APS010 APPLICATION NOTE

WIRELESS SENSOR NETWORKS AND THE DW1000

Version 1.1

This document is subject to change without notice

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

This application note describes the unique strengths of the DW1000 device and how they can complement and enhance wireless sensor network (WSN) technology.

The DW1000 is a physical layer ultra-wideband (UWB) radio and brings the features of location awareness, robust communications and resilience to multipath fading to a WSN.

In order to open up new applications with the combination of UWB and WSN, a clear understanding of the capabilities and limitations of the underlying technology is required. This application note aims to develop that understanding in the reader.

In section 2 the concept of the WSN is introduced, section 3 describes the network topologies that are possible and explains the advantages of multi-hop communications.

Section 4 describes the physical layer strengths of the DW1000 and provides a technical background on how the previously mentioned features are achieved.

In section 5 we discuss the layers of protocol stack that are required for a WSN node and show how the ranging and channel estimation capabilities of the DW1000 augment recent developments in WSN security.

Section 6 describes existing standards and summarizes some hardware and software platforms used for WSN realisation.

2 WHAT IS A WIRELESS SENSOR NETWORK?

A wireless sensor network (WSN) is a group of wireless nodes that are dispersed over a physical area and transport data.

This data may be the sample of some quantity (sensing) or the data may be a command to some device (actuating).

The main purpose of a WSN is to transport data wirelessly over a physical distance that is larger than a single wireless link between nodes.

The concept of a WSN originated from research into military applications by DARPA in the 1970's. For a more in-depth treatment on the history and evolution of WSNs see the following references (1), (2), (3).

A more formal definition of a WSN is that it could be considered as a physically distributed computing system that interacts with the surrounding environment and provides a means to efficiently transfer this interaction over a span of physical area larger than the transmission range of the individual radio links between nodes.

The nodes in a WSN may be static or mobile and will possess the following properties;

- They can communicate wirelessly with other nodes.
- They can perform remotely for an extended duration.
- They may sense some physical parameter in the environment.
- They may actuate some device in the environment.
- They may aggregate data from other nodes.
- They may disseminate data to other nodes.

Some nodes in a WSN may also have the following properties;

- They change behaviour of other nodes.
- They can route messages in a multi-hop networking capacity
- They can organise the topology of the network.
- They can bridge messages to another network.
- They can change behaviour to optimise some function such as energy consumption.

A WSN can provide a communications network with little or no wired infrastructure, which has efficiencies and economic benefits that may enable new applications that were not possible before.

A WSN may use a heterogeneous array of nodes and use an assorted mix of technology and protocol stacks within those nodes.

As a general rule because nodes in a WSN may be remote and unwired, energy efficiency is of vital importance to achieve practical network lifetimes.

Energy efficiency has important ramifications on the protocol stack in a WSN node and we will discuss energy efficiency in terms of DW1000 features and protocol stacks in later sections of the document.

2.1 The WSN design space

The design space for WSNs is immense and there is a large body of active research in many areas of WSN. Consider that in 2013 a search for "wireless sensor networks" in IEEE Xplore yields nearly 50,000 papers and a search on amazon.com returns 4,800 books.

Some practitioners (4) believe that WSN design is a far greater challenge than mobile phone networks and would like more realism to be reflected in WSN scientific publications in general.

The design of a WSN is outside the scope of this application note; however the reader will be directed to various references throughout. The following references may provide a better understanding of some of the issues involved in the design of WSNs (2) (5) (6) (7) (8) (9).

3 NETWORK ARCHITECTURES

The group of nodes in a WSN is typically deployed over some physical region of interest and has at least one node that performs as a sink node (also known as a gateway node) that communicates to an outside network.

3.1 Generic network architecture

Consider the generic WSN depicted in Figure 1. It has 17 sense nodes and 2 sink nodes.

The sink node connection to the outside network may be a wired or wireless link.

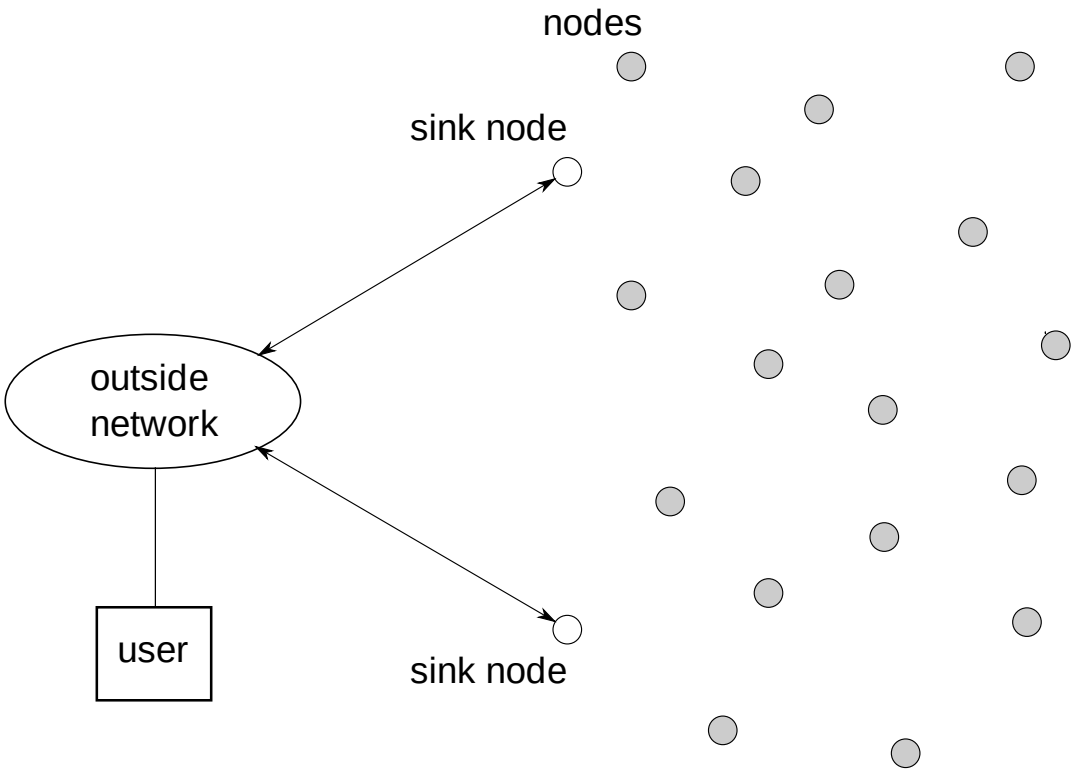

Figure 1: Wireless sensor network architecture.

We will now consider some different network architectures from this generic WSN.

3.2 Single-hop network architecture

A simple method to have nodes participate in the WSN is the single-hop network architecture as shown in Figure 2.

In the single-hop architecture the nodes have the ability to communicate with sink nodes but not with other nodes.

Some nodes in the figure are unconnected to the sink nodes because they are out of range so they cannot participate in the WSN with this simple architecture. This is a disadvantage of the single-hop architecture.

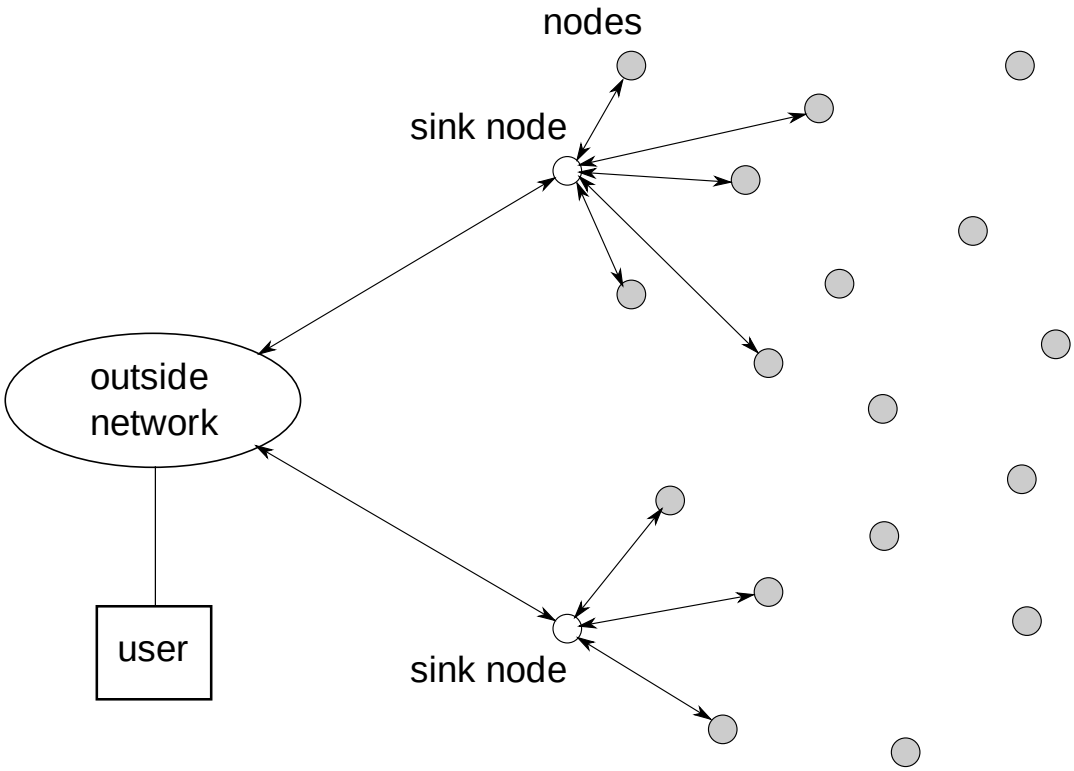

Figure 2: Single-hop wireless sensor network architecture.

In order to access the nodes that are further away from the sink nodes, it is necessary to alter the network architecture so that those nodes can participate.

Altering the network architecture consist of changing the behaviour of nodes. This is normally done by changing the software stack running on a node.

3.3 Cluster multi-hop network architecture

With the network architecture shown in Figure 3, some nodes have been assigned to function as cluster nodes.

The cluster nodes provide the following additional abilities;

- To aggregate data from other nodes.
- To disseminate data to other nodes.
- To perform a multi-hop routing function.

Because of the multi-hop function of the cluster nodes, almost all the nodes in the network are now reachable and can participate in the WSN. However one node is out of range from any cluster node so it cannot participate in the WSN.

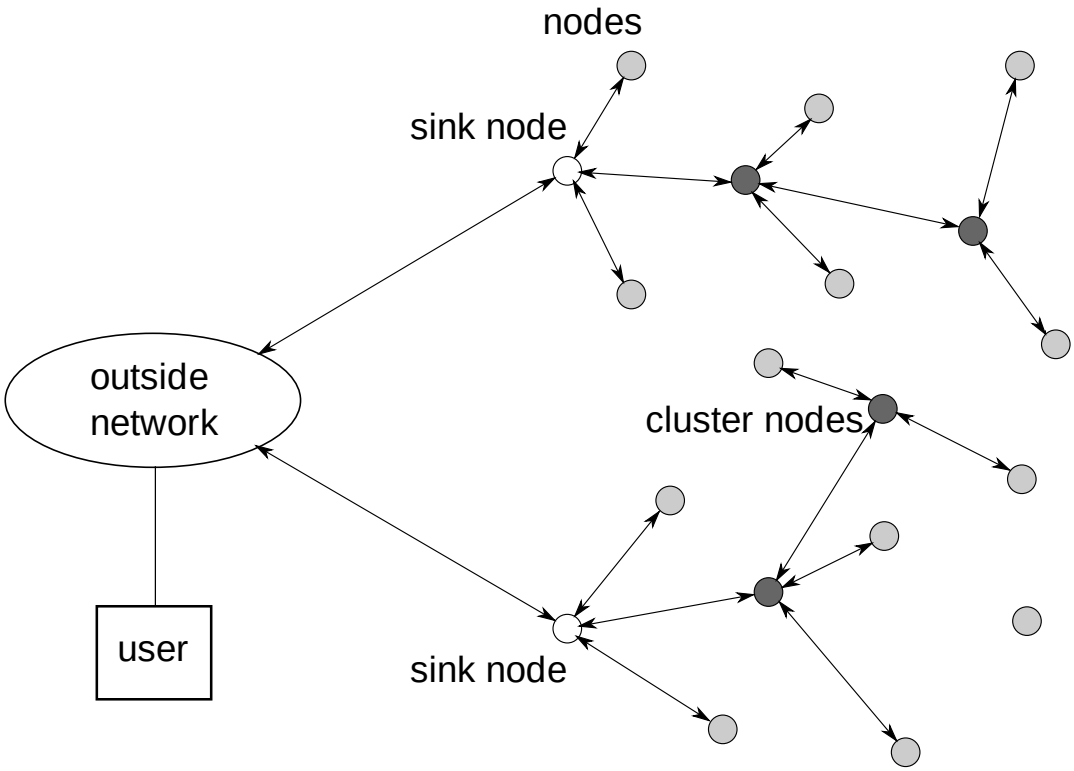

Figure 3: Cluster multi-hop wireless sensor network architecture.

However if any one of the cluster nodes is unreachable or unavailable, then the network will lose connectivity with any nodes that are associated with that cluster node.

3.4 Mesh multi-hop network architecture

In the network architecture shown in Figure 4, all of the nodes have the ability to communicate with multiple neighbouring nodes and also have the ability to aggregate, disseminate and multi-hop data through the network. Now all the nodes in the network are reachable.

If a communication link between any nodes is unavailable due to malfunction or mobility, there may be an alternative path through the network for communication with one of the sink nodes.

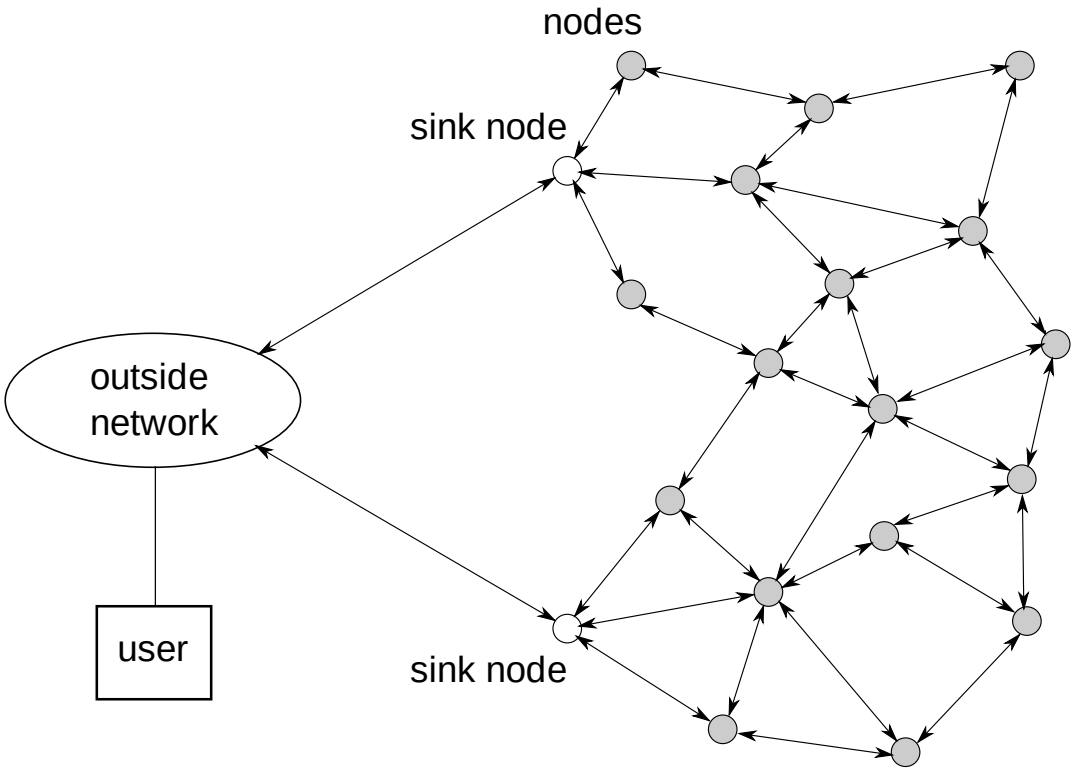

Figure 4: Mesh multi-hop wireless sensor network architecture.

A good discussion on some of the current industry standards that provide mesh networking capability is given in the paper (10).

In summary these WSN architectures are designed in advance depending on the application of the WSN. They are determined by the protocol stack running on the nodes which will be discussed in a later section.

3.5 The advantage of multi-hop communications

The nodes in a WSN will generally have severe energy constraints, primarily due to their power source being a battery. Therefore it is important to see the benefit of a multi-hop WSN architecture.

The radio communications over a link between nodes is relatively expensive in terms of power. The communications of 1-bit of information over a radio link is equivalent to the execution of 1000 to 3000 instructions on a microprocessor, see (11).

In a line of sight radio system, the losses are mainly due to free-space path loss (FSPL); the following equation which describes that path loss is due to Friis (12).

$$FSPL(dB) = 10log10(\frac{4\pi df}{c})^2$$

$$FSPL(dB) = 20log10(d) + 20log10(f) + 20log10(\frac{4\pi}{c})$$

So if the distance reduced by a factor of two but all other factors remain unchanged, then d = d/2, so the FSPL will change by,

$$20log10(0.5) = -6\ dB$$

This change of -6 dB is a four-fold reduction in power required for the link.

This means a sensor node needs a quarter of the transmit power to communicate over half the distance. This means that multi-hop networking is more efficient in terms of transmit power and the expense of more nodes.

A node in any WSN could use a routing table with range to neighbouring nodes as a metric to control the transmit power to the minimum it requires to reliably communicate with that neighbouring node.

For the DW1000 UWB PHY, the receive power is a constant for any link distance, therefore the policy or protocol that controls when the receiver is active is very important for energy conservation. This aspect will be confronted later in the discussion about the protocols used at the MAC sub-layer.

4 THE STRENGTHS AND CAPABILITIES OF THE DW1000

The building block of any node within a WSN is the physical layer (PHY) link. The DW1000 PHY has the capability to provide communication and precision ranging functions, even where a line of sight (LOS) radio path may not exist.

These capabilities enable a WSN to operate in harsh radio propagation channels where non line of sight (NLOS) conditions and many radio reflections exist such as inside buildings, shipping container yards and factories with metal objects.

The advantages of using UWB PHY technology in harsh radio environments has been evident for some time, in 1998 Scholtz and Win (13) showed that UWB radio propagation is robust against multipath fading.

4.1 The UWB impulse waveform

The DW1000 PHY device is a carrier-based impulse radio. For a better understanding of the strengths and capabilities of the DW1000, it is beneficial to review the waveforms that are transmitted.

The fundamental transmit waveform is the UWB impulse, it depends on,

- The carrier frequency.
- The baseband impulse shape and bandwidth.

The UWB impulses of the DW1000 are always generated at the chipping rate of 499.2MHz

The transmitter can only generate +1 or -1 UWB impulses as shown in Figure 5 and in this case the baseband impulse has a bandwidth of 499.2 MHz and the carrier frequency is 3494.4 MHz.

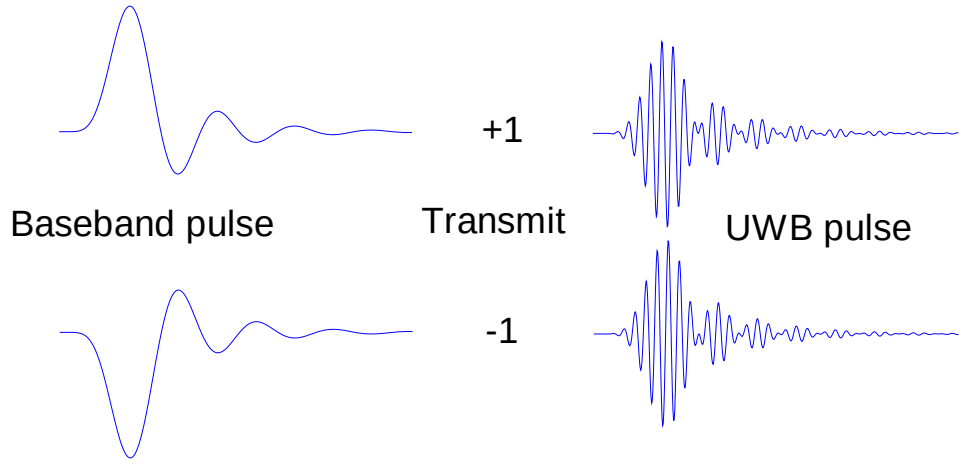

Figure 5: The UWB impulse waveform

By grouping together special patterns of +1 and -1 UWB impulses, the DW1000 PHY link obtains desirable properties. These patterns and their properties are discussed in the next sections.

4.2 DW1000 ranging capability

The DW1000 derives ranging capability from calculations using its ability to precisely timestamp message transmission and reception events.

The DW1000 acquires these precision timestamps by building an accurate estimate of the channel impulse response (CIR) and processing this data.

The DW1000 builds estimates of the CIR by correlating a known preamble sequence against the received signal and accumulating the result over a period of time. These preamble sequences are based on preamble codes from the large family of codes called perfect ternary sequences (14).

The preamble codes used in the DW1000 are defined in the IEEE802.15.4-2011 standard and are based on the work of Hoholdt (15) and Ipatov (16) but have been further modified, analysed and selected for the following properties,

- Perfect periodic autocorrelation in coherent and non-coherent receivers.
- Low cross-correlation between codes in the same complex channel.

The preamble codes are drawn from a ternary alphabet {-1, 0, +1} and an example length 31 code is as follows;

-0000+0-0+++0+-000+-+++00-+0-00

This code is then spread by inserting zero valued chips between the elements of the ternary code above. In the DW1000 this spreading yields preamble symbols that have nominal pulse repetition frequencies (PRF) of 16 MHz or 64 MHz, where each preamble symbol has a duration of approximately 1us.

The preamble symbols modulate the polarity of a single chip UWB pulse and are transmitted by the DW1000 in the synchronisation header (SHR).

The SHR consists of a synchronisation (SYNC) field and a start of frame delimiter (SFD) field. The SYNC field consists of a number of repeated preamble symbols.

The estimated CIR provides information about the first received radio path from another node. This radio path is known as the first path or leading edge of the CIR. The DW1000 contains signal processing technology that finds this leading edge in the CIR and produces timestamps to a resolution of 15 picoseconds. By using the DW1000 generated timestamps a ranging application can produce ranges to a precision of 10 cm.

The method used by DW1000 for ranging is known as threshold based time of arrival (TOA). For a more general background on the challenge of ranging in a multipath environment, see (17).

4.3 DW1000 communications robustness

As mentioned previously, a node based on the DW1000 will possess a robust communications link in environments considered harsh for radio propagation. To understand how this robustness is derived, the properties of the payload will be explained.

The DW1000 payload consists of a number of symbols. A single symbol carries two information bits.

- The payload bit is encoded as a burst in the symbol position
- The convolutional parity bit is encoded as the polarity of the burst.

A coherent receiver such as the DW1000 has the ability to see the polarity of a transmitted burst and so may utilise it in a convolutional decoding algorithm. This is known as systematic forward error correction (FEC) as the encoding preserves the original data bits

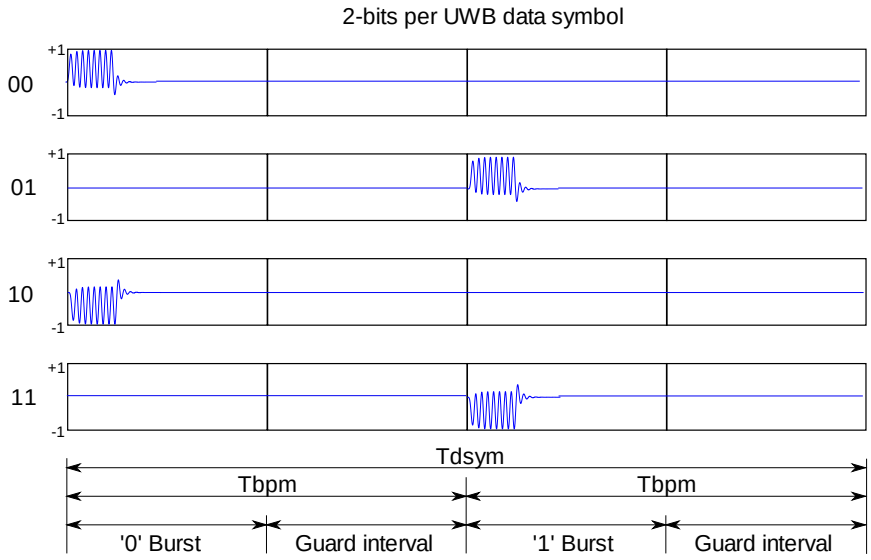

Figure 6: BPM-BPSK UWB data symbols with 8 chips per burst (unspread).

The guard intervals in the data symbols provide resistance to intersymbol interference

The CIR also provides a means to perform matched filtering on the payload. The matched filtering is performed at sample rate. This maximises the signal to noise ratio of each chip in the burst of each symbol before demodulation in the receiver. To understand more about the benefits of matched filtering, see the paper by Turin (18) .

Multi-user ability (on a different complex channel) is due to the spreading of the data payload.

This spreading consists of burst time-hopping and chip-rate polarity scrambling

The polarity spreading introduces a polarity scrambling at chip rate onto the burst.

- Provides additional interference suppression among coherent receivers.
- Provides spectral smoothing of transmit waveform.

The time-hopping introduces a pseudo-random hop-position onto the burst of chips.

- Provides for multi-user interference rejection.

The initial state of the LFSR is derived from the preamble sequence and each devices LSFR will be seeded asynchronously.

The DW1000 uses a coherent receiver architecture, which enables it to take advantage of the systematic convolutional FEC.

A non-coherent receiver cannot use the systematic convolutional FEC but it could use the

systematic Reed-Solomon FEC.

A reduced complexity receiver may choose to ignore the systematic FEC. This FEC provides a total coding gain of 8 dB[1] which extends the communications range of the DW1000.

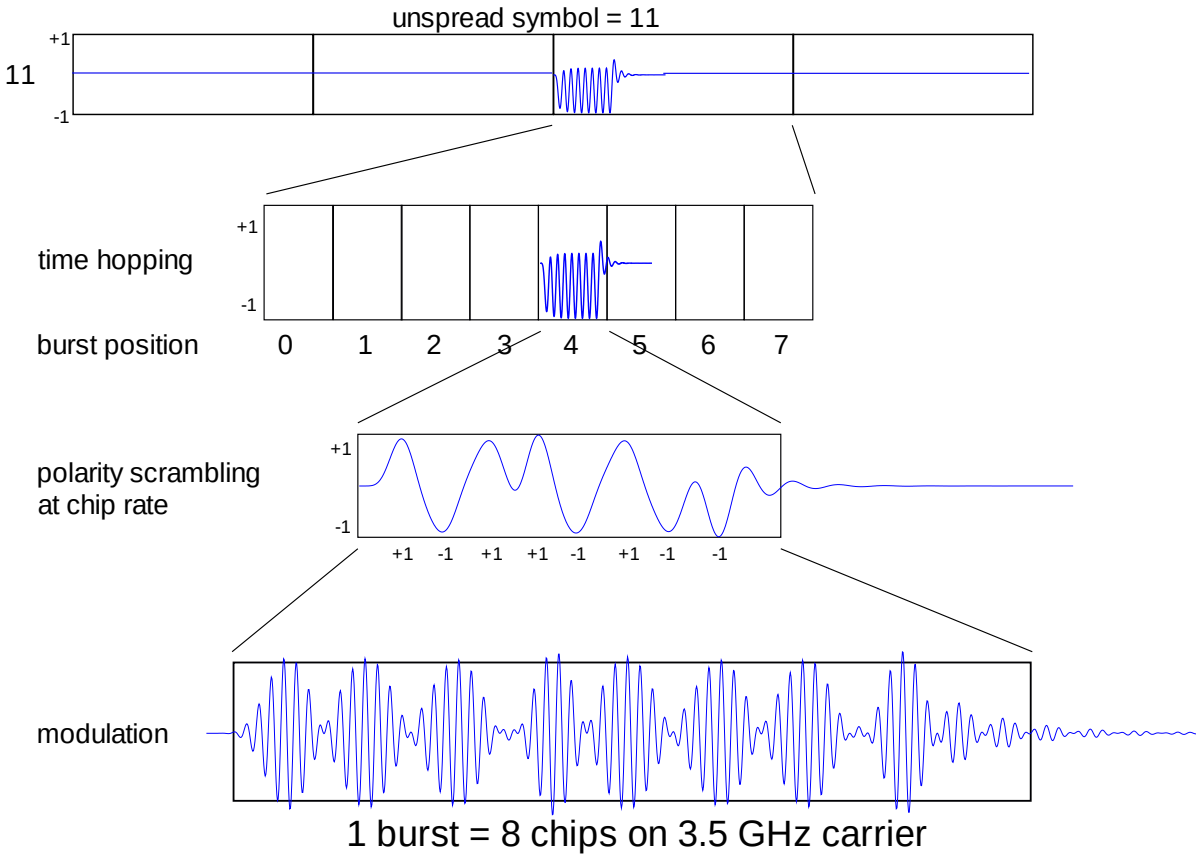

Figure 7: Spread spectrum BPM-BPSK UWB data symbol

The type of FEC used in the DW1000 is a concatenation of convolution coding and Reed-Solomon coding. The concatenation of these two error coding schemes, also known as inner and outer coding, was first suggested in 1966 by Forney (19).

The tutorial paper by Massey (20) is a good introduction into why this concatenation of different codes is beneficial.

The PHY symbol structure uses guard intervals of up to 2 us, so even in rich multipath environments, the communications are resistant to intersymbol interference

The PHY symbol structure also provides a mechanism for simple medium access due to time-hopping spread-spectrum which allows multi-user access (21).

The paper by Zhang and Molisch (22) provides further credibility in the benefits of using a UWB device such as the DW1000 in a WSN application.

[1] 3 dB BPSK, 3 dB rate ½, 2 dB RS.

5 WSN NODE PROTOCOL STACK

The functions required of a sensor node can be viewed as a partition of multiple layers of abstraction as shown in Figure 8. The WSN node protocol stack is modelled after the open systems interconnection (OSI) reference model (23).

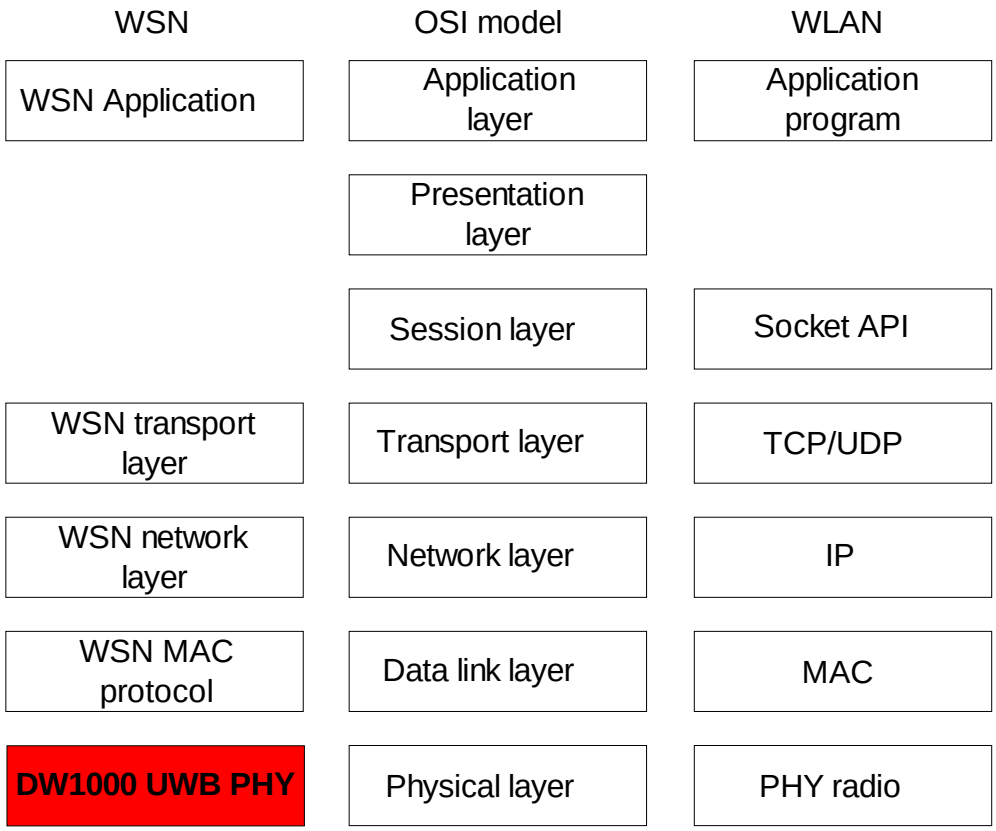

Figure 8: WSN node protocol stack compared to OSI model and WLAN device stack.

The DW1000 provides the physical layer of the protocol stack and has some MAC protocol assist features. The remaining layers of the protocol stack are realised as software executing on an external microprocessor.

5.1 WSN MAC protocol

The primary task of the WSN MAC protocol is to arbitrate access to a shared medium and avoid collisions. Thus, the MAC protocol determines when the node will transmit and when the node will receive.

As the lifetime of a node is a very important factor in WSN design, the behaviour of the MAC protocol has a pronounced effect on a nodes energy usage because the majority of the energy consumption is in the communications link.

There are other important factors such as scalability and adaptability in the design of a MAC protocol for a WSN node. Indeed, it may be worth trading other factors such as throughput or latency for energy efficiency.

In the MAC protocol, the four main sources of energy waste are: -

- Collisions – When two or more nodes transmit at the same time on the same complex channel. As a result there may be corruption and a re-transmissions are required.
- Overhearing – When a node receives a frame destined for another node.
- Listening – When a node is listening to the radio channel but there are no frames in the air.
- Control overhead – When the node is using the radio channel for control and not communications.

Plenty of research work has gone into the study and design of the MAC protocol of WSN nodes. A detailed survey on over 70 MAC protocols for WSN is presented in (24), while more recent developments in WSN MAC protocols are available in (25).

5.2 WSN Network layer

The WSN network layer is responsible for packet forwarding. This is where the multi-hop communications ability of the WSN emerges.

The distributed and dynamic nature of a WSN topology places demanding requirements on a routing protocol. To minimize energy consumption and maximise the lifetime of the WSN a routing protocol must be energy-efficient. The routing protocol may also have specific characteristics depending on the application and the network architecture.

The routing protocols for WSN are classified at a high level by network structure, communication model, topology and reliability. These can be further subdivided yielding 9 possible classifications. Under these classifications, 57 routing protocols for WSN are examined in the survey paper of (26).

Of particular interest to WSN users of the DW1000 are the location-based routing protocols. These take advantage of position information to relay data to specific regions of the WSN and not the entire WSN, thus saving energy.

5.3 WSN Transport layer

The WSN transport layer provides end-to-end communication services between nodes, such as between a sensor node and a sink node over multiple hops.

This layer provides services to the upper layer such as reliability, flow-control, congestion control, and an error free data stream. This layer has to deal with packets that have errors, lost or out-of-order.

Traditional TCP and UP based transport protocols are considered to have numerous disadvantages when used with WSNs. These disadvantages include,

- Overhead of connection-oriented handshake protocol.
- Congestion control reducing network bandwidth and wasting energy.
- End-to-end ACKs and retransmission is wasteful of energy.

For a more detailed discussion of these issues the reader is directed to chapter 11 of (27).

There are a least 15 transport layer protocols designed for WSNs, the following papers provide a survey of these, (28) (29).

5.4 WSN Application layer

This is the application layer of the sensor node, not to be confused with the user application of the WSN; however they will be closely related. This is the top level of the sensing or actuating stack where data enters or leaves the node.

In an energy efficient node, the flow of data at the application layer should be event-driven, so that the radio communications component, which cost the most energy, can be powered off most of the time.

A node can decide when an event has been detected, then trigger the radio channel and transmit the data associated with the event.

An example event could be when 1000 samples from a temperature sensor have been gathered and compressed, or when a mobile node has moved from a certain location.

This is the also the layer in a WSN where data is consumed or generated and aggregated or disseminated.

5.5 The Internet of things

The Internet of things (IoT) is a concept that arises because of the 128-bit address space available in IPv6. Previously IPv4 had 32-bit addresses, now with 128-bit addresses every networkable “thing” on the planet can have a unique address.

There is no requirement to have TCP/IP running on nodes in a WSN, however some researchers in (27) consider there are significant disadvantages to doing so.

Dunkels thesis (30) states that “While it is unquestionably true that TCP/IP protocols were not designed to run in the kind of environments where sensor networks are envisaged, the claim that TCP/IP is inherently unsuitable for wireless sensor networks has not been verified”.

Given the pervasiveness of TCP/IP, the ability to have TCP/IP across a WSN may be an advantage. Proposals for a standardized protocol stack for IoT are presented in (31).

In an IP-connected IoT, WSNs will be connected to the untrusted, unreliable and vulnerable internet. The paper in (32) analyses the security challenges that arise in these WSNs.

5.6 Ranging and location

Because the DW1000 has the capability to precisely timestamp message events to a resolution of 15 ps, ranging to an accuracy of 10 cm and subsequent location of sensor nodes in the WSN is possible.

In two-way ranging, a node exchanges timestamps with another node to calculate a time of flight (TOF) between the nodes. This allows the calculation of a range between the two nodes.

In one-way ranging, a node can transmit blinks to a number of other receiving nodes. The timestamps from these other receiving nodes are used as time difference of arrival (TDOA) values. A multilateration algorithm can then calculate the position of the transmitting node from the TDOA values.

If the receiving nodes are in fixed location then the scheme is known as anchor based location. If the receiving nodes are mobile then the scheme is known as anchor-less

location, however the receiving nodes may need to locate themselves before the TDOA multilateration is performed.

Another scheme of relevance to WSNs is cooperative localization. This is where neighbouring nodes assist a node in the process of location determination, see (33) .

5.7 WSN security

As WSNs have many applications in both commercial and military areas, it is critical to consider security mechanisms in the WSN.

A well secured WSN should have security services in three places,

- At the WSN MAC layer, this is node-to-node communication.
- At the WSN application layer, this is sensor-to-app communication.
- At the interface to the outside network, this is gateway-to-server communication.

An example WSN with these three security services is shown in Figure 9.

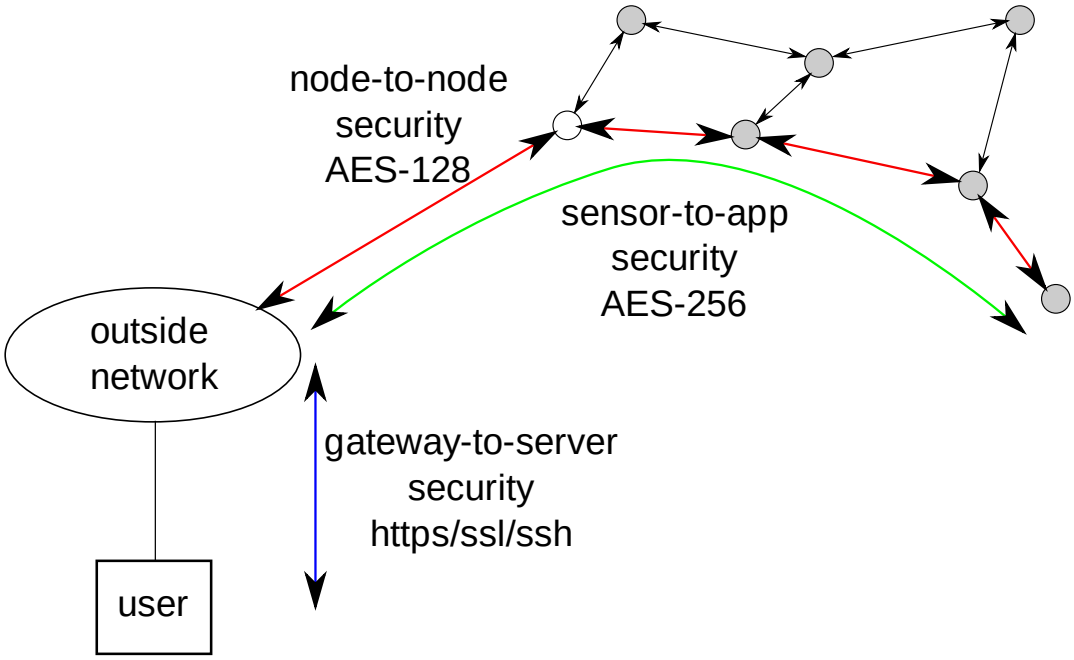

Figure 9: Three layers of security in a WSN.

Figure 10 shows the protocol stack and simplified view of the payloads associated with the layering of security in the WSN.

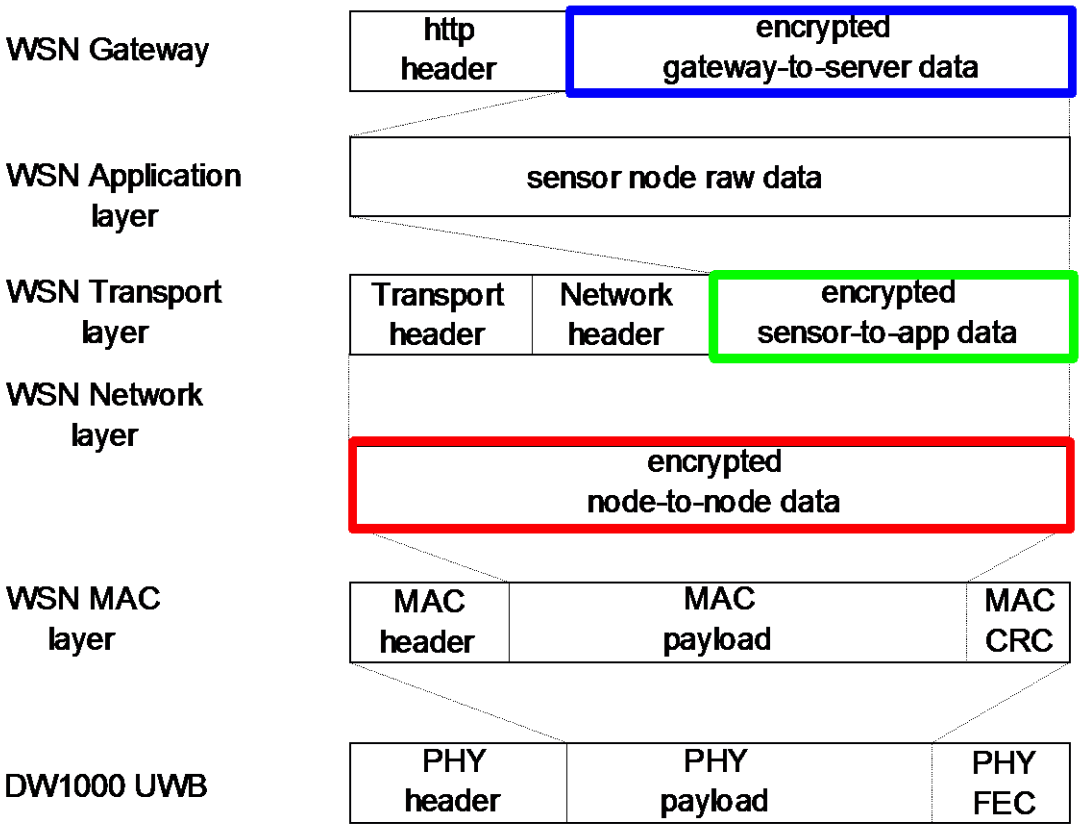

Figure 10: A simplified view of a secure WSN protocol stack

A secure WSN should provide services that meet most of the following requirements;

- Confidentiality – To protect against eavesdropping.
- Authenticated encryption – Need to ensure data has not been tampered with.
- Privacy – This desirable if location information of source and destination nodes is to remain hidden.
- Denial of service – The attacker introduces interference to modify in-air packets.
- Non-repudiation of origin – The source node cannot deny having sent a message.
- Non-repudiation of receipt – The destination node cannot deny having received a message.
- Freshness – This is to avoid replay attacks, timestamps may be used.
- Key distribution – The task of distributing secret keys to all the communicating nodes.

Some of these seemingly modest requirements have large computational burdens. These transform into challenging problems when they are expected to be realised on resource and energy constrained sensor nodes.

There are recent developments in WSN security using the ranging capability of nodes to improve WSN security. The paper by Capkun and Hubaux (34) analyses attacks on the positions of nodes and they propose a mechanism called verifiable multi-lateration for the secure location of nodes in a WSN. It is based on an authenticated ranging protocol as opposed to a distance bounding protocol where the nodes are untrusted.

Other interesting developments use the reciprocity of the UWB channel estimate between two nodes as a common signature (35). This may be used for generation of a shared secret

between the nodes. This can avoid the computational burden of public key crypto for key sharing.

To summarise, the ranging and channel estimation capabilities of the DW1000 enable the implementation of these recent schemes which improve the security of WSNs.

6 EXISTING WSN STANDARDS AND PLATFORMS

At present there is no common standardised WSN platform. Various standards, hardware are software platforms are in existence. In this section we will cover a subset of the available standards and platforms.

6.1 Standards based WSN protocols

6.1.1 IEEE 802.15.4

IEEE 802.15.4 is a publicly available standard specification that defines the physical layer and medium access sub-layer for low-rate wireless personal area networks. It focuses on low-cost, low-rate ubiquitous communications between wireless devices. It is designed to operate in unlicensed, international frequency bands.

It is the basis for higher layer specifications including ZigBee and WirelessHART.

The DW1000 device implements the UWB physical layer of IEEE 802.15.4 specification.

6.1.2 ZigBee

ZigBee is a proprietary specification for a suite of high level communications protocols using IEEE 802.15.4 based radios. The technology defined by the specification is intended to be simpler and less expensive than other WPAN standards such as Bluetooth.

6.1.3 WirelessHART

WirelessHART is a proprietary specification for a wireless mesh network that sits on top of IEEE 802.15.4 radios. The specifications are available for purchase. The WirelessHART protocol is based on the original highway addressable remote transducer (HART) wired protocol which superimposes digital signals using FSK on the 4-20mA analog current loop signals. It defines and adds capabilities to the HART protocol while maintaining compatibility with existing HART devices, commands and tools.

6.1.4 ISA100

ISA100 is an acronym for a committee within the international society for automation (ISA). The ISA100 committee develops a family of standards. The ISA100.11a is a standard for wireless field devices in scalable plant-wide systems and is available for purchase. It supports 6LoWPAN over IEEE 802.15.4 radios.

6.1.5 6LoWPAN

6LoWPAN is an acronym of IPv6 over low power wireless personal area networks. It is the name of an IETF working group. The working group has defined encapsulation and header compression mechanisms that allow IPv6 packets to be sent and received over IEEE 802.15.4 based networks. The base specification developed by the working group is RFC 4944 (http://tools.ietf.org/html/rfc4944)

6.1.6 IP500

IP500 is an open, non-proprietary and high-performance platform intended for secure building automation. It uses and supports IEEE 802.15.4-2006, 6LoWPAN, IPv6, IPSec, BACnet and AES128.

6.1.7 IEEE 802.15.5

IEEE 802.15.5 is a recommended practice to define mesh networking capabilities for low-rate and high-rate wireless personal area networks (LR-WPAN and HR-WPAN). The low-rate mesh is built on the IEEE 802.15.4 MAC, while the high-rate mesh is built on the IEEE 802.15.3 MAC. The two mesh networks are independent and cannot communicate with each other. See (36) for further details on this.

Detailed comparison of two industrial standards WirelessHART and ISA100 is presented in (37), while the ZigBee standard is also compared with them in (38).

6.2 WSN Software platforms

This section looks at the various options for programming the nodes within a WSN before deployment. However the basic question of how a WSN should be reprogrammed after deployment still remains un-standardised. Once deployed, the nodes in a WSN may be physically unreachable. A spectrum of re-programmability needs emerges, from simple parameter adjustments in the nodes, to uploading of complete binary images to hundreds of nodes. A survey of operating systems is given in (39).

6.2.1 Contiki

Contiki is a free open source operating system designed for the Internet of Things. It supports IPv6, IPv4, and recently standardized IETF 6lowpan, RPL, CoAP. Applications are written in standard C. With the Cooja simulator a Contiki network can be simulated. It provides mechanisms for estimating systems power consumption to understand where power was spent. It runs on a wide variety of hardware platforms.

6.2.2 TinyOS

TinyOS is a free open source operating system designed for WSNs. It supports multiple microcontroller families and radio chips. Because TinyOS has thousands of users and its existing design is over 5 years old, the code is robust and efficient and has very few bugs. TinyOS is programmed in a dialect of C called nesC, this provides linguistic support for the underlying execution and programming model. For further information see http://www.tinyos.net

6.2.3 Lorien

Lorien is a pure dynamic operating system targeted at WSN platforms. It is built with a dynamic component model and the entire software systems is uniformly modelled. This allows any components from drivers to applications to be downloaded at runtime and loaded into the running system.

6.2.4 Squawk virtual machine

The Squawk virtual machine (VM) is a Java VM written in Java and designed for resource constrained devices and is open source.

Squawk provides a wireless API for the IEEE 802.15.4 protocol, this extends on the generic connection framework and provides for radio and radiogram connection types.

6.2.5 Maté virtual machine

Maté is a byte-code interpreter that runs on TinyOS. It is a single TinyOS component that sits on top of several systems components, including sensors, the network stack and non-

volatile storage. The high-level interface of Maté allows programs to be very short, reducing the energy cost of transmitting new programs.

6.2.6 TinyDB

TinyDB is a query processing systems for extracting information from a network of TinyOS sensor nodes. TinyDB does not require you to write embedded C code for the nodes, instead it provides a simple SQL-like interface to specify the data you want to extract, along with additional parameters, like the rate at which the data should be refreshed.

Given a query specifying your data interests, TinyDB collects that data from nodes in the WSN, filters it, aggregates it together and routes it out to you.

The primary goal of TinyDB is to make life as a programmer significantly easier and allow data-driven applications to be developed and deployed much more quickly by freeing you from the burden of writing low-level code for nodes.

6.2.7 WSN Middleware

The purpose of middleware is to support the development, maintenance and deployment of WSN based applications. It is required to bridge the gap between the software running on WSN nodes and users applications by providing mechanisms to formulate high-level sensing task and communicating them to the WSN. The software components mentioned above such as Mate and TinyDB are classes of middleware. WSN middleware is a large subject in its own right and beyond the scope of this application note; some surveys are available in (40) and (41).

6.3 WSN Hardware platforms

This section looks at some of the commercially available WSN hardware platforms. They are all essentially variations on the same fundamental components of a sensor node, a microprocessor, a radio, some transducers and a battery.

6.3.1 WaspMote

The WaspMote from Libelium features a motherboard based on the Atmel ATmega1281. It provides for socketed interface of radio boards and sensor boards. There are 7 radio boards, Zigbee, WiFi, 6LoWPAN, 3G/GPS, GSM, Bluetooth, RFID. Any two radio boards can be simultaneously connected to the motherboard. There are 8 sensor boards available and includes a 3.7V 6600mAh rechargeable lithium-ion battery. It is programmed in C and the software libraries available for the platform enable over the air programming and encryption.

6.3.2 SunSPOT

The SunSPOT (Sun small programmable object technology) is a sensor node developed by Sun Microsystems. Some of the hardware design is open source and complete kits are sold by Oracle. It has a processor board based on the ARM920T core and includes an IEEE 802.15.4 radio. It also has a sensor board and includes a 3.7V 750mAh rechargeable lithium-ion battery. It is programmed in Java ME and runs the Squawk virtual machine.

6.3.3 TelosB/TMote

The TelosB and TMote Sky motes are based on open source designs from the University of California, Berkeley. They are based on the MSP430 and use the CC2420 IEEE 802.15.4 radio. They have a number of on-board sensors and have been designed with a form factor to accommodate 2x AA batteries. The software is based on TinyOS.

6.3.4 Shimmer

The Shimmer is a wearable mote originally developed by Intel Digital Health Group for the Mercury project at Harvard sensor networks lab. A direct derivative, the shimmer3 is commercially available and is a body worn wireless sensor node. It is also based on the MSP430 with 802.15.4 radio and a Bluetooth radio. It has multiple sensors on-board and includes a 450mAh rechargeable lithium-ion battery. The software is based on TinyOS.

7 REFERENCES

1. **C. Chong, S. Kumar.** Sensor networks : Evolution, opportunitites and challenges. *Proceedings of the IEEE.* August, 2003, Vol. 91, 8, pp. 1247-1256.
2. **C. Buratti, A. Conti, D. Dardari, R. Verdone.** An Overview on Wireless Sensor Networks Technology and Evolution. *MDPI Sensors.* 2009, Vol. 9.
3. **Editors.** A Sense of Things to Come. *The Economist.* 2007, April 28th.
4. **M. Kuorilehto, M. Kohvakka, J. Suhonen, P. Hamalainen, M. Hannikainen, T. Hamalainen.** *Ultra-Low Energy Wireless Sensor Networks in Practice : Theory, Realization and Deployment.* s.l. : John Wiley and Sons, 2007.
5. **Kenneth, C.** Wireless Sensors : A Device and Material Perspective. 2010.
6. **D. Puccinelli, M. Haenggi.** Wireless sensor networks : Applications and challenges of ubiquitous sensing. *IEEE Circuits and systems magazine.* 2005, Third quarter.
7. **G. Barrenetxea, F. Ingelrest, G. Schafer, M. Vetterli.** The hitchhikers guide to successful wireless sensor network deployments. *SenSys 08, Proceedings of the 6th ACN conference on embedded network sensor systems.* 2008.
8. **P. Corke, T. Wark, R. Jurdak, W. Hu, P. Valencia, D. Moore.** Environmental Wireless Sensor Networks. *Proceedings of the IEEE.* November, 2010, Vol. 98, No. 11.
9. **A. Mahapatro, P. Khilar.** Fault Diagnosis in Wireless Sensor Networks : A Survey. *IEEE Communications Surveys and Tutorials.* 2013.
10. **D. Rodenas-Herraiz, A. Garcia-Sanchez, F. Garcia-Sanchez, J. Garcia-Haro.** Current Trends in Wireless Mesh Sensor Networks : A Review of Competing Approaches. *MDPI Sensors Journal.* 2013, Vol. 13.
11. **W.M. Merrill, K. Sohrabi, L. Girod, J. Elson, F. Newberg, W. Kaiser.** Open standard develoment platforms for distributed sensor networks. *Proceedings of SPIE.* Unattended Ground Sensor Technologies and Applications IV, 2002, Vol. 4743.
12. **Friis, H.T.** A Note on a Simple Transmission Formula. *Proceedings of the IRE.* May, 1946, Vol. 34, 5.
13. **M. Win, R. Scholtz.** On the Robustness of Ultra-Wide Bandwidth Signals in Dense Multipath Environments. *IEEE Communications Letters.* February, 1998, Vol. 2, 2.
14. *Difference Sets, Sequences and their Correlation Properties.* **A. Pott, P. Kumar, T. Helleseth, D. Jungnickel.** 542, s.l. : NATO Science Series, 1999, Vol. Series C : Mathematical and Physical Sciences.
15. *Ternary sequences with perfect periodic autocorrelation.* **Hoholdt, T. Justensen, J.** 29, s.l. : IEEE Transactions on Information Theory, 1983.
16. *Ternary sequences with ideal periodic autocorrelation properties.* **Ipatov, V.** 24, s.l. : Radio Engineering and Electronic Physics, 1979.
17. **D. Darrdari, A. Conti, U. Ferner, A. Giorgetti, M. Win.** Ranging with Ultrawide Bandwidth Signals in Multipath Environments. *Proceedings of the IEEE.* February, 2009, Vol. 97, 2.
18. *An introduction to digital matched filters.* **Turin, G.** 7, s.l. : Proceedings of the IEEE, 1976, Vol. 64.
19. *Concatenated codes, PhD. dissertation.* **Forney, D.** s.l. : MIT Press, 1966.
20. *The How and Why of Channel Coding.* **Massey, J.** s.l. : Internation Zurich Seminar, 1984, Vols. March 6-8.
21. **M. Win, R. Scholtz.** Ultra-Wide Bandwidth Time-Hopping Spread-Spectrum Impulse Radio for Wireless Multiple-Access Communications. *IEEE Transactions on Communications.* April, 2000, Vol. 48, 4.
22. **J. Zhang, P. Orlik, Z. Sahinoglu, A. Molisch, P. Kinney.** UWB Systems for Wireless Sensor Networks. *Proceedings of the IEEE.* 2009, Vol. 97, February.
23. **Zimmerman, H.** OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection. *IEEE Transactions on Communications.* 1980, Vols. COM-28, 4.
24. **A. Bachir, M. Dohler, T. Watteyne, K. Leung.** MAC essentials for wireless sensor networks. *IEEE Communications Surveys and Tutorials.* Second Quarter, 2010, Vol. 12, No. 2.

25. **P. Huang, L. Xiao, S. Soltani, M. Mutka, N, Xi.** The Evolution of MAC protocols in Wireless Sensor Networks : A Survey. *IEEE Communications Surveys and Tutorials.* 2013, Vol. 15, 1.
26. **N. Pantazis, S. Nikolidakis, D. Vergados.** Energy-Efficient Routing Protocols in Wireless Sensor Networks : A Survey. *IEEE Communications Surveys and Tutorials.* Second Quarter, 2013, Vol. 15, 2.
27. **J. Zheng, A. Jamalipour.** *Wireless Sensor Networks : A Networking Perspective.* s.l. : IEEE, 2009.
28. **Ayadi, A.** Energy-Efficient and Reliable Transport Protocols for Wireless Sensor Networks : State-of-Art. *Scientific Research : Journal of Wireless Sensor Network.* 3, 2011.
29. **C. Wang, K. Sohraby, L. Bo, M. Daneshmand.** A Survey of Transport Protocols for Wireless Sensor Networks. *IEEE Network.* 2006, Vol. 20, 3.
30. **Dunkels, A.** *Towards TCP/IP for Wireless Sensor Networks.* Vasteras, Sweden : Department of Computer Science and Electronics, Malardalen University, 2005.
31. **M. Palattella, N Accettura, X. Vilajosana, T. Watteyne, L. grieco, G. Boggia, M. Dohler.** Standarized Protocol Stack for the Internet of (Important) Things. *IEEE Communications Surveys and Tutorials.* 2013, Vol. 15, 3.
32. **F. Li, P. Xiong.** Practical Secure Communication for Integrating Wireless Sensor Networks into the Internet of Things. *IEEE Sensors Journal.* October, 2013, Vol. 13, 10.
33. **N. Patwari, J. Ash, S. Kyperountas, A. Hero, R. Moses, N. Correal.** Locating the Nodes : Cooperative Localization in Wireless Sensor Networks. *IEEE Signal Processing Magazine.* 2005, July.
34. **S. Capkun, J. Hubaux.** Secure Positioning in Wireless Networks. *IEEE Journal on Selected Areas in Communications.* 2006, Vol. 24, 2.
35. **R. Wilson, D. Tse, R. Scholtz.** Channel Identification : Secret Sharing using Reciprocity in Ultrawideband Channels. *IEEE International Conference on Ultra-Wideband.* 2007.
36. **M. Lee, R. Zhang, C. Zhu, T. Park, C. Shin, Y. Jeon, S. Lee, S. Choi, Y. Liu, S. Park.** Meshing Wireless Personal Area Networks : Introducing IEEE 802.15.5. *IEEE Communications Magazine.* January, 2010.
37. **Low, A.** Evolution of Wireless Sensor Networks for Industrial Control. *Technology Innovation Management Review.* 2013, May.
38. **P. Radmand, A. Talevski, S. Petersen, S. Carlsen.** Comparison of Industrial WSN Standards. *IEEE International Conference on Digital Ecosystems and Technologies.* 4th, 2010.
39. **M. Farooq, T. Kunz.** Operating Systems for Wireless Sensor Networks : A Survey. *MDPI Sensors.* 2011, Vol. 11.
40. **I. Chatzigiannakis, G, Mylonas, S. Nikoletseas.** 50 ways to build your application : A survey of Middleware and Systems for Wireless Sensor Networks. *IEEE Conference on Emerging Technogies and Factory Automation.* 2007, September.
41. **S. Afzal, C. Huygens, W. Joosen.** Extending middleware frameworks for Wireless Sensor Networks. *Internation Conference on Ultra Modern Telecommunications.* 2009, October.

8 DOCUMENT HISTORY

Table 1: Document History

Revision	Date	Description
0.1		Initial release
1.1	08/08/18	Updates for new logo and template. And added these revision tables.

9 MAJOR CHANGES

V0.1

Page	Change Description
All	Initial external release

v1.1

Page	Change Description
All	New logo and template.
28	New section for “Further Information”
28	New revision 1.1 and addition to Revision table for Document History.

10 FURTHER INFORMATION

Decawave develops semiconductors solutions, software, modules, reference designs - that enable real-time, ultra-accurate, ultra-reliable local area micro-location services. Decawave's technology enables an entirely new class of easy to implement, highly secure, intelligent location functionality and services for IoT and smart consumer products and applications.

For further information on this or any other Decawave product, please refer to our website www.decawave.com.