Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

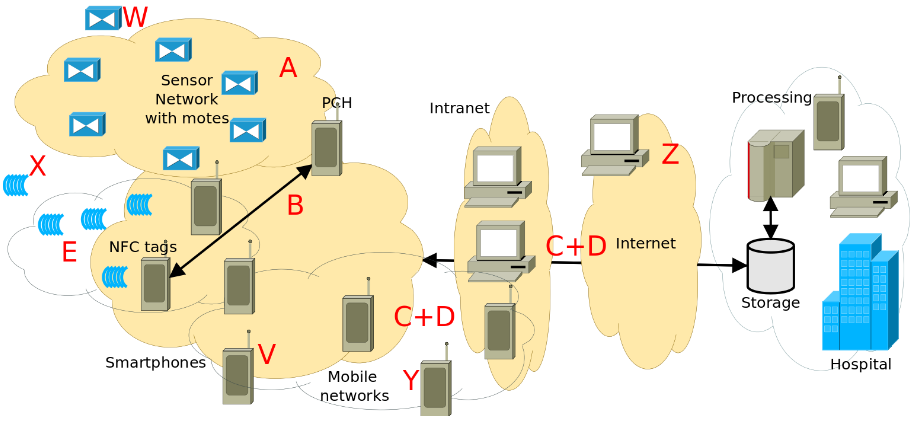
Note

Defining the ASSET Lab

ASSET D6.2 Technical Note:

Case study simulation and evaluation

Version 1



Note no DART/16/12

Authors
Wolfgang Leister
Pål Anders Floor
Yared Berhanu Woldegiorgis
Ilangko Balasingham
Habtamu Abie

Date December 2012

The authors

Wolfgang Leister, assisting research director at Norsk Regnesentral, received the Dr. rer. nat. degree in 1991 from the Universität Karlsruhe, Germany. His research interests cover smart information systems, multimedia, computer graphics, computer and sensor networks, health care applications, mobile systems, and free software.

Yared Berhanu Woldegiorgis is a master student at the University of Oslo. He completed his undergraduate degree in computer science from Addis Ababa University and worked at Hawassa University, Ethiopia, as graduate assistant and network administrator. His research interests include wireless sensor networks, cloud computing for the IoT and automation based expert systems.

Pål Anders Floor is currently a postdoctoral fellow at the Intervention Centre at the Oslo University Hospital. He received his PhD degree from the NTNU in 2008. His research interest are joint source-channel coding, information theory, and signal processing applied on point-to-point links, in small and large networks, as well as in neuroscience.

Habtamu Abie is currently a Senior Research Scientist at NR. He received his B.Sc., M.Sc. and Ph.D. from the University of Oslo, and has many years of experience in computing, both as practitioner and researcher. He has a solid and extensive background in the design and development of real-time systems, and the design, modeling and development of security for distributed object computing systems.

Ilangko Balasingham is Senior Research Scientist at the Interventional Center, Oslo University Hospital. He received the Siv.Ing (MSc) and Dr.Ing. (PhD) degrees from the NTNU in 1993 and 1998, respectively. His research interests include medical signal and image processing, wireless biomedical sensor networks for short range sensing, imaging, localization and communication, and multimedia patient record systems.

Norwegian Computing Center

Norsk Regnesentral (Norwegian Computing Center, NR) is a private, independent, non-profit foundation established in 1952. NR carries out contract research and development projects in the areas of information and communication technology and applied statistical modeling. The clients are a broad range of industrial, commercial and public service organizations in the national as well as the international market. Our scientific and technical capabilities are further developed in co-operation with The Research Council of Norway and key customers. The results of our projects may take the form of reports, software, prototypes, and short courses. A proof of the confidence and appreciation our clients have for us is given by the fact that most of our new contracts are signed with previous customers.

Title	**Defining the ASSET Lab** **ASSET D6.2 Technical Note:** **Case study simulation and evaluation – Version 1**
Authors	**Wolfgang Leister, Pål Anders Floor, Yared Berhanu Woldegiorgis, Ilangko Balasingham, Habtamu Abie**
Quality assurance	Åsmund Skomedal, Trenton Schulz
Date	December 2012
Publication number	DART/16/12

Abstract

This note represents Deliverable D6.2 of WP4 in the ASSET project (Case Study, simulation and evaluation of results in eHealth). In this note we describe the contents of a laboratory for experimenting with adaptive security. Starting from a security model for equipment used in eHealth, we identify classes of suitable devices in the Internet of Things, describe their characteristics, and give a market survey of such devices.

Keywords	ASSET, lab, motes, sensors, equipment, Internet of Things, adaptive security
Target group	Participants
Availability	Open
Project	ASSET
Project number	320485 (NFR 213131/O70)
Research field	Internet of Things, Security
Number of pages	44
© Copyright	Norwegian Computing Center

Contents

1 Introduction

The ASSET project will research and develop risk-based adaptive security methods and mechanisms for the Internet of Things (IoT) that will estimate and predict risk and future benefits using game theory and context awareness. The security methods and mechanisms will adapt their security decisions based upon those estimates and predictions.

ASSET focuses on the following activities that will provide the research hypotheses: *a*) building models for estimating and predicting risks and benefits using game theory and context awareness; *b*) building methodology for security measurement and metrics for validating the effectiveness of the adaptation based on best practice; *c*) prototyping the adaptive methods for authentication and access control for IoT and using them in a simulated eHealth patient monitoring scenario in Oslo University Hospital; and *d*) building light-weight abilities in smart things that will allow them to detect in real-time unknown security and privacy threats, respond to them, and adapt to the environment and changing degree of security and privacy breaches.

The main application area of ASSET is health and welfare. Health organisations may deploy IoT-based services to enhance traditional medical services and reduce delay for treatment of critical patients. ASSET's case study will lead to a simulation experiment at the test-bed that belongs to the Oslo University Hospital: Blood pressure, electrocardiogram (ECG) and heart rate values will be gathered from patients, where the patient ID will be removed and the sensor data made anonymous. The sensor data will be stored in different biomedical sensor nodes that are capable of communicating with any of the following connectivity options available: ZigBee, Wi-Fi, 3G, GPRS, Bluetooth, and 802.15.4. A smartphone, for instance, with a ZigBee-transceiver will act as an access point that communicates with both ZigBee sensor nodes and a Medical Centre.

In the current document we will present suggetions for an experimentation lab that will support and facilitate practical experiences for the adaptive technologies research in ASSET. The selection of the lab equipment is motivated from the ASSET scenarios developed in a separate document (Leister et al., 2012a), and from previous projects, especially from the SAMPOS project (see, e.g., Leister and Schulz, 2010; Leister et al., 2011), the demonstrator in the DISSH project (Balasingham et al., 2007), and the lab defined in the EUX2010SEC project (Strand, 2010).

1.1 Purpose of this Note.

In the current document, we will *1*) review labs that have been developed in our earlier projects; *2*) define technologies and their properties for the ASSET lab; *3*) describe the planned experiments, and their requirements; *4*) list possible platforms and equipment; and *5*) give recommendations for equipment for the ASSET lab.

1.2 Purpose of the Experimentation Lab

The ASSET lab will enable us to have an infrastructure for experimentation, analysis and testing of devices in the IoT in connection with healthcare applications. The experimentation is envisaged to cover various exquipment addesseing all communication layers, and give the possibility to alter as many parameters, protocols, etc. as possible, in order to achieve adaptation. This gives us an advantage over a pure theoretical approach only using simulations.

We have defined the following goals for the testbed:

- Use the test bed to try out attacks in a controlled environment, and to test the adaptive security measures on all appropriate layers.
- Develop best practises for adaptive security in healthcare, and evaluate these in practice using the testbed.
- Replicate "IoT in healthcare" installations based on requirements from practitioners to improve adaptive security goals.
- Implement a configuration management of the lab that enables the reuse of a given testbed configuration, and also makes a tracability of the research possible. This includes a description of all performed experiments in a logbook.
- Use the testbed as a training area for researchers, project partners, and, after the ASSET project is finished, as a service for customers.

2 Testbeds Developed by ASSET partners

In this section, we present labs and testbeds that have been developed by the partners in the ASSET project in previous projects. The reason for including these laboratories is to bring experiences from these laboratories into our work.

2.1 Testbed and Demonstrator for SAMPOS

For the *SAMPOS* project, we developed a testbed to verify our results regarding the viability of the concept of the Medical Digital Items (MDI); see Leister and Schulz (2010). For the proof of concept we implemented the functionality as application programs on PCs using the available implementations from the reference software (instead of implementing this functionality on a real sensor node). The testbed showed evidence about the size of the MDI, and how to implement the necessary schemas.

The configuration of this testbed, shown in Figure 1, consists of PCs emulating sensor nodes, using the MPEG-21 reference software and the EXIficient and DIS implementation. Another PC is used to emulate the receiver part, or PCH. Further PCs can be used to implement the healthcare infrastructure, and terminals to access the content. Note that many mobile devices are so powerful today that software implemented in Java can be run on these devices.

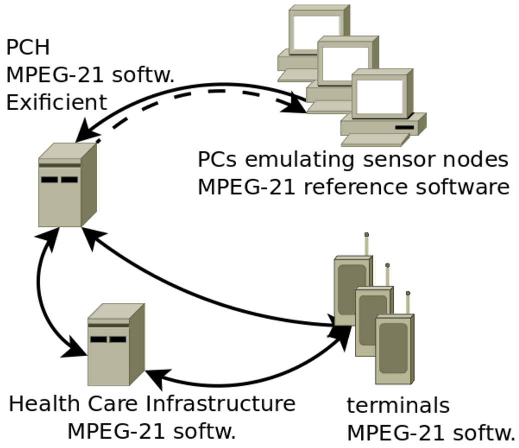

PCH
MPEG-21 softw.
Exificient
PCs emulating sensor nodes
MPEG-21 reference software
Health Care Infrastructure
MPEG-21 softw.
terminals
MPEG-21 softw.

Figure 1. The testbed for medical digital items used in the *SAMPOS* project.

2.2 The EUX2010sec Testbed

Strand (2010) describes a testbed for VoIP infrastructure experimentation, analysis and testing that has been used in the EUX2010sec project[1]. This testbed consists of hardware (several computers and virtual machine servers), phones (soft-phones and hard-phones of several brands), network components (e.g., routers), and software components (VoIP client software, system software, and monitoring). The Lab has also the possibility to connect to the public telephony services.

2.3 The DISSH Demonstrator

For the DISSH-project (Distributed Infrastructure Support for Specialized Hospitals), Balasingham et al. (2007) describe a demonstrator for facilitating data exchange between hospitals for second opinions. The solution consists of a computer running the system (code, web server) and a test database of medical data that was implemented with free and open source software. See also the report by Leister et al. (2005).

2.4 The Eye Tracking and UU Lab

NR has a the uu-lab, a lab for universal design and usability[2] that includes video equipment for user studies, the logging tool “Morae”, and eye-trackers for screens and mobile phones (by Tobii).

2.5 Motes Lab

The Intervention Center at the Oslo University Hospital uses a *micaZ* motes network. Some of these motes include sensor data obtained from wired sensors such ECG, blood pressure and pulse. The motes are connected with WLAN devices, that function as gateway hub nodes with access to a database.

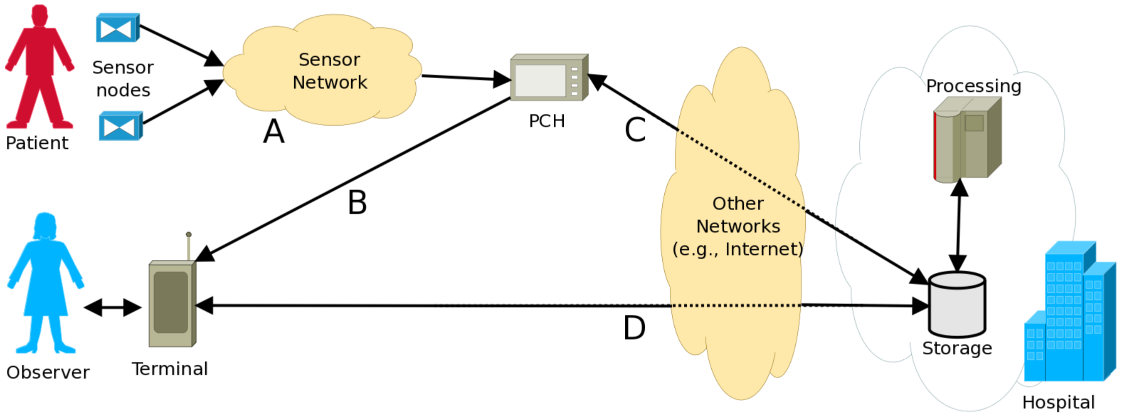


Figure 2. Generic system model with Channel A shown in detail.

3 Technology Requirements for the ASSET Lab

We describe the technologies and their properties for the ASSET lab, and we review important technologies and standards used in the area of eHealth. These include *a*) biomedical sensors and networks; *b*) mobile phones, smartphones, tablets, and similar; *c*) RFID/NFC technologies; and *d*) hospital infrastructure. The involved devices communicate using protocols such as 3G, GPRS, WiFi, Wireless Hart, 6LoWPAN, Zigbee, ANT+, Bluetooth, and so on.

A generic system model for the data flow in patient monitoring systems using elements of the IoT is presented by Leister et al. (2011). We show this model in Figure 2. For ASSET, we use this model to define the elements that need to be evaluated in a lab setting. Some of these elements are represented as real devices, some are represented as services, while others are emulated using suitable replacement devices. Parts of the following descriptions are taken from the technical reports by Liang et al. (2007) and Salden et al. (2008).

3.1 Biomedical Sensors and Networks

A wireless sensor network consists of spatially distributed autonomous devices using sensors to cooperatively monitor physical, environmental or biomedical conditions, such as temperature, sound, vibration, pressure, motion, pollutants or biomedical signals at different locations. In health care, biomedical sensors are used to monitor parameters such as blood gas[3], blood pressure, pulse rate, temperature, electrocardiogram (ECG), and electroencephalogram (EEG).

3.1.1 Biomedical Sensor Nodes

A biomedical sensor network consists of nodes, i.e., electronic devices that perform the tasks of sensing, processing, sending, or receiving biomedical data. From a data-flow perspective, a generic biomedical sensor node can be decomposed into the four *abstract* parts shown in Figure 3: sensor, receiver, processing unit, and transmitter. The capabilities of these nodes are limited due to size, cost, memory, and lifetime constraints. A single node has limited processing power, memory, and energy so that complex or computation

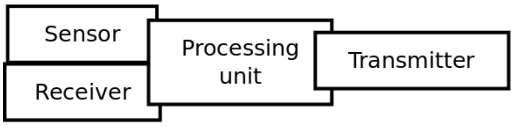


Figure 3. Generic block diagram of biomedical sensor node.

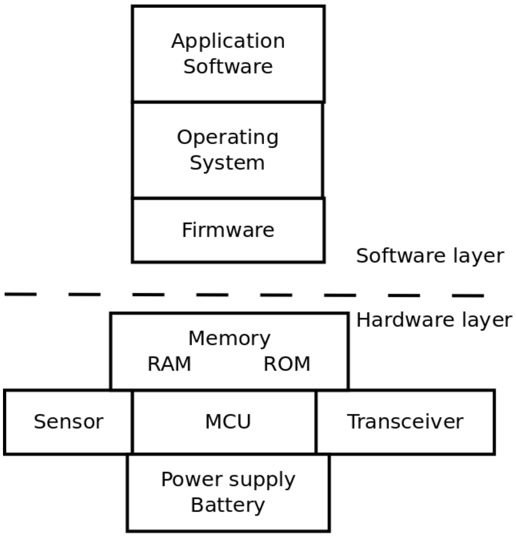


Figure 4. Technical building blocks of a biomedical sensor node.

intensive algorithms cannot be performed on an individual node.

Technically, a sensor node is built up of a microcontroller unit (MCU), memory (RAM, ROM), a (wireless) communication device, the biomedical sensors, and the power supply or battery. The technical building blocks of a biomedical sensor node are illustrated in Figure 4. The functionality of the biomedical sensor is controlled by software, usually consisting of firmware, an operating system, and specific application software for treating the biomedical signals, and their transfer.

Sensor nodes employ short-range wireless communication devices using broadcast over the medium as a communication primitive. As a consequence, messages may be subject to fading, other propagation losses, or collisions even if nodes are not in direct communication with each other (Arora et al., 2004). In many occasions, a routing protocol is needed to direct messages from any node in the network to the sink node, which often is implemented as the patient cluster head (PCH). The dynamic nature of the wireless communication medium can result in unstable connections and frequent route changes.

3.1.2 Biomedical Sensor Networks

A biomedical sensor network (BSN) may consist a large number of sensor nodes and sink nodes, which are connected by a wireless medium. The wireless communication of sensor nodes can be single-hop communication or multi-hop communication. The main information flow in a BSN is from the sensor to a sink node. The sink node, often implemented in the PCH, communicates with other services, devices or infrastructure. The biomedical sensor network for one patient is also referred to as a wireless body area net-

Table 1. Specifications of the sensor data.

Biomedical sensor	*Sampling frequency* (Hz)	*Sampling resolution* (bits)	*Data rate* (bps)
ECG (3 channels)	250	16	12000
EEG	1000	12	12000
EMG	800	12	9600
SPO_2	125	12	1500
Blood pressure	125	12	1500
Body temperature	1	12	12

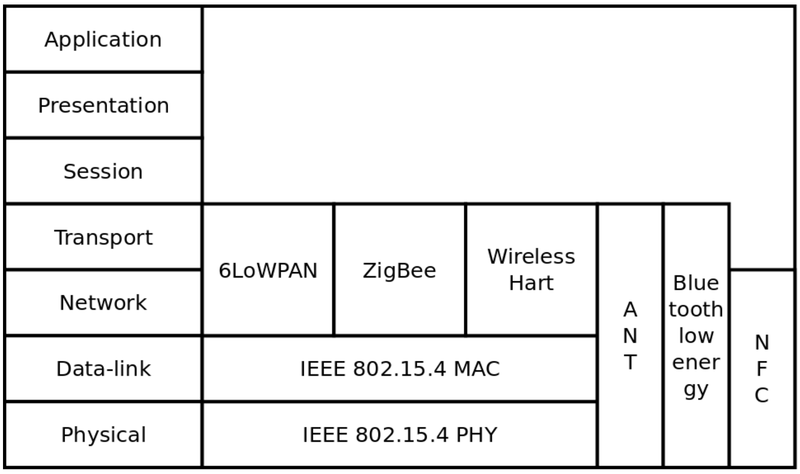


Figure 5. Communication technologies in the IoT and layers

work (WBAN) or wireless personal area network (WPAN) in the literature. The BSN is part of a network consisting of three tiers that facilitate the transport of biomedical data from the patient to the health care personnel (Otto et al., 2006).

3.1.3 Properties of biomedical sensor data

Different biomedical sensors can produce measurements for different kinds of biomedical data, e.g., ECG, EEG, EMG, SPO_2, blood pressure, temperature or sound. The biomedical sensor data consist of one or more tracks of sampled measured values. A sensor could measure a physical entity that is converted from analogue to a digital representation, quantised, and sampled into a sequence of sampled values. The properties of medical data include sampling frequency and sampling resolution. Table 1 shows the properties of one-dimensional biomedical signals processed by the sensors[4]. Additionally, the raw medical data is supplemented with administrative data, e.g., a time-stamp and the identity of the sensor. Some biomedical sensors process and communicate two-dimensional data, such as images.

3.1.4 Communication Technologies for Biomedical Sensor Networks

Biomedical sensor networks transmit the biomedical data wirelessly, using the IEEE 802.15 standard group[5], which specialises in WPAN standards. Some medical equipment uses the IEEE 802.15.4 standard (for the physical and link layers), and the *ZigBee*[6] vendor standard for the upper communication layers.

The ISO Open Systems Interconnection Basic Reference Model (ISO/OSI Reference Model or OSI model for short) (ISO/IEC, 1994) is a layered, abstract description for communications and computer network protocol design, developed as part of the Open Systems Interconnection initiative. The following paragraphs refer to the structure different layers of the OSI model.

Physical layer

The physical layer defines all the electrical and physical specifications for devices. The features of the physical layer are activation and deactivation of the radio transceiver, energy detection (ED), link quality indication (LQI), channel selection, clear channel assessment (CCA) and transmitting, as well as receiving packets across the physical medium.

In the CC 2420 a bandwidth of 250 kbps in the 2.4 GHz frequency band is given. Receiver sensitivity is -85 dBm for the 2.4 GHz band. The achievable range is a function of receiver sensitivity and transmitter power.

Typical radio propagation models are described as follows. The power of received signal, P_{rx}, is calculated as $P_{rx} = P_{tx} - pl$, where P_{tx} and pl represent the power of transmitted signal, and path loss, respectively.

Free space propagation. The free space propagation model assumes a transmit antenna and a receive antenna to be located in an otherwise empty environment. Neither absorbing obstacles nor reflecting surfaces are considered. The path loss is calculated as $pl = 32.5 + 20\log(d) + 20\log(f)$, where d is the distance in km and f is the frequency in MHz.

Additive white Gaussian noise (AWGN). In an AWGN channel model, the only impairment is the linear summation of wide-band or white noise with a constant spectral density[7] and a Gaussian distribution of the amplitude. The model does not account for the phenomena of fading, frequency selectivity, interference, nonlinearity, or dispersion. However, it produces simple, tractable mathematical models that are useful for gaining insight into the underlying behaviour of a system before these other phenomena are considered.

The assumption of an AWGN channel is valid as long as the channel is coherent during the transmission of a packet (slow fading). With the maximum packet size of 133 bytes transmitted at the raw rate of 250 kbps, the packet transmission takes 4 ms, which is smaller than the coherence time encountered in the 2.450 GHz band without mobility issues (Bougard et al., 2005).

Rayleigh channel. Rayleigh fading is caused by multipath reception. The mobile antenna receives a large number of reflected and scattered waves. Because of wave cancellation effects, the instantaneous received power seen by a moving antenna becomes a random variable, dependent on the location of the antenna. Deep fades occur occasionally. Although fading is a random process, deep fades have a tendency to occur approximately every half a wavelength of motion.

Rician channel. The model behind Rician fading is similar to that for Rayleigh fading, except that in Rician fading a strong dominant component is present. This dominant component can, for instance, be the line-of-sight wave.

The indoor wireless RF channel typically behaves as a Rician channel. If the line-of-sight is blocked, Rayleigh fading becomes an appropriate model.

Data link layer

The data link layer provides the functional and procedural means to transfer data between network entities, as well as the facility to detect and possibly correct errors that may occur in the physical layer. This layer may be split into sub-layers, such as the media access control (MAC) layer, and the logical link sub-layer (LLC), depending on the standard being used. The features of *MAC sub-layer* are beacon management (optional), channel access, GTS management, frame validation, acknowledged frame delivery, association and disassociation. Carrier sense multiple access with collision avoidance (CSMA/CA) is used as channel access mechanism. Both the physical layer and the MAC layer are defined in the IEEE 802.15.4 standard (IEEE, 2003).

Wireless channel packet error rate (PER)/bit error rate (BER). In an IEEE 802.15.4 system, all communication is based on packets. It is more accurate to measure the PER than the BER since it mirrors the way the actual system operates. In the IEEE 802.15.4 standard, the PER is $\leq 1\%$, when the received signal $\geq$ -85 dBm. The Physical layer Service Data Unit (PSDU) length should be 20 bytes. The link link layer discards packets that are recognised to be corrupted, and cannot be recovered by mechanisms of the IEEE 802.15.4 standard, like CRC. However, occasionally defective packets are not recognised and are passed to the upper layers.

Network layer

The network layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks while maintaining the quality of service requested by the transport layer. The network layer performs network routing functions; it might also perform segmentation, de-segmentation, and report delivery errors. In sensor networks, the network layer mainly performs network routing functions.

For routing in BSN several methods can be used, such as fixed routing tables, the Ad-hoc on-demand distance vector (AODV), or the Cluster-tree algorithm. Fixed routing schemes often use routing tables that dictate the next node to be routed to, given the current message location and the destination node. Routing tables can be large for large networks, and cannot react to events in real-time, such as failed links, nodes with backed up queues, or congested links (Lewis, 2004). Leister et al. (2012b) present a simulation of the AODV-algorithm using the modelling languages *Creol* and *ABS*.

3.2 IEEE 1451 and TEDS

The IEEE 1451 (IEEE1451.0, 2007; IEEE1451.5, 2007) represents a family of smart transducer interface standards. These standards describe a set of open, network-independent communication interfaces for connecting transducers to microprocessors, instrumentation systems, and networks. The key feature of these standards is the definition of Transducer Electronic Data Sheets (TEDS) that store transducer identification, calibration, correction data, measurement range, and other relevant sensor node data. The IEEE 1451 can be relevant for the WSN part of a patient monitoring system, since the capabilities of sensor nodes and parts of the communication stack are represented in the standards.

3.3 802.15.4

The IEEE 802.15.4[8] is a standard proposed for low rate wireless personal area networks and focuses on low cost of deployment, low complexity, and low power consumption. As a result, most devices that use IEEE 802.15.4 are suitable for Low-Rate Wireless Personal Area Networks (LR-WPANs). The IEEE 802.15.4 standard allows the formation of the star and peer-to-peer topology for communication between network devices where, in the latter topology, ad hoc and self-configuring networks can be formed. The standard is designed to support *a*) wireless sensor applications that require short range communication to maximise battery life; *b*) Physical and data-link layer protocols. The PHYhysical (PHY) layer supports 868/915 MHz low bands and 2.4 GHz high bands while the Media Access Control (MAC) layer controls access to the radio channel using the carrier sense multiple access with collision avoidance (CSMA-CA) mechanism, hence enabling global or regional deployment (Hourtane, 2004).

The IEEE 802.15.4 channel access method is CSMA-CA and Aloha and the theoretical raw data rate extends up to 250 Kb/s. However, it is much lower in practice due to interference, Multi-hop communication and MAC layer constraints. IEEE 802.15.4 Networks can operate either in peer-to-peer or star network topologies. They also support for both 16-bit short or IEEE 64-bit extended MAC addresses (Kushalnagar et al., 2007). In addition, they have capabilities of energy detection, link quality indication and low power consumption. However, these networks are vulnerable to different kind of attacks since they are low-cost and have limited capabilities in terms of computing power, available storage, and power drain, which is a hindrance when implementing tight security measures (IEEE, 2011).

3.4 ZigBee

ZigBee[9] is an industry standard that implements the layers above the link layer, on top of the IEEE 802.15.4 standard. ZigBee is widely used for sensor networks. See also Section 3.1.4.

3.5 6LoWPAN

The 6LoWPAN (IPv6-based Low power Wireless Personal Area Networks)[10] is a standard that supports IPv6 packets communication over an IEEE 802.15.4-based network where low power device can communicate directly with IP devices using IP-based protocols.

It provides an adaptation layer, new packet format, and address management to fit the larger IPv6 packet sizes into smaller IEEE 802.15.4 frame sizes.

IPv6 over IEEE 802.15.4 communication was charted to the Internet Engineering Task Force (IETF) to define an open standard that conforms and provides interoperability with other IP links and devices, as well as among 802.15.4 devices [4]. It is intended to enable IPv6 communication on LoWPAN devices (sensors and controllers) with the assumption of providing all or most service benefits to the standard IP networks. 6LoWPAN networks share the same limitation and strength as IEEE 802.15.4 networks in computation, communication and security-wise (Hui and Thubert, 2011).

Possible threats in 6LoWPAN include intrusion, sink-hole and replay attacks. A possible solution, however, to address security issues in 6LoWPAN networks, includes implementing SSL or IPSec on top of link layer security, which protects against impersonation and data stealing. On the other hand, intrusions can be protected from Link layers (Arch Rock Corporation, 2007).

3.6 Wireless Hart

The WirelessHART[11] is a standard for a wireless network communication protocol for process measurement and control applications, and is based on IEEE 802.15.4 for low power 2.4 GHz operation. Its key capabilities are reliability, security, and effective power management. It supports mesh networking, star, and combined network topologies.

On top of physical layer, WirelessHART implements its own time-synchronised MAC layer. It maintains central network manager and network wide time synchronisation. It uses channel hopping and blacklisting and AES-128 ciphers and keys. Moreover, self-organising and self-healing of such mesh networking allow messages to be routed around interference and obstacles (Song et al., 2008). However it has interoperability limitation with other communication protocols using 802.15.4 standard.

3.7 ANT and ANT+

ANT[12] is a compact, wireless sensor network proprietary protocol designed in consideration of ultra-low power usage of microcontroller and the ability to handle from simple to complex topologies. It runs on 2.4 GHz ISM band with connectivity distance up to 30m. The ANT platforms are mainly used for sport- and home-based health monitoring and wellness applications. They have two major components, ANT protocol engine that mainly focuses on communication establishment and maintenance, and microcontroller (MCU) for application specific communication instantiation.

To keep the interoperability of ANT-enabled devices running smoothly, ANT+ has been introduced as an integration profile. This helps users to select devices without interoperability concern. ANT platforms have been implemented in different production and research projects to monitor health and sporting activities. There are also devices that use ANT-to-IP called ANT adapters. In general, ANT platforms are suitable for home health monitoring as the application space and mobility is limited. ANT platforms consume less power and can stay active longer than other devices, which reduces or alleviates battery replacement hassles for the patient.

ANT+ (or ANT Plus) is an interoperability function that can be added on top of the ANT protocol. It is targeted at manufacturers of "bike computers, diagnostics, power meters, heart rate monitors, etc." and is promoted by the ANT+ Alliance.[13] ANT+ is primarily designed for collection and transfer of sensor data, to manageable units of various types. The three main areas of operation are sport, wellness and home health. It can be used for data-transfer for a number of devices, such as heart rate monitors, speed sensors, cadence sensors, foot pods, power meters, activity monitors, calorimeters, body mass index measuring devices, blood pressure monitors, blood glucose meters, pulse oximeters, positions tracking, short range homing beacons, weight measuring devices, control of music players, and temperature sensors. This allows for ANT+ to be used for general fitness tasks as well as medical functions.

Currently the ANT+ is implemented on more than 35 applications, produced by 27 different manufacturers. The ANT+ Alliance is organised by Dynastream Innovations Inc, a subsidiary of Garmin Ltd. As of September 30, 2010, it had more than 300 members including Adidas AG, Concept2, Garmin, Suunto, McLaren, Microsoft, Sony Ericsson, Texas Instruments, Timex and Trek.

3.8 Bluetooth

Bluetooth[14] is a proprietary open wireless technology standard for exchanging data over short distances from fixed and mobile devices. Bluetooth uses short-wavelength radio transmissions in the ISM band, 2400–2480 MHz, and it creates personal area networks (PANs) with high levels of security.

Bluetooth low energy (BLE)[15] is a feature of Bluetooth 4.0 wireless radio technology, aimed at new, principally low-power and low-latency, applications for wireless devices within a short range (up to 50 metres). This facilitates a wide range of applications and smaller form factor devices in the healthcare, fitness, security and home entertainment industries.

3.9 DASH7

DASH7 is an open source wireless sensor networking standard for wireless sensor networking[16], which operates in the 433 MHz unlicensed ISM band. DASH7 follows the ISO/IEC 18000-7 standard, provides long battery life, range of up to 2 km, indoor location with 1 meter accuracy, low latency for connecting with moving things, a very small open source protocol stack, AES 128-bit shared key encryption support, and data transfer of up to 200 kbit/s.

3.10 NFC

At NR, the NEMO project has looked into *near field communication* (NFC)[17] technologies[18]. NFC is a set of standards for smartphones and similar devices to establish radio communication with each other by touching them together or bringing them into close proximity, usually no more than a few centimetres. NFC standards cover communications protocols and data exchange formats, and are based on existing radio-frequency identification (RFID) standards including ISO/IEC 14443 and FeliCa. The standards include ISO/IEC 18092 and those defined by the NFC Forum, which was founded in 2004 by Nokia, Philips and Sony.

3.11 Mobile Data

GSM/GPRS/UMTS are cell phone communication standards that have high power consumptions for better data communication rates. However, they can be relevant when connectivity is important to send collected data from sensors, mobile data centers, or cloud computing platforms for short time intervals, or when enough battery capacity is available, e.g., from a smartphone to the hospital infrastructure.

The Universal Mobile Telecommunication System (UMTS) is a third generation (3G) mobile communications system that provides broadband services to wireless and mobile communications. It delivers low-cost, mobile communications at data rates of up to 2 Mbps, and uses Wide-band Code Division Multiple Access (CDMA) technology. On the other hand, GSM/GPRS are second generation (2G) networks which use time-division multiple access (TDMA) technology to switch data[19].

3.12 Smartphones

There are a variety of smart phone architectures available, such as Android, iOS, and windows phone. Due to the availability of more sensors on smartphones, the Android platform is preferred for lab experiments; iOS is on second place. Smartphones can be seen as a powerful, portable computers with extended communication possiblities. The communication facilities include telephony (speech) and wireless data (via diverse mobile networks), wired connections using USB, as well as short-distance communication using WLAN, Bluetooth, NFC, and, for some models, other wireless protocols (e.g., ANT, DASH7).

4 Lab Content

We apply the model shown in Figure 2 to a generic setting for the ASSET lab. This is illustrated in Figure 6, where we can identify lab elements for the following parts:

- Channel A, i.e., a (body) sensor network that takes measurements and conveys the data to the PCH. The PCH is implemented by using a smartphone, and is also part of a network of smartphones using short-range communication, near-field communication, or mobile networks (Channels B, C, D, and E).

- The model includes an unwanted Channel W, which denotes an attacker node in the wireless sensor network.

- Channel B denotes a network of smartphones using short-range wireless communi-

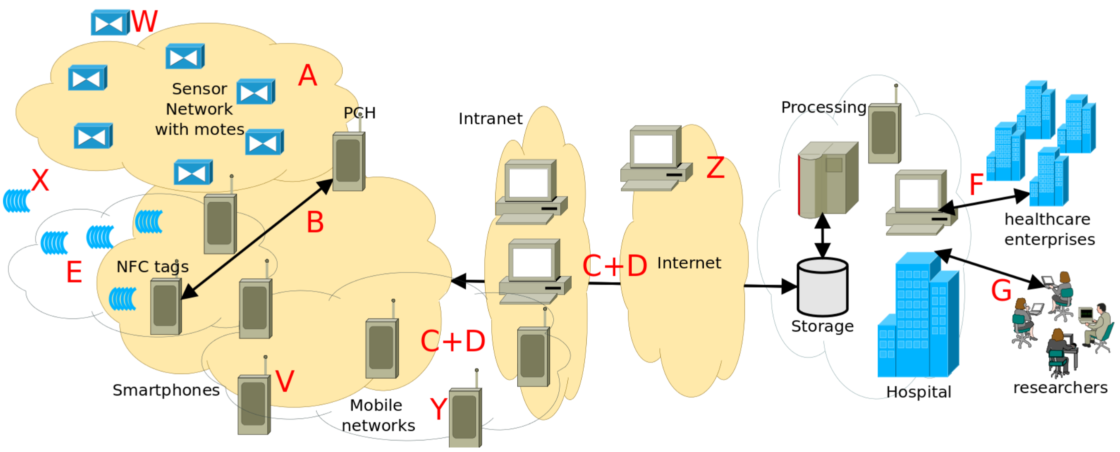


Figure 6. Generic model for the content in the ASSET lab.

cation technologies, such as WLAN, Bluetooth.

- The model includes an unwanted Channel V, which denotes an attacker node (smartphone) in the short-range wireless communication network.

- Channels C and D denote the communication over the Internet, using wired and wireless communication technologies.

- Note that the mobile networks are part of the Channels C and D, since these channels are not defined by the used technology. The use of the mobile networks is the use of the Internet over mobile networks, and, thus, comparable with using the Internet over a wireless network.

- The model includes the unwanted Channels Y and Z. Channel Y denotes an attacker in the mobile network while Channel Z denotes an attacker from the Internet.

- In the ASSET lab, the hospital infrastructure, implementing functionality such as the electronic health record system, will be emulated by a PC with the necessary interfaces. Depending on the scenario, this PC can be placed inside or outside the ASSET lab network zone.

- Channel E denotes communication over near-field communication (NFC) technologies. NFC nodes communicate with smartphones.

- The model includes the unwanted Channel X, which denotes an attacker NFC device.

Based on this model, we suggest the following content for the ASSET lab:

1. A body sensor network consisting of motes connected through wireless technologies.

2. NFC devices that can connect to smartphones.

3. Smartphones that can connect to diverse networks such as short-range (WLAN, Bluetooth, Zigbee, ANT, etc.) and long-range (GSM, 3G, 4G, etc.) technologies. Some of the smartphones need to connect to the body sensor network to implement the

PCH functionality using the appropriate communication technology. Some of the smartphones used in the ASSET lab need to implement NFC technologies.

4. PCs that can be used to implement office PCs, emulation of the hospital infrastructure, implementation of diverse devices and services used in health-care, and attackers in the intranet or Internet. Possibly, a PC needs to be able to implement the PCH using suitable hardware to connect to the technology chosen for the body sensor network.
5. Diverse devices to implement the necessary infrastructure, such as routers, switches, gateways to the communication technologies to be used in the experiments and programming the sensor network devices.
6. Software that is suited to perform the planned experiments, such as software development environments for sensor networks, NFC technologies, etc.

4.1 Contents of the Lab

We refer to Section 7 for a market survey of potential devices for the ASSET lab. We envisage having biomedical sensor nodes, NFC technology, and smartphones as the main ingredients in the lab. We also envisage useing an emulated hospital information system.

Biomedical sensor nodes. The lab should contain a selection of sensor nodes so that a biomedical sensor network can be built, and attacker nodes can be implemented. Different kinds of sensor node technologies are available, which will be discussed in Section 6. The biomedical sensor nodes can operate with communication technologies, such as IEEE 802.15.4, 6LoWPAN, Wireless hart, ZigBee, WiFi.

NFC technology. A selection of NFC tags, NFC-enabled sensors, and NFC-enabled smartphones need to be content of the lab.

Smartphones. A selection of smartphones using the suitable communication technologies, tablets, etc. need to be content of the lab. These can be used both for the PCH (i.e., for the patient), and for the medical personnel. The smartphones can operate with communication technolgies for mobile data (see Section 3.11), Bluetooth, WiFi, etc.

4.2 Hospital Infrastructure

The hospital infrastructure implements the Electronic Patient Journal (EPJ), and other medical data services that are used to store and process medical data. For the purposes of a lab, we implement the necessary standards, using the most relevant protocols and functionality. See, e.g., the demonstrator of the DISSH project (Balasingham et al., 2007). There is a variety of free and open source (FOSS)-based products that are available for the purpose of simulation and validation; see, e.g., the note by Leister and Røe (2005). A similar approach was taken to implement the SAMPOS demonstrator (Leister and Schulz, 2010).

5 Security Issues in the OSI Model

In this section, we briefly describe security issues, typical attack strategies, as well as countermeasures connected to each layer of the OSI model. These issues are further related to the ASSET scenarios (Leister et al., 2012a), and some research problems are defined at the end.

5.1 Security issues connected to each layer in OSI model

A summary of possible attack and damage strategies on the different layers of the OSI model, as well as measures to counteract them are described in the following sections. This summary is partly based on the work done by Reed (2003) and Surman (2002).

Layer 1. Physical Layer

Security issues on this layer concerns both accidental and deliberate events. Accidental issues here are loss of power, damage to equipment due to electronic malfunction and electromagnetic pulses like lightning, and interference from other equipment.

In a hospital environment security measures towards loss of power and unwanted electromagnetic pulses are usually already in place of due to the devastating effect loss of power on medical equipment may have on human lives. In a home environment, these issues need to be considered, however. Electronic malfunction and reliability is mainly solved by investing in high quality equipment. Interference from other equipment may be eliminated by cognitive radio algorithms or CDMA based modulation. Channel coding (which is performed on Layer 2) may also be used to remove errors due to noise or interferences.

The main issue is intentional physical damage to important equipment (by mechanical destruction or electromagnetic impulses) or jamming, and eavesdropping of the physical media, by picking up radiation from wireless links or cables.

Many of these issues may be eliminated by proper shielding of and protection of cables, relevant rooms and buildings, as well as restricting access to rooms with important equipment. Again, such measures are easier to deal with in the hospital environment. The risk of eavesdropping can be eliminated by proper encryption of the data (more about this on the Layer 5). For wireless networks, one should also make sure that the power range is so small that it is difficult to connect to the network from outside the room or building where the wireless network resides.

Layer 2. Data link Layer

Attacks on the data link layer usually happen inside local networks; that is, before the data reaches a router. One method of intrusion is MAC address spoofing: In local wired and wireless dynamic networks, each entering node must have a unique network address, or MAC address, and is given a corresponding IP through ARP (Address Resolution Protocol), which is basically a mapping from IP addresses, to MAC addresses. When a node wants to send a message to a certain IP address, an ARP packet that requests the MAC address for that IP is broadcasted on the network. The node that owns this IP then returns an ARP packet with its MAC address and the requesting node sends its data and stores this IP-to-MAC mapping. In this procedure, an attacker may falsely reply that it is the host of the requested IP address, and thereby receive data not intended for it. If this IP-to-MAC mapping is stored in a node, the node will transmit to the attacker every time it sends something to that IP address.

Proper encryption will stop the attacker from interpreting the data, but the intended receiver will never receive the data intended for it. Since ARP's does not cross router boundaries, one may avoid this problem, at least in small networks, by manually giving IP addresses to any new node introduced into the network.

For wireless networks, Layers 1 and 2 are specifically sensitive to attacks. For this reason, encryption technology for authentication and privacy should be considered on Layer 2.

Layer 3. Network Layer

Security issues on this layer are (among other things) concerned with an attack on network routers. The attacker may then be outside the local network. An attacker may steal an identity, i.e. take a given IP address and claim to be the intended host, thereby receive data not intended for it, or it may send malicious packets. The attacker can also hack the router to take control of all data passing through it. Many public routers (like Internet routers) only have elementary levels of security in their routing protocols. They may, for instance, lack the ability to determine if another router is trustworthy or not, and so spurious network routes may be introduced.

The best tool for preventing router attacks is a firewall that only let the necessary traffic pass through it. Encryption and authentication methods can be used to reveal an attacker with stolen identity (see also Layers 5 and 6). One may also use certain "route filters" to avoid spurious routes. Most importantly, only well protected data should be allowed to be sent via public routers.

Layer 4. Transport Layer

To target a specific application on a system an attacker must, in addition to an IP address, know the port number assigned to the application. An attack usually starts by scanning all known ports to gather information about open ports in the system. During a handshake procedure a port will be designated, allowing for a possible full connection. The port scanner can connect to this port, and then shut down the connection before a full connection is created. The port scanner can then tell which port is open or not from the response given by the targeted node. Many transport protocols do not have solid ways of validating the source of a packet, or if a packet is a legitimate part of a stream of a data transmission. The attacker can therefore inject false packets, interrupting and falsifying the flow of higher level data.

To prevent attacks on this layer, one can again resort to a firewall. The firewall must be able to detect a port scan as well as determining if any packet is likely to be in response to an existing flow of data. One should also use an implementation of TCP where the sequence number assignment is based on a random number generator, making it harder to take over a TCP session (see also Layer 5).

Layer 5. Session Layer

Whereas an attacker on Layer 4 tries to find open ports to intrude, or inject of false packets, on the session layer its about hijacking the communication (TCP) session itself or listening in to the communication to gain access to private data (eavesdropping). The problem lies in authentication and session identification. An attacker may try to hijack a password by listening in during the password exchange procedure, try out different passwords through educated guesses, or try out every likely password in an exhausting manner. With valid authentication, the attacker basically has full access to the node under attack.

One may prevent attacks on this layer through cryptography. Password exchange and storage should be encrypted (by e.g., the RSA algorithm) and every user account should have an expiration date. Session identification information should also be encrypted. By setting a limit on the number of login attempts, one can avoid the problem of repeated guessing of passwords.

Layer 6. Presentation Layer

This layer deals with presentation of data and dissimilar hosts with different formats of data (like different binary representations and character sets). Attackers may feed unexpected or illegal input intro presentation layer facilities, gaining results that are undesired or contrary to what the designers of the system intended (sabotage). Cryptographic presentation services can be vulnerable to weaknesses in their implementation or fundamental design, and thereby give access to attackers.

Security measures are thorough specification and checking of received input incoming to applications and a continuous review of cryptography solutions to ensure security against emerging threats.

Layer 7. Application Layer

Attacks on this layer are usually in the form of trojans, viruses and worms etc. All these attacks are mainly meant for sabotage. Security measures on this layer are mainly good virus programs that are updated on a regular basis so that it can cope with any new threat that emerges.

5.2 Security measures across several layers

From the security issues outlined in Section 5.1, it is clear that threats on many of the layers are closely related. Security measures designed across several layers is therefore common. Some of the security issues described in Section 5.1 are, in fact, concerned with the borders between the different layers. For instance, APR spoofing on Layer 2 is actually happening on the border between Layers 2 and 3, since ARP is a protocol communicating between Layers 2 and 3.

A firewall is the main protection on Layers 3 and 4, and one firewall that takes care of all issues on these layers should therefore be considered. Since cryptography shows up on several layers, one cryptography solution adapted to all these threats could therefore be considered. Note also that if data is well encrypted, an attacker will not be able to interpret sensitive data. With a good cryptography protocol, the main concern will then be sabotage or loss of data.

5.3 Relation to ASSET scenario and possible research problems

Attacks from W, X, V in Figure 6 will be the only ones of concern for Layers 1-2 since they are the only ones within the router boundary. X and V may also attack Layers 3-7. Attackers Y and Z may attack on Layers 3-7.

When a new system or network is designed, like in the ASSET project, one is free to make designs across layers or even new designs, with the exception of the parts that concerns already existing mobile networks, the Internet and existing standards. For the wireless sensor network shown in Figure 6, we are basically free to optimise, or design entirely new security schemes.

Since the motes of the sensor network should be simple, security issues would concentrate on Layers 1-2 (and maybe 3 if the motes are supposed to collaborate, that is, if they should communicate with each other). To make communication secure and reliable one must introduce some overhead or redundancy to the data one wishes to transmit (in order to encrypt or perform channel coding). Any specific application has a certain demand on rate, delay, and reliability of the transmission. Once these demands are given, one may ask the following questions:

1. What is the necessary overhead or redundancy needed to make the transmission adequately secure? I.e., what is the total rate necessary to achieve adequate security?
2. Given a complexity constraint on the motes, as well as a bound on the total transmission rate, what are the best security measures we can take given these constraints?

For simple motes one would like to implement efficient algorithms, that is, algorithms providing secure communication at low complexity. There will be a trade-off between security, rate and complexity. One will also have to find out what is adequately secure and make the solution as simple as possible. One may try to optimise existing schemes, to evaluate if they are adequate, or one will need to design entirely new security schemes that better suits our needs. Several existing cryptography and coding solutions may be tested. One may also investigate the use of CDMA with pseudo-random spreading codes.

It is also important to investigate the effect of network topology on security. Will the topology that has the highest reliability and capacity be the most secure topology? Is it again necessary to find the best trade-off?

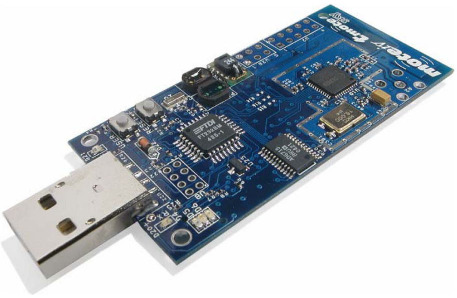


Figure 7. The Moteiv Tmote Sky.

6 Platforms

Many of the platforms are described in the *Sensor Network Museum*[20].

6.1 Mote platforms

Johnson et al. (2009) and Karani et al. (2011) give an overview mote platforms that include the (*a*) Telos B or Tmote Sky, (*b*) the Mica2 and MicaZ, (*c*) the SHIMMER (Sensing Health with Intelligence, Modularity, Mobility, and Experimental Reusability), (*d*) the IRIS, (*e*) the Sun SPOT (Small Programmable Object Technology by Sun Microsystems), and the (*f*) EZ430-RF2480/2500 by Texas Instruments. Additionally, we mention the *Arduino* platform which we describe in Section 6.2.

6.1.1 Tmote Sky Platform

The Moteiv Tmote Sky platform[21] (also denoted as Telos B) includes a hardware platform and a software platform; see Figure 7. If the Tmote Sky is used as a sensor hardware platform, the *Tmote Connect* could be used as gateway between sensor networks and TCP/IP-based networks, and play the role of a sink node in the sensor network.

The most important properties of the Tmote Sky are summarised in Table 2. The *Tmote Sky* is a low-power wireless module for use in sensor networks, equipped with both IEEE 802.15.4 and USB communication capabilities, an 8 MHz processor, and humidity, temperature, and light sensors[22]. Both the sensor nodes and the sink nodes use TinyOS as the operating system.

Tmote Connect[23] will be used as a gateway in our experiments. It can be used to bridge wireless sensor networks and wired local area networks, and provides bi-directional connectivity for data transfers to and from wireless sensor networks over TCP/IP sockets.

TinyOS, used by the Tmote Sky, is an open source component-based operating system and a platform for targeting wireless sensor networks. TinyOS is an embedded operating system.[24] TinyOS is developed by a consortium led by the University of California, Berkeley, in co-operation with Intel Research.[25] TinyOS employs a special C-dialect, called *nesC*.[26]

The Tmote Sky can be connected to a host computer[27] to communicate via a USB con-

Table 2. Characteristics of the Tmote Sky sensor node platform

Platform	*Tmote Sky*
MCU	8MHz TI MSP430F1611
Raw data transmission rate	250kbps
Wireless transceiver	CC 2420 2.4 GHz, IEEE 802.15.4 radio
RAM	10K
ROM	48K flash ROM
ADC, DAC	12bit integrated
Communication range (m)	50 (in doors)/125 (outdoors)
Operating system	TinyOS
Wakeup from sleep	6 μs
external flash	1024 kbytes

Table 3. Typical current consumption of the Tmote Sky device

Current consumption	*Normal value*
MCU on, Radio RX	21.8 mA
MCU on, Radio TX	19.5 mA
MCU on, Radio off	1.8 mA
MCU idle, Radio off	54.5 μA
MCU standby	5.1 μA

nector. The device is programmed through the on-board USB connector. The Tmote Sky supports re-programming over the radio link. The steps in this procedure are as follows: (*1*) Each node in the network receives application software via radio link. (*2*) Check and verify the program image. (*3*) The bootloader loads the new program image. (*4*) Reprogramming the micro-controller. (*5*) Reboot the node using the new program.

The same technique has been used in satellite software reprogramming. Obviously, this technique is not very reliable, especially in multi-hop sensor networks. However, it is the only way to re-program the sensor node when the node is not reachable physically.

Power consumption is an important issue for biomedical sensors. The Tmote Sky is powered by two AA batteries; the voltage supply should be between 2.1 to 3.6 V DC. Table 3 describes the typical current consumption of sensor node platforms.

Transceiver. The transceiver, containing the functionality of transmitter (sender) and receiver, is IEEE 802.15.4 compliant, working in the 2.4 GHz band. The *Chipcon 2420* (CC 2420) transceiver[28] is used in the sensor network. Note that the transceiver cannot transmit and receive simultaneously. The CC 2420 supports four states (transmitting, receiving, idle, shutdown) and switches between these four states when operating, in order to save energy (Bougard et al., 2005).

The CC 2420 has programmable output power, which can be varied from -25 dBm to 0

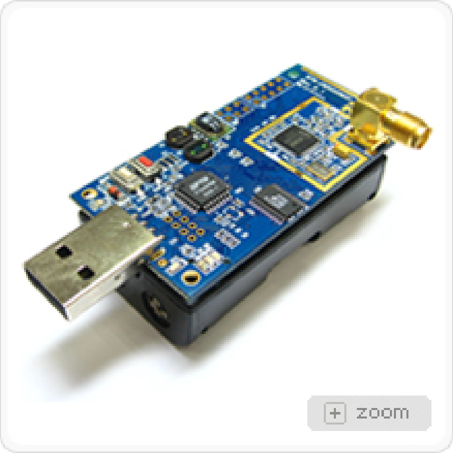


Figure 8. The Maxfor MTM CM5000 MSP node.

dBm. The received signal strength can be obtained by reading a digital received signal strength indicator.

6.1.2 Alternative to Telos B

Other kinds of nodes that are similar to Telos B nodes can run the TinyOS[29], such as the *Shimmer Mote* (Liao et al., 2012).

The mote by MAXFOR[30], see Figure 8, builds on an IEEE 802.15.4 Wireless sensor network platform, uses a TI MSP430 Processor, the CC2420 RF communication chip and has support for the TinyOS. It contains temperature, humidity, and light sensors, as well as a USB downloader.

For a more sophisticated software stack like ZigBee, nodes from Linear (who bought Dust Networks recently), can be used[31]. Dust Networks was founded by Prof. Kris Pister of UC Berkeley, and they have complete software and hardware solution for smart mesh networking. Literature on using Dust Network's solutions is by Doherty et al. (2007a,b); Doherty and Teasdale (2006). The main application area of Dust Networks is, according to their web site, for industrial applications. They offer both the product lines *SmartMesh IP* based on 6LoWPAN and 802.15.4e standards, and *SmartMesh WirelessHART* for industrial environments based on the WirelessHART (IEC 62591) standard.

6.2 Arduino

The Arduino platform can be used as building blocks for motes. The Arduino platform[32] can be suitable for the ASSET lab (Vasaasen, 2012), since both sensors and actuators can be implemented with this platform. The Arduino hardware reference designs are distributed under a CC BY-SA 2.5 license available on the Arduino Web site[33], while its software is released under the GPL.[34] *Adafruit* is one of the largest producer of "things", e.g., the upcoming edition of a standard Arduino[35]. An important aspect of the Arduino is the standard way that connectors are exposed, allowing the CPU board to be connected to a variety of interchangeable add-on modules known as *shields*. Some shields communicate with the Arduino board directly over various pins, but many shields are individually addressable via an I^2C serial bus, allowing many shields to be stacked and used in parallel.

Examples of a configuration include an Arduino Nano[36] and fifty individually addressable LEDs[37]. The Arduino blog (http://arduino.cc/blog/) offers more examples.

6.3 NFC

For NFC as a platform we consider both active and passive devices. Passive devices come usually in the form of NFC-tags, NFC-enabled textiles, NFC-cards, etc. Examples for writable tags are Samsung TecTiles, and NFC-tags by Xperia (Sony). These can be writable with a suitable writing device like an NFC-enabled smartphone. Note that some parts of the NFC-tag memory cannot be written or are protected with the suitable security credentials. To write certain NFC-tags, specific writing equipment might be necessary.

Smartphones can be NFC-enabled and act as reading- and writing-devices for passive NFC-tags. An updated list of NFC-enabled phones can be found on the Internet[38].

Smart-phones can act as active NFC-enabled devices, e.g., when two smartphones are held closely into each other data can be exchanged between these. This can be used to read sensor data from sensors that do not need a constant data flow.

6.4 ANT and ANT+

ANT+ is the wireless technology that allows accessories such as heart rate monitors, speed/cadence sensors, foot pods and power meters to “talk” to a device. Now ANT+ has gone a step further by allowing certain Garmin devices and accessories to link to fitness equipment. This unique technology allows you to bridge the gap between your indoor and outdoor fitness activities so you can track and store data even from a treadmill run or a spin bike workout.[39] Example of watches can be found in an article in Wired (Senese, 2012).

Chipsets providing the ANT functionality are manufactured by Nordic Semiconductors[40]. Nordic Semiconductors also have more information about the use areas, e.g., in sports and fitness.[41]

6.5 USRP platform for Software Defined Radio (SDR)

The Universal Software Radio Peripheral (USRP)[42] products are computer-hosted software radios designed by Ettus Research, LLC[43]. The platform can be used in the ASSET lab to experiment with SDR and Cognitive radio. Cognitive Radio security is a problem hitherto not solved.

A cognitive radio[44] is a transceiver that automatically detects available channels in wireless spectrum and accordingly changes its transmission or reception parameters so more wireless communications may run concurrently in a given spectrum band at a place. This process is also known as dynamic spectrum management.

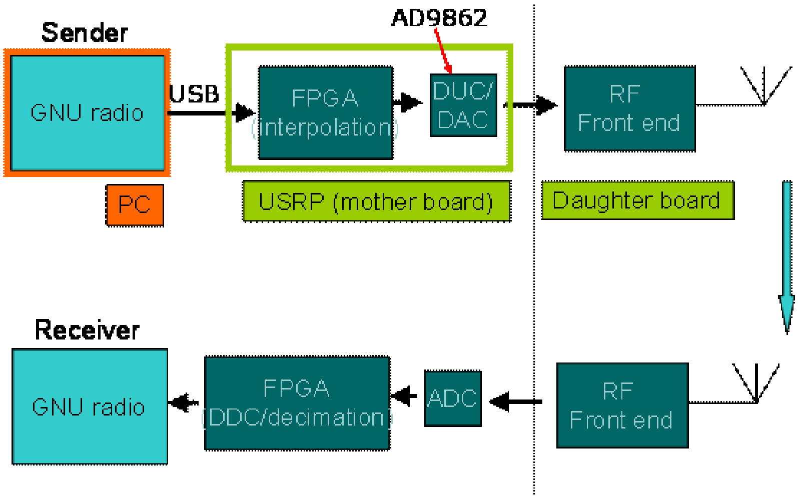


Figure 9. GNU radio data path

6.6 GNU radio for Cognitive Radio Networks

The content of this section is taken from the Wikipedia page on Gnu Radio[45] and the work by Choi et al. (2009).

GNU Radio is a free and open source software development toolkit that provides signal processing blocks to implement software defined radio. It can be used with available low-cost external RF hardware to create software defined radios, or without hardware in a simulation-like environment. It supports Linux and OS X. Programming languages are C++ used for performance critical applications and signal processing blocks as well as Python for non performance critical applications. GNU radio environment contains the most common filter types, modulation- and coding schemes. Figure 9 shows the GNU radio data path.

The GNU Radio project utilises Universal Software Radio Peripheral (USRP), which is a computer based transceiver containing four 64 Msample/sec 12-bit analog-to-digital converters, four 128 Msample/sec 14-bit digital-to-analog converters, a programmable FPGA, and support circuitry for the interface to the host computer. Depending on the model, the host-to-USRP interface is either USB 2.0 or Gigabit Ethernet. The USRP can process signal-bandwidths up to 25 MHz, depending on the model. Several transmitter and receiver plug-in daughter boards are available covering bands between 0 and 5.9 GHz. Two models of USRP exist: USRP1, shown in Figure 10, and USRP2. Table 4 shows a comparison between USRP1 and USRP2.

USRP2 also have multiple-input and multiple-output (MIMO) capabilities, i.e., a MIMO cable port to exchange clock data among USPR2 boards.

There are also possibilities for TCP/IP over GNU Radio and USRP, where the physical layer is provided by GNU radio and the other layers are as provided in Linux. Figure 11 shows the protocol stack.

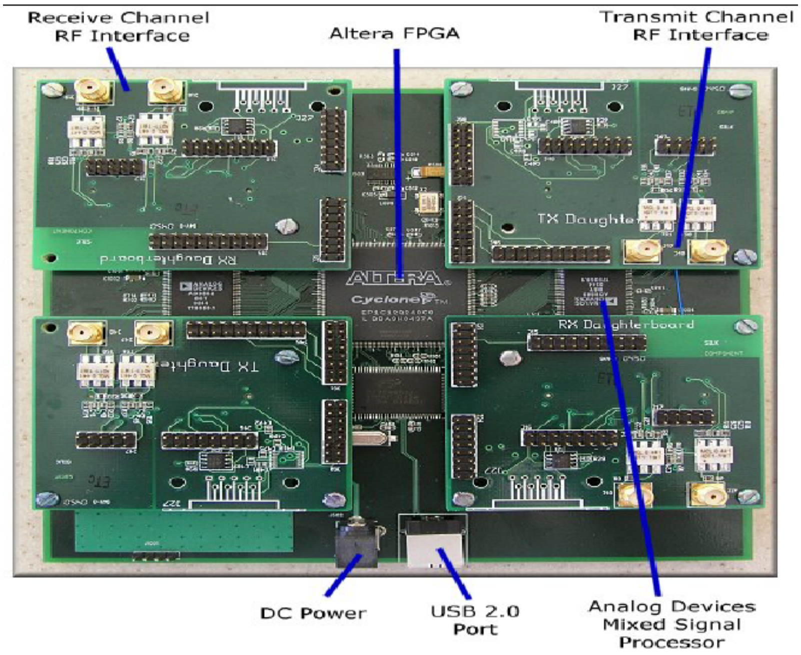


Figure 10. USRP1

Table 4. A comparison between USRP1 and USRP2

	USRP1	USRP2
Internal clock	64MHz	100MHz
Transmission rate	≈ 500kbps, overhead included	≈ 500kbps, overhead included
Range	25-200 m	25-200 m
Interface	USB 2.0 (32Mbit/sec)	Gigabit Ethernet
FPGA	Altera EP1C12	Xilinx Spartan 3 2000
RF Bandwidth to/from host	8 MHz at 16bits	25 MHz at 16 bits
Cost	$700	$1400
ADC samples	12 bit, 64 Msamples/sec	14 bit, 100 Msamples/sec
DAC samples	14-bit, 128 Msamples/sec	16-bit, 400 Msamples/sec
Daughterboard capacity	2 Tx, 2 Rx	1 Tx, 1 Rx
SRAM	None	1 Mbyte
Power	6V, 3A	6V, 3A

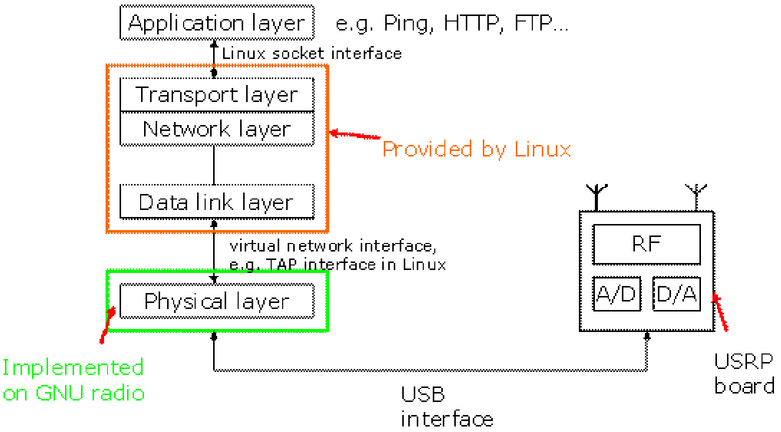


Figure 11. GNU radio and TCP/IP

7 Market Survey

We present a survey of items that are suitable for the ASSET lab. This survey does not represent an exhaustive list, and it is open for feedback. The current price figures are from the distributors' website, and the final cost may vary due to taxes and delivery fees. Recommendations from different suppliers and practitioners suggestions that starter or professional kits are better to go for. These packs and kits contain all the necessary equipment to setup the WSN test bed. For comparison purposes, the kit-options are also included. Tables 5 and 6 present a market survey, including properties and price information.

Table 5. Market survey on wireless sensor network (WSN) devices

#	Company/ Device	Price in USD	Order cond.	Communication	Additional information
1	MoteIV				
	Tmote sky/ TelosB modules platform	90.42 - 120.99	online	USB, an IEEE 802.15.4 compliant, with integrated antenna	Note [46]
	Tmote connect gateway	495.43	online		
	Sensor boards	45.84 - 108.25	online		
	interface modules	26.75	online		
	Tmote sky kit	2101.43	online		1 gateway, 1 interface board, 6 motes, 6 sensor boards and accesories; Note [47]
2	Maxfor				
	TIP mote	90.68	online	IEEE 802.15.4 and USB	Note [48]
	TIP sensor	67.69	online		
	TIP Interface	26.82	online		
	TIP canal gate	83.02	online		
	TIP software	–	online		
3	MEMSIC				
	MICA2/ MICAz platforms /modules	85-120	On request	IEEE/ZigBee 802.15.4; 868/916 MHz multi-channel radio transceiver.	Note [49]
	USB PC Interface Board	95	On request		
	MTS400 sensor board	120	On request		
	MDA300 data acquisition board	–	–		

#	Company/ Device	Price in USD	Order cond.	Communication	Additional information
	MoteView software	–	–		
	kits				tools for development of wireless sensor networks; available in 2.4GHz.
	MEMSIC professional kit	–	–		8 wireless modules, variety of sensor and data acquisition boards, 2 gateway and programming boards, housings for prototype deployment and MoteView visualization software [50]
	MEMSIC classroom kit	–	–		30 wireless modules, 20 sensor and data acquisition boards, 10 gateway and programming boards; [51]
4	Adafruit				
	Arduino uno R3	30	online		Note [52]
	xbee modules	25	online	2.4 GHz IEEE /ZigBee 802.15.4	Note [53]
	arduino shields	20	online		
	other accessories	35	online	USB	
	xbee explorer	20	online		
	Professional kit	450 -520	online		
5	Shimmer				
	Shimmer motes	270	online	2.4 GHz IEEE 802.15.4 radio module with USB port	device designed for mobile health sensing applications
	Shimmer sensors	187.41	online		
	Shimmer kit	1529.88	online		SDK with 3 Shimmer baseboards with enclosures, 3 expansion boards, 1 span platform, 3 USB readers / programming docks with USB leads, 3 2GB microSD cards with adapter, 3 live distribution USB keys, manual [54]
6	Libelium				
	WaspMote		online	ZigBee, Bluetooth, wifi, GSM/GPRS, RFID/NFC, USB	Note [55]
	WaspMote sensors	17	online		
	Waspmote internet gateway/meshlium	115	online		It contains 5 different radio interfaces: Wifi 2.4GHz, Wifi 5GHz, 3G/GPRS, Bluetooth and ZigBee.
	Waspmote - Easy kit ZB pro	1650	online		5 Waspmote ZB PRO SMA 2 DBI, 1 Waspmote Gateway ZB PRO SMA 2 DBI, 1 gases board, 1 events board, 1 temperature sensor, 1 humidity sensor, 1 GPS Module, 1 GSM / GPRS Module, rechargeable batteries; [56]

#	Company/ Device	Price in USD	Order cond.	Communication	Additional information
7	TinyOSMall				
	Kmote Starter Kit	400	online	IEEE 802.15.4 Compliant and programmable vai USB	consist of 1 Kmote-platform, 2 Kmote-sensor boards, software and documentation; [57]
8	NFC Platform				
	RaceTrack NFC, NXP NTAG203		online	contactless NFC	access control, 144 bytes of user memory; [58]
	BullsEye NFC, NXP NTAG203		online	contactless NFC	access control, 144 bytes of user memory; [59]
	Xperia Smart Tags	2.50	online	contactless NFC	no built-in security
	Samsung Tec-Tiles	2.50	online	contactless NFC	no built-in security
9	USRP platform				
	USRP Bus/network series	600/1650	online		Includes 64 MS/s dual ADC, 128 MS/s dual DAC and USB 2.0. Can operate from DC to 6 GHz. Streaming up to 8 MS/s to/ from host applications. Users custom functions in the FPGA fabric. [60]
	Daughterboards	75	online		
	Antennas	45	online		
	cables	30	online		
	accessories	25	online		
10	ANT				
10.1	Maxfor				
	Watch type WSN device	–	On request	2.4 IEEE802.15.4 compliant and Internal ANT	Human body monitoring device based on TinyOS with sensors : body temperature, ECG, momentum, pulsation, air temperature; [61]
10.2	Dynastream				
	ANT Development Kit	428.57	online		4 RF drop-in modules, 2 battery boards, 2 I/O or EEPROM boards, 2 USB interface boards, 2 CR2032 coin cells; Note [62]
	ANT+ enabled sensor platforms	–	online	2.4 IEEE802.15.4 compliant and Internal ANT	Heartbeat, blood pressure , blood sugar level, temperature; Note [63]
11	Smart phones - Android	There are number of smart phones (Sony Xperia™ S can support NFC and ANT+ communications)			

Following pages: Table 6. Fine-grained market survey on wireless sensor network nodes

#	Company /item	sensor type	security	Comm.								Remark
				IEEE 802.15.4	Wifi	BT	Zig Bee	ANT	NFC	GPRS GSM	USB UART	
1	Advanticsys / MEMSIC											
	Tmote sky /TelosB	built-in temperature, light and humidity	hardware link-layer encryption and authentication	✓							✓	custom sensor boards like accelerometer, gyroscope, EMG[64], pulse oximeter or EKG can be integrated
	Tmote sky kit	temperature, light, humidity		✓							✓	– “ –
2	Crossbow											
	MICAz		built-in cryptosystems, e.g., AES[65]	✓			✓				✓	can integrate custom sensor boards of accelerometer, gyroscope, EMG, pulse oximeter, or EKG
	MICAz professional kit	temperature, humidity, barometric pressure, acceleration, ambient light		✓			✓				✓	
3	Adafruit											
	Arduino uno R3, xbee modules			✓			✓				✓	gyro, magnetometer, ECG, EMG, GSR, GPS, temperature, strain gauge modules
	Professional kit			✓			✓				✓	
4	Shimmer											
	Shimmer motes	three-axis accelerometer, vibration switch	built-in cryptosystems, e.g., AES	✓		✓					✓	prepared for gyro, magnetometer, ECG, EMG, GSR, GPS, temperature, strain gauge

#	Company /item	sensor type	security	Comm.								Remark
				IEEE 802.15.4	Wifi	BT	Zig Bee	ANT	NFC	GPRS GSM	USB UART	
	Shimmer kit	accelerometer, gyro, magnetometer, ECG, EMG, GSR, strain gauge, GPS, temperature, barometric pressure		✓		✓					✓	
5	Libelium											
	WaspMote	accelerometer, gyro, magnetometer, strain gauge, GPS, temperature, barometric pressure	cryptography layers: AES 128, point-to-point authentication using AES 256 and public key encryption	✓	✓	✓	✓		✓	✓	✓	With reachargeable battery
	Waspmote – Easy kit ZB pro	many sensors for different areas and applications		✓	✓	✓	✓		✓	✓	✓	With reachargeable battery
6	TinyOSMall											
	Kmote Starter Kit	integrated humidity, temperature, light sensors		✓							✓	
7	NFC platform											
	NFC-enabled smart-phones	many different sensors available		(✓)	(✓)	(✓)	(✓)		✓	(✓)	(✓)	Android-based phones; Many manufacturers, e.g., Samsung, Motorola, LG, HTC, Sony Xperia; [66]

#	Company /item	sensor type	security	Comm.								Remark
				IEEE 802.15.4	Wifi	BT	Zig Bee	ANT	NFC	GPRS GSM	USB UART	
	RaceTrack NFC, NXP NTAG203		access control						✓			antenna size 45 × 76 mm, dry, wet (white) paper face tag
	BullsEye NFC, NXP NTAG203		authentication purpose						✓			antenna size ∅35 mm, dry, wet (white) paper face tag
	Samsung Tec Tiles								✓			TecTiles are programmable NFC tags
	Xperia Smart Tags								✓			programmable NFC tags
8	USRP platform											
	Ettus USRP platform										✓	USRP Bus/ network series (Daughterboards, antennas, cables, accessories)
9	ANT											
9.1	Maxfor											
	Watch type WSN device for healthcare	body temperature, ECG, momentum, pulsation, air temperature		✓				✓				Use internal ANT
9.2	Dynastream											
	ANT+ enabled sensor platforms	heartbeat, blood pressure, blood sugar level, temperature						✓				different ANT+ devices are capable to communicate with smartphones

#	Company /item	sensor type	security	Comm.								Remark
				IEEE 802.15.4	Wifi	BT	Zig Bee	ANT	NFC	GPRS GSM	USB UART	
	ANT Development Kit			✓				✓				
10	Smart phones – Android											
	Sony Xperia™ S and Xperia™ ion	yes	Android built-in security		✓	✓		✓	✓	✓	✓	
	TPH-ONE	accelerometer, 3-axis gyro, magnetometer, ambient light, GPS, proximity sensor	java card 3.01, GlobalPlatform 2.1.1, embedded security elements		✓	✓	✓	✓	✓	✓	✓	TazTag [67].

8 Suggested Devices for the ASSET Lab

Based on the market survey in Section 7 we suggest to consider the devices listed in Table 7 which summarises the main characteristics of these devices. Following these recommendations, the devices listed in Table 8 have been decided to be used in the experiments planned for the ASSET lab.

Table 7. Suggested devices for the ASSET lab

Mote platforms	Shimmer kit	**Sensor:** Accelerometer, gyro, magnetometer, ECG, EMG, GSR, strain gauge, GPS, temperature and barometric pressure. **Communication:** Wi-Fi, Bluetooth, USB. **other:** With rechargeable battery and highly customizable
	WaspMote – Easy kit ZB pro	**Sensor:** Accelerometer, 3-axis gyro, magnetometer, ambient light, GPS, and proximity sensor. **Communication:** Wi-Fi, Bluetooth, GSM, ZigBee, NFC, USB. **other:** With rechargeable battery and highly customizable
Sensor watch	Garmin forerunner[68]	**Sensor:** Body temperature, ECG, momentum, pulse, temperature. **Communication:** Ant
	MOTOACTV	**Sensor:** Body temperature, ECG, momentum, pulse, temperature. **Communication:** Ant
Smartphone	Sony Xperia S and Xperia ion	**Sensor:** Accelerometer, gyro, proximity and compass. **Communication:** Wi-Fi, Bluetooth 3.0, GSM, NFC, USB (USB, microUSB v2.0, USB On-the-go), Ant+. **OS:** Android
	TPH-ONE (taztag.com)	**Sensor:** Accelerometer, 3-axis Gyro, Magnetometer, ambient light, GPS, and proximity sensor. **Communication:** Wi-Fi, Bluetooth 3.0, GSM, ZigBee, NFC, USB. **OS:** Android, **Storage:** microSD
	HTC Rhyme	**Sensor:** ambient light, GPS, digital compass and proximity sensor. **Communication:** Wi-Fi, Bluetooth 3.0, GSM/HSPA/WCDMA, USB, Ant+. **OS:** Android, **Storage:** microSD
Tablet	TAZPAD	**Sensor:** Accelerometer, 3-axis Gyro, Magnetometer, ambient light, GPS, and proximity sensor. **Communication:** Wi-Fi, Bluetooth, GSM, ZigBee, NFC, USB. **OS: Android**. **Storage:** microSD
	Samsung Galaxy Tab 10.1	**Sensor:** Accelerometer, 3-axis Gyro, Magnetometer, ambient light, GPS, and proximity sensor. **Communication:** Wi-Fi, Bluetooth 3.0, HSPA+ and additional adapter needed for the USB. **OS:** Android.

Table 8. Devices planned or purchased for the ASSET lab and price estimation

#	Device type	Unit	Price per unit	No units	Total price	Notes
1	Mote platform	Shimmer platinum kit	21701	1	21701	Notes [69] [70]
2	DASH7	WizziKit with accessories	1683	2	3367	Note [71]
3	Cooking hacks ehealth kit	eHealth Sensor Platform Complete Kit	1851	2	3702	
		Raspberry Pi + Starter Kit	777	2	1555	
4	Smartphone	Sony Xperia S	2806	1	2806	Note [72]
5		Galaxy Nexus 4	3795	1	3795	
6	Tablet	Samsung Galaxy 10	3500	1	3500	
			Max Total	11	44222	—

References

Arch Rock Corporation (2007). IP based wireless sensor networking: Secure, reliable, low power IP connectivity for IEEE 802.15.4 networks. white paper, Arch Rock Corporation. Available from: http://www.cs.berkeley.edu/~jwhui/6lowpan/Arch_Rock_Whitepaper_IP_WSNs.pdf. 15

Arora, A., Dutta, P., Bapat, S., Kulathumani, V., Zhang, H., Naik, V., Mittal, V., Cao, H., Demirbas, M., Gouda, M., Choi, Y., Herman, T., Kulkarni, S., Arumugam, U., Nesterenko, M., Vora, A., and Miyashita, M. (2004). A line in the sand: A wireless sensor network for target detection, classification, and tracking. *Computer Networks: The International Journal of Computer and Telecommunications Networking*, 46:605–634. 10

Balasingham, I., Ihlen, H., Leister, W., Røe, P., and Samset, E. (2007). Communication of medical images, text, and messages in inter-enterprise systems: A case study in Norway. *IEEE Transactions on Information Technology in Biomedicine*, 11(1):7–13. 6, 8, 19

Bougard, B., Catthoor, F., Daly, D. C., Chandrakasan, A., and Dehaene, W. (2005). Energy efficiency of the ieee 802.15.4 standard in dense wireless microsensor networks: Modeling and improvement perspectives. In *Proc. Design, Automation and Test in Europe (DATE'05)*, pages 1530–1591, MESSE Munich, Germany. 12, 25

Choi, S., Han, K., Lee, H., Kim, S., and Kwak, K. (2009). Gnu radio – cognitive radio network. In *Future Internet Winter Camp 2009*. Seoul National University. Available from: http://fif.kr/fiwc2009/doc/shchoi.pdf. 28

Doherty, L., Lindsay, W., and Simon, J. (2007a). Channel-specific wireless sensor network path data. In *ICCCN*, pages 89–94. IEEE. 26

Doherty, L., Lindsay, W., Simon, J., and Pister, K. S. (2007b). Channel-specific wireless sensor network path analysis. Technical report, Dust Networks. 26

Doherty, L. and Teasdale, D. A. (2006). Towards 100% reliability in wireless monitoring networks. In Bao, L. and Lassous, I. G., editors, *PE-WASUN*, pages 132–135. ACM. 26

Hourtane, A. (2004). Facing the challenges in building a next-generation transmission network. *Connected Planet*. accessed February 9, 2013. Available from: http://connectedplanetonline.com/access/infocus/telecom_facing_challenges_building/. 14

Hui, J. and Thubert, P. (2011). Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks. RFC 6282 (Proposed Standard). Available from: http://www.ietf.org/rfc/rfc6282.txt. 15

IEEE (1999). *IEEE P1073.1.3.6/D6.0 Draft Standard for Medical Device Communications - Medical Device Data Language (MDDL) Virtual Medical Device, Specialized - ECG*. IEEE, New York, NY, USA. 42

IEEE (2003). *IEEE Std 802.15.4-2003 Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*. IEEE, New York, NY, USA. 13, 42

IEEE (2011). 802.15.4-2011: IEEE standard for local and metropolitan area networks–part 15.4: Low-rate wireless personal area networks (LR-WPANs). *IEEE Standard*, pages 1 –314. 14

IEEE1451.0 (2007). IEEE standard for a smart transducer interface for sensors and actuators - common functions, communication protocols, and transducer electronic data sheet (TEDS) formats. *IEEE Std 1451.0-2007*, pages 1–335. 14

IEEE1451.5 (2007). IEEE standard for a smart transducer interface for sensors and actuators wireless communication protocols and transducer electronic data sheet (TEDS) formats. *IEEE Std 1451.5-2007*, pages C1–236. 14

ISO/IEC (1994). *ISO/IEC 7489:1-4 Information technology – Open Systems Interconnection – Basic Reference Model*. International Organization for Standardization, Geneva, Switzerland. 12

Johnson, M., Healy, M., van de Ven, P., Hayes, M. J., Nelson, J., Newe, T., and Lewis, E. (2009). A comparative review of wireless sensor network mote technologies. In *IEEE Sensors 2009*, pages 1439–1442. IEEE Press. 24

Karani, M., Kale, A., and Kopekar, A. (2011). Wireless sensor network hardware platforms and multi-channel communication protocols: A survey. *IJCA Proceedings on 2nd National Conference on Information and Communication Technology*, NCICT(5):20–23. Published by Foundation of Computer Science, New York, USA. 24

Kushalnagar, N., Montenegro, G., and Schumacher, C. (2007). IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem

Statement, and Goals. RFC 4919 (Informational). Available from: http://www.ietf.org/rfc/rfc4919.txt. 14

Leister, W., Abie, H., and Poslad, S. (2012a). Defining the ASSET scenarios. NR Notat DART/17/2012, Norsk Regnesentral. confidential. 6, 20

Leister, W., Bjørk, J., Schlatte, R., Johnsen, E. B., and Griesmayer, A. (2012b). Exploiting model variability in abs to verify distributed algorithms. *International Journal On Advances in Telecommunications*, 5(1&2):55–68. Available from: http://www.iariajournals.org/telecommunications/tele_v5_n12_2012_paged.pdf. 13

Leister, W. and Christophersen, N. D. (2012). Itled4240: Compendium spring 2012: Open source, open collaboration and innovation. Technical Report DART/01/2012, Norsk Regnesentral. 43

Leister, W. and Røe, P. (2005). A short memo on open source software for PACS. Technical Report DART/04/05, Norsk Regnesentral. 19

Leister, W., Røe, P., Balasingham, I., Ihlen, H., Roterud, H., Haugland, K.-R., Hauen, O.-M., Kaland, M., and Bosgraaf, R. (2005). Transmission of digital ultrasound images. Technical Report 1003, Norsk Regnesentral. 8

Leister, W. and Schulz, T. (2010). Medical digital items for use in patient monitoring systems. Technical Report DART/13/10, Norsk Regnesentral. 6, 7, 19

Leister, W., Schulz, T., Lie, A., Grythe, K. H., and Balasingham, I. (2011). *Biomedical Engineering Trends in electronics, communications and software*, chapter Quality of Service, Adaptation, and Security Provisioning in Wireless Patient Monitoring Systems, pages 711–736. INTECH. 6, 9

Lewis, F. L. (2004). Wireless sensor networks. In *Smart Environments: Technologies, Protocols, and Applications*. Wiley. 13

Liang, X., Østvold, B. M., Leister, W., and Balasingham, I. (2007). Credo: Modeling and analysis of evolutionary structures for distributed services – user driven requirements. 9

Liao, D., Kewalramani, T., Luo, R., and Shin, J. (2012). Wireless body area sensor networks for biomedical applications. *Governor's School of Engineering and Technology Research Journal*. Available from: http://soe.rutgers.edu/gov-school-research-papers. 26

Otto, C., Milenkovic, A., Sanders, C., and Jovanov, E. (2006). System architecture of a wireless body area sensor network for ubiquitous health monitoring. *Journal of Mobile Multimedia*, 1:307–326. 11

Reed, D. (2003). Applying the osi seven layer network model to information security. Information security reading room, SANS Institute. Available from: http://www.sans.org/reading_room/whitepapers/protocols/applying-osi-layer-network-model-information-security_1309. 20

Salden, A., Stam, A., Balasingham, I., Steffen, M., Kyas, M., Leister, W., Liang, X., and Østvold, B. M. (2008). Credo deliverable 6.1: User driven requirements — addendum. Addendum to Deliverable D6.1, EU IST project, number 33826. 9

Senese, M. (2012). The rundown on sports training watches. Wired. Available from: http://www.wired.com/reviews/2012/03/ts_revtechwatches/. 27

Shnayder, V., Chen, B., Lorincz, K., Fulford-Jones, T. R. F., and Welsh, M. (2005). Sensor networks for medical care. Technical Report TR-08-05, Harvard University, Boston. 42

Song, J., Han, S., Mok, A., Chen, D., Lucas, M., Nixon, M., and Pratt, W. (2008). Wirelesshart: Applying wireless technology in real-time industrial process control. In *Proceedings of the 2008 IEEE Real-Time and Embedded Technology and Applications Symposium*, RTAS '08, pages 377–386, Washington, DC, USA. IEEE Computer Society. 15

Strand, L. (2010). VoIP Lab as a research tool in the EUX2010sec project. NR Note DART/08/10, Norsk Regnesentral. 6, 8

Surman, G. (2002). Understanding security using the osi model. Information security reading room, SANS Institute. Available from: http://www.sans.org/reading_room/whitepapers/protocols/understanding-security-osi-model_377. 20

Vasaasen, E. (2012). Arduino hardware and sensors. personal communication. 26

Notes

[1] EUX2010sec is the name of the Enterprise Unified eXchange 2010 Security project, funded by the Research Council of Norway under project number 180054.

[2] The official name is *uu-lab: Lab for universell utforming og brukskvalitet*.

[3] Blood gas is a measure how much oxygen and carbon dioxide is in the blood.

[4] The sampling rates and resolutions are taken from the the following documents: *IEEE P1073.1.3.6/D6.0 Draft Standard for Medical Device Communications – Medical Device Data Language (MDDL) Virtual Medical Device, Specialised – ECG* (IEEE, 1999), *Biomedical Signal Processing Laboratory* (http://bsp.pdx.edu/Data/), the *Cognition and Brain Sciences Unit EEG Laboratory* (http://www.mrc-cbu.cam.ac.uk/EEG/doc/eeg_intro.shtml), and the *CodeBlue Project* (Shnayder et al., 2005).

[5] See also http://www.ieee802.org/15/.

[6] See http://www.zigbee.org/ (IEEE, 2003) for information on ZigBee. The IEEE 802.15.4 task group 4 (Low Rate WPAN) works also on IEEE 802.15.4a (WPAN Low Rate alternative physical layer), which is providing communications and high precision ranging capabilities, high aggregate throughput, and ultra-low power, using either the 2.4GHz spectrum or the UWB Impulse Radio.

[7] The spectral density is expressed in watts per hertz of bandwidth.

[8] See http://www.ieee802.org/15/pub/TG4.html.

[9] See http://www.zigbee.org/.

[10] See http://6lowpan.net/.

[11] See http://www.hartcomm.org/.

[12] See http://en.wikipedia.org/wiki/ANT_(network) and http://www.thisisant.com/.

[13] See www.thisisant.com.

[14] See http://en.wikipedia.org/wiki/Bluetooth.

[15] See http://en.wikipedia.org/wiki/Bluetooth_low_energy.

[16] See www.dash7.org and http://en.wikipedia.org/wiki/DASH7.

[17] See http://en.wikipedia.org/wiki/Near_Field_Communication.

[18] See https://intern.nr.no/wiki/index.php/NEMO_scrap_page and https://intern.nr.no/wiki/index.php/SIS_Proposal_Nemo and https://intern.nr.no/wiki/index.php/NEMO_RFIDlab_notes.

[19] See also http://www.cisco.com/univercd/cc/td/doc/product/wireless/moblwrls/cmx/mmg_sg/cmxgsm.htm.

[20] See http://www.snm.ethz.ch/snmwiki/Main/HomePage.

[21] The data sheet for the *Tmote Sky* is available at http://www.moteiv.com/products/docs/tmote-sky-datasheet.pdf.

[22] We can consider to use a version of the Tmote Sky where the sensors for humidity, temperature, and light are not included on-chip.

[23] The data sheet for the Tmote Connect is available at http://moteiv.com/products/docs/tmote-connect-datasheet.pdf.

[24] TinyOS is intended to be incorporated into smartdust. Smartdust is a hypothetical network of tiny wireless micro-electromechanical systems (MEMS) sensors, robots, or devices, installed with wireless communications, that can detect anything from light and temperature, to vibrations, etc.

[25] More information on TinyOS can be found at http://www.tinyos.net/.

[26] *nesC* is an acronym for "network embedded system C". A description is available from http://csl.stanford.edu/~pal/pubs/tinyos-programming.pdf.

[27] Drivers for the host computer are available for Windows, Linux, BSD, Macintosh, and Windows CE.

[28] Detailed information of CC 2420 is available in Chipcon's datasheet at http://www.chipcon.com/files/CC2420_Data_Sheet_1_4.pdf

[29] Thanks to Mohammad Mostafizur Rahman Mozumdar, Ph.D., assistant professor at California State University, Long Beach, mohammad.mozumdar@csulb.edu.

[30] See http://www.maxfor.co.kr/eng/en_sub1.html.

[31] See http://www.linear.com/products/wireless_sensor_networks.

[32] See http://en.wikipedia.org/wiki/Arduino.

[33] See arduino.cc.

[34] About licensing of hardware, content, and software see Leister and Christophersen (2012).

[35] See http://www.adafruit.com/products/659.

[36] See http://www.dealextreme.com/p/arduino-nano-v3-0-81877.

[37] See http://www.dealextreme.com/p/12mm-rgb-bare-point-source-red-green-blue-50-led-string-light-111682.

[38] The list of NFC-enabled phones is available from http://www.nfcworld.com/nfc-phones-list/. The first category on this list is relevant for the ASSET lab, i.e., phones that can be bought today.

[39] See http://www8.garmin.com/intosports/antplus.html.

[40] See http://www.nordicsemi.com/eng/Products/ANT; see, e.g., the product *nRF24AP2* http://www.nordicsemi.com/eng/Products/ANT/nRF24AP2-1CH.

[41] See http://www.nordicsemi.com/chi/Applications/Sports-and-Fitness.

[42] See http://en.wikipedia.org/wiki/Universal_Software_Radio_Peripheral.

[43] See www.ettus.com.

[44] See http://en.wikipedia.org/wiki/Cognitive_radio.

[45] See http://en.wikipedia.org/wiki/Gnu_radio and http://gnuradio.org.

[46] See http://www.advanticsys.com/shop/prokit-p-11.html.

[47] See http://www.advanticsys.com/shop/prokit-p-11.html.

[48] See http://www.advanticsys.com/shop/mtsem1000-p-12.html.

[49] See http://www.memsic.com/products/wireless-sensor-networks/wireless-modules.html.

[50] See http://www.memsic.com/support/documentation/wireless-sensor-networks/category/7-datasheets.html?download=154%3Awsn-professional-series.

[51] See http://www.memsic.com/support/documentation/wireless-sensor-networks/category/7-datasheets.html?download=171%3Aclassroom-kits.

[52] See http://www.adafruit.com/category/17.

[53] See http://dx.com/s/arduino.

[54] See http://www.shimmer-research.com/p/products/development-kits/lab-development-kit.

[55] See http://www.libelium.com/products/waspmote/hardware.

[56] See http://www.cooking-hacks.com/index.php/shop/waspmote/waspmote-easy-kit-zb-pro.html.

[57] See http://www.tinyosmall.com/Kmote_Starter_Kit_p/300-201.htm.

[58] See http://nfctags.com/racetrack-nfc-nxp-ntag203.

[59] See http://nfctags.com/smartrac-bullseye-nfc-ntag.

[60] See https://www.ettus.com/product/category/USRP_Bus_Series.

[61] See http://maxfor.co.kr/eng/en_sub4_3.html.

[62] See http://webapps.nuhorizons.com/storefront/PartSearch.do.

[63] See http://www.thisisant.com/directory/.

[64] EMG = electromyogram

[65] AES = advanced encryption system for cryptographic operations.

[66] See list at http://www.nfcworld.com/nfc-phones-list/.

[67] See http://www.taztag.com/index.php.

[68] Several models available; see https://buy.garmin.com/shop/shop.do?cID=142.

[69] incl. multi-gang charger

[70] see http://www.shimmer-research.com/p/products/development-kits/platinum-development-kit.

[71] See http://www.wizzilab.com/shop/wizzikit/.

[72] See Elkjop.no/Expert.no