1ST QUARTER 2008, VOLUME 10, NO. 1

IEEE COMMUNICATIONS SURVEYS
The Electronic Magazine of Original Peer-Reviewed Survey Articles

www.comsoc.org/pubs/surveys

MESHED HIGH DATA RATE PERSONAL AREA NETWORKS

SAHIBZADA ALI MAHMUD, SHAHBAZ KHAN, AND HAMED AL-RAWESHIDY, BRUNEL UNIVERSITY
KUMARENDRA SIVARAJAH, AVANTI COMMUNICATIONS

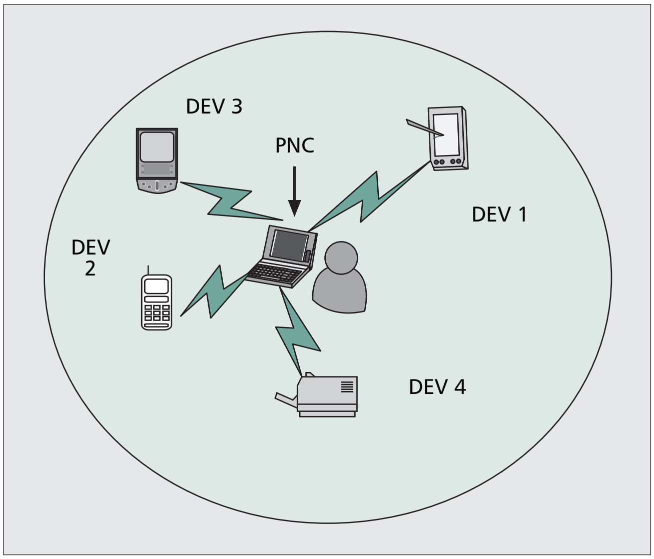
ABSTRACT

Wireless mesh networks have proven to be of great potential in providing new and innovative applications in many areas in the last few years. WMNs can address some limitations and optimize the performance of existing standardized networks in terms of cost, reliability, simplified network configuration, extended coverage and so on. This article is a tutorial on the technical aspects of meshed personal area networks. The proposed solutions for meshing high data rate PANs (802.15.3) are discussed along with related issues where applicable. The article starts by giving an overview of the high data rate PAN standard (802.15.3) and its inherent limitations to operate in a mesh configuration. It discusses the main drivers behind meshing PANs and describes the architecture, operation in a mesh configuration, and the hidden node/exposed node issue, which is pronounced in mesh networks. The added functionality of routing in meshed PANs, optimizations due to multi-interface/multichannel communication, improved dynamic channel selection, transmitted power control procedures, and security aspects are also given in this article. The article concludes by summarizing the proposed approaches for meshing PANs.

The advent of low-power communication devices started with Bluetooth, which operated via short-range radio frequencies. It covered relatively shorter distances than a traditional wireless local area network (WLAN) with lower throughputs. Due to the popularity of Bluetooth devices and the short operating space, the term *personal area network* (PAN) came into existence. A wireless PAN (WPAN) is characterized by a small operating space in which information is conveyed among fewer participants with short distances. It is different than a WLAN (apart from the smaller area covered by a PAN) in a sense that it has little or no infrastructure, which allows inexpensive and power-efficient solutions to be implemented for a range of devices. IEEE released the first standard for PANs based on Bluetooth called 802.15.1, which supported data rates up to 1 Mb/s. Although later industrial implementations supported higher data rates (e.g., Bluetooth 1.2, Bluetooth 2.0), they were still not enough to support multimedia applications that were growing in volume and popularity. To overcome this deficiency, IEEE released 802.15.3, which is the standard for high data rate WPANs supporting data rates from at least 20 Mb/s, which is considered to be the lower bound for multimedia applications. The goals for an 802.15.3 WPAN were to provide low complexity, low cost, low power consumption, and high data rate wireless connectivity among devices.

Although 802.15.3 can provide high data rates with provision of measures that can lower the power consumption of devices (DEVs), there are some limitations that affect performance, especially when the number of DEVs is increased.

Wireless mesh networks (WMNs) have emerged as a potential technology to improve most of the limitations of ad hoc networks, sensor networks, WPANs, WLANs, and WiMAX. Due to the new and innovative applications WMNs have to offer, most industries, in order to gain market share, introduced solutions for community and municipal areas that were premature and not optimized. Furthermore, the solutions were not standardized, and each network offered different incentives for a particular application. To optimize WMNs for supporting high data rates, voice, and video, further research is still needed to resolve many challenges such as efficient routing metrics, scalable capacity, and optimized medium access control (MAC) to support multiple transmissions. The IEEE formed working groups to address the problem of standardization for WMNs. The working groups formed were 802.15.5 (mesh extensions for WPANs), 802.11s (mesh extensions for WLANs), and 802.16 (mesh extensions



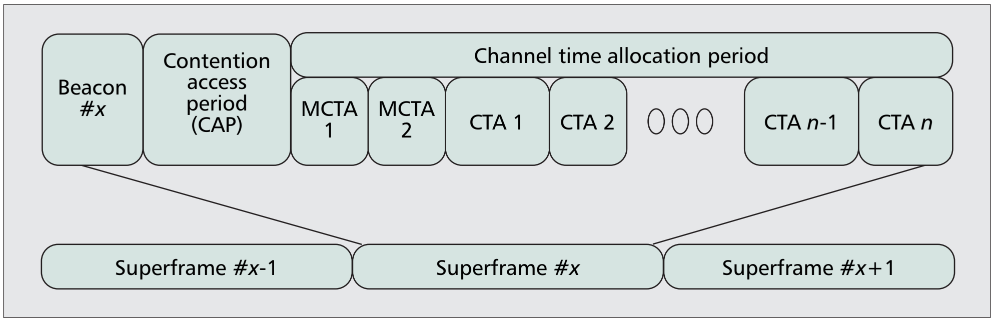
■ **Figure 1.** *An 802.15.3 piconet.*

for WiMAX). The remaining article continues by giving an overview of 802.15.3, which is the standard for high data rate PANs. It gives the limitations of PANs to operate in a mesh configuration followed by the main drivers behind meshing PANs, and gives the architecture of meshed PANs. Next, the operation in a mesh configuration is described, as well as the hidden node/exposed node problem, routing, multi-interface/multichannel communication, improved solutions for dynamic channel selection, transmitted power control, and security.

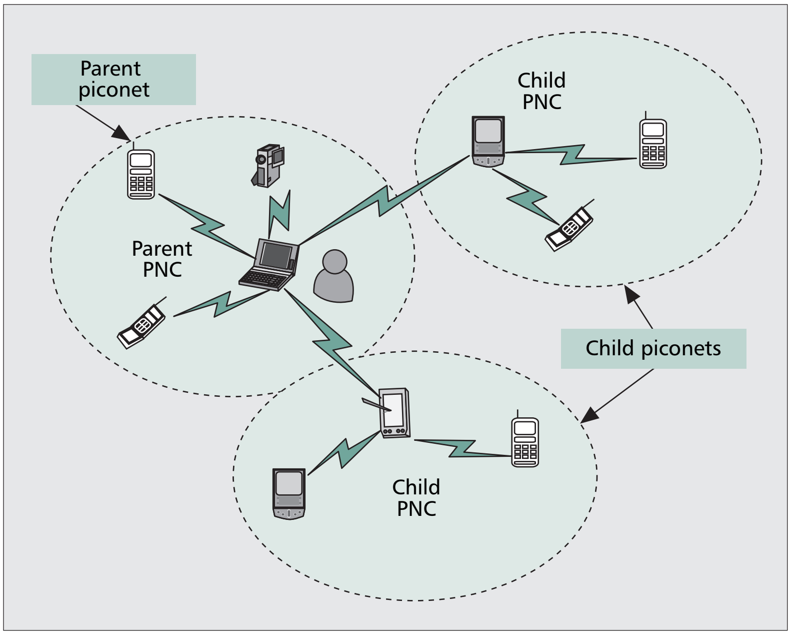
OVERVIEW OF 802.15.3

The communication among DEVs in an 802.15.3 WPAN is organized in the form of a *piconet* (Fig. 1), which typically covers a personal operating space of 10 m in all directions and envelops a person or DEV whether stationary or in motion. The communication among independent DEVs is coordinated by a single DEV, which assumes the role of a piconet coordinator (PNC). The PNC provides the basic timing for the piconet by transmitting a beacon that is heard by all members of the piconet. The PNC also manages the quality of service (QoS) requirements, power save modes, and access control to the piconet. The data in the piconet is exchanged in a peer-to-peer manner. The timing is provided by a PNC through a superframe (Fig. 2) that consists of a beacon, contention access period (CAP), and channel time allocation periods (CTAPs). The beacon is used to set the timing allocations and communicate management information for the piconet. The CAP, which is based on carrier sense multiple access with collision avoidance (CSMA/CA) for medium access, is used to communicate commands and/or asynchronous data if it is present in the superframe. The CTAP, which is based on a standard time-division multiple access (TDMA) protocol, has channel time allocations (CTAs) including management CTAs (MCTAs). CTAs are used for commands, isochronous streams, and asynchronous data connections. If the DEV needs channel time on a regular basis (for real-time traffic), it requests isochronous channel time from the PNC. Depending on available resources, the PNC allocates time in a CTA for the DEV. If the CAP is present in the superframe, DEVs in the piconet are able to use it to send small amounts of data. For asynchronous allocation, an asynchronous channel time request is made, which is a request for the total amount of time to be used to transfer its data. In order for a DEV to participate in a piconet, it needs to send an association request to the PNC. When associated, the DEV is given a unique identifier, the Device Identifier (DEVID) for the piconet. The DEVID is 1 octet in length instead of the DEV's address (MAC address), which is 8 octets in length, to save address overhead in the system. If the DEV wants to leave the piconet or if the PNC wants the DEV to be removed from the piconet, the disassociation process is used. For the purpose of sharing resources, the DEVs in the piconet need to know about the services available in the piconet and in turn they need to advertise their own services. The piconet services information element (IE) is used to achieve that and is exchanged optionally in the association process. To request more detailed services offered by the DEVs in the piconet, the DEV can also use the PNC information request command, probe request command, and announce command.

In order to start a piconet, a DEV that is capable of acting as a PNC scans the available channels to find one that is not being used. Either an open scan is performed, in which the DEV searches for any beacon frame, or the DEV ignores all received frames not matching the piconet identifier (PNID) and beacon source identifier (BSID) parameters in the request. The PNID and BSID are used to uniquely identify a piconet. After scanning through all the channels, if the DEV finds a clear channel, after waiting for a specified period of time the DEV can start a piconet by simply sending the beacon. If there are no available channels, the DEV can start a dependent piconet. A piconet can be independent (having no dependent piconets), or it can have dependent piconets such as a *child piconet* or a *neighbor piconet*. The already established piconet then acts as their parent piconet and allocates them private CTAs from its superframe to operate. The child piconet functionality is useful for either extending the area of coverage of the piconet or shifting some computational or memory requirements to another PNC-capable DEV. A parent piconet can have more than one child or neighbor piconets. A neighbor piconet is useful for sharing the frequen-



■ **Figure 2.** *An 802.15.3 superframe.*



■ **Figure 3.** *Parent-child hierarchy in 802.15.3.*

cy spectrum between different piconets when there are no vacant PHY channels. Child and neighbor piconets have distinct PNIDs and are autonomous apart from the fact that they depend on a private CTA from the parent. The difference between a child and a neighbor piconet is that a child PNC is a member of the parent piconet and thus able to exchange data with any DEV in the parent piconet. A child PNC is also a member of the child piconet and therefore able to exchange data with any DEV in the child piconet. A neighbor PNC, on the other hand, is not a member of the parent piconet and thus cannot exchange data with any DEV in the parent piconet. This imparts a limitation on the 802.15.3 standard to function in a mesh configuration. We discuss in detail the limitation imposed by the child and neighbor piconet model, and the main drivers for mesh networking in WPANs.

LIMITATIONS OF 802.15.3

A PAN operating in a mesh configuration can be of two connection arrangements, full mesh topology or partial mesh topology. In a full mesh topology, each node is connected directly to each of the others. In a partial mesh topology, some nodes are connected to all the others, but some are connected only to those other nodes with which they exchange the most data. In 802.15.3 the parent-child hierarchy as shown in Fig. 3 enables the child PNC to exchange data with the parent PNC and all DEVs in the parent piconet. The child PNC can also communicate with the DEVs in its own piconet. The limitation this imposes is that the DEVs in the child piconet cannot communicate with the parent PNC or the DEVs in the parent piconet even if they are in transmission range of each other. For a true mesh configuration the DEVs should have peer-to-peer relationships with their neighbors even if it is a partial mesh topology. Since the neighbor PNC is not a member of the parent piconet, it cannot communicate with the DEVs in the parent piconet. The parent-child model also presents a single point of failure. If the parent supports two or more child piconets, if the parent PNC wants to shut down, it selects one of the child piconets to continue operation and all other dependent piconets cease operation, resulting in the termination of all active sessions. If the parent PNC crashes, all the dependent piconets cease operation until the association timeout period (ATP) expires.

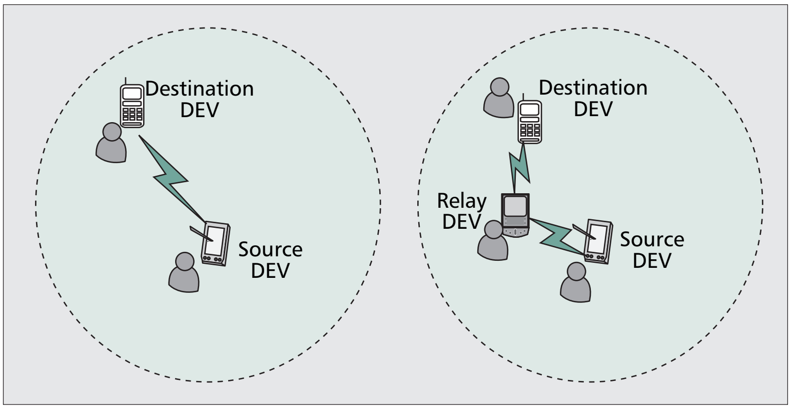
IMPETUS BEHIND MESHING PANS

Mesh networks can address many issues present in WPANs and significantly improve their performance. The existing 802.15.3 PAN is based on a single hop; therefore, the DEVs sometimes need to transmit at a higher power to reach DEVs that are further away. In a mesh network we have intermediate DEVs that can relay the data from a source DEV to a destination DEV. In this way the network is extended, and the single hop distance between neighboring DEVs is reduced (Fig. 4), resulting in significant power saving throughout the network. When considering single-hop communication with longer distances, it is not just a question of transmitting more power to communicate. When having short distance multihop communication instead, there are four factors to be considered that aid in saving energy:

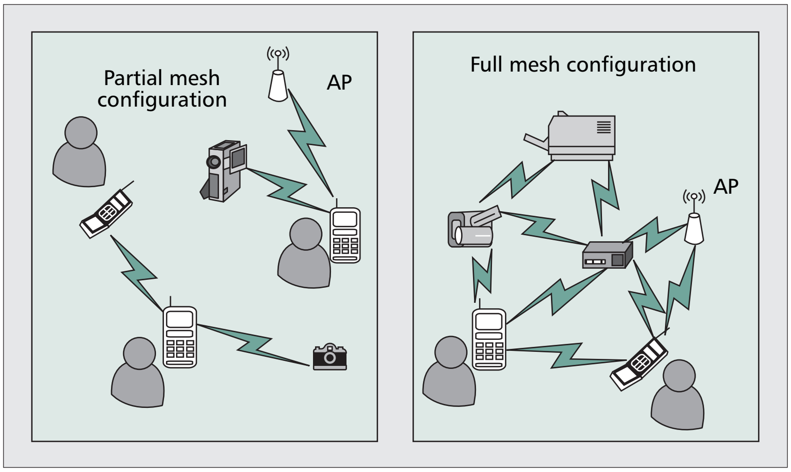
1 There is less transmitted power by the source DEV and less received power by the destination DEV.
2 By transmitting less power, there is less interference with the nearby DEVs, and hence reduced dropped packets with fewer retransmissions.
3 Power increases/decreases more than linearly with the distance (by a factor of two, four or more) depending on whether the communication is indoor or outdoor.
4 Due to a short distance between the communicating DEVs, the throughput is increased because there are fewer errors, and the link quality is improved.

When considering point 1 above, there is a minimal effect on the total energy utilization of the whole network if all the communicating DEVs are energy constrained. In contrast, if the source and destination DEVs are mobile but select an intermediate relay DEV that is not energy constrained and is stationary, there can be significant energy savings in the network. Point 4 suggests that due to short distances between the communicating DEVs, the link quality is improved due to fewer errors. As a result there are fewer retransmissions, which saves energy.

The reliability of the network is increased when working in



■ **Figure 4.** *Power saving by using the mesh configuration.*



■ **Figure 5.** *Partial and full mesh configurations.*

a mesh configuration because of route redundancy. In both full and partial mesh topologies, as shown in Fig. 5, a DEV always has links to its immediate neighbors. When one link goes down, another relay DEV can forward the data on behalf of the source DEV toward the destination. In addition, since all the mesh PNCs (MPNCs) are connected to each other, there is no single point of failure for the mesh network. When an MPNC goes down, only the intra-PAN communication is affected in the piconet governed by the failed MPNC instead of the entire network. WMNs make the network configuration a lot easier because the mesh DEVs are self-configured. As soon as a DEV is turned on, it undergoes the configuration necessary to be a part of the mesh network. Mesh DEVs also have increased battery life due to fewer retransmissions. The MAC layer for 802.15.3 PANs assumes that only one connection can be active for a DEV at a given time. Mesh extensions for PANs should enable the MAC to handle multiple connections at a given time so that a DEV can be engaged in its own data transfer and at the same time relay data for its neighbors using different channels. The following sections describe briefly the issues faced by meshing PANs and the extensions made to the high data rate PAN (802.15.3).

Architecture

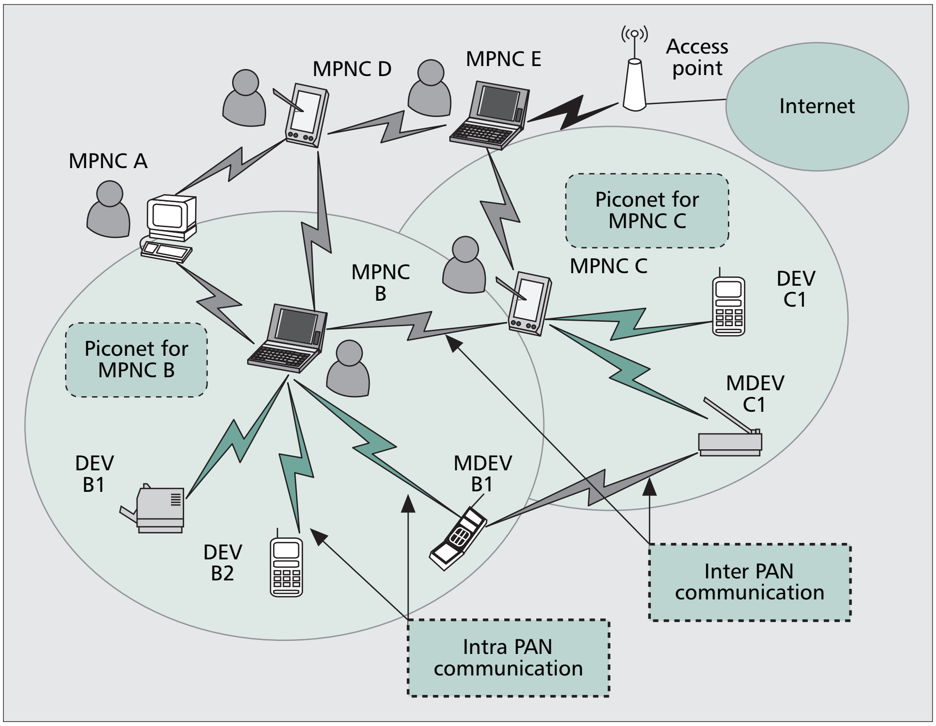
In 802.15.3 a single PNC coordinates a piconet, and the DEVs can communicate among themselves and with the PNC. In the mesh configuration, several homogenous set of MPNCs negotiate the occupancy of channel access among them. The resulting hierarchy is shown in Fig. 6. In the mesh configuration, apart from the Intra PAN communication, Inter PAN communication also exists. In intra-PAN communication, DEVs in one piconet can communicate among themselves and with the MPNC. In inter-PAN communication, the DEVs can communicate with DEVs and MPNCs of another piconet. The MPNCs can also communicate with each other. One of the MPNCs can act as a gateway to the Internet by having a direct connection to it and sharing it with others, or it can act as a gateway to other networks (e.g., WLAN, WiMAX). The layered reference model which is an upgrade to the 802.15.3 model with mesh extensions is shown in Fig. 7. The MAC and physical (PHY) layers conceptually include management entities called the MAC sublayer management entity (MLME) and PHY layer management entity (PLME), respectively. The major part of the new functionality for mesh is included in the frame convergence sublayer (FCSL) and device management entity (DME). There are also enhancements in the MAC layer and its management entity.

Operation in a Mesh Configuration

Different aspects of operating in a mesh configuration can be divided into beacon alignment, starting of a mesh enabled piconet, network self-organization, and address assignment.

Beacon Alignment

The superframe, which is the basic timing structure, is divided into equal length medium access slots (MASs) used to address medium reservations between MPNCs. This helps to minimize interference for those MDEVs that can receive beacons from multiple MPNCs, and there are less beacon collisions as a result. Beacon alignment is mandatory because if two independent piconets overlap, if their respective MPNCs transmit their beacon at the same time, there is a collision, and the DEVs would not be able to communicate. For intra-PAN communication the existing superframe structure of 802.15.3 is used. There should be a mechanism to determine a common superframe length among the piconets by the MPNCs for



■ **Figure 6.** *Mesh WPAN architecture with inter-PAN and intra-PAN communication.*

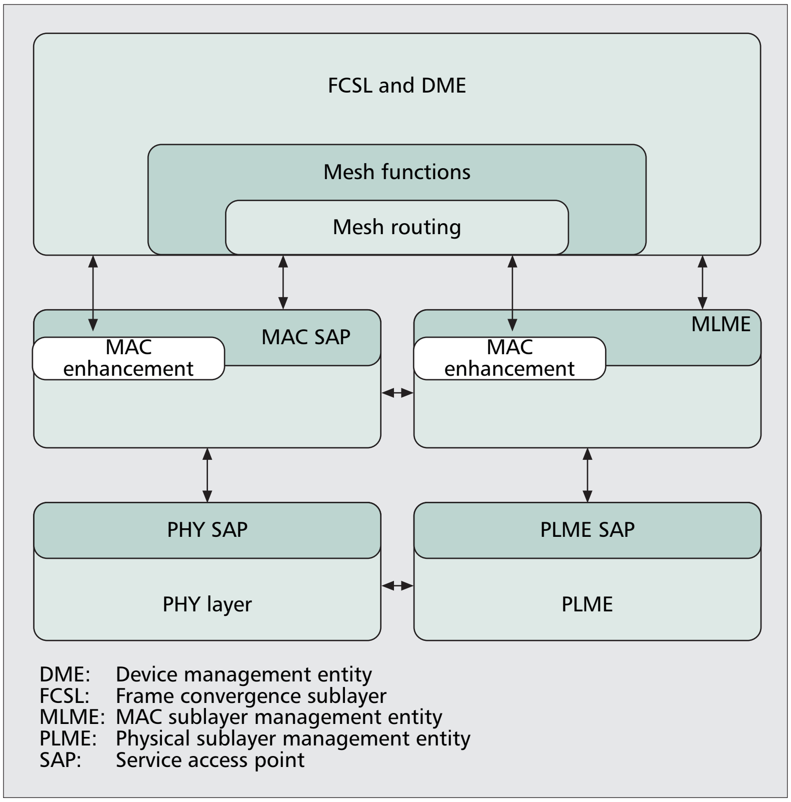

FCSL and DME
Mesh functions
Mesh routing
MAC enhancement
MAC SAP
MAC enhancement
MLME
PHY SAP
PHY layer
PLME SAP
PLME
DME: Device management entity
FCSL: Frame convergence sublayer
MLME: MAC sublayer management entity
PLME: Physical sublayer management entity
SAP: Service access point

Figure 7. *Mesh enhancements to 802.15.3 layers.*

effective communication. Each piconet has a different start time defined by the corresponding MPNC. The offset has to be multiple MASs to synchronize the slot start times throughout the mesh network. If beacons are aligned in subsequent MASs, the period from the first to the last beacon in the group is called a beacon period (BP) (Fig. 8). When a new MPNC is powered up, it scans for an available beacon period. If it finds one, it joins the beacon period by transmitting a beacon on one of the available MASs reserved by the already running MPNCs (which are transmitting in the same BP). In each transmitted beacon an MPNC includes the beacon transmission times and the corresponding IDs of its neighbors.

Whenever an MPNC receives a beacon in which its beacon slot is marked as occupied with a different ID as its own, it defers from transmitting the beacon in that slot to avoid a collision. If two separate mesh networks come into the vicinity of each other such that the beacon transmission of one overlaps with the MAS of the other, both of them should inform their neighbors so that they can replace the data transmissions placed on the affected MAS. The two mesh networks shall synchronize their MAS boundaries. The MPNCs can optionally choose to change their beacon transmission so that both of them can be a part of the same BP. To reserve slots for transmission, the source MPNC either sends a reservation request management frame or includes a reservation request IE into its beacon, which indicates the MASs that shall be reserved. The destination, upon reception, checks if there is no overlap of the requested slots with the ones that exist. If suitable, it sends a reservation reply, which also notifies neighbor MPNCs of the new reservation. The source MPNC then announces the reservation to its neighbors by including a *reservation request* IE into its beacon, which remains there in the beacons of the source and destination MPNCs unless cancelled.

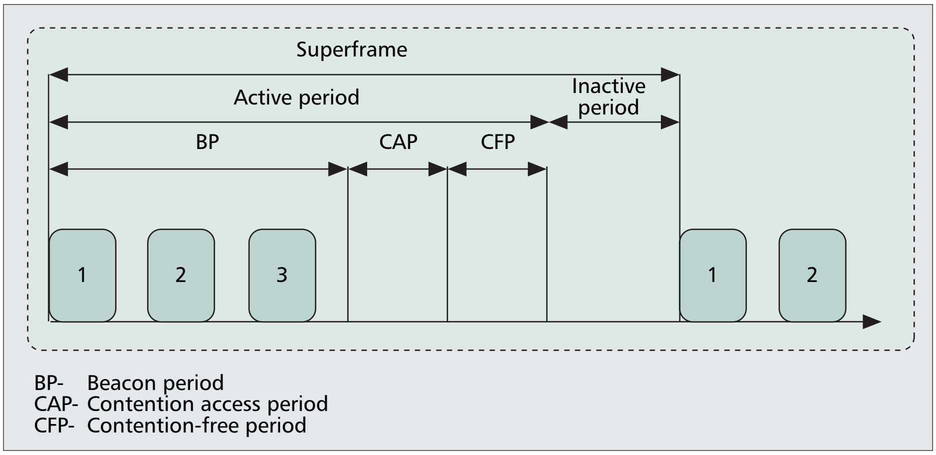


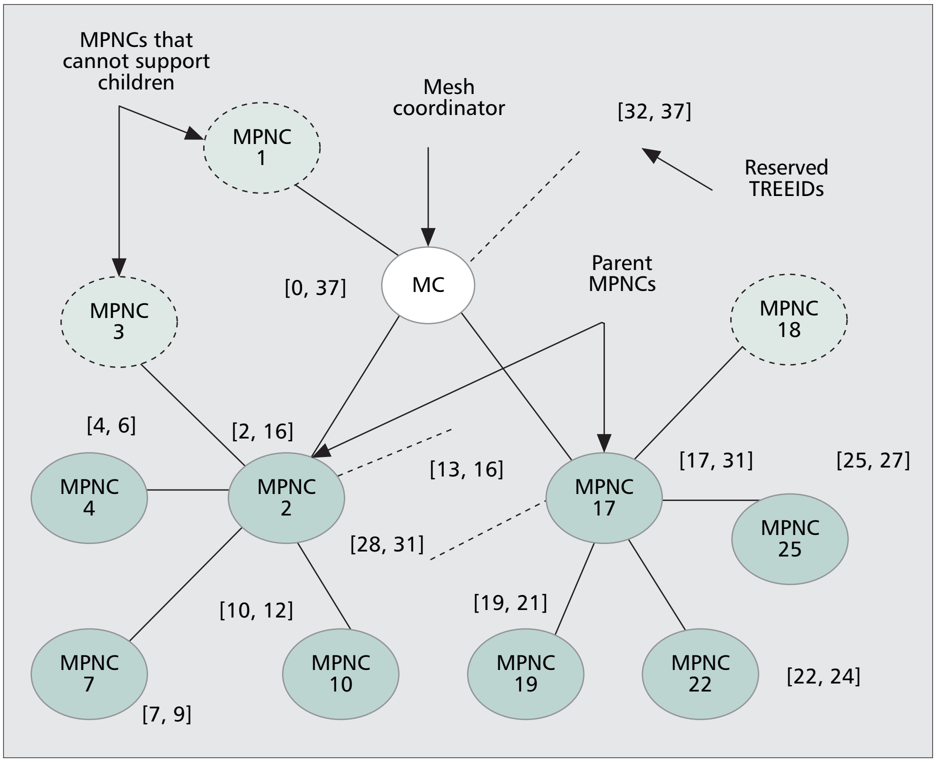
Figure 8. *Divided superframe with a beacon period.*

Starting a Mesh Enabled Piconet

To start a mesh enabled piconet, a DEV (capable of being a MPNC) scans the available channels. If there is a free channel and no established PNC or MPNC is found, the DEV shall assume the role of an MPNC by allocating medium access time required for beacon frame transmission and CAP/MCTA, and send the beacon. If there is a PNC found in the scan, the MPNC can either associate with the PNC or choose to change the operating channel to one not used by the PNC. If it associates with the PNC, it requests a pseudo-static CTA to perform its beacon transmission within the CTA. If, after performing the channel scan, only an MPNC is found, the DEV wanting to be an MPNC shall select a reference MPNC to synchronize its slot boundary with other MPNCs. After the DEV synchronizes its slot boundary with a reference MPNC, it shall perform an announcement procedure to inform its neighbors of its presence by sending an alien MPNC announcement command during the CAP or MCTA of the destination MPNC. Upon reception, the destination MPNC shall respond using immediate acknowledge (IMM-ACK).

Network Self-Organization

The MPNC that initiates a mesh WPAN becomes a mesh coordinator (MC). The MC shall select a mesh ID that uniquely identifies the mesh network. To start a mesh network, an MC shall include a *mesh capacity* IE in its beacons. The mesh capacity IE has information whether a DEV can support a new child and/or can relay packets for other DEVs. It also indicates what type of topology is in use for the mesh network. The MC can choose to build a tree topology, shown in Fig. 9, and announce its desire to do so in its beacons. The neighbors of the MC may join the tree by sending a *tree association request* command. This command contains information



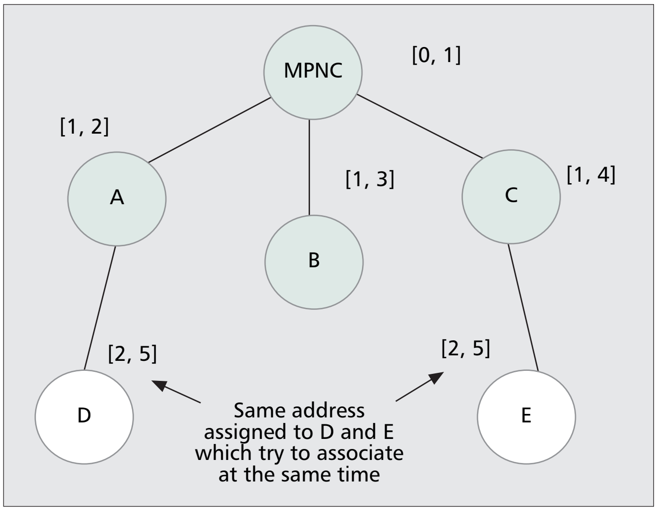
■ **Figure 9.** *Tree topology formed by the MC.*

about the actual descendant number or expected descendant number of an MPNC. If the MPNC is not sure, it can send an expected number of descendents in this subfield. When the MC receives an association request command from a neighboring MPNC, it decides whether it can support the MPNC and its descendent by consulting its available address space to assign TREEIDs. If it can support the MPNC and its descendents (expected or actual), it shall send a *tree association response* command to the MPNC. Apart from notifying the destination MPNC of its association status, the tree association response command contains information about available TREEIDs, topology servers, and address servers. Since in the initial stages of tree formation, the MC might not assign the TREEIDs efficiently, it can therefore in some cases delay the assignment of the TREEID during the association process. The associated MPNC then adds the MC as its new parent to its tree table and sends a beacon with the mesh capacity IE included to show its intentions of adding more devices as its children. If an MPNC receives beacons from two or more tree members, and all of them are willing to accept new children, it may select the one that has the smallest route cost to the MC as its parent. A parent MPNC can use a *tree disassociation request* command frame to disassociate its child. A child can also use the same command to be released from the parent. The disassociation command frame also has the reason for disassociation, which can be because there is not enough TREEID space, the MPNC wants to associate with a new parent, or some other defined reason. A tree disassociation confirmation command frame is sent by either the parent MPNC or child MPNC to complete the disassociation process. For efficient working of the tree topology, the following two important considerations should be taken into account:

- Due to high mobility of an MDEV, it might have to disassociate and make new associations very frequently, which shall change the topology very frequently. This might cause a high number or traffic just for topology updates. To remedy this problem, those DEVs that have minimum or no mobility and are capable of being an MPNC should be preferred to become the MPNC.
- Since a tree topology is meant for a high number of MDEVs, a pragmatic value for the number of descendent MDEVs should be defined for an MC to operate in an acceptable fashion. More MDEVs mean splitting the available bandwidth among more MDEVs to send their beacon. This could severely restrict the capacity of the mesh network because in addition to splitting the bandwidth, there shall be more frequent topology changes and topology updates, which is an additional overhead. A practical limit can be improved on by addition of efficient dynamic channel algorithm schemes to combat interference, multiple channels with multiple interfaces (multihoming), dual radios, and so forth.

Address Assignment

In a large mesh network with a tree topology, there can be address conflicts if addressing is not done properly. Addressing can be done by assigning a block of addresses in a hierarchy, centralized or distributed. With hierarchical block addressing, the address space might not be utilized properly, and some of the addresses might be wasted. Centralized addressing can be time consuming and not appropriate for some routing algorithms. In distributed addressing, which is fast, address conflicts can arise. One solution is to allocate addresses in such a way that the MPNC, after assigning the addresses to new DEVs, sends information to other DEVs (including its children) so that they know the last address assigned (LAA) [1]. The problem with this approach is that if two nodes try to associate at the same time, as in Fig. 10, they


MPNC
[0, 1]
[1, 2]
A
[1, 3]
B
C
[1, 4]
[2, 5]
[2, 5]
D
E
Same address assigned to D and E which try to associate at the same time

■ **Figure 10.** *Real-time address assignment conflict.*

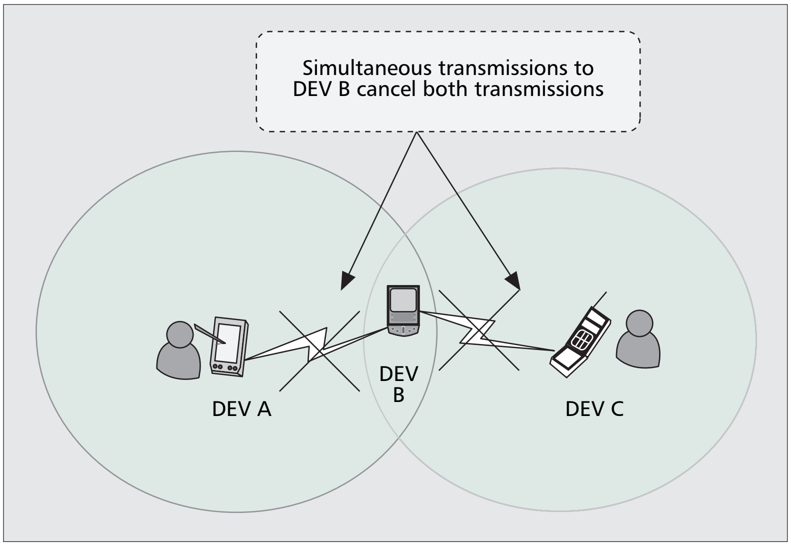

Simultaneous transmissions to DEV B cancel both transmissions
DEV A
DEV B
DEV C

Figure 11. *Hidden node problem.*

might be assigned the same address. This can be resolved if the MPNC sends an *address reassignment* command to the later arriving device. In a large network resolving the conflicts might take a long time. Since this approach is not structured, it can be inefficient for tree routing. The approach followed in [2] is suited to a tree topology and is described briefly.

To get information about the tree topology formed and assign TREEIDs accordingly, the MC broadcasts a *tree topology discovery* frame. The transmission type of this frame is set to tree broadcast so that only the children of this MC accept and process this frame. The source MDEVID and DEVID subfields of the frame are set as the identity of the MC. An MPNC, upon receiving a tree topology frame from its parent, sends it to its children if it has some. If it does not have any children, it shall create a tree topology update command frame, set the terminator MDEVID of the frame to the initiator MDEVID (MC) of the tree topology discovery frame, and send the frame to its parent. If the MPNC has children, it shall wait for the topology update command frame from its children, and then create its own topology update command frame and send it to its parent. The MC maintains a TREEID pool, and first assigns single TREEIDs to those children who cannot support any child. It then reserves some TREEIDs for future descendents and lastly divides the remaining TREEIDs among children that support descendents. Each of the children (which can support descendents) is assigned a TREEID block, which contains its own TREEID and TREEIDs of its existing and potential descendents. The MC has a record of the assigned TREEIDs and sends a TREEID assignment command frame to each child to notify it of the assigned TREEID and TREEID block. Once an MPNC sets aside a TREEID pool for future descendents, it can assign TREEIDs from this pool to newly joined children. If the TREEID pool of the parent MPNC is not large enough to support the new child and its descendents, it shall request a TREEID reassignment from its own parent through a tree topology update command frame. Figure 9 shows the hierarchy formed by the MC and the TREE IDs assigned. If an MPNC cannot contact its parent for a long time, it may select a new parent from its neighbor MPNCs and try to associate with the new parent. One or more MPNCs can serve as an address server to have a mapping of all the addresses. An address server may periodically broadcast a server notification command frame to the whole mesh to announce its existence. The server notification command frame can also be used to announce the existence of other specialized servers like a topology server, a gateway, and any other server. An MDEV can also get information about the existence of an available server through the association response frame while associating. It can send a server inquiry frame to its parent, and its parent can send a server notification command frame that carries the identity of the server. The address server is updated regularly by every MPNC by sending an address update command frame to it.

Hidden Node and Exposed Node Problem

In WPANs the operating space of a piconet is generally limited to 10 m centered at the user. In such small operating spaces, as the DEV density increases, the hidden and exposed node problems can occur more frequently. In meshed WPANs these problems can become worse because of multiple overlapping piconets. If we consider Fig. 11 for the hidden node problem, DEV B comes in the transmission range of DEVs A and C, but DEVs A and C are not aware of each other because they are out of transmission range of each other. If DEVs A and C try to transmit to DEV B at the same time, a collision will occur, and both transmissions shall be cancelled. The problem of hidden node can be solved by using a request to send/clear to send (RTS/CTS) mechanism in which a source DEV sends a request to transmit to the destination DEV. The destination DEV sends a reply if the medium is clear. Consider Fig. 12 for the exposed node problem in which there are four DEVs. When DEV B transmits to DEV A, DEV C thinks that the medium is busy because of CSMA/CA and that it is in the transmission range of DEV B. It should be noted that the problems of hidden and exposed nodes occur during the CAP, as shown in Fig. 13, which uses CSMA/CA. During the CFP, the respective MPNC or PNC takes care of the timing by allocating CTAs to transmitting DEVs. The exposed node problem can be solved by using neighbor tables [3]. If DEV B in Fig. 12 maintains a neighbor table of the DEVs in its transmission range, it can make an

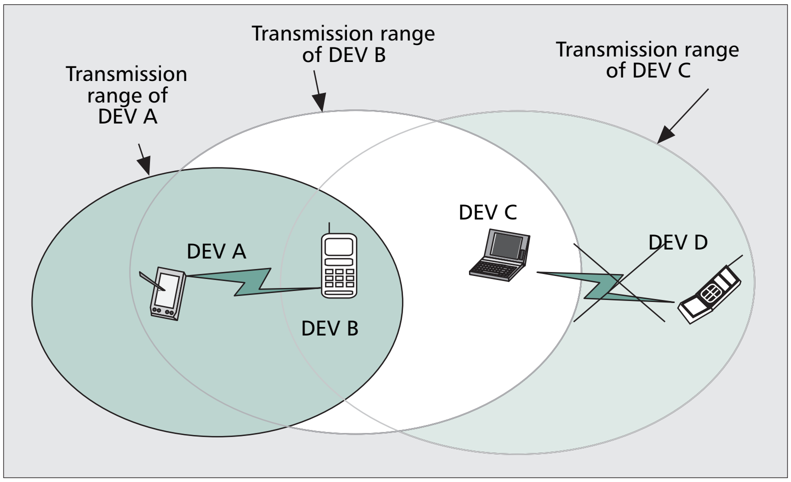
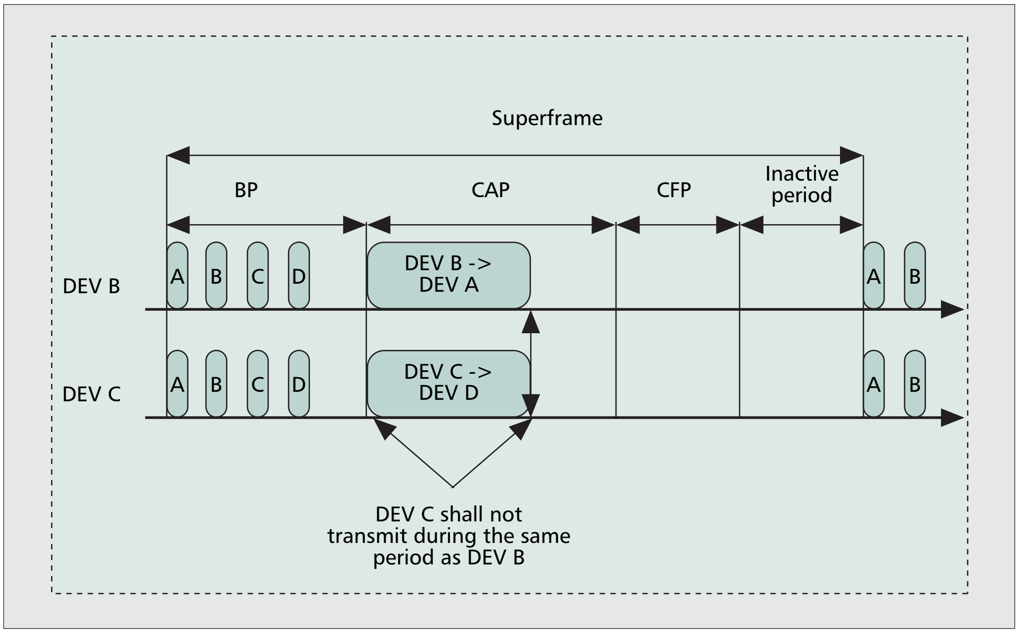

Transmission range of DEV A
Transmission range of DEV B
Transmission range of DEV C
DEV A
DEV B
DEV C
DEV D

Figure 12. *Exposed node problem.*



■ **Figure 13.** *DEV B's transmission preventing DEV C from transmitting to DEV D.*

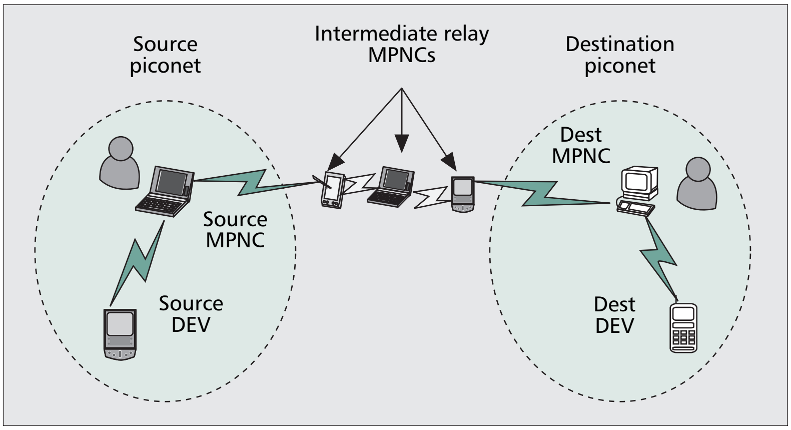
entry for DEV A to which it wants to transmit. DEV C then knows that it can transmit to DEV D because the destination of DEV B is not in its neighbor table and hence is out of its transmission range.

Routing

In 802.15.3 the communication between DEVs and the PNC is single-hop. The MAC for 802.15.3 is therefore designed for single-hop communication. In a mesh network, since the MDEVs can act as relays to forward data on behalf of their neighbors, the communication is multihop. Therefore, a meshed WPAN needs a routing strategy to efficiently forward the data from source to destination along a better path. Since mesh networks allow the use of dual radios, multiple interfaces per MDEV, and some infrastructure, an efficient routing protocol might be different than the conventional routing protocols for mobile ad hoc networks (AODV, DSR, TORA, DSDV, WRP, ARP, etc.). A decision has to be made whether a proactive (table-driven), reactive (on-demand), or hybrid type of routing protocol suits meshed WPANs. Since each of them have their advantages and disadvantages, the recommendations for a routing protocol included in [2] are made very flexible to accommodate a wide variety of routing protocols depending on the application the meshed WPAN is going to support. When a source DEV wants to send a packet to a destination outside its PAN, it shall always forward the packet to its MPNC, which is called source MPNC, via intra-PAN communication. The source MPNC shall deliver the packet to the MPNC (destination MPNC) (Fig. 14) of the destination piconet, which shall forward the packet to the destination DEV using intra-PAN communication. The following routing strategies for the meshed WPAN make it flexible to adapt to new and efficient routing protocols:

- *Local routing*: If a source MPNC finds that the destination is in its direct reach, it shall forward the packets directly. Otherwise, it shall check if it is in direct reach of one of its neighbors and send it to the corresponding neighbor.
- *Remote routing*: In remote routing there is proactive routing, tree routing, centralized routing, location-based routing, and distributed routing.

Each of the above approaches have their applicability in certain scenarios, and routing protocols can be designed for each of them respecting the demands of the particular application with which the meshed WPAN must cope. In proactive routing each MPNC shall maintain a routing table and a route discovery table. This might add some additional overhead in the system because of frequent messages needed to keep the table updated. The tree structure and TREEID assignment method enable MPNCs to route packets based on their TREEID block information and their children's TREEID block information. An MPNC can check if the TREEID of the destination MPNC falls into its own TREEID block and forward the packet to its parent if it does not. If the TREEID of the destination falls into one of its children's TREEID blocks, it shall forward the packet to the respective child. The address assignment should be quick enough so that, due to mobility and other factors, the TREEIDs are assigned on time to reassociating DEVs. In centralized routing one or more MPNCs may serve as topology servers to store link state information of all MPNCs. When a topology server is available in



■ **Figure 14.** *Routing from source DEV to destination DEV through MPNCs.*

the mesh network, all MPNCs shall register their link states at the topology server. To prevent the single point of failure, multiple topology servers can exist in which some serve as a backup server. The main server synchronizes its knowledge with the backup server by forwarding the link state registration command frames to it. If the main server fails, the neighbors of the main server shall forward all link state registration frames and route discovery frames to the backup server. If the network is too large for one topology server, partial topology servers can exist that cover a specific area of the tree. The whole tree can be divided into subtrees, and each subtree is handed over to a local partial topology server.

If the PHY layer allows making accurate range measurements among DEVs, a coordinate system can be established to cover the whole mesh network. A source MPNC shall set the packet transmission method as location-based routing and put the location of the destination MPNC as well as its own location in the routing assistant field. The source MPNC then calculates the distance between the destination MPNC and each of its neighbor MPNCs. The neighbor closest to the destination MPNC is chosen as the next forwarding DEV. If none of the mentioned approaches are feasible, a source MPNC may opt for distributed routing and shall broadcast a *route discovery* frame to the whole mesh network to find an optimal route to the destination. When an MPNC receives a broadcast route discovery frame, it shall update the route cost between it and the frame transmitter. If it already has a routing entry for the source MPNC, it shall update the frame if the route cost in the route discovery frame is less than that of its route entry. If the MPNC is the destination MPNC and its routing entry is updated by the frame, it shall create a *route formation* command frame and send the frame to the source MPNC. The source DEVID shall be set as the identity of the destination MPNC, and the destination DEVID in the frame shall be set as the identity of the source MPNC. The relay list of the frame shall be set as an empty list. If the MPNC receiving the route discovery frame is not the destination of the frame and it receives the frame for the first time, it shall record the frame in the route discovery table and rebroadcast the frame. Otherwise, if it has received the frame before, it shall only rebroadcast it if its routing entry is updated by this frame. When an MPNC receives the route formation frame with an empty relay list, it shall first check the source DEVID against its routing table. If it does not have a routing entry for the destination MPNC, it shall create one. Otherwise, it shall update its route entry and the cost of the route formation frame to the next-hop relay by consulting the routing entry for the source MPNC. When the source MPNC receives the route formation command frame, it shall create a routing entry for the destination MPNC and start sending data packets.

MULTIRADIO/MULTI-INTERFACE COMMUNICATION

An important aspect in mesh networks to improve capacity is using multi-interfaces. In conventional communication, each DEV is equipped with a single network interface with static channel assignment. This arrangement can cause capacity issues, especially in multihop mesh networks. Two DEVs sending data to different destinations and operating on the same radio frequency can cause severe interference if they come in transmission range of each other. Static channel assignment does not utilize the available radio frequency spectrum efficiently. In a single-interface multichannel design, only one channel can be assigned to the interface at a time, but the interface can switch channels according to changing network conditions. Algorithms can be designed so that the DEVs are intelligent enough to detect interference and switch channels accordingly. This approach can enhance the performance of the network in terms of interference mitigation and capacity. The drawback of such an approach is that two DEVs who want to communicate do not have a common channel between them will not be able to communicate. This can cause network partitioning. The broadcast messages sent from a DEV on one channel are not heard by those DEVs operating on different channels. Appropriate functionality should therefore be put in the MAC layer to coordinate communication between DEVs so that they communicate using a common channel. In a multi-interface multichannel design, different channels can be assigned to the available interfaces. Since in WLANs 802.11b has three nonoverlapping channels and 802.11a has 12 nonoverlapping channels, many approaches have been proposed to take advantage of the available channels. Some statically assign available channels to available interfaces [4], while some dynamically assign channels to available interfaces [5–7]. A preferred approach is that one of the channels can be permanently assigned to an interface and can therefore act as a common control channel to coordinate communication among DEVs. The common channel can be used to hear broadcasts, and can collect information about the dynamics of the network to switch the channel on the other interface/interfaces accordingly. Suitable dynamic channel switching algorithms can then be implemented to combat interference, and further enhance network capacity and throughput [8]. Reference [5] shows that to keep multi-interface DEVs cost effective, the number of interfaces is kept lower than the number of available channels. Reference [7] shows that increasing the number of interfaces does not affect the throughput significantly, but increasing the number of channels per DEV does. Multiple interfaces can be homogeneous (using the same wireless technology) and heterogeneous (using different wireless technologies). In a meshed PAN those MDEVs that have multiple homogeneous interfaces can communicate simultaneously with two or more DEVs (depending on the number of interfaces). They can also be involved in intra-PAN communication and inter-PAN communication simultaneously because of the same reason. Homogeneous multi-interface MDEVs are indispensable in meshed PANs because they can dramatically improve the performance by enhancing capacity and throughput since the superframe is shared by multiple MPNCs in transmission range of each other. By sending the beacon on different radio frequency channels, an MPNC can isolate intra-PAN communication from inter-PAN communication without interference. Furthermore, those MDEVs that have multiple heterogeneous interfaces (Bluetooth, WLAN, WiMAX, UMTS, etc.) can be made to act as mesh routers and extend the coverage by connecting PANs at different sites (office, home, etc.) used by the same user.

DYNAMIC CHANNEL SELECTION

When a mesh WPAN operates in a tree topology and the number of MDEVs is increased, the superframe is divided more and more by the neighboring MPNCs to allocate channel time for their piconets to operate. This can restrict capacity, and the number of simultaneous supported connections is decreased. Furthermore, since the network operates in a dynamic environment and under unlicensed operation rules, it is subject to interference from licensed users and other wireless entities in its channels. These factors make the need for a dynamic channel selection algorithm imperative. The shifting from one channel to another should be transparent so that the existing active sessions are not affected. In 802.15.3 the procedure to change the channel is described, but the performance parameters on which to base decisions are left out. In the existing mechanism the PNC initiates dynamic channel selection if it determines that the current channel conditions are poor. The PNC may perform a PNC channel scanning procedure or the remote scan procedure, or collect the channel status from its member DEVs by sending a channel status request command. When the PNC determines that there is a channel with better characteristics than the present one, it undergoes a channel switching procedure. The dependent piconets shall either change to the new channel with the parent PNC or cease operation. The problems with this approach are that the PNC listening range is limited (one hop), and the PNC does not know which nodes it should inquire for the channel status and when to inquire it of them. The process of switching channels in a mesh WPAN is made complex by the fact that since there can be many overlapping piconets in a large tree with each piconet managed by its own MPNC, if each MPNC changes its channel, it might have to undergo the beacon alignment procedure again. This can cause a delay, and its existing sessions can be disturbed. Also, if the other MDEVs want to communicate with it, they shall have to switch channels too. This problem can be solved to an extent by using dual radios with each MDEV operating simultaneously on two channels. This approach can increase capacity and further minimize interference. One approach proposed by [9] is that the MDEVs decide to do interference detection by themselves. Another approach in [10] uses a distributed dynamic channel allocation algorithm to allow each piconet to decide the set of channels based on the information available locally. A centralized approach for WLAN mesh networks is given in [7] that makes use of multiple channels and uses their approach to optimize routing. Further research efforts are imperative in acknowledging the specific requirements of a WPAN mesh network and designing an optimal centralized or distributed dynamic channel algorithm.

The channel scanning in meshed WPANs can be triggered by instances like too many retransmissions, high packet loss rates, or some other performance parameters. The MDEVs can also do periodic scanning to check properties of the channel used. There should, however, be a criterion to define the minimum and maximum channel switching time to define a threshold for active sessions, especially real-time sessions, not to be disturbed by it. If the MPNC responsible for a piconet suffers severe interference, it can affect the whole piconet concerned. MDEVs should also have an alternate way to switch channels if their MPNC experiences severe interference.

Power Control

Controlling transmitted power in a piconet has many advantages. The main advantage is reduced interference with other wireless networks that share the same channel. The power usage in DEVs is also reduced, increasing their battery lifetime. There are two methods provided by 802.15.3 for controlling transmitted power. Since the length of the link between the PNC and the farthest DEV from it (in its transmission range) determines the length of the piconet, the first method is to set a maximum transmit power for the CAP (since all the DEVs can contend for transmission), beacon, and MCTAs (excluding association MCTAs). The second method allows a source DEV that has a good link to use a CTA to request either an increase or decrease in the transmit power of the remote destination DEV. If the PNC determines that there is interference in the existing channel, it may also choose to lower its transmit power.

Since the above method for power control for communicating DEVs only concerns the link between two DEVs, a more thorough approach is given in [11] that makes use of a power table. A power table records the transmitted power levels at which a node transmits signals to neighbor nodes. The transmitting node then finds the corresponding transmitted power (TP) level before it transmits any frames to its neighbor node. There is a neighbor-power table that combines a power table of neighbors. A DEV can then change its transmitted power to its neighbors according to their distance and link quality. There are two methods for transmit power control (TPC) in [11], centralized and distributed. In the centralized TPC method, one of the MDEVs can be assigned the role of a power control server. It might have the whole or partial topology information (depending on size and number of DEVs). When a source DEV wants to change its TP level to a destination, it sends a request to the power control server. The power control server then calculates the appropriate power level and sends the response back to the source DEV. In the decentralized method for TPC, every DEV has a routing table and a neighbor-power table. Each DEV makes a TPC decision by itself as a result. The centralized TPC method can adapt to a small network, and can save power since a single server is dedicated to make all the calculations. The network structure and performance is improved as a result. For a larger network, multiple power control servers can be implemented. The distributed TPC method can be adapted to a large network. It relieves the burden of having the overhead to communicate with a single power control server. A single DEV therefore does not have to use most of its resources to calculate power for other DEVs.

Security

Security is one of the most important aspects of any network design and therefore efficient algorithms should be implemented to protect sensitive information. According to [12], there are two modes of security, mode 0 and mode 1. In mode 0 the DEVs do not require a secure membership to join the piconet. The only form of security imposed by the PNC is the list of DEV addresses it maintains. The same list is checked to give access to a particular DEV in that list. In mode 1 the DEVs are required to establish secure membership before they can access resources or communicate with member DEVs in the piconet. The data sent after establishing a secure membership is also protected by cryptographic techniques. In mode 1, [12] adopts a 128-bit Advanced Encryption Standard (AES) suite to protect the beacon, command, and data frames. The encryption and authentication operation is defined to use AES in CCM (CTR+CBC–MAC) mode. However, the process of establishing secure membership and the initial key establishment schemes are not specified in the standard and are open for implementation. Therefore, a framework should be designed to diagnose and cater to the requirements of secure intra-PAN communication and, in addition, protect inter PAN-communication. There have been certificate-based and ID-based schemes proposed to establish trust for WPANs. Both schemes have more or less the same computational complexity and overall security level. In a certificate-based security system there must be a DEV to act as a certificate authority (CA) to establish and distribute certificates for other DEVs in the system. In a distributed mesh topology a central CA cannot suffice by presenting a single point of failure. Therefore, there can be multiple topology and partial topology servers that are assigned this role.

For complete trust establishment in a piconet, a DEV or MDEV should first become a secure member of the piconet by mutual authentication with the PNC or MPNC. Second, the source and destination DEV who want to communicate should also form a secure peer-to-peer relationship. In a meshed WPAN, there can be different levels of security (intra-PAN) required for different WPANs. Therefore, access to those piconets that can have sensitive information should be limited. The meshed WPAN imposes more security challenges because of its dynamic topology and mobile nature. Trust relationships can be established among different piconets, so the MDEVs that are mobile and require frequent access to those piconets do not have to establish a secure membership every time. The security framework should be designed so that a common security mode is available for the MDEVs to communicate with DEVs in different piconets.

A complete security solution should encompass security components of prevention, detection, and reaction. In an unsecured mesh WPAN any DEV can forward data on behalf of its peers and therefore act as a router. Malicious DEVs can also have access to the networks and start acting as routers. They can start sending bogus update messages that do not comply with the implemented routing protocol and flood the network. Malicious DEVs can direct traffic toward certain destinations and cause packets to be forwarded along a route that is not optimal or even nonexistent. An attacker can create routing loops in the network, and introduce severe network congestion and channel contention in certain areas. WMNs are also prone to denial of service (DoS) attacks. In a DoS attack the attacker injects a large amount of junk packets into the network. These junk packets waste a significant portion of the network's resources, and introduce severe wireless channel contention and congestion. An attacker along an established route may drop the packets or modify them.

In a mesh WPAN beacons periodically broadcast by MPNCs and processed by MDEVs and DEVs ensure the proper operation of a mesh. It is therefore important to guarantee the authenticity of beacons. An attacker may use beacon flooding attacks by sending a large number of bogus beacons to disturb the normal functioning of the network. A solution to digitally sign the beacons for authenticity can impose a heavy burden for low-end DEVs due to the frequency of beacon reception. There should be a lightweight yet effective solution to address this problem.

There are several approaches for message authentication among DEVs like keyed hashing for message authentication codes (HMAC) [13], digital signatures [14], and one-way keychain-based authentication [15]. In HMAC two DEVs share a secret key using a cryptographic one-way hash function h. The computation is efficient for low-end DEVs. Since an HMAC can be verified by an intended receiver, it is not efficient for broadcast message authentication. Digital signature is another approach that is relatively more computation-intensive. It is based on asymmetric key cryptography. Although scalable, it is prone to DoS attacks. An attacker can feed a victim node with a large number of bogus signatures to exhaust its computational resources. The computation for one-way keychain-based authentication is lightweight, and one authenticator can be verified by a large number of receivers. It requires strict clock synchronization, and the receivers need to buffer a message to verify it. This can incur significant delay in the verification of routing updates and other control messages.

Many schemes have been proposed for secure routing like Ariadne [16] for source routing (DSR), Secure Link State Routing (SLSR) [17] for link state routing protocols, SAODV [18] for distance vector routing, ARAN [19], and so on. Each approach is suitable for a specific scenario. Mesh WPANs offer further unique requirements and changes in the existing solutions because of having multiple-interface/multichannel communication. The routing protocols for mobile ad hoc networks have to be modified to become radio-aware. Since a mesh WPAN is a multihop network, a centralized security solution can delay attack detection and taking appropriate measures. Therefore, an optimum solution can possibly be a hybrid one with certain MDEVs assigned the role of handling security functionality. Proactive security approaches relate to prevention of security hazards, and reactive approaches deal with detection and taking appropriate action against potential threats. There should be a compromise in the complexity of the security solution and network performance because highly complex solutions require more computational power from energy constrained DEVs.

Conclusion

Making enhancements to enable WPANs to operate in a meshed configuration can improve their performance and make way for new applications. In this tutorial the proposals and solutions described to address different aspects of mesh WPANs are still tentative, and there is scope for further research and improvement. The initial draft [2] addressed some of the issues for mesh WPANs, and is made flexible and scalable to accommodate future solutions that are better and optimized for specific applications. The task group to standardize 802.15.5 (TG 5) is active in proposing new solutions to enable WPANs to utilize the full potential of mesh networks. It can be expected in the future that some of the existing solutions will revised and new techniques introduced to further enhance the functionality of mesh WPANs.

References

[1] ftp://ftp.802wirelessworld.com/15/06/15-06-0344-00-0005-routing-algorithm-efficient-real-time-network-address-allocation-mechanismsbased-laa-concept-in-mesh-network

[2] IEEE Draft 15-06-0237-02-0005, "Recommended Practice to Standard for Information Technology — Telecommunications and Information Exchange between Systems — Local and Metropolitan Networks — Specific Requirements — Part 15.5: Mesh Enhancements for IEEE 802.15 WPANs," 2006

[3] ftp://ftp.802wirelessworld.com/15/06/15-06-0267-00-0005-Solution-to-Exposed-Node-Problem-in-Mesh-Networks

[4] R. Draves, J. Padhye, and B. Zill, "Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks," *2004 Proc. MobiCom*, Philadelphia, PA, Sept. 26–Oct. 1, 2004.

[5] P. Kyasanur and N. H. Vaidya, "Routing and Interface Assignment in Multi-Channel Multi-Interface Wireless Networks," *IEEE Wireless Commun. and Networking Conf.*, vol. 4, 2005.

[6] K. Ramachandran *et al.*, "Interference-Aware Channel Assignment in Multi-Radio Wireless Mesh Networks," *IEEE INFOCOM 2006*.

[7] A. Raniwal, K. Gopalan, and T. Chiueh, "Centralized Channel Assignment and Routing Algorithms for Multi-Channel Wireless Mesh Networks," *ACM SIGMOBILE Mobile Comp. and Commun. Rev.*, vol. 8, 2004, pp. 50–65.

[8] M. Kodialam and T. Nandagopal, "Characterizing the Capacity Region in Multi-Radio Multi-Channel Wireless Mesh Networks," *Proc.11th Annual Int'l Conf. Mobile Comp. and Networking*, 2005, pp. 73–87.

[9] ftp://ftp.802wirelessworld.com/15/06/15-06-0227-00-0005-dynamic-channel-selection-ppt.ppt

[10] A. Rangnekar and K. M. Sivalingam, "QoS Aware Multi-Channel Scheduling for IEEE 802.15.3 Networks," *Springer Mobile Networks and Apps.*, vol 11, 2006, pp. 47–62.

[11] ftp://ftp.802wirelessworld.com/15/06/15-06-0226-00-0005-

two-methods-transmitting-power-control-mesh-network

[12] IEEE Std. 802.15.3, "Information Technology — Telecommunications and Information Exchange between Systems — Local and Metropolitan Area Networks —Specific Requirements," 2003.

[13] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," IETF RFC 2104, 1997.

[14] R. L. Rivest, A. Shamir and L. M. Adleman, "On Digital Signatures and Public-Key Cryptosystems," MIT, Lab. for Comp. Sci., 1977.

[15] A. Perrig *et al.*, "The TESLA Broadcast Authentication Protocol," *RSA CryptoBytes*, vol. 5, 2002, pp. 2–13.

[16] Y. C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," *Wireless Networks*, vol. 11, 2005, pp. 21–38.

[17] P. Papadimitratos and Z. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks," *Proc. 2003 Symp. Apps. and the Internet Wksp.*, pp. 379–83.

[18] M. G. Zapata, "Secure Ad Hoc On-Demand Distance Vector Routing," *ACM SIGMOBILE Mobile Comp. and Commun. Rev.*, vol. 6, 2002, pp. 106–07.

[19] K. Sanzgiri *et al.*, "A Secure Routing Protocol for Ad Hoc Networks," *Proc.10th IEEE Int'l Conf. Network Protocols*, 2002, pp. 78–87.

Biographies

SAHIZADA A MAHMUD (sahizada.mahmud@brunel.ac.uk) received his B.Sc. degree in electrical engineering from NWFP University of Engineering & Technology, Peshawar, Pakistan. Currently, he is with Wireless Networks & Communications Group, Brunel University, West London, United Kingdom. His research mainly focuses on wireless mesh networks, meshing of PANs, and routing and MAC layer issues during PAN formation and meshing. He has authored several publications in this area and is currently working on the IST project MAGNET-beyond.

KUMARENDRA SIVARAJAH (indran.sivarajah@avanti-communications.com) has over six years' experience in telecommunications field covering significant expertise in 2G (GSM, GPRS, EDGE) and 3G (WCDMA, UTRA-TDD, HSPA, LTE) cellular systems, WiFi, WiMAX, and PAN. He completed his Ph.D. research at Kent University, United Kingdom, on network optimization for UMTS networks in 2004. He worked for three years at Brunel University on the EU IP FP6 project called My Personal Adaptive Global Network (MAGNET), which was trying to find an innovative solution for seamless always on networks for the future. He also has vast knowledge of project management as a technical and proposal coordinator. He is now with Avanti Communications, since January 2007, working for a satellite operator as a wireless consultant.

SHAHBAZ KHAN [M'06] (shahbaz.khan@brunel.ac.uk) received his B.E degree in computer science from the National University of Sciences & Technology, Rawalpindi, Pakistan, in 2004. Currently, he is with Wireless Networks & Communications Group, Brunel University. His research mainly focuses on cross-layer optimization techniques for wireless networks; specifically, on multimedia application support, mobility management techniques, fast handover mechanisms, and optimized routing.

HAMED AL-RAWESHIDY [M'91, SM'96] (hamed.al-raweshidy@brunel.ac.uk) joined the Optoelectronics group at Strathclyde University in 1987 after completing the postgraduate course in optical information processing at Glasgow University. He subsequently obtained his Ph.D. degree for work in the area of spread spectrum multiplexing for communication networks. Between 1990 and 1993 he worked as a research fellow at Oxford University where his main area of investigation was spread spectrum in satellite applications. During the summer of 1992 he worked with the fiber access network group at British Telecom Laboratories. In January 1993 he joined the Department of Electrical and Electronic Engineering at Manchester Metropolitan University as a senior lecturer. In November 1998 he joined the Department of Electronics at the University of Kent. He is currently a professor and group leader of the Wireless Communications & Networks Research Group at Brunel University. He is a member of IEE and New York Academy of Sciences. He has been awarded a Nuffield research grant as a newly appointed university lecturer in science and engineering and UK-Dutch Scientific Research in collaboration with the International Research Centre for Telecommunications-Transmission and Radar, Delft University, Netherlands, for work involving the development of radio over fiber for 3G microcellular mobile communications. He has acted as guest editor for the *International Journal of Wireless Personal Communications* Special Issue on Radio over Fibre Systems Technologies and Applications. He is a member of several international conference advisory committees, such as VTC, PIMRC, and GLOBECOM, and has organized several workshops on wireless lightwave interaction and radio over fiber for 3G mobile communications in Europe and Japan. He is a member of journal editorial boards such as *Communications and Mobile Computing and Wireless Personal Communications*. His main areas of interest are radio over fiber, software radio networks, and IP mobility. He has published over 100 learned journal and conference papers in these areas. He is editor of a book entitled *Radio over Fiber Technologies for Mobile Communications Networks* (March 2002).