A Review: Wireless Sensor Networks and Its Application, Platforms, Standards and Tools

K.Sarammal [1], R.A.Roseline[2]
[1]*M.Phil Scholar, Government Arts College, Coimbatore.*
[2]*Assistant Professor of Computer Science*
Government Arts College, Coimbatore.

Abstract:
Wireless Sensor Networks (WSN) is formed by a large number of networked sensing nodes. The main goal of a WSN is to produce meaningful information from raw local data collected by individual sensors. The low cost, flexibility, fault tolerance, high sensing fidelity, and rapid deployment characteristics of sensor networks create many new and exciting application areas for remote sensing. In this paper, a survey on Wireless Sensor Networks (WSN) and their architecture, applications, standards in WSN are carried out. Further, the test beds used in WSNs and network tools are surveyed.

***Keywords*:** Wireless Sensor Network, Sensor Nodes, Applications, Standards, Test beds, Network tools.

I. INTRODUCTION

Modern wireless sensor networks are made up of a large number of inexpensive devices that are networked via low power wireless communications. Wireless sensor networks (WSNs) have gained worldwide attention in recent years, particularly with the proliferation in Micro-Electro-Mechanical Systems (MEMS) technology which has facilitated the development of smart sensors [1]. Smart sensor nodes are low power devices equipped with one or more sensors, a processor, memory, a power supply, a radio, and an actuator. Advances in hardware and wireless network technologies have created low-cost, low power, multifunctional miniature sensor devices. Sensor network is composed of a large number of sensor nodes, which are densely deployed and are prone to failure.

Sensor nodes are limited in power, computational capacities, and memory. Unlike traditional networks, a WSN has its own design and resource constraints. Resource constraints include a limited amount of energy, short communication range, low bandwidth, and limited processing and storage in each node. Design constraints are application dependent and are based on the monitored environment. The environment plays a key role in determining the size of the network, the deployment scheme, and the network topology. The size of the network varies with the monitored environment. For indoor environments, fewer nodes are required to form a network in a limited space whereas outdoor environments may require more nodes to cover a larger area. Wireless sensor networks contain hundreds or thousands of these sensor nodes, and these sensors have the ability to communicate either among each other or directly to an external base station.

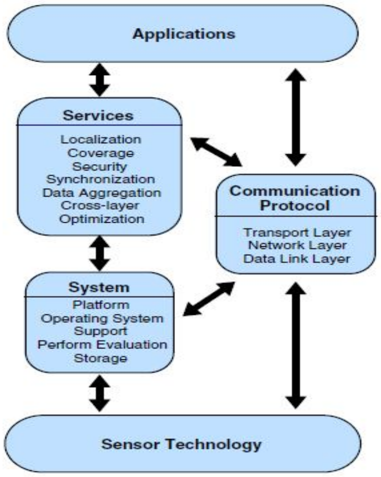

Fig.1: Broad classification of various issues in a WSN.

Wireless sensor technologies can be classified into three groups as shown in the Fig.1: system, communication protocols and services. System is the first group. Each sensor node is an individual system. In order to support different application software on a sensor system, researchers need to develop new platforms, operating systems, and storage schemes. The second group is communication protocols, which enable communication between the application and sensors. They also enable communication between the sensor nodes. The communication protocol consists of five standard protocol layers for packet switching: application layer, transport layer, network layer, data-link layer, and physical layer. Implementation of protocols at different layers in the protocol stack can significantly affect energy consumption, end-to-end delay, and system efficiency. It is important to optimize communication and minimize energy usage.

Traditional networking protocols do not work well in a WSN since they are not designed to meet these requirements. Hence, researchers must look into new energy-efficient protocols though some have been proposed for all layers of the protocol stack to meet WSN requirement. The last group is services which are developed to enhance the application and to improve system performance and network efficiency. Network services include sensor provisioning, management, and control. These are developed to co-ordinate and manage sensor nodes. Provisioning involves coverage and localization. Management and control services play key roles in WSNs as they provide support to middleware services such as security, synchronization, data compression and aggregation cross-layer optimization, etc.

Wireless sensor technologies enable two primary functions. The first is monitoring, for which information flows from the field to the user. The second is control, that is, management of the sensor system itself or the environment in which it is embedded [2]. In fact, two properties of sensor networks can be exploited to improve communication efficiency: the cooperative nature of the sensors and application-dependent performance measures.

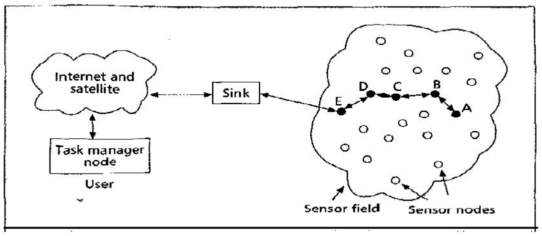

Figure 2: Communication architecture of wireless sensor networks

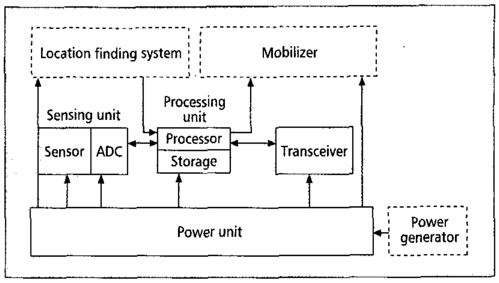

Figure 3: The components of a sensor node

II. SENSOR NODES AND ARCHITECTURE

The sensors also have the ability to transmit and forward sensing data to the base station. Most modern WSNs are bi-directional, enabling two-way communication, which could collect sensing data from sensors to the base station as well as disseminate commands from base station to end sensors. The sensor nodes are usually scattered in the sensor field where the sensor nodes are deployed as shown in the Fig. 2. When deployed in large quantities in a sensor field, these sensors can automatically organize themselves to form an adhoc multihop network to communicate with each other and with one or more sink nodes. A remote user can inject commands into the sensor network via the sink to assign data collection, processing and transfer tasks to the sensors and it can later receive the data sensed by the network through the sink. Each of these scattered sensor nodes has the capability to collect and route data either to other sensors or back to the sink. The sink may communicate with the task manager via Internet or satellite.

A sensor node consists of four components as shown in the Fig. 3: a sensing unit, a processing unit, a transceiver unit, and a power unit [3]. Sensing units are usually composed are two subunits: sensors and analog to digital converters (ADCs). The analog signals produced by the sensors are converted into digital signals by the ADC, and then fed into the processing unit. The processing unit is associated with a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks. A transceiver unit allows the transmission and reception of data to other devices connecting a wireless sensor node to a network.

Wireless sensor nodes typically communicate using an RF (radio frequency) transceiver and a wireless personal area network technology such as Bluetooth or complaint protocols. One of the important components of a sensor node is power unit. Power units may be supported by power scavenging units such as solar cells. Energy from the power scavenging techniques may only be stored in rechargeable (secondary) batteries. For battery-operated sensors, energy conservation is one of the most important design parameters, since replacing batteries may be difficult or impossible in many applications. Thus sensor network design must be optimized to extend the network lifetime. The sensor node also consists of additional components such as location finding system, power generator and mobilizer.

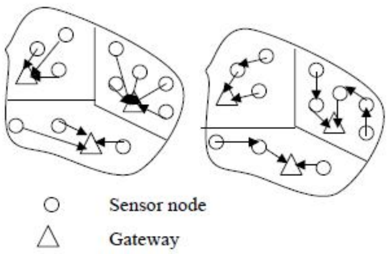

Figure 3: Two configurations for sensor networks

Figure 3 shows two different configurations for wireless sensor networks [4]. In both configurations the nodes are scattered in a geographical are, the area is divided into clusters with a gateway in each cluster. Nodes in each cluster communicate with the gateway. The gateway collects the data and forwards it to the user. In (a) nodes directly communicate with the gateway in its cluster, while in (b) nodes use chaining in order to communicate with the gateway. Using chaining reduces the energy used in transmission, but increases the energy used in processing since each node should receive and forward the message to and from other nodes. Some sensor networks may have more than one level of aggregation. Typically, sensor networks works in one of two modes. Continuous operation, or query mode. In continuous operation mode, the node is continuously sensing the environment and sending the data (or the processed data) to neighboring or a central node. In query mode, the node is usually powered down waiting for a command from a central node, or neighboring node. When the node receives the commands (usually on the form of report on so and so) it collects data from the sensor, processes it and sends it to the requesting node.

III. APPLICATIONS OF SENSOR NETWORK:

Sensor networks may consist of many different types of sensors such as seismic, low sampling rate magnetic, thermal, visual, infrared, and acoustic and radar, which are able to monitor a wide variety of ambient conditions [5]. Sensor nodes can be used for continuous sensing, event detection, event ID, location sensing, and local control of actuators. The concept of micro-sensing and wireless connection of these nodes promises many new application areas. We categorize the applications into military, environment, health, home and other commercial areas. Wireless sensors have become an excellent tool for military applications involving intrusion detection, perimeter monitoring, information gathering and smart logistics support in an unknown deployed area. Some other applications: sensor-based personal health monitor, location detection with sensor networks and movement detection.

Recently, Wireless Sensor Networks are focusing on national security applications and consumer applications such as:-

1. Military applications
   - Monitoring, tracking and surveillance of borders
   - Nuclear, biological and chemical attack detection
   - Battle damage assessment
2. Environmental applications
   - Flood and oceans detection
   - Forest fire detection
   - Precision agriculture
3. Health applications
   - Drug administration
   - Remote monitoring of physiological data
   - Tracking and monitoring doctors and patients inside a hospital
4. Home applications
   - Automated meter reading
   - Home automation
   - Instrumented environment
5. Commercial applications
   - Monitoring vibration that could damage the buildings structures
   - Monitoring traffic flow and road condition
   - Vehicle tracking and detection

IV. SYSTEM PLATFORM AND OS SUPPORT

In order to facilitate ease and rapidity in the development of sensor network applications, a sensor Operating System (sensorOS) provides the necessary software infrastructure.

We mentioned two platforms: a Bluetooth-based sensor system [6] and a detection-and-classification system [7].

A. BLUETOOTH

There are two types of radio components: fixed frequency carriers, spread –spectrum transmissions. Sensor nodes based on fixed frequency carriers shared a single channel to transmit data within the communication range whereas Bluetooth is based on the spread- spectrum transmission uses separate channel to transmit data within the communication range. Spread spectrum techniques increase the channel reliability and the noise tolerance by spreading the signal over a wide range of frequencies. The Bluetooth protocol is complex with its six layers. Bluetooth has a relatively high power consumption, it also has long connection setup times and a lower degree of freedom with respect to possible network topologies. The Bluetooth module embeds both the physical layer and the MAC layer through the three bottom layers of the Bluetooth stack (baseband, link manager and the host controller interface). We designed and implemented a tiny Bluetooth stack for TinyOS and ported it into the BTnodes. The BTnodes were developed by ETH Zurich. In order to support a multi-hop network, each BTnode is equipped with two radios: one configured to operate as a master and the other as a slave. Bluetooth connections are estsblished between a master and a slave. The nodes cannot exchange information before they have established a connection. In addition, slaves cannot communicate with other slaves or overhear the communication taking place on other connections.

B.DETECTION-AND-CLASSIFICATION SYSTEM:

The detection and classification system in VigilNet, which classifies vehicles, persons, and persons carrying ferrous objects, and tracks these targets with a maximum error in velocity of 15%. The VigilNet surveillance system [5] is a WSN with 200 sensors Nodes VigilNet uses the ExScal motes as sensor nodes. Each sensor node is equipped with a magnetometer, a motion sensor, and a microphone. The hierarchical classification architecture is comprised of four tiers – sensor-level, node-level, group-level, and base-level. The lowest level deals with individual sensors and comprises the sensing algorithms for the corresponding sensors. After processing the sensor data, each sensing algorithm delivers the confidence vector to the higher level module – the node-level detection and classification module. The node-level classification deals with output from multiple sensors on the node. The node-level classification module monitors the sensors' status and performs sanity control over sensors. The sensor-level and node-level classification functions both reside on a single node. The group-level classification is performed by groups of nodes. The input to the group-level classification is the node-level confidence vectors. The highest level in the hierarchical classification architecture is the base-level classification. The group-level classification results are serving as the input to the base-level classification algorithm which is transported via multiple hops to the base mote. The base-level classification algorithm finalizes the result and report the result.

V. STANDARDS

The standard defines the functions and protocols necessary for sensor nodes to interface with a variety of networks. Some of these standards include IEEE802.15.4[8], ZigBee[9,10], WirelessHART [11, 12], IETF 6LoWPAN [13], IEEE 802.15.3 [14], Wibree [15]. The following paragraphs describe these standards in more detail.

A. IEEE 802.15.4:

IEEE 802.15.4 is a proposed standard addressing the needs of low-rate wireless personal area networks.

IEEE 802.15.4 focuses on low cost of deployment, low complexity, and low power consumption. The IEEE 802.15.4 devices are proposed to operate in the 2.4 GHz industrial, scientific and medical (ISM) band. The standard allows the formation of two possible network topologies: the star topology or the peer-to-peer topology. In the star topology, the communication is performed between network devices and a single central controller. Peer-to-peer topology allows more complex network formations to be implemented; e.g. ad hoc and self-configuring networks. IEEE 802.15.4 can operate at bandwidths of 250 kbit/s at 2.4 GHz, 40 kbit/s at 915 MHz (America) and 20 kbit/s at 868 MHz (Europe). The IEEE 802.15.4 medium access control (MAC) sub layer controls the access to the radio channel employing the CSMACA mechanism. The 802.15.4 MAC is also responsible for flow control via acknowledged frame delivery, frame validations as well as maintaining network synchronization, and network services. The standard is characterized by maintaining a high level of simplicity, allowing low cost and low power implementations.

B. ZigBee:

ZigBee standardizes the higher layers of the protocol stack. The network layer (NWK) is in charge of organizing and providing routing over a multihop network (built on top of the IEEE 802.15.4 functionalities), while the Application Layer (APL) intends to provide a framework for distributed application development and communication. Besides the star topology, the ZigBee network layer also supports more complex topologies like the tree and the mesh. ZigBee identifies three device types. A ZigBee end-device, ZigBee router, ZigBee coordinator. Security services provided for ZigBee include methods for key establishment, key transport, frame protection, and device management. To provide security for the MAC Layer frames, ZigBee would use MAC Layer security specified in the 802.15.4 specifications. The energy efficiency approach of the ZigBee standard is mainly at the physical and MAC layers. ZigBee supports two operating modes. One is based on a TDMA algorithm and it is very effective but limited in scope to star network configurations the other operating mode is based on CSMA and basically tries to reduce power consumption with very low duty cycles. The ZigBee protocol promises to provide a long battery life (months or even years on a single battery charge) and to be a lower-cost alternative to Bluetooth for wireless sensing and control applications.

C. 6LoWPAN:

The Internet of Things (IoT) is the main justification for the Future Internet, where IPv6 is the fundamental technology. 6LoWPAN is an acronym of IPv6 over Low power Wireless Personal Area Networks. 6LoWPAN is the name of a working group in the Internet area of the IETF. The 6LoWPAN concept originated from the idea that "the Internet Protocol could and should be applied even to the smallest devices," and that low-power devices with limited processing capabilities should be able to participate in the Internet of Things. The 6LoWPAN group has defined encapsulation and header compression mechanisms that allow IPv6 packets to be sent to and received from over IEEE 802.15.4 based networks. IPv4 and IPv6 are the work horses for data delivery for local-area networks, metropolitan area networks, and wide-area networks such as the Internet. IPv6 requires the maximum transmission unit (MTU) to be at least 1280 Bytes. In contrast, IEEE 802.15.4's standard packet size is 127 octets. 6LoWPAN is designed for applications with low data rate devices that require Internet communication.

D. Wibree:

Wibree is a new interoperable radio technology for small devices[15]. It can be built into products such as watches, wireless keyboards, gaming and sports sensors, which can then connect to host devices such as mobile phones and personal computers. Wibree is mainly designed for applications where ultra low power consumption, small size and low cost are the critical requirements. One of the most important aspects of Wibree is that it envisages dual-mode chips that can support both Bluetooth and Wibree. The dual modes are targeted at mobile phones, multimedia computers and PCs. Wibree operates in 2.4 GHz ISM Wibree link layer specification Wibree link layer provides ultra low power idle mode operation, simple device discovery and reliable point-to-multipoint data transfer with advanced power-save and encryption functionalities. The link layer provides means to schedule Wibree traffic in between Bluetooth transmissions. Wibree will enable C2M - Consumer to Machine|| or Consumer to Middleware|| applications at a price point that makes them mass market. M2M is only just beginning to deliver against its promises. Wibree may result in C2M delivering an even larger promise in a shorter timescale.

E. IEEE 802.15.3:

The IEEE 802.15.3 medium access control (MAC) protocol is an emerging standard for high bit-rate wireless personal area networks, specifically for supporting high quality multimedia streams**.** These technologies include both medium access control (MAC) and physical layer protocols. It supports 2.4 GHz physical layer is capable of a maximum data rate of 55

Mb/s. The current IEEE 802.15.3 MAC offers excellent support for real-time applications since it uses a connection-orientated time division multiple access (TDMA) approach. the IEEE 802.15.3 MAC offers fast connection time, ad-hoc network configuration, QoS, security, and dynamic membership. The IEEE 802.15.3 MAC offers three acknowledgment policies, namely no acknowledgment (No-ACK), immediate acknowledgment (Imme-ACK) and delayed acknowledgment (Dly-ACK). When a flow uses the No-ACK policy, it is implicitly assumed that all packet transmissions are successful. In contrast, for a flow using the Imme-ACK policy, an explicit acknowledgment is sent for every packet. Finally, the Dly- ACK policy, used only in the CTAP, allows the transmission of a burst of packets before the receiver is required to send a group acknowledgment. The standard is used in devices such as wireless speakers, portable video electronics, and wireless connectivity for gaming, cordless phones, printers, and televisions.

VI. TESTBEDS:

WSN testbeds are deployed in a controlled environment, generally with public access and ongoing maintenance. It is a intermediate tool between a real deployment and a simulator or emulator. It provides researchers a way to test their protocols, algorithms, network issues and applications. Here we discuss about various testbeds.

A. MoteLab:

MoteLab **[17]** consists of a set of permanently deployed sensor network nodes connected to a central server which handles reprogramming and data logging while providing a web interface for creating and scheduling jobs on the testbed. In its original design, the testbed was comprised from Mica2 nodes, each connected to Ethernet backbone via dedicated Crossbow interface boards, providing TCP forwarding for the serial ports. MoteLab consists of several different software components: MySQL Database Backend, Web Interface, DBLogger and Job Daemon**.** MoteLab uses a MySQL database to store all information needed for testbed operation. MoteLab uses PHP to generate dynamic web content, and JavaScript to provide an interactive user experience. This allows users to access the lab in a platform-independent way. DBLogger is a Java program started at the beginning of every job. It connects to each node (via the each node’s interface board’s data logging TCP port described in Section III-A) and uses class introspection to parse messages sent over its serial port and insert them into the appropriate MySQL database. The job daemon is responsible for re-programming each node and starting and stopping system components. MoteLab is also a valuable tool for teaching sensor network concepts, allowing students to experiment with a real testbed. MoteLab is unique in its ability to manage a network of real, network-attached wireless sensor network nodes.

B. ORBIT:

The ORBIT[18] testbed consists of an indoor radio grid emulator for controlled experimentation and an outdoor field trial network for end-user evaluations in real-world settings. The ORBIT testbed consists of an indoor radio grid emulator for controlled experimentation and an outdoor field trial network for end-user evaluations in real-world settings.

The radio node is a custom wireless node which consists of:

− 1-GHz VIA C3 processor with 512 MB of RAM and a 20 GB local hard disk

− two wireless mini-PCI 802.11a/b/g interfaces

− Two 100BaseT Ethernet ports for experimental data and control respectively.

_ integrated chassis manager that is used to remotely monitor the status of each radio node’s hardware.

VII. NETWORK TOOLS:

Simulation is one of the important technologies in modern time. In this section the most relevant simulation environments used to study WSN are introduced, and their main features and implementation issues described.

A. Network simulator-2:

Network simulator-2[19] NS is an event driven network simulator developed at Berkeley that simulates variety of IP: networks. It implements network protocols such as TCP and UDP, traffic source behavior such as FTP, Telnet, Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBQ, routing algorithms such as Dijkstra, and more. **NS** is an object oriented simulator, written in C++, with an OTcl interpreter as a frontend. NS uses two languages C++ and OTcl. The user describes a network topology by writing OTcl scripts, and then the main NS program simulates that topology with specified parameters. When a simulation is finished, NS produces one or more text-based output files that contain detailed simulation data, if specified to do so in the input Tcl script. The data can be used for simulation analysis or as an input to a graphical simulation display tool called Network Animator(NAM) that is developed as a part of VINT project. NAM has a nice graphical user interface similar to that of a CD player, and also has a display speed controller. Furthermore, it can graphically present information such as throughput and number of packet drops at each link, although the graphical information cannot be used for accurate simulation analysis.

B. QualNet:

QualNet [20**]** is a comprehensive suite of tools for modeling large wired and wireless networks. It uses simulation and emulation to predict the behavior and performance of networks to improve their design, operation and management.

QualNet enables users to:

• Design new protocol models.

• Optimize new and existing models.

• Design large wired and wireless networks using pre-configured or user-designed models.

- Analyze the performance of networks and perform what-if analysis to optimize them.

QualNet GUI consists of Architect, Analyzer, Packet Tracer, and File Editor. Architect is a network design and visualization tool. It has two modes: Design mode and Visualize mode.

In Design mode, you can set up terrain, network connections, subnets, mobility patterns of wireless users, and other functional parameters of network nodes. You can create network models by using intuitive, click and drag operations. You can also customize the protocol stack of any of the nodes. You can also specify the application layer traffic and services that run on the network.

In Visualize mode, you can perform in-depth visualization and analysis of a network scenario designed in Design mode. As simulations are running, users can watch packets at various layers flow through the network and view dynamic graphs of critical performance metrics. Real-time statistics are also an option, where you can view dynamic graphs while a network scenario simulation is running.

Analyzer is a statistical graphing tool that displays the metrics collected during the simulation of a network scenario in a graphical format. You can customize the graph display. All statistics are exportable to spreadsheets in CSV format.

Packet Tracer provides a visual representation of packet trace files generated during the simulation of a network scenario. Trace files are text files in XML format that contain information about packets as they move up and down the protocol stack.

File Editor is a text editing tool that displays the contents of the selected file in text format and allows the user to edit files.

C. NetSim:

NetSim is a discrete event simulator developed by Tetcos in 1997, in association with Indian Institute of Science. NetSim has also been featured with Computer Networks and Internets V edition by Dr. Douglas Comer, published by Prentice Hall. It has an object-oriented system modeling and simulation (M&S) environment to support simulation and analysis of voice and data communication scenarios for High Frequency Global Communication Systems (HFGCS).

NetSim is available both commercial and academic versions, and can be used for modeling and simulation of various network protocols, including WLANs, Ethernet, TCP/IP, and asynchronous transfer mode (ATM) switches [19]. NetSim allows a detailed performance study of Ethernet networks, including wireless Ethernet. The effect of relative positioning of stations on network performance, a realistic signal propagation modeling, the transmission of deferral mechanisms, and the collision handling and detection processes can also be investigated. The main strength of NetSim is that the package can be run on a variety of operating systems. However, the use of NetSim is limited to academic environments only.

VII. CONCLUSION

In this research work, a survey on Wireless Sensor Networks (WSN) and their technologies, standards and applications was carried out. Wireless sensor networks consist of small nodes with sensing, computation, and wireless communications capabilities. Unlike other networks, WSNs are designed for specific applications. Applications include, but are not limited to, environmental monitoring, industrial machine monitoring, surveillance systems and military target tracking. Each application differs in features and requirements. To support this diversity of applications, the development of new communication protocols, algorithms, designs, and services are needed. Network tools for WSNs are also discussed. In future a lot of work needs to be done in sensor networks in order to mature and become an acceptable technology.

REFERENCES:

[1]. Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal. “Wireless sensor network survey” Department of Computer Science, University of California, Davis, CA95616, United State. 2008.

[2]. Kriti Jain, Upasana Bahuguna, “Survey on Wireless Sensor Network”, Tulas Institute, Dehradun, India, 2012.

[3]. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, “A survey on sensor networks”, IEEE Communications Magazine 40 (8) (2002) 102–114.

[4]. Mokhtar Aboelaze, Fadi Aloul, “Current and Future trends in Sensor Networks: A Survey”.

[5] I.F. Akyildiz, W.J. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Computer Networks 38 (2002) 393–422.

[6] M. Leopold, M.B. Dydensborg, P. Bonnet, Bluetooth and sensor networks: a reality checks, in: Proceedings of the Sensys’03, Los Angeles, CA, 2003.

[7] L. Gu, D. Jia, P. Vicaire, T. Yan, L. Luo, A. Tirumala, Q. Cao, T. he, J.A. Stankovic, T. Abdelzaher, B.H. Krogh, Lightweight detection and classification for wireless sensor networks in realistic environment, in: Proceedings of the Sensys’05, Los Angeles, CA, 2005.

[8] I. Howitt, J.A. Gutierrez, IEEE802.15.4 low rate-wireless personal area network coexistence issues, Wireless Communications and Networking 3 (2003) 1481–1486.

[9] ZigBee: wireless control that simply works, <http://www.zigbee. org>.

[10] ZigBee Standards Overview, <http://www.freescale.com/webapp/sps/site/overview.jsp?nodeId=01J4Fs25657725>.

[11] HART – The Logical Wireless Solution, <http://www.hartcomm2.org/hart_protocol/wireless_hart/hart_the_logical_solution.html>.

[12] Draft standard: What’s in the April’07 WirelessHART specification, <http://www.controleng.com/article/CA6427951.html>.

[13] G. Mulligan, L.W. Group, The 6LoWPAN architecture, in: Proceedings of the EmNets, Cork, Ireland, 2007.

[14] IEEE Standard 802.15.3, Wireless medium access controls (MAC) and physical layer (PHY) specifications for high rate wireless person area networks (WPANs), September 2003.

[15] Wibree, <http://www.wibree.com/>.

[16] J. Newsome, D. Song, GEM: Graph EMbedding for routing and data centric storage in sensor networks without geographic information in: Proceedings of the Sensys’03, San Diego, CA, 2003.

[17] G. Werner-Allen, P. Swieskowski, M. Welsh, MoteLab: a wireless sensor network testbed, in: ISPN, 2005.

[18] D. Raychaudhuri, I. Seskar, M. Ott, S. Ganu, K. Ramachandran, H. Kremo, R. Siracusa, H. Liu, M. Singh, Overview of the ORBIT radio grid testbed for evaluation of next-generation wireless network protocols, in: Proceedings of the IEEE Wireless Communications

and Networking Conference, 2005.
[19] Nurul I. Sarkar, Senior Member, IEEE and Syafnidar A. Halim, “A Review of Simulation of Telecommunication
Networks: Simulators, Classification, Comparison, Methodologies, and Recommendations”.