Chapter 5
Cross-Layer Protocols for WSNs

5.1 Why Cross-Layering in WSNs

WSNs achieved a collaborative sensing notion to overcome resource constraints thru adopting the networked deployment of sensor nodes. Moreover, spatiotemporal correlation is a significant characteristic of sensor networks (Vuran and Akyildiz 2006):

- Dense deployment of sensor nodes makes the sensor observations highly correlated in the space domain with noticeable effect of internode proximity.
- Some of WSN applications such as event tracking require sensor nodes to periodically sample and communicate the sensed event features, yielding temporal correlation between each consecutive observation of a sensor node.

Most of the proposed communication protocols exploiting the collaborative nature of WSNs and its correlation characteristics improve energy efficiency. However, they follow the traditional layered protocol architectures; specifically, the majority of these communication protocols are individually developed for different networking layers, i.e., transport, network, medium access control (MAC), and physical layers. While they may realize high performance in terms of the metrics related to each of these individual layers, they are not jointly optimized to maximize the overall network performance while minimizing the energy expenditure. Considering the scarce energy and processing resources of WSNs, joint optimization, and design of networking layers, i.e., cross-layer design, stands as the most promising alternative to inefficient traditional layered protocol architectures.

The basic principle of cross-layer design is to make information available to all levels of the protocol stack. It allows the definition of protocols or mechanisms that do not meet the isolation layers of the OSI model (van der Schaar and Shankar...
In fact, cross-layer integration and design techniques result in significant improvement in terms of energy conservation in WSNs (van Hoesel et al. 2004; Yetgin et al. 2015). Several researches started by focusing on the cross-layer interaction and design to develop new communication protocols (Melodia et al. 2005). Yet, these works either provide analytical results without communication protocol design or perform pairwise cross-layer design within limited scope, e.g., only MAC and network layers, which do not consider all of the networking layers involved in WSNs communication, such as transport, network, MAC, and physical layers.

Considering the scarce energy and processing resources of WSNs, joint optimization, and design of networking layers, i.e., cross-layer design, stands as the most promising alternative to inefficient traditional layered protocol architectures. There are considerable benefits of rethinking the protocol functions of networking layers in a unified way so as to provide a single communication module for efficient communication in WSNs.

Accordingly, an increasing number of recent papers have focused on the cross-layer development of WSN protocols. Researches on WSNs, as detailed in this chapter, reveal that cross-layer integration and design techniques result in significant improvement in terms of energy conservation. Three main reasons stand behind this improvement (Melodia et al. 2005):

- The stringent energy, storage, and processing capabilities of wireless sensor nodes necessitate such an approach. The significant overhead of layered protocols results in high inefficiency.
- Recent empirical studies necessitate that the properties of low-power radio transceivers and the wireless channel conditions be considered in protocol design.
- The event-centric approach of WSNs requires application-aware communication protocols.

On the other hand, a cross-layer solution generally decreases the level of modularity, which may waste the decoupling between design and development process, making it more difficult to add design improvements and innovations. Moreover, it increases the risk of instability caused by functional dependencies, which are not easily foreseen in a non-layered architecture.

In the literature, three main approaches are followed for cross-layering in WSNs (Melodia et al. 2005; Pompili and Akyildiz 2010):

- Layers interactions. The cross-layer interaction is considered, where the traditional layered structure is preserved, while each layer is informed about the conditions of other layers. However, the mechanisms of each layer stay intact. Studies are classified in terms of interactions or modularity among physical (PHY), medium access control (MAC), network, and transport layers. Resource allocation problems are treated thru considering simple interactions between two communication layers. Section 5.2.1 comprehensively presents this approach. Layers interaction does not consider, though, the tight coupling among function-
alities handled at all layers of the protocol stack distinctive, for instance, of multihop underwater networks (Pompili and Akyildiz, A Multimedia Cross-Layer Protocol for Underwater Acoustic Sensor Networks 2010).

- Single-layer integrated module. These approaches integrate different communication functionalities into a coherent mathematical framework and provide a unified foundation for cross-layer design and control in multihop wireless networks. Solutions in this category seek optimality based on an application-dependent objective function and provide guidelines and tools to develop mathematically sound distributed solutions. Section 5.2.2 takes care of detailing this approach.

The heuristic approach is the third to be proposed with little literature adopting it (Pompili and Akyildiz 2010). Resource allocation problems following this approach consider interactions between several communication functionalities at different layers, since it is not always possible to model and control the interactions between functionalities. Solutions in this category rely on heuristics, which often leads to sub-optimal performance. Cross-layer interactions can have a negative effect on desirable properties of the software architecture such as modularity. If cross-layer interactions are not performed in a controlled fashion, it might not be possible to exchange a module without (major) changes to others. In addition, when modules interact closely, they cannot be developed independently. Therefore, if cross-layer interactions are needed, as it is the case in WSNs, they have to be used thoughtfully (Lachenmann et al. 2005).

Sections 5.2.1 and 5.2.2, respectively, detail the layers interactions approach and the single-layer integrated module approach. Table 5.1 offers the taxonomy of cross-layering approaches offered in this chapter.

## 5.2 Cross-Layer Design Approaches

### 5.2.1 Layers Interactions

Targeting the minimization of energy consumption and the enhancement of the WSNs lifetime, several works in WSN have revealed meaningful interactions between different layers of the protocol stack. This has led to several propositions for the cross-layer design. There are protocol designs based on interactions between physical and MAC layers (Venkitasubramaniam et al. 2003; Haapola et al. 2005), between physical and network layers (Zamalloa et al. 2008), between physical and transport layers (Chiang 2005), between MAC and application layers (Song and Hatzinakos 2007), between MAC and network layers (Chilamkurti et al. 2009; Hefeida et al. 2013; Petrioli et al. 2014), between physical, MAC, and network layers (Madan et al. 2006; Bai et al. 2008). More implementations are highlighted all over Sects. 5.2.1.1 and 5.2.1.2.
5.2.1.1 Cross-Layering MAC and Network Layers

To minimize energy consumption in WSNs, several energy-efficient MAC protocols have been proposed to reduce the wasted energy due to the idle listening, by turning OFF the sensor nodes radio (Ye et al. 2002; van Dam and Langendoen 2003) or by scheduling the transmissions of control packets and data packets to avoid data packet collision (Xie and Cui 2007).

At the network layer, energy-efficient routing protocols were proposed. Initially, routing protocols have focused on consuming low power by finding the minimum energy path or by finding the path with nodes having the maximum residual energy or by combining both. The flaw in these protocols is using the optimal path for all nodes communications; consequently, the energy of nodes along such paths quickly drains out causing a network disconnection. As a way out, there has been a focus on maximizing the network lifetime by delaying as possible the occurrence of disconnection. This is implemented by balancing the traffic throughout several sub-optimal paths, so that the nodes consume the energy more equitably. In order to ensure the energy consumption balancing, multipath routing protocols have been proposed (Bouabdallah et al. 2009; Semchedine et al. 2012).

However, the multipath approach is not that sufficient to balance the energy consumption. In fact, a node balances the use of the multiple paths by considering only its data packets without those of other neighboring nodes. Hence, the node has no knowledge about the real amount of the transmitted data by its forwarding nodes. This limitation is treated by devising routing protocols that exploit the interaction between the MAC and the network layers giving rise to a cross-layer approach, as presented in this section. Worth noticing, several works in WSNs have early revealed important interactions between the MAC and network layers, leading to several propositions for the cross-layer design (Melodia et al. 2005; Pompili et al. 2006).

Cross-Layer Network Formation for Energy-Efficient IEEE 802.15.4/ZigBee WSNs (PANEL)

In a WSN the position of the nodes can be predefined to realize optimal coverage and connectivity constraints. PAN coordinator election (PANEL) is proposed for optimal node positioning to minimize the required number of nodes, yet guaranteeing perfect sensing coverage of the monitored field (Cuomo et al. 2013). However, in several contexts, the position of the nodes cannot be predefined. When WSNs are used for pervasive data collection in urban areas or to provide real-time monitoring in emergency scenarios, sensors may be randomly scattered and possibly redeployed over time in the considered area.

The development of self-managing, self-configuring, and self-regulating network and communication infrastructures is interesting, both in the research and industrial communities (Cardei and Du 2005; Dobson et al. 2006; Cipollone et al. 2007). There is a need to identify optimal topology formation and efficient PAN
election for urban sensing or disaster recovery applications. The IEEE 802.15.4 personal area network (PAN) standard addresses the formation and management of low-energy and low-cost WSNs (LAN/MAN Standards Committee 2006); it defines the physical and MAC layers, while the upper layers of the protocol stack (network and applications) are specified by the ZigBee Alliance guidelines (Zigbee Alliance 2020). An overview is made for the energy efficiency, communication, data management, and security solutions that can be adopted for the IEEE 802.15.4 (Baronti et al. 2007). Other works have been proposed to address networking issues in the IEEE 802.15.4/ZigBee, such as efficient data broadcasting (Ding et al. 2006), coexistence of multiple colocated networks under different interference conditions (Lo Bello and Toscano 2009), and device localization (Pichler et al. 2009).

The position of the PAN coordinator strongly affects the network energy consumption for both network formation and data routing (Cipollone et al. 2007; Abbagnale et al. 2008). PANEL is resource aware and energy efficient for PAN coordinator election in IEEE 802.15.4/ZigBee WSNs. Adopting a cross-layer approach, PANEL operates at the network layer of a WSN that relies on the IEEE 802.15.4 MAC layer for the network formation, as displayed in Fig. 5.1; it reconfigures the network topology in order to achieve optimal PAN coordinator placement, improve energy savings, and reduce routing delay. The topology of a WSN formed according to the IEEE 802.15.4 MAC layer is a cluster tree where the PAN coordinator is at the root of this tree.

Functionally, as the cluster tree topology is formed, PANEL assigns the role of PAN coordinator to different nodes in the tree. To do so, a distributed approach is adopted to determine for the network a new tree topology where the maximum and the average number of hops to the PAN coordinator are minimized. PANEL reduces the energy cost of the network and improves its performance by minimizing the number of hops between the source of the sensor readings and the sink and lessening the packet drop rate due to fewer packet collisions at the MAC layer. Experimental
evaluation disclosed that PANEL successfully prolongs WSN lifetime and achieves optimal PAN coordinator election.

PANEL can be easily integrated on top of the IEEE 802.15.4/ZigBee stack; it is fully compliant since it relies on data structures and transmission packets defined in the IEEE 802.15.4 standard, such as the beacon packets. By exploiting the beacons, PANEL is able to:

• Obtain information about the cluster tree topology formed by the IEEE 802.15.4 MAC layer
• Leverage the beacon packet fields to enclose topological information that are needed to optimally reconfigure the network topology

An IEEE 802.15.4 WSN is composed of one PAN coordinator, denoted as $p$ and a set of nodes (LAN/MAN Standards Committee 2006). The network topology defined is called cluster tree, where nodes associated with $p$ establish parent-child relationships and form a tree rooted at $p$. Two node typologies can be identified in an IEEE 802.15.4 network:

• Full function devices (FFDs), which are allowed to associate with other nodes in the network. The PAN coordinator and the intermediate nodes that perform data relay belong to the FFD class.
• Reduced function devices (RFDs), which are not allowed to associate with other nodes. The nodes that are leaves in the cluster tree are part of the RFD category.

The PAN coordinator is the controller of the network and is responsible for initiating the network setup. All nodes relaying data traffic can be also considered coordinators, named $c$ to distinguish from the PAN coordinator $p$. Two logical and hierarchical layers can be identified in the network, as illustrated in Fig. 5.2, specifically, the FFD and RFD layers. PANEL operates only at the FFD layer, i.e., only on nodes acting as coordinators.

IEEE 802.15.4 defines the steps taken by $p$ and the other nodes to initialize and form the network. Node $p$ starts by selecting a suitable communication channel. This selection is performed by the energy detection scan, which assesses the level of interference on each channel thru measuring the peak energy on each available channel (16 channels in the 2.4 GHz ISM band). Nodes join the network according to the association procedure, where each node performs several tasks:

• Searching for available networks
• Selecting a node coordinator (either a $p$ or $c$ coordinator), if a network is available
• Starting an exchange of signaling packets with the chosen coordinator to complete the association

Discovery of available WSNs is accomplished thru monitoring the beacon frames broadcasted by coordinators (LAN/MAN Standards Committee 2006). After scanning the channels, a node selects the coordinator to join and then sends an association request message to this coordinator. The coordinator communicates its decision to accept or reject the node by responding with an association response command
The result of the association procedure, having established parent-child relationships between nodes, is a tree-shaped topology rooted at the PAN coordinator $p$. Following the network formation, each node in the tree stores a neighbor table built during the association procedure, which includes a description of its children (cardinality and type) and its parent (Zigbee Alliance 2020). The neighbor table allows identifying all 1-hop distant nodes.

Level $l$ of a node is the number of hops from the top node. The tree depth $L$ is defined as the maximum value of $l$ within the network, so it identifies the longest path between one of the nodes in the network and $p$. The mean level of nodes $\bar{L}$ is defined as:

$$\bar{L} = \frac{\sum_{l=1}^{L} l \cdot x_l}{N}$$  \hspace{1cm} (5.1)

where

- $x_l$ is the number of nodes at level $l$ within the tree
- $L$ is the tree depth of the cluster tree
- $N$ is the total number of nodes in the cluster tree

$L$ and $\bar{L}$ are affected by the position of the PAN coordinator; they have an impact on the energy consumption of the network during data delivery, as to be clarified in Eq. 5.2.

After the initial setup, the PAN coordinator role could be assigned to different nodes in the network to balance the high-energy drain incurred by a single PAN coordinator (Kim et al. 2003; Sulaiman et al. 2007). Dynamic PAN coordinator election is then needed to achieve several goals:

- Improving the energy efficiency of the network topology.
- Boosting the network resiliency by promptly selecting a new PAN coordinator if the current PAN coordinator runs out of battery power, fails, or becomes unsuitable because of movement.
- Supporting the interconnection between different colocated WSNs.
As instance, assume in Fig. 5.2 that the IEEE 802.15.4 association procedure assigns the role of PAN coordinator to node I₁. Among all the coordinators at the FFD layer, node F would be more suitable than node I₁ to take this role. This is because node F is at a more central position than node I₁, hence minimizing the number of hops with respect to all the other nodes in the network. PANEL identifies node F as the new PAN coordinator and reconfigures the tree where the root is the new PAN coordinator F.

The energy cost associated with the data delivery from a node-generating traffic and the sink can be divided into two components:

- The energy necessary to transmit the data packets along a routing path, denoted as \( E_{\text{routing}} \).
- The energy spent at the MAC layer to access the medium, \( E_{\text{mac}} \), which includes the energy for data re-transmission in case of packet corruption.

IEEE 802.15.4/ZigBee WSNs typically employ hierarchical routing protocols; these are simple to implement, do not require high node computational capability, and do not need additional overhead to establish paths from source to destination within the cluster tree network (Cuomo et al. 2007). According to these protocols, data is relayed by intermediate nodes along the cluster tree paths from the source to the sink identified by the parent-child relationship. Therefore, the energy spent to send data on the routing paths is proportional to the number of hops along the path from source to the PAN coordinator, as destination, since every node on the path spends energy to receive data from its children and to forward the same data to its parent. All nodes are assumed to generate one packet directed to the PAN coordinator without performing data aggregation. Then the \( E_{\text{routing}} \) component for a single packet can be calculated as:

\[
E_{\text{routing}} = (E_{\text{TX}} + E_{\text{RX}}) \times L \times N
\]

where \( E_{\text{TX}} \) and \( E_{\text{RX}} \) are the energy spent by a node to transmit and to receive a data packet at 1-hop distance, respectively.

Equation 5.2 suggests that \( E_{\text{routing}} \) can be reduced if \( L \) is minimized. It is to be noticed that reducing \( L \) also reduces \( L \); this can be obtained by properly controlling the PAN coordinator position. Figure 5.3 shows the impact of the PAN coordinator position on \( L \) and \( L \). Figure 5.3a shows the topology formed by the IEEE 802.15.4 association procedure, where the PAN coordinator is node A, \( L = 4 \) and \( L = 23 \). The goal of PANEL is to elect a new PAN coordinator that guarantees smaller values of \( L \) and \( L \) without changing the association relationships already established among the nodes. The resulting topology after running PANEL is shown in Fig. 5.3b, where the new PAN coordinator role is assigned to node B. In this new scenario \( L = 3 \) and \( L = 2 \). By reducing \( L \) and \( L \), the value of \( E_{\text{routing}} \), driven by Eq. 5.2 decreases.

The cost of \( E_{\text{mac}} \) is proportional to the number of transmissions at the MAC layer. Therefore, \( E_{\text{mac}} \) depends on the sensor nodes spatial distribution and transmission
Transmission collisions are due to overlapping transmission regions between nodes, given the broadcast nature of the wireless medium. The goal of PANEL is to minimize such collisions by positioning the PAN coordinator so as to balance the utilization of the paths in the network. In Fig. 5.4, after moving the PAN coordinator from node A to node B, radio overlapping regions are not modified; the nodes are not physically moved from the configuration of Fig. 5.4a to the configuration of Fig. 5.4b. The modification instead is on the utilization pattern of some of the links, e.g., the link between nodes A and B. While three data flows are converging onto node A according to the configuration of Fig. 5.4a, only two data flows traverse the A-B link in the configuration of Fig. 5.4b, thus reducing data transmission collisions on this link. PANEL design revolves around driving down the $E_{\text{routing}}$ cost by minimizing $L$ and $\bar{L}$, while reducing the radio transmission collisions over the paths toward the PAN coordinator.

Experimentation is carried thru the ns-2 simulator implementing the physical and MAC layers of the IEEE 802.15.4 standard, including the association procedure. It is unveiled that PANEL on average decreases the tree depth and mean level of nodes by determining a new network topology; hence, a new PAN coordinator starting from the initial IEEE802.15.4/ZigBee cluster trees. It is also shown that the network lifetime increases over the basic IEEE 802.15.4/ZigBee configuration.
when PANEL is applied to a network with different data traffic patterns. The experimentation outcomes depict improvement on the tree depth and mean level of nodes, as well a network lifetime increase due energy saving:

- Tree depth and mean level of nodes improvement. In terms of topological characteristics, i.e., tree depth and mean level of nodes, a comparison is made between cluster trees formed by the IEEE 802.15.4 association procedure and the network topology obtained with PANEL. The network scenario consists of \( N \) nodes, with a number, \( N_F \), of FFDs randomly deployed in a square area of side \( S \). The number of FFDs is \( N_F = \lceil 0.33 \times N \rceil \). The choice of this value of \( N_F \) is justified by the fact that in real WSNs only a fraction of nodes is usually assigned the role of coordinator. At the beginning of each experiment, the initial PAN coordinator is randomly selected.

First, the effect of PANEL is illustrated when applied to an IEEE 802.15.4/ZigBee cluster tree topology. In the simulation model, both physical layer propagation effects and MAC layer radio collisions, including the collisions occurring during the association procedure, are modeled. For the physical layer, ns-2 uses the two-ray ground propagation model. Each packet received at the physical layer should be above the receive threshold value, assumed equal to \(-97 \text{ dBm}\). As for the collisions, when two packets are received simultaneously, the receiver chooses the strongest among them, based on the capture threshold.

Figure 5.5 illustrates the findings for two scenarios, where \( N = 50 \) and 100. It is displayed that PANEL improves the topology configuration, as seen from the reduced width and increased height of the node level probability density function curve. Clearly, with PANEL the probability to find nodes with smaller number of levels is higher than in the IEEE 802.15.4 scenario; shorter routing paths are established between any node and the PAN coordinator. From Eq. 5.2, shorter routing paths imply node energy savings and reduced data delivery delay.

Figure 5.6 shows a comparison of the average tree depth and mean level values for both the IEEE 802.15.4/ZigBee and the PANEL topology configurations.

- Energy considerations and network lifetime increase. The impact of PANEL on the energy consumption of the network is obtained by theoretical considerations taking into account the energy needed to execute PANEL over a basic IEEE 802.15.4 configuration. A thorough energy evaluation requires accounting for the energy needed by each node to execute PANEL, which is directly proportional to the number of iterations each node is required to perform. The energy needed to run PANEL can be divided into two components:

  - The energy, \( E_p \), spent by the PAN coordinator at an iteration beginning.
  - The energy, \( E_c \), spent by the PAN coordinator children at an iteration beginning.

Given these two terms, the energy required by a WSN to run PANEL can be expressed as:
where given a network of $N$ nodes:

\[ E_{\text{PANEL}} = E_p \times N_p + E_c \times N_c \]  

(5.3)

where

- $E_p$ is the energy spent by the PAN coordinator at the beginning of a PANEL iteration
- $E_c$ is the energy spent by the child becoming PAN coordinator at the beginning of a PANEL iteration
$N_p$ is the number of nodes that temporarily take the role of PAN coordinator during the execution of PANEL.

$N_c$ is the total number of children of all the temporary PAN coordinators during the execution of PANEL.

The values of $E_p$ and $E_c$ are related to the number and type of instructions that can be found in the PANEL algorithms. Some of the instructions involve data processing; others comprise data transmission and reception. Data processing instructions

---

Fig. 5.6 Panel and IEEE 802.15.4 compared in terms of tree depth and mean level of nodes. (a) Tree depth comparison, (b) Mean level of nodes comparison. (Cuomo et al. 2013)
require less energy than data transmission and reception. \( E_p \) and \( E_c \) can be expressed as:

\[
E_p = (E_{RX} \times L_{payload}) + \left[ E_{RX} \times L_{payload} \times (N - 1) \right] + (E_{instr} \times num_{instr}^p) \quad (5.4)
\]

\[
E_c = (E_{RX} \times L_{payload}) + (E_{instr} \times num_{instr}^c) + (E_{TX} \times L_{payload}) \quad (5.5)
\]

where

\( E_{TX} \) and \( E_{RX} \) are, respectively, the energy spent by a node to transmit and receive one bit at 1-hop distance

\( L_{payload} \) is the size, expressed in bits, of packets exchanged to transmit data between the PAN coordinator and its children, during each iteration of PANEL

\( N \) is the total number of nodes in the WSN

\( E_{instr} \) is the energy spent by a node for data processing, e.g., addition, bitwise operations, etc.

\( num_{instr}^p \) indicates the number of different data processing instructions that the PAN coordinator executes at each iteration

\( num_{instr}^c \) designates the number of different data processing instructions every PAN coordinator child executes at each iteration.

The size of the packet payload used by the PAN coordinator and the children is assumed constant and equal to \( L_{payload} \).

To exhibit the impact on the energy cost when the network runs PANEL, simulations were run with \( N \) randomly deployed nodes in a square area of side \( S \). A subset of these \( N \) nodes is composed of a number, \( N_F \), of FFDs. The nodes have a transmission range \( T_R \). The basic IEEE 802.15.4 association procedure returns topologies called \( \{ T_{802.15.4} \} \), while PANEL produces topologies called \( \{ T_{PANEL} \} \). For both topologies, a constant bit rate traffic (CBR) pattern is applied to all nodes sending one data packet every superframe. All packets flow toward the PAN coordinator. Under these conditions, the average energy, needed to send the data within a superframe for both \( \{ T_{802.15.4} \} \) and \( \{ T_{PANEL} \} \), is calculated. Moreover, \( E_{PANEL} \) is calculated from the execution of PANEL using Eq. 5.3–Eq. 5.5.

The cost of \( E_{PANEL} \) is spread across all the superframes to obtain the total energy consumption for \( \{ T_{PANEL} \} \). Figure 5.7 shows the mean value of the difference between the energy usage of \( \{ T_{802.15.4} \} \) and of \( \{ T_{PANEL} \} \) for a single superframe. As it can be noted, the value of this difference is always greater than zero. Therefore, the energy consumption in a superframe related to topologies reconfigured with PANEL is always smaller than the energy consumed in a superframe by topologies obtained applying the basic IEEE 802.15.4 association procedure. Gains in the range 20–27% are realized; if in the same scenario, performance gain is computed as a percentage with respect to the average energy needed to send a superframe in case of \( \{ T_{802.15.4} \} \).

The energy consumption of \( \{ T_{PANEL} \} \) also includes the consumption from the execution of PANEL in the worst-case scenario, according to Eq. 5.4–Eq. 5.5. As
illustrated in Fig. 5.7, the energy saving is a lower bound on the energy saving achievable with PANEL. It can also be seen that PANEL performance increases as the number $N$ of nodes grows, signifying that PANEL scales well with the size of the network.

Figure 5.8 illustrates the percentage increase of network lifetime with PANEL over IEEE 802.15.4 topologies. This experiment involves two different fractions of FFDs. In both cases, the network lifetime with PANEL increases over 50% when $N = 200$. The performance boost is more evident with $N_F = \lceil 0.5 \times N \rceil$ than with $N_F = \lceil 0.33 \times N \rceil$, because higher value of $N_F$ guarantees greater density of FFDs, which implies larger availability of coordinators eligible for the role of PAN coordinator. This is a significant result considering the need to maintain low-power usage of WSN in order to maximize its operational lifetime.

Lastly, the development of self-managing, self-configuring, and self-regulating protocols for PAN coordinator election for IEEE 802.15.4/ZigBee in WSNs needs further probing. In this direction, PANEL is a cross-layer approach that addresses the election of the PAN coordinator node. By selecting the best PAN coordinator, PANEL allows to reduce the energy consumption in WSNs. The PANEL distributed solution performs the following operations:

- Reconfiguring a network topology previously formed by the IEEE 802.15.4 association procedure
- Introducing little or no overhead in the wireless packet transmission
- Selecting PAN coordinators that are in “balanced” positions at the network, i.e., where the tree depth and the average mean level of nodes are minimized

These operations result in limiting the energy depletion of the network, thus extending its lifetime. PANEL is flexible, in that it transparently cooperates with the IEEE 802.15.4 standard without modifying the underlying 802.15.4 basic function-
A Cross-Layer Routing Protocol for Balancing Energy Consumption in WSNs (CLB)

The purpose of the suggested CLB is to enhance the WSNs lifetime by balancing the energy consumption in the forwarding task (Yessad et al. 2015). The energy efficiency concern can be addressed by finding the minimum energy path, while load balancing can be achieved by using multiple sub-optimal paths. CLB exploits the interaction between the MAC and the network layers, with the goal of enhancing the WSN lifetime. A mathematical model and simulations evaluate the performance of the proposed protocol. The obtained results show that the CLB cross-layer routing protocol uses all forwarding nodes in an equitable manner; this enables avoiding network partitioning and enhances the network lifetime.

The CLB-routing protocol is a bottom-up approach where the network layer uses information given by the MAC layer for the choice of the next forwarding hop. It just defines a communication interface between the MAC layer and the network layer; this is intended to facilitate enhancements in the MAC and network layers separately and easily considering other design concerns such as delay, quality of service, and congestion avoidance. CLB has two phases, the initialization phase and the data transmission phase. In the initialization phase, the sink broadcasts a route request message to find sub-optimal routes from each source node to the sink. Then, in the data transmission phase, the MAC layer informs the network layer about all the overheard communications of the neighboring nodes. With this information, a sending node can know how many times each forwarding node has routed data. Accordingly, to balance the energy consumption of the forwarding nodes, a sending node chooses its next hop among the less-used. Differently from several multipath

![Network lifetime increase](image)
routing protocols, the choice of the next hop is not probabilistic and leads to better balancing of energy consumption.

Before introducing CLB in details, a differentiation from other approaches is highlighted in what follows:

- The adaptive load-balanced algorithm (ALBA) was designed to consider load balancing and congestion; it is a packet forwarding protocol for ad hoc and sensor networks (Casari et al. 2006). ALBA follows the integrated approach that combines geographic routing and medium access control (MAC), thus exploiting the knowledge of node positions in order to achieve energy-efficient forwarding (Sect. 5.2.2). The considered scenario is critical for medium and high traffic, as contentions for channel access and the resulting collisions lead to performance degradation. To counter this effect, leverage on network density favors the choice of relay candidates that are not overloaded. With ALBA, nodes strive to channelize traffic toward uncongested network regions, rather than just maximizing the advancement toward the final destination. All eligible forwarder nodes of a source node calculate two indices in their path toward the sink, namely, the geographic priority index (GPI) and the priority queue index (QPI). Noticeably, the load balancing viewed in ALBA focuses on congestion avoidance, not energy consumption balancing as studied in CLB.

- A many-to-one real-time sensor network is considered, where sensing nodes are to deliver their measurements to a basestation under a time constraint, with the overall target of minimizing the energy consumption at the sensing nodes (Puccinelli et al. 2006). The quality of the links and the remaining energy in the nodes are the primary factors that shape the network graph; link quality may be measured directly by most radios, whereas residual energy is related to the node battery voltage, which may be measured and fed into the microcontroller. These quantities may be used to form a cost function for the selection of the most efficient route. Moreover, the presence of a time constraint requires the network to favor routes over a short number of hops in order to minimize delay. Hop number information may be incorporated into the cost function to bias route selection toward minimum-delay routes. Based on the integrated approach, a cross-layer cost function that mixes the physical and network layers is obtained (Sect. 5.2.2); it includes raw hardware information (remaining energy), physical layer data (channel quality), and a network layer metric (number of hops). A route selection scheme based on these principles intrinsically performs node energy control for the extension of the lifetime of the individual nodes and for the achievement of energy balancing in the network; intuitively, the long-hop approach permits the time-sharing of the critical area among more nodes. As a comparison, CLB balances energy consumption based on specific information about the amount of routed data from each node; hence, it is not probability based and does not rely on heuristics.

- CLB aims to enhance the network lifetime by balancing energy consumption; other approaches target energy efficiency by maximizing the sleep time. Achieving minimum energy consumption is the goal of MAC-CROSS (Suh et al. 2006). Based on the layers interactions approach (Sect. 5.2.1), MAC-CROSS exploits the interactions between MAC and network layers to achieve energy
efficiency for WSNs (Suh et al. 2006). Routing information at the network layer is used in the MAC layer such that it can maximize the sleep duration of each node. Through implementation on a MICA mote platform (Crossbow 2002) and simulation study using ns-2 simulator (Chap. 7), the performance of MAC-CROSS is evaluated.

Also, based on the integrated approach (Sect. 5.2.2), the cross-layer energy-efficient protocol (CLEEP) targets prolonging the nodes sleep time by adopting a strategy that considers the physical, MAC, and network layers (Liu et al. 2008). In the physical layer, CLEEP coordinates the transmission power between two nodes and maintains the nodes neighbor tables periodically to save the transmission energy. Then, the optimal routing path is constructed by exploiting the transmission power and neighbor tables of the physical layer, which minimizes the total energy consumption. Finally, in order to prolong the node sleep time, the MAC layer makes use of the routing information to determine the node duty-cycle.

Moreover, integrating MAC and network layers (Sect. 5.2.2), an enhanced cross-layer protocol (ECLP) is designed for energy efficiency and latency in WSNs to realize efficient data delivery (Kim et al. 2009). To reduce energy wastage due to idle listening and overhearing and to alleviate long delay, ECLP uses an adaptive duty-cycle scheme with the adaptive time-out and reservation request-to-send (RRTS). Moreover, a tree-based energy-aware routing algorithm is developed in ECLP to minimize overhead cost and prolong the network lifetime.

Basically, to augment the WSN lifetime by balancing energy consumption during the forwarding task, sensor nodes must be used fairly. If two nodes have the same cost for routing source node data, they must be used as relays for the same number of times. Based on this idea, two routing protocols fair energy-aware routing (FEAR) (Yessad et al., Proposition and Evaluation of a Novel Routing Protocol for Wireless Sensor Networks 2011) and balanced energy efficient routing (BEER) (Yessad et al. 2012) were previously proposed as improvements of the energy-aware routing (EAR) (Shah and Rabaey 2002). FEAR improved the network lifetime by reducing the probability of using the highly demanded sensor nodes in the network, i.e., those belonging to several routes. BEER reduces the probability of using forwarding nodes belonging to a source node in a unique route. Even though FEAR and BEER provide more equity among sensor nodes when compared to EAR, they suffer from increased overhead. On the other hand, in EAR, FEAR, and BEER, the sub-optimal paths are probabilistically chosen; so, load balancing is probabilistic.

In order to achieve an accurate energy consumption balancing without overhead, CLB-routing at the network layer exploits information given by the MAC layer. CLB-routing operates in two phases:

- First phase. After the network deployment, sensor nodes establish their forwarding tables as in EAR. The sink broadcasts a route request message with a field cost initialized to 0. Each node, receiving the route request message, updates the cost field according to its residual energy and the power required for the communication between that node and the sender of the route request, and then it
broadcasts the route request message. If a given node \( i \) receives a route request from a node \( j \) with the cost field \( cost_j \), it calculates \( cost_i \) as follows:

\[
    cost_i = cost_j + C_{ij}
\]

such that

\[
    C_{ij} = e_{ij}^\alpha \times R_i^\beta
\]

where

- \( e_{ij} \) is the power required for the communication between nodes \( i \) and \( j \)
- \( R_i \) is the residual energy of node \( i \) normalized with respect to its initial energy
- \( \alpha \) and \( \beta \), the weighting factors, can be chosen to find the minimum energy path or the path with nodes having the maximum residual energy or the combination of both

After the reception of the route request message from all neighbors, a node can establish its forwarding table by adding neighbors with minimal cost. Then, for forwarding the route request message, it calculates the average cost that it sets in the cost field:

\[
    cost_i = \frac{\sum_{k \in FT_i} cost_k}{|FT_i|}
\]

where \( |FT_i| \) is the number of routes recorded in the forwarding table of node \( i \).

This phase ends when the route request message is broadcasted over the whole network, and all nodes have set their forwarding tables with routes to the sink.

- Second phase. Sensor nodes sense phenomena in the field of interest according to their application and send data to the sink. Initially, nodes send data over the neighbor in their forwarding table having the minimal cost. Progressively, the network layer of each node will have information about the use of its neighbors for routing data. Nodes are supposed to use the CSMA/CA-based MAC protocols, S-MAC (Ye et al. 2002) or T-MAC (van Dam and Langendoen 2003) with RTS/CTS sequence. When a sensor node wants to send data over a neighbor node, it sends an RTS message and then receives a CTS message from the forwarding node; CTS is received by all its neighbors. In CLB, if the node receiving a CTS message is the destination, it sends the data packet to the sender of the CTS message. Otherwise, instead of dropping the CTS as it is the case in layered protocol, it sends the source address of the CTS message to the network layer. Upon receiving the CTS message, the network layer increments the variable \( N \) associated to the sender of the message. The variable \( N \) is a field in the forwarding table, which counts the number of times that each neighbor node has routed data. Whenever a given node \( j \) has data to send, it calculates the value of \( B \) associated with each forwarding node \( i \). Then, it sends its data via the neighbor having the greater value of \( B \).
To evaluate the performance of CLB-routing, a mathematical model evaluates and compares its performance with those of EAR, FEAR, and BEER. The WSN model under study has the following properties:

- The sensor network is composed of $M$ sensor nodes scattered in a field of interest in flat manner, i.e., all sensor nodes play the same role in the network.
- There are $k$ source nodes that send the sensed data in the environment to the sink. The network can be divided into levels of $k$ nodes; the first level $L_1$ is the one composed of source nodes. The $i^{th}$ node of the $j^{th}$ level, $L_j$, represented as $N_{ji}$, has $i$ forwarding nodes in the next level $L_{j+1}$ (Fig. 5.9).
- There is one sink that gathers the sensed data.
- The nodes and the sink are not mobile.
- The sensor nodes are not rechargeable.
- There is no method of getting location information about sensor nodes.
- The network application can be query driven, event driven, time driven, or the hybridization of the three.

The energy $E$ consumed by a node $N_{ji}$, in the network model, to route $S$ packets of data to the sink is calculated for EAR, FEAR, and BEER. Node $N_{ji}$ can route data sent by nodes $N_{(j-1)(i)}$, $N_{(j-1)(i+1)}$, $N_{(j-1)(i+2)}$, …, and $N_{(j-1)(k)}$, respectively, with the probabilities $P_{N_{(j-1)(i)}N_{ji}}$, $P_{N_{(j-1)(i+1)}N_{ji}}$, $P_{N_{(j-1)(i+2)}N_{ji}}$, …, and $P_{N_{(j-1)(k)}N_{ji}}$. Accordingly:
\[ E = P_{N_{(j-1)(0)}}N_{(j)} * (E_r + E_t) + P_{N_{(j-1)(i+1)}}N_{(j)} * (E_r + E_t) + \ldots + P_{N_{(j-1)(k)}}N_{(j)} * (E_r + E_t) \]  

(5.10)

where

\[ E_r \text{ and } E_t \text{ are the energy required for the reception and transmission of data by node } N_{ji}, \text{ respectively.} \]

In EAR, \( E \) is calculated as (Shah and Rabaey 2002):

\[ E = \left( E_r + E_t \right) * \left[ \frac{1}{C} + \frac{1}{C} \frac{1}{i+1} + \frac{1}{C} \frac{1}{k} \right] \]

(5.11)

where all nodes in the network are assumed to have the same cost \( C \). This assumption holds in the calculation of \( E \) in FEAR, BEER, and CLB.

FEAR evaluates \( E \) as follows (Yessad et al. 2011):

\[ E = \left( E_r + E_t \right) * \left[ \frac{1}{k-i+1} \sum_{m=k-i}^{k} \frac{1}{m} \right] \]

(5.12)

For BEER, \( E \) is computed as (Yessad et al. 2012):

\[ E = \left( E_r + E_t \right) * \left[ \frac{1}{k-i+1} \frac{1}{\sum_{m=k-i}^{k} \frac{1}{m}} \right], \text{ for } i < k \]

(5.13)

In CLB, node \( N_{ji} \) can route data sent by nodes \( N_{(j-1)(0)}, N_{(j-1)(i+1)}, N_{(j-1)(i+2)}, \ldots, \) and \( N_{(j-1)(k)} \). As in Eq. 5.11–Eq. 5.13, the cost \( C \) of all nodes in the network is the same. For the first packet, the performance is influenced by the position of the node which first sends data. The nodes are supposed to send data in the order of their identifications. This means that if node \( N_{ji} \) starts communication, the second will be \( N_{ji((i+1) \mod k)} \) and then the third will be \( N_{ji((i+2) \mod k)} \) and so forth, until the last node \( N_{ji((i+k-1) \mod k)} \) sends its data.

If node \( N_{(j-1)(m)} \) starts the communication, node \( N_{ji} \) can be solicited by the nodes:
- \( N_{j-1}(i) \) and \( N_{j-1}(m+i-1) \), if \( i < m \) and \( m < k - i + 2 \)
- \( N_{j-1}(m+i-1) \), if \( (i \geq m \) and \( m < k - i + 2) \)
- \( N_{j-1}(i) \), if \( i < m \) and \( m \geq k - i + 2 \)
- None, if \( i \geq m \) and \( m \geq k - i + 2 \)

As there is no probabilistic routing, a node can route data from two, one, or no node. So, the energy consumed by a given node \( N_j \) is calculated to be:

\[
E = \begin{cases} 
(E_r + E_r) * 2, & \text{if } i < m \text{ and } m < k - i + 2 \\
(E_r + E_r), & \text{if } (i \geq m \text{ and } m < k - i + 2) \text{ or } (i < m \text{ and } m \geq k - i + 2) \\
0, & \text{if } i \geq m \text{ and } m \geq k - i + 2 
\end{cases} 
\] (5.14)

For the energy, as driven in Eq. 5.11–Eq. 5.14, the standard deviation is drawn versus the number of nodes, \( k \), at a certain level (Fig. 5.10), and the number of packets sent, \( S \) (Fig. 5.11). The following is remarked:

- Sending one data packet (\( S = 1 \)) for \( k = 1 \) to 10, where for each value of \( k \), \( i \) takes values in the interval \([1, k]\). For CLB-routing, multiple graphs are plotted according to the value of \( m \), the identification of the node starting the communication (Fig. 5.10).

- Calculating the standard deviation for the number of packets sent, \( S = 2–5 \), where \( k \) is set to 10. It is revealed from Fig. 5.11 that in CLB-routing, the standard deviation is constant while for EAR, FEAR, and BEER, it increases with the increase of \( S \). As noticed, the standard deviation of the energy levels of nodes, in CLB throughout the communication, remains the same. This is because after a

![Fig. 5.10](image-url)  
Standard deviation versus number of nodes at a network level. (Yessad et al. 2015)

Legend:
The number of packets sent, \( S = 1 \)
cross 2, cross 4, cross 6, and cross 8 represent the CLB-routing graphs for \( m = 2, 4, 6, \) and 8 respectively
certain amount of communications in a given zone, all sending nodes in that zone gain information about the amount of data packets forwarded by each node and hence can easily balance the use of their forwarding nodes. As shown in the figure, CLB uses sensor nodes equitably, while EAR, FEAR, and BEER use some nodes more than others in the routing task.

Using SenSim (Chap. 7), more comparative simulations of CLB versus EAR, FEAR, and BEER are performed.

5.2.1.2 Cross-Layering Physical and MAC and Network Layers

Cross-Layer Optimized Routing in WSNs with Duty-Cycle and Energy Harvesting (TPGFPlus)

The two-phase geographic greedy forwarding (TPGFPlus) is a cross-layer optimized routing algorithm, where the physical, MAC, and network layers cooperate to choose the optimized transmission route (Han et al. 2015). TPGFPlus is the first cross-layer optimized work to consider 2-hop-based geographic routing for duty-cycled and energy renewable WSNs. Specifically, an energy harvesting model is introduced, such that each node has the ability to adjust its transmission power depending on its current energy level. Also, the energy consumed uniformly connected $k$-neighborhood (EC-CKN) algorithm is applied for sleep scheduling at the MAC layer (Yuan et al. 2011). The physical layer provides the remaining energy and transmission radius information for sleep scheduling at the MAC layer, which dynamically schedules the sleep rate of the network. Then, the network layer chooses the routes that reduce energy consumption, while the physical layer adjusts the transmission power accordingly.

TPGFPlus, which is inherently loop free, addresses several issues:
• How to find a good approach to facilitate the geographic routing in duty-cycled WSNs with energy harvesting?
• How the geographic forwarding policy with 1-hop neighbor information is suitable for duty-cycled WSNs?
• How to design an efficient geographic node-disjoint multipath routing algorithm that allows higher sleep rate in WSNs?

On the basis of extensive simulations, it was found that geographic routing in duty-cycled WSNs should be 2-hop-based, not 1-hop-based. The 2-hop-based geographic forwarding policies achieve better routing performance than the previously proposed 1-hop TPGF (Shu et al. 2010), in terms of both the average number of explored paths and the average path length. What is more the cross-layer optimized routing allows considerable higher sleep rate in the network.

To describe the interactions of the multiple layers, Fig. 5.12 illustrates how a cross-layer optimized framework underlies the proposed TPGFPlus scheme. The framework takes into account the physical, the MAC, and the network layers:

• The physical layer. The network model is first to be introduced. Let $\mathcal{N}(v_i)$ and $\mathcal{N}(v_i)'$ be respectively the sets of node $v_i$ 1-hop and 2-hop neighbor nodes; that is, $v_i$ 2-hop neighbors are the neighbors of $v_i$ 1-hop neighbors after removing the duplicated nodes. The considered simple scenario embodies only one source node in the outdoor network.

The network embodies $N$ sensor nodes randomly deployed. The locations of sensor nodes and the basestation are fixed and can be obtained using the GPS. Each node knows its own location and the position information of its 1-hop and 2-hop neighbors. The Euclidean distance between any two node $v_i$ and $v_j$ is denoted as $\text{Dist}_{i,j}$. Both the source and the sink nodes are assumed with unlimited power supply. Each sensor node is powered thru rechargeable batteries with the capability to harvest solar power from one additional solar cell. The energy harvesting rate and energy consumption rate in each individual sensor node are different and unpredictable, since many factors can affect the energy level, such as the unstable local weather, the different number of 1-hop neighbor nodes, and the unexpected query tasks from users.

Also, each node uses an adjustable transmission power depending on its battery level. An example of such sensor nodes is Berkeley Motes (Hill et al. 2000). Instead of transmitting at maximum power, nodes take their energy resource into consideration and collaboratively adjust their transmission power accordingly. Any node, if rich in residual energy, will have the ability of enlarging its maximum transmission radius; thus, network connectivity and network sleep rate are directly affected.

• MAC layer. To balance energy consumption and prolong network lifetime, all nodes are assumed to operate with EC-CKN-based sleep/awake duty-cycling. The 2-hop neighbors are gathered when executing EC-CKN for sleep scheduling in WSNs. Each sensor node switches the radio ON and OFF in turn based on the 2-hop neighbors remaining energy information. Time is divided into epochs,
where each epoch is represented by $T$. In each epoch, the node will first transmit packets and then run the EC-CKN sleep/awake scheduling algorithm to schedule the state of the next epoch, whether sleep or awake. Sensor nodes take their current energy level information, as the parameter, to decide whether a node is to be active/sleep and to dynamically adjust the network sleep rate. The parameter $k$, which is considered for controlling the sleep rate of the network, can directly affect the number of awake nodes for geographic routing.

- **Network layer.** In this layer, a 2-hop geographic multipath routing, TPGFPlus, is proposed.

In the proposed routing algorithm, each node locally maintains its 1-hop and 2-hop neighbors information such as location, residual energy, energy-harvested rate, and energy consumed rate. The algorithm is a 2-hop geographic forwarding for a cross-layer optimized multipath routing. The gathering of 2-hop neighbors is not an extra overhead for TPGFPlus algorithm, as the 2-hop neighborhood information is already gathered when executing EC-CKN. TPGFPlus consists of two phases, namely, 2-hop geographic forwarding and path optimization:
• 2-hop geographic forwarding. In this phase, two policies are introduced, explicitly, the greedy forwarding and step back and mark. For the greedy forwarding policy, a forwarding node always chooses its next-hop node that is closest to the basestation, among all its 1-hop and 2-hop neighbor nodes, and the next hop node to the basestation can be farther than itself. Once the forwarding node is done choosing its next-hop node among its 2-hop neighbor nodes that have not been labeled, it finds an intermediate 1-hop direct neighbor that has not been labeled according to some selection policy. A digressive number-based label is given to the chosen sensor node along with a path number, which will be kept during the path exploration period. Thus, it is feasible even for resource-constrained sensors. This greedy forwarding principle is different from the greedy forwarding principle in (Karp and Kung 2000; Leong et al. 2005; Holland et al. 2011), where a forwarding node always chooses the 1-hop neighbor node that is closer to the basestation than itself. Moreover, it is characterized by the absence of the local minimum problem.

Among candidate nodes with similar progress to the destination, the one with higher-energy harvesting rate and residual energy will be chosen first. Figure 5.13 describes the geographic forwarding process of TPGFPlus. Noticeably, in 1-hop routing, forwarding packets is always to the 1-hop neighbor that is nearest to the sink. While in 2-hop routing, a forwarding node always chooses its next hop node to be the closest to the basestation, among all its 1-hop and 2-hop neighbors. Once the forwarding node chooses its next-hop node among its 2-hop neighbor nodes that have not been labeled, it finds an intermediate 1-hop direct neighbor that has not been labeled according to some selection policy.

Although such a method does not have a well-known local maximum problem, there may be block situations (Shu et al. 2010). During a path discovery, if any forwarding node has no 1-hop neighbors except its previous hop node, this node is marked as a block node and the situation as a block situation; in such situation, the step back and mark course will start. The block node steps back to its previ-

![Fig. 5.13](image)

**Legend:**
Node A chooses a 2-hop neighbor node G as its next-hop node that is closest to the sink among all A’s 1-hop and 2-hop neighbors. Once node G is chosen, node A must first select node B as an intermediate 1-hop direct neighbor based on a certain selection policy. As shown, if node G has a considerable higher-energy level, it can increase its transmission power

$TR_1, TR_2$ are transmission ranges
ous-hop node, which will attempt to find another available neighbor as next-hop node. This procedure is repeated until a node successfully finds a next-hop node to convert back to the greedy forwarding course.

TPGFPlus does not include the face routing concept, making it different from existing geographic routing algorithms.

- **Path optimization.** As shown in Fig. 5.14a, a path circle occurs if for any given routing path, two or more nodes in a path are neighbor nodes of another node in this path. To optimize the found routing path, unnecessary circles are to be removed; for this purpose, the label-based optimization is suggested. The principle is that any node in a path only relays the acknowledgement to its 1-hop neighbor node that has the same path number and the largest node number. In Fig. 5.14b, after path optimization, a shorter path is obtained. Once the optimized path is found, a release command is sent to all other nodes in the path that are not used for transmission. These released nodes can be reused for exploring additional paths. After receiving the successful acknowledgment, the source node starts to send sensed data to the successful path with the preassigned path number.

The greedy forwarding mechanism, the main component of geographic routing, usually follows the principle that each node forwards packets to the neighbor node that is closest to the destination with the assumption of highly reliable links. However, this assumption is not realistic. To optimize the forwarding choices, the performance of TPGFPlus is observed under three different forwarding mechanisms:

- **Policy 1.** Finding an intermediate 1-hop direct neighbor node that is closest to the 2-hop neighbor node. For this forwarding policy, TPGFPlus finds a neighbor closest to the 2-hop neighbor node and makes the maximum progress toward the destination, which is commonly employed. But while assuming the wireless channel reliable, this policy may not work well, as it may choose a neighbor farthest from the current node with a poor link (Seada et al. 2004).

![Fig. 5.14 Path optimization. (a) The found routing path with circles, (b) The optimized routing path after eliminating circles. (Han et al. 2015)](image-url)
• Policy 2. Finding an intermediate 1-hop direct neighbor node that forwards packet from the current node to its 2-hop neighbor node with the shortest distance. This forwarding policy attempts to minimize total geographic distance between the source node and the sink.

• Policy 3. Finding an intermediate 1-hop direct neighbor node with the most remaining energy, or the best link quality (interference minimized), or even the optimal multifactor weighted cost function value, and so on. In this forwarding policy, the adopted forwarding strategy is $\text{Resi} \_\text{Energy} \times \text{Distance}$ for the adopted energy-aware geographic routing, where $\text{Resi} \_\text{Energy}$ is the current energy level of the candidate node and $\text{Distance}$ is the distance from current node to the 2-hop neighbor node via the candidate node.

In summary, the goal is to study 2-hop geographic node-disjoint multipath routing in duty-cycled WSNs with energy harvesting and to find optimal forwarding strategy for different application requirements.

Duty-cycle characteristics in the proposed TPGFPlus need to be introduced. The duty-cycle is defined typically as the ratio between active period and the full active/sleep period (Wang et al. 2003; Yan et al. 2003; Liu et al. 2004; Gu et al. 2007). Sensor nodes alternate between sleep and active states. In the sleep state, they go to sleep and thus consume little energy, while in the active state, they actively perform sensing tasks and communications, consuming significantly more energy (Wang and Liu 2009). CKN and EC-CKN are different from other existing duty-cycle algorithms as there is no waiting delay and for the simplicity of their synchronization mechanism:

• Avoidance of waiting delay. In a time-varying connectivity network, a message can either be forwarded over the currently awake nodes by using opportunistic routing algorithms or be temporarily buffered in en route nodes until a better next-hop node wakes up. In opportunistic routing, the number of hops may increase significantly, which incurs high-energy overheads. Using temporary buffering, the end-to-end latency may increase significantly, e.g., if the next-hop node is not scheduled to wake up for many epochs and the buffering requirements and waking times also increase (Nath and Gibbons 2007).

MAC designs for WSNs mostly elect to reduce energy consumption but at the expense of increased latency, since a sender must wait for the receiver to wake up before it can send data; this is the “sleep delay” due to the receiver being in sleep state (Ye et al. 2004). However, in the proposed sleep scheduling, once the source node is within the transmission radius of the destination node, it simply waits until the destination wakes up and then hops to it directly; or the next-hop node is chosen from currently awake neighbors. Thus, waiting delays are avoided.

• Simplification of synchronization. If the number of nodes in a network is small, it may be possible to wake up all nodes for broadcasting through global synchronization with customized active/sleep schedules. However, for larger-scale
WSNs, synchronization remains an open problem (Wang and Liu 2009). As shown in Fig. 5.15, to synchronize the sleep schedules of neighboring nodes, each node wakes up at the beginning of each epoch, which reduces latency and control overhead. Therefore, EC-CKN is simple and feasible even for large-scale networks.

Two theorems describe the relationship between the latency of greedy geographic routing and the number of awake neighbors $k$; that is, the bounds of expected number of rounds to reach within a specified distance from the destination in TPGFPlus algorithm under EC-CKN-based network. Figure 5.16 shows the two limiting scenarios, in which the destination $X$ is as far away and as close as possible. Nodes are assumed uniformly located and the disk-$r$ communication model is adopted.

Before introducing the theorems, the following notation is used:

- For given $k$ in the EC-CKN algorithm, $E(v_i)$ and $E(v_i)'$ are the subsets of $N(v_i)$ and $N(v_i)'$ having $E_{rank}_{v_j} > E_{rank}_{v_i}$, $v_j \in N(v_i)$.
- $|N(v_i)|$, $|N(v_i)'|$, $|E(v_i)|$ and $|E(v_i)'|$ are the number of elements in $N(v_i)$, $N(v_i)'$, $E(v_i)$ and $E(v_i)'$, respectively.
- Let $m_{v_i} = |E(v_i)| + |E(v_i)'|$ be the total number of $v_i$’s 1-hop and 2-hop neighbor nodes.
- $D$ is the Euclidean distance from source node $S$ to its destination $X$ and $D > r$.
- $E_i(D)$ is the expected rounds needed to reach the destination.
- For TPGFPlus algorithm, the range of possible forwarding progress for two hops is divided into $t \geq 2$ equally spaced segments.

Straightaway, the theorems state:
Theorem 1. Under TPGFPlus algorithm, the expected rounds to reach within $r$ from the destination is at most:

$$D \leq \frac{1}{\frac{r}{D} \sum_{i=0}^{t-1} (i+1) P_i^{(m_i)}} - 2^{m_i}$$  \hspace{1cm} (5.15)

where $q_{2\text{hop}}$ is the probability of the neighbor moving farther from the destination:

$$q_{2\text{hop}} = 2^{-m_i}$$  \hspace{1cm} (5.16)

$P_i^{(m_i)}$ is the probability of the neighbor, among the $m_i$ random 1-hop or 2-hop neighbors of $S$, moving at least $\frac{1-t}{2}$ closer but at most $\frac{i+1}{t} \leq 2* r$, $(i = 1, \ldots, t-2)$ closer to the destination:

$$P_i^{(m_i)} = \prod_{m_i} (1-f_{i+1}) \prod_{m_i} \left(1 - \frac{1-f_i}{1-f_{i+1}}\right)$$  \hspace{1cm} (5.17)

in which:

$$f_i = \frac{2}{\pi} \cos^{-1} \left(\frac{1}{t} \sqrt{1 - \left(\frac{1}{t}\right)^2}\right)$$  \hspace{1cm} (5.18)

$D$ is the Euclidean distance to the destination.

Theorem 2. For the setup in the theorem, the expected rounds to reach within $r$ from the destination is at least:

$$D \geq \frac{1}{\frac{r}{D} \sum_{i=0}^{t-1} (i+1) P_i^{(m_i)}}$$  \hspace{1cm} (5.19)
where

\[ q = \left( \frac{1}{3} + \frac{\sqrt{3}}{2 \pi} \right)^{m_i} \] (5.20)

\[ P_i^{(m_i)} = \prod_{m_i} (1 - f_{i+1}) \left( 1 - \prod_{m_i} \left( \frac{1 - f_i}{1 - f_{i+1}} \right) \right) \] (5.21)

\[ f_i = \frac{1}{\pi} \left( 2 \cos^{-1} \left( 1 - \frac{w_i}{2} \right) + 2 \cos^{-1} \left( \frac{\sqrt{w_i}}{2} \right) - x_i \right) \] (5.22)

where

\[ x_i = \sqrt{w_i} \left( 4 - w_i \right) \] (5.23)

Extensive simulations were run on the new sensor network simulator NetTopo (Chap. 7). The studied WSN was \( 800 \times 600 \text{ m}^2 \), and the number of nodes ranged from 100 to 1000. A source node was positioned at the location \((50, 50)\) and the sink node at the location \((750, 550)\). The transmission radius for each node was initially set to 60 m. Each node is initialized with 500 energy units and has power harvesting capability.

To evaluate the overall performance of the cross-layer optimized routing protocol, TPGFPlus, multiple performance metrics were adopted and evaluated under the three aforementioned forwarding policies. Two test setups were formed, namely, fixed transmission power and adjustable transmission power.

For the fixed transmission power setup, the chosen metrics confirm better TPGFPlus performance:

- Average number of found paths. TPGFPlus finds more transmission paths than TPGF.
- Optimized average hops of found paths. TPGFPlus paths are shorter than those in TPGF in terms of the number of hops.
- Network sleep rate. Compared with TPGF, TPGFPlus allows more nodes to sleep, while achieving the same average number of paths and average path length.

Considering adjustable transmission power setup, each node transmission power is adjustable depending on its current energy level. A node can adjust its transmission power to a discrete value, e.g., 60 m, 70 m, and 80 m. When the current energy of a node is more than the preset value, the node amplifies its transmission power. Thus, it consumes more energy, balances the whole network energy consumption, and gets more neighbor nodes to choose from. In this way, adjustable transmission power affects network connectivity and network sleep rate. For TPGFPlus on
EC-CKN-based WSN with energy harvesting, useful findings were obtained thru comparing the adjustable transmission power setup with the fixed transmission power setup. The comparison metrics are the average number of paths, the optimized average hops of paths, the network sleep rate, and the network average residual energy:

- The average number of paths. The adjustable transmission power setup performs better by finding more transmission paths in higher-density network.
- The optimized average hops of paths. The fixed transmission power setup performs better, as paths have fewer hops, than the adjustable power when the network is sparse. But when the network is dense, the adjustable power setup has better performance, especially under policy 3.
- The network sleep rate. The network sleep rate for adjustable transmission power is much higher than for the fixed transmission power. Thus, a more balanced network can be obtained through increasing the transmission power for nodes that have much more energy. Consequently, nodes with less energy will have more chance to sleep and thus having enough time to recharge.
- The network average residual energy. For the adjustable transmission power, the residual average energy is slightly lower, because enlarging transmission radio incurs more energy consumption. Also, the network average residual energy is more balanced than in the fixed transmission power, with less fluctuation.

Concluding, the proposed TPGFPlus realized several main findings:

- Geographic routing in duty-cycled WSNs should be 2-hop based, not 1-hop based, because in most existing sleep-scheduling algorithms, it is mandatory to gather 2-hop neighborhood information. Simulation results further support this argument.
- Cross-layer optimized routing allows more nodes to sleep while achieving the same desired routing performance.
- The performance of the fixed and adjustable transmission power scenarios were evaluated under three forwarding policies. Routing decisions were taken locally by considering the progress to the destination, the shortest distance toward the destination, the residual energy level of nodes, and the environmental energy harvesting.

### 5.2.2 Single-Layer Integrated Module

Geographic random forwarding (GeRaF, pronounced as “giraffe”) is used to enable nodes to be put to sleep and waken up without coordination and to integrate physical, MAC, and network layers into a single layer (Zorzi and Rao 2003). GeRaF is based on the assumption that sensor nodes have a means to determine their location and that the positions of the final destination and of the transmitting node are explicitly included in each message. In this scheme, a node, which hears a message, is able
based on its position toward the final destination, to assess its own priority in acting as a relay for that message. All nodes that received a message may volunteer to act as relays and do so according to their own priority. This mechanism tries to choose the best positioned nodes as relays. In addition, since the selection of the relays is done a posteriori, neither topological knowledge nor routing tables are needed at each node, but the position information is enough.

An implementation of this approach was in the development of a multimedia cross-layer protocol for underwater acoustic sensor networks; a resource allocation framework is built to accurately model every aspect of the layered network architecture (Pompili and Akyildiz 2010). The proposed cross-layer communication solution can adapt to different application requirements and seek optimality in several different situations. The solution relies on a distributed optimization problem to jointly control the routing, MAC, and physical functionalities in order to achieve efficient communications in the underwater environment. In particular, it combines a 3D geographical routing algorithm (network layer functionality), a novel hybrid distributed CDMA/ALOHA-based scheme to access the bandwidth-limited high delay shared acoustic medium (MAC layer functionality), and an optimized solution for the joint selection of modulation, FEC, and transmit power (physical layer functionalities). The proposed solution is tailored for the characteristics of the underwater acoustic physical channel, e.g., it takes into account the very high propagation delay, which may vary in horizontal and vertical links due to multipath, the different components of the transmission loss, the impairment of the channel, the scarce and range-dependent bandwidth, the high bit error rate, and the limited battery capacity. These characteristics lead to very low utilization efficiencies of the underwater acoustic channel and high-energy consumptions when common MAC and routing protocols are adopted in this environment.

The interaction of key underwater communication functionalities was explored, and the developed cross-layer communication solution allows for the efficient utilization of the bandwidth-limited high delay underwater acoustic channel. It was shown that end-to-end network performance improves in terms of both energy and throughput when highly specialized communication functionalities are integrated in a cross-layer module.

The coming section provides a different implementation of the single-layer integrated module.

5.2.2.1 A Cross-Layer Protocol for Efficient Communication in WSNs (XLP)

A cross-layer protocol (XLP) is proposed to achieve congestion control, routing, and medium access control in a cross-layer fashion (Vuran and Akyildiz 2010). XLP integrates functionalities from all layers, starting from the physical layer up to the transport layer, into a single cross-layer protocol. To realize efficient and reliable communication in WSNs, the design principle of XLP is based on a proposed
cross-layer concept of “initiative determination,” which enables receiver-based contention, initiative-based forwarding, local congestion control, and distributed duty-cycle operation. The “initiative determination” requires simple comparisons against thresholds; thus it is simple to implement, even on computationally impaired devices. XLP was shown to significantly improve the communication performance and outperforms the traditional layered protocol architectures in terms of both network performance and implementation complexity.

The design principle of XLP is a unified cross-layering such that both the information and the functionalities of three fundamental communication paradigms are considered in a single protocol operation while considering the channel effects; explicitly, medium access, routing, and congestion control are the targeted layers. Multiple concepts form the backbone of XLP, namely, initiative determination, transmission initiation, receiver contention, and angle-based routing. Each of these concepts will be clarified in the following items:

• Initiative determination. The initiative determination concept coupled with the receiver-based contention mechanism grants each node the freedom to participate in communication. In WSNs, the major goal of a communication suite is to successfully transport event information by constructing, as possible, multihop paths to the sink. The cross-layer initiative determination concept constitutes the core of the XLP and implicitly incorporates the intrinsic communication functionalities required for successful communication in WSNs. A node $i$ initiates transmission by informing its neighbors that it has a packet to send. This is achieved by broadcasting a request to send (RTS) packet. Upon receiving this packet, each neighbor of node $i$ decides whether to participate in the communication or to abstain. This decision is made through the initiative determination based on the current state of the node. The initiative determination is a binary operation where a node decides to participate in communication if its initiative is 1. Denoting the initiative as $\mathcal{I}$, it is determined as follows:

$$\mathcal{I} = \begin{cases} 
1, & \xi_{\text{RTS}} \geq \xi_{\text{Th}}, \\ 
\lambda_{\text{relay}} \leq \lambda_{\text{Th}}, \\ 
\beta \leq \beta_{\text{max}}, \\ 
E_{\text{rem}} \geq E_{\text{min}}, \\ 
0, & \text{otherwise}
\end{cases}$$

The initiative is set to 1 if all four conditions in Eq. 5.24 are satisfied, where each condition constitutes certain communication functionality in XLP:

– The first condition, $\xi_{\text{RTS}} \geq \xi_{\text{Th}}$, ensures reliable links constructed for communication based on the current channel conditions. For this purpose, for a node to participate in communication, it is required that the received signal to noise...
ratio (SNR) of an RTS packet, $\xi_{RTS}$, be above some threshold $\xi_{Th}$. The effect of this threshold on routing and energy consumption performance is analyzed, and its most efficient value will be chosen as illustrated in Figs. 5.21 and 5.22.

- The conditions $\lambda_{\text{relay}} \leq \lambda_{\text{relay}}^{Th}$ and $\beta \leq \beta^{\text{max}}$ are used for local congestion control in XLP. As will be elaborated later in Eq. 5.25–Eq. 5.31; the condition $\lambda_{\text{relay}} \leq \lambda_{\text{relay}}^{Th}$ prevents congestion by limiting the traffic a node can relay. More specifically, a node participates in the communication if its relay input rate, $\lambda_{\text{relay}}$, is below some threshold $\lambda_{\text{relay}}^{Th}$.

- The condition $\beta \leq \beta^{\text{max}}$ ensures that the buffer occupancy level, $\beta$, of a node, does not exceed a specific threshold, $\beta^{\text{max}}$, so that the node does not experience buffer overflow, thus preventing congestion.

- The last condition, $E_{\text{rem}} \geq E_{\text{rem}}^{\text{min}}$, ensures that the remaining energy, $E_{\text{rem}}$, of a node stays above a minimum value, $E_{\text{rem}}^{\text{min}}$. This constraint helps preserving uniform distribution of energy consumption throughout the network.

The cross-layer functionalities of XLP lie in these constraints that define the initiative of a node to participate in communication.

- Transmission initiation involves a transmitting node and receiving nodes:
  - When a node $i$ has a packet to transmit, it first listens to the channel for a specific period of time. If the channel is occupied, the node performs backoff based on its contention window size, $CW_{RTS}$. When the channel is idle, the node broadcasts an RTS packet, which contains the location information of the sensor node $i$ and the sink. This packet also serves as a link quality indicator that helps the neighbors to perform receiver contention, as will be clarified.
  - When a neighbor of node $i$ receives an RTS packet, it first checks the source and destination locations. The region where the neighbors of a node that are closer to the sink reside is the feasible region, and the remaining neighborhood is in the infeasible region. A node receiving a packet, first checks if it is inside the feasible region. To save energy, nodes inside the infeasible region switch to sleep for the duration of the communication.

The nodes inside the feasible region perform initiative determination as detailed earlier. If a node decides to participate in communication, it performs receiver contention as to be clarified in the following bullet.

- Receiver contention involves several functionalities:
  - The receiver contention operation of XLP leverages the initiative determination concept with the receiver-based routing approach (Akyildiz et al. 2006). After an RTS packet is received, if a node has an initiative to participate in the
communication, i.e., \( J = 1 \), it performs receiver contention to forward the packet. The receiver contention depends on the routing level of each node, which is determined according to the progress a packet would make if the node forwards the packet. The feasible region is divided into \( N_p \) priority regions, i.e., \( A_i, i = 1, \ldots, N_p \). Nodes with longer progress have higher priority over other nodes.

According to the location information, each node determines its priority region and performs contention for medium access. As Fig. 5.17 portrays, each priority region, \( A_i \), corresponds to a backoff window size, \( CW_i \). Depending on its location, a node backs off for \( \sum_{j=1}^{i-1} CW_j + cw_i \), where \( cw_i \) is randomly chosen such that \( cw_i \in [0, CW_{max}] \), where \( CW_{max} = CW_i - CW_{i-1}, \forall i \). The backoff scheme helps to differentiate nodes of different progress into different prioritization groups. Only nodes inside the same group contend with each other. The winner of the contention sends a CTS packet to node \( i \) indicating that it will forward the packet. On the other hand, if during backoff a potential receiver \( k \) receives a CTS packet, it determines that another potential receiver \( j \) with a longer progress has accepted to forward the packet, and node \( k \) switches to sleep for the duration of the communication.

**Fig. 5.17** Prioritization mechanism. (based on (Vuran and Akyildiz, XLP 2010))

Legend:
For \( N_p = 3 \) priority regions, based on its potential advancement, each feasible node corresponds to one of the three priority regions \( A_1, A_2, \) or \( A_3 \). The backoff scheme determines the possible times to send a CTS packet. For instance, if a node in \( A_2 \) satisfies the initiative function, it first waits for \( CW_2 \) in addition to a random \( cw_2 \) value. Consequently, the node in \( A_3 \) can transmit the CTS packet only if no node in \( A_1 \) transmits a CTS packet.

\( D \) is the distance from node \( i \) to the sink
\( D_1 \) and \( D_2 \) are the distances from the farthest end of \( A_1 \) and \( A_2 \), respectively.
When node \( i \) receives a CTS packet from a potential receiver, it determines that the receiver contention has ended and sends a DATA packet with the position of the winner node in the header. The CTS and DATA packets both inform the other contending nodes about the transmitter-receiver pair. Hence, other nodes stop contending and switch to sleep. In the case of two nodes sending CTS packets without hearing each other, the DATA packet sent by node \( i \) can resolve the contention. It may happen that multiple CTS packets from the same priority region can collide and a node from a lower priority region can be selected. XLP does not try to resolve this hitch, as its probability is significantly low since the contention region is already divided into multiple regions and the cost of trying to resolve outweighs the gains.

It is to be noted that node \( i \) may not receive a CTS packet due to any of three reasons:

- CTS packets collide.
- There exists no potential neighbors with \( J = 1 \).
- There exist no nodes in the feasible region.

However, node \( i \) cannot differentiate these three cases by the lack of a CTS packet. Hence, the neighbors of node \( i \) send a keep alive packet after \( \sum_{j=1}^{N_p} CW_j + cw \) if no communication is overheard, where \( cw \) is a random number, such that \( cw \in [0, CW_{max}] \) and \( N_p \) are the number of priority regions. The existence of a keep-alive packet notifies the sender that there are nodes closer to the sink, but the initiative in Eq. 5.24 is not met for any of these nodes. With the reception of this packet, the sender performs retransmission; however, if a keep-alive packet is not received, the node continues retransmission if there is a CTS packet collision. If no response is received after \( m \) retries, node \( i \) determines that a local minimum is reached and switches to angle-based routing mode as described next.

- Angle-based routing. Since the routing decisions depend, partly, on the locations of the receivers, there may be cases where the packets reach local minima; i.e., a node may not find feasible nodes that are closer to the sink than itself. This situation is known as communications void in geographical routing-based approaches and is generally resolved through face routing techniques (Karp and Kung 2000; Leong et al. 2005; Chen and Varshney 2007; Urrutia 2007). Although localized, face routing requires a node to communicate with its neighbors to establish a planarized graph and construct routes to traverse around the void. This entails information exchange between the neighbors of a node. Since such communication increases the protocol overhead, the angle-based routing technique is a stateless solution proposed to face routing.

The main principle of the angle-based routing can be seen in Fig. 5.18. When a packet reaches node \( i \), which is a local minimum toward the sink, the packet has to be routed around the void either in clockwise direction (through node \( j \)) or in counter clockwise direction (through node \( k \)). Lines are drawn between node \( i \) and the sink, \( s \), as well as between node \( i \) and its neighbors. Comparing the
angles between the line $i,s$ and the other lines, the angle $\angle sij$ (angle $\angle sik$) has the smallest angle in the counter clockwise (clockwise) routing direction. Using this geometric property, routes can be constructed around the void. Once a direction is set (clockwise or counter clockwise), the packet traverses around the void along the same direction; hence, for angle-based routing, the term traversal direction indicates this direction\(^1\).

When a node switches to angle-based routing mode, it also sets the traversal direction to clockwise and sends an RTS packet, which indicates both the routing mode and the traversal direction. The nodes that receive this packet calculate their angle relative to the source-sink direction. Denoting the angle by $\theta_{ij}$, node $j$ sets its contention window to $c * \theta_{ij} + cw_i$, where $cw_i$ is a random number, and $c$ is a constant that can be selected according to the latency requirements and the density of the network. The node with the smallest angle, hence, the smallest contention window, sends a CTS packet; then, data communication takes place. This procedure is repeated until the packet reaches a local minimum; in this case, the traversal direction is set to counter clockwise, and the procedure is repeated. Angle-based routing is terminated, and the basic XLP is performed when the packet reaches a node that is closer to the sink than the node that initiated the angle-based routing.

After the illustration of the basic concepts that form the XLP backbone, the new hop-by-hop local cross-layer congestion control component is to be introduced. This component is devised based on the buffer occupancy analysis presented in Eq. 5.25–Eq. 5.33. The objective of this component is to perform hop-by-hop congestion control thru exploiting the local information in the receiver-contention and

\(^1\)Note that clockwise (counter clockwise) traversal direction refers to the traversal direction of the packets rather than the way the angles are measured.
avoiding the need for end-to-end congestion control. It also exploits the local reliability measures taken by the channel access functionality and, consequently, does not necessitate traditional end-to-end reliability mechanisms.

In WSNs, a sensor node has two duties; explicitly, source duty and router duty. Accordingly, there are two sources of traffic as input to each node buffer:

- Generated packets. The first source is the application layer, i.e., the sensing unit of a node, which senses the event and generates the data packets to be transmitted. The rate of the generated packets is denoted by $\lambda_{ii}$.
- Relay packets. In addition to generated packets, as a part of its router duty, a node also receives packets from its neighbors to be forwarded to the sink due to the multihop nature of WSNs. The rate at which node $i$ receives relay packets from node $j$ is denoted as $\lambda_{ji}$.

Since the sensor nodes utilize a duty-cycle operation, their buffer occupancy build up while they sleep because of the generated packets, unless appropriate actions are taken. The local cross-layer congestion control component of XLP has two main measures to regulate congestion. In router duty, by providing the sensor nodes with the freedom of deciding whether or not to participate in the forwarding of the relay packets based on the current load on the node. In source duty, by explicitly controlling the rate of the generated packets.

The upper bound for the total relay packet rate that will prevent congestion is analyzed first. Accordingly, a decision bound is derived for local congestion at each node. More specifically, this bound, denoted by $\lambda_{relay}^{Th}$, is used in the XLP initiative determination as presented in Eq. 5.24.

The overall input packet rate at node $i$, $\lambda_{i}$, can be represented as:

$$\lambda_{i} = \lambda_{ii} + \lambda_{i,relay} = \lambda_{ii} + \sum_{j \in \mathbb{N}_i^n} \lambda_{ji}$$  \hspace{1cm} (5.25)

where

$\lambda_{ii}$ represents the generated packet rate
$\lambda_{ji}$ is the relay packet rate from node $j$ to node $i$
$\mathbb{N}_i^n$ depicts the set of nodes from which node $i$ receives relay packets
$\lambda_{i,relay}$ is the overall relay packet rate of node $i$

Node $i$ aims to transmit all the packets in its buffer, and hence, the overall output rate of node $i$ is given by:

$$\mu_i = (1 + e_i) \cdot (\lambda_{ii} + \lambda_{i,relay})$$ \hspace{1cm} (5.26)

where

$e_i$ is the packet error rate
$1 + e_i$ approximates the retransmission rate since the routes are selected by considering a high SNR value through the initiative determination process
Noticeably, since the node retransmits the packets that are not successfully sent, the output rate is higher than the input rate.

According to Eq. 5.25 and Eq. 5.26, in a long enough interval, $T_\infty$, the average times node $i$ spends in transmitting and receiving are given respectively by:

$$T_{tx} = \lambda_{i,relay} \ast T_\infty \ast T_{PKT}$$  \hfill(5.27)

$$T_{tx} = (1 + e_i) \ast (\lambda_{ii} + \lambda_{i,relay}) \ast T_\infty \ast T_{PKT}$$  \hfill(5.28)

where $T_{PKT}$ is the average duration to transmit a packet to another node including the medium access overhead.

To prevent congestion at a node, the generated and received packets should be transmitted during the time the node is active. Because of the duty-cycle operation, on the average, a node is active $\delta \ast T_\infty$ sec. Therefore:

$$\delta \ast T_\infty \geq \left[(1 + e_i) \ast \lambda_{ii} + (2 + e_i) \ast \lambda_{i,relay}\right] \ast T_\infty \ast T_{PKT}$$  \hfill(5.29)

Consequently, the input relay packet rate, $\lambda_{i,relay}$ is bounded by:

$$\lambda_{i,relay} \leq \lambda_{i,relay}^{Th}$$  \hfill(5.30)

where the relay rate threshold, $\lambda_{i,relay}^{Th}$, is given by:

$$\lambda_{i,relay}^{Th} = \frac{\delta}{(2 + e_i) \ast T_{PKT}} - \frac{1 + e_i}{2 + e_i} \ast \hat{\lambda}_{ii}$$  \hfill(5.31)

The above analysis shows that by throttling the input relay rate, congestion at a node can be prevented. This result is incorporated into XLP through a hop-by-hop congestion control mechanism, where nodes participate in routing packets as long as Eq. 5.30 is satisfied. The implementation of Eq. 5.30 necessitates a node to calculate the parameters $e_i$, $T_{PKT}$ and $\lambda_{ii}$. The generated packet rate, $\lambda_{ii}$, is easily extracted from the rate of injected packets from the sensing boards to the communication module. The packet error rate, $e_i$, is stored as a moving average of the packet loss rate encountered by the node. Similarly, $T_{PKT}$ is determined by using the delay encountered in sending the previous packet by the node. Consequently, each node updates these values after successful or unsuccessful transmission of a packet.

According to Eq. 5.31, the relay rate threshold, $\lambda_{i,relay}^{Th}$, is directly proportional to the duty-cycle parameter, $\delta$, suggesting that the capacity of the network decreases as $\delta$ is reduced. Moreover, Eq. 5.30 ensures that the input relay rate of source nodes, i.e., nodes with $\lambda_{ii} > 0$, is lower than that of the nodes that are only relays, i.e., $\lambda_{ii} = 0$. This provides homogenous distribution of traffic load in the network, where source nodes relay less traffic.

The inequality Eq. 5.30 controls the congestion in the long term. However, in some cases, the buffer of a node can still be full due to short-term changes in the
traffic. To prevent buffer overflow in these cases, nodes use the third inequality in Eq. 5.24 to determine their initiative. More specifically, the inequality $\beta \leq \beta^{\text{max}}$ ensures that the buffer level, $\beta$, is lower than the threshold, $\beta^{\text{max}}$, which is the maximum buffer length of a node. Consequently, a node does not participate in communication, if its buffer is full.

In addition to regulating the relay functionality as discussed above, the XLP local congestion control component also takes an active control measure by directly regulating the amount of traffic generated and injected into the network. During the receiver-contention mechanism described earlier, node $i$ may not receive any CTS packets but receive keep-alive packets; in this case, it decides that there is congestion in the network. Then, it reduces its transmission rate by decreasing the amount of traffic it generates. In other words, since the traffic injected by any node due to its router duty is controlled based on Eq. 5.30, the active congestion control is performed by controlling the rate of generated packets $\lambda_{ii}$ at the node $i$.

In case of congestion, the XLP node reduces the rate of generated packets $\lambda_{ii}$ multiplicatively:

$$\lambda_{ii} = \lambda_{ii} \times \frac{1}{v}$$  \hspace{1cm} (5.32)

where $v$ is defined to be the transmission rate throttle factor.

If there is no congestion, then the packet generation rate can be increased conservatively to prevent oscillation in the local traffic load. Therefore, XLP node increases its generated packet rate linearly for each ACK packet received. Hence:

$$\lambda_{ii} = \lambda_{ii} + \alpha$$  \hspace{1cm} (5.33)

XLP adopts a rather conservative rate control approach, mainly because it has two functionalities to control the congestion for both the source and the router duties of a sensor node. As the node decides to take part in the forwarding based on its buffer occupancy level and relay rate, it already performs congestion control as a part of the XLP forwarding mechanism. Hence, an XLP node does not apply its active congestion control measures, i.e., linear increase and multiplicative decrease, to the overall transmission rate. Instead, only the generated packet rate, $\lambda_{ii}$, is updated.

Since the local congestion control is specific to certain regions and may not apply to the entire event area, nodes inside a congested region may reduce their transmission rates, and the overall event reliability may still be met at the sink from other nodes data due to the sheer amount of correlated data flows (Akan and Akyildiz 2005). Thus, instead of an inefficient end-to-end reliability mechanism, the local cross-layer congestion control exploits the local congestion control and reliability to maintain high network utilization and overall reliability in a distributed manner. In fact, this is also clearly observed in the performance evaluation results portrayed in Figs. 5.20, 5.21, and 5.22.
Fig. 5.19 Average energy consumption versus duty-cycle for different values of $D$ (Vuran and Akyildiz 2010)

Fig. 5.20 Route failure rate for XLP with/without angle-based routing (Vuran and Akyildiz 2010)
Fig. 5.21 Average throughput/goodput versus duty-cycle for different values of SNR threshold. (a) Average throughput, (b) Average Goodput. (Vuran and Akyildiz 2010).
The choice of the duty-cycle value, \( \delta \), is main for XLP performance; consequently, the effect of the duty-cycle on the network energy consumption is clarified in Figs. 5.19, 5.20, 5.21, and 5.22. In this respect, the energy consumed by the network for a packet sent to the sink as a function of the distance of its source to the sink is investigated. In the network model of XLP operation, each node performs a distributed duty-cycle operation such that the transceiver circuit of the node is ON for a certain fraction of the time and is switched OFF for the remaining fraction, where the sensors can still sample data. The ON/OFF periods are managed through a duty-cycle parameter, \( \delta \), which defines the fraction of the time a node is active. More specifically, each node is implemented with a sleep frame of length \( T_s \) sec. A node is active for \( \delta \times T_s \) sec and is asleep state for \( (1 - \delta) \times T_s \) sec.

Note that the start and end times of each node sleep cycle are not synchronized. Consequently, a distributed duty-cycle operation is employed. Furthermore, each node is assumed to be aware of its location through either an onboard GPS or a localization algorithm (Moore et al. 2004). This assumption is motivated by the fact that WSN applications inherently require location information to associate the observed information by each node to a physical location. Thus, it is ordinary to leverage this information for communication. The network model is also geared toward event-based information flow, where nodes send information to a single stationary sink if an event occurs in their vicinity. The area where an event occurs is denoted as the event area and the nodes in this area generate event information.

The total energy consumed from a source node at distance \( D \) from the sink can be found to be:

\[
E_{\text{flow}}(D) = E_{\text{per-hop}} \times E[n_{\text{hop}}(D)]
\]

(5.34)

where

...
$E_{\text{per-hop}}$ is the average energy consumed in one hop for transmitting a packet $E[n_{\text{hop}}(D)]$ is the expected hop count from a source at distance $D$ to the sink. An accurate approximation for the expected hop count is given in (Akyildiz et al. 2006):

$$E\left[n_{\text{hop}}(D)\right] \approx \frac{D - R_{\text{inf}}}{E[d_{\text{next-hop}}]} + 1$$

(5.35)

where

$E[d_{\text{next-hop}}]$ is the expected hop distance

$R_{\text{inf}}$ is the approximated transmission range

The energy consumed in one hop has three components as given by:

$$E_{\text{per-hop}} = E_{\text{TX}} + E_{\text{RX}} + E_{\text{neigh}}$$

(5.36)

where

$E_{\text{TX}}$ is the energy consumed by the node transmitting the packet (Eq. 5.37)

$E_{\text{RX}}$ represents the energy consumed by the node receiving the packet (Eq. 5.41)

$E_{\text{neigh}}$ is the energy consumed by the neighbors of the transmitter and receiver nodes (Eq. 5.42)

To successfully transmit the packet, a pair of nodes needs to accomplish the four-way handshaking. The distance between the pair of nodes is $d_h = E[d_{\text{next-hop}}]$. Moreover, the probabilities to successfully receive a data packet and a control packet at this distance are $p_s^D(d_h)$ and $p_s^C(d_h)$, respectively. The lengths of the RTS, CTS, and ACK packets are assumed to be equal. When a transmitter node sends an RTS packet, it is received by the receiver node with probability $p_s^C(d_h)$, which then replies with a CTS packet. If the CTS packet is received, also with probability $p_s^C(d_h)$, the transmitter node sends a DATA packet, and the communication is completed with an ACK packet. In every failure event, the node begins retransmission. Therefore, the expected energy consumed by the transmitting node is:

$$E_{\text{TX}} = \frac{K}{\left(p_s^C\right)^3 * p_s^D}$$

(5.37)

where
\[ K = E_{\text{sense}} + \left(p_s^C\right)^2 \left[E_{\text{tx}}^R + E_{\text{wait}}^C + E_{\text{rx}}^C\right] \]
\[ + \left(1 - \left(p_s^C\right)^2\right)E_{\text{tx}}^C + \left(p_s^C\right)^3 \left[p_s^D \left[E_{\text{tx}}^D + E_{\text{rx}}^D\right]\right] \]
\[ + \left(p_s^C\right)^2 \left(1 - p_s^C \cdot p_s^D\right)E_{\text{tx}}^A \]

such that

\( E_{\text{sense}} \) is the energy consumption spent sensing the region
\( E_{\text{tx}}^R, E_{\text{tx}}^C, E_{\text{tx}}^D, \) and \( E_{\text{rx}}^C \) are the transmission and reception energies spent for RTS, CTS, DATA and ACK packets, respectively
\( E_{\text{wait}}^{\text{CTS}} \) is the expected energy consumed waiting for a receiver CTS
\( E_{\text{del}} \) is the energy consumed before the transmitter node times out, deciding that a suitable relay node does not exist
\( E_{\text{tx}}^C \) and \( E_{\text{rx}}^C \), in Eq. 5.37, are the only system dependent terms

According to the previous discussion on the receiver contention, on the average, each node in priority region, \( A_i \), waits for \( \frac{C\text{W}_{\text{max}}}{2} \) in its priority slot in addition to waiting for the previous priority slots. Denoting the probability that the next hop, \( \mathcal{N}_i \), for node \( i \) exists in \( A_k \) by \( P_i = P \{ \mathcal{N}_i = j, \text{such that } j \in A_k \} \), the average waiting time for the next hop is:

\[ E_{\text{wait}}^C = e_{\text{rx}} \left[\sum_{i=1}^{N_k} \left[\sum_{k=1}^{i-1} \frac{C\text{W}_k}{2} \right] \right] \cdot P_i \]

where

\[ P_i = \left(1 - p_{[A_i(\gamma_i-1)\mathcal{N}_k]}\right) \cdot p_{[A_i(\gamma_i)\mathcal{N}_k]} \]

\[ p_{[A_i(\gamma_i)\mathcal{N}_k]} = 1 - p_i \]

\( p_i \) is given in (Vuran and Akyildiz 2009)
\( e_{\text{rx}} \) is the energy consumption for receiving
\( \gamma_{ik} \) is maximum distance from the sink for nodes in \( A_i \)

Using the same approach, the energy consumption of the receiver node can be calculated:

\[ E_{\text{rx}} = \frac{1}{\left(p_s^C\right)^3 \cdot p_s^D} \left\{ E_{\text{rx}}^C + E_{\text{wait}}^C + E_{\text{tx}}^C + E_{\text{rx}}^D + E_{\text{rx}}^A \right\} \]
\[
E_{\text{Neigh}} = \frac{1}{(p_s^c)^2} \left\{ \rho \delta \left( \pi R_{\text{inf}}^2 - 2 \right) p_s^c E_{\text{tx}}^R + \left( \rho \delta A(D, R_{\text{inf}}, D) - 2 \right) \left( E_{\text{wait}}^C + E_{\text{tx}}^C + \frac{E_{\text{rx}}^D}{2} \right) \right\} 
\]  
(5.42)

where for the two summed terms in the brackets, the first is the energy consumption for RTS packet reception by the neighbors of the transmitter node residing in the area \( \pi R_{\text{inf}}^2 \); the second term models the remaining neighbors of the receiver node residing in the area \( A(D, R_{\text{inf}}, D) \) while listening only to the CTS message it sends, and \( R_{\text{inf}} \) is the approximated transmission range, \( D \), the distance from a source node to the sink, \( \delta \), the duty-cycle parameter, \( \rho \), the density of a 2-D Poisson distribution of the sensor nodes over the network, \( p_s^c \) and \( p_s^D \) are given in Eq. 5.43 and Eq. 5.44 respectively.

The probabilities of receiving a control or a DATA packet are given respectively by (Zuniga and Krishnamachari 2004):

\[
p_s^C = \left( 1 - \frac{1}{2} e^{-\frac{\xi}{1.28}} \right)^{16l_c} \quad (5.43)
\]

\[
p_s^D = \left( 1 - \frac{1}{2} e^{-\frac{\xi}{1.28}} \right)^{16l_D} \quad (5.44)
\]

where

- Mica2 architecture is assumed with Manchester encoding
- \( \xi \) is the received SNR
- \( l_c \) and \( l_D \) are the control and DATA packet lengths in bits, for \( p_s^C \) and \( p_s^D \), respectively

The total energy consumed from a source node at distance \( D \) from the sink, \( E_{\text{flow}}(D) \), as described in Eq. 5.34, is fully computed from Eq. 5.35 to Eq. 5.44. Using numerical integration methods, the effect of the distance, \( D \), on the energy consumption of a flow is shown in Fig. 5.19. Clearly, the energy consumption of a flow is minimal for duty-cycle parameter \( \delta \approx 0.002 \). However, in relatively small sized networks of less than 1000 nodes, this operating point may not provide network connectivity. On the other hand, the energy consumption has a local minimum around \( \delta \approx 0.2 \).

To gain more insight into the protocol operation, the effects of XLP parameters on the overall network performance are to be investigated. XLP is evaluated on a cross-layer simulator (XLS) developed at the laboratory in C++. XLS consists of a realistic channel model based on (Zuniga and Krishnamachari 2004) and ns-2 and
an event-driven simulation engine. The channel errors, packet collisions, and the energy consumption at the transceiver are accurately modeled based on ns-2 (Chap. 7). Simulation results are obtained for a sensor topology of 300 nodes randomly deployed in a 100×100 m² sensor field. The sink is located at the coordinates (80,80). In each simulation, an event occurs in an event area located at coordinates (20,20) with an event radius of 20 m. Each source node reports its event information to the sink. To investigate the effect of duty-cycle, each simulation is performed for duty-cycle values of $\delta \in [0.1,1]$. Each simulation lasts for 300 s, and the average of 10 trials for each of 10 different random topologies are shown along with their 95% confidence intervals.

To assess XLP, the performance metrics evaluated are the throughput, goodput, energy efficiency, number of hops, and latency:

- **Throughput.** It is defined to be the number of bits per second received at the sink. Only unique packets are considered since multiple copies of a packet can be received at the sink for certain protocols.
- **Goodput.** It is the ratio between the total number of unique packets received at the sink and the total number of packets sent by all the source nodes. As a result, the overall communication reliability is investigated.
- **Energy efficiency.** The most important metric in WSNs. The average energy consumption per unique packet that is received at the sink is considered in this analysis; it is the inverse of energy efficiency. Hence, a lower value refers to a more energy-efficient communication.
- **Number of hops.** It is set to be the number of hops each received packet traverses to reach the sink. This metric is used to evaluate the routing performance of each suite.
- **Latency.** It is the time that passes between the time where a packet is generated at a source node and the time it is received at the sink. This delay accounts for the queuing delay and the contention delay at the nodes, as well as specific protocol operation overhead.

A multiplicity of factors influences XLP operation; these are the angle-based routing, SNR threshold, $\xi_{th}$, and duty-cycle parameter, $\delta$. The effects of these parameters on the XLP performance metrics are laid out:

- **The route failure rate versus the duty-cycle, $\delta$, with and without angle-based routing.** In these experiments, a snapshot of the network is considered, and the routes are found considering this topology. The route failure is the ratio of the number of unsuccessful routes between each node in the network and all possible routes.

The results shown in Fig. 5.20 disclose that route failure rate increases as the duty-cycle parameter $\delta$ is decreased. On the other hand, angle-based routing limits the route failure rate to less than 10% for $\delta \geq 0.3$. This leads to up to 70% drop in failure rate. Note that the failure rate of XLP with angle-based routing also rises as $\delta$ is further decreased since the probability that at any given time the network is partitioned increases.
• The total throughput received at the sink versus the duty-cycle, \( \delta \), for different SNR threshold, \( \xi_{Th} \), values. Figure 5.21a displays the increase in network throughout as the duty-cycle, \( \delta \), increases. Clearly, the step-up in the duty-cycle results in an augmentation in the number of nodes that are active at a given time; consequently, the capacity of the network increases. This is also evident from the buffer occupancy analysis in Eq. 5.25–Eq. 5.31.

The effect of the SNR threshold, \( \xi_{Th} \), is also shown in Fig. 5.21a. The No_\( \xi_{Th} \) curve is the case where the first condition in Eq. 5.24 is not implemented. In other words, nodes contend for participating in routing irrespective of the received SNR value. It can be observed that increasing the SNR threshold, \( \xi_{Th} \), improves the network throughput up to a certain \( \xi_{Th} \); above this value, the network throughput degrades. This shows that a very conservative operation of XLP leads to performance degradation.

• The goodput versus the duty-cycle, \( \delta \), for different SNR threshold, \( \xi_{Th} \), values. As Fig. 5.21b clarifies, XLP provides reliability above 90% for \( \delta \geq 0.2 \) and \( \xi_{Th} \leq 10 \) dB. The lessening in goodput at \( \delta = 0.1 \) is due to the fact that the connectivity of the network cannot be maintained at all times. Moreover, for \( \xi_{Th} = 15 \) dB, the goodput decreases to 0.7 as the duty-cycle is reduced. This is because potential receivers with the desired channel quality cannot be found; hence, the reliability of XLP degrades.

For high duty-cycle \( \delta > 0.7 \), a slight decrease in goodput is observed for \( \xi_{Th} < 15 \) dB. This accounts for the increased contention in the network since higher number of nodes is active for participation in routing at a given time. Contrarily, for \( \xi_{Th} = 15 \) dB, fewer number of nodes are selected for contention in participation; thus, collisions are limited and the goodput is not affected.

• End-to-end latency versus the duty-cycle, \( \delta \), for different SNR threshold, \( \xi_{Th} \), values. In Fig. 5.22, it is obvious that increasing the SNR threshold, \( \xi_{Th} \), improves the end-to-end latency performance up to a certain \( \xi_{Th} \) value. Also, \( \xi_{Th} = 10 \) dB results in the lowest latency. Moreover, there is a suitable operating point for duty-cycle, \( \delta \), considering end-to-end latency (\( \delta \cong 0.6 \)); above this value, the end-to-end delay starts to increase as a result of the increase in receiver-based contention.

Last, throughout this section, it was emphasized that XLP provides the functionalities of medium access, routing, and congestion control. Based on the initiative determination concept, XLP serves as a proof of concept that performs receiver-based contention, initiative-based forwarding, local congestion control, and distributed duty-cycle operation to realize efficient and reliable communication in WSNs. The “initiative determination” concept is the first step in cross-layering that replaces the whole traditional layered WSNs protocol architecture, so that both the information and the functionalities of traditional communication layers are blended in a single module. Analytical performance evaluation and simulation experiment results have shown that XLP improves the communication performance and outperforms
the traditional layered protocol architectures in terms of both network performance and implementation complexity.

### 5.3 Cross-Layer Design for WSNs Security

As this book reveals, a wide range of WSNs applications have been recognized in oceans and wildlife, manufacturing machinery performance, buildings safety, earthquakes monitoring, military arenas, etc. The aspects of WSNs have been under intense research, mainly on energy efficiency, network protocols, and distributed databases. However, relatively few works have been reported on security issues, which are also important, especially in the battlefield applications, premises security and surveillance, and critical systems such as airports, hospitals, etc. A network cannot perform efficiently or may become useless at the worst, with the absence or lack of a security mechanism that protects the privacy and integrity of data. Although different applications may require different security levels, there are four fundamental security requirements, namely (Xiao et al. 2006b):

- **Availability.** The service offered by WSN nodes should be available to their users whenever expected.
- **Authenticity of origin.** The identity of which one interacts with is the expected one.
- **Authentication of data (integrity).** The received data should be authentic and not tampered.
- **Confidentiality (privacy).** The information exchanged should be understood by the intended users only. This is often realized by encrypting the messages with a key that is usually made available by the authentication process.

For a WSN, two additional requirements arise:

- **Survivability.** The ability to provide a minimum level of service in the presence of power loss, failures, or attacks.
- **Leveling of security services.** The possibility of changing security levels as resources availability changes.

The typical characteristics of WSNs, as clarified all over this book, make providing an efficient and scalable security solution remarkably tricky for the following causes (Perrig et al. 2004; Xiao et al. 2006a; Pathan et al. 2006):

- **Vulnerability of channels owing to the shared wireless medium.**
- **Vulnerability of nodes in open network architecture.** Providing open access architecture contributes to help end-users control their content without relying on big Internet companies and to foster innovation by enabling experiments and deployment of innovative functionalities within the network for small players as well.
- **Absence of infrastructure that form its backbone.**
• Changing network topology due to mobility or duty-cycling that puts some nodes on a standby mode. WSN topology may also change due to power depletion or nodes failure.
• Hostile deployment environments. A main motive for WSNs is their deployment in hard to reach or hostile locations.
• Resource limitations, such as limited processing power and small memory size.
• Large number of nodes densely distributed.

Due to their features, WSNs are vulnerable to unique attacks that may not threaten traditional networks. Various kinds of active and passive attacks have been recognized (Xiao et al. 2006b):

• Denial-of-service attack (DoS) for the purpose of exhausting battery power. For instance, a malicious node could prohibit another node from going back to sleep causing the battery to drain.
• Eavesdropping and invasion. This is fairly easy in wireless communication, if no proper security measures are taken. An adversary could easily extract useful information from conversations between nodes. With this information, a malicious user could join the network undetected by impersonating as a trusted node, to access private data, disrupt the normal network operations, or trace the actions of any node in the network.
• Physical node tampering leading to node failure.
• Battery exhaustion on a node.
• Radio jamming at the physical layer.

In light of these attacks, security techniques that consider the characteristics of WSNs are to be devised. Since large numbers of sensor nodes are distributed in a WSN, low cost and low power are becoming the core design challenges. Low cost constrains the resources that can be implemented on the devices, while the low power requires the operations to be done efficiently. Moreover, because of the large-scale and distributed nature of WSNs, the protocols and algorithms must be scalable. A number of solutions have been proposed specifically for securing WSNs (Wood and Stankovic 2002; Perrig et al. 2002; Liu and Ning 2003; Shi and Perrig 2004; Hu et al. 2005; Liu et al. 2005a). Most of the solutions deal with attacks targeting one protocol layer; yet, the layered scheme is inadequate in providing security for WSNs; instead, cross-layer solutions are needed to improve performance.

### 5.3.1 Challenges of Layered Security Approaches

As WSNs pose unique challenges, security techniques used in traditional networks cannot be applied directly for several reasons (Naeem and Loo 2009; Kumar et al. 2014):

• Economically, to make WSNs viable, sensor devices are limited in their energy, computation, and communication capabilities.
Unlike traditional networks, sensor nodes may be deployed in accessible areas, thus increasing the risk of physical attacks.

WSNs interact closely with their physical environments and with people, posing new security problems.

Consequently, existing security mechanisms are inadequate, and new approaches become justifiable. Owing to WSNs resource limitations on computation, storage, and bandwidth, the following aspects should be carefully considered when designing a security scheme (Xiao et al. 2006a):

- Power efficiency. Energy supply is scarce, and hence energy consumption is a primary metric to be considered.
- Nodes density and reliability. WSNs may be intended to scale up to large number of nodes, hence instigating more scalable solutions, contrarily to ad hoc networks. Sensor nodes are prone to failures, while existing security designs can address only a small, fixed threshold number of compromised nodes; the security protection breaks down when such threshold is exceeded (Ye et al. 2005).
- Adaptive security. With numerous combinations of sensing, computing, and communication technology, WSNs are deployable with network densities, ranging from extreme sparse to extreme dense deployments. Moreover, WSNs are intended to interact with environments whose traffic patterns are not human driven; this requires different or at least adaptive security protocols.
- Self-configurability. Like ad hoc networks, WSNs are required to be self-configured. However, factors such as traffic versus energy trade-offs may necessitate innovative solutions; for instance, sensor nodes may have to learn about their geographical position.
- Simplicity. Since sensor nodes are tiny and their energy is limited, the operating and networking software must be kept orders of magnitude simpler as compared to other computing networks.
- Sensor nodes may not have a unique ID like an IP address. This is because the unique ID will generate a significant overhead resulting from the large number of sensors.

To effectively address the above issues, it may be advantageous to break with the conventional layering rules for networking software. The limitations of the layered security approaches are presented in the coming section.

### 5.3.2 Limitations of Layered Security Approaches

To effectively address the challenges emphasized in the previous section and move to the cross-layered designs, the limitations of the layered security approaches are to be laid out and understood (Xiao et al. 2006a):

- Redundant security provisioning. WSNs are subject to a large number of attacks, and each security mechanism consumes some tangible resources, such as...
battery, memory, computation power, and bandwidth. The provision of maximum-security services in each sensor node can lead to unnecessary waste of system resources and can significantly reduce the network lifetime. Without a systematic view, individual security protocols developed for different protocol layers might provide redundant security services and hence consume more WSN resource than needed. An unorganized design of security provisioning while consuming network resources may accidentally launch a DoS attack, denoted as security service DoS (SSDoS) attack. Generally, there may be several protocol layers within the network protocol stack capable of providing security services to the same attack. In such a case, when the original data goes downward through the protocol stack from the highest layer, some part of the data packets may redundantly go through the security-provision operations of different layers.

- Non-adaptive security services. Because attacks on a WSN may come from any protocol layer, a counter attack scheme in a protocol layer is unlikely to guarantee security all the time. Specifically, link layer security typically addresses confidentiality provisioning, two-party authentication, and data freshness, but none of the security problems of the physical layer. However, an insecure physical layer may practically render the entire network insecure; understandably, multi-layer solutions or cross-layer solutions can achieve better performance. Furthermore, self-adaptive security services are flexible in dealing with the dynamic network topology as well as with various types of attacks.

- Power inefficiency. In designing a WSN, energy efficiency is crucial. Several causes of power consumption arise, such as idle listening, retransmissions resulting from collisions, control packets overhead, and unnecessarily high transmission power. Correspondingly, different methods were developed for reducing power consumption. Some approaches limit the transmission power so as to increase the spatial reuse, while maintaining network connectivity (Wattenhofer et al. 2001; Chen et al. 2002; Santi 2005; Wang 2008). At the network layer, power-aware routing protocols result in significant power savings (Aslam et al. 2003; Chang and Tassiulas 2004). At the MAC layer, the wireless transceivers can be turned OFF whenever possible, to reduce the idle listening power as well as the number of collisions (Liu et al. 2005b). Depending on the specific applications, measures can be taken at the application layer to efficiently improve power consumption (Madden et al. 2002, 2003, 2005). In order to reduce power consumption, several key management techniques were tailored for WSNs (Yu and Guan 2008; Zhang and Varadarajan 2010; Bechkit et al. 2013). Progressively, it has been conceived that power efficiency design cannot be addressed completely at any single layer of the WSN protocol stack (Min et al. 2002).
5.3.3 Guidelines for Securing WSNs

Being aware of the challenges and limitations of layered security approaches, four guiding principles arise as worthy of care for securing WSNs (Jones et al. 2003):

- Security of a network is determined by the security over all protocol layers. Specifically, provisioning confidentiality, two-party authentication, and data freshness address security of the link layer. Referring to Fig. 5.23, it is clear that securing the link layer confers the layers above some security; however, it does not address security problems in the physical layer below, most notably jamming. An insecure physical layer may practically render the entire network insecure, even if the layers above are secure. This is especially true in the WSN environment since basic wireless communication is inherently not secure.

- In a massively distributed network, security measures should be amenable to dynamic reconfiguration and decentralized management. Given the nature of WSNs, a security solution must work without prior knowledge of the network configuration after deployment. Also, the security solution should work with minimal or no involvement of a central node to communicate, globally or regionally, shared information.

- In a given network, at any given time, the cost incurred due to the security measures should not exceed the cost assessed due to the security risks at that time. The sensor network is expected to experience different magnitudes of risk at different times, especially considering the, typically, long-lived nature of a network. In principle, security services should adapt to changes in assessed security risk. This entails that a cost model for both security provisioning and risk must be an integral part of the security model.

![Fig. 5.23 Holistic view of cross-layer design. (Fu et al. 2014)](image)

Legend:
A cross-layer design normally targets at least one of the three goals, security, QoS, or mobility.
• If physical security of nodes in a network is not guaranteed, the security measures must be resilient to physical tampering with nodes in the field of operation. For example, a WSN deployed in a battlefield should exhibit graceful degradation if some network nodes are captured.

5.3.4 Trends in Cross-Layer Design for Security

Several works addressed cross-layer security design at different levels of the protocol stack. A cross-layer design approach was introduced for key management in multicast communications in wireless ad hoc networks (Lazos and Poovendran 2004). Following this approach, cryptographic keys to valid group members are distributed in an energy-efficient manner. It was ascertained that a cross-layer design approach for key distribution incorporating network layer (routing) as well as physical layer (energy) parameters leads to energy savings. Moreover, it was disclosed that heuristics are needed to reduce the computational complexity. Further reduction in energy expenditure is achieved by assigning common keys to nodes in order to receive messages from a sender via a common path (Salido et al. 2007). Based on the Hamming distance between codewords, a computationally viable heuristic called VP3 is developed by using codewords to represent paths and to group nodes based on the length of the common path. Simulation results illustrate the improvements achieved by VP3.

Considering the physical and network layer in combination, an optimization problem was formulated to minimize the energy required for rekeying (Eschenauer and Gligor 2002). In this formulation, a sub-optimal cross-layer algorithm that considers the node transmission power (physical layer property) and the multicast routing tree (network layer property) is devised to construct an energy-efficient key distribution scheme (application layer property).

A robust and energy-efficient solution for secure operation of WSNs is proposed (Jones et al. 2003). The approach motivates a new paradigm where security is based on using parameterized frequency hopping and cryptographic keys in a unified framework, to provide differential security services that can be dynamically configured in order to accommodate changing application and network system state in WSNs.

5.3.5 Proposals for Cross-Layer Design for Security

The paradigm is to secure WSNs based on a holistic approach that secures multiple layers in the protocol stack (Fig. 5.23). An important aspect of this paradigm is the exploitation of the interplay between security measures in different layers to provide a security service for the whole network. For security provisioning in WSNs, each protocol layer emphasizes particularly on specific aspects. The physical layer
improves information confidentiality using encoding. The MAC layer and network layer are concerned with the encryption of data frames and routing information. The application layer focuses on management and exchange of keys, which provides security support for encryption and decryption of the lower layers.

When considering the security issues in WSNs, the characteristics of each layer should be under focus, and the cross-layer design should compromise between security and network performance with a focus on reducing as much redundancy as possible. For instance, if the objective is to provide energy-efficient security provisioning, the following measures may be integrated:

- At the physical layer, transmission power can be automatically tuned according to the interference strength, which reduces energy consumption and avoids congestion attacks.
- At the MAC layer, the number of retransmissions can be reduced, thus preventing exhaustion attacks while saving energy.
- At the network layer, multipath routing can be adopted, which avoids the routing “energy hole problem” and reduces the energy consumption due to congestion (Li and Mohapatra 2007) and (Popa et al. 2007).

As discussed throughout, security of WSNs involves all protocol layers. Moreover, at each protocol layer, multiple functional blocks are cross-related to a security solution. Therefore, an effective approach is to develop a cross-layer security scheme individually for each category of security issues, as the following bullets illustrates (Xiao et al. 2006a):

- Cross-layer security for diverse requirements and service types. A WSN may include different types of sensors and perform multiple concurrent applications. Different application scenarios have diverse security requirements. Even within an application, each individual task may have different security concerns. Resource limitations and the specific architecture of WSNs call for customized security mechanisms. An approach is presented to classify the types of data existing in WSNs and to identify possible communication security threats according to that classification (Slijepcevic et al. 2002). A communication security scheme defines a security mechanism for each type of data. By employing this multi-tiered security architecture where each mechanism has different resource requirements, efficient resource management is realized, which is essential for WSNs. A link layer security framework, SecureSense, provides energy-efficient secure communication in WSNs (Xue and Ganz 2003). Using runtime security service composition, the proposed SecureSense enables a sensor node to optimally allo-

---

2 The traffic pattern inherent to WSNs is convergecast, i.e., messages are generated from sensor nodes and are collected by the sink. As a consequence, nodes closer to the sink are more overloaded than others and are subject to premature energy depletion. This issue is known as the funneling effect or the “energy hole problem,” since the neighbors of the sink represent the bottleneck of traffic; it is also called the “crowded center effect.” Mobile elements can help reduce the funneling effect, as they can visit different regions in the network and spread the energy consumption more uniformly, even in the case of a dense WSN architecture.
cate its resources (CPU cycles, memory consumption, and RF messages) to appropriate security services depending on observed external environments, internal constraints, and application requirements. SecureSense service composition varies with respect to both security provision strength (how easy it can be broken) and security concerns (e.g., integrity versus confidentiality). Compared to a stationary security model with maximum security provision, SecureSense can significantly prolong the network lifetime without degrading the security requirements of the applications.

These schemes have considered diverse security concerns for diverse requirements and services. However, they have not taken into account the fact that the diversity of these services or requirements may also be reflected at different protocol layers. Different service types require messages to be encrypted differently. Different encryption schemes also consume different amounts of energy. Security overhead and energy consumption should correspond to the sensitivity of the encrypted information. Security requirements can span different layers jointly, so as to minimize the security-related energy consumption.

- Cross-layer for intrusion detection. Detecting intrusion has been under focus on routing and MAC protocols; however, the existing secure protocols or intrusion detection schemes are proposed for one protocol layer which does not address the security concerns that may arise at other protocol layers. Overall security is hence clearly lacking, thus imposing the necessity to have a security monitoring tool that embodies a cross-layer detection framework which consolidates various schemes in different protocol layers.

Protocols design has the task to consider cross-layer architecture for intrusion detection (Xue and Ganz 2003). Noticeably, some existing solutions for one protocol layer are also falling short; specifically, the general assumption that MAC is for one-hop connectivity may not actually be true in WSNs (Akyildiz et al. 2002). Intrusion at the physical layer has mostly been overlooked; however, this type of attack is serious and may go undetected. Indeed, if a channel is intentionally jammed by malicious users, security detection schemes based on MAC or routing protocols will fail.

- Cross-layer design for power efficiency. It is desirable to consider the energy consumption at each design stage and across protocol layers, so as to achieve the trade-off between energy consumption, network performance, and complexity, and maximize the lifetime of the whole WSN. A cross-layer approach can conserve energy while providing network security provisioning.

At the MAC layer, the carrier detection is liable to DoS attacks. A malicious node can take advantage of the interactions in MAC layer to repeatedly request for channel, thus preventing other nodes from connecting with the target node and exhausting its battery due to frequent responses. From the information collected from other layers, the malicious node can be identified and isolated or restrained. At the network layer, a suitable route may be followed using information from other layers. From the information of the battery usage, a node with more energy left is selected to stand more computational load for security or to relay more traffic. While from the authentication information, the choice is for a route far
from malicious nodes or attacked areas. The geographical location information can help resist attacks such as sinkhole\(^3\) (Shafiei et al. 2014). The safest and most energy-conserving node is the inactive node, i.e., the node in sleeping mode. Various node-sleeping schemes deserve more consideration.

- Cross-layer design for key management. Due to the limited capacity of a sensor node, it is required to save storage space, decrease computational complexity, and reduce communication overhead required for key management. Key management schemes, such as basic random key (Eschenauer and Gligor 2002) and polynomial poll-based key (Deng et al. 2005), are different in complexity, scalability, and effectiveness in resisting cracking. Adaptive key management schemes have to account for information such as security level, congestion, location, and remaining energy, essentially is deriving the overall optimization to extend across multiple protocol layers. Key management schemes based on such optimization embody different interacting components located at multiple layers to really deliver overall optimized performance.

- Cross-layer design for detecting selfish nodes. In a WSN, the connectivity of the network critically relies on the cooperation among nodes. If a node intentionally stops forwarding packets for its neighboring nodes, the network will eventually become out of service; such node is called a selfish node. To avoid this common issue, two techniques are available:
  - Implementing a mechanism in the communication protocols to guarantee that a node has enough interest in forwarding packets to other nodes.
  - Developing a scheme for the communication protocols to detect selfish nodes, then warning or penalizing them when selfishness is detected, and quickly taking them back to the collaboration mode.

Both solutions heavily depend on the cross-layer design methodology, as selfish behavior can emerge at any protocol layer, in particular, MAC and network layers. When cross-layer design is considered, the solution is more effective in avoiding selfish behavior at one particular protocol layer and as well at multiple protocol layers. As an approach, a component may be contained in the network layer of a node to monitor packet forwarding by this node successors, while another component contained in the node MAC layer appends two-hop information such as two-hop acknowledgments to the standard MAC packets and forwards them. Such two-hop information will be used by the upper layer component to detect selfish nodes. When detected, actions can be taken by the component in the MAC layer. Such a scheme can detect a selfish node more quickly, due to the faster actions of a MAC protocol than a networking protocol. This cross-layer architecture also reduces the communication overhead compared with a standard one-layer approach and gives more robustness against selfish behavior.

\(^3\) In sinkhole attack, a malicious node advertises itself as a best possible route to the basestation, which deceives its neighbors to use the route more frequently. Thus, the malicious node has the opportunity to tamper with the data, damage the regular operation, or even conduct further challenges to the security of the network.
Table 5.1 Cross-layer design approaches classified

| Cross-layer design approaches (Sect. 5.2) | Taxonomy |
|----------------------------------------|----------|
| Cross-layering MAC and network layers (Sect. 5.2.1): | Single-layer integrated modules (Sect. 5.2.2): |
| • PANEL (the proposed solution combines the network formation procedure defined at the MAC layer by the IEEE 802.15.4 standard with a topology reconfiguration algorithm operating at the network layer. PANEL is devised to self-configure the IEEE 802.15.4/ZigBee WSN by electing, in a distributed way, a suitable PAN coordinator. A protocol implementing this solution in IEEE 802.15.4 is also provided. Performance results show that the proposed cross-layer approach minimizes the average number of hops between the nodes of the network and the PAN coordinator allowing to reduce the data transfer delay and determining significant energy savings compared with the performance of the IEEE 802.15.4 standard) | • XLP (it achieves congestion control, routing, and medium access control in a cross-layer fashion. The design principle is based on the cross-layer concept of “initiative determination”, which enables receiver-based contention, initiative-based forwarding, local congestion control, and distributed duty-cycle operation to realize efficient and reliable communication in WSNs. The initiative determination requires simple comparisons against thresholds and thus is very simple to implement, even on computationally impaired devices. XLP is the first protocol that integrates functionalities of all layers from physical to transport into a cross-layer protocol. A cross-layer analytical framework is developed to investigate the performance. XLP significantly improves the communication performance and outperforms the traditional layered protocol architectures in terms of both network performance and implementation complexity) |
| • CLB (it is a simple cross-layer routing protocol that enhances the WSN lifetime by balancing the energy consumption in the forwarding task. To do so, the MAC layer informs the network layer about all the overheard communications of the neighboring nodes. According to this information and in order to balance the energy consumption of the forwarding nodes, a node chooses its next hop among the less-used ones. Hence, the choice of the next hop is not probabilistic and leads to better energy consumption balancing. The obtained results have shown that CLB uses all forwarding nodes in an equitable manner; this enables to avoid the network partitioning and to enhance the network lifetime) | |

5 Cross-Layer Protocols for WSNs
Cross-layer design approaches (Sect. 5.2)

- Cross-layering physical and MAC and network layers (Sect. 5.2.1.2):
  - TPGFPlus (to optimize the system as a whole, this algorithm is designed on the basis of multiple layers interactions, taking into account the following. At the physical layer, sensor nodes are developed to scavenge energy from the environment, i.e., node rechargeable operation. Each node can adjust its transmission power depending on its current energy level (the main object for nodes with energy harvesting is to avoid the routing hole when implementing the routing algorithm). At the MAC layer, where an energy balanced sleep scheduling scheme, duty-cycle, and energy consumption-based connected $k$-neighborhood are applied to allow sensor nodes to have enough time to recharge energy, which takes nodes current energy level as the parameter to dynamically schedule nodes to be active or asleep. At the network layer, a forwarding node chooses the next-hop node based on 2-hop neighbor information rather than 1-hop. Performance of TPGFPlus was evaluated under three forwarding policies. Simulations show that by cross-layer optimization, shorter paths are found, resulting in shorter average path length, without causing much energy consumption. On top of these, a considerable increase of the network sleep rate is achieved)
5.4 Conclusion for Reality

A book is a whole life full of emotions, visions, and feelings. This chapter lived the eruption of the coronavirus. An outbreak of respiratory disease caused by the new coronavirus was first detected in China and has spread in more than 213 countries. The virus has been named “SARS-CoV-2,” and the disease it causes has been named “coronavirus disease 2019” (COVID-19). On January 30, 2020, the World Health Organization (WHO) declared the outbreak a public health emergency of international concern (PHEIC). Early on, many of the patients at the epicenter of the outbreak in Wuhan, Hubei Province, China, had some link to a large seafood and live animal market, suggesting animal-to-person spread. Later, a growing number of patients reportedly did not have exposure to animal markets, indicating person-to-person spread. Person-to-person spread was subsequently reported outside Hubei and in countries outside China. On Wednesday, March 11, 2020, the coronavirus outbreak has been labeled a pandemic by the WHO chief. A pandemic is defined as a disease that can infect and sicken humans, can transmit easily from one human to another, and has spread worldwide. Pandemics occur when a new form of virus emerges (either a mutated version or a combination with another variation) and is capable of transmitting from person to person. As of submitting the book manuscript in November 14th, 2020, the world has seen a total of 53,796,100 confirmed cases, 37,555,673 recoveries, and 1,310,250 deaths (worldometer 2020). The economic fallout was dangerous; there have been widespread supply shortages of pharmaceuticals and manufactured goods due to factory disruption in China. The technology industry, in particular, has been hit by delaying shipments of electronic goods. A worldwide rolling recession resulted as the disease spread to different areas. The economic impacts of quarantines and travel restrictions were severe. Schools, universities, theaters, and stadiums were shut. Tokyo 2020 summer Olympics that were due from July 21 to August 9 were postponed for 1 year, marking the first time that an entire Olympics has ever been postponed, since 1896, the start of the modern Olympics in Athens.

Back to cross-layering, WSNs differ from other wireless networks in several ways:

• They consist of physically small network nodes, which perform sensing, processing, and then radio communications.
• Each node is configured the same peer-to-peer networking protocol, thereby allowing a group of sensor nodes to form a self-configuring network.
• The sensor nodes are energy constrained since they are designed to operate in specific areas for years with no maintenance.

Depending on the specific application for which they are used, WSNs can be further divided into event-driven sensor networks or continuous monitoring sensor networks:
• On event-driven sensor networks, the nodes remain in the sleep mode until some event occurs, as in the case of a sensor network devised for sensing forest fires. However, the main problem with this type of networks is being able to switch nodes from a sleeping mode to a listening mode in a defined time.

• On continuous monitoring sensor networks, data are continuously transmitted from source nodes to sink nodes.

One of the main and foremost problems faced by WSNs is that they are energy constrained, due to the fact that WSNs consist of sensor nodes which are battery operated; therefore it is impossible to recharge them, as they are intended to operate in specific areas for years with no maintenance. Hence, it is important to devise ways by which the energy efficiency of these sensor nodes can be increased so that the overall lifetime of the network is also improved. Cross-layer techniques can achieve the goal of maximizing the energy efficiency in WSNs.

Cross-layer design is a new concept, which has been devised for protocols of wireless networks such as ad hoc networks and sensor networks. Significant number of papers has proposed the use of cross-layer techniques in WSNs in order to achieve different objectives. Furthermore, it has been proved that cross-layer techniques help to improve energy conservation in WSNs.

With cross-layer techniques, the different layers of the conventional Open System Interconnection (OSI) model interact with each other, irrespective of their positions in the model, to achieve a specific result. The traditional OSI layer architecture is modular in nature and has been implemented successfully in the case of wired networks. In the case of WSNs, which have many constraints in terms of processing, memory, and energy, it becomes difficult to apply only the traditional protocol structure. Cross-layer designs have emerged as an effective approach and have been applied to WSNs. Constraints on energy, memory, storage resources, and low radio transmission capabilities of the wireless sensor nodes make cross-layer support more attractive.

Architecture is important for proliferation of technology, and at a time when wireless networking may be on the verge of a takeoff, its importance needs to be kept in mind. In venturing into the space of cross-layer design, it may, however, be useful to note some adverse possibilities and exercise appropriate attention (Kawadia and Kumar 2005):

• Unbridled cross-layer design can lead to a spaghetti design and stifle further innovations since the number of new interactions introduced can be large.

• Such design can suppress proliferation since every update may require complete redesign and replacement.

• Cross-layer design creates interactions, some intended, and others unintended. Dependency relations may need to be examined, and timescale separation may need to be enforced. The consequences of all such interactions need to be well understood, and theorems establishing stability may be needed.
Proposers of cross-layer design must therefore consider the totality of the design, including the interactions with other layers, and also what other potential suggestions might be barred because they would interact with the particular proposal being made. They must also consider the long-term architectural value of the suggestion. Cross-layer design proposals must therefore be holistic rather than fragmenting.

Not to be overlooked, cross-layer designs are expected to be the suitable solution to closely examine the trade-off between added security, vulnerability, and network performance. Several interesting issues and open questions arise. To name a few, how to trade off the security level and system performance with minimal power computation? How will be the cross-layer interactions for detecting attacks and providing intrusion tolerance and graceful degradation designs for sake of network survivability? How to tolerate the lack of physical security, through redundancy or knowledge about the physical environment?

Cross-layering is a WSN specificity, it deserves more attention, further exploration.

5.5 Exercises

1. Search the literature for more protocols that can be categorized based on Sect. 5.2.1.
2. Explore for more protocols that can be categorized based on Sect. 5.2.2.
3. Write a technical report on the heuristic approach hinted in Sect. 5.1.
4. Section 5.3 elaborates on the cross-layer design for security. Write your own report on this topic.

References

Abagnale, A., Cipollone, E., & F. Cuomo. (2008). Constraining the network topology in IEEE 802.15.4. Vol. 265, in Advances in ad hoc networking: The 7th IFIP annual mediterranean ad hoc networking workshop, by P. Cuenca, C. Guerrero, R. Puigjaner, & B. Serra, 167–178. Boston: Springer.
Akan, O., & Akyildiz, I. (2005). Event-to-sink reliable transport in wireless sensor networks. Transactions on Networking (IEEE/ACM), 13(5), 1003–1016.
Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002, August). A survey on sensor networks. Communications Magazine (IEEE), 40(8), 102–114.
Akyildiz, I. F., Vuran, M. C., & Akan, O. B. (2006). A cross-layer protocol for wireless sensor networks. In 40th annual conference on information sciences and systems (pp. 1102–1107). Princeton: IEEE.
Aslam, J., Li, Q., & Rus, D. (2003, March). Three power-aware routing algorithms for sensor networks. Wireless Networks and Mobile Computing (John Wiley & Sons, Inc.), 3(2), 187–208.
References

Bai, Y., Liu, S., Sha, M., Lu, Y., & Xu, C. (2008, November). An energy optimization protocol based on cross-layer for wireless sensor networks. *Journal of Communications* (Academy Publisher), 3(6), 27–34.

Baronti, P., Pillai, P., Chook, V., Chessa, S., Gotta, A., & Hu, Y. (2007). Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards. *Computer Communications* (Elsevier B.V.), 30(7), 1655–1695.

Bechkit, W., Challal, Y., Bouabdallah, A., & Tarokh, V. (2013). A highly scalable key predistribution scheme for wireless sensor networks. *Transactions on Wireless Communications* (IEEE), 12(2), 948–959.

Bouabdallah, F., Bouabdallah, N., & Boutaba, R. (2009). On balancing energy consumption in wireless sensor networks. *Transactions on Vehicular Technology* (IEEE), 58(6), 2909–2924.

Cardei, M., & Du, D.-Z. (2005, May). Improving wireless sensor network lifetime through power aware organization. *Wireless Networks* (Springer Nature), 11, 333–340.

Casari, P., Nati, M., Petrioli, C., & Zorzi, M. (2006). ALBA: An adaptive load-balanced algorithm for geographic forwarding in wireless sensor networks. In *The conference on Military Communications (MILCOM)* (pp. 1–9). Washington, DC: IEEE.

Chang, J.-H., & Tassiulas, L. (2004, August). Maximum lifetime routing in wireless sensor networks. *Transactions on Networking* (IEEE/ACM), 12(4), 609–619.

Chen, B., Jamieson, K., Balakrishnan, H., & Morris, R. (2002, September). Span: An energy-efficient coordination algorithm for topology maintenance in Ad Hoc wireless networks. *Wireless Networks* (Kluwer Academic Publishers), 8(5), 481–494.

Chiang, M. (2005, January). Balancing transport and physical layers in wireless multihop networks: Jointly optimal congestion control and power control. *Journal on Selected Areas in Communications* (IEEE), 23(1), 104–116.

Chilamkurti, N., Zeadally, S., Vasilakos, A., & Sharma, V. (2009, April). Cross-layer support for energy efficient routing in wireless sensor networks. *Journal of Sensors* (Hindawi), 2009, 1–9.

Cipollone, E., Cuomo, F., Luna, S. D., Monaco, U., & Vacirca, F. (2007). Topology characterization and performance analysis of IEEE 802.15.4 multi-sink wireless sensor networks. In *The 6th annual mediterranean ad hoc networking workshop* (pp. 196–203). Corfu: Ionian University.

Crossbow. (2002January 1). MICA2. . http://www.eol.ucar.edu/isf/facilities/isa/internal/CrossBow/DataSheets/mica2.pdf. Accessed 3 Feb 2014.

Cuomo, F., Luna, S. D., Monaco, U., & Melodia, T. (2007). Routing in ZigBee: benefits from exploiting the IEEE 802.15.4 association tree. In *International Conference on Communications (ICC)* (pp. 3271–3276). Glasgow: IEEE.

Dobson, S. A., et al. (2006, December). A survey of autonomic communications. *Transactions on Autonomous and Adaptive Systems* (ACM), 1(2), 223–259.

Eschenauer, L., & Gligor, V. D. (2002). A key-management scheme for distributed sensor networks. In *The 9th conference on Computer and Communications Security (CCS)* (pp. 41–47). Washington, DC: ACM.
Fu, B., Xiao, Y., Deng, H., & Zeng, H. (2014). A survey of cross-layer designs in wireless networks. *Communications Surveys & Tutorials (IEEE)*, 16(1), 110–126.

Gu, Y., Hwang, G., He, T., & Du, D. (2007). uSense: A unified asymmetric sensing coverage architecture for wireless sensor networks. In *The 27th International Conference on Distributed Computing Systems (ICDCS)*. IEEE: Toronto.

Haapola, J., Shelby, Z., Pomalaza-Ráez, C., & Mähönen, P. (2005). Cross-layer energy analysis of multi-hop wireless sensor networks. In *The 2nd international conference on Embedded Wireless Systems and Networks (EWSN)* (pp. 33–44). Istanbul: ACM/SIGBED.

Han, G., Dong, Y., Guo, H., Shu, L., & Wu, D. (2015, November). Cross-layer optimized routing in wireless sensor networks with duty cycle and energy harvesting. *Wireless Communications and Mobile Computing* (John Wiley & Sons, Inc.), 15(16), 1957–1981.

Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D., & Pister, K. (2000). System architecture directions for networked sensors. In *The 9th international conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS IX)* (pp. 93–104). Cambridge, MA: ACM.

Holland, M., Wang, T., Tavli, B., Seyedi, A., & Heinzelman, W. (2011, February). Optimizing physical layer parameters for wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)* (ACM), 7(4), 28:1–28:20.

Hu, Y., Perrig, A., & Johnson, D. B. (2005). Ariadne: A secure on-demand routing protocol for ad hoc networks. *Wireless Networks* (Springer Nature), 11, 21–38.

Jones, K. H., Wadaa, A. H., Olariu, S., Wilson, L. T., & Eltoweissy, M. Y. (2003). Towards a new paradigm for securing wireless sensor networks. In *The workshop on New Security Paradigms (NSPW)* (pp. 115–121). Ascona: ACM.

Karp, B., & Kung, H. T. (2000). GPSR: Greedy perimeter stateless routing for wireless networks. In *The 6th annual international conference on Mobile Computing and Networking (MobiCom)* (pp. 243–254). Boston: ACM SIGMOBILE.

Kawadia, V., & Kumar, P. R. (2005, February). A cautionary perspective on cross-layer design. *Wireless Communications* (IEEE), 12, 3–11.

Kim, W. S., Kim, I. W., Hong, S. E., & Kang, C. G. (2003, August). A Seamless Coordinator Switching (SCS) scheme for wireless personal area network. *Transactions on Consumer Electronics* (IEEE), 49(3), 554–560.

Kim, J., Lee, J., & Kim, S. (2009). An enhanced cross-layer protocol for energy efficiency in wireless sensor networks. In *The 3rd international conference on Sensor Technologies and Applications* (pp. 657–664). Glyfada: IEEE.

Kumar, V., Jain, A., & Barwal, P. N. (2014). Wireless sensor networks: Security issues, challenges and solutions. *International Journal of Information & Computation Technology* (International Research Publications House), 4(8), 859–868.

Lachennmann, A., Marrón, P. J., Minder, D., & Rothermel, K. (2005). An analysis of cross-layer interactions in sensor network applications. In *International conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)* (pp. 121–126). Melbourne: IEEE.

LAN/MAN Standards Committee. (2006). Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs). Computer Society, Washington, DC: IEEE.

Lazos, L., & Poovendran, R. (2004). Cross-Layer Design for Energy-Efficient Secure Multicast Communications in Ad Hoc Networks. In *International Conference on Communications (ICC)* (pp. 3633–3639). Paris, France: IEEE.

Leong, B., Mitra, S., & Liskov, B. (2005). Path vector face routing: Geographic routing with local face information. In *The 13th international conference on Network Protocols (ICNP)* (pp. 147–158). Boston: IEEE.
Li, J., & Mohapatra, P. (2007, June). Analytical modeling and mitigation techniques for the energy hole problem in sensor networks. *Pervasive and Mobile Computing* (Elsevier B.V.), 3(3), 233–254.

Liu, D., & Ning, P. (2003). Location-based pairwise key establishments for Static Sensor Networks (SASN). In *The 1st workshop on Security of Ad Hoc and Sensor Networks* (pp. 72–82). Fairfax: ACM.

Liu, J., Zhao, F., Cheung, P., & Guibas, L. (2004, December). Apply geometric duality to energy-efficient non-local phenomenon awareness using sensor networks. *Wireless Communications* (IEEE), 11(6).

Liu, D., Ning, P., & Li, R. (2005a, February). Establishing pairwise keys in distributed sensor networks. *Transactions on Information and System Security* (ACM), 8(1), 52–61.

Liu, Y., Elhanany, I., & Qi, H. (2005b). An Energy-Efficient QoS-Aware Media Access Control Protocol for Wireless Sensor Networks. In *The International Conference on Mobile Adhoc and Sensor Systems (MASS)* (pp. 189–191). Washington, DC: IEEE.

Liu, S., Bai, Y., Sha, M., Deng, Q., & Qian, D. (2008). CLEEP: A Novel Cross-Layer Energy-Efficient Protocol for Wireless Sensor Networks. In *The 4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCom)* (pp. 1–4). Dalian, China: IEEE.

Lo Bello, L., & Toscano, E. (2009, May). Coexistence issues of multiple co-located IEEE 802.15.4/ ZigBee networks running on adjacent radio channels in industrial environments. *Transactions on industrial informatics* (IEEE), 5(2), 157–167.

Madan, R., Cui, S., Lall, S., & Goldsmith, A. (2006, November). Cross-layer design for lifetime maximization in interference-limited wireless sensor networks. *Transactions on Wireless Communications* (IEEE), 5(11), 725–729.

Madden, S., Franklin, M. J., Hellerstein, J. M., & Hong, W. (2002, Winter). Tag: A tiny aggregation service for ad hoc sensor networks. *Operating Systems Review, 36*, 131–146.

Madden, S., Franklin, M. J., Hellerstein, J. M., & Hong, W. (2003). The design of an acquisitional query processor for sensor networks. In *The international conference on Management of Data (SIGMOD)* (pp. 491–502). San Diego: ACM SIGMOD.

Madden, S. R., Franklin, M. J., Hellerstein, J. M., & Hong, W. (2005). TinyDB: An acquisitional query processing system for sensor networks. *Transactions on Database Systems (TODS)* (ACM), 30(1), 122–173.

Melodia, T., Vuran, M. C., & Pompili, D. (2005). The state of the art in cross-layer design for wireless sensor networks. Vol. 3883, in Lecture notes in computer science-wireless systems and network architectures in Next Generation Internet (EuroNGI), by M. Cesana & L. Fratta, 78–92. Berlin/Heidelberg: Springer.

Min, R., Bhardwaj, M., Ickes, N., Wang, A., & Chandrakasan, A. (2002). Microsensors, the hardware and the network: Total-system strategies for power aware wireless. In *CAS workshop on wireless communications and networking*. IEEE: Pasadena.

Moore, D. C., Leonard, J. J., Rus, D. L., & Teller, S. J. (2004). Robust distributed network localization with noisy range measurements. In *The 2nd international conference on Embedded Networked Sensor Systems (SenSys)* (pp. 50–61). Baltimore: ACM.

Naeem, T., & Loo, K. K. (2009, March). Common security issues and challenges in wireless sensor networks and IEEE 802.11 wireless mesh networks. *International Journal of Digital Content Technology and its Applications (JDCTA)* (Advanced Institute of Convergence IT), 3(1), 88–93.

Nath, S. K., & Gibbons, P. B. (2007). Communicating via fireflies: Geographic routing on duty-cycled sensors. In *The 6th international conference on Information Processing in Sensor Networks (IPSN)* (pp. 440–449). Cambridge, MA: ACM.

Pathan, A. S. K., Lee, H.-W., & Hong, C. S. (2006). Security in wireless sensor networks: Issues and challenges. In *The 8th International Conference Advanced Communication Technology (ICACT)* (pp. 1043–1048). Phoenix Park, IEEE.
Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002, September). SPINS: Security protocols for sensor networks. Wireless Networks (Springer Nature), 8, 521–534.
Perrig, A., Stankovic, J., & Wagner, D. (2004, June). Security in wireless sensor networks. Communications (ACM), 47(6), 53–57.
Petrioli, C., Nati, M., Casari, P., Zorzi, M., & Basagni, S. (2014, March). ALBA-R: Load-balancing geographic routing around connectivity holes in wireless sensor networks. Transactions on Parallel and Distributed Systems (IEEE), 25(3), 529–539.
Pichler, M., Schwarzer, S., Stelzer, A., & Vossiek, M. (2009, October). Multi-channel distance measurement with IEEE 802.15.4 (ZigBee) devices. Journal of Selected Topics in Signal Processing (IEEE), 3(5), 845–859.
Pomplili, D., & Akyildiz, I. F. (2010, September). A multimedia cross-layer protocol for underwater acoustic sensor networks. Transactions on Wireless Communications (IEEE), 9(9), 2924–2933.
Pomplili, D., Vuran, M. C., & Melodia, T. (2006). Cross-layer design in wireless sensor networks. In M. P. Mahalik (Ed.), Sensor network and configuration: fundamentals, techniques, platforms, and experiments. Berlin/Heidelberg: Springer.
Popa, L., Rostamizadeh, A., Karp, R., Papadimitriou, C., & Stoica, I. (2007). Balancing traffic load in wireless networks with curveball routing. In The 8th international symposium on Mobile Ad Hoc Networking and Computing (MobiHoc) (pp. 170–179). Quebec: ACM.
Puccinelli, D., Sifakis, E., & Haenggi, M. (2006). A cross-layer approach to energy balancing in wireless sensor networks. Vol. 331, in Lecture notes in control and information: Networked embedded sensing and control, by P. Tabuada, 309–324. Berlin/Heidelberg: Springer
Salido, J., Lazos, L., & Poovendran, R. (2007, December). Energy and bandwidth-efficient key distribution in wireless ad hoc networks: A cross-layer approach. Transactions on Networking (IEEE/ACM), 15(6), 1527–1540.
Santi, P. (2005, June). Topology control in wireless ad hoc and sensor networks. Computing Surveys (CSUR) (ACM), 37(2), 164–194.
Seada, K., Zúñiga, M. A., Helmy, A., & Krishnamachari, B. (2004). Energy-efficient forwarding strategies for geographic routing in lossy wireless sensor networks. In The 2nd international conference on Embedded Networked Sensor Systems (SenSys) (pp. 108–121). Baltimore: ACM.
Semchedine, F., Bouallouche-Medjkoune, L., Bennacer, L., Aber, N., & Aïssani, D. (2012). Routing protocol based on tabu search for wireless sensor networks. Wireless Personal Communications (Springer Nature), 67, 105–112.
Shafiei, H., Khonsariab, A., Derakhshia, H., & Mousavia, P. (2014, May). Detection and mitigation of sinkhole attacks in wireless sensor networks. Journal of Computer and System Sciences (Elsevier B.V.), 80(3), 644–653.
Shah, R. C., & Rabaei, J. M. (2002). Energy aware routing for low energy ad hoc sensor networks. In Wireless Communications and Networking Conference (WCNC) (pp. 350–355). Orlando: IEEE.
Shi, E., & Perrig, A. (2004, December). Designing secure sensor networks. Wireless Communications (IEEE), 11(6), 38–43.
Shu, L., Zhang, Y., Yang, L. T., Wang, Y., Hauswirth, M., & Xiong, N. (2010, June). TPGF: Geographic routing in wireless multimedia sensor networks. Telecommunication Systems (Springer Nature Switzerland, AG), 44, 79–95.
Slijepcevic, S., Potkonjak, M., Tsiatsis, V., Zimbeck, S., & Srivastava, M. B. (2002). On communication security in wireless ad-hoc sensor networks. In The 11th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE) (pp. 139–144). Los Alamitos: IEEE.
Song, L., & Hatzinakos, D. (2007, February). A cross-layer architecture of wireless sensor networks for target tracking. Transactions on Networking (IEEE/ACM), 15(1), 145–158.
References

Srivastava, V., & Motani, M. (2005, December). Cross-layer design: A survey and the road ahead. *Communications Magazine (IEEE)*, 43(12), 112–119.

Suh, C., Ko, Y.-B., & Son, D.-M.. (2006). An energy efficient cross-layer mac protocol for wireless sensor networks. Vol. 3842, in Lecture notes in computer science-advanced web and network technologies, and applications (APWeb), by H.T. Shen, J. Li, M. Li, J. Ni, & W. Wang, 410–419. Berlin/Heidelberg: Springer.

Sulaiman, T. H., Sivarajah, K., Al-Raweshidy, H. S. (2007, December). Improved PNC selection criteria and process for IEEE802.15.3. *Communications Magazine (IEEE)*, 45(12), 102–109.

Urrutia, J. (2007, September). Local Solutions for Global Problems in Wireless Networks. *Journal of Discrete Algorithms* (Elsevier B.V.), 5(3), 395–407.

van Dam, T., & Langendoen, K. (2003). An adaptive energy-efficient MAC protocol for wireless sensor networks. In *The 1st international conference on Embedded Networked Sensor Systems (SenSys)* (pp. 171–180). Los Angeles: ACM.

van der Schaar, M., & Shankar, N. S. (2005, August). Cross-layer wireless multimedia transmission: Challenges, principles, and new paradigms. *Wireless Communications (IEEE)*, 12(4), 50–58.

van Hoesel, L., Nieberg, T., Wu, J., & Havinga, P. J. M. (2004, December). Prolonging the lifetime of wireless sensor networks by cross-layer interaction. *Wireless Communications (IEEE)*, 11(6), 78–86.

Venkitasubramaniam, P., Adireddy, S., & Tong, L. (2003). Opportunistic ALOHA and cross layer design for sensor networks. In *Military Communications Conference (MILCOM)* (pp. 705–710). Boston: IEEE.

Vuran, M. C., & Akyildiz, I. F. (2006, April). Spatial correlation-based collaborative medium access control in wireless sensor networks. *Transactions on Networking (IEEE/ACM)*, 14(2), 316–329.

Vuran, M. C., & Akyildiz, I. F. (2009, August). Error control in wireless sensor networks: A cross layer analysis. *Transactions on Networking (IEEE/ACM)*, 17(4), 1186–1199.

Vuran, M. C., & Akyildiz, I. F. (2010, November). XLP: A cross-layer protocol for efficient communication in wireless sensor networks. *Transactions on Mobile Computing (IEEE)*, 9(11), 1578–1591.

Wang, Y. (2008). Topology control for wireless sensor networks. In Y. Li, M. T. Thai, & W. Wu (Eds.), *Wireless sensor networks and applications. Signals and communication technology* (pp. 113–147). Boston: Springer.

Wang, F., & Liu, J. (2009). Duty-cycle-aware broadcast in wireless sensor networks. In *The 28th international conference on Computer Communications (INFOCOM)* (pp. 468–476). Rio de Janeiro: IEEE.

Wang, X., Xing, G., Zhang, Y., Lu, C., Pless, R. B., & Gill, C. (2003). Integrated coverage and connectivity configuration in wireless sensor networks. In *The 1st international conference on Embedded Networked Sensor Systems (SenSys)* (pp. 28–39). Los Angeles: ACM.

Wattenhofer, R., Li, L., Bahl, P., & Wang, Y.-M. (2001). Distributed topology control for power efficient operation in multihop wireless ad hoc networks. In *The conference on computer communications – The 20th annual joint conference of the IEEE Computer and Communications Societies (INFOCOMM)* (pp. 1388–1397). Anchorage, IEEE.

Wood, A. D., & Stankovic, J. A. (2002, October). Denial of service in sensor networks. *Computer (IEEE)*, 35(10), 54–62.

Worldometer. (2020January 1). *COVID-19 Coronavirus Pandemic*. https://www.worldometers.info/coronavirus/? Accessed 8 July 2020.

Xiao, M., Wang, X., & Yang, G. (2006a). Cross-layer design for the security of wireless sensor networks. In *The 6th world congress on intelligent control and automation* (pp. 104–108). Dalian: IEEE.
Cross-Layer Protocols for WSNs

Xiao, M., Wang, X., & Yang, G. (2006b). Cross-layer design for WSNs security. In Y. Xiao (Ed.), Security in sensor networks (pp. 311–328). Boca Raton: CRC Press.

Xie, P., & Cui, J.-H. (2007). R-MAC: An energy-efficient MAC protocol for underwater sensor networks. In The 2nd international conference on Wireless Algorithms, Systems and Applications (WASA) (pp. 187–198). Chicago: IEEE.

Xue, Q., & Ganz, A. (2003). Runtime security composition for sensor networks (SecureSense). In The 58th Vehicular Technology Conference (VTC) (pp. 2976–2980). Orlando, FL: IEEE.

Yan, T., He, T., & Stankovic, J. A. (2003). Differentiated surveillance for sensor networks. In The 1st international conference on Embedded Networked Sensor Systems (SenSys) (pp. 51–62). Los Angeles: ACM.

Ye, W., Heidemann, J., & Estrin, D. (2002). An energy-efficient MAC protocol for wireless sensor networks. In The 21st Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM) (pp. 1567–1576). New York: IEEE.

Ye, W., Heidemann, J., & Estrin, D. (2004, June). Medium access control with coordinated adaptive sleeping for wireless sensor networks. *IEEE/ACM Transactions on Networking* (IEEE/ACM), 12(3), 493–506.

Ye, F., Luo, H., Lu, S., & Zhang, L. (2005, April). Statistical en-route filtering of injected false data in sensor networks. *Journal on Selected Areas in Communications* (IEEE), 23(4), 839–850.

Yessad, S., Bouallouche, L., & Aissani, D. (2011). Proposition and evaluation of a novel routing protocol for wireless sensor networks. In The 5th international workshop on Verification and Evaluation of Computer and Communication Systems (VECONS) (pp. 1–9). Tunis: BCS, The Chartered Institute for IT.

Yessad, S., Tazarart, N., Bakli, L., Medjkoune-Bouallouche, L., & Aissani, D. (2012). Balanced energy efficient routing protocol for WSN. In *International Conference on Communications and Information Technology (ICCIT)* (pp. 326–330). Hammamet: IEEE.

Yessad, S., Bouallouche-Medjkoune, L., & Aissani, D. (2015). A cross-layer routing protocol for balancing energy consumption in wireless sensor networks. *Wireless Personal Communications* (Springer Nature), 81, 1303–1320.

Yetgin, H., Cheung, K. T. K., El-Hajjar, M., & Hanzo, L. (2015, August). Cross-layer network lifetime maximization in interference-limited WSNs. *Transactions on Vehicular Technology* (IEEE), 64(8), 3795–3803.

Yu, Z., & Guan, Y. (2008, October). A key management scheme using deployment knowledge for wireless sensor networks. *Transactions on Parallel and Distributed Systems* (IEEE), 19(10), 1411–1425.

Yuan, Z., Wang, L., Shu, L., Hara, T., & Qin, Z. (2011). A Balanced Energy Consumption Sleep Scheduling Algorithm in Wireless Sensor Networks. In *The 7th International Wireless Communications and Mobile Computing Conference (IWCMC)* (pp. 831–835). Istanbul, Turkey: IEEE.

Zamalloa, M. Z., Seada, K., Krishnamachari, B., & Helmy, A. (2008, June). Efficient geographic routing over lossy links in wireless sensor networks. *Transactions on Sensor Networks* (ACM).

Zhang, J., & Varadharajan, V. (2010, March). Wireless sensor network key management survey and taxonomy. *Journal of Network and Computer Applications* (Elsevier B.V.), 33(2), 63–75.

Zigbee Alliance. (2020). Zigbee. Zigbee Alliance. January. 1. [https://zigbeealliance.org/solution/zigbee/](https://zigbeealliance.org/solution/ zigbee/). Accessed 18 Apr 2020.
Zorzi, M., & Rao, R. R. (2003, October/December). Geographic Random Forwarding (GeRaF) for ad hoc and sensor networks: Multihop performance. *Transactions on Mobile Computing (IEEE)*, 2(4), 337–348.

Zuniga, M., & Krishnamachari, B. (2004). Analyzing the transitional region in low power wireless links. In *1st annual communications society conference on Sensor and Ad Hoc Communications and Networks (SECON)* (pp. 517–526). Santa Clara: IEEE.