

Research Article

MAC Protocols Used by Wireless Sensor Networks and a General Method of Performance Evaluation

Joseph Kabara¹ and Maria Calle²

¹ School of Information Sciences, University of Pittsburgh, Pittsburgh, PA 15260, USA

² Department of Electrical and Electronics Engineering, Universidad del Norte, Barranquilla, Colombia

Correspondence should be addressed to Joseph Kabara, jkabara@ieee.org

Received 15 June 2011; Revised 13 September 2011; Accepted 16 September 2011

Academic Editor: Yuhang Yang

Copyright © 2012 J. Kabara and M. Calle. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Many researchers employ IEEE802.15.4 as communication technology for wireless sensor networks (WSNs). However, medium access control (MAC) layer requirements for communications in wireless sensor networks (WSNs) vary because the network is usually optimized for specific applications. Thus, one particular standard will hardly be suitable for every possible application. Two general categories of MAC techniques exist: contention based and schedule based. This paper explains these two main approaches and includes examples of each one. The paper concludes with a unique performance analysis and comparison of benefits and limitations of each protocol with respect to WSNs.

1. Introduction

Wireless sensor networks (WSNs) have hundreds or potentially thousands of nodes, each of which are small computers capable of measuring physical characteristic(s) of the surrounding environment and transmitting the information using a radio link. WSNs can be used in monitoring applications such as weather, crops, surveillance, human health care, and structural health [1, 2]. However, WSNs are different from typical computer networks in that individual nodes have very limiting constraints in memory and processing power. Additionally, energy usage is a major limitation since nodes usually employ physically small hardware platforms and they are very likely to be battery powered. Once a battery is depleted, it is often very difficult, if not impossible, to recharge or replace it, so the node is considered dead [1]. One example application is structural health monitoring of a bridge. There may be hundreds of nodes measuring vibrations in the bridge and transmitting this information to a sink (main receiver) not located on the bridge. The information can be used by engineers to schedule maintenance or repairs. When batteries are depleted, nodes must be replaced or recharged. As an illustration, consider the application presented in [3], where a node transmits every

80 milliseconds and the hardware platform uses 120.12 joules in one hour. If the hardware employs two AA batteries with a capacity of 1200 mAh, the node can work 65.96 hours before someone must climb the bridge to replace hundreds of batteries. Another example application is leakage in an industrial plant with hazardous chemicals. People must evacuate, but a sensor network may be deployed by dropping nodes from a plane. In this case there is no control over the network topology and no way to recharge batteries either.

An additional complication is that individual monitoring applications have widely different requirements in throughput, delay, network topology, and so forth. Regarding physical topology, the bridge monitoring and the chemical leak monitoring are applications using nodes possibly located in random positions. In contrast, if the situation is patient monitoring in a medical facility, the network may need a specific layout in order to avoid interference with medical equipment. Regarding delay, human health monitoring may have a tighter delay requirement than the other two mentioned applications since vital signs of the patient may indicate the need of immediate treatment. Since different applications have different requirements, WSNs will employ a family of communication standards, each member designed to optimize the critical parameter(s).

2. Background

Since the terminology for wireless sensor networks is often used with different meanings in the literature, a single, common set of definitions is necessary to prevent confusion.

(i) *MAC Layer.* The IEEE802 LAN (local area network) and MAN (metropolitan area network) Reference Model [4] defines medium access control (MAC) as a sublayer of the data link layer presented in the OSI model. The MAC layer main functions are frame delimiting and recognition, addressing, transfer of data from upper layers, error protection (generally using frame check sequences), and arbitration of access to one channel shared by all nodes [4]. MAC layer protocols for WSNs must be energy efficient to maximize lifetime. Additionally, protocols must be scalable according to the network size and should adapt to changes in the network such as addition of new nodes, death of existing nodes, and transient noise on the wireless channel [5].

(ii) *Sleep.* Node state where the radio is turned off [6].

(iii) *Frame.* Data unit containing information from a MAC layer protocol and possibly from upper layers [4].

(iv) *Packet.* Data unit with information from a network layer protocol and possibly from upper layers [4].

(v) *Collision.* Event where two or more frames are received at the same time, damaging the resulting signal. All information is lost [5].

(vi) *Overhearing.* To receive a packet whose destination is any other node [6]. Overhearing results in wasted energy.

(vii) *Idle Listening.* Another source of wasting energy occurs when a node has its radio on, listening to the medium while there are no transmissions [6].

(viii) *Overemitting.* To transmit a message when the destination is not ready for receiving it. Energy for sending the message is wasted [5].

(ix) *Control Frames Overhead.* All frames containing protocol information and not application data. Energy for transmitting and receiving these frames is considered to be wasted [6].

(x) *Capture Effect.* Phenomenon present in some analog modulation schemes, such as frequency modulation (FM). Two signals with different amplitudes arrive at a receiver and go through the passband filter at the same time. The lower amplitude signal is greatly attenuated at the demodulator output, so the stronger signal is successfully received [7].

(xi) *Broadcast.* Sending a message to all nodes in the network [5].

(xii) *Clock Drift.* Most clocks in networking equipment use quartz oscillators, which change with age, temperature, magnetic fields, and mechanical vibration. As the oscillator changes, the time presented by the clock also changes and this is called clock drift [8].

3. Wireless Standards

Standards for wireless communications exist for different applications: cellular telephony, satellite communications, broadcast radio, local area networks, and so forth. Three well-known standards for wireless data communication have been proposed for use in WSNs, each with certain advantages. However, WSNs do not have widely accepted standard communication protocols in any of the layers in the OSI model sense. The following subsections describe standardized protocols which may match WSN requirements. The protocols provide wireless data transmission with appropriate data rates for a wide range of applications, they can be implemented in battery-powered devices, and they do not require complicated planning and setup. Several commercial products use these wireless standards, which could be an advantage for WSNs in cost and ease of implementation. The purpose of this section is to familiarize the reader with the standards, show their advantages and disadvantages, and discuss their use in WSNs.

3.1. *IEEE802.11.* IEEE802.11 is a family of standards for wireless data communications with definitions for characteristics in the Physical and MAC layers. IEEE802.11b, for example, uses direct sequence spread spectrum (DSSS) with varying modulation schemes to maximize the data rate in a given noise environment. Differential binary phase shift keying (DBPSK) is used for 1 Mbps, differential quadrature phase shift keying (DQPSK) for 2 Mbps, and complementary code keying (CCK) for 5.5 and 11 Mbps [9]. The MAC protocol has two modes [9].

(a) *DCF (Distributed Coordination Function).* Mode with no central device controlling the communication. DCF uses CSMA/CA in any of the following ways.

Carrier sensing: a node senses the medium. If it is idle, the node transmits the data frame. If the medium is busy, the node waits until it becomes idle again, waits for a random time and transmits. Upon frame reception, the receiver node answers with an ACK (acknowledgment) control frame. If a collision occurs, transmitting nodes wait a random time and try again later.

Virtual carrier sensing: a node with a frame to transmit senses the medium. If it is idle, the node sends a control frame called RTS (request to send), which contains the intended receiver address and the time required to send the information (transmission delay). If the destination node agrees to communicate, it will answer with a CTS (clear to send) control frame which also contains the delay. All nodes hearing RTS or CTS should refrain from transmission until the transmission delay has elapsed and the medium is

idle again. The receiver must respond with an ACK for each data frame received.

(b) *PCF (Point Coordination Function)*. A special node, the access point (AP), polls every node and controls the communication process. An AP periodically broadcasts a beacon control frame with parameters and invitations to join the network [9].

Advantages of IEEE802.11 include that it is widely used, so it is easy to find networks supporting the standard. Data rates are high for wireless end user transmission and radio ranges can be hundreds of meters. Also, as IEEE802.11 supports well-known protocols as TCP and IP, devices connected with this technology may have easy access to the Internet and this way they can send information anywhere in the world.

Disadvantages include the large overhead in control and data packets. 802.11 requires 34 bytes for the header and the checksum, TCP and IP require a minimum of 20 bytes for each header, so there is at least 74 bytes of overhead to send application information, which in WSNs may be only two bytes. Another possibility is using UDP which employs less overhead, 8 bytes for the header. However, UDP uses IP and 802.11 MAC headers add 62 bytes total to the application information. Perhaps the most important problem for using 802.11 in WSNs is energy consumption. Even though the standard has power saving mechanisms, according to Ferrari et al. "power consumption is rather high, and the short autonomy of a battery supply still remains the main disadvantage of the proposed IEEE802.11 sensor system" [10].

3.2. IEEE802.15.1, Bluetooth. The IEEE also defined MAC and physical layer characteristics for the 802.15.1 standard. In this standard, the physical layer uses 2.4 GHz, frequency hopping spread spectrum (FHSS) with Gaussian frequency shift keying (GFSK) as the modulation scheme. The result is a 1 Mbps data in the basic rate; however, much of the capacity is used for control purposes. The enhanced data rate provision has two data rates, 2 Mbps using $\pi/4$ -differential quadrature phase shift keying (DQPSK) and 3 Mbps using 8 DPSK [11]. IEEE802.15 defines wireless personal area networks (WPANs) allowing connectivity in a 10-meter range. However, some Bluetooth devices have 100-meter range [12].

An 802.15.1 master node controls up to 7 active slave and up to 255 nonactive slave nodes. These networks are referred to as piconets and several piconets may communicate using a bridge node, forming a scatternet. The MAC protocol uses polling with a time division multiplexing (TDM) scheme called time division duplex. In one time slot, the master will poll a single slave, inquiring if it has something to send. If the slave has data to transmit, it sends it to the master in the next time slot [13]. A master node must periodically transmit, even if there is no data to be exchanged, to keep slaves synchronized. Slaves cannot communicate directly; the information must go through the master node. Using the most reliable communication mode, a Piconet can support

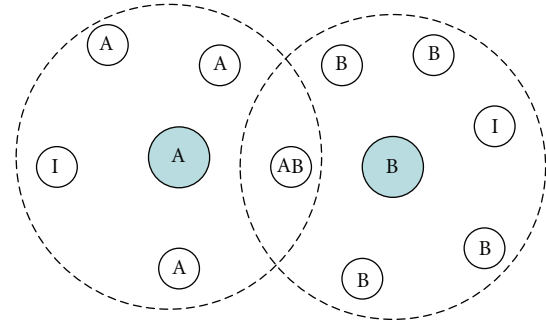


FIGURE 1: Bluetooth scatternet. Shaded circles are master nodes in two different piconets, A and B. White circles show slaves belonging to each piconet. Active slaves are labeled according to the network they belong to; inactive slaves have label I. AB is a slave belonging to both piconets. The figure shows coverage areas of both master nodes.

one full duplex channel with 64 kbps master-slave and another 64 kbps slave-master through the basic rate [13]. Figure 1 illustrates an example scatternet [14].

An advantage to using 802.15.1 for WSNs is that the hardware is designed to have low cost [11]. Disadvantages of 802.15.1 include that a WSN using Bluetooth requires that a group of nodes transmit to one master, located just one hop away. WSNs literature calls this organization cluster based, and the master node is referred to as cluster head [15]. Research shows that a problem in this approach is the master/cluster head becomes a single point of failure, which can isolate all other members of the network [16]. Another problem arises in applications with random deployment because it is not always possible to ensure that all slave nodes are within range of the master. Additionally, the periodic transmissions used for synchronization waste energy at both the transmitter and the receivers.

3.3. IEEE802.15.4. The IEEE defined physical and MAC layer characteristics for establishing connectivity between devices with low-power consumption, low cost, and low data rate. The standard is related to ZigBee technology since The ZigBee Alliance (association of several companies such as Samsung and Motorola) defines the other communication layers (above MAC) for 802.15.4 compliant devices. Frequency bands are 2.4 GHz and 868/915 MHz, both working with DSSS. The 2.4 GHz band has a 250 kbps data rate using offset quadrature phase shift keying (O-QPSK) modulation. The 868/915 MHz band has data rates up to 240 kbps using BPSK [17]. Typical radio range according to the standard is 10 meters. Maximum packet size is 128 bytes with payload of 104 bytes. 64-bit IEEE or 16-bit addresses can be used [17]. The 802.15.4 standard defines two types of devices.

FFD (Full Function Device): Supports all characteristics from the standard. One FFD can be a network coordinator, a router, or a gateway which connects the network to other networks. FFDs can communicate with any other device [17].

RFD (Reduced Function Device): It has very limited characteristics and it can only talk to a FFD [17]. RFDs have low-power consumption and low complexity.

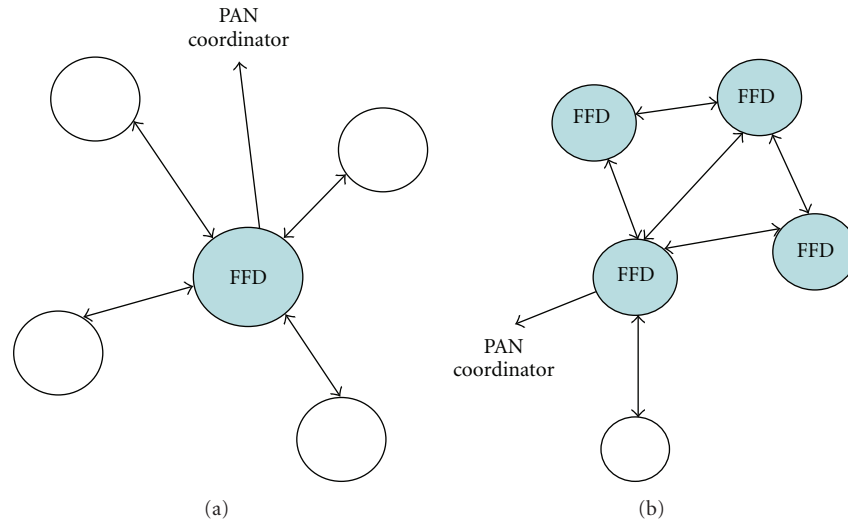


FIGURE 2: (a) Star topology with one full function device and 4 reduced function devices (white circles). (b) Peer-to-Peer topology.

Figure 2 presents two possible topologies using 802.15.4. Both topologies have a PAN (personal area network) coordinator, which is a FFD [17].

The 802.15.4 MAC layer has two modes [17]:

Nonbeacon mode employs CSMA/CA. A node checks the medium; if busy, it waits for a random period of time before trying to transmit. If idle, the node transmits.

Beacon mode employs two periods: active (divided in 16 time slots) and inactive (devices enter a low-power mode), as presented in Figure 3 [17]. At the beginning of the active period, the coordinator sends beacon frames with information regarding the period duration so the duty cycle can vary. The contention access period (CAP) follows the Beacon, allowing devices to send frames using slotted CSMA/CA. A node waits for a random time, then checks the medium and if the channel is clear, transmits. If the channel is busy, the device waits again. The first waiting time (before checking the medium) can be very small to minimize idle listening in low traffic. The node can sleep immediately after receiving an acknowledgement.

When the CAP ends, the collision free period (CFP) begins. The CFP uses guaranteed time slots (GTSs), in a TDMA fashion, to support devices requiring low latency or dedicated bandwidth. The coordinator cannot interact with the PAN during the inactive period and may sleep [17].

The major advantage to using 802.15.4 for WSNs is that the hardware for the nodes is designed to be inexpensive [18]. Disadvantages to using 802.15.4 for WSNs include that a star topology is only appropriate for the clustered model of WSNs since this model requires all RFDs to be close enough for their signal to be received by a FFD. However, like 802.15.1, a random deployment does not guarantee the position of any device. 802.15.4 energy usage may be another issue; the standard is designed to minimize usage but still some ZigBee radio devices consume more energy than devices using just FSK modulation and Manchester encoding [19]. In one example, the MICAz radio works at 250 kbps (802.15.4 compliant radio), requiring 19.7 mA for receiving

and 17 mA for transmitting with 1 mW transmission power. MICA2 uses the same microcontroller and memory but the radio works at 38.4 kbps, requiring 7 mA for receiving and 10 mA for transmitting with the same power as MICAz [19]. Transmitting a fixed size packet requires more energy in MICA2 than MICAz. However, if both platforms spend the same time in idle listening (receiving nothing), MICAz uses more energy than MICA2.

3.4. WirelessHART. The HART Communication Foundation extended the wired HART protocol for communication requirements in industrial plants, specifically compensating for electrically noisy environments and real-time delay constraints. WirelessHART was accepted as international electrotechnical commission (IEC) standard 62591. The protocol defines functionality in the physical, MAC, network, transport and application layers [20]. WirelessHART uses the physical layer from IEEE802.15.4, but the MAC layer uses TDMA and channel hopping, in order to minimize interference [21]. A blacklist feature blocks occupied channels, so hopping can take place at most in 16 different frequencies. Time division multiplexing employs 10 msec time slots which can be allocated to a single transmitter and receiver pair, or several devices in a contention access method similar to CSMA. A group of time slots is called a superframe with size defined by a network manager device, which also maintains synchronization and creates routes in the network. WirelessHART creates a mesh network with six different types of devices, as shown in Figure 4 [22].

NM (network Manager) It creates and manages the TDMA schedule and routes in the network.

FD (Field Device) communication devices directly connected to the monitored machines.

RD (Field Device) router devices not directly connected to the monitored machines. Router devices assist in the communication process and may be used to increase network coverage. RDs are optional in the standard.

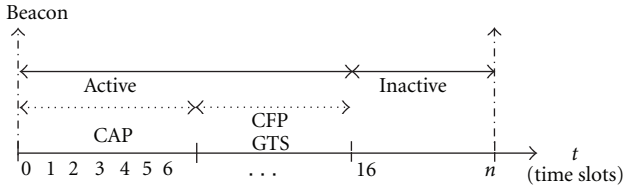


FIGURE 3: Beacon mode structure. Active period has contention (CAP) and noncontention (CFP) modes.

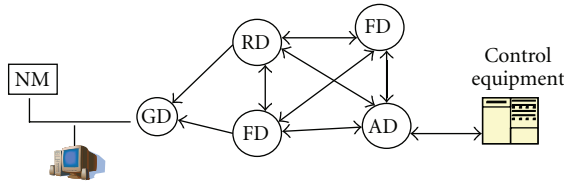


FIGURE 4: Different devices in a WirelessHART network.

AD (Adapter Device) machines with an integral wired HART protocol adapter can connect to the wireless network using an AD.

HD (Handheld Device) allows for mobile monitoring, configuration, and preservation of nodes in a WirelessHART network.

GD (Gateway Device) a gateway connects a WirelessHART compatible network to a network with a different technology, employed in the industrial plant. The network is often the plant automation system.

One advantage of WirelessHART is robustness to harsh industrial communication environment. The main disadvantage is that the NM is a single point of failure; although one backup NM can be implemented, only one active NM is allowed in the network [22].

3.5. ISA100. ISA100 is a family of standards for wireless communications created by the International Society of Automation (ISA) [23]. ISA100a corresponds to process automation, and it shares several features with WirelessHART. Both standards use the physical layer from IEEE802.15.4, and a MAC layer with TDMA, frequency hopping, CSMA, and channel blacklisting [23]. The majority of differences between ISA100 and WirelessHART are in network, transport, and application layers. However, one distinct feature of the ISA100 MAC layer is that it allows dedicated time slots or shared time slots. When sharing a time slot a CSMA-CA algorithm employing priorities is used to control access. A network using ISA100a requires a data link (DL) subnet, with input/output devices, routing and portable devices. There is a backbone network (BN) with routers and gateways (GW) and, finally, a manager network (MN) with a security manager and a system manager [24].

One advantage of ISA100a is that it allows direct connection with different industrial wired standards, such as HART, Fieldbus, and Profibus. One disadvantage is that it requires two manager nodes to control the network, increasing system complexity.

4. Categorization of MAC Protocols for Wireless Sensor Networks

MAC protocols presented in the literature can be classified in two groups according to the approach used to manage medium access: contention based and schedule based [25]. All protocols presented in this paper assume no mobility in the network, only one radio available in each sensor and bidirectional links (meaning if node A can listen to node B, node B can listen to node A).

4.1. Contention Based. Medium access is distributed; there is no need for central coordination for the nodes to use the medium. Examples include the following.

(a) Sensor MAC (S-MAC). S-MAC [6] operates by placing a node in a state that listens to the medium; if a node hears nothing it sends a SYNC packet with a schedule defining listen and sleep periods. All nodes hearing this packet will adopt the schedule. Nodes may adopt two or more schedules (if different neighbors have different schedules). Nodes keep tables with the schedules of their neighbors. During a listen period, a node with a packet to send executes a procedure similar to 802.11 virtual channel sensing, it will send a request to send (RTS) frame and the receiver node will answer with a clear to send (CTS) frame. All nodes not involved in the conversation will enter a sleep state while the communicating nodes send data packets and ACKs. Sleeping decreases energy consumption but introduces latency since communication with a sleeping node must wait until it wakes up [6]. Figure 5 shows an example of the sequence of events occurring in communication between four nodes using S-MAC.

Advantages of S-MAC include sleeping, which reduces energy consumption. The protocol adapts easily to changes in topology and has been tested in hardware. Additionally, there is no need for a central entity or for tight synchronization. Disadvantages of S-MAC include the need to maintain loose synchronization for the schedules to work properly. Clock drift in the nodes can result in nodes becoming unsynchronized. Control frames such as RTS and CTS generate overhead and increase energy usage. Idle Listening still occurs, as shown in Figure 5, where node D is not receiving any packet but must stay awake during the entire listening phase.

S-MAC has been extensively studied and several subsequent protocols include suggestions for performance improvement. Examples include timeout MAC (T-MAC) [26] and dynamic sensor-MAC (DS-MAC) [27]. The B-MAC protocol suggests a different approach which decreases the overhead generated by control frames and does not explicitly synchronize the transmitter and the receiver.

(b) Berkeley Media Access Control for Low-Power Sensor Networks (B-MAC). B-MAC [28] employs an adaptive preamble to reduce idle listening, a major source of energy usage in many protocols. When a node has a packet to send, it waits during a backoff time before checking the channel. If

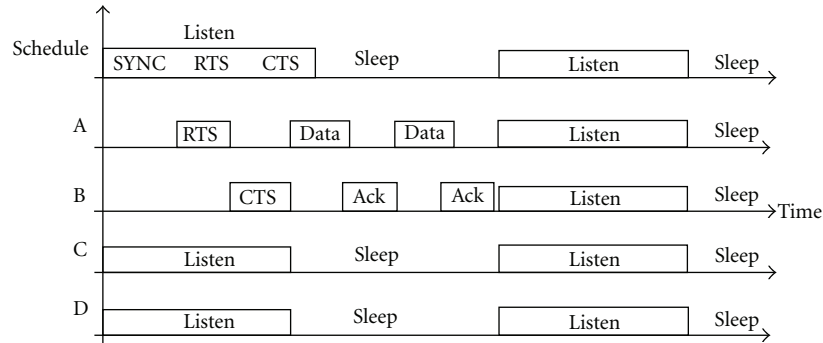


FIGURE 5: S-MAC example. Nodes A, B, and C are within range of each other. D is within range of C and A transmits to B.

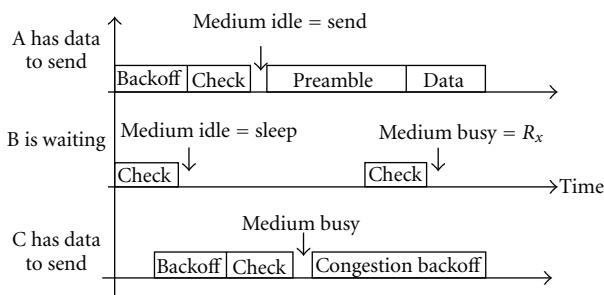


FIGURE 6: B-MAC communication example. All nodes are within range of each other.

the channel is clear, the node transmits; otherwise it begins a second (congestion) backoff. Each node must check the channel periodically using LPL (low-power listening); if the channel is idle and the node has no data to transmit, the node returns to sleep [28]. Figure 6 illustrates one example transmission using B-MAC.

The B-MAC preamble sampling scheme adjusts the interval in which the channel is checked to equal the frame preamble size. As an example, if the medium is checked every 100 ms, the preamble of the packet must last 100 ms as a minimum, in order for the receiver to detect the packet. Upper layers may change the preamble duration, according to the application requirements [28].

An advantage of using B-MAC in WSNs is that it does not use RTS, CTS, ACK, or any other control frame by default, but they can be added. Additionally, it is one of the few specialized MAC protocols whose implementation was tested in hardware. No synchronization is required, and the protocol performance can be tuned by higher layers to meet the needs of various applications. The main disadvantage is that the preamble creates large overhead. One example presents 271 bytes of preamble to send 36 bytes of data [28].

(c) *Predictive Wake-UP MAC (PW-MAC)*. PW-MAC [29] improves on protocols like S-MAC and B-MAC because it uses pseudo random schedules, thus not all nodes will wake up and transmit at the same time, avoiding collisions. A node that has just woke up sends a short beacon so other nodes know it is up. A sender can then transmit a data packet and

request more information from the receiver, such as current time and current seed for the pseudo random schedule used by receiver. By using the seed in a linear congruential generator (LCG), sender in PW-MAC can predict when a receiver will wake up; hence sender sleeps until a little bit before the receiver is awake.

However, there are hardware variations that generate errors in the sender prediction. PW-MAC uses a “sender wake-up advance time” [29], a compensating value particular to every platform, including clock drift, operating system delay, and hardware latency. The value helps correcting errors each node can do when predicting a receiver wake-up time.

One advantage of using PW-MAC is that sleeping until the receiver is up effectively decreases duty cycle in the sender. Additionally, the protocol has been tested on hardware, using MicaZ motes, and memory footprint is small.

Disadvantages of using PW-MAC include overhead created by beacons and idle listening, even if it is small [29] compared to other protocols such as WiseMAC [30], RI-MAC [31], and X-MAC [32].

4.2. *Schedule Based*. Protocols arbitrate medium access by defining an order (called schedule) for nodes to transmit, receive, or be inactive. Generally speaking, each node communicates during specific time slot(s) and can be inactive the rest of the time. Schedule-based protocols use a variety of approaches, as illustrated below.

(a) *Low-Energy Adaptive Clustering Hierarchy (LEACH)*. LEACH [33] includes application, routing, MAC, and physical characteristics for communication in WSNs. A specific application considered is remote monitoring where data gathered by neighboring nodes may be redundant. LEACH assumes all nodes are synchronized, they can control their transmission power, and they can reach one base station (BS, equivalent to the sink in other protocols) if needed. The nodes also have sufficient processing capabilities to implement different MAC protocols and perform signal processing functions, such that all information can be aggregated in only one message. The LEACH protocol works in rounds, as presented in Figure 7. Nodes organize in clusters, elect a cluster head (CH), and then start sending

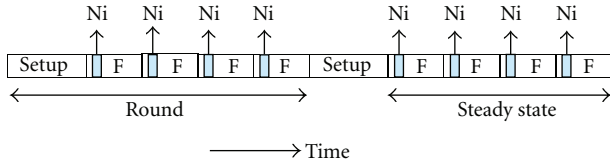


FIGURE 7: LEACH operation rounds. F are frames divided in time slots. Ni are slots assigned to node i .

information. Every cluster uses DSSS with a different code, to minimize interference [33].

During the setup phase, nonpersistent CSMA is used as the MAC protocol. Node i elects itself as a CH with probability $P_i(t)$. The probability is selected in such a way that every node can be a CH and those who have recently been elected have a smaller chance to be selected in the next round. Each elected node sends an advertisement message. Nonelected nodes receive several of these messages and decide which cluster to join, based on the received signal strength of the messages. The nodes inform the CH using a join-request message. The CH creates a TDMA schedule using this information and sends it to all nodes in the cluster. In normal, steady-state operation, every node uses only its assigned time slot to send data to the CH and sleeps the rest of the time. Cluster heads aggregate their cluster data and send it to the BS using CSMA [33].

Advantages of LEACH include saving energy through sleeping. CH rotation extends the lifetime of the network by balancing the rate of energy usage over all nodes, so any one node takes longer to exhaust its energy resources. Including several other networking layers in the protocol design benefits the whole communication scheme by reducing energy usage due to inefficiencies between layers. Disadvantages of LEACH include overhead associated with the death of a CH. When a CH dies, the whole cluster becomes inactive during the remaining steady-state phase, even if several nodes inside the cluster have enough energy to function. Also, LEACH assumes one-hop communication between the nodes and the CH and also among the cluster heads and the BS, something that is not easily achieved in a randomly deployed network. DSSS increases the complexity of the hardware. LEACH requires tight synchronization (for the TDMA schedule and for using DSSS) which is not included as part of the protocol and will require additional energy and overhead to accomplish.

(b) *Power-Efficient and Delay-Aware Medium Access Protocol (PEDAMACS)*. PEDAMACS [34] assumes one access point (AP, also called sink) with the ability to reach all sensor nodes in one hop. However, sensor nodes may employ more than one hop to reach the AP. There are three transmission power levels defined to reach three distances: P_l the maximum, P_m the medium, and P_s the minimum. The protocol has the following four phases, which are illustrated in Figure 8.

Topology learning: the AP broadcasts a packet with P_l to synchronize the nodes. After that, the AP sends another packet with P_m which will be retransmitted through the entire network, so all nodes receive the topology currently

held by the AP and can update it. Using the received signal strength and interference models, each node identifies its local neighbors (nodes able to decode a packet transmitted with P_s), its interferers (nodes unable to decode a packet transmitted with P_s , but with received signal strength high enough to interfere with other signals), and its parent node in the route to the AP. During this phase, the protocol employs a protocol similar to 802.11, with RTS and CTS, since there is no schedule yet.

Topology collection: each node sends topology information to the AP using P_s , so data may possibly go through several hops. The protocol also uses CSMA in this phase.

Scheduling phase: the AP broadcasts the schedule so every node adjusts its clock and knows the time slots allowed for it to transmit and receive. The rest of the time, the nodes sleep. A guard interval for each time slot compensates for synchronization errors. Nodes transmit data with P_s .

Adjustment: at the end of the scheduling phase, the AP requests and the nodes send adjustment topology packets indicating changes in neighbors or interferers. Nodes can also send this information during the scheduling phase inside data packets [34].

PEDAMACS considers characteristics from physical and network layers, to its advantage. Other advantages include that PEDAMACS can be used for sending periodic data or for event-driven sensing, using the assigned time slots only when the event happens; otherwise, the nodes keep on sleeping. The protocol can be extended to use more than one AP and to handle nodes outside the range of the AP. Delay results are bounded for different network sizes [34].

The disadvantages of PEDAMACS include considerable additional overhead beside RTS, CTS, and ACK packets. The protocol assumes an AP which can communicate to all nodes, with an infinite energy supply. Such an AP may not be possible in WSNs, especially with random deployment. Additionally, low transmission power levels save energy, but radio ranges decrease significantly. One example with Mica2 motes shows 25 cm radio range for -20 dBm which is the minimum transmission power [3], so nodes must be very close to each other to maintain connectivity in the network.

(c) *Priority-Based MAC Protocol for Wireless Sensor Networks (PRIMA)*. PRIMA [35] uses a similar procedure as LEACH [33] to create clusters and elect cluster heads (CHs) and to control communication and keep synchronization inside each cluster; CH will rotate every 15 minutes. PRIMA defines four priorities for information by making application layer to add two bits at the end of each packet. MAC layer uses two different protocols: classifier MAC (C-MAC) adds each packet to one of four different queues, according to each priority. The other protocol is channel access MAC (CA-MAC) which uses CSMA/CA and TDMA slots. Random access slots allow for different nodes to request a time slot and CH to broadcast schedules. Nodes send data according to schedule using TDMA slots without collisions. A similar situation happens when CHs want to transmit to the base station (main node, BS). There will be a CSMA phase to create schedules and a TDMA phase where each CH can transfer data without collisions.

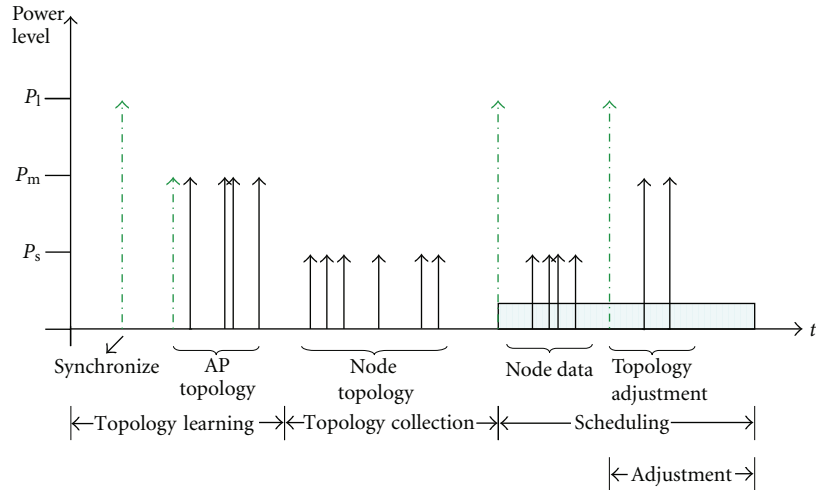


FIGURE 8: PEDAMACS phases: solid arrows are packets sent by nodes; dashed arrows show packets sent by the AP. Different power levels are used in different situations. Only the scheduling phase has defined time slots.

TABLE 1: WSNs MAC Protocol Comparison.

Name	Implemented	Applications	Synch. requirement	Overhead
S-MAC	Hardware	Event-driven, long idle periods, delay order of message time	Loose	RTS, CTS, ACK, SYNC
B-MAC	Simulation/hardware	Delay tolerant	None	Preamble
PW-MAC	Hardware	Low delay, long idle periods	None	Beacon
LEACH	Simulation	Periodic data collection and monitoring	Tight	ADV, Join-Req, schedule
Pedamacs	Simulation	Delay bounded	Tight	RTS, CTS, ACK, Synch, topology learning
PRIMA	Simulation	Different QoS	Tight	Synch, Schedule, CH election
IEEE 802.11	Simulation/hardware	High data rates, large energy source, smart terminals	None	RTS, CTS, ACK
IEEE 802.15.1	Simulation/hardware	Medium to low data rates, low-energy consumption	Tight	Synch transmissions, S, C
IEEE 802.15.4	Simulation/hardware	Medium to low data rates, low-energy consumption	Tight	Beacon, ACK
WirelessHART	Simulation/hardware	Process automation	Tight	Synch, schedule, routing, other
ISA100a	Simulation/hardware	Process automation	Tight	Synch, schedule, routing,

The main advantage of PRIMA is reducing packet delivery delay according to traffic requirements. PRIMA also shares with LEACH advantages in CH rotation, helping increase lifetime. However, if a CH dies, all nodes in the cluster become useless until a new CH election takes place, just as in LEACH. Additionally, overhead packets increase energy consumption.

5. MAC Protocol Summary

Table 1 summarizes the protocols presented in this paper, comparing some of their characteristics. Notice all contention-based protocols have been implemented in hardware, at least for tests shown in the particular cited study, while schedule-based ones have been implemented only in

simulations. Also notably, only PEDAMACS shows bounded delay for different network sizes.

The Applications column in Table 1 shows characteristics of applications that could benefit from the particular protocol. The Overhead column presents the type of control frames or other type of overhead used by each protocol. One example with no control frames is B-MAC where overhead is caused by the preamble size of the data frame. Regarding standards, control frames mentioned in the table are not the only ones used in each case: 802.15.1 uses supervisory (S) and control (C) frames, 802.11 uses control and management frames, and 802.15.4 has command frames. A detailed explanation of all control frames is in the standards presented in [9, 13, 17, 36, 37]. When using the Overhead column for comparison purposes, note each protocol has

TABLE 2: Performance comparison. Protocols in bold are the main subject in each reference mentioned. Others are the benchmarks considered in each case.

Protocol	Maximum energy consumption		Performance metric		Maximum latency	
	Value	Units	Comparison performed using	Platform/Tool	Value	Units
S-MAC [6]	6	Joules	Hardware	Mica	11	Seconds
S-MAC no sleep	29	Joules	Hardware	Mica	1	Second
B-MAC [28]	15	Milliwatts	Hardware	Mica2	1700	Milliseconds
S-MAC	35	Milliwatts	Hardware	Mica2	2700	Milliseconds
PW-MAC [29]	10	%duty cycle	Hardware	MicaZ	1	Second
WiseMAC	70	%duty cycle	Hardware	MicaZ	85	Second
RI-MAC	65	%duty cycle	Hardware	MicaZ	1	Second
X-MAC	70	%duty cycle	Hardware	MicaZ	77	Second
PEDAMACS [34]	13	Millijoules	Simulation	TOSSIM	0.2×10^6	Bit time
S-MAC	21	Millijoules	Simulation	TOSSIM	2.8×10^6	Bit time
IEEE802.11	19.5	Millijoules	Simulation	TOSSIM	0.45×10^6	Bit time
PRIMA-RT [35]	0.015	J/packet/node	Simulation	OMNeT++	15	Seconds
Q-MAC-RT	0.024	J/packet/node	Simulation	OMNeT++	5	Seconds

different control frame sizes and they are sent during different phases of communication, so the total overhead for a particular communication session varies and must be analyzed with respect to a particular application. However, as an illustration, consider a network with four nodes all within range of each other and only one node needs to send one packet. The communication procedure using S-MAC in that network is as follows: one node sends a SYNC frame, all nodes hear it and adopt the schedule and the node with a packet sends an RTS. The receiver answers with CTS, the data packet is transmitted, and the receiver sends one ACK. There are four control frames to send one packet. Now consider the same network using LEACH. One node sends an advertisement message (ADV) saying it is the cluster head, the other three nodes send join request messages, and the CH sends the TDMA schedule. After that, the node with data to transmit sends the packet. Total overhead in this case is five packets. So, even though Overhead column shows three types of control frames for LEACH and four types for S-MAC, the total overhead generated by each protocol may be smaller or larger depending upon the application and current state of the network.

Every protocol tries to improve on a particular metric, thus different performance variables are used to evaluate protocol usefulness. Table 2 shows detailed results presented in the papers as examples of the benefits of using each protocol. The Protocol column shows the main protocol presented in every study using bold characters and the protocol used as a benchmark in each paper with regular characters. The Maximum Energy Consumption column in Table 2 presents the highest value reported for each protocol. Not all papers used energy measurement units, so this column shows data for energy, power, or current consumption for comparison purposes, since the metrics are related. The Platform/Tool column shows the specific hardware or software used in

the experiments of each protocol, since not all protocols were tested using the same procedures. The Maximum Latency column illustrates the highest delay presented for each protocol. Tests are performed with different network sizes, topologies, and energy consumption models in each paper, making it difficult to directly compare protocols. Not all tests use the same units.

Results in Table 2 illustrate the performance comparison presented in each study; in all cases the main protocol has better performance than the protocols employed for comparison purposes. Note that PRIMA-RT means the real-time version of the protocol.

One of the protocols presented in Section 4 is not presented in Table 2, evaluation of the LEACH protocol employed the ns software package, but not for energy consumption or delay.

6. Conclusions

Previously there were no standard methods of comparing the performance of scheduled-based and contention-based protocols, or even for protocols belonging to the same category. The lack of standard evaluation metrics has made it difficult to evaluate and select a protocol, even if the requirements of a particular application are known. The number of wireless sensor network protocols is rapidly expanding so a set of protocols covering the widest possible breadth was selected for analysis. Using the analysis method and metrics presented in this paper suggests that contention-based approaches may be helpful when the network topology is random, application requirements are not delay constrained, and there is no mechanism to ensure tight synchronization. Analysis also shows that schedule-based approaches may be more energy efficient if deployment is not random and the base stations

include high-power transmitters and large energy stores which can be used to manage synchronization and schedules.

Protocol designers and users benefit from standard test methods that can be applied across all communication protocols for WSN, so that protocols can be measured using the same references and units, allowing for comparison and evaluation.

References

- [1] I. F. Akyildiz, S. Weilian, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.
- [2] X. Ning, R. Sumit, C. Krishna Kant et al., "A wireless sensor network for structural monitoring," in *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, pp. 13–24, ACM Press, November 2004.
- [3] M. Calle and J. Kabara, *Energy Consumption in Wireless Sensor Networks: Measuring Energy Consumption and Lifetime*, VDM Verlag, Saarbrücken, Germany, 2008.
- [4] IEEE, "IEEE Standards for local and metropolitan area networks: overview and architecture," *IEEE Std 802–2001 (Revision of IEEE Std 802–1990)*, 2001.
- [5] I. Demirkol, C. Ersoy, and F. Alagöz, "MAC protocols for wireless sensor networks: a survey," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 115–121, 2006.
- [6] W. Ye, J. Heidemann, and D. Estrin, "Medium access control with coordinated adaptive sleeping for wireless sensor networks," *IEEE/ACM Transactions on Networking*, vol. 12, no. 3, pp. 493–506, 2004.
- [7] K. Leentvaar and J. H. Flint, "The Capture Effect in FM Receivers," *IEEE Transactions on Communications*, vol. 24, no. 5, pp. 531–539, 1976.
- [8] R. Tjoa, K. L. Chee, P. K. Sivaprasad, S. V. Rao, and J. G. Lim, "Clock drift reduction for relative time slot TDMA-based sensor networks," in *Proceedings of the 15th Personal, Indoor and Mobile Radio Communications, (PIMRC '04)*, pp. 1042–1047, September 2004.
- [9] IEEE, "IEEE standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part II: wireless LAN medium access control (MAC) and physical layer (PHY) specifications IEEE Std 802.11g," pp. 67, 2003.
- [10] P. Ferrari, A. Flammini, D. Marioli, and A. Taroni, "IEEE802.11 sensor networking," *IEEE Transactions on Instrumentation and Measurement*, vol. 55, no. 2, pp. 615–619, 2006.
- [11] Bluetooth-SIG, *Specification of the Bluetooth System. Wireless Connections Made easy. Covered Core Package Version: 2.0+EDR*, 2004.
- [12] S. Rathi, "Bluetooth protocol architecture," *Dedicated Systems Magazine*, pp. 28–33, 2000.
- [13] IEEE, "IEEE Std 802.15.1—2005 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs)," *IEEE Std 802.15.1-2005 (Revision of IEEE Std 802.15.1-2002)*, pp. 0_1-580, 2005.
- [14] A. Tanenbaum, *Computer Networks*, Prentice Hall, Upper Saddle River, NJ, USA, 4th edition, 2003.
- [15] K. Sohrabi, J. Gao, V. Ailawadhi, and G. J. Pottie, "Protocols for self-organization of a wireless sensor network," *IEEE Personal Communications*, vol. 7, no. 5, pp. 16–27, 2000.
- [16] T.-Y. Lin, Y.-C. Tseng, K.-M. Chang, and C.-L. Tu, "Formation, routing, and maintenance protocols for the blueRing scatter-net of bluetooths," in *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*, p. 10, 2003.
- [17] IEEE, "IEEE standard for information technology—telecommunications and information exchange between systems—local and metropolitan area networks specific requirements part 15.4: wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs)," *IEEE Std 802.15.4-2003*, pp. 0_1-670, 2003.
- [18] G. Lu, B. Krishnamachari, and C. S. Raghavendra, "Performance evaluation of the IEEE 802.15.4 MAC for low-rate low-power wireless networks," in *Proceedings of the 23rd IEEE International Performance, Computing, and Communications Conference (IPCCC '04)*, pp. 701–706, April 2004.
- [19] Crossbow, *MPR- Mote Processor Radio Board MIB- Mote Interface/Programming Board User's Manual*, Crossbow Technology, 2006.
- [20] J. Song, S. Han, A. K. Mok et al., "WirelessHART: applying wireless technology in real-time industrial process control," in *Proceedings of the 14th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS '08)*, pp. 377–386, April 2008.
- [21] M. D. Biasi, C. Snickars, K. Landernäs, and A. J. Isaksson, "Simulation of process control with wirelessHART networks subject to packet losses," in *Proceedings of the 4th IEEE Conference on Automation Science and Engineering (CASE '08)*, pp. 548–553, August 2008.
- [22] T. Lennvall, S. Svensson, and F. Hekland, "A comparison of WirelessHART and ZigBee for industrial applications," in *Proceedings of the 7th IEEE International Workshop on Factory Communication Systems (WFCS '08)*, pp. 85–88, May 2008.
- [23] H. Hayashi, T. Hasegawa, and K. Demachi, "Wireless technology for process automation," in *Proceedings of the ICROS-SICE International Joint Conference*, pp. 4591–4594, Tokyo, Japan, August 2009.
- [24] N. Q. Dinh, S.-W. Kim, and D.-S. Kim, "Performance evaluation of priority CSMA-CA mechanism on ISA100.11a wireless network," in *Proceedings of the 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT '10)*, pp. 991–996, 2010.
- [25] V. Rajendran, K. Obraczka, and J. J. Garcia-Luna-Aceves, "Energy-efficient, collision-free medium access control for wireless sensor networks," *Wireless Networks*, vol. 12, no. 1, pp. 63–78, 2006.
- [26] T. V. Dam and K. Langendoen, "An adaptive energy-efficient MAC protocol for wireless sensor networks," *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys '03)*, ACM Press, pp. 171–180, 2003.
- [27] P. Lin, C. Qiao, and X. Wang, "Medium access control with a dynamic duty cycle for sensor networks," *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '04)*, vol. 3, pp. 1534–1539, 2004.
- [28] J. Polastre, J. Hill, and D. Culler, "Versatile low power media access for wireless sensor networks," in *Proceedings of the Second International Conference on Embedded Networked Sensor Systems (SenSys '04)*, pp. 95–107, ACM Press, November 2004.
- [29] L. Tang, Y. Sun, O. Gurewitz, and D. B. Johnson, "PW-MAC: an energy-efficient predictive-wakeup MAC protocol

- for wireless sensor networks,” *Proceedings of the IEEE INFOCOM*, pp. 1305–1313, 2011.
- [30] A. El-Hoiydi and J. -D. Decotignie, “WiseMAC: an ultra low power MAC protocol for multi-hop wireless sensor networks,” in *Proceedings of 1st International Workshop, Algorithmic Aspects of Wireless Sensor Networks*, vol. 3121, pp. 18–31, 2004.
- [31] Y. Sun, O. Gurewitz, and D. B. Johnson, “RI-MAC: a receiver initiated asynchronous duty cycle MAC protocol for dynamic traffic loads in wireless sensor networks,” in *Proceedings of the International Conference on Embedded Networked Sensor System (SenSys '08)*, 2008.
- [32] M. Buettner, G. V. Yee, E. Anderson, and R. Han, “X-MAC: a short preamble MAC protocol for duty-cycled wireless sensor networks,” in *Proceedings of the 4th International Conference on Embedded Networked Sensor Systems (SenSys '06)*, pp. 307–320, November 2006.
- [33] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, “An application-specific protocol architecture for wireless microsensor networks,” *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, 2002.
- [34] S. C. Ergen and P. Varaiya, “PEDAMACS: power efficient and delay aware medium access protocol for sensor networks,” *IEEE Transactions on Mobile Computing*, vol. 5, no. 7, Article ID 1637439, pp. 920–930, 2006.
- [35] J. Ben-Othman, L. Mokdad, and B. Yahya, “An energy efficient priority-based QoS MAC protocol for wireless sensor networks,” in *Proceedings of the IEEE International Conference on Communications*, pp. 1–6, 2011.
- [36] H. C. Foundation, *Wireless Devices Specification, HCF SPEC 290 Revision 1.0*, 2007.
- [37] Isa 100a. W. Group, *Wireless Systems for Industrial Automation: Process Control and Related Applications*, 2009.