A Survey of MAC Protocols for Mission-Critical Applications in Wireless Sensor Networks

Petcharat Suriyachai, Utz Roedig, and Andrew Scott

***Abstract*—Wireless Sensor Networks (WSNs) are generally designed to support applications in long-term deployments, and thus WSN protocols are primarily designed to be energy efficient. However, the research community has recently explored new WSN applications such as industrial process automation. These mission-critical applications demand not only energy efficient operation but also strict data transport performance. In particular, data must be transported to a sink in a timely and reliable fashion. Both WSN's data transport performance and energy consumption pattern are mainly defined by the employed medium access control (MAC) protocol. Therefore, this survey paper explores to what extent existing MAC protocols for WSNs can serve mission-critical applications. The reviewed protocols are classified according to data transport performance and suitability for mission-critical applications. The survey reveals that the existing solutions have a number of limitations and only a few recently developed MAC protocols are suitable for this application domain.**

***Index Terms*—Medium Access Control Protocols, Mission-Critical Applications, Quality of Service, Safety-Critical Applications, Time-Critical Applications, Wireless Sensor and Actuator Networks, Wireless Sensor Networks, Survey.**

I. Introduction

WIRELESS Sensor Networks (WSNs) consist of small autonomous devices called nodes or motes that harvest information such as temperature, pressure or vibration from their physical environment. The collected information is, in most cases, transported hop-by-hop through the network to a central control station where it is analyzed and decisions are made.

Initial applications supported by WSNs were mostly in the domain of environmental monitoring [60]. Example applications are bird observation on Great Duck Island [61] and glacier motion monitoring [62]. In this domain, operation with little or no human intervention for long periods of time is required. As sensor nodes have limited energy resources, network protocols for this application domain have energy-efficiency as the main design goal. Hence, existing network protocols are very energy efficient but provide only simple best-effort data delivery. Such behavior poses no problem in this application scenario as long data transport delays can be tolerated. For example, in a glacier monitoring application, plenty of time is available to forward sensor readings because the observed phenomenon is changing only slowly and the collected data is not used to trigger actions immediately. The abundance of available forwarding time can also be used to retransmit lost messages and compensate for message losses.

WSNs have been subsequently extended to support many other application domains such as military target tracking [63], [64], patient monitoring [66], [67] or industrial process monitoring [69]. The aforementioned best-effort data delivery is no longer adequate for these application domains. Instead, *improved* data delivery is required as the applications can only function properly if data arrive in a timely and reliable fashion. For example, a WSN for battlefield surveillance is only useful if information about an approaching enemy arrives in time.

Wireless Sensor and Actor Networks (WSANs) have recently attracted considerable interest from the research community. WSANs have very strict requirements regarding network performance as actuator nodes must react to data collected by sensor nodes within a tight deadline. Most WSAN applications are only implementable if the network can provide deterministic network performance [48], [49]. For instance, a WSAN can be employed to control a chemical production process. Sensors observing pressure in pipes must deliver messages to an actuator connected to a valve in a timely and reliable fashion. The control loop can only be implemented if a strict upper bound on data transfer delay between sensor and actuator can be given.

The novel WSN applications outlined in the above two paragraphs have two characteristics in common: (1) energy efficiency cannot be the only design concern and (2) the best-effort data delivery is not sufficient. These features motivate an investigation of the implementation of WSNs for mission-critical applications. In this paper, *mission-critical WSN applications are defined as applications demanding data delivery bounds in the time and reliability domains*. A vast number of potential mission-critical WSN applications can be found in the area of process automation and control [69], [70]. To support these applications the network must provide both timely and reliable data delivery. Network performance parameters such as delay, reliability and throughput must therefore be considered during network design. Furthermore, energy consumption remains a design concern as a reasonably long network lifetime is still desirable.

The design of a WSN is often started with the definition of a Medium Access Control (MAC) protocol as it fundamentally determines the energy consumption properties and the basic data transport capabilities of the network. Additional network mechanisms such as routing or topology control are often integrated into the MAC protocol or closely aligned with its design choices. Hence, to support mission-critical applications, a necessary first step is to find a MAC protocol that is capable

Manuscript received 23 March 2010; revised 17 September 2010, 15 December 2010, and 25 December 2010.

The authors are with InfoLab21, Lancaster University, UK (e-mail: {p.suriyachai, u.roedig, a.scott}@lancaster.ac.uk).

Digital Object Identifier 10.1109/SURV.2011.020211.00036

of supporting performance bounds on data transport delay and reliability. This survey paper explores to what extent existing MAC protocols can serve mission-critical applications. Moreover, the survey covers solutions that not only contain a MAC protocol at their core but also specify additional mechanisms considered crucial to enable the mission-critical data delivery.

A large number of MAC protocols for wireless sensor networks have been proposed in literature, and an exhaustive list can be found in [54], [55], [56], [57]. The majority of existing MAC protocols are purely designed to minimize energy consumption. A small number of them consider delay, reliability or other design concerns that are essential to support mission-critical applications. This review differs from existing MAC protocol surveys [54], [55], [56], [58] as it analyzes recent MAC protocols with regard to their suitability for mission-critical applications. The surveyed protocols are classified by the fundamental performance objectives: *data transport delay* and *reliability*. We believe that these two objectives are most relevant in the context of mission-critical applications, while energy efficiency could be addressed additionally if required. Some of the surveyed protocols address only one objective, while others address both objectives concurrently. This paper provides a comparison of merits and drawbacks of these protocols. In addition, it identifies open research questions in the field of MAC protocols for mission-critical WSN applications.

The remainder of the paper is organized as follows. Section II elaborates mission-critical application scenarios and a taxonomy that is used to categorize the reviewed protocols. Delay-aware MAC protocols and reliability-aware MAC protocols are presented in Section III and Section IV, respectively. Section V explains MAC protocols that concurrently address both delay and reliability objectives. Section VI describes limitations of the reviewed protocols leading to open research issues and a discussion of future directions of MAC protocol research for mission-critical applications. Finally, concluding remarks are given in Section VII.

II. Mission-Critical Data Delivery

This section explores common application scenarios in WSNs and categorizes them into four application classes; one of these classes represents the mission-critical applications of interest. For each surveyed WSN MAC protocol, we state the application class it is able to support. In addition, since WSNs are generally designed for specific applications, we give the underlying WSN design assumptions to enable a fair comparison of the reviewed MAC protocols. We also provide a definition of network performance parameters that we use to evaluate the performance of the surveyed protocols. Furthermore, we introduce a performance-driven MAC protocol classification scheme that is used to identify which MAC protocols should be included in this survey. Besides the classification scheme, we detail S-MAC [28] protocol which is chosen as the reference point for protocol comparison.

A. Application Scenarios

Although WSNs can be applied in a number of application scenarios, they are typically deployed for monitoring, control or tracking scenarios [61], [62], [63], [64], [65]. Given the large number and variety of different application scenarios, it is not useful to classify WSNs in terms of application context. Instead, other more generic application characteristics are generally used for classification. For example, WSN applications can be classified in terms of how they extract data (periodic or aperiodic), what type of deployment they require (static or ad hoc) or data volume they generate (large or small sample size). However, in the context of this paper we classify applications in terms of the *data delivery performance* they demand.

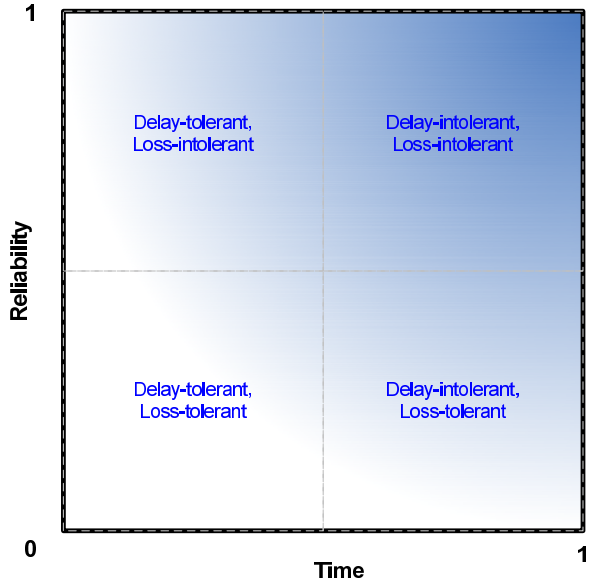


Fig. 1. Application Classes Based on Network-Driven Performance

Applications can be characterized in terms of performance needs using two different definitions: data-driven and network-driven. The data-driven performance depends on the packet content, and thus issues such as sensing accuracy and sensing fidelity are design concerns. In contrast, the network-driven performance depends on the packet delivery being timely and/or reliable. In this paper, the data delivery performance in both the time and reliability domains is used to classify applications.

The performance in the time domain depends on *when data is received at the destination*. Parameters such as message transfer delay and jitter are commonly used to quantify this performance aspect. The performance in the reliability domain depends on *how much data is received at the destination*. Delivery ratio and packet loss rate are measurements often used to represent this reliability performance. In addition, the performance in the time and reliability domains are interdependent. Data delivered late can be considered as lost data. Likewise, additional time for data transmission can be used to improve reliability, such as seen when retransmissions are employed. The interdependency is often characterized by measuring throughput.

As delay and loss can be used as a pair of network-driven performance metrics, WSN applications can be classified based on such a pairing. The classification result is displayed in Figure 1. The scales of the x-axis and y-axis are from 0 to 1, signifying the level of increasing performance intolerance of an application. The value 0 represents complete performance

relaxation, while the value 1 represents absolute performance guarantee. For example, an application at point (1, 1) requires that a defined amount of data readings must be delivered within a strict time bound. Moreover, the classification assumes a uniform distribution on the performance values in both axes, and thus the value 0.5 is defined as the mid-point which divides two performance areas: tolerant and intolerant. An elaboration of each application class and corresponding data delivery requirements are given below.

- *Delay-tolerant, Loss-tolerant Class*. The applications in this class accept high data transport delay and loss. Examples of such performance independent scenarios are environmental monitoring applications [61], [62] where the application can still function as desired even if high data losses are incurred and some data requires a long time for delivery. For such lenient applications, the data delivery requirements can be relaxed in both the time and reliability domains.
- *Delay-tolerant, Loss-intolerant Class*. Applications in this class can tolerate large delays in data delivery but data must eventually arrive. For example, a car park monitoring application [68] keeps track of the number of cars that enter or leave a monitored area. To determine available parking spaces for potential customers, the monitoring must be accurate but data delivery times in order of minutes can be tolerated. To accommodate applications in this class, the data delivery can be relaxed in the time domain but must obey a stringent requirement in the reliability domain.
- *Delay-intolerant, Loss-tolerant Class*. In contrast to the previous class, relatively high loss rates are acceptable in this class but data must arrive in a timely manner. For instance, a target tracking application might require timely data delivery but may not require that a high percentage of data readings reaches the destination [63]. To accommodate applications in this class, the data delivery must obey a stringent requirement in the time domain but can be relaxed in the reliability domain.
- *Delay-intolerant, Loss-intolerant Class*. The applications in this class demand strict performance in both the time and reliability domains. Monitoring transmission pipelines in an oil refinery is one example of this application class [69], [70]. If a sensor detects a dangerous overpressure in a pipe, its alarm message has to be transported in a timely and reliable manner to an actuator that operates a shutter valve. Given the strict delivery requirements, the mission-critical applications mentioned in the paper represent this class of delay-intolerant and loss-intolerant applications.

The aim of this survey is to determine which available MAC protocols ensure that data delivery obeys a stringent requirement in both the time and reliability domains. The protocols thus can be used to support applications that fall into the *delay-intolerant and loss-intolerant* class. These applications are *mission-critical* and located in the top right quadrant of Figure 1. We will use Figure 1 to present the findings of this survey graphically. Each MAC protocol is placed in the application area that it is able to support well (See Section VI).

It is important to reiterate that in our opinion the delay and reliability performance aspects are most relevant to enabling mission-critical applications and must be addressed before considering energy efficiency. Figure 1 thus depicts only the delay and reliability aspects while excluding the energy issue. However, energy efficient operation is required in many mission-critical applications to support a long network lifetime. We therefore investigate energy consumption of the reviewed protocols in addition to their delay and reliability performance.

B. Design Assumptions

As mentioned above, WSNs are designed and tailored for distinctive applications. Consequently, one system prototype that is applicable to certain application scenarios may fail to perform adequately in other scenarios because of different design assumptions. Furthermore, in contrast to traditional IP networks, the design of WSN protocols has not yet followed any standardized or layered structure. As a result, there is no one-size-fits-all solution in WSNs. The designs of MAC protocols that are discussed in the WSN literature generally utilize the assumptions listed below. Although it is not complete, this list covers most popular assumptions. For the presented MAC protocol survey it is necessary to take these design assumptions into consideration. For example, a MAC protocol might be suitable for mission-critical applications but only if a very narrow set of design assumptions is met.

Sensor Deployment (Random or Planned): Sensor deployment can be classified as random or planned. In a planned deployment the location of nodes can be carefully selected. Conversely, in a random deployment node locations cannot be influenced, especially during network design. MAC protocols for planned deployments are generally more efficient than those for random deployments as more information about network structure can be exploited when protocols are designed.

For instance, in many environmental monitoring applications, nodes are assumed to be dropped from an airplane, resulting in a random deployment. Certain probability distributions are commonly used to further describe such deployments, for example, uniform or Poisson distributions. In other scenarios, nodes are assumed to be placed manually at specific locations in a planned deployment. In such a deployment, nodes would often be placed as required without a pre-defined physical topology being formed. However, some work assumes that nodes are placed in a grid, while other work assumes tree-based topologies.

Topology Formation (Flat or Hierarchical): A logical topology in a wireless sensor network is defined as flat or non-hierarchical when all nodes perform the same functionality. In contrast, a topology is hierarchical when some nodes have additional functionality or take on a more prominent role than other nodes. For instance, a hierarchical deployment may employ cluster heads that are used to relay messages between nodes. In a hierarchical tree topology, a parent node may act as a data aggregation point for its child nodes. MAC protocols differ significantly in their design and achievable performance if the presence of hierarchical structures is assumed.

Network Traffic Pattern (Convergecast, Broadcast or Local Gossip): Applications in WSNs usually generate three types of network traffic patterns: convergecast, broadcast, and local gossip. Convergecast traffic is observed in most monitoring applications that require some or all nodes to report to one or a few specific nodes such as sinks, cluster-heads or data fusion nodes. Alternatively, queries or control messages from sinks are distributed over the network generating broadcast traffic. In the local gossip pattern, node communication with one another produces a local traffic pattern. For instance, a tracking application requires nodes to trace an object's movement. Upon detecting such a movement, a node communicates with its direct neighbors in order to request collaboration to maintain the current location of the object. Therefore, the network traffic pattern follows the direction of this object's movement. In order to meet a performance goal, the design of a MAC protocol should take account of expected traffic patterns. For example, a protocol designed for convergecast usually provides poor performance if it is used to support a local gossip traffic pattern.

Cross-layer Support: In contrast to traditional wired networks including the Internet, construction of WSNs does not always follow a layered protocol stack but instead exploits cross-layer information to obtain additional optimization. Some designs of MAC protocols for WSNs utilize cross-layer information extensively. For example, information from the routing layer [7] or the application layer [35] is used to improve MAC protocol performance. However, other MAC protocols pursue the conventional layered approach and avoid any integration with other layers to promote protocol reusability.

Transceiver Type: MAC protocols are tailored to a specific type of transceiver hardware. Conventional MAC protocols [4], [28] usually assume that one single data radio is available, while other modern platforms provide a second additional radio to further conserve energy [43], [44]. This low power control radio often remains on all times and prompts the high power radio to wake up for actual data transmission or reception. Besides the assumption about the number of transceivers per node, the type of transceiver deployed also influences MAC protocol design and performance. Most MAC protocols assume homogeneous transceivers for all nodes in a network; all nodes and sinks use identical transceivers and settings such as transmission power. In contrast, some protocols assume heterogeneous transceivers. For example, in [16] a sink node employs a high power radio that can directly reach other nodes in a network, but these nodes use low power radios to forward data to the sink.

C. Performance Parameters

As defined in Section II-A, mission-critical applications require messages to be delivered in a timely and reliable fashion. Furthermore, this application domain may demand a network with a reasonably long lifetime. The network lifetime is determined by the energy consumption patterns of battery-powered sensor nodes. Thus, a MAC protocol for mission-critical applications should be evaluated considering both transport performance and energy consumption; the energy issue could, however, be less important in some mission-critical scenarios. For protocol evaluation within this survey, we use the following performance metrics.

Message Transfer Delay: The message transfer delay is defined as the amount of time needed to transport a message from one node to another. This transfer delay is measured from the time the message is passed to the MAC layer at the sending node to the time the message is passed from the MAC layer to its upper layer at the receiving node. In addition to propagation delay, the message transfer delay includes processing delays at the MAC layer. In this paper, the term delay is used interchangeably with the term message transfer delay.

Message Transfer Reliability: The message transfer reliability is defined as the probability of successfully delivering a message from a sender to a receiver. A simple way to estimate message transfer reliability is to measure a packet loss rate or packet delivery ratio. The issue of message transfer reliability is mostly addressed outside the MAC protocol. For example, transport protocols are often used to address message transport reliability [50], [51]. However, recent work supporting mission-critical applications [24], [27], [39] has shown that it is beneficial to address message transfer reliability within the realm of MAC protocols. In the remainder of the paper, we use message transfer reliability and reliability interchangeably.

Energy Consumption: Communication uses more energy than other operations by several orders of magnitude, and it is generally regarded as the highest source of power expenditure in MAC protocols for WSNs. As a result, only energy consumption regarding the communication is taken into account when evaluating the performance of MAC protocols. The communication-related energy consumption of a sensor node is mostly influenced by the time the communication transceiver is operated in an active state, which include transmitting, receiving and idle listening. The energy efficiency of a MAC protocol can be quantified by the so-called duty cycle. This duty cycle P is the ratio of radio on time Δ_{on} to the sum of radio on time Δ_{on} and radio off time Δ_{off}, and thus is formally defined as $P = \Delta_{on}/(\Delta_{on} + \Delta_{off})$. The radio on time represents the time the radio is in the aforementioned active state, while the radio off time represents that in an power-efficient sleep state.

D. Taxonomy

A multitude of MAC protocols for WSNs have been proposed in literature, and an exhaustive list can be found in [55], [56], [57], [58]. These MAC protocols are described using well known classification schemes. For example, MAC protocols in wireless sensor networks are commonly categorized into three main groups based on the degree of node coordination to avoid collision of data transmission[1]: *contention-based*, *schedule-based*, and *hybrid* approaches. Alternatively, Langendoen [56] proposes a classification according to how nodes organize access to the shared transmission channel. Therefore, three classes of organization are defined: *random access*, *slotted*

[1]It is important to emphasize that the term collision is shortened from *collision of data transmission* as some schedule-based MAC protocols could employ the contention-based approach when transmitting control packets during their setup phase.

access and *frame-based access*. However, for the presented survey, existing classification schemes are not very useful as they do not capture the network performance parameters of interest. Therefore, we propose a classification scheme based on performance achievements in terms of delay and reliability.

The review focuses on a group of protocols that are capable of meeting mission-critical application requirements. In particular, the protocols must ensure that data delivery is timely and reliable, while the goal of energy efficiency is of secondary importance. Therefore, the following two main categories are used: *delay-aware* and *reliability-aware*. All surveyed MAC protocols are classed as delay-aware and/or reliability-aware. In addition, sub-classes are used to indicate how a protocol addresses delay or reliability issues. For the delay issue the four sub-classes are *node-to-node decrease, node-to-node guarantee*, *end-to-end decrease* and *end-to-end guarantee*. In contrast, for the reliability issue the four sub-classes are *node-to-node increase*, *node-to-node guarantee*, *end-to-end increase* and *end-to-end guarantee*. The exact definition of the classification scheme is provided next.

In our definition, a protocol is categorized as delay-aware if it *clearly aims* to achieve timely delivery. Similarly, a protocol is categorized as reliability-aware if it *clearly aims* to cope with fluctuating channel quality to enable reliable delivery.

A delay-aware MAC protocol can be designed to *decrease* or *guarantee* message transfer delay. The term decrease is used to describe a protocol when it can reduce delay in comparison with S-MAC [28] protocol, which is our reference point and described next in Section II-E. Alternatively, the term guarantee is used when a protocol can provide timely delivery. This performance guarantee is further divided into two forms: *probabilistic* and *worst-case*. A delay-aware MAC protocol classified as *probabilistic guarantee* ensures that delays of successfully delivered messages follow a particular pre-defined distribution. In contrast, a delay-aware MAC protocol regarded as *worst-case guarantee* ensures that all successfully delivered messages arrive within a fixed pre-defined time. As to be argued later in Section VI, almost all delay-aware guarantee MAC protocols in this survey provide *worst-case guarantees*. Thus, for simplicity we often describe these protocols as providing *guarantees* but explicitly describe the remaining protocols as providing *probabilistic guarantee*.

In addition, the delay performance of MAC protocols can be considered at *node-to-node* or *end-to-end* levels. In general, MAC protocols are designed for channel arbitration among only neighboring nodes, and in this survey they are classified as *node-to-node decrease* or *node-to-node guarantee*. In contrast, some delay-aware MAC protocols address data delivery at a larger scale and consider the complete delivery path between sensor nodes and sinks. These protocols are classified here as *end-to-end decrease* or *end-to-end guarantee*, and they are explained in detail along with other delay-aware MAC protocols in Section III.

The performance in the reliability domain is categorized in a similar fashion. A reliability-aware protocol can be designed to *increase* or *guarantee* message transfer reliability. The reference point to measure an increase in reliability is again S-MAC [28], which does not provide any mechanisms to improve reliability. In addition, the performance guarantee can be given as *probabilistic guarantee* or *worst-case guarantee*. Reliability can also be addressed by a MAC protocol on a *node-to-node* or *end-to-end* basis. In this survey, reliability-aware MAC protocols can therefore be classed as one of these four types: *node-to-node increase, node-to-node guarantee, end-to-end increase* and *end-to-end guarantee*. The details of these protocols are presented in Section IV.

In contrast to the delay issue, reliability is rarely addressed by MAC protocols. Often, other protocols such as transport or routing protocols [50], [51], [52], [53] are designed to handle the reliability challenge. However, studies such as [24], [26], [27] show that in order to improve data delivery performance, MAC protocols must address packet losses. Most mechanisms to improve reliability require increased data transport delays, for example, acknowledgements and retransmissions. Therefore, it is necessary to address delay and reliability together, and Section V explains the protocols with these two objectives.

E. Reference Point for Protocol Comparison

Before we perform an in-depth analysis of the reviewed MAC protocols in the subsequent three sections, we here provide an example network topology and symbols that are used to illustrate MAC protocol operations in the remainder of the paper. Furthermore, we explain the S-MAC [28] protocol that is used as the reference point for protocol comparison.

To describe the functionality of the surveyed protocols, we use a simple tree topology that is commonly adopted in many WSN deployments. Data are usually forwarded multiple hops toward the sink node, and in Figure 2 they are transferred from node C to the sink node. We adopt this forwarding path to illustrate operations of the reviewed protocols. Figure 2 also presents the notation used to help depict these operations.

In addition, it has to be noted that most reviewed protocols use one frequency channel for transmission, and we do not include any notation to indicate this single channel in their figures. In contrast, for the protocols that utilize more than one frequency channel, their transmission channels are displayed as shaded and labeled clearly. Furthermore, most reviewed protocols do not specify if the sink is power constrained, whereas only a few state otherwise. In the illustration of protocol operation, we therefore assume that the sink performs radio duty cycling. This assumption enables us to achieve consistency when comparing the protocols. Nevertheless, the result of the protocol comparison should be similar to ours if all reviewed protocols assume that the sink is always on. These protocols are compared with S-MAC [28] whose description is summarized below.

S-MAC [28] is one of the prominent pioneering studies on MAC protocols in WSNs, and we use it as the reference point for protocol comparison in this survey. Having energy efficiency as the primary design goal, the protocol introduces the periodic duty-cycle concept to reduce idle listening. Figure 3 illustrates this concept in which nodes alter periodically between active and sleep state. A node coordinates its fixed sleep/active period with neighbors using SYNC packets. Within an active period nodes follow the IEEE 802.11 standard to transmit messages. The protocol uses an exchange of Request-To-Send (RTS) and Clear-To-Send

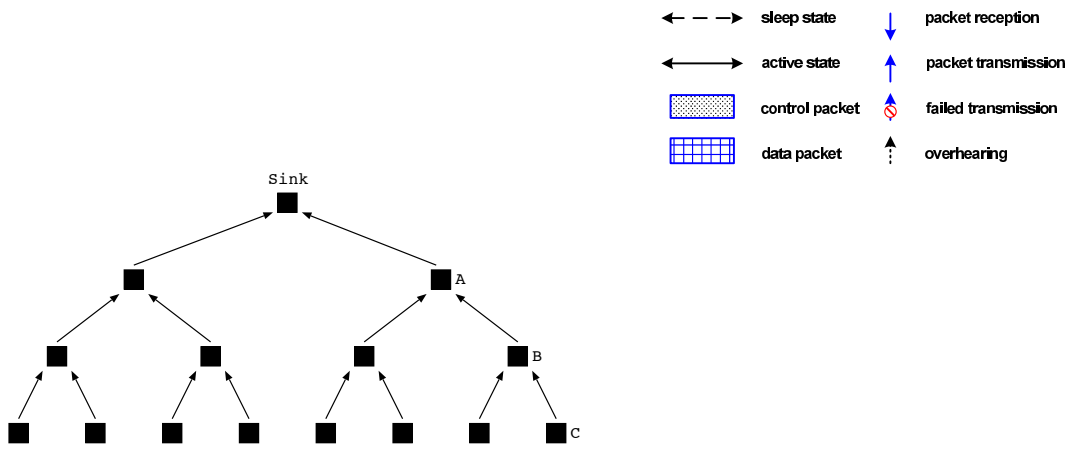


Fig. 2. Topology and Legend Used for Protocol Comparison

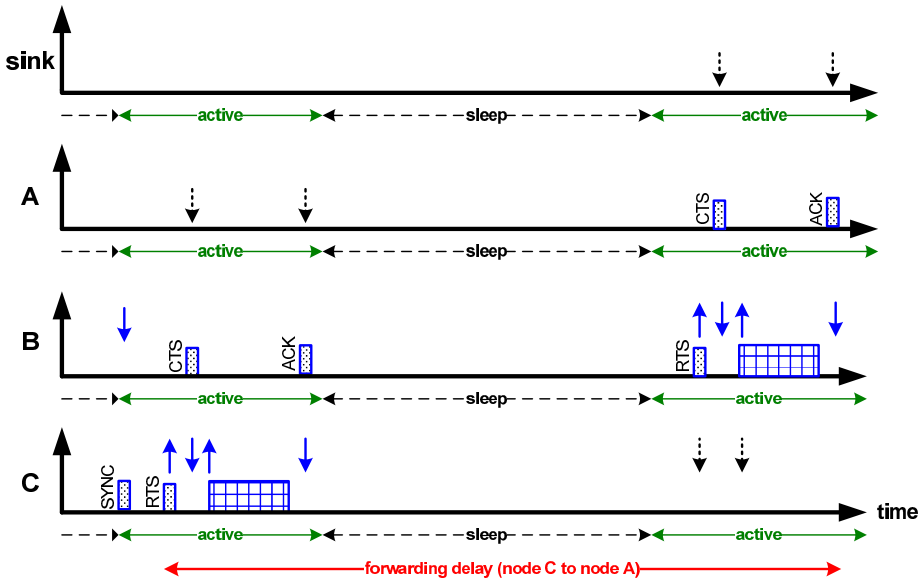


Fig. 3. S-MAC [28] Protocol Used as the Reference Point

(CTS) packets as a contention mechanism in the active period. Packets transported using S-MAC can experience high delays in a multi-hop network as they might have to be queued at a node until the next active period.

This S-MAC [28] protocol was the first reasonable protocol for WSNs, but it does not aim to provide timely or reliable data delivery. In contrast, all protocols that we discuss in the next three sections aim to do so. We therefore highlight how the surveyed protocols improve data transport performance in comparison to the chosen S-MAC baseline.

Table I shows the result of this survey using the aforementioned classification scheme and comparing with S-MAC. It also illustrates how the MAC protocols address energy conservation, which could be implemented after the delay and reliability requirements are met. Furthermore, in this table we state which design assumptions, previously described in Section II-B, are taken into account during the design phase of the protocols.

The next three sections discuss the reviewed MAC protocols in detail. These sections are motivated by our taxonomy defined in Section II-D and present *delay-aware MAC protocols*, *reliability-aware MAC protocols* and *delay-and-reliability-aware MAC protocols*, respectively. Figure 4 depicts the structure of this presentation. Within each section, the reviewed MAC protocols are ordered according to our taxonomy whenever possible. However, to improve the readability of this survey we decided to discuss and group the protocols in each section according to their common principles. In any group, we clearly state how each described protocol maps onto the proposed taxonomy.

III. Delay-Aware MAC Protocols

In this section, we describe MAC protocols that can be classified as *delay-aware* using the aforementioned classification scheme based on performance achievements. For each surveyed MAC protocol, we discuss which specific performance feature it provides: *node-to-node decrease*, *node-to-node guarantee*, *end-to-end decrease* or *end-to-end guarantee*. Details of contention-based delay-aware protocols are presented first, and then a discussion of schedule-based delay-aware protocols follows.

TABLE I
COMPARISON OF MAC PROTOCOLS AND SUPPLEMENTARY TECHNIQUES FOR MISSION-CRITICAL APPLICATIONS IN WIRELESS SENSOR NETWORKS

Protocols	Performance Objectives			Assumptions				
	Energy	Delay	Reliability	Deployment	Topology	Network Pattern	Cross-layer Support	Transceiver
S-MAC-AL [1], T-MAC [2], DSMAC [3]	duty cycling	node-to-node decrease (a few hops)	no	random	flat	any	no	single, homogeneous
DMAC [4], LEEMAC [5]	duty cycling	end-to-end decrease	no	random	tree	convergecast	no	single, homogeneous
FPA/GSA [6] Algorithms	duty cycling	end-to-end decrease	no	n/a	flat	any	routing	single, homogeneous
RMAC-R [7]	duty cycling	end-to-end decrease	no	random	flat	any	routing	single, homogeneous
LE-MAC [8]	duty cycling	end-to-end decrease	no	random	flat	any	carrier sensing, routing	single, homogeneous
Q-MAC [9]	duty cycling	end-to-end decrease	no	random	flat	convergecast (query-based)	no	single, homogeneous
PTW [10]	duty cycling	end-to-end decrease	no	random	flat	any	no	dual, homogeneous
LEEM [11]	duty cycling	end-to-end decrease	no	random	flat	convergecast	routing	dual, homogeneous
T-MALOHA [12]	n/a	node-to-node probabilistic guarantee	no	planned	star (single hop)	convergecast	no	multiple at sink, single at others, homogeneous
Alert [13]	no	node-to-node decrease	no	planned	star (single hop)	convergecast	no	single, homogeneous
f-MAC [14]	no	node-to-node guarantee	no	random	flat	any	no	single, homogeneous
FTDMA [12]	n/a	node-to-node guarantee	no	planned	star (single hop)	convergecast	no	multiple at sink, single at others, homogeneous
RT-Link [15]	duty cycling	end-to-end guarantee	no	planned	tree	convergecast	no	single, homogeneous
PEDAMACS [16]	duty cycling	end-to-end guarantee	no	random	tree	convergecast	no	single, heterogeneous (high-power sink)
HyMAC [17]	duty cycling	end-to-end guarantee	no	random	tree	convergecast	no	single, homogeneous
RMAC [18]	no	no	node-to-node increase	random	flat	any	routing	single, homogeneous
E2RMAC [19]	duty cycling	no	node-to-node increase	random	flat	any	routing	dual, homogeneous
Back-off [20] Algorithms	n/a	no	end-to-end increase	random	flat	broadcast	routing	single, homogeneous
ATPC [21] Algorithm	n/a	no	node-to-node increase	random	flat	any	no	single, homogeneous
MMSPEED [22]	no	end-to-end probabilistic guarantee	end-to-end probabilistic guarantee	random	flat	any	routing	single, homogeneous
Dwarf [23]	duty cycling	end-to-end decrease	end-to-end increase	random	ring	convergecast	routing	single, homogeneous
QoS-MAC [24]	duty cycling	node-to-node guarantee	node-to-node guarantee	planned	tree	convergecast	routing	single homogeneous
WirelessHART [25]	duty cycling	end-to-end guarantee	end-to-end increase	random	mesh	any	no	single homogeneous
Burst [26] Algorithm	n/a	end-to-end guarantee	end-to-end guarantee	planned	flat	any	routing	single homogeneous
GinMAC [27]	duty cycling	end-to-end guarantee	end-to-end guarantee	planned	tree	convergecast	routing	single homogeneous

A. Contention-based MAC Protocols

Contention-based MAC protocols can operate either in a *synchronous* or *asynchronous* fashion. Nodes using synchronous protocols are aware of roughly when a neighboring node is able to receive a message. However, this collaboration of transmission schedules is not as strict as the synchronization employed in schedule-based MAC protocols. Collisions are not eradicated by using synchronous protocols since nodes still contend for the channel when becoming active. In contrast to the synchronous protocols, nodes using asynchronous protocols do not keep track of activity schedules of neighboring nodes at all. To enable communication, a sender must ensure that a transmission falls in the active period of a receiver. For example, a transmission can be prolonged such that reception is guaranteed. We analyze synchronous protocols and then asynchronous protocols as presented below.

1) Localized Transmission Scheduling: There are several subsequent studies that are based on S-MAC [28]. Instead of a fixed active period used in S-MAC, they employ an adaptive active period to improve per-hop delays in multi-hop networks. For example, in [1], which we call S-MAC-AL for presentation in the survey, nodes use overheard RTS and CTS messages to schedule an additional wake-up period at the end of the announced data transmission. In case the

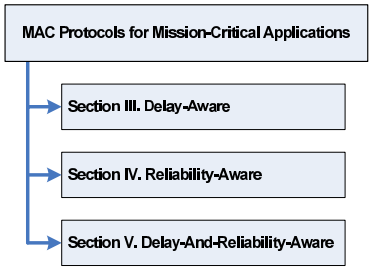


Fig. 4. Section Structure According to the Taxonomy Given in Section II-D

overhearing node is the next hop in the delivery path, packets can be forwarded without waiting for the next scheduled active period. Figure 5 shows the adaptive listening enhancement of S-MAC-AL that decreases forwarding delay. In particular, node C sends a packet whose final destination is the sink to its next-hop forwarder: node B. As being an immediate neighbor of node B, node A overhears the CTS packet from node B and thus can determine the duration of the packet transmission between node C and node B. Subsequently, node A switches off its radio and adaptively wakes up at the end of this duration. As node A is the next-hop node in its transmission path, node B immediately passes the packet to node A. Hence, the forwarding delay from node C to node A in S-MAC-AL is less than that in S-MAC. Note that due to a space constraint we cannot illustrate the forwarding delay from node C to the sink, unlike other illustrations of most subsequent protocols. However, this end-to-end delay is likely to be reduced as a result of the adaptive active period in S-MAC-AL.

Other protocols similar to S-MAC-AL include T-MAC [2] and DSMAC [3]. Adopting an adaptive active period clearly enables these protocols to reduce the forwarding delay compared to S-MAC. The improvement of forwarding delays is nevertheless local and not designed to cover the whole message delivery path through the network. A packet traveling through the network may still experience long queuing times at some points in its delivery path. Therefore, these three variants of S-MAC can only *decrease node-to-node* delay and are not suitable to enforce timely data delivery.

2) Path-Aware Transmission Scheduling: In the aforementioned variants of S-MAC, not all nodes in the network are aware of the data transmission path. Therefore, unnecessary sleep delays may add to the end-to-end delay, and their sleep/active scheduling causes a data forwarding interruption problem. To remedy this problem, another group of protocols coordinates sleep schedules along forwarding paths to decrease the overall latency in a multi-hop network.

DMAC [4] applies a staggered wake-up schedule which allows nodes along the data-gathering tree to wake up sequentially as a packet traverses toward the sink. Three different types of time slots are used: receiving, sending and sleep. In a receiving slot, a node might receive one packet which is acknowledged. In a sending slot a node might transmit one packet and expects an acknowledgement. A transceiver is shut down in a sleep slot to save energy. Each node adopts a periodic interval that consists of one receiving slot, one sending slot and multiple sleep slots. The protocol ensures that a node higher up in a collection tree is in a receiving slot while the node below is in a sending slot. Therefore, a wake-up schedule of a node is skewed ahead from that of its parent node as shown in Figure 6. A packet forwarded through the network does not experience additional delays due to node sleep phases. In addition, when a node has multiple packets to transmit in one sending slot, it uses a slot-by-slot renewal mechanism. A more data flag in the MAC header is set to request an additional active period. If granted, the active period follows a fixed sleep period lasting three slots. As the following nodes on the path will forward the packet in these slots, the interim sleep period serves as a mechanism to avoid collisions. Compared to S-MAC, DMAC obviously reduces the overall end-to-end delay, but it suits only applications where traffic flows from sensor nodes to a single sink.

Similar to DMAC, there are other protocols whose designs are aware of a packet transmission path. Examples of such protocols are LEEMAC [5], FPA/GSA [6], RMAC-R[2] [7], LE-MAC [8] and Q-MAC [9]. The MAC protocols in this group of path-aware transmission scheduling *decrease end-to-end delay*. However, they are not designed to give guarantees as they contain non-deterministic elements. For example, DMAC is not able to give delay guarantees as a number of child nodes must still compete for a transmission slot to a parent node where random back-off is used.

The protocols discussed so far in this path-aware transmission scheduling group address the data forwarding interruption problem, which is caused by radio duty cycling. However, there are a few somewhat similar studies that use a slightly different approach to enhance the delivery performance. For example, funneling-MAC [36] improves throughput and reduces packet loss in the high traffic area near the sink. It is a hybrid MAC protocol that uses both CSMA/CA (contention-based) and TDMA (schedule-based) schemes to support many-to-one communication, which is similar to the data-gathering tree in DMAC. The CSMA/CA scheme is implemented network-wide, whereas the TDMA scheme is used to allocate additional transmission opportunities to nodes near the sink. Another work that also addresses the many-to-one traffic pattern is a time-optimum packet scheduling algorithm described in [37]. The algorithm can minimize message transfer delay in a tree topology and enables nodes to adjust duty cycles locally. Several ideal assumptions are also made to lower interference among transmission links, and therefore they could be violated in a real deployment.

Both the time-optimum scheduling algorithm [37] and funneling-MAC [36] may not yet be able to support mission-critical applications. In particular, although the algorithm can determine optimal delay, some applications prefer guaranteed performance to fast data delivery. Funneling-MAC alleviates the problem of high traffic near the sink and aims to improve throughput instead of giving a guaranteed delay.

3) Transmission Scheduling Using Wake-up Radios: In general, MAC protocols for wireless sensor networks are designed for nodes with one transceiver. Some MAC protocols

[2]This protocol is introduced and called RMAC in [7]. However, in this survey we rename the protocol RMAC-R to distinguish it from the RMAC [18] protocol that will be explained in Section IV.

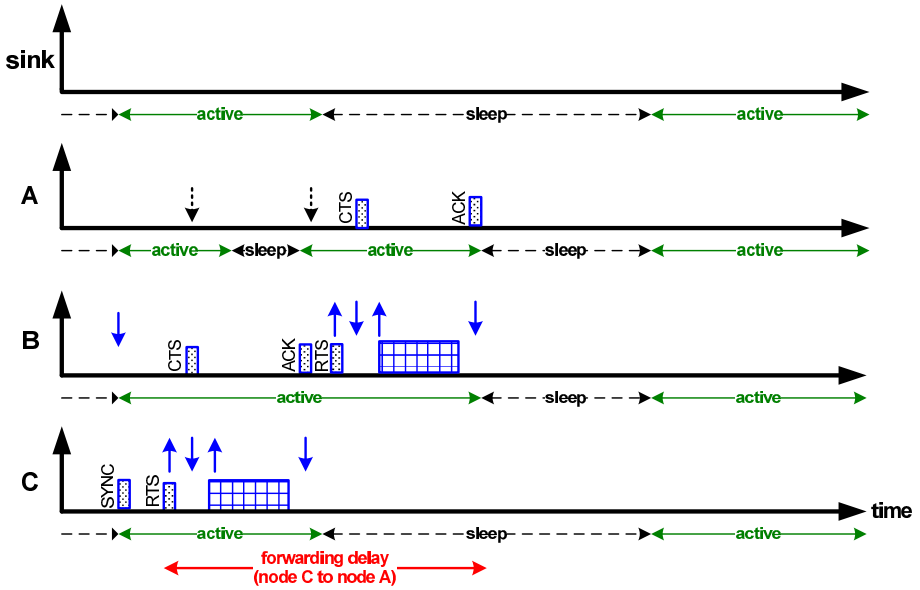


Fig. 5. S-MAC with Adaptive Listening or S-MAC-AL [1] Protocol

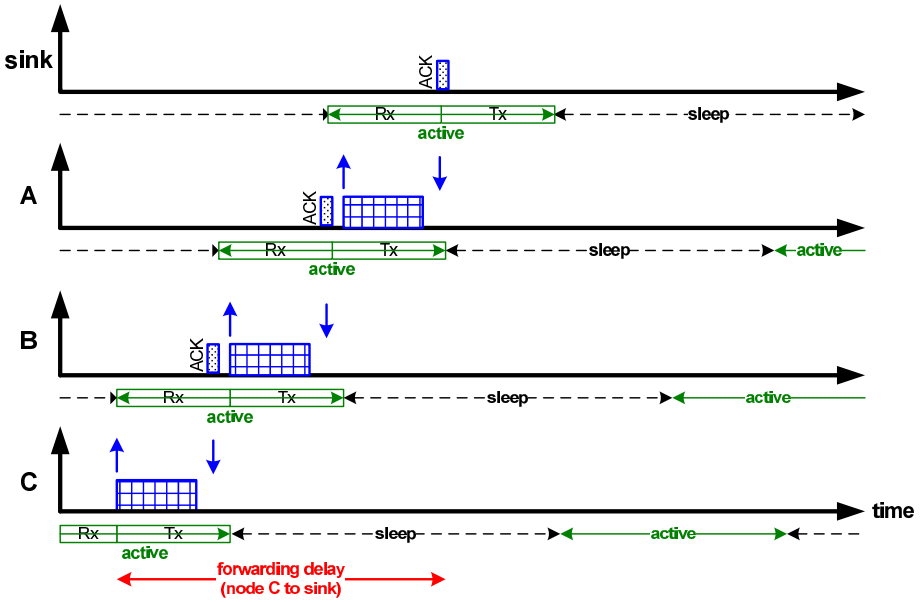


Fig. 6. Skewed Wake-up Schedules in DMAC [4] Protocol

nevertheless assume the presence of additional transceivers as this allows for improving delay performance, and examples of such protocols are discussed next.

A Pipelined Tone Wakeup (PTW) scheme [10] uses two radios: wake-up radio and data radio, to transmit a wake-up tone and transmit data packets, respectively. The wake-up radio adopts a periodic duty cycle and turns on the data radio upon detecting a wake-up tone during its active time. As there is no synchronization among nodes, the wake-up tone needs to be long enough to wake up all nodes within the transmission range of a sending node. At the end of the wake-up tone, the sender transmits a short notification (NTF) containing an intended receiver's identification using the data radio. The notification message allows other receivers to quickly turn off their data radios. The receiver responds with a wake-up procedure to awaken all of its neighbors. For instance, node B transmits a tone on the wake-up or control channel, which is shown as shaded in Figure 7, to wake up all of its neighbors: node A and the sink. By the end of the tone period, these neighbors are awakened and turn on their data radios. Node B then sends the NTF packet via the data channel to indicate that the data packet is intended for node A, and the sink that overhears this NTF packet switches off its data radio. Data reception at node A occurs at the same time as waking up its next hop node. The wake-up pipeline is thus created to reduce a wake-up delay at each hop and improve end-to-end delay. The protocol performs well when the packet size is large enough such that its transmission delay exceeds a wake-up delay. In contrast, if the packet size is small, the wake-up delay remains in this scenario and a reduction of end-

to-end delay becomes limited. However, PTW can achieve a significant improvement regarding end-to-end delay compared to S-MAC.

There is one variant of PTW: LEEM [11], that also utilizes the wake-up radio concept. However, as both PTW and LEEM can *decrease end-to-end delay*, they cannot give delay guarantees as wake-up periods can overlap and contention is not removed. Therefore, they cannot support the target mission-critical applications. In addition, their performance is only evaluated by simulation. Low-power radio hardware has recently emerged (see [45] and [46]) and consequently made implementations of MAC protocols that use a dual radio architecture possible. The platform described in [46] has an extremely low powered wake-up radio which allows the system to keep the wake-up radio always on to reduce wake-up delays significantly. Despite the advantages, the hardware cost of an additional radio must be included in the design consideration.

4) Transmission Scheduling Using Time and Frequency Multiplexing: In contrast to PTW and LEEM, the technique called T-MALOHA in [12] exploits both time and frequency multiplexing. In particular, it is a transmission pipelined multi-channel ALOHA, which is based on the well-known slotted ALOHA protocol. Time is divided into frames, and each frame is further subdivided into a fixed number of transmission slots. Each node uses a single transceiver, but the sink is equipped with m transceivers. These sink transceivers operate at different frequencies and consequently facilitate parallel transmissions from nodes which are assumed to be only one hop away. Compared with traditional frame-based protocols, T-MALOHA achieves a small frame size because of the number of m transceivers and a smaller slot basis due to the transmission pipelining scheme in which the periods of nodes' transmissions over the air are placed immediately one after the other. In particular, while one node is transmitting data over the air, another is preparing to transmit. Besides the transmission pipelining scheme, a node determines whether to transmit a packet in a frame with a pre-defined probability. Having decided to transmit, the node uniformly selects one time-frequency transmission slot in the frame, and at the end of the frame the controller transmits acknowledgments in the acknowledgment slot. This protocol thus can provide *probabilistic node-to-node delay guarantees*.

T-MALOHA [12] is tailored for a discrete control application that requires a bounded delivery time analogous to the time aspect of our mission-critical scenario. The use of multiple transceivers clearly improves throughput and delay since the controller can receive packets from a subset of triggered sensors at the same time over different channels. The work assumes that the maximum number of sensors being triggered is known and utilizes this knowledge to determine if the delivery deadline can be met. The main drawback of this work lies in its support of only a single-hop communication.

5) Transmission Scheduling Using Multiple-Channel Transceivers: As opposed to single channel utilization per transceiver, a recent study proposes a MAC protocol called Alert [13] to exploit multiple channel support in a transceiver. This feature is available in most commercial radio devices, such as the CC2420 radio [47].

Each node is equipped with one such transceiver, and its transmission channel is selected adaptively from the available N channels and independently from other nodes. The channels are associated with different selection probabilities. The protocol assumes that all nodes are time synchronized and that time is divided into smaller slots, named Alert slots. Each Alert slot accommodates one data transmission and its acknowledgement. At the beginning of each Alert slot, a sender chooses a frequency channel randomly based on the pre-specified channel selection probabilities. As shown in Figure 8 a), there are $N = 3$ channels with non-uniform probability distribution to reduce the chance of collision among other senders. In this example, we assume that node A or the sender chooses channels f3 and f2 for transmission in slots 1 and 2, respectively. The sender then switches to the chosen channel, transmits a long preamble (control packet) and a data packet, and finally awaits an acknowledgement. If the acknowledgement is not received, the sender retransmits in the next slot. Simultaneously, a receiver samples the signal level, Received Signal Strength Indicator (RSSI), on each of N channels. Once a high signal level is sensed implying a potential preamble transmission, the receiver terminates the channel sampling and remains active on this frequency channel for possible data reception. Parallel transmissions in different frequency channels occur independently, while the receiver performs its reception in one of these channels. Unacknowledged transmissions continue in the next slot, and the receiver can collect messages from all senders eventually. Figure 8 b) summarizes protocol operations at both sender (node A) and receiver (the sink) sides in which the transmission becomes successful in slot 2.

Alert is designed for an event-driven application in which messages are transmitted very infrequently but must be conveyed to one base station or receiver urgently. Given this assumption, event rarity and message importance, Alert omits any energy-saving technique and trades energy for *decreased node-to-node* message transfer delay. In addition, the protocol currently supports only a star topology in which multiple senders can simultaneously transmit urgent messages to a receiver. As Alert cannot guarantee delay performance, it is not adequate for mission-critical applications. However, based on our observation, this protocol is part of recently increasing efforts to enable prompt data delivery, and thus an improvement could make it able to support mission-critical data delivery.

6) Asynchronous Transmission Scheduling : In the absence of any node coordination, f-MAC [14] achieved *guaranteed node-to-node* delay on data delivery between nodes. In particular, potential receivers listen for incoming packets continuously and, thus, f-MAC does not employ energy saving techniques. A sender repeatedly transmits duplicates of a packet using its specific retransmission intervals such that at least one copy is guaranteed to be received without collision. As the protocol requires no coordination among neighboring nodes, it achieves simplicity. f-MAC operates well in a small network but does not scale to larger networks as transmission

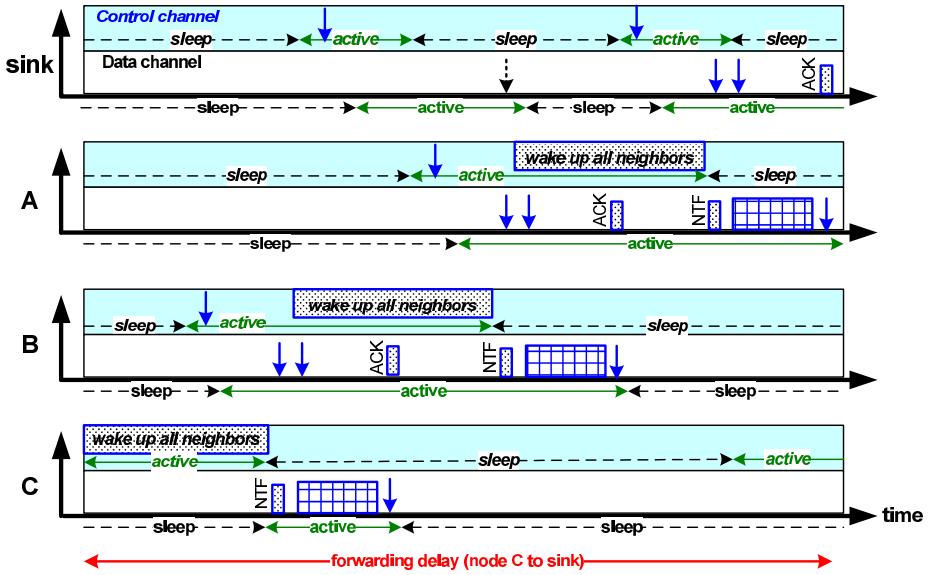


Fig. 7. Adopting Dual Radios in PTW [10] Protocol

delay grows exponentially with the number of nodes. The delay bound is only valid for error-free transmission channels. Hence, adding a reliability scheme to f-MAC could render the protocol applicable for a mission-critical application.

B. Schedule-Based MAC Protocols

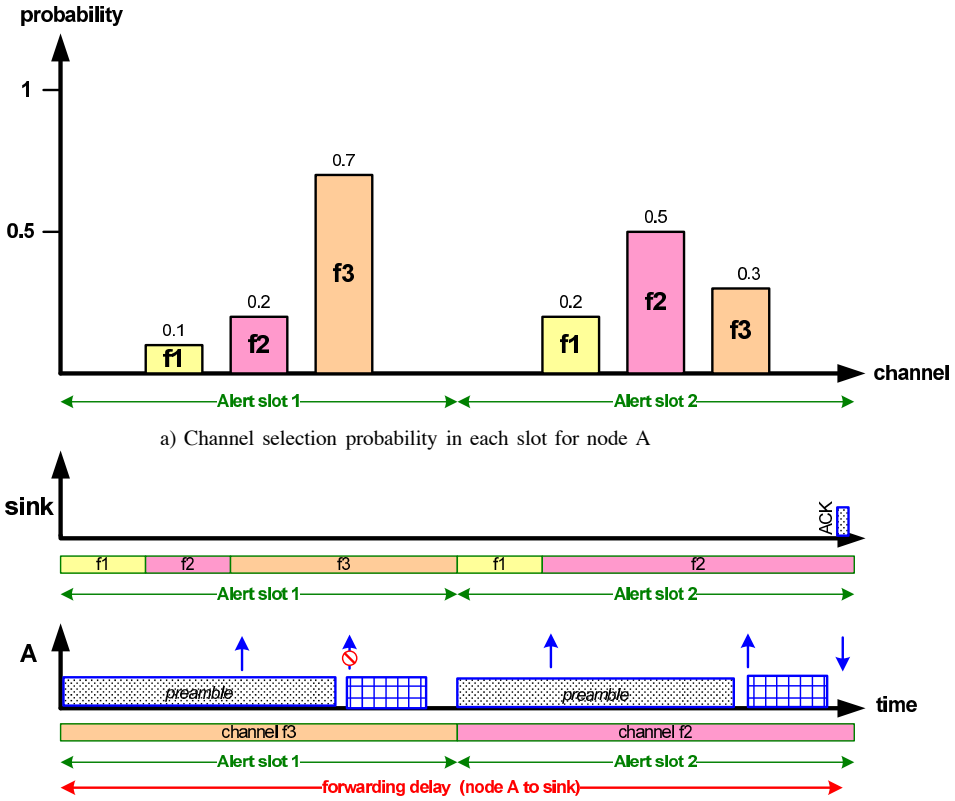
Schedule-based protocols require tight or complete coordination among nearby or all nodes in the network. Most schedule-based protocols adopt the Time Division Multiple Access (TDMA) technique for such coordination. In this technique nodes transmit at dedicated points in time, leading to collision free data delivery and predictable data transfer delays. Therefore, the schedule-based protocols are potentially able to provide a per-hop bound on data transfer delay. Furthermore, it is possible to construct transmission schedules that guarantee end-to-end delay bounds. A selection of notable protocols that can provide such performance bounds is presented next.

1) Transmission Scheduling Using Time and Frequency Multiplexing: Similar to T-MALOHA which is detailed in [12] and previously discussed in this Section, another protocol in the same work uses time and frequency multiplexing. This frequency-time division multiple access (FTDMA) protocol [12], however, employs the schedule-based technique to ensure a bounded delivery time. In particular, time is divided into frames, and each frame is further divided into a fixed number of transmission slots. Each node utilizes a single transceiver, while the sink is equipped with m transceivers to operate at different frequencies and consequently facilitate parallel transmissions from nodes. Furthermore, a node is located one hop away and assigned a unique time-frequency slot within a frame to avoid transmission collision. A traditional TDMA MAC protocol often defines a frame length of n time slots to fairly accommodate transmissions of n nodes in the system. In contrast, a frame duration in FTDMA is reduced by a factor of m transceivers at the sink and by a smaller slot size due to the transmission pipelining.

In the absence of packet losses, all messages arrive at the controller within one frame duration. By contrast, if there are transmission losses, several frames may be required for retransmissions. FTDMA therefore provides *worst-case node-to-node delay guarantees* for its target of discrete control applications. Such delay guarantees enable this protocol to be able to support the timely delivery required by mission-critical applications. However, FTDMA does not scale in a large network as its performance is limited by the number of available frequencies. Addition efforts are also needed to extend this work for multi-hop WSNs, which could support more mission-critical applications.

2) Transmission Scheduling Using Dedicated Hardware: RT-Link [15] is a TDMA-based link protocol adopting a periodic sleep/wake-up schedule. It relies on special hardware for achieving out-of-band and network wide time synchronization. In an active period, the protocol supports two types of slots: Scheduled Slots (SS) and Contention Slots (CS). Nodes operating in SS obtain reserved slots to transmit and receive. On the other hand, nodes transmitting in CS select to transmit randomly as in a slotted Aloha algorithm. These slots provide new nodes an opportunity to join the network. Based on global topology information, the protocol creates a connectivity graph and a collision-free slot schedule. The schedule ensures a node using scheduled slots achieves an *end-to-end delay guarantee* across multiple hops and thus can support mission-critical applications. However, the requirement for out-of-band time synchronization leads to additional hardware cost and limits the application scenarios in which the protocol can be used. For example, the transmitter of the time synchronization signal must cover the whole network area. In addition, absolute global time synchronization might also not be necessary to achieve timely delivery in many application scenarios (see [24], [39]).

3) Transmission Scheduling Using High Power Sink: PEDAMACS [16] addresses the difficulty of developing a



a) Channel selection probability in each slot for node A

b) Data transmission between node A and the sink

Fig. 8. Exploiting Multiple Channel Support in Alert [13] Protocol

TDMA scheme in an unplanned network. The protocol uses a powerful sink to perform tree topology discovery and slot scheduling. The high-power sink can reach all nodes in one hop and thus provides accurate time synchronization. Nodes forward data to the sink in several hops. A node uses a signal-to-interference-plus-noise (SIRN) ratio to determine its parent, neighbors and interferers. Once the sink obtains knowledge of the complete network topology, it creates and broadcasts a scheduling frame that specifies the time slots assigned to nodes. At the beginning of the scheduling frame, each scheduled node generates data packets. PEDAMACS applies a scheduling algorithm ensuring that these packets reach the sink by the end of the scheduling phase. The schedule is also adaptive to topology changes. PEDAMACS gives *end-to-end delay guarantees* in a multi-hop network for each scheduling phase. However, the protocol is evaluated only through simulation. Its assumption about the high-power sink that can directly connect to all nodes may also be problematic in a realistic setting of mission-critical applications. For example, in an office building, there may be many obstacles that hinder the direct signal communication from the sink.

4) Transmission Scheduling Using Multiple-Channel Transceivers: Many recent MAC protocols [17], [42] exploit advanced transceivers capable of providing multiple transmission channels. The previously described Alert [13] protocol, for example, uses multiple-channel transceivers but adopts the contention-based approach. Alternatively, MAC protocols with multiple-channel transceivers can use the schedule-based approach as discussed below.

When a multiple-channel transceiver is used, a set of channels is available for transmission. Therefore, the node coordination must occur not only in the time domain but also in the frequency domain. HyMAC [17] is an example of MAC protocols in this category which combine features of TDMA and Frequency Division Multiple Access (FDMA). This hybrid TDMA/FDMA MAC protocol divides time into fixed-length frames, and each frame is further divided into time slots. These slots are classified as either scheduled or contention. The scheduled slots provide collision-free transmissions, while the contention slots are used to transmit control messages to the base station. Both existing nodes and new nodes include their neighbor lists in the control messages. The base station utilizes these lists to construct a tree topology and a minimum delay schedule for the network by assigning nodes with appropriate time slots and frequency channels. As a result, HyMAC can provide high throughput and *end-to-end delay guarantees*. However, in the case of an error-prone channel which could corrupt data transmission, these guarantees become invalid. HyMAC consequently cannot enable a highly mission-critical application. The protocol also relies on the base station to determine the transmission schedule, and thus this base station is presumably constrained by neither power nor storage capacity. Furthermore, the protocol may incur energy overhead due to control message transmissions.

IV. Reliability-Aware MAC Protocols

The issues of message transfer reliability in WSNs are mostly addressed by transport protocols [50], [51] or routing

protocols [52], [53]. However, there are a few proposals in the literature that investigate reliability solely at the MAC layer. Common techniques used or integrated into the MAC protocols to improve reliability are discussed in this section. It has to be noted that all of these techniques are for unicast traffic in which a packet has a single destination. There are a few studies that address broadcast traffic [38], but they are beyond the scope of this survey.

A. Automatic Repeat Request (ARQ)

Automatic repeat request (ARQ) is an error control mechanism which adopts acknowledgements and timeouts to verify a successful packet transmission. In the case of transmission failure, the protocol attempts a retransmission. RMAC [18] enforces reliability using both implicit and explicit acknowledgements. Following the CSMA/CA approach, this contention-based protocol listens to the channel and uses a back-off period before transmission to lower a collision risk. However, an intermediate node skips this back-off period after packet reception and immediately relays the packet to the next hop. A sender overhearing this immediate forwarding can consequently infer that its transmission to the intermediate node was successful. Such forwarding acts as an implicit acknowledgement to the sender. If no implicit acknowledgement is detected, the sender waits for a back-off period and then retransmits. In contrast to the implicit acknowledgements, the explicit acknowledgement is transmitted by the destination node to acknowledge the multi-hop data forwarding. The implicit acknowledgement not only ensures reliability but also potentially reduces the end-to-end delay as the back-off period suppression creates a pipeline data transmission. Figure 9 presents an ARQ operation of RMAC. For instance, after transmitting a packet to node B, node C overhears this node relaying the packet and thus concludes that its transmission is a success. Besides using acknowledgements, RMAC adopts an adaptive retransmission scheme which adjusts the maximum retransmission attempts based on the packet error rate observed at a node. Furthermore, the protocol introduces the transmission rate control to avoid the hidden-terminal problem. After receiving an implicit acknowledgement, a transmitting node refrains from data transmission for twice the communication delay between two nodes. Therefore, the transmission rate control scheme decreases the collision probability. Although RMAC represents an improvement of a CSMA/CA protocol in terms of both delay and reliability, the performance gain cannot be guaranteed. RMAC may not be a suitable candidate for applications with a strict reliability requirement as it can only *increase node-to-node reliability*.

B. Multiple Channels/Transceivers

Retaining most of RMAC's fundamentals to obtain link reliability, E2RMAC [19] augments RMAC [18] with an energy saving technique using a dual radio concept. The additional radio is used to increase energy efficiency and reliability. Similar to the primary data radio, the low-power radio also employs a carrier-sense and back-off scheme to reduce collisions. When a node has a packet to send, its low-power radio transmits a tone after a random back-off period to inform all neighbor nodes to switch on their data radio. If the wake-up channel is unavailable, the node determines a back-off period and sleeps before repeating the procedure. Otherwise, the node switches on the primary radio and senses the channel before transmitting first a filter packet. The filter packet contains a destination address that enables the intended recipient to remain active and other neighbors to switch off the data radio. As a result, energy is conserved, and *node-to-node reliability* is increased. E2RMAC nevertheless fails to provide any guarantees on reliability as needed for highly mission-critical applications.

Transmitting packet replicas, as seen in the retransmission part of the ARQ approach, is a common technique to enhancing reliability. Based on this technique, one possible idea is to use multiple transceivers to create parallel transmissions from one source. The multi-transceiver method allows packet replicas to be transmitted simultaneously over several channels and thus increases the probability of packet reception. Despite its promising reliability improvement, the parallel rendezvous might have been deemed neither economical nor practical as it is not implemented much in the WSN literature.

In contrast to the multi-transceiver method, a single radio whose communication jumps from one frequency channel to another can be used to increase reliability. This frequency-hopping scheme combats interference stemming from other communications sharing unlicensed frequency spectrum. The scheme was initially designed for the mobile ad-hoc networks field [73], [74], which is related to the WSN area. Additional modification is therefore needed to extend its usage to WSN applications. Nevertheless, it has to be noted that a few studies in this review utilize the frequency channel shifting but not explicitly to enhance reliability against channel fading and interference. For example, Alert [13], which is described in Section III, uses this frequency shifting to primarily enable simultaneous transmissions for the delay reduction instead of the reliability improvement. Alert is thus discussed in the delay-aware protocol category rather than here.

C. Multiple Transmission Paths

A family of protocols in [20] is proposed to reduce collision when transmitting broadcasts; we refer to these as Back-off Algorithms for presentation in the survey. Each proposed protocol defines a random back-off scheme according to specific network characteristics and conditions. Besides introducing a random delay before a broadcast, a routing protocol called Probabilistic Forwarding Protocol (PFR) is used to forward packets towards the sink. The combination of multi-path forwarding and tailored back-off schemes can be used within a MAC protocol to increase the chance of end-to-end packet delivery. This work appears simple as there is little overhead in node coordination and hardware. However, this advantage may be outweighed due to the energy waste for multi-path transmission as the knowledge of transmission success is not shared. Furthermore, the back-off delay needs to be chosen properly to lower the collision probability while simultaneously delivering an acceptable delay. In an extreme case, the multi-path technique in this work may trade delay for reliability resulting in unfavorable performance for a mission-critical application. Consequently, the work in [20] might be

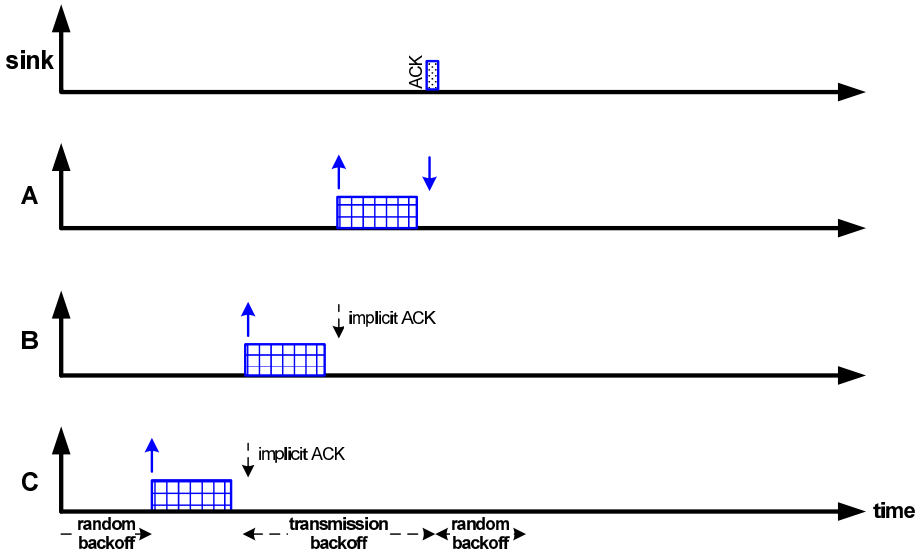


Fig. 9. Exploiting Implicit ACK in RMAC [18] Protocol

useful for scenarios where time and reliability requirements can tolerate some performance variations because it is able to *improve end-to-end reliability*.

D. Transmission Power Control

An increase in transmission power can overcome channel noise and thus achieve a higher probability of successful data transmission. Motivated by this fact, a proper power control scheme can be integrated into a MAC protocol to lower energy consumption and to reduce packet loss rates [72]. Adaptive Transmission Power Control (ATPC) [21] correlates transmission power and link quality. In addition, a feedback loop is applied to dynamically adjust the power required to maintain individual link quality over time. The power control topic is not new in the WSN literature as it can mitigate energy expenditure while preserving basic performance metrics, such as connectivity and throughput. ATPC stands out from other power control techniques because of its individual reliability support for each packet transmission. As a result, ATPC is able to *improve node-to-node reliability* but may not be adequate to support mission-critical applications. It has to be noted that although existing power control techniques provide promising benefits, their design and implementation could be complex. For instance, the code size and processing time of ATPC might pose problems when it is integrated with time-critical MAC protocols. In practice many MAC protocols would not adopt a power control technique but assign all nodes with the same transmission power to achieve simplicity instead.

V. Delay-and-Reliability-aware MAC Protocols

The previous two sections discuss MAC protocols and complimentary techniques that focus on either delay or reliability as an absolute. The following presents a review of several studies that treat both issues together. To achieve the dual objectives, most protocols in these studies span both routing and MAC protocols. The number of these protocols is small, and they appear to be able to serve mission-critical applications. Hence, in contrast to the protocols in the previous two sections, we list and discuss them in more detail.

A. MMSPEED

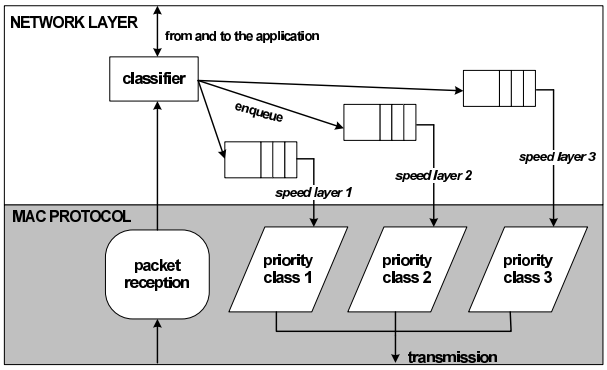
The work in [22] presents a packet delivery mechanism called Multi-Path and Multi-SPEED Routing (MMSPEED) protocol that provides service differentiation and probabilistic guarantees in terms of data transport delay and reliability as described below.

To obtain the traffic differentiation and timely data delivery, MMSPEED extends across both network and MAC layers as depicted in Figure 10 a). The network layer adopts localized geographic routing and a classifier to isolate packets into different speed layers, while the MAC layer provides a prioritization service to accommodate the classifier. These multiple speed layers are implemented across the network in order to provide network-wide speed options. Based on the content of the sensor data, a source node selects an appropriate end-to-end deadline $Treq$. Since geographical distances among nodes are assumed to be available, the source node can determine the distance $Dist$ to its final destination node and thus the minimum speed required to forward a packet $Sreq = Dist/Treq$. The packet is placed into the speed layer S_l such that $S_l = min_{i=1}^{L}\{S_i \mid S_i \geq Sreq\}$, where L is the total number of speed layer options. Subsequently, the packet is sent to a neighbor node whose estimated progress speed to the destination is higher than S_l. If the neighbor node successfully receives the packet, it calculates and updates the remaining time of the deadline $Treq'$. The node also uses this new deadline to determine if the speed layer S_l needs to be changed to compensate for potential delays, which could have occurred after the packet has travels several hops. This dynamic compensation and the network-wide speed options help enable timely delivery; a packet that reaches its destination is likely to meet its deadline. However, the timely delivery is not always guaranteed as some packets are discarded when their set speed layer S_l cannot be supported. A mechanism to address this packet loss is explained next.

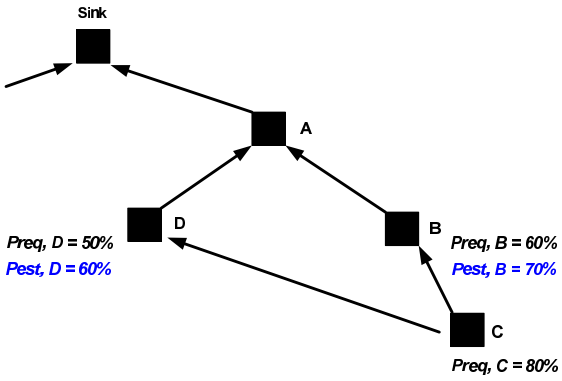
To achieve the reliability goal, MMSPEED adopts the probabilistic multipath forwarding approach. In this approach, each packet is broadcast to a set of neighbors whose forwarding contribution to the total end-to-end reliability is greater than or equivalent to the required reliability. Figure 10 b) illustrates this forwarding concept in which node C must send a packet to the sink with the end-to-end reliability of $Preq, C = 80\%$; the end-to-end reliability is defined as the end-to-end reaching probability of a packet. Suppose that this source node selects to forward the packet to two neighbors: node B and node D, based on its local estimation of the end-to-end reliability: $Pest, B = 70\%$ and $Pest, D = 60\%$, respectively. The total end-to-end reliability via these two nodes is calculated as $1-(1-Pest, B)\cdot(1-Pest, D) = 88\%$, which exceeds the required reliability $Preq, C$. In addition, the source node specifies the expected probability of delivery for each packet in relevance to its content. For instance, the receiver nodes: node B and node D, are assigned with the required reliability $Preq, B = 60\%$ and $Preq, D = 50\%$, respectively. This assignment ensures that the packets from node C will be forwarded further with the required reliability of $1 - (1 - Preq, B) \cdot (1 - Preq, D) = 80\%$.

MMSPEED utilizes the network-wide speed options to achieve the timeliness goal and concurrently uses reliable multicast for parallel packet transmissions to address the reliability issue. In particular, as described above, a packet is first associated with an appropriate speed layer S_l based on its end-to-end deadline and geographical distance to the final destination. The packet is then sent via multicast service to multiple forwarding nodes among those with the progress speed higher than S_l such that the total end-to-end reliability is at least the required end-to-end reliability. It is important to emphasize that using the multicast service at the MAC layer ensures parallel transmissions along multiple paths, and consequently each copy of the packet can meet the end-to-end deadline. In addition, since each copy progresses in parallel and its progress speed is supported by the described network-wide speed options, the copy that finally arrives at the destination can meet the deadline with a *high* probability (see [22] for more details on this claim).

The main advantage of MMSPEED is the service differentiation, which renders it suitable for mission-critical applications with mixed periodic and aperiodic traffic. However, the flexibility in supporting diverse requirements comes at the price of *probabilistic end-to-end* guarantees in both the time and reliability domains, instead of worst-case guarantees which may be required in some stringent mission-critical scenarios. In addition, this work does not include the issue of power consumption in its scope, and thus further investigation is needed to address the impact of energy-saving techniques, such as radio duty cycling, on the achieved delivery performance.



a) Protocol structure at each node



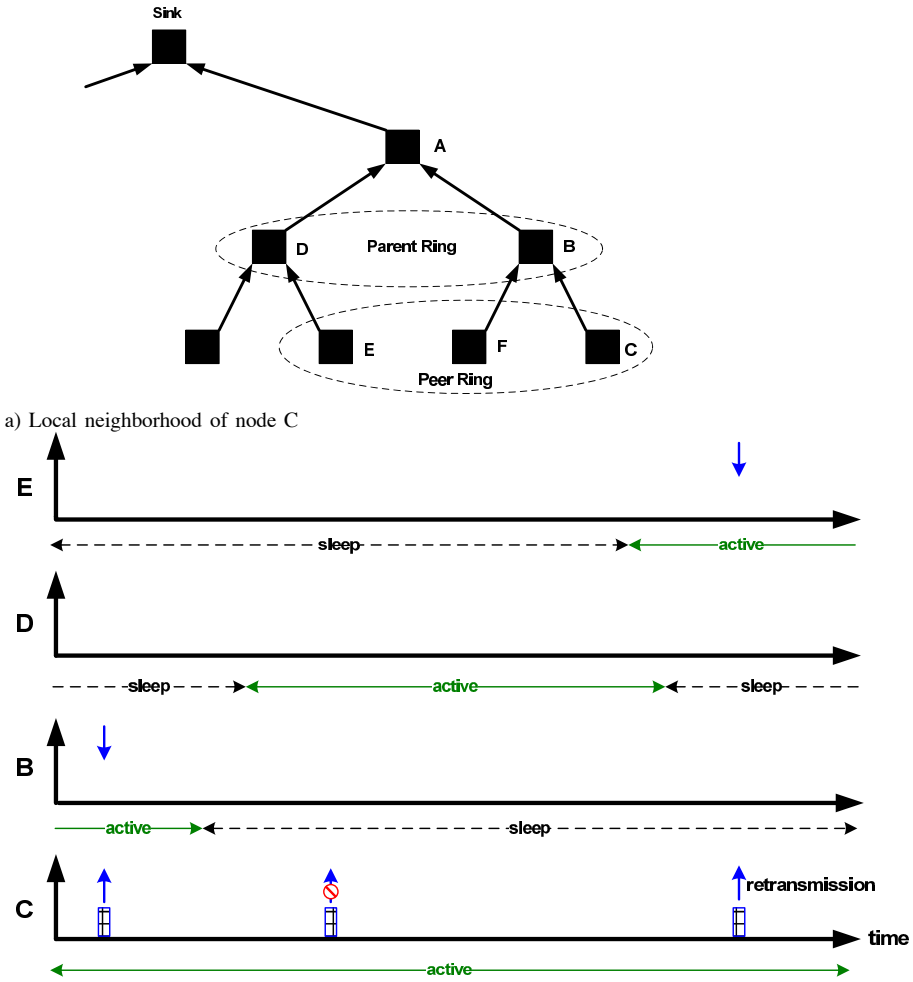
b) Multipath forwarding

Fig. 10. Traffic Differentiation in MMSPEED [22] Protocol

B. Dwarf

In contrast to MMSPEED which lacks an energy preservation technique, Dwarf [23] addresses energy efficiency in addition to data transport reliability and delay. Dwarf uses unicast-based partial flooding, which limits the degree of transmission redundancy to preserve energy while maintaining reliability. All nodes are categorized into rings based on their distance to the nearest sink, and thus the nodes with the same distance are defined as being in the same ring. The neighbors of a node are divided into: parents, peers, and children. To illustrate this neighborhood definition, we add three node identifications in the reference topology, which is shown in Section II. As a result, Figure *11* a) depicts node C with 2 parents (B and D), 2 peers (E and F), and no children. In this example, node C can transmit to these nodes in the defined rings, and its routing is not restricted to the tree structure, which is shown for consistent comparison with other protocols. A node sends a new message to a number of k parents and peers. The selection of these parents and peers depend on their wake-up times in order to decrease end-to-end delay. In addition, all parents must be considered being one of the k forwarding neighbors before the peers are.

In the case of transmission failure, a packet is retransmitted up to k' times, and thus this scheme results in a maximum of $k + k'$ transmissions per message. Furthermore, the packet is sent to a different forwarding neighbor, which is selected according to the level and wake-up time of the neighbors. As a result, each retransmission is also treated in the fastest way possible. A forwarding example of node C when $k = 2$ and $k' = 1$ is shown in Figure *11* b). In this scenario node C forwards a message to the parents B and D based on their wake-up times. Moreover, as the transmission to node B failed, node C retransmits to the peer E. Note that in Figure *11* b) we only show the data transmission, while the transmission of control packets is omitted.



a) Local neighborhood of node C

b) Transmission of node C when $k = 2$ and $k' = 1$

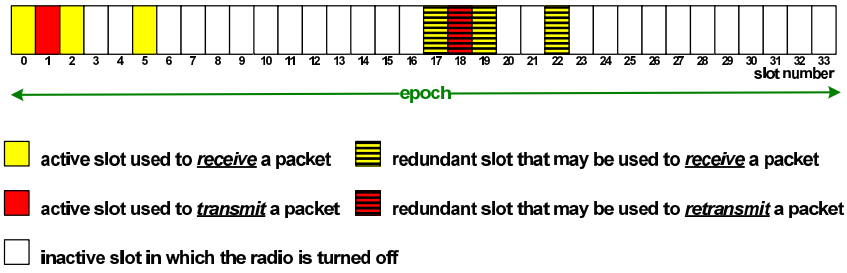
Fig. 11. Unicast-based Partial Flooding in Dwarf [23] Protocol

Furthermore, the forwarding scheme in Dwarf is actually combined with an enhanced version of the WiseMAC [41] protocol, which uses the preamble sampling technique. In this technique, a node transmits a preamble or control packet for a duration that ensures that the periodically listening receiver will eventually receive the preamble, and then the data transmission begins. The enhanced MAC protocol in this work follows this technique but exploits knowledge of neighbor' sampling schedules to minimize wake-up preamble length. In addition, the modification includes an API for querying this knowledge as the wake-up times of neighbors are needed during node forwarder selection. As Dwarf aims for the fast and robust delivery required in a safety-critical system, attention has been placed more on reliability than delay. This protocol achieves a reliable data delivery with *low* end-to-end latency and *low* energy consumption. Therefore, further improvement is needed to make it suitable for mission-critical applications.

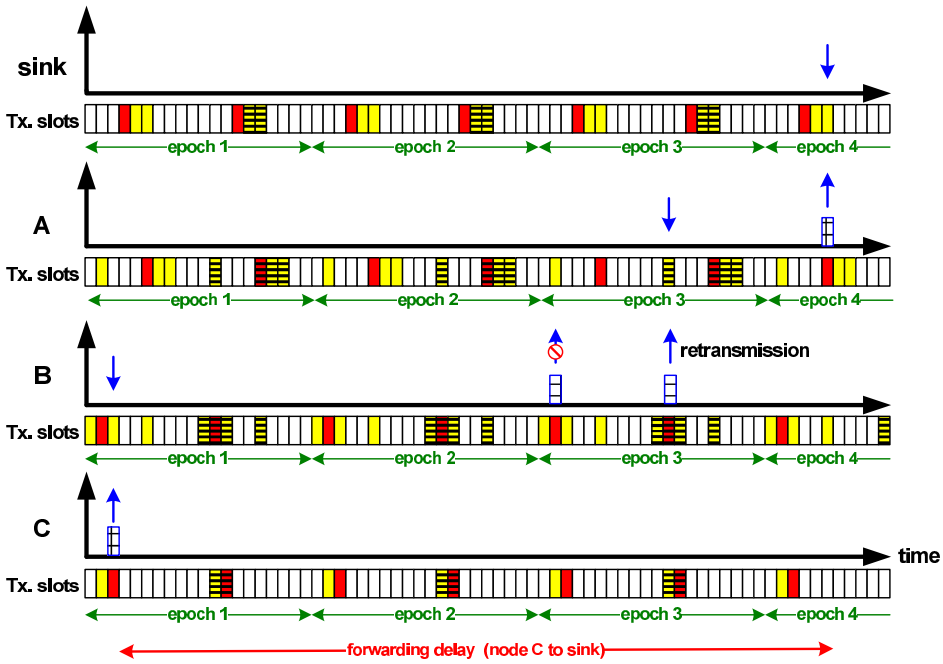
C. QoS-MAC

Unlike MMSPEED and Dwarf, the work detailed in [24] addresses delay and reliability at the node-to-node level; we call this work QoS-MAC based on its aim of supporting Quality of Service (QoS) in terms of message transfer delay and reliability. QoS-MAC is a TDMA-based MAC protocol that also provides routing. It assumes a tree topology with a sink at its root and a network of at most n nodes. The time axis is divided into fixed-length base units called epochs, and each epoch is subdivided into $k \cdot n$ time slots. Figure 12 a) exemplifies an epoch of node B in the topology shown in Figure 2 a) when $k = 2$ and $n = 17$; slots that may become active in case of packet loss are shown as striped. The value k is determined depending on reliability requirements of the application and the worst-case channel model assumed or estimated during pre-deployment. A node can transmit one message per epoch but has k exclusive transmission chances to successfully achieve that. As a result, QoS-MAC can ensure an upper bound for the node-to-node message transfer delay, which is influenced by the epoch length E. The protocol also provides a lower bound for the node-to-node message reliability required by its application. The performance guarantee is achieved only in the case of data traveling from sensor nodes toward the sink because QoS-MAC employs simple routing that gives a preferential treatment to data in the up-tree direction.

As QoS-MAC can provide the *node-to-node guarantees* of data delivery in both the delay and reliability domains,



a) Slot usage of node B when $k = 2$ and $n = 17$



b) Potential data transmission from node C to the sink

Fig. 12. QoS-MAC [24] Protocol

it can effectively enable a mission-critical application that requires a single-hop network. However, many mission-critical applications are likely to be supported by a multi-hop network, and this protocol alone cannot serve such applications. Figure 12 b) depicts one possible packet forwarding in which QoS-MAC achieves the node-to-node delivery guarantees but unpredictable end-to-end performance. Due to space limitation, the TDMA schedules with transmission (Tx.) slots in this figure are not shown in detail, and the epoch length E is not of an actual size. However, Figure 12 b) suffice to demonstrate the relevant components of the forwarding. In the illustration node C successfully transmits its packet to node B in epoch 1. The packet is then enqueued at node B and forwarded in epoch 3. The packet forwarding from node B to node A is successful at the second transmission attempt ($k = 2$), and the packet finally reaches the sink, which is the final destination, at epoch 4. In this example, the packet is reliably delivered to a next-hop node within one epoch, and the end-to-end delay is approximately three epochs as there is only a queuing delay of 1 epoch at node B. The end-to-end delay could, however, have been higher when there is a high queuing delay at node B or other intermediate nodes. In the presence of queuing delays, QoS-MAC cannot guarantee an end-to-end delay bound. Nonetheless, if this protocol is integrated with, for example, an analytic tool such as the Sensor Network Calculus [40] that uses node-to-node delay guarantees as one input, it is possible to determine the worst-case value of end-to-end delays. QoS-MAC in combination with an analytical tool is then able to support mission-critical applications in a multi-hop network setting. Such integration represents a modular solution that achieves simplicity in comparison with the protocol alternative, which includes an end-to-end performance analysis to produce a complete but potentially less flexible solution. Examples of this alternative are Burst [26] and GinMAC [27] which will be explained subsequently in this section.

D. WirelessHART

WirelessHART [25] is the first open wireless standard and a wireless mesh network technology for process automation applications. In its architecture, the three principle elements are the network manager, gateways and field devices (nodes). Figure 13 depicts a basic WirelessHART network. The network manager performs network configuration, scheduling communication between devices, and monitoring network status.

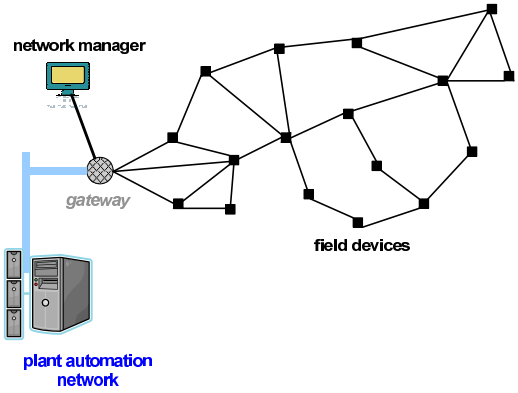


Fig. 13. Elements in a Typical WirelessHART [25] Network

Gateways enable communication between host applications and field devices that are connected to process equipment. WirelessHART is designed to largely represent all layers of the OSI communication stack. Here we focus only on its MAC protocol and reliability schemes that are responsible for timely and reliable data delivery. The MAC protocol, which is based on Time Synchronized Mesh Protocol (TSMP) [34], combines the TDMA and FDMA techniques. Additionally, the network manager specifies a time slot and frequency channel for a communication link between two field devices. The specification enables collision-free and deterministic communication, and therefore WirelessHART can *guarantee* end-to-end delay.

In addition, WirelessHART uses several features to *improve* end-to-end reliability. For instance, the channel hopping technique, which is integrated with the MAC protocol, enhances transmission reliability as frequency diversity is achieved. WirelessHART also introduces the concept of channel blacklisting in which the frequency channels that are affected by consistent inferences are recorded and not used. Furthermore, as WirelessHART uses a full mesh network, its network consists of multiple redundant communication paths. Such redundancy allows packets to be routed around physical obstructions or interference, and thus reliability can be significantly increased in a well-formed mesh network. The MAC protocol of WirelessHART also employs retransmissions to improve reliability and in most cases can retry in the next time slot or the one following.

WirelessHART can guarantee end-to-end delay and improve end-to-end reliability. Hence, it can serve some mission-critical applications that impose time restrictions on data delivery but tolerate some packet loss. The delivery performance of WirelessHART essentially depends on its network manager component, whose important tasks include generating routes and network-wide transmission schedules. WirelessHART thus is a centralized solution with complexity and communication overheads introduced by this network manager. Moreover, as all details of how to implement the network manager are not specified [29], various designs of this manager are possible. For instance, the network manager can produce different routes depending on the selected goals, such as load balancing or average delay. As a result, further investigations and performance assessments may be essential to help enable WirelessHART to support more mission-critical applications.

There are other on-going efforts [32], [33] to develop wireless standards for industrial applications [59] similar to WirelessHART. However, additional work is required to address their shortcomings before a successful deployment in the mission-critical area is possible. For instance, a recent study in [31] presents an evaluation of a MAC protocol [32] that is currently in the standardization process to become the IEEE 802.15.4e standard [30], which supports real-time communication in low-rate Wireless Personal Area Networks (WPANs). This evaluation illustrates that the protocol can provide a delay guarantee for a star network with an approximate size of $n \leq 24$ nodes, but the essential issue of reliable transmission is still under investigation [31].

E. Burst

A recent study [26] presents a static scheduling algorithm that achieves both timely and reliable data delivery, and for presentation in this survey we call it Burst. The study assumes that a network topology is available and a deployment can be planned. Prior to an actual network deployment, measurements were conducted over a period of 21 days to characterize transmission links by their maximum burst length $Bmax$ and interference from other links. The new metric $Bmax$ captures the stationarity of link quality better than the packet reception rate (PRR), which has been commonly used in many studies. Furthermore, Burst assumes that a set of periodic streams is given. This algorithm calculates and ensures an upper bound of the end-to-end delay for each stream by taking account of $Bmax$ and link interference. In particular, it allocates sufficient transmission slots for each link to effectively overcome the link burstiness and interference problems; additional slots are assigned for potential retransmission. The algorithm also selects a least-burst-route that minimizes the sum of $Bmax$ over all links in the route.

Burst achieves *end-to-end guarantees* of data delivery in both the delay and reliability domains, and therefore it can support a mission-critical application. The algorithm is one of the few efforts that result in a WSN providing reliable transmission within latency bounds. This success largely depends on the empirical data collected over an observation period to characterize the link quality and subsequently to devise a network-wide transmission schedule. Hence, a careful network planning is required before an actual deployment. This requirement might first appear as a limitation of the Burst algorithm if compared with many early WSN applications which exploit a fast and random network deployment, especially those applications in the area of environmental monitoring [60]. Nevertheless, some WSN applications are designed for industrial process monitoring, and in such a case pre-deployment measurements in production plants are practical. In addition, the proper network planning could allow, for example, constructing an optimal topology with good link quality and consequently improving transmission reliability.

F. GinMAC

Another recent work called GinMAC [27] can deliver data in a timely and reliable manner, and its design principles are similar to Burst [26]. This protocol aims to support a

control loop in an industrial process automation system. In such a setting, sensor data must be forwarded to the sink within a time bound, and similarly a command from the sink must be transported to an actuator by a deadline. To meet these strict requirements, GinMAC encompasses three features: off-line network dimensioning, an exclusive TDMA schedule and delay conform reliability control. Firstly, in the off-line dimensioning process, application traffic, channel characteristics and a tree topology are defined. Pre-deployment measurements are also carried out to determine the worst-case burst length $Bmax$ of all transmission links, which is the previously described metric of the Burst algorithm. Secondly, the TDMA schedule, which is the output of the dimensioning process, contains exclusive transmission slots for each node and has a fixed epoch[3] length E. Within this length, each node can forward one message to the sink, and the sink can transmit one message to each actuator. Finally, based on the observed channel characteristics, redundant transmission slots are added in the frame for reliability control without violating the calculated delay bound of E. These redundant slots are used to enhance reliability via two methods. The first one is to create temporal transmission diversity by retransmitting a packet if there is loss. The second one is to achieve temporal and spatial transmission diversity by transmitting duplicates of a packet to another m disjoint tree topologies.

Figure 14 presents in detail how GinMAC ensures *end-to-end guarantees* of both delay and reliability while simultaneously achieving energy efficiency; only the uplink traffic is presented here. The network is dimensioned to support a topology of at most $n \leq 15$ nodes as shown in Figure 2 a). The figure illustrates the forwarding of a packet from node C to the sink and the TDMA schedules of all nodes in the packet path. Each node can transmit its data at most one packet per frame and must forward all packets received from its child nodes within one frame. Therefore, the number of transmission (Tx.) slots assigned to a node depends on its location in the tree topology. For instance, node C needs 1 transmission slot as it is a leap node, whereas node B requires 3 slots to support its own packet and the traffic from 2 child node. Furthermore, the reliability control method in this illustration aims for the temporal transmission diversity. The redundant transmission slots, which are depicted as striped in Figure 14, are determined according to $Bmax$ and added in the frame. All transmission slots of a node are also located after the slots used by its child nodes, ensuring uplink data can travel to the sink within one frame. When a slot is not used for transmission or reception, a node switches off its radio to preserve energy.

Although GinMAC can support mission-critical data delivery, it has some limitations. For example, the protocol is tailored for a control loop setting in which sensor data must be forwarded to the sink, resulting in a convergecast traffic pattern. Some mission-critical applications, such as battlefield tracking, may create different traffic patterns and thus cannot be supported by GinMAC. Furthermore, as GinMAC is a TDMA-based protocol with exclusive slot usage, it is suitable for a dense and relatively small network. In order to remove this scalability restriction and enable a broader set of mission-critical applications, additional work is required.

[3]The term *frame* is used in the original GinMAC description [27] but is renamed epoch here so that we can effectively compare GinMAC with other similar protocols, such as QoS-MAC [24].

The first four protocols discussed in this section represent decent effort to enable mission-critical applications although each of them may pose some limitations. For instance, QoS-MAC can ensure message transfer delay and reliability only at the *node-to-node* level and thus requires further investigation to achieve the end-to-end performance guarantee for a multi-hop network. Moreover, Dwarf can *decrease* end-to-end delay and *increase* end-to-end reliability, while WirelessHART can only *guarantee* end-to-end delay but not end-to-end reliability. MMSPEED also delivers an *end-to-end guarantee* in both the time and reliability domains, but only *probabilistically*. Consequently, these protocols may not support highly mission-critical applications. In contrast, the last two studies: Burst and GinMAC, can enable these applications, but they also have some drawbacks and could be improved in the future. Consequently, the area of MAC protocols for mission-critical applications has not matured yet, and some open issues and potential research directions are described in the next section.

VI. Findings and Future Directions

In this section, we summarize key features of the reviewed protocols and reiterate whether these features could render them suitable for mission-critical applications. Open research problems and future directions are also provided.

A. Summary of Findings

All contention-based protocols intend to *decrease* delay. Using a staggered transmission schedule, as in DMAC, along a forwarding path represents the most effective approach to lower delay. However, this technique can only decrease end-to-end latency and provides no guarantees on a worst-case bound of delivery time. Furthermore, potential packet losses and necessary retransmission times are ignored in the design of these protocols. Only T-MALOHA and f-MAC can provide *probabilistic* and *worst-case* delay guarantees, respectively. However, their delay guarantees cannot be achieved in the presence of a lossy channel. In addition, T-MALOHA supports only a star network, and f-MAC does not scale to large multi-hop networks.

Schedule-based protocols can potentially provide a node-to-node bound on data transfer delay, and some of them construct transmission schedules that guarantee end-to-end delay bounds (for example, PEDAMACS and HyMAC). Nevertheless, despite achieving the delay guarantee, some schedule-based protocols make assumptions regarding deployment which could be impractical. For example, PEDAMACS utilizes a high-power sink to perform network-wide synchronization in one hop. Finally, all schedule-based protocols ignore the presence of error-prone channels in their design, and the worst-case delay bounds that they provide do not take error control measures into consideration.

MAC protocols cannot be used for mission-critical applications if they do not address potential packet losses. It is not useful for mission-critical applications to receive data in time while suffering high loss rates. The review therefore investigates techniques used to enhance the reliability of

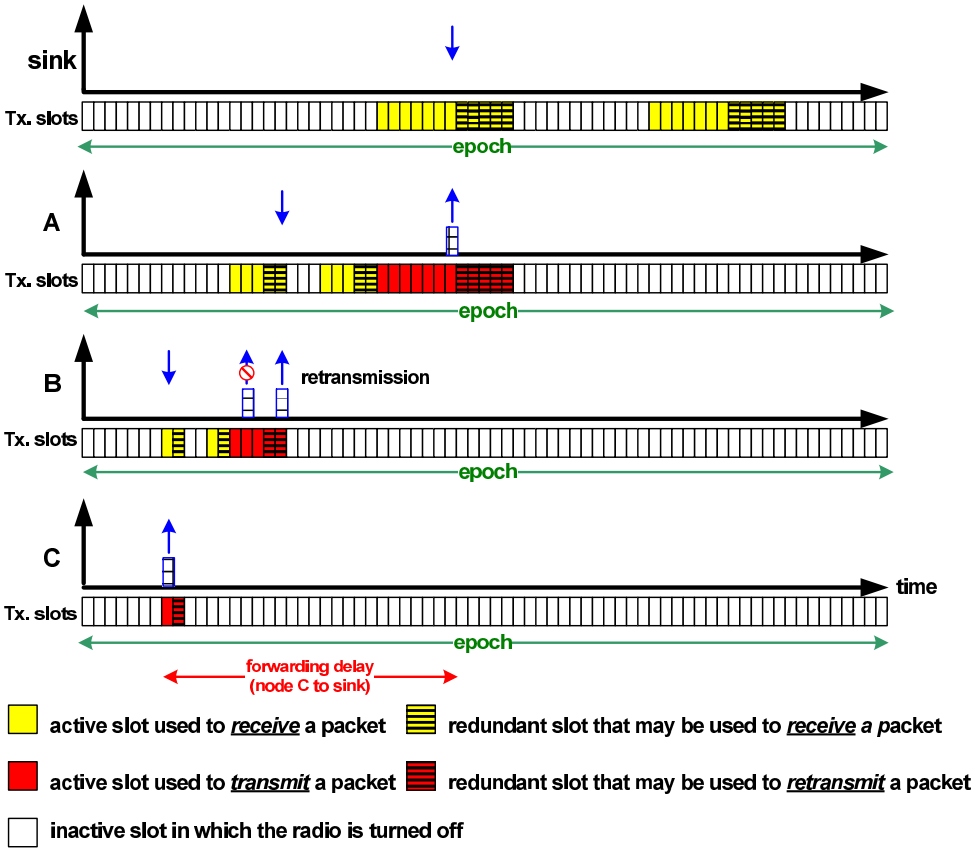


Fig. 14. GinMAC [27] Protocol

MAC protocols. Compared to energy-efficient and delay-aware MAC protocols, reliability-aware MAC protocols are in a minority. They utilize techniques such as ARQ, multiple channels/transceivers/paths and power control to improve reliable delivery. However, none of them offers a worst-case guarantee on reliability.

Surprisingly, little research that addresses both delay and reliability performance objectives together exists. Here we revisit a handful of the studies with these dual objectives. Dwarf routes packet replicas through a set of nodes that display fast delivery potential in terms of wake-up time and distance to the sink. Dwarf thus represents a best-effort solution for mission-critical data delivery as it cannot provide any hard guarantees on latency and reliability. MMSPEED uses a set of different network-wide speed layers to differentiate services meeting various traffic demands, and thus it provides probabilistic guarantees in both timeliness and reliability. QoS-MAC can ensure message transfer delay and reliability only at the node-to-node level, but an additional analytical tool, such as Sensor Network Calculus [40], would be required to provision a network for an end-to-end delay bound. WirelessHART is able to schedule transmission flows such that delay bounds are achieved and reliability is improved. However, WirelessHART has drawbacks such as the complexity of using a central network manager. Only Burst algorithm and GinMAC protocol can deliver the delay and reliability bounds for mission-critical applications.

In summary, the survey has demonstrated that few protocols are capable of ensuring the delivery performance in both the delay and reliability domains [26], [27]. It has also revealed that most available WSN MAC protocols are unsuitable for most mission-critical applications for the following reasons:

- The majority of the delay-aware MAC protocols aim to decrease end-to-end delay and cannot guarantee the worst-case transport delay.
- The few delay-aware protocols that can provide worst-case delay guarantees overlook the nature of an inherently error-prone channel [15], [16], [17]. As a result, only packets that are not lost during transmission can be guaranteed to arrive in time, while corrupted packets may arrive after the delay guarantees or not at all.
- A small number of protocols can give performance guarantees on a node-to-node level, but it is unclear how to they could be enhanced to deliver the end-to-end guarantees for multi-hop networks [12], [14].
- Some protocols make assumptions about operating conditions that will likely be found in few application scenarios. For example, unrealistic assumptions regarding topology, traffic patterns or available hardware are often made in their protocol design [16].
- All reviewed protocols except WirelessHART are based on academic or theoretical studies and thus might not be suitable for deployment in real application scenarios.

B. Graphical Interpretation

Furthermore, we present the findings of this survey graphically and follow three steps to achieve this presentation.

Firstly, the delay and reliability performance objectives of each protocol are assigned to the x-y coordinates shown in Table II. Secondly, the protocols that have the same x-y coordinates are grouped together, resulting in groups A to L as illustrated in Table III. Finally, each protocol group is mapped onto the application classes that are introduced in Section II. The result of this mapping process is displayed in Figure 15, indicating which MAC protocol group is useful for which application class. This graphical summary greatly simplifies the survey results and excludes the energy issue, which can be addressed after the timely and reliable data delivery is achieved. To judge and compare the capabilities of particular MAC protocols in detail, we recommend using Table I in addition to the graphical summary. Next, we elaborate how the surveyed MAC protocols are grouped and how they obtain their position in the graph shown in Figure 15.

The scales of both x and y axes in Figure 15 range from 0 to 1, signifying the performance demands of an application. For instance, the value 0 represents absolute performance relaxation or absence of any performance requirement, while the value 1 indicates absolute performance guarantees which are required by the application. Therefore, at the point $(1, 1)$ the application requires that data delivery is absolutely guaranteed in both the time and reliability domains. A MAC protocol that does not address the delay and reliability objectives is placed at $(0, 0)$. Such a protocol can support *delay-tolerant and loss-tolerant* applications but is far from being able to support either *delay-intolerant* or *loss-intolerant* applications. Likewise, MAC protocols that aim to improve delay and/or reliability performance on either a node-to-node or end-to-end level can still support only *delay-tolerant and/or loss-tolerant* applications. We assign values of 0.125 or 0.25 to map these protocols to Figure 15 (see Table II for more details). MAC protocols that provide probabilistic guarantees on a node-to-node level are mapped using a value of 0.375, and similarly they can support *delay-tolerant and/or loss-tolerant* applications. In contrast, MAC protocols that achieve (worst-case) guarantees on a node-to-node level are mapped using a value of 0.5. Such protocols can be used in principle for *delay-intolerant and/or loss-intolerant* applications, but additional analytical tools are essential to further determine their end-to-end performance bounds. Furthermore, protocols that provide probabilistic end-to-end guarantees are mapped using a value of 0.75 as many mission-critical applications could be implemented with this support. Finally, MAC protocols that are able to give guarantees on an end-to-end level are mapped using a value of 1. These protocols can enable *delay-intolerant and/or loss-intolerant applications* with stringent performance demands.

It is important to note that the above mapping is just one interpretation of the results. Therefore, other x and y values could certainly be used to quantify the performance of the reviewed protocols. However, we believe that the given mapping is reasonable as the surveyed protocols are mapped onto the application class they can support and the mapping allows a ranking of MAC protocol performance capabilities.

Figure 15 illustrates that the majority of the surveyed protocols lie in the quadrant of *delay-tolerant and loss-tolerant* applications. As a result, a MAC protocol that suits one particular *delay-tolerant and loss-tolerant* application scenario is likely to be found there. A wide variety of protocols occurs in this quadrant because most WSN application scenarios considered by the research community are of a *delay-tolerant and loss-tolerant* nature. In contrast, a few MAC protocols are in the quadrant of *delay-intolerant and loss-intolerant* applications in Figure 15. For example, the MAC protocols in groups I and J: QoS-MAC and MMSPEED, fall into this area and thus can be considered suitable for some mission-critical applications. Burst and GinMAC in group L also fall into this area and can serve the mission-critical applications with more stringent requirements. As this pool of available protocols is very small, certain specific scenarios of *delay-intolerant and loss-intolerant* applications may not always be fully supported. In addition, as WirelessHART in group K is located not far from the quadrant of *delay-intolerant and loss-intolerant* applications, further refinement could help place this protocol along with QoS-MAC and MMSPEED protocols, increasing the size of the aforementioned pool. Therefore, the research domain of MAC protocols for mission-critical applications is largely open for more investigation. We address some of the open research challenges and potential directions of this research domain next.

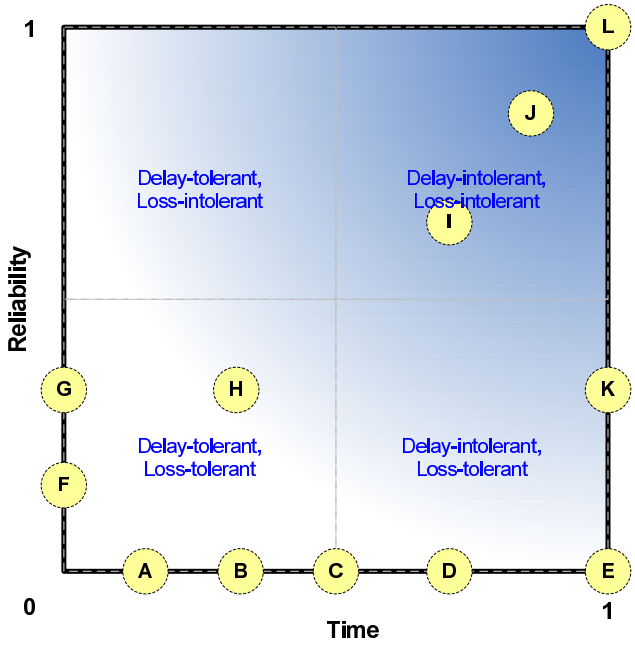


Fig. 15. Mapping the Surveyed Protocols onto the Defined Application Classes

C. Open Research Problems and Future Directions

Our review indicates that a variety of work must still be carried out in order to enable successful deployment of WSNs for mission-critical applications. Here, we list the areas in which we believe research advancements are necessary to deliver such success. In addition, we discuss potential future developments that will most likely have an impact on the development of mission-critical WSN applications.

Deployment Assumptions: WSN deployments have many different requirements, for example, in terms of network

TABLE II
MAPPING OF PERFORMANCE OBJECTIVES ONTO X-Y PERFORMANCE COORDINATES

Delay Objectives	X-Coordinates	Reliability Objectives	Y-Coordinates
not addressed	0	not addressed	0
node-to-node decrease	0.125	node-to-node increase	0.125
end-to-end decrease	0.25	end-to-end increase	0.25
node-to-node probabilistic guarantee	0.375	node-to-node probabilistic guarantee	0.375
node-to-node guarantee	0.50	node-to-node guarantee	0.50
end-to-end probabilistic guarantee	0.75	end-to-end probabilistic guarantee	0.75
end-to-end guarantee	1	end-to-end guarantee	1

TABLE III
CLASSIFICATION OF THE REVIEWED PROTOCOLS USING X-Y PERFORMANCE COORDINATES

Group	X-Y Coordinates (Delay, Reliability)	Performance Objectives (Delay, Reliability)	Protocols
A	(0.125, 0)	(node-to-node decrease, no)	SMAC-AL [1], T-MAC [2], DSMAC [3], Alert [13],
B	(0.25, 0)	(end-to-end decrease, no)	DMAC [4], LEEMAC [5], FPA/GSA[6] Algorithms, RMAC-R [7], LE-MAC [8], Q-MAC [9], PTW [10], LEEM [11],
C	(0.325, 0)	(node-to-node probabilistic guarantee, no)	T-MALOHA [12]
D	(0.50, 0)	(node-to-node guarantee, no)	FTDMA [12], f-MAC [14]
E	(1, 0)	(end-to-end guarantee, no)	RT-Link [15], PEDAMACS [16], HyMAC [17]
F	(0, 0.125)	(no, node-to-node increase)	RMAC [18], E2RMAC [19] ATPC [21] Algorithm
G	(0, 0.25)	(no, end-to-end increase)	Back-off [20] Algorithms
H	(0.25, 0.25)	(end-to-end decrease, end-to-end increase)	Dwarf [23]
I	(0.50, 0.50)	(node-to-node guarantee, node-to-node guarantee)	QoS-MAC [24]
J	(0.75, 0.75)	(end-to-end probabilistic guarantee, end-to-end probabilistic guarantee)	MMSPEED [22]
K	(1, 0.25)	(end-to-end guarantee, end-to-end increase)	WirelessHART [25]
L	(1, 1)	(end-to-end guarantee, end-to-end guarantee)	Burst [26] Algorithm, GinMAC [27]

topology or traffic patterns. This has led to the development of various MAC protocols which are often optimized for a specific application scenario. A MAC protocol used in a scenario where it was not designed for will perform poorly or may even be impractical to be used. Similarly, mission-critical application scenarios have a variety of requirements. It is unlikely that one MAC protocol will fit all scenarios, and as such there are two open questions. The first is what the different types of application scenarios are. The second is what MAC protocols will be needed to support these. The existing MAC protocols for mission-critical applications are certainly not useful to support all potential scenarios.

Analytical Tools: For the operation of a mission-critical WSN, it is important to know before network deployment what delay and reliability bounds can be supported and thus whether the application needs can be fulfilled. For MAC protocols that are designed and deployed to schedule all traffic such that *end-to-end* delay and reliability targets are met, these questions are trivial to answer. However, these protocols tend to be relatively inflexible as assumptions regarding topology and traffic must be made beforehand. MAC protocols that support *node-to-node worst-case bounds* are more flexible as they can be used to support arbitrary topologies and traffic patterns. Nevertheless, an analytic tool must be available to determine end-to-end performance bounds achievable in the application scenario under consideration. There is currently a lack of tools to determine performance bounds before network deployment. Sensor Network Calculus [40], however, represents one of the few examples of such a tool.

Performance Monitoring: MAC protocols for mission-critical WSNs are designed to work in environments with stable channel characteristics. For instance, MAC protocols are provisioned for a possible number of retransmissions to achieve required reliability levels. However, in a wireless deployment it is always possible that links fail completely for long time periods or that channel conditions fall below the

channel quality assumed during network design. Currently, it is not clear how mission-critical applications should deal with such situations.

Energy Consumption: Nearly all surveyed protocols include radio duty cycling as an energy saving scheme as they commonly have a goal of power preservation. Nevertheless, one study called Alert [13] takes a more extreme route of excluding energy efficiency and instead concentrates on achieving other performance objectives of data delivery. Such an *energy-independent* MAC protocol may be more applicable for mission-critical applications. For example, in typical deployment areas of mission-critical WSN applications such as factories, power can be obtained easily from mains electricity and thus is not a critical constraint. The reduction in the cost of communication cabling is instead more important. Moreover, power distribution networks are necessary for operating machinery and cannot be removed. Hence, this monitored machinery could use energy harvesting as an option for providing energy to nodes.

Additional Performance Parameters: All surveyed protocols address data transport delay and reliability. Nevertheless, there is a need to consider additional performance parameters such as throughput and jitter. These two parameters are important for supporting multimedia data streams, and a number of WSN applications that use audio and video signals exist. For instance, safety and security applications [71] often rely on video data.

Node Mobility: All available protocols for mission-critical WSNs assume static deployments, and mobility is not considered. However, many mission-critical applications will include nodes with relative mobility. For example, assembly lines in factories contain moving machinery, and thus some limited mobility of nodes must be considered in protocol design.

Hardware Limitations: Most available MAC protocols are designed to support standard WSN node hardware. These protocols are designed to support a node with one CPU having a small processing capability and one 802.15.4 compliant transceiver. Nevertheless, this hardware configuration may not be the most suitable for mission-critical WSN applications. It may be feasible to design a node comprising multiple processors and transceivers. In this case, a MAC protocol may need to be designed in a very different way.

VII. Conclusion

The area of MAC protocols for wireless sensor networks has drawn much attention from the research community, and therefore a plethora of WSN MAC protocols exists. In this survey these protocols are analyzed in terms of their suitability for mission-critical WSN applications. The mission-critical applications represent a new type of future WSN applications where energy efficient operation is no longer the only design objective. These applications also demand data delivery bounds in both the time and reliability domains. Multimedia sensor applications and event-driven control applications are examples of such applications where data must be transported in a timely and reliable fashion. The reviewed protocols were categorized by the two fundamental performance objectives: *message transfer delay* and *message transfer reliability*. Some surveyed protocols address only one objective, while others address both objectives concurrently. The survey shows that most delay-aware protocols can decrease delays but fail to guarantee any end-to-end delay bound. A small number of MAC protocols address the reliability issue but again fail to offer any performance guarantee. In addition, there currently exists only a handful of MAC protocols that address the joint objective of achieving delay and reliability performance bounds, but few of them can support mission-critical applications. Consequently, we conclude that significant research effort is vital to propel a development of a suitable set of MAC protocols for mission-critical applications in wireless sensor networks.

Acknowledgement

This work has been partially supported by the European Commission under the FP7 contract FP7-ICT-224282 (GINSENG).

References

[1] W. Ye, J. Heidemann, and D. Estrin, "Medium access control with coordinated adaptive sleeping for wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 12, pp. 493-506, Jun. 2004.

[2] T. v. Dam, and K. Langendoen, "An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks," in *Proc. 1st ACM Conf. Embedded Networked Sensor Systems*, Los Angeles, CA, USA, 2003, pp. 171-180.

[3] P. Lin, C. Qiao, and X. Wang, "Medium access control with a dynamic duty cycle for sensor networks," in *Proc. 2004 IEEE Wireless Communications and Networking Conf.*, Atlanta, GA, USA, 2004, vol. 3, pp. 1534-1539.

[4] G. Lu, B. Krishnamachari, and C. S. Raghavendra, "An adaptive energy-efficient and low-latency MAC for data gathering in wireless sensor networks," in *Proc. 18th Int. Parallel and Distributed Processing Symp.*, Santa Fe, NM, USA, 2004, pp. 224-231.

[5] S. W. Hussain, T. Khan, and S. M. H. Zaidi, "Latency and Energy Efficient MAC (LEEMAC) Protocol for Event Critical Applications in WSNs," in *Proc. 2006 Int. Symp. Collaborative Technologies and Systems*, Las Vegas, NV, USA, pp. 370-378.

[6] Y. Li, W. Ye, and J. Heidemann, "Energy and latency control in low duty cycle MAC protocols," in *Proc. 2005 IEEE Wireless Communications and Networking Conf.*, New Orleans, LA, USA, 2005, vol. 2, pp. 676-682.

[7] S. Du, A. K. Saha, and D. B. Johnson, "RMAC: A Routing-Enhanced Duty-Cycle MAC Protocol for Wireless Sensor Networks," in *Proc. 26th IEEE Conf. Computer Communications*, Anchorage, AK, USA, 2007, pp. 1478-1486.

[8] C. Suh, D. M. Shrestha, and Y.-B. Ko, "An Energy-efficient MAC protocol for Delay-Sensitive Wireless Sensor Networks," in *Proc. 2nd Int. Workshop RFID and Ubiquitous Sensor Networks*, Seoul , Korea, 2006, pp. 445-454.

[9] N. A. Vasanthi, and S. Annadurai, "Energy Efficient Sleep Schedule for Achieving Minimum Latency in Query based Sensor Networks," in *Proc. IEEE Int. Conf. Sensor Networks, Ubiquitous, and Trustworthy Computing*, Taichung, Taiwan, 2006, vol. 2, pp. 214-219.

[10] X. Yang, and N. H. Vaidya, "A Wakeup Scheme for Sensor Networks: Achieving Balance between Energy Saving and End-to-end Delay," in *Proc. 10th IEEE Real-Time and Embedded Technology and Applications Symp.*, Toronto, Canada, 2004, pp. 19- 26.

[11] M. Dhanaraj, B. S. Manoj, and C. S. R. Murthy, "A New Energy Efficient Protocol for Minimizing Multi-Hop Latency in Wireless Sensor Networks," in *Proc. 3rd IEEE Int. Conf. Pervasive Computing and Communications*, Kauai Island, HI, USA, 2005, pp. 117-126.

[12] K. K. Chintalapudi, and L. Venkatraman, "On the Design of MAC Protocols for Low-Latency Hard Real-Time Discrete Control Applications over 802.15.4 Hardware," in *Proc. 7th ACM/IEEE Int. Conf. Information Processing in Sensor Networks*, St. Louis, MO, USA, 2008, pp. 356-367.

[13] V. Namboodiri, and A. Keshavarzian, "Alert: An Adaptive Low-Latency Event-Driven MAC Protocol for Wireless Sensor Networks," in *Proc. 7th ACM/IEEE Int. Conf. Information Processing in Sensor Networks*, St. Louis, MO, USA, 2008, pp. 159-170.

[14] U. Roedig, A. Barroso, and C. J. Sreenan, "f-MAC: A Deterministic Media Access Control Protocol Without Time Synchronization," in *Proc. 3rd European Workshop Wireless Sensor Networks*, Zurich, Switzerland, 2006, pp. 276-291.

[15] A. Rowe, R. Mangharam, and R. Rajkumar, "RT-Link: A Time-Synchronized Link Protocol for Energy-Constrained Multi-hop Wireless Networks," in *Proc. 3rd Annu. IEEE Communications Society Conf. Sensor, Mesh and Ad Hoc Communications and Networks*, Reston, VA, USA, 2006, vol. 2, pp. 402-411.

[16] S. C. Ergen, and P. Varaiya, "PEDAMACS: Power Efficient and Delay Aware Medium Access Protocol for Sensor Networks," *IEEE Trans. Mobile Comput.*, vol. 5, pp. 920-930, Jul. 2006.

[17] M. Salajegheh, H. Soroush, and A. Kalis, "HyMAC: Hybrid TDMA/FDMA Medium Access Control Protocol for Wireless Sensor Networks," in *Proc. 18th IEEE Int. Symp. Personal, Indoor and Mobile Radio Communications*, Athens, Greece, 2007, pp. 1-5.

[18] R. Biswas, V. Jain, C. Ghosh, and D. P. Agrawal, "On-Demand Reliable Medium Access in Sensor Networks," in *Proc. 7th IEEE Int. Symp. a World of Wireless, Mobile and Multimedia Networks*, Buffalo, NY, USA, 2006, pp. 251-257.

[19] V. Jain, R. Biswas, and D. P. Agrawal, "Energy-Efficient and Reliable Medium Access in Sensor Networks," in *Proc. 8th IEEE Int. Symp. a World of Wireless, Mobile and Multimedia Networks*, Helsinki, Finland, 2007, pp. 1-8.

[20] I. Chatzigiannakis, A. Kinalis, and S. Nikoletseas, "Wireless sensor networks protocols for efficient collision avoidance in multi-path data propagation," in *Proc. 1st ACM Int. Workshop Performance Evaluation of Wireless Ad hoc, Sensor, and Ubiquitous Networks*, Venezia, Italy, 2004, pp. 8-16.

[21] S. Lin, J. Zhang, G. Zhou, L. Gu, J. A. Stankovic, and T. He, "ATPC: adaptive transmission power control for wireless sensor networks," in *Proc. 4th ACM Conf. Embedded Networked Sensor Systems*, Boulder, CO, USA, 2006, pp. 223-236.

[22] E. Felemban, C.-G. Lee, and E. Ekici, "MMSPEED: Multipath Multi-SPEED Protocol for QoS Guarantee of Reliability and Timeliness in Wireless Sensor Networks," *IEEE Trans. Mobile Comput.*, vol. 5, pp. 738-754, Jun. 2006.

[23] M. Strasser, A. Meier, K. Langendoen, and P. Blum, "Dwarf: Delay-aWAre Robust Forwarding for Energy-Constrained Wireless Sensor Networks," in *Proc. 3rd IEEE Int. Conf. Distributed Computing in Sensor Systems*, Santa Fe, NM, USA, 2007, pp. 64-81.

[24] P. Suriyachai, U. Roedig, and A. Scott, "Implementation of a MAC Protocol for QoS Support in Wireless Sensor Networks," in *Proc. 1st Int. Workshop Information Quality and Quality of Service for Pervasive Computing, in conjunction with 7th Annu. IEEE Int. Conf. Pervasive Computing and Communications*, Galveston, TX, USA, 2009, pp. 1-6.

[25] HART Communication Foundation, "WirelessHART Technology," [Online]. Available: http://www.hartcomm.org/protocol/wihart/ wireless_technology.html, Dec. 2009.

[26] S. Munir, S. Lin, E. Hoque, S. M. S. Nirjon, J. A. Stankovic, and K. Whitehouse, "Addressing Burstiness for Reliable Communication and Latency Bound Generation in Wireless Sensor Networks," in *Proc. 9th ACM/IEEE Int. Conf. Information Processing in Sensor Networks*, Stockholm, Sweden, 2010, pp. 303-314.

[27] P. Suriyachai, J. Brown, and U. Roedig, "Time-Critical Data Delivery in Wireless Sensor Networks," in *Proc. 6th IEEE Int. Conf. Distributed Computing in Sensor Systems*, Santa Barbara, CA, USA, 2010, pp. 216-229.

[28] W. Ye, J. Heidemann, and D. Estrin,"An energy-efficient MAC protocol for wireless sensor networks," in *Proc. 21st Annu. Joint Conf. IEEE Computer and Communications Societies*, New York, NY, USA, 2002, vol. 3, pp. 1567-1576.

[29] J. Song, S. Han, A. Mok, D. Chen, M. Lucas, M. Nixon, and W. Pratt, "WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control," in *Proc. 14th IEEE Real-Time and Embedded Technology and Applications Symp.*, St. Louis, MO, USA, 2008, pp. 377-386.

[30] IEEE802.15.4e Task Group, [Online]. Available: http://www.ieee802.org/15/pub/TG4e.html, Aug. 2010.

[31] F. Chen, R. German, and F. Dressler, "Towards IEEE 802.15.4e: A study of Performance Aspects," in *Proc. 2nd Int. Workshop Information Quality and Quality of Service for Pervasive Computing, in conjunction with 8th Annu. IEEE Int. Conf. Pervasive Computing and Communications*, Mannheim, Germany, 2010, pp. 68-73.

[32] F. Chen, T. Talanis, R. German, and F. Dressler, "Real-time Enabled IEEE 802.15.4 Sensor Networks in Industrial Automation," in *Proc. IEEE Int. Symp. Industrial Embedded Systems*, Lausanne, Switzerland, 2009, pp. 136-139.

[33] ISA100 Wireless Systems for Automation, [Online]. Available: http://www.isa.org/MSTemplate.cfm?MicrositeID=1134&CommitteeID=6891, Aug. 2010.

[34] K.S.J. Pister, and L. Doherty, "TSMP: time sychronized mesh protocol," in *Proc. IASTED Symp. Parallel and Distributed Computing and Systems*, Orlando, FL, USA, 2008.

[35] A. Barroso, U. Roedig, and C. J. Sreenan, "μ-MAC: an energy-efficient medium access control for wireless sensor networks," in *Proc. 2rd European Workshop Wireless Sensor Networks*, Istanbul, Turkey, 2005, pp. 70-80.

[36] G.-S. Ahn, E. Miluzzo, A. T. Campbell, S. G. Hong, and F. Cuomo, "Funneling-MAC: A Localized, Sink-Oriented MAC For Boosting Fidelity in Sensor Networks," in *Proc. 4th ACM Conf. Embedded Networked Sensor Systems*, Boulder, CO, USA, 2006, pp. 293-306.

[37] W.-Z. Song, F. Yuan, and R. LaHusen, "Time-Optimum Packet Scheduling for Many-to-One Routing in Wireless Sensor Networks," in *Proc. 3rd IEEE Int. Conf. Mobile Ad-hoc and Sensor Systems*, Vancouver, BC, Canada, 2006, pp. 81-90.

[38] F. Wang, and J. Liu, "Duty-Cycle-Aware Broadcast in Wireless Sensor Networks," in *Proc. 28th IEEE Conf. Computer Communications*, Rio de Janeiro, Brazil, 2009, pp. 468-476.

[39] P. Suriyachai, U. Roedig, and A. Scott, "Poster Abstract: Implementation of a Deterministic Wireless Sensor Network," in *Proc. 5th European Conf. Wireless Sensor Networks*, Bologna, Italy, 2008.

[40] J. Schmitt, and U. Roedig, "Sensor Network Calculus - A Framework for Worst-Case Analysis," in *Proc. 1st IEEE Int. Conf. Distributed Computing in Sensor Systems*, Marina del Rey, CA, USA, 2005, pp. 141-154.

[41] A. El-Hoiydi, J. D. Decotignie, C. Enz, and E. L. Roux, "Poster abstract: WiseMAC, an ultra low power MAC protocol for the wiseNET wireless sensor network," in *Proc. 1st ACM Conf. Embedded Networked Sensor Systems*, Los Angeles, CA, USA, 2003, pp. 302-303.

[42] Y. Kim, H. Shin, and H. Cha, "Y-MAC: An Energy-Efficient Multi-channel MAC Protocol for Dense Wireless Sensor Networks," in *Proc. 7th ACM/IEEE Int. Conf. Information Processing in Sensor Networks*, St. Louis, MO, USA, 2008, pp. 53-63.

[43] M. J. Miller, and N. H. Vaidya, "A MAC Protocol to Reduce Sensor Network Energy Consumption Using a Wakeup Radio," *IEEE Trans. Mobile Comput.*, vol. 4, pp. 228-242, May-June 2005.

[44] L. Gu, and J. A. Stankovic, "Radio-Triggered Wake-Up Capability for Sensor Networks," in *Proc. 10th IEEE Real-Time and Embedded Technology and Applications Symp.*, Toronto, Canada, 2004, pp. 27-36.

[45] J. Ansari, D. Pankin, and P. Mähönen, "Demo Abstract: Radio-Triggered Wake-ups with Addressing Capabilities for Extremely Low Power Sensor Network Applications," in *Proc. 5th European Conf. Wireless Sensor Networks*, Bologna, Italy, 2008.

[46] J. Brown, J. Finney, C. Efstratiou, B. Green, N. Davies, M. Lowton, and G. Kortuem, "Network interrupts: supporting delay sensitive applications in low power wireless control networks," in *Proc. 2nd Workshop Challenged Networks*, Montreal, Quebec, Canada, 2007, pp. 51-58.

[47] TI/Chipcon CC2420 Datasheet, [Online]. Available: http://focus.ti.com/lit/ds/symlink/cc2420.pdf, Mar. 2010.

[48] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, "A survey on wireless multimedia sensor networks," *Elsevier J. Comput. Netw.*, vol. 51, no. 4, pp. 921-960, Mar. 2007.

[49] I. F. Akyildiz, and I. H. Kasimoglu, "Wireless Sensor and Actor Networks: Research Challenges," *Elsevier J. Ad Hoc Networks*, vol. 2, no. 4, pp. 351-367, Oct. 2004.

[50] C. Wang, K. Sohraby, B. Li, M. Daneshmand, and Y. Hu, "A survey of transport protocols for wireless sensor networks," *IEEE Network*, vol. 20, pp. 34-40, May-June 2006.

[51] A. Willig, and H. Karl, "Data Transport Reliability in Wireless Sensor Networks. A Survey of Issues and Solutions," *J. Praxis der Informationsverarbeitung und Kommunikation*, vol. 28, no. 2, pp. 86-92, Apr.-Jun. 2005.

[52] K. Akkaya, and M. Younis, "A survey on routing protocols for wireless sensor networks," *Elsevier J. Ad Hoc Networks*, vol. 3, no. 3, pp. 325-349, May 2005.

[53] C. Yin, and A. Orooji, "Routing Protocols for Sensor Networks," in *Proc. 2006 Int. Conf. Wireless Networks*, Las Vegas, NV, USA, pp. 15-21.

[54] I. Demirkol, C. Ersoy, and F. Alagoz, "MAC protocols for wireless sensor networks: a survey," *IEEE Commun. Mag.*, vol. 44, pp. 115-121, Apr. 2006.

[55] K. Kredo II, and P. Mohapatra, "Medium access control in wireless sensor networks," *Elsevier J. Comput. Netw.*, vol. 51, no. 4, pp. 961-994, Mar. 2007.

[56] K. Langendoen, "Medium Access Control in Wireless Sensor Networks," in *Medium Access Control in Wireless Networks*, H. Wu and Y. Pan, Eds.: Nova Science Publishers, 2007, ch. 20, pp. 535-560.
[57] K. Langendoen, "MAC Alphabet Soup," [Online]. Available: http://www.st.ewi.tudelft.nl/~koen/MACsoup/, Mar. 2009.
[58] A. Bachir, M. Dohler, T. Watteyne, and K. K. Leung, "MAC Essentials for Wireless Sensor Networks," *IEEE Communications Surveys and Tutorials*, vol. 12, no. 2, pp. 222-248, 2010.
[59] A. Willig, "Recent and Emerging Topics in Wireless Industrial Communications: A Selection," *IEEE Trans. Ind. Informat.*, vol.4, pp. 102-124, May 2008.
[60] K. Römer, and F. Mattern, "The design space of wireless sensor networks," *Wireless Commun.*, vol. 11, pp. 54-61, Dec. 2004.
[61] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, "Wireless sensor networks for habitat monitoring," in *Proc. 1st ACM Int. Workshop on Wireless Sensor Networks and Applications*, Atlanta, GA, USA, 2002, pp. 88-97.
[62] K. Martinez, R. Ong, and J. Hart, "Glacsweb: a sensor network for hostile environments," in *Proc. 1st Annu. IEEE Communications Society Conf. Sensor and Ad Hoc Communications and Networks*, Santa Clara, CA, USA, 2004, pp. 81-87.
[63] K. Römer, "Tracking Real-World Phenomena with Smart Dust," in *Proc. 1st European Workshop Wireless Sensor Networks*, Berlin, Germany, 2004, pp. 28-43.
[64] T. He, S. Krishnamurthy, J. A. Stankovic, T. Abdelzaher, L. Luo, R. Stoleru, T. Yan, L. Gu, J. Hui, and B. Krogh, "Energy-efficient surveillance system using wireless sensor networks," in *Proc. 2nd Int. Conf. Mobile Systems, Applications, and Services*, Boston, MA, USA, 2004, pp. 270-283.
[65] A. Arora, P. Dutta, S. Bapat, V. Kulathumani, H. Zhang, V. Naik, V. Mittal, H. Cao, M. Demirbas, M. Gouda, Y. Choi, T. Herman, S. Kulkarni, U. Arumugam, M. Nesterenko, A. Vora, and M. Miyashita, "A line in the sand: a wireless sensor network for target detection, classification, and tracking," *Elsevier J. Computer Networks, Special Issue Military Communications Systems and Technologies*, vol. 46, no. 5, pp. 605-634, Dec. 2004.
[66] W. B. Heinzelman, A. L. Murphy, H. S. Carvalho, and M. A. Perillo, "Middleware to support sensor network applications," *IEEE Network*, vol. 18, pp. 6-14, Jan. 2004.
[67] L. Schwiebert, S. K. S. Gupta, and J. Weinmann, "Research challenges in wireless networks of biomedical sensors," in *Proc. 7th Annu. Int. Conf. Mobile Computing and Networking*, Rome, Italy, 2001, pp. 151-165.
[68] J. P. Benson, T. O'Donovan, P. O'Sullivan, U. Roedig, C. Sreenan, J. Barton, A. Murphy, and B. O'Flynn, "Car-Park Management using Wireless Sensor Networks," in *Proc. 1st IEEE Int. Workshop Practical Issues in Building Sensor Network Applications*, Tampa, FL, USA, 2006, pp. 588-595.
[69] L. Krishnamurthy, R. Adler, P. Buonadonna, J. Chhabra, M. Flanigan, N. Kushalnagar, L. Nachman, and M. Yarvis, "Design and deployment of industrial sensor networks: experiences from a semiconductor plant and the north sea," in *Proc. 3rd ACM Conf. Embedded Networked Sensor Systems*, San Diego, CA, USA, 2005, pp. 64-75.
[70] I. Stoianov, L. Nachman, S. Madden, and T. Tokmouline, "PIPENET: A Wireless Sensor Network for Pipeline Monitoring," in *Proc. 6th ACM/IEEE Int. Conf. Information Processing in Sensor Networks*, Cambridge, MA, USA, 2007, pp. 264-273.
[71] R. Mangharam, A. Rowe, R. Rajkumar, and R. Suzuki, "Voice over Sensor Networks," in *Proc. 27th IEEE Int. Real-Time Systems Symp.*, Rio de Janeiro, Brazil, 2006, pp. 291-302.
[72] L. H. A. Correia, D. F. Macedo, D. A. C. Silva, A. L. d. Santos, A. A. F. Loureiro, and J. M. S. Nogueira, "Transmission power control in MAC protocols for wireless sensor networks," in *Proc. 8th ACM Int. Symp. Modeling, Analysis and Simulation of Wireless and Mobile Systems*, Montreal, Quebec, Canada, 2005, pp. 282-289.
[73] J. So, and N. H. Vaidya, "Multi-channel mac for ad hoc networks: handling multi-channel hidden terminals using a single transceiver," in *Proc. 5th ACM Int. Symp. Mobile Ad Hoc Networking and Computing*, Tokyo, Japan, 2004, pp. 222-233.
[74] R. Maheshwari, H. Gupta, and S. R. Das, "Multichannel MAC Protocols for Wireless Networks," in *Proc. 3rd Annu. IEEE Communications Society Conf. Sensor, Mesh and Ad Hoc Communications and Networks*, Reston, VA, USA, 2006, vol. 2, pp. 393-401.

Petcharat Suriyachai received B.S. and M.S. degrees in electrical and computer engineering from Carnegie Mellon University, USA in 2000 and 2002, respectively. After graduation, she became a Lecturer at the Department of Computer Engineering, Faculty of Engineering at Prince of Songkla University, Thailand. Since May 2007, she has been working toward her PhD degree in computer science at Lancaster University, UK. Her research interests include network provisioning, performance control and medium access control protocols for wireless sensor networks.

Utz Roedig received a PhD degree in computer science from Darmstadt University of Technology, Germany in 2002. Between 2002 and 2006, he was a postdoctoral researcher in the Department of Computer Science at University College Cork, Ireland. He currently serves as a Lecturer at the School of Computing and Communications, Lancaster University, UK, which he joined in October 2006. Aspects of his research are embedded systems communication and in particular wireless sensor networks.

Andrew Scott (M'06) received B.Sc. (Hons.) and PhD degrees in computer science from Lancaster University, UK in 1987 and 1991, respectively. He is a Senior Lecturer in the School of Computing and Communications, Lancaster University, UK. His research interests include wireless networks, embedded and mobile devices, network protocols and testbeds. Dr. Scott is also a member of the ACM, BCS, and IET.