Wireless Technologies for Integrated e-Operations in Offshore Environments

Malka N. Halgamuge*
University of Melbourne, Australi

Jayantha P. Liyanage
Center for Industrial Asset Management, University of Stavanger, Stavanger, Norway

Priyan Mendis
University of Melbourne, Australia

**Email: malka.nisha@unimelb.edu.au*

ABSTRACT: **In large and complex production environments it is impossible to install a full-featured physically wired network to manage operations, 24/7, because of nature and the complexity of activities and data. Wireless networking can bring major benefits in such settings, and in particular where e-Operations and smart technical solutions remains the ambition. Wireless sensor network (WSN) have the capability of real-time monitoring and automatic control of in-building environment is a vital application. Some of the challenges, for instance, the poor link quality in the transitional region may be attributed to the many obstacles within the path including concrete element, brick walls, plasterboard partitions, office furniture and other items that either absorbs or reflects these waves leading to signal loss or multi-path effects. Therefore, combination of technologies, for instance, wireless local area network (WLAN), radio frequency identification (RFID), Bluetooth, ZigBee and remote sensors would be the best solution in congested sites. Sensors can be connected to a WLAN, which then collect data and transmit it to a central location. Experts in production environments can monitor their equipment, production and process condition from a control room or an office. This paper presents a framework for potential application of such a combined solution for offshore oil & gas production environments.**

Index Terms – Assets management, Integrated operations, offshore oil & gas production, wireless communication,

1 INTRODUCTION

Many industrial sectors across the world undergo major changes today as the conditions under which commercial operations have to be performed have taken significant turns. Various factors ranging from economic recessions to new regulations have brought many challenges where high-risk sectors in particular are compelled to find novel and innovative solutions to manage their commercial operations. Offshore oil & gas production industry has over the last few years begun to launch many advanced solutions committing USD billions of investments so that complex production facilities can continue to be operated for a prolonged period of time. Across the world, while there is a constant growth in the demand for energy on one hand, the available production capacity has large limitations on the other. In North Sea, in particular the challenges to the offshore oil & gas production process became very evident in the early 2000s. It became very clear that a considerable proportion of the existing production facilities have reached the maturity in production with a forecast that production can only be limited to 2-3 decades ending the prospects. Moreover, new findings were quite marginal restricting further investments for field development as the cost levels were calculated to be quite high limiting economical feasibility of new projects. The entire sector clearly identified the need for innovative solutions, so that production costs can significantly be reduced, and at the same time safety and other risks can be effectively met, while prolonging the commercial lives of major assets. Obviously, the

possible access to advanced technological solutions provided a major hope to this change process. Subsequently, a concept termed *Integrated e-Operations (IO)* was introduced to North sea assets anticipating long-term commercial benefits (Liyanage, 2008, Liyanage & Langeland, 2008).

The IO initiative, since then gradually began to restructure the sector. The IO concept was completely dedicated to find smarter solutions to manage offshore assets more effectively and efficiently through collaborative solutions. Major players today have begun to explore various options where the 'distances' for instance between offshore-onshore, operator-service providers, etc. can drastically be reduced while enhancing decision making and work management processes based on real-time data. The basic configuration of IO is briefly illustrated in Figure 1.

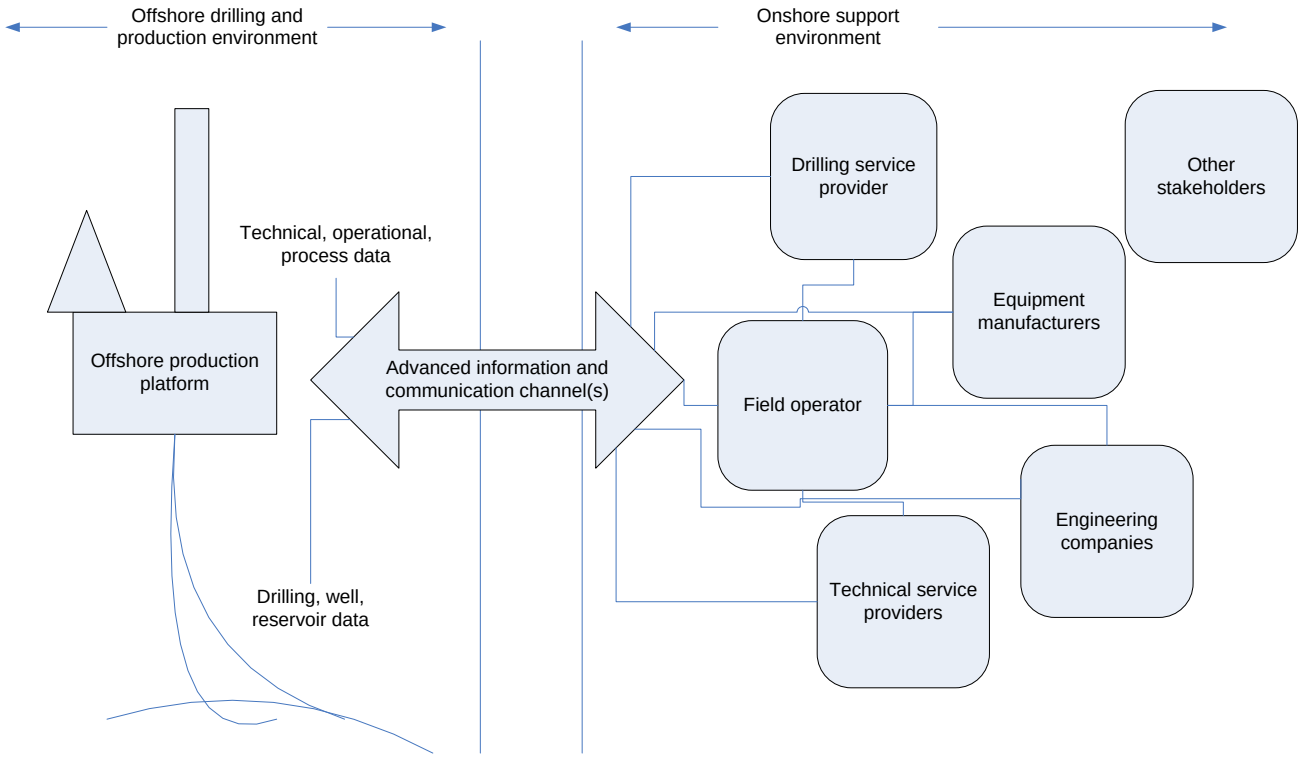

Figure 1. A schematic illustration of the Integrated e-Operations concept.

The ongoing improvements to offshore-onshore connectivity under IO setting are expected to make a significant difference the way in which complex operations are managed. Some of the key features of IO include;

i. Gradual transition to 24/7, online, real-time operating environment
ii. Advanced data management solutions involving novel data transfer and analysis tools
iii. Decision support systems for instance involving 3D simulation and interpretation solutions
iv. Onshore support centers equipped with video links, online communication tools, and real-time offshore data retrieval channels
v. Enhanced connectivity between field operators and contractual business partners who shares common data for collaborative decision making
vi. Advanced information and communication structure to enable real-time online connection between offshore and onshore
vii. Etc.

Obviously, data management and decision support environment play critical roles on the success of the new environment. This calls for secure and reliable technical solutions and infrastructures that can handle large chunk of data traffic connected to different sources in a 'live' operating network. However, due to inherent complexity of operations as well as for sensitivity and security issues the development in this context can be seeing taking place in different stages, namely:

i. Intra-organizational interfaces, where different sources of data and decision making settings are integrated within an organization.
ii. Inter-organizational interfaces, where different

organizations who are involved in performing various tasks in an offshore facility are connected together, for instance drilling service providers and engineering companies involved in modification projects.

iii. Inter-regional interfaces, where geographical barriers are broken to connect 'live' to other regions to enhance round-the-clock operations and collaborative decision making capabilities.

In this setting, it is perhaps the information and communication technologies that continue to provide the most critical technical foundation to achieve the true impact of e-Operations. Under the present circumstances, a large fiber-optic network and other forms of web-based applications are being used to establish the connectivity between offshore and onshore. There appears to be a greater potential on the use of advanced wireless solutions, for instance as discussed by Raza & Liyanage (2010), and many application service providers are in the process of exploring and testing suitable solutions for offshore applications. Despite various such wireless solutions are at disposal, their technical and functional capabilities are obviously defining many applications in complex and high risk environments (Emmanouilidis, Liyanage, et.al. 2009).

In this particular setting, certain disciplines such as asset maintenance, is subjected to major discussions owing to their impact on the risk exposure of the facility. The unexpected equipment downtime and mal-functioning safety critical equipment in principal can question both the overall technical integrity as well as safety integrity of the platform raising major risk concerns. When the production platforms are prepared for a 24/7 run mode, they also require major solutions to improve existing surveillance and control techniques for the asset. Recently, there has been an increasing demand for testing and implementing intelligent techniques to make maintenance smarter to ensure system's health (Raza, 2009). Wireless sensor networks in this regard are seen as potentially appealing that can be integrated actively as an integral part of maintenance data management and decision settings. The principal objective of this paper is to review a set of selected wireless solutions that are considered as potential candidates towards offshore applications.

The paper is organized as follows. In Section 2, we describe the offshore-onshore challenges and the technical circumstances. In Section 3, we propose few wireless technologies to use in offshore-onshore environments and Section 4 describes the challenges in wireless communication. Section 5 analyses signal propagation and then Section 6 show experimental results of link quality and received signal strength for different onshore environment. In Section 7 we explain future research and Section 8 concludes the paper.

2 THE OFFSHORE-ONSHORE CHALLENGE AND THE TECHNICAL SCENARIO

As the Integrated e-Operation setting demands smarter and cost-effective application solutions, the traditional practices relating to physical equipment maintenance are seen greatly challenged today. In this context, condition surveillance, machine-to-machine communication, smart sensors and data transfer techniques, etc. have gathered the attention of many, seeking some form of 'machine intelligence' (Raza & Liyanage, 2009). Such an intelligent environment is to be based on three principal components, namely;

i. Smart sensors that continuously or periodically monitor the condition of a given item automatically, and transfer signals to receiving units on the health of the item

ii. Data processing and analysis solutions that compile complex data within designated units, process and analyse them for feature / pattern recognition

iii. Advanced data transfer and communication channels that connect a given set of data sources to a given set of user groups / decision makers located remotely.

As discussed by Liyanage & Bjerkebæk (2007), integrated solutions involving all such features are still under development and full-proof solutions are far from real-time implementation.

In terms of physical equipment maintenance tasks, sensor networks embedded within the physical equipment configuration of a facility allowing real-time 24/7 signal transfer between an identified set of units has major contributions on the technical and safety integrity assurance processes. What in principal required, is a setting where the sensors attached to production or safety critical equipment actively communicate to a set of receiving units centrally located within the offshore production environment.

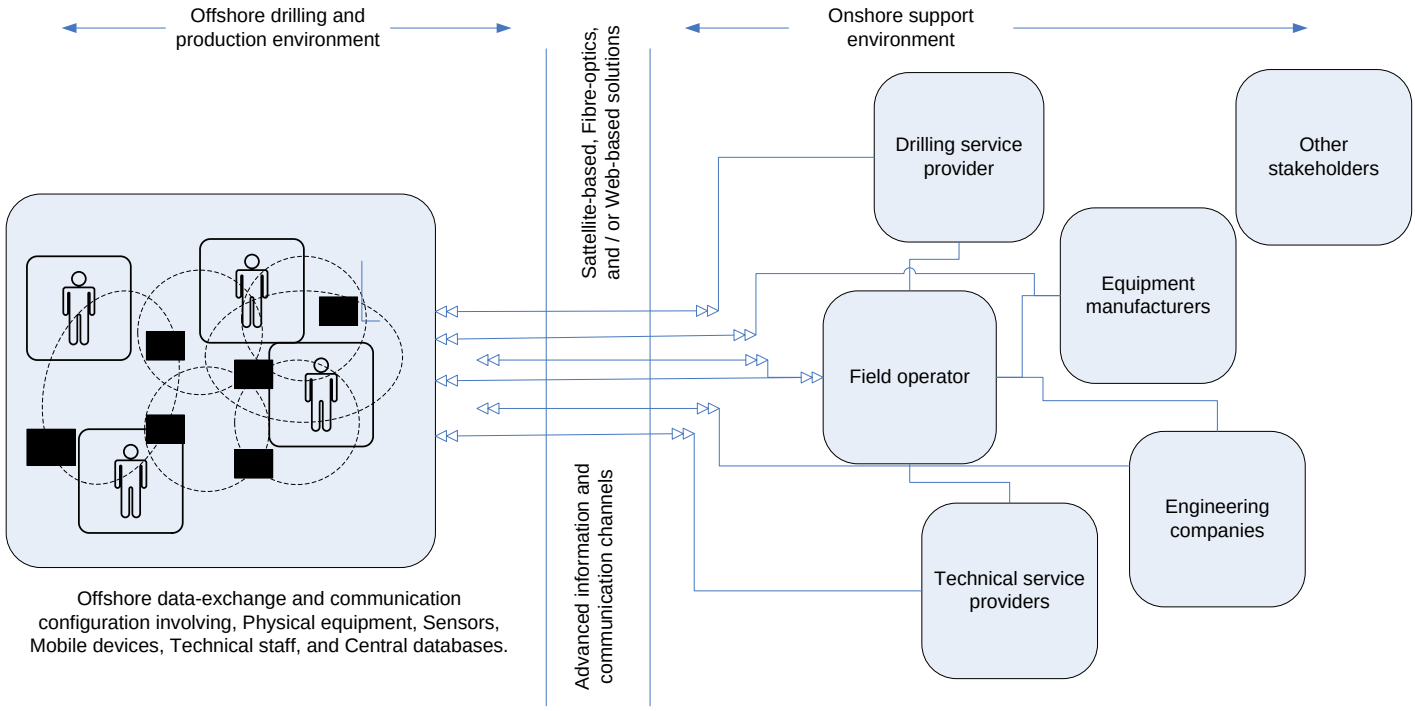

Figure 2. The Information and communication scenario for physical equipment maintenance based on networking solutions.

Such receiving units can include for instance, PDAs, Smart phones, or other data retrieval gadgets, used by the technical staff located within the facility who bear responsibilities on equipment availability assurance, as well as data retrieval units attached to offshore control centers. An ideal situation is where in a given local area the sensors communicate actively with;

i. other sensors based a pre-defined logic that facilitates feature mapping and troubleshooting based on if-then logical reasoning
ii. hand-held devices used by the technical and operational crews where a given set of signals can continuously be received and monitored without having to physically access the equipment
iii. central data retrieval units, which then stores the chunk of data and readily transfer them to other remote distances such as onshore control centers located 100s of kms from offshore facility, as well as mobile experts located for instance in other geographically distant sites.

This involves a various levels of networking solutions ranging from more localized sensor networks to large communication networks such as satellite-based, fiber-optics, or web-based solutions (Figure 2) Next sections discuss about possible wireless technoligies and the application potential.

3 POSSIBLE WIRELESS TECHNOLOGIES

Radio frequency spectrum is an costly and limited resource. Nonetheless, the unlicensed bands, Industrial, Scientific, and Medical (ISM) are becoming more congested therefore the coexistence problem of heterogeneous systems is facing. This ISM band is available for medical uses; however, they are shared with other users. ISM band is an unregulated band that was approved by the FCC in 1985. Generally, wireless local area networks (WLAN) devises are powered up with main current and wireless personal area network (WPAN) devices with batteries. There are different ways to minimize power consumption in battery-powered devices. The transmission distance or coverage area in a wireless system is the estimated percentage of area or distance within a cell that has received power than a required minimum. This varies widely based on radio frequency used and the physical surroundings. WLAN can be either infrastructure mode or ad-hoc mode (Glodsmith, 2005). If infrastructure mode, then assume a fixed access point (AP). AP provides wireless LAN devices to connect into a wired network or bridge between the wireless and wired network. An ad-hoc wireless network is a group of wireless mobile nodes that self configure to create a network without any infrastructure and then allow devices to communicate dynamically with oth-

er peer devices. The main advantage of ad-hoc mode is quick deployment. IEEE 802.15 uses ad-hoc mode.

Unmanned Aerial Vehicle (UAV) communication system is a small fuelled unmanned aircraft that flies without a human crew on board the aircraft. Transmission distance of UAVs is, generally, 100 m to 10 km with 62−744 kbps data rates. Altitude of small UAV is 300m. The repeater-UAV can sends a real-time video feed to the central control place (Mahmood, 2007). UAVs and the ground station are based on the radio systems in the UHF band and low earth orbiting (LEO) satellite links. Small UAV radio network are typically used for civil purposes like forest fire surveillance, police surveillance, environmental studies (collecting air samples) and farmers etc. This technology can help cut labour expenses within some industries such as beef industry. In lots of countries, like India, Pakistan, and the USA, their homeland security departments already have plans to deploy UAVs to watch coastal areas and protect major oil and gas pipelines.

Directed data transmission or signal travelling in a straight line is called line-of-sight or LOS, otherwise, non-line-of-sight (NLOS). Today's wireless local area networks (WLAN) are based on IEEE 802.11a/b/g standards. Several proposed wireless technologies that can be used for offshore application are described here, mainly, radio frequency identification (RFID), ZigBee, IEEE 802.11g, Bluetooth and sensor network. All wireless technologies have different capabilities in terms of transmission range, data throughput, power usage, operating frequency and security. For ease of comparison information about each standard is put into the Table I. We calculate signal attenuation (as in Table 01) for proposed wireless technologies for constant atmospheric CO_2 and relative humidity levels.

ZigBee: Transmission distance of the ZigBee or IEEE 802.15.4 low-rate, low-power and low-cost wireless personal area network (LR-WPAN) is higher than Bluetooth (10-75 m). Networking topologies of ZigBee can be ad-hoc, peer-t-peer, star or mesh. ZigBee provides for the connectivity of simple fixed and mobile devices that require only low data rates between 20 and 250 Kbps. ZigBee devices are designed to remain inactive for long periods of time, hence, consumes a minimum amount of power. Due to mesh networking capability ZigBee provides greater transmission range and height reliability. Intended applications for ZigBee-compliant devices are lighting controls, automatic meter readers (gas, water, and electricity), wireless smoke detectors, home security sensors, environmental sensors, equipment for medical monitoring, universal remote control to a set-top box, including home control and industrial and building automation controls for remote machine monitoring. ZigBee devices are designed to remain quiescent (inactive) for long periods of time. ZigBee transmissions are designed to be short in range and some ZigBee devices have the ability to route packets to other devices. ZigBee devices are engineered to automatically associate with and join the network. ZigBee uses Binary phase shift keying (BPSK) and offset quadrature phase shift keying (O-QPSK) modulation technique (Olenawa, 2007).

IEEE 802.11g: IEEE 802.11g is enhancement of for IEEE 802.11b networks and was published in June 2003. Data transfer rate for IEEE 802.11g is 54 Mbps as IEEE 802.11a, however, it operates in the same frequency band (unlicensed ISM band) as IEEE 802.11b as2.4 GHz. Number of channels available with IEEE 802.11g is three.

RFID: Radio frequency identification (RFID) is the technology similar to barcode labels and stores information in electronic tags. RFID uses radio frequency waves instead of laser light to read the product code. RFID stores more info than barcode. Data held in read-write or read-only memory. These data can be date, time, and location where the product was manufactured, the manufactured name, product serial number, etc. Advantage of RFID with single worldwide standards is possibility of RFID to be implemented and utilized in a global context. Can be programmed in a tag and attached to any physical product. Readers (also called interrogators) that work with passive tags also provide the energy that activates the tags (Olenawa, 2007). A reader or interrogator communicates with both the tags and the corporate network. Read distance is determined by the size and location of the tag and the reader antennas as well as the amount of power transmitted. Tags are initially programmed with a unique identification code obtained from EPCglobal. Because of the unique number or code associated with each item it can be identified electronically. RFID tags Includes an integrated circuit that contains some non-volatile memory and a simple microprocessor. RFID tags can be read not considering of their position or orientation. This technology can be used for animal tracking, asset management, and access cards for security-controlled doors.

Bluetooth: This is the technology that designed for very short-range (up to 100 m) transmission to eliminate cables between devices and follow ad-hoc mode. This communicates using small low power radio modules built in-to tiny microprocessor chips. Data can be sent through physical barriers like walls. Bluetooth uses Two-level Gaussian frequency shift keying (2-GFSK) modulation technique and 2.4 GHz Industrial, Scientific, and Medical (ISM) radio frequency band (Olenawa, 2007). Bluetooth uses the same frequency band as IEEE 802.11b WLANs and therefore interference. Bluetooth version 1.2 adds a feature called Adaptive Frequency Hopping (AFH) that improves compatibility issues with IEEE 802.11b. Piconets are created by Bluetooth devices forming a master and up to seven active slaves, hence, this is suitable for small scale requirements.

Table 1: Proposed wireless technologies

Wireless Technology	Sensor	RFID	ZigBee (802.15.4)	IEEE 802.11g	Bluetooth (802.15.1)
Network Type			WPAN	WPAN	WPAN
Frequency	2.4 GHz – 2.483 GHz (ISM band)	860-930 MHz (ISM band)	868 MHz,915 MHz, 2.4 GHz (ISM band)	2.4 GHz (ISM band)	2.4 GHz (ISM band)
Signal Attenuation (dB/m)	16.11	16.91-16.89	16.91, 16.89	16.11	16.11
Modulation	DSSS	-	BPSK, O-QPSK	DSSS-OFDM, BPSK	FSK, 2-GFSK, FHSS
No of channel	16	-	27	3	79
Data rate	62.5 Kbs	140 kbps (up-link) 70 kbps (down-link)	20, 40, 250 kbps	54 Mbps	1-3 Mbps
Coverage	<10 m >100m with directional antenna	100 m	10-75 m	38 m (indoor) 140 m (out door)	1-100 m
Medium Access	-	-	CSMA/CA	CSMA/CA	TDMA
Bandwidth	13 MHz		5 MHz	20 MHz	1 MHz
Advantages	Simple, easy to deploy	world-wide standard for product identification	increased reliability, NLOS, low power, low cost	hardware is fully backward compatible with 802.11b	wider availability
Disadvantages	limited distance, battery	short range, low security, low data rate	low speed, low security	Interference from other products operating in the 2.4 GHz range, low reception	limited distance, low speed
Applications	Sensing temperature, humidity level, CO2, motion etc.	product tracking, inventory/assets management, industrial automation	home automation, industrial plant		hands-free headset (cable replacement)

Sensor: A sensor network is a spatially distributed device using sensors to monitor conditions at different locations, such as temperature, sound, vibration, pressure, motion or pollutants. Usually these devices are small and inexpensive, so that they can be produced and deployed in large numbers, and so their resources in terms of energy, memory, computational speed and bandwidth are severely constrained.

Various research problems of sensor networks such as data aggregation or fusion (Boulis, 2003), packet size optimization (Sankarasubramaniam, 2003), cluster formation (Halgamuge, 2003 & 2005), target localization (Zou, 2003), battery management (Halgamuge, 2003), network protocols (Heinzelman, 2002; Intanagonwiwat, 2000) are discussed in the literature with respect to crucial energy limitations and network lifetime maximization (Halgamuge, 2009). The efficient design of a wireless sensor network with a large number of nodes can potentially monitor a section of forested land to provide high resolution environmental data such as temperate, humidity, rainfall, solar radiation, gas concentration (oxygen, carbon dioxide and air pollutants), water quality (dissolved oxygen, salinity, pH and water pollutants) will provide the basis for developing data for environmental modelling and calibrating models for fire risks. The sensor system consists of three major components: sensor nodes, transceivers, and a central unit. Sensor nodes are connected to the power grid (at outlets or fuse boxes) to measure power consumption and for their own power supply. Sensor nodes directly transmit sensor readings to transceivers. The transceivers form a multi-hop network and forward messages to the central unit. The central unit acts as a gateway to the Internet and forwards sensor data to a database system.

4 WIRELESS COMMUNICATION CHALLENGES

4.1 Wireless Network Deployment Issues

Advantages of wireless networking are better access, greater physical mobility, easier and less expensive installation, high reliability, disaster recovery and disadvantages are radio signal interference, security and health risks. Deployment and operation issues, bandwidth, delays and packet losses are the inherent problems to wireless networks. Problem of the ad-hoc mode is that wireless client can only communicate between themselves and no access to wired network. Lack of infrastructure is the inherent problem in ad-hoc wireless network. Some of the other wireless communication challenges are competition among other standards, industry support for other communication technologies, and cost of wireless components, protocol functionality limitations and spectrum conflict. WLAN applications are found in a wide variety of industries and organizations. Bluetooth and WLAN 802.11b/g operates in same radio frequency (2.4 GHz), therefore interference. WLAN devices use same frequency band but with low power transmitters, hence, short useful range with minimum interference.

The growing demand of enterprise-wide asset tracking and management has become a challenge for existing technologies. RFID technologies have been dominating this market for a long time and have been quite successful in supply-chain management. However, RFID technology does not many applications, because of its range limitations. RFID is suitable for pure identification applications where readers are located close to goods at reader points. Ultra-high frequency RFID tags promise longer identification range, however with an extremely high cost of readers. One of the main challenges of RFID systems is the issues of implementation: The system can direct the readers to question all of the RFID tags every five minutes or so. Therefore, this scanning adds lot of traffic to the network. The huge volume of data that can be generated by RFID systems significantly increases the need to store information accurately and reliably. The need to remotely monitor and administer RFID readers from a central location happens to a critical factor: add to this the task of managing and tracking millions of RFID tags.

Compared to Bluetooth, Zigbee is superior in several ways. Efficient power usage, better security mechanisms, operating frequency range, simple implementation and wide variety of network topologies are plus points over Bluetooth. Bluetooth beats Zigbee only when it comes to data throughput. In years to come there will be numerous revisions for both standards and if somehow Zigbee improves its data throughput. Bluetooth is primarily used to provide wireless connectivity between devices such as mobile phones, laptops, headsets, PDAs, printer adaptors, Keyboard and mice. On the other hand Zigbee got a wide variety of applications such as home control and automation, sensor networks, building automation, Industrial control and monitoring, toys and games. Due to its power efficiency and security features Zigbee enable devices are very popular in medical industry.

4.2 Sensing and Data Integration Issues

In offshore production platform sensors can be utilized to sense ambient climatic conditions such as temperature, carbon dioxide level and relative humidity except to monitor 24/7 operations. High-speed fiber-optic network is currently used to establish the connectivity between offshore and onshore. Hence, this can be used to make all sensed data available anywhere anytime. However, integration of these data is another challenging problem. Nevertheless, the amount of sensor data is considerably increased when combined with other information. Particularly, images and other sensor data over the network should integrate and transmit to monitoring site for analysis purpose. Peer-to-peer data transfer over sensor networks, complicated sensor scheduling and data processing is possibly a feasible for various sensing solutions.

Alternative approaches to communications, such as peer-to-peer data transfer over sensor networks, sophisticated sensor scheduling, event triggered sensing and data processing, may determine the viability of many sensing solutions. Smarter sensing can conserve power; smarter data sharing can reduce network load. Energy issues (battery resources) and bandwidth are critically important for 24/7 operation networks over periods of time. Local computation and data fusion as opposed to transmission in a central location to reduce power consumption would be one solution to this. At the moment, a number of sensing problems basically have no practical solution. However, sensor localization is one solution to the attenuation of wireless signal strength. An integrated database of comprehensive different data streamed from a very large number of varied sensors will still be a great challenge. At last, it is known that robust smart sensors are not available at a price that makes their use cost-effective.

4.3 Security Concern in Wireless Network

Broadcasting network traffic over the airwaves has created an entirely new set of issues for keeping data transmissions secure. Some of the most dangerous attacks against WLANs are Access Point (AP) impersonation, hardware theft, passive monitoring and Denial of Service (DoS). IEEE 802.11 secures a wireless network using an authentication server, push-button wireless security, virtual private network (VPN), reduce WLAN transmission power, antivirus and antispyware software, change the default security settings on the APs, place firewall between the WLAN and the wired LAN. Use of RFID devices has generated a large number of security and privacy concerns. In the USA, in particular, the concerns are centered on privacy. Another problem is security related to RFID readers falls under the wired network security policy. Thus, communications have the same vulnerabilities as any wireless network. In RFID passive tags do not employ authorization or encryption security methods: they do not have own power supply and have chips with low processing power.

Security should be of little concern with WPANs and much more difficult task than in other networking technologies. Bluetooth provides security at the Link Management Protocol (LMP) layer by using device authentication and limited encryption processes. ZigBee uses symmetric keys for authentication and encryption.

Bluetooth defines three security modes, which can be selected based on the practical application. Security mode 1 is the insecure operation mode, generally used for applications which security is not required. Devices in this mode allow all the other Bluetooth devices to connect to it. Security mode 2, provide authentication, confidentiality and authorization at service level. Finally security mode 3 provides authentication and authorization at link level. Authentication of Bluetooth devices a facilitated by a pre-shared PIN and a challenge response mechanism built into Bluetooth (Karygiannis, Owens, 2002). Link-key (128 bit) is derived from the pre shared PIN and it can vary in length from 1 to 16 bytes.

Zigbee unlike some of the older wireless standards was designed with security kept in mind. Security is a primary objective in Zigbee and implementation is rather simple. Three security levels are specified in Zigbee; none, Asynchronous connectionless (ACL) link and Encryption with Advanced Encryption Standard (AES) symmetric key. Zigbee allows only authentication and encryption. This is one of the major differences compared to Bluetooth, which provide authorization as well. Zigbee authentication can be done at network level or at device level. Network level authentication requires a common network key to be configured on all the participating devices. Unique link keys facilitates device level authentication. Original Zigbee standard does not specify automated key distribution mechanisms and all the keys needs be hard coded. Simplicity of the Zigbee security becomes much clearer while fo

cusing on Zigbee encryption. Zigbee employs 128-bit symmetric key AES encryption at network and device levels. The same key used for authentication is used for encryption, requiring fewer resources and consuming less power.

Considering security mechanisms available for all wireless technologies, it is obvious that none of them are completely secure. However, if an automatic key distribution mechanism can be implemented, ZigBee would be the more secure than Bluetooth. Bluetooth is fairly older standard compared to ZigBee and when it was initially drafted, security was not a major objective. ZigBee on the other hand, was designed with security as one of the prime objectives.

5 WIRELESS SIGNAL PROPAGATION

The most important issue in wireless communication is the amount of information or number of bits per second, which carried over a wireless channel. According to Shannon theory the upper bound of the bit rate of any channel (with bandwidth B Hz) is given by $W = B\ log_2(1+S/N)$, where S/N is the signal to noise ratio. However, in actual system the bit rate is significantly lower than this value because of signal fading.

5.1. Signal Attenuation Due to Path Loss

Indoor settings are different broadly in the materials corridors, windows, and open areas, the location and used for walls and floors, the arrangement of rooms, obstructing objects, and the size of the room and the number of floors (Goldsmith, 2005). Altogether of these factors have a significant impact on path loss in an indoor environment. Thus, it is difficult to find standard models that can be perfectly applied to verify empirical path loss in a specific indoor setting. Indoor path loss models must accurately summarize the effects of attenuation across floors due to partitions, the same as among floors. The experimental data for floor and partition loss can be added to an analytical or empirical dB path. The path loss that attenuate signal is defined as the difference between transmitted and received power. As in (Rappaport, 2002), by ignoring antenna gain path loss, L_p, at the free space path loss between two isotropic antenna is given by $L_p = 20\log_{10}\left(4\pi d / \lambda\right)$, where wavelength $\lambda = c/f$, the speed of light $c = 3\times10^8$ ms^{-1} and f is the frequency of the signal and d is distance between transmission and receiver antenna.

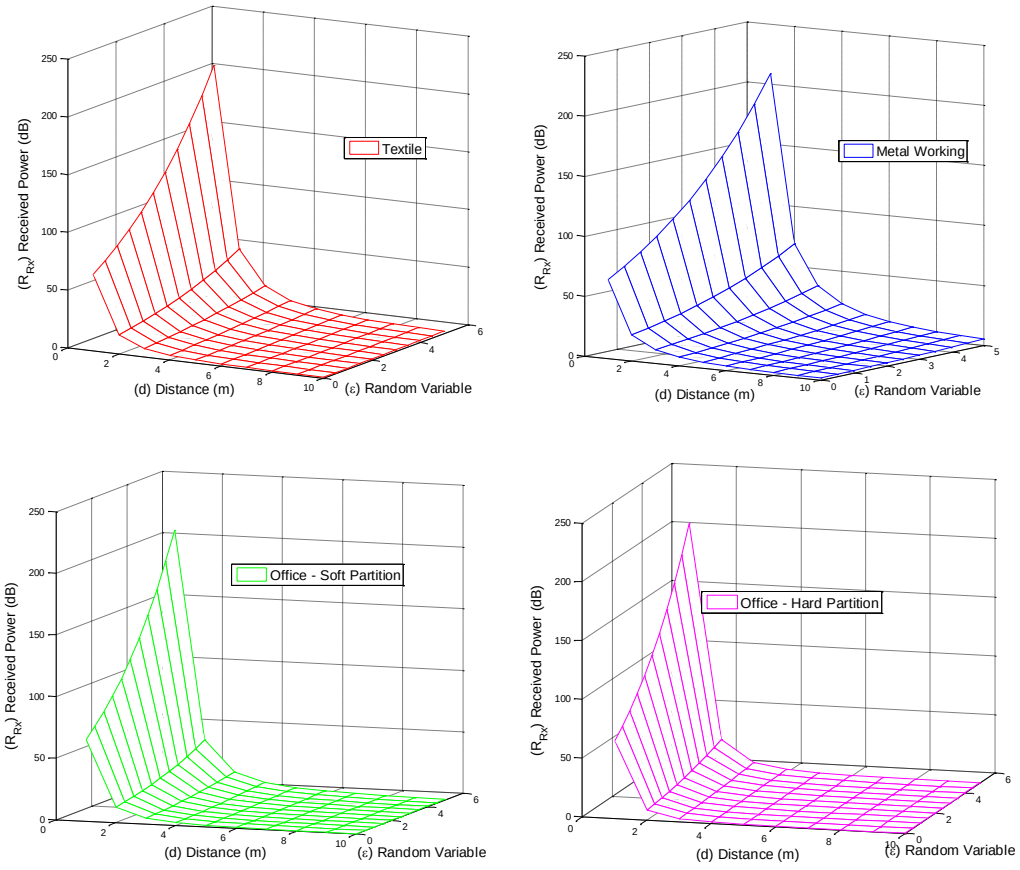

Figure 3: Received power for different factory environment

As in (Rappaport, 2002), Table 2 shows typical path loss exponents acquired in different radio environments. Figure 3 illustrates the affect of distance and random variable to received signal power in different factory environment

5.2 Received Signal Power

The value of path loss exponent, *n*, depends on the specific propagation environment. Higher the value of *n* with more obstruction presents.

Table 2: Typical path loss exponent values for various environments

Environment	(n) Path Loss Exponent (dB)
Textile	2.0
Metal working	1.6
Office – soft partition	2.4
Office – hard partition	3
Factory – obstructed	2 - 3

When user goes behind a large building the wireless signal will be weaken due to electromagnetic shadow. The fading due to huge obstacles that generate electromagnetic shadows is called shadow fading. When user moves away from transmitting antenna this fading change, considerably. The variation due to shadowing effects can be represented by a log-normal distribution of a shadow fading random variable, β. Received signal power, P_{Rx} is given by $P_{Rx} = P_{Tx} d^{n} 10^{\beta/10}$ where P_{Tx} is the transmitted power from the base station or transmission antenna, d is the distance between transmitter and the receiver, *n is* the path loss exponent and β shadow fading random variable.

6 EXPERIMENTAL RESULTS FOR SIGNAL QUALITY ANALYSIS

Given that offshore environments are technically challenging for sensor networks, some experiments were initially planned and implemented in laboratory settings that replicate the offshore setting in order to identify the impact of certain conditions on the signals. These conditions include; i) effect of ambient conditions (e.g. noise, vibration, wind) ii) effect of physical configuration (e.g. obstacles, distance, etc.). An offshore facility located few hundreds of kms into the sea are exposed to various ambient conditions. In certain geographical areas such as North sea, an offshore platform can be exposed to heavy wind and snowy conditions that may have direct influence on performance of sensors and instruments. On the other hand, within those platforms noise and vibrations are quite common phenomena as the construction involves various structural components, heavy operations (e.g. lifting, drilling, etc.), and constitutes a range of rotating equipment. It has been a common experience that certain signals are generated and/or influenced due to such secondary reasons than primary technical causes directly associated with the equipment of concern. On the other hand platforms are tightly built introducing many obstacles for signal propagation as well as retrieval. This can for instance include, structural members, heavy machinery, walls located on the path of the signal, etc. Thus the density of the configuration as well as the distances can have major impact on the success of applying sensor networks and their direct use on the data retrieval and decision making processes.

Replicating an offshore setting in a laboratory environment is not obviously an easy task. However, some simple experiments under certain conditions can help much in understanding if a full-scale test would be worthwhile, and if so, what type of experimental set-up would be necessary. In order to get such an initial idea, few tests were done in controlled laboratory settings as explained below.

6.1 Experimental set-up

IntelMote2 or Imote2 sensors are used for this experiment (imote2). Our sensor network consists of many sensor nodes that can be deployed in any random positions. Each sensor component include: Intel PXA271 processor, 32MB SRAM, SDRAM and flash memory to store sensed data, CC2420 radio board (IEEE 802.15.4-2003) with 2.4GHz Industrial, Scientific & Medical (ISM) frequency band with integrated surface mount antenna, and uses DSSS (Direct Sequence Spread Spectrum) 250 kb/s data rate with 16 channels. The imote2 uses radio transceiver with integrated surface mount antenna that provides nearly 30 m line-of-sight distance. Nevertheless, transmission distance and added reliable communication performance can be drastically improved by utilizing an external antenna.

In general, a sensor node will be asleep during idle mode and wake up for duration of T_A and then sleep for T_S, assuming that $T_S >> T_A$ to save battery power, however except the clocks. In this experiment, processing is not done in the board; instead, transmit all sensed data to the base station or to the hub. The nodes were powered with standard 3XAAA batteries with 3.2-4.5 V battery voltages. Sensors are pre-mounted on the sensor boards. Current draw in deep sleep mode is 390 µA, active mode while radio is off is 31 mA and radio is on while transmitting or receiving mode is 44 mA.

Each received packet is logged with link quality and received signal strength, transmitter and receiver number and the time stamp. Link quality indication measurement classifies strength and the quality of received packet and higher this value is the better. Signal quality is determined by bit error rate (BER) and level of levels of the ratio of signal-plus-noise-plus-distortion to noise-plus-distortion (SINAD) (Polishuk, 1997). Received signal strength indication (RSSI) is obtained from every radio packet read from CC2420 radio.

In our work, we observe channel estimation parameters like Link quality indication (LQI) and Received Signal Strength Indication (RSSI). For each received packet, IEEE 802.15.4 Low Rate Wireless Pan (LR-WPAN) standard sustain measurement of both RSSI and LQI (Ilyas, 2009). As in (Ilyas, 2009) bit error rate of n^{th} packet is given by (number of error bits in n^{th} received packet) / (number of bits in n^{th} received packet) and this is calculate over every received packet. Moreover, this process cannot be directly monitored. Cyclic Redundancy Check (CRC) examine number of bits with errors is non-zero instead information on the number of errors (Olenewa, 2007). Hence, we use BER estimation. Both RSSI and LQI measurements are maintained by IEEE 802.15.4 LR-WPAN standard for each received packet and these are the two Channel State information (CSI) parameters. The transmitter and the receiver was blocked with a wall, partitions and several other items, hence, the link between transmitter and the receiver is not line-of-sight.

6.2 Experimental Results

We observed reasonble signal strength reduction due to humidity effect when pressure level is 1000.2 hPa as shown in Figure 4. Figure 5 illustrates the typical wind affect for received signal strength when humidity level is 85% and pressure level is 1015.2 hPa Here wind level was maintained for 4 km\hr.

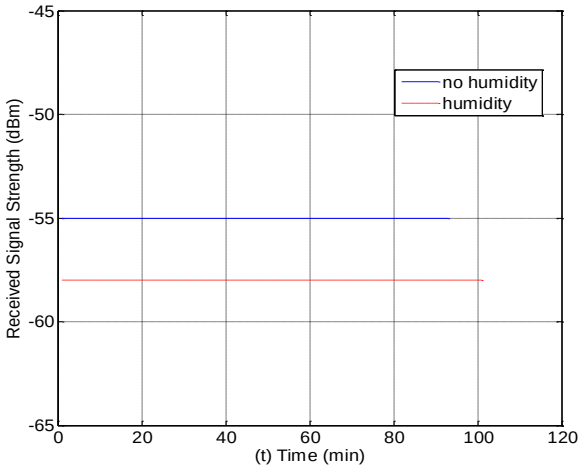

Figure 4: Humidity effect for received signal strength where pressure level is 1000.2 hPa

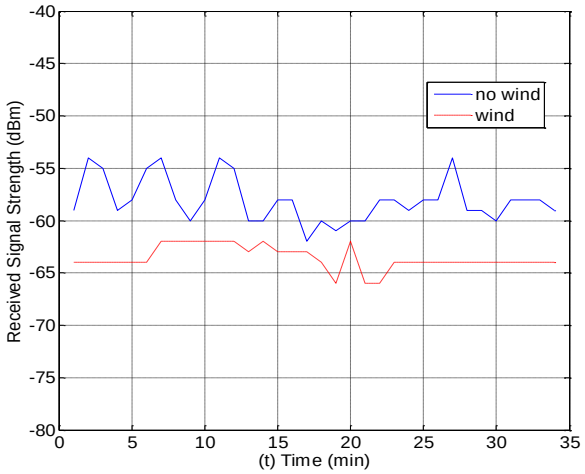

Figure 5: Wind speed effect for received signal strength where humidity level is 85% and pressure level is 1015.2 hPa and Wind level is 4 km\hr.

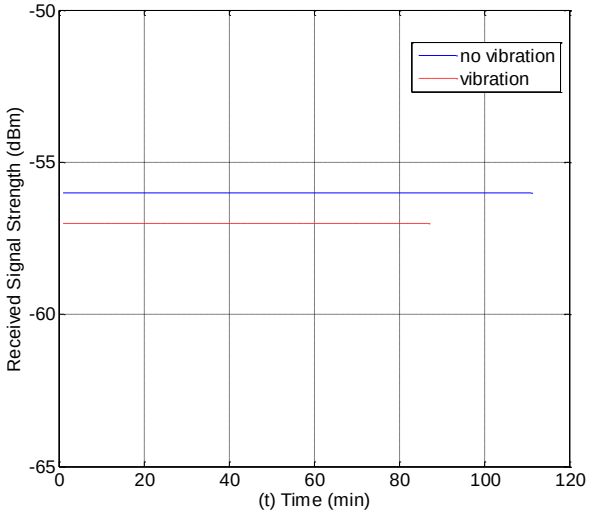

Figure 6: Vibration effect for received signal strength where humidity level is 39% and pressure level is 1000.2 hPa.

Finally, Figure 6 shows vibration effect for received signal strength where humidity level is 39% and pressure level is 1000.2 hPa. Hence, our results show high humidity, vibration and wind affect, considerably, to signal attenuation in onshore environment.

7. FUTURE RESEARCH

Notably the development in offshore asset management environment is conducive for novel and innovative application solutions. However, due to inherent risks associated with offshore production operations, new applications are subjected to greater scrutiny. It is often considered an acceptable practice to adapt systematic approach where the ideas and potential solutions are taken through a step-by-step process. This is to allow the proper basis for further steps based on systematic collection of data, analysis, as well as quality assurance of the solution development process. In more complex cases, the process may have to go through pre-defined decision gates where certain criteria are applied to qualify further work.

The study presented in this paper took the form of a pre-qualification process where known dominating conditions are tested against a technical requirement. Obviously, sensor networks have great application potential in offshore asset management setting. Yet given the conditions under which such technology has to be applied as well as the level of influence, it is necessary to have an awareness on those condition that have direct implications of the design and deployment of effective solutions. Offshore platforms may be exposed to extreme and severe conditions in certain periods of the year, where the technological solutions have to survive and retain its functional integrity. The tests performed in this study in principal identified the impact potential of a set of dominating parameters, and provided the first-level understanding on the effect of the condition both on link quality and signal strength.

Further work has to be designed with the access to real-time data relating to these parameters to reveal if dominating effects can be found, and if so within what ranges. The usable range-values may change from one setting to another, based on various factors ranging from, age of the installation and equipment, structural construction concepts used, configuration and space, to the location. Obviously, it is not possible to replicate the complex offshore setting in a laboratory, nor could get access to a real operating environment to conduct the testing. However, this is feasible coupled with certain approximations based on initial data received from targeted environments.

8 CONCLUSIONS

In this paper possible wireless solutions for offshore applications have been discussed in search of a robust and a combined solution in the light of emerging demands. Some of the technical issues that may hinder application potential with respect to operational conditions in offshore oil & gas production environments have been investigated in controlled laboratory settings.. This is a pilot experiment to observe link quality distribution of onshore like environment. Our results predict high humidity, vibration and wind affect, significantly, to signal attenuation in potential application of such a combined solution for offshore oil and gas production environments. Based on the outcomes, further studies will be planned and conducted in more exposed natural environments that replicate specific operational conditions in offshore production environments.

REFERENCES

Boulis A, Ganeriwal S, Srivastava MB (2003) Aggregation in sensor networks: an energy-accuracy tradeoff, Proc. Int. Sensor Network Protocols and Applications, 128–138.

Emmanouilidis, C., Liyanage, J.P:, Jantunen, E., (2009), Mobile Solutions for Engineering Asset and Maintenance Management, Journal of Quality in Maintenance Engineering, Emerald, vol.15, no. 1, pp 92-105

Goldsmith, A, (2005) Wireless communications, Stanford University, Cambridge University Press, 644 pages.

Halgamuge MN, Guru SM, Jennings A, (2003) Energy efficient cluster formation in wireless sensor networks, Proc. IEEE Int. Telecommunications Conf. French Polynesia, Feb.-Mar, 2:1571–1576.

Halgamuge MN (2005) Centralised strategies for cluster formation in sensor networks, ser. Classification and Clustering for Knowledge Discovery. Springer-Verlag, Aug, pp. 315–334, ISBN: 3-540-26073-0.

Halgamuge MN (2007) Efficient battery management for sensor lifetime, Proc. IEEE AINA Conf., Niagara Falls, Canada, May, 1:56–61.

Halgamuge MN Zukerman M, R. Kotagiri R and Vu H (2009) An Estimation of Sensor Energy Consump-

tion, Progress In Electromagnetics Research B, 12, 259-295.

Heinzelman WR, Chandrakasan A, Balakrishnan H, (2002) An application-specific protocol architecture for wireless microsensor networks, IEEE Tran. on Wireless Comm., 1(4):660–670.

Imote2, [onlie] http://www.xbow.jp/imote2.pdf

Imote2 for Structural Health Monitoring User's Guide, [online] http://shm.cs.uiuc.edu

Intanagonwiwat C, Govindan R, Estrin E (2000) Directed diffusion: A scalable and robust communication paradigm for sensor networks, University of Southern California, Los Angeles, Tech. Rep. 00-732.

Ilyas M. U., Kim M. and X Radha H. (2009) Reducing Packet Losses in Networks of Commodity IEEE 802.15.4 Sensor Motes Using Cooperative Communication and Diversity Combination, IEEE INFOCOM, 1818-1826

Karygiannis, T, Owens, L. (2002). Wireless Network security 802.11, Bluetooth and Handheld Devices, Gathersburg: NIST.Liyanage, J.P., Bjerkebæk, E., (2007), Key Note paper: Use of advanced technologies and information solutions for North sea offshore assets: Ambitious changes and Socio-technical dimensions, Journal of International Technology and Information Management (JITIM), pp 1-10

Liyanage, J.P., Langeland, T., (2008) Smart assets through digital capabilities, Mehdi Khosrow-Pour (ed.), Encyclopaedia of Information Science and Technology, IGI Global, USA., pp 3480-3485.

Liyanage, J.P., (2008) Integrated eOperations-eMaintenance: Applications in North Sea Offshore Assets, Murthy, P., & Kobbacy, K., (ed.), Complex Systems Maintenance, Springer. pp 585-609.

Mahmood, S., (2007). Unmanned Aerial Vehicle (UAV) Communications, *Master Thesis*, Blekinge Institute of Technology, Sweden.

Olenewa, J., Ciampa, M. (2007). Wireless Guide to Wireless Communications. 2nd Edition. Thompsan.

Polishuk P (1997) Fiber optics weekly update, Technology & Engineering.

Rappaport TS (2002) Wireless Communications Principles and Practice, 2nd Edition. Prentice Hall..

Raza J, Liyanage JP (2009) Application of intelligent technique to identify hidden abnormalities in a system: A case study from oil export pumps from an offshore oil production facility, Journal of Quality in Maintenance Engineering 15(2): 221-235.

Raza, J., Liyanage, J.P., (2009), An assessment of gaps and technical risks in sophisticated technology implementation efforts in complex operations: A case from an integrated production monitoring environment, European Safety and Reliability Conference (ESREL), Prague, Czech Republic., Sept., Taylor and Francis Group. Pp.89-96.

Raza, J., Liyanage, J.P., (2010) Managing hidden systems threats for higher production regularity using intelligent technological solutions: A case study, European Journal of Industrial Engineering, vol. 4, no.2, pp 249-263.

Sankarasubramaniam Y, Akyildiz IF, and McLaughlin SW, (2003) Energy efficiency based packet size optimization in wireless sensor networks, Proc. IEEE Int. Sensor Network Protocols and Applications Conf., 1–8.

Zou Y, Chakrabarty K (2003) Target localization based on energy considerations in distributed sensor networks, Proc. IEEE Int. Sensor Network Protocols Conf., May, pp. 51–58.