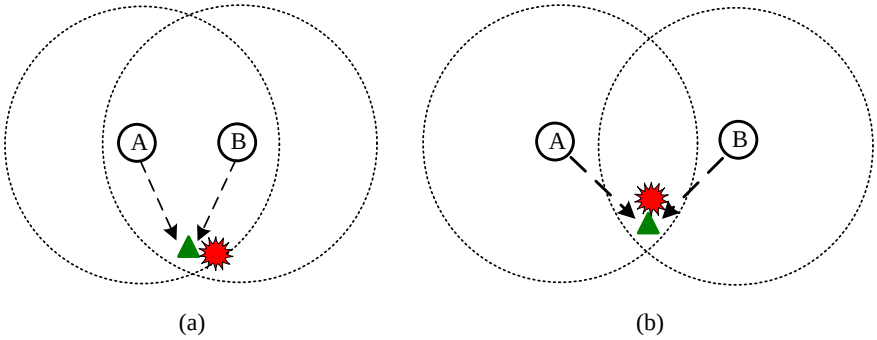

Fig. x. 11. Beacon conflicts in a ZigBee tree network: (a) direct beacon conflict and (b) indirect beacon conflict.

5. Broadcasting in ZigBee Networks

The ZigBee network specification version 1.0 defines the broadcast procedure in mesh networks. The network layer informs the MAC layer to broadcast network-layer packets. In ZigBee, the broadcast initiator can specify the scope of this broadcast. A device that receives a broadcast packet will check whether the radius field in the broadcast packet is larger than zero. If so, the device will rebroadcast the packet; otherwise, this packet will not be further broadcast. ZigBee defines a passive acknowledgement mechanism to ensure the reliability of broadcasting. After broadcasting, the ZigBee device records the sent broadcast packet in its *broadcast transaction table (BTT)*. The BTT will be combined with its neighbor table. This allows devices to track whether their broadcast packets have been properly rebroadcast or not. If a device finds that a neighbor does not rebroadcast, it will rebroadcast to guarantee reliability.

In ZigBee, devices use different strategies to broadcast packets according to the parameter *maxRxOnWhenIdle* in the MAC layer. *maxRxOnWhenIdle* controls whether a device can receive data when idle. By the nature of wireless communication, devices can detect radio signals when idle. However, they will refuse to process the received signals if *maxRxOnWhenIdle* is False. When broadcasting is needed, a device with *maxRxOnWhenIdle* = True will do so immediately. This device will also unicast the broadcast packet to those neighbors with *macRxOnWhenIdle* set to False. On the other hand, a device with *macRxOnWhenIdle* set to False can only unicast the broadcast packet to its neighbors. This is because that the device may miss passive acknowledgements from neighbors. Unicasting can ensure reliability. Fig. x. 12 shows an example that router A sets *macRxOnWhenIdle* to False. After receiving the broadcast packet from S, A will relay the packet to B and C by unicasting.

However, broadcasting in ZigBee network may cause redundant transmissions. Reference (Ding et al., 2006) introduces a tree-based broadcast scheme to relieve this

problem. The authors utilize the properties of ZigBee address assignment to find a set of forwarding nodes in the network. The proposed algorithm incurs low computation cost.

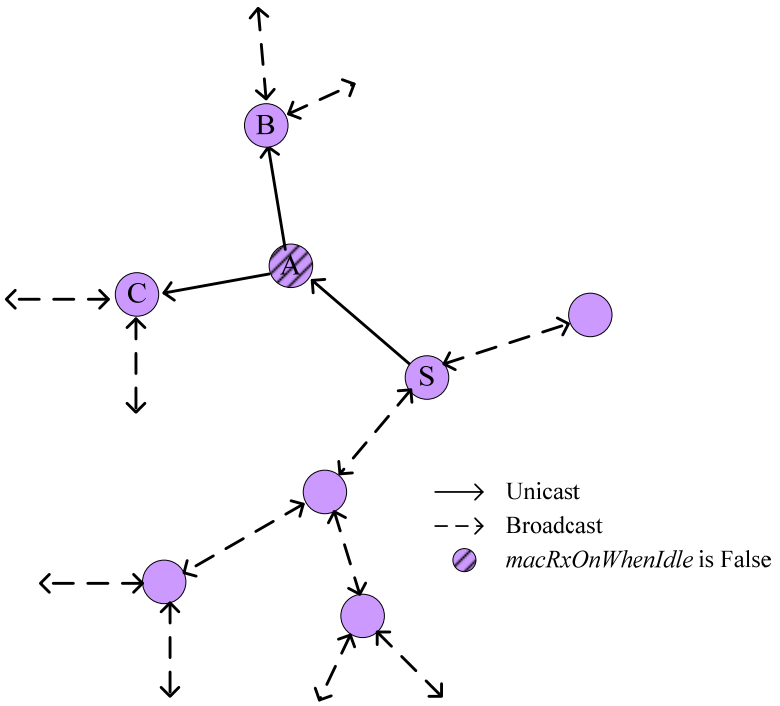

Fig. x. 12. A broadcast example in a ZigBee Network.

6 Applications of Wireless Sensor Networks

Many research institutes have developed various applications of wireless sensor networks. In this section, we introduce two such applications: medical care and emergency guiding. The underlying communication protocols in these systems are all based on ZigBee/IEEE 802.15.4 or similar protocols.

6.1 Medical Care Applications

Harvard University and Boston University have developed a medical care application called CodeBlue based on wireless sensor networks (Lorincz et al, 2004). CodeBlue is a remote medical care system. Patients can be well monitored no matter they are in hospital or at home. Two wearable sensors, wireless pulse oximeter sensor and 2-lead electrocardiogram sensor, have been developed on MICA2 MOTE and Telos MOTE platforms (Xbow, 2005) to detect patients' physiological statuses. These sensors can be used to collect heart rates and oxygen saturation information. Sensors use an ad hoc routing protocol to send information to a sink. The sink keeps track of patients' statuses so that doctors can make remote diagnoses. Moreover, wireless sensors are

integrated with PDAs. Patients and rescuers can watch for vital signs on PDAs in a real-time fashion. When detecting abnormal events from patients, sensors will automatically alert nearby hospitals or doctors. Rescuers can quickly locate patients by location tracking services implemented in CodeBlue.

Reference (Ho et al., 2005) integrates wireless sensor networks with the RFID technology to develop an elder healthcare application. This system utilizes RFID to identify medications and uses wireless sensors to monitor if elders take right medications. Each medication has an unique ID. A patient wears a RFID reader connected to a MOTE. When the patient moves a medication bottle, a weight sensor on the bottom of this bottle can detect this event. This system can monitor whether the patient doses the right medication or the correct amount of drugs and generate alarms when necessary. Moreover, this system tracks elders by equipping RFID tags on them. When elders do not take medications on time, this system will generate alarms to them.

6.2 Fire Emergency Applications

The University of California at Berkeley developed a project called Fire Information and Rescue Equipment (FIRE, 2005) to improve fire-fighting equipments. It can protect fire fighters and help to relieve victims. Fire fighters are equipped with a Telos mote, a wearable computer, and a fireproof mask called FireEye. Wireless smoke and temperature sensors are deployed in a building to monitor the environment. When a fire emergency occurs, wireless sensor can provide real-time emergency-related information, which can be shown on the FireEye. FireEye mask can also show other fire fighters' locations. The Telos sensor monitors fire fighter's heart rate and air tank level and propagates the information to other fire fighters.

In some situations, fire fighters may not be able to go into the fire scenes. The integrated mobile surveillance and wireless sensor (iMouse) system (Tseng et al., 2005) supports a mobile sensor car to help monitoring a fire emergency. The iMouse system consists of some wireless sensors deployed in a building and a mobile sensor car. This mobile sensor car is equipped with a WebCam, a wireless LAN card, and a Stargate (Xbow, 2005). At normal time, sensors are responsible for monitoring the environment. When a fire emergency is detected, the mobile sensor car can utilize the information reported from sensors and find a shortest path to visit all emergency sites. After moving to each emergency site, the mobile sensor car will take snapshots around this site and send back these pictures through its WLAN interface. The architecture of the iMouse system is shown in Fig. x. 13.

In a fire emergency, another important issue is to safely guide people inside the emergency scene to exits. Reference (Tseng et al., 2006) designs a distributed emergency navigation algorithm to achieve this goal. As in the previous systems, sensors are responsible for monitoring the environment at normal time. When emergencies occur, sensors will identify hazardous regions. After locating hazardous regions, each sensor will compute a safe guidance direction to one of the exits in a distributed manner. In this system, sensors will avoid leading people to go through hazardous regions. When passing hazardous regions is inevitable, sensors can also guide people as farther away from emergency locations as possible. Fig. x. 14 shows the guidance interface developed in (Tseng et al., 2006). The guiding direction will be

shown on the LED panel depending on the judgement of the sensor attached to the LED panel.

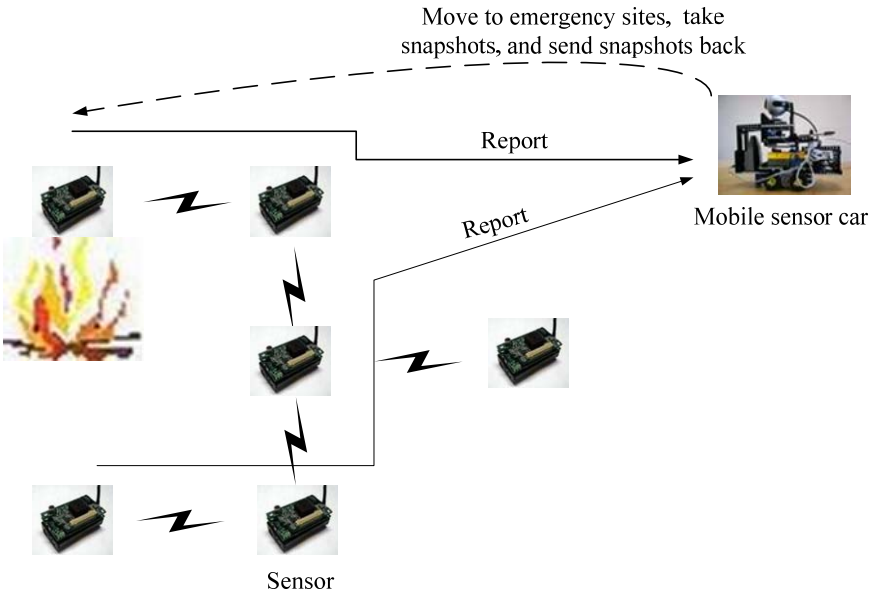

Fig. x. 13. The iMouse system architecture.

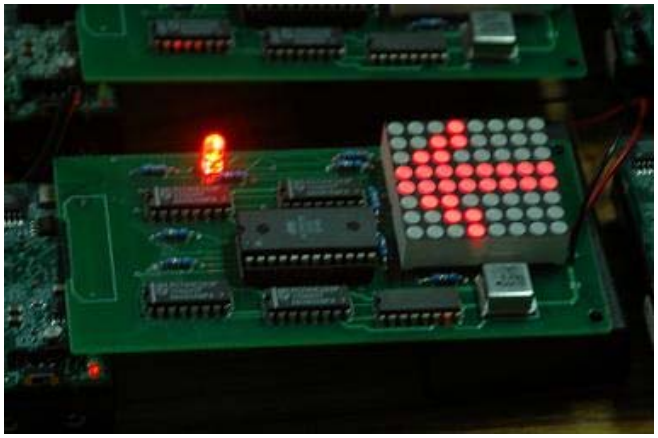

Fig. x. 14. The guiding interface developed in (Tseng et al., 2006) for emergency guidance applications.

7 Summary

In this chapter, we have introduced the design of IEEE 802.15.4 and ZigBee network layer protocols. A lot of research institutes and industrial companies have developed their sensor platforms based on ZigBee/IEEE 802.15.4 solutions. ZigBee and IEEE 802.15.4 are designed for lightweight sensor platforms. We have also addressed some

applications such as medical care and fire emergency applications and some prototyping systems. For further readings, (Intanagonwiwat et al., 2003; Schurgers and Srivastava, 2001) address routing protocols and (Dam and Langendoen, 2003; Gandham et al., 2005; Ye et al., 2002) discuss energy efficient MAC protocols in WSN.

Reference

Chipcon (2005) Chipcon corporation. http://www.chipcon.com/

Dam T, Langendoen K (2003) An adaptive energy-efficient MAC protocol for wireless sensor networks. In Proc. of ACM Int'l Conf. on Embedded Networked Sensor Systems (SenSys)

Ding G, Sahinoglu Z, Orlik P, Zhang J, Bharhava B (2006) Tree-based data broadcast in IEEE 802.15.4 and ZigBee Networks, IEEE Transations on Mobile Computing (to appear)

DustNetworks (2005) Dust network Inc. http://dust-inc.com/flash-index.shtml

Ember (2005) Ember – Wireless semiconductor. http://www.ember.com/

FireBug (2004) Design and construction of a wildfire instrumentation system using networked sensors. http://firebug.sourceforge.net/

FIRE (2005) The fire information and rescue equipment (FIRE) project. http://kingkong.me.berkeley.edu/fire/

Freescale (2005) Freescale semiconductor. http://www.freescale.com

Gandham S, Dawande M, Prakash R (2005) Link scheduling in sensor networks: Distributed edge coloring revisited. In *Proc. of IEEE INFOCOM*

GreatDuckIsland (2004) Habitat monitoring on great duck island. http://www.greatduckisland.net/technology.php

IEEE Std 802.15.4 (2003) IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks specific requirements part 15.4: wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs)

Ho L, Moh M, Walker Z, Hamada T, Su C (2005) A prototype on RFID and sensor networks for elder healthcare: progress report, In Proc. of SIGCOMM workshop on Experimental approaches to wireless network design and analysis

Huang C, Lo L, Tseng Y, Chen W (2005) Decentralized energy-conserving and coverage-preserving protocols for wireless sensor networks, In Proc. Int'l Symp. on Circuits and Systems (ISCAS)

Intanagonwiwat C, Govindan R, Estrin D, Heidemann J, Silva F (2003) Directed diffusion for wireless sensor networking. IEEE/ACM Trans. Networking, 11(1):2–16

Li Q, DeRosa M, Rus D (2003) Distributed algorithm for guiding navigation across a sensor network. In Proc. of ACM Int'l Symp. on Mobile Ad Hoc Networking and Computing (MobiHOC)

Lin C, Tseng Y (2004) Structures for in-network moving object tracking in wireless sensor networks. In Proc. of Broadband Wireless Networking Symp (BroadNet)

Lorincz K, Malan D, Fulford-Jonse T, Nawoj A, Clavel A, Shnayder V, Mainland G, Moulton S, Welsh M (2004) Sensor networks for emergency response: challenges and opportunities, IEEE pervasive computing, special issue on pervasive computing for first response, Oct-Dec, 2004

Perkins C, Belding-Royer E, Das S (2003) Ad hoc on-demand distance vector (AODV)

routing. IETF RFC (3561)
Pottie G, Kaiser W (2000) Wireless integrated network sensors. Commun. ACM, 43(5):51–58
Schurgers C, Srivastava M (2001) Energy efficient routing in wireless sensor networks. In Proc. of Military Communications Conference (MILCOM)
Sohrabi K, Gao J, Ailawadhi V, Pottie G (2000) Protocols for self-organization of a wireless sensor network. IEEE Personal Commun., 7(5):16–27
Tseng Y, Kuo S, Lee H, Huang C (2003) Location tracking in a wireless sensor network by mobile agents and its data fusion strategies. In Proc. of Int'l Symp. on Information Processing in Sensor Networks (IPSN)
Tseng Y, Wang Y, Cheng K (2005) An integrated mobile surveillance and wireless sensor (iMouse) system and its detection delay analysis. In ACM/IEEE International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM)
Tseng Y, Pan M, Tsai Y (2006) A distributed emergency navigation algorithm for wireless sensor networks. IEEE Computer (to appear)
Xbow (2005) Crossbow technology inc. http://www.xbow.com/
Yan T, He T, Stankovic J (2003) Differentiated surveillance for sensor networks. In *ACM Int'l Conf. on Embedded Networked Sensor Systems (SenSys)*
Ye W, Heidemann J, Estrin D (2002) An energy-efficient MAC protocol for wireless sensor networks. In Proc. of IEEE INFOCOM
ZigBee (2004) ZigBee Alliance. http://www.zigbee.org