Marine based Wireless Sensor Networks: Challenges and Requirements

Walid Elgenaidi, Thomas Newe
Optical Fibre Research Centre Department of
Electronic and Computer Engineering University of
Limerick,
Limerick-Ireland

Abstract—**Marine environmental monitoring based on wireless sensor networks (WSN) is a challenging area of research due to the instability of the water field. Due to the characteristics of the water environment, there are certain considerations which must be taken into account before the establishment of marine based wireless sensor networks. These include the deployment of wireless nodes (WNs), energy consumption, network connectivity and security. This paper compares and contrasts the basic parameters relating to WSNs, while highlighting the main components necessary to form an ideal marine based WSN system, and some difficulties of implementing security in Marine WSNs such as the management of the cryptographic keys.**

Keywords: Marine WSNs; Key management; Security; Wireless Communication Standards.

I. INTRODUCTION

Electronics and wireless communication have assisted in the development of marine environmental monitoring. This has increased the growth of low cost, low power and small multi-functional sensors, which communicate in multi- ranges [1]. Sensors transmit the collected data from different forms of natural and human made phenomenon such as sound, light, temperature, salinity and pollution in water areas to a server 'sink/gateway' and subsequently to the end-user. In order to provide a system suitable for use in the marine environment many researches are looking at using wireless networks. In particular ad-hoc network systems with wireless sensor nodes which contain large numbers of inexpensive nodes with sensing flexibilities are being considered. This paper is structured as follows. In section two, the general layout and architectural structure of marine based wireless sensor networks and their challenges are discussed and the necessary equipment is outlined. In the third section, different communication standards suitable for Marine WSNs are outlined and summarized in terms of Transmission Frequency, Data Rates and Network Topology. The fourth section provides details on published marine WSN implementations, which are summarized and compared in terms of technology, network topology, standards and power supply requirements. The fifth section presents the objectives and difficulties of security for this application domain. Finally, conclusions are provided be way of requirements for designing an ideal marine based WSN.

II. MARINE BASED WSNS ARCHITECTURAL STRUCTURE AND CHALLENGES

A. Marine based WSN General Architecture

Figure 1 illustrates the general architecture of wireless sensor networks that apply in marine environmental monitoring. The marine environmental monitoring system generally consists of two major parts: Wireless Underwater Acoustic Networking and Wireless Aerial Networking.

1) *Wireless Underwater Acoustic Networking*: This part consists of underwater sensor nodes and autonomous underwater vehicles, which are deployed to carry out cooperative surveillance in a given area. The typical physical layer technology in underwater networks involves acoustic communication. The architectures of underwater acoustic sensor networks can be categorized depending on the network topology used. Thus, network topology is considered as a crucial factor in terms of the capacity of the network, as well as the energy consumption requirements.

a) Static Underwater Sensor Networks: In this type of network, a group of sensor nodes are anchored to the bottom of the water area with a deep water anchor. In order to send the data to the surface station, wireless acoustic link interconnections are used between underwater sensor nodes and underwater sinks via direct links or through multi-hope pathways.

b) Moving Underwater Sensor Networks: Underwater sensor nodes are attached to a surface buoy or anchor to the bottom of the water area, with flexibility of movement in a specific area.

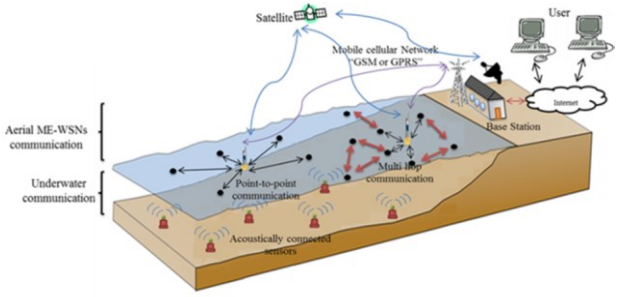

Figure 1. General architecture of WSNs

c) *Underwater Sensor Networks with autonomous underwater vehicles:* Autonomous Underwater Vehicles (AUVs) are used to enhance the capabilities of underwater sensor networks in terms of self-configuration of sensor nodes,(e.g. maintenance of underwater network infrastructure), adaptive sampling, power supply issues and depth capability which can reach up to 1500m. Furthermore, global position satellite (GPS) technology can be used to track the location of the vehicles on or near the surface.

2) *Wireless Aerial Networking*: This consists of a number of wireless sensor nodes deployed on the water surface, communicating with a base station.

a) Wireless Sensor Nodes: In general, wireless sensor nodes are small electronic devices which involve sensors and transmitters to sense and transmit data to aggregation points.

b) Wireless Network Connectivity: Wireless network connectivity in marine environmental monitoring depends on the deployment of Wireless Sensor Nodes. Indeed wireless communications between nodes on the water surface rely on network topologies and network characteristics such as Tree, Star or Mesh topology. In addition, to cover large areas and distances between nodes and base stations, suitable approaches for long range communication may be used including GSM/GPRS, Wi-Fi and WiMAX [2].

Sensor nodes are interconnected by point-to-point and multi-hop communication networks. Wireless sensor network infrastructure requires standards and protocols (zigbee, IEEE 802.15.4 etc) which take into account the battery life of the node, node cost in addition to the operating environment.

B. *Difficulties and Challenges in WSNs in the marine environment*

In the marine environment, there are a number of issues which are challenging and need to be addressed including:

1) Movement: The sea water creates environmental conditions which negatively influence the network parameters, such as breaking up the buoy nodes and sometimes the WSN may need reconfiguring.

2) Management of energy consumption: In general, batteries are the power supply utilized in marine WSNs. This means that energy management of sensor nodes is one of the significant issues that marine WSNs rely on. In order to save energy, wireless communication mechanisms have been applied which aim to minimize radio activity.

3) Software Design of the Network: In general, WSNs are heavily based on the Network Embedded System. The operating system is considered to be the core of wireless communication networks. The program code manages the connectivity and data delivery between the nodes, base station and the end-users.

4) Data Transmission and Security: communication between marine WSN components is suffering from a number of issues such as environmental conditions and network design. For instance, the water environment decreases the radio signal strength of the data transmission and can result in an unstable line-of-signal between wireless nodes[12]. Additionally, to ensure the confidentiality and integrity of the gathered data, security protocols and techniques must be applied.

TABLE I. *COMMUNICATION STANDARDS AND SYSTEMS*

STANDARD		TRANSMISSION FREQUENCY	DATA RATE	NETWORK CONNECTIVITY	OTHER FEATURES
IEEE802.15.4		868 MHZ	20 Kbps	Star/Mesh Peer-to-Peer	Link quality indication, which is useful for Multihop mesh networking. The transmission distance could reach to 100 meters or less. A device in this standard network can use 64-bit IEEE address or a 16-bit short address, and can accommodate up to 216 devices.
		902-928 MHz	40Kbps		
		2.48–2.5 GHz	250Kbps		
ZigBee		2.4 GHz	250Kbps	Star/Mesh Peer-to-Peer/Tree	In a Star ZigBee network every device in the network can communicate only with the coordinator In a Mesh ZigBee network the end device does not participate in the message routing. In Mesh and Tree topologies each device can communicate directly with any other device.
IEEE802.15.1 "Bluetooth"	Class 1	2.4 GHz	1 Mbps	Star (up to 7 nodes)	The distance range covered by Bluetooth classes: Class 1 covers 100m, class 2 covers <20m, and class 3 covers 1m.
	Class 2		3 Mbps		
	Class 3		50-480 Mbps		
IEEE802.16		2GHz-11GHz For fixed	1-75Mbps	Point-to-point mobile cellular	Provide broadband services 50Km for fixed stations and 5 to 15Km for mobile stations.
		2GHz-6GHz For mobile			
IEEE802.11	a	5GHz	54Mbps	Based on a cellular structure WLAN/WiFi	Covering approx 120m
	b	2.4GHz	11Mbps		Covering approx 140m
	g	2.4GHz	54Mbps		Using OFDM modulation covering 140m
	n	2.4GHz	248Mbps		Provide data rate up to 600Mbps using MIMO radio technology, covering 250m
GSM		For Europe: 900/1800 MHz For USA: 900 MHz	9.6 Kbps	Point-to-point mobile cellular	Provide broadband services 50Km for fixed stations and 5 to 15Km for mobile stations.
GPRS		2.5 GHz	56-144 Kbps		

III. COMMUNICATION STANDARDS IN MARINE BASED WSNS

Regarding the MWSNs issues and challenges that were described in the previous section, standards and network topology have been summarised depending on the amount of the transmitted data and the distances that they cover. These are shown in Table I.

IV. COMPARISON AND STUDY OF MARINE BASED WSN IMPLEMENTATIONS

Table II provides a comparison of various marine WSN implementation studies. These implementations are summarized in terms of technology, network topology, standards and power supply requirements.

V. SECURITY IN MARINE BASED WSNS

Security is considered as a central issue in WSNs, providing confidentiality, authentication, and the integrity of sensor data transmission. In order to achieve secure data transmission between nodes, complex cryptographic algorithms are required. However, the capabilities and constraints of marine based WSNs dictate the security services that are needed and the mechanisms that can be used. In particular, with communication between a large number of sensor nodes, power consumption, capability of key storage and computation of new security keys [21] must be considered.

A. Objectives and Difficulties of Security in Marine WSNs

In this section, the objectives and difficulties of implementing security in a Marine based WSNs is discussed. In general terms the services provided by the CIA triad, shown in figure 2 are needed to secure sensitive sensor data. These services include; confidentiality, authentication, integrity of data and node/data availability. The WSN world in particular offers many obstructions/difficulties in providing these services. These difficulties are discussed below.

1) Confidentiality: Sensor nodes may be attacked in order to reveal the sensor data. Encrypted information with a secret key will maintain data confidentiality. This data should only be exposed to permissible users, who can decrypt the data with the correct key.

2) *Authentication*: Data transmission between nodes must be trusted. As such the receiver must ensure that any data received is authenticated. This can be provided using resource friendly tools such as hardware implemented hashing algorithms.

3*) Integrity:* The same hashing algorithms that can be

TABLE II. *COMPARISON OF PUBLISHED MARINE WSN IMPLEMENTATION STUDIES*

NO	Project	Organization and Country	Topology and Standards used	Type of used chips and Power Supply	Year	Ref
1	Water Environment Monitoring System Based on ZigBee Wireless Sensor Network	University of science and Technology of China, Institute of Advanced Manufacturing ,China and Hefei Institute of Physical Science ,China	Star topology ZigBee "CC2530" GPRS "SI300"	Battery Box / USB power supply	2013	4
2	Water pollution Monitoring ystem based on ZigBee Wireless Sensor Network	JiangXi University of Science and Technology China	IEEE802.15.4/ZigBee GPRS "SIM100"	JN5139 CMOS (jennic) Battery	2011	7
3	Fresh Water Real-Time Monitoring Based on wireless Sensor Network and GSM	University Sains Malaysia Malaysia	Point-to-point and point-to-Multipoint IEEE802.15.4 GSM	XBEEE 805.12.4, RF module and M24068 GSM module Green power source harvesting the solar day light	2011	8
4	Wireless Sensor Network in Coastal Marine Environments: Study Coast Outcome	Centre for Marine Studies University of Queensland Australia	Sensor nodes have been arranged in a line on total length of roughly 100m, and one hub "star". Adaptive TDMA radio modem 2.4GHz ISM (RS232)	Solar energy	2009	10
5	Smart Environmental Measurement & Analysis Technology (SEMAT): Wireless Sensor Network in Marine Environment	Centre of Marine Studies ,University of Queensland _ Australia Dipantimento di Elettrotecnica, Politecnico di Milano_Italy	Gateway acts as hub on the sea surface, and gathering data which is sent from underwater acoustic network. Acoustic network for underwater and RF radio for water surface network	Solar/cable	2008	9
6	Development of Data Video Base Station in Water Environment Monitoring Oriented Wireless Sensor Networks	Institute of Information and Control, Hangzhou Dianzi University China	Mesh topology IEEE802.15.4/ZigBee between data monitoring nodes and data video station (C2420). The communication between data video station and remote monitoring centre based on CDMA network (DTG-800) module.	Not mentioned	2008	11

Figure 2. CIA Triad Security Services

used to provide source authentication are used to provide data integrity. Hardware implementations of these algorithms can limit their draw on system resources such as power and memory.

4) *Availability:* Nodes in the network may suffer from Denial-of-Service (DoS) attacks. Network systems can protect the availability of nodes be enabling them to be self-organising and through the use of suitable re-keying algorithms. This re-keying will enable the network to be self-healing while keeping security of data at the fore.

B. Key Management in Marine WSNs

To ensure the security of any application in WSNs, key management mechanisms are a most critical operation. These include generating, distributing and revoking cryptographic keys. In Marine WSNs, there are two kinds of keying schemes generally used: Network-wide and node-specific pre-deployed keying. The former supplies the same system wide master key to each sensor node for the entire network, whereas the latter equips each neighbouring node with a unique key to allow communication pairing between neighbour nodes to take place. This section describes some issues related to key management in marine WSNs.

1) *Key pre-distribution:* Keys are generated and then installed in the memory of each sensor node, which creates a key ring. Furthermore, the key ring identifiers of each sensor node and its associated key ring are kept in a controller node in the network. This phase must be completed before deploying the sensor nodes [14].

2) Discovery of the common shared-key: In this step, nodes broadcast their identifier key ring in order to discover a pairwise key. At this point in the operation, the topology of the network is established by the communication links between the nodes that share a common key [12].

3) Establishment of path-key: In some cases if the node does not discover a shared-key with other nodes, and they are connected by a multi-hop path, then it is possible for a path key to be established between the nodes. This key is known as an end-to-end path key.

4) *Revocation of stray sensor nodes:* During the operation of marine WSNs, some nodes may not function as expected due to reasons such as a compromised sensor nodes, or power becoming exhausted. As a result of this these nodes must be isolated. Revoking the entire key ring of these nodes from the network will remove particular communication links in the network. Revocation messages consist of a set of key identifiers of revoked nodes which are broadcast by controller nodes [13].

5) Re-keying: This phase occurs after isolating deviant nodes. The re-keying step must take place in sensor nodes in order to generate and replace the expired key rings after employing the revocation algorithm.

VI. Discussion

From this review, it can be stated that the design of an ideal marine WSNs which can be subjected to many kinds of node/data attacks is dependent on many factors, such as; environmental and water conditions, energy constrained operation requirements, suitable network communication and software design/topologies and finally security.

A Marine WSN architecture can be classified into two classes based on the required coverage area: small coverage area and wide coverage area. Personal area networks (PAN) connect sensor nodes in a wireless communication range up to 10m in the 2.4GHz ISM band. For instance, IEEE 802.15.4 or Bluetooth can be used to connect several wireless sensors inside a circle with a radius of ten meters, with low power consumption and a data rate up to 480 Mbps [15][16]. Wireless Local Area Networks (WLAN) with a communication range of 250 meters in some cases up to 600Mbps [17]. On the other hand, point to point mobile cellular networks used in Marine WSNs offer ranges up to 50km such as with IEEE802.15.1 or GPS/GRPS.

Secondly, a particularly important factor in the deployment of Marine WSNs is how to overcome security attacks with dynamically changing network topology. These attacks can consist of node impersonation, denial of service and data disclosure attacks. Hence, applying different kinds of security mechanisms and management techniques is particularly important in order to prevent and detect attacking attempts and to ensure integrity, confidentiality and authentication of transmitted data.

To facilitate this, key management and encryption schemes are at the core of security communication requirements. Dynamic key management schemes are finding considerable use in Marine WSNs, where they are capable of adding new nodes and ejecting compromised nodes.

In some approaches, to ensure the security of the network, sensor nodes share a single symmetric key, known as a network wide master key, which is used to facilitate re-keying of a network with session keys used for encrypting and decrypting messages. These session keys can be updated and re-distributed when the sensor nodes change, drop out of the network or are attacked (re-keying) [19].

Another approach is Neighbourhood Key Management. In this approach, each sensor node only keeps and shares a symmetric key with its closest nodes (neighbours). The sender encrypts the message key with the neighbourhood key

and attaches the encrypted key (like a single session key) to the message, after that only the message key needs to be decrypted. Thus, in order to forward the message, the node must re-encrypt the message key. When the node needs to send data to another node for the first time, the received node demands a certificate from the sender which identifies it as a legitimate node. Once the receiver ensures the authentication of the sender by exchanging certificates, the secret keys can be exchanging to use for encrypting and signing messages [20].

All of the methods discussed here are experimental and have yet to be deployed on a large scale Marine based ad-hoc network. The focus of future work in this area will be the testing and evaluation of these schemes in a real world test scenario with particular emphasis on security and the problem of key management/distribution.

VII. CONCLUSSION

The studies discussed here show some important issues for Marine WSNs including general architecture and network communication techniques employed. From this paper, it is fair to conclude that the design of wireless sensor networks for marine applications depends upon various factors. These factors include; gathering and transmitting data (choosing communication standards with suitable data rate and power consumption), network shape and topology (relying on size of area to monitor and its security requirements) and the lifetime of deployment required (time between maintenance of sensor nodes and energy conservation methods employed).

REFERENCES

[1] Fauzi, M, and Shazali. K, "Wireless Sensor Network Applications : A Study in Environment Monitoring System," Elsevier Ltd. doi. vol. 41,pp. 1204–1210, 2012.

[2] Albaladejo. C, Sánchez. P, Iborra. A, Soto. F, López. J, and Torres. R. "Wireless Sensor Networks for oceanographic monitoring: a systematic review", Sensors. Basel, Switzerland, vol. 10, pp. 6948–68, 2010.

[3] Tjensvold. J, "Comparison of the IEEE 802.11, 802.15.1, 802.15.4 and 802.15.6 wireless standards," pp. 1-7, September 2007.

[4] Wu. L, Province. A, Kong. L, Zhang. Z, Technology. M, and Province, J. (n.d.)." Water Environment Monitoring System Based On ZigBee Wireless Sensor Network,", IEEE. China ,pp. 898–901, June 2013.

[5] J. Zheng, and M. Lee, "A Comprehensive Performance Study of IEEE 802.15.4,"New York USA, pp 1–14.

[6] D. Dharmistha, and Vishwakarma, " IEEE 802.15.4 and ZigBee: A Conceptual Study," IJARCCE, vol. 1, pp. 477–480 ,September 2012.

[7] S. Zhang, and L. Zhang, "Water pollution monitoring system based on Zigbee wireless sensor network," ICECC, pp. 1775–1779, 2011.

[8] M. Nasirudin, A. Za'bah, U. Nurulhaiza, and O. Sidek, "Fresh water real-time monitoring system based on Wireless Sensor Network and GSM, "IEEE Conference on Open Systems, Langkawi, Malaysia, pp. 354–357, November 2011.

[9] R. Johnstone, D. Caputo , U. Cella, A. Gandelli, C.Alippi, F. Grimaccia, R. ZichE. "Smart Environmental Measurement & Analysis Technologies (SEMAT): Wireless sensor networks in the marine environment," Australia, 2008 "unpublished".

[10] U. Cella, P. Shuley, and P. Johnstone, " Wireless Sensor Networks in Coastal Marine Environments : a Study Case Outcome," WUWNet Berkeley, CA, USA , November 2009.

[11] K.Yifan, and J. Peng, "Development of Data Video Base Station in Water Environment Monitoring Oriented Wireless Sensor Networks," (ICESS2008), Symposia, pp. 281–286, February 2008.

[12] B. Arazi, I. Elhanamy, O. Arazi, and H. Qi." Revisiting public –key cryptography for wireless sensor neworks, Computer," ISSN 0018-9162 pp. 103-105, 2005.

[13] D. Djenouri, L. Kallida, and A. N. Badache," A survey of security issues in mobile ad hoc and sensor networks" IEEE communications Survey and Tutorials, vol 7, pp. 2-28, 2005.

[14] F. Hu, N. K. Shaarma," Security considerations in ad hoc sensor networks," Elsevier, vol. 3, pp. 69-89, 2005.

[15] B. Lichun, J. Garcia-Luna-Aceves, "Transmission scheduling in ad hoc networks with directional antennas, in: Proceedings of the Eighth ACM International Con- ference on Mobile Computing and Networking", MOBI- COM 2002, Atlanta, GA, pp. 23–28, September, 2002.

[16] I. Chlamtac, M. Conti, J. Jennifer. N. Liu, " Mobile ad hoc networking: imperatives and challenges" Elsevier, vol. 1, pp. 13-64, 2005.

[17] W. Stallings," Local & Metropolitan Area Networks," Prentice Hall, Englewood Cliffs, NJ, 1996.

[18] J. Liebeherr, G. Dong, " An overlay approach to data security in ad-hoc networks," Elsevier, vol. 5, pp. 1055-1077, 2007.

[19] L. Xiao,"Prioritized overlay multicast in mobile ad hoc environments," IEEE Computer, vol. 2 ,pp. 37 67–74 February 2004.

[20] N. Wang, S. Fang, "A hierarchical key management scheme for secure group communications in mobile ad hoc networks," Elsevier, vol. 80, pp. 1667-1677, 2007.

[21] A. Menezes, P. van Oorschot, S. Vanstone, "Handbook of Applied Cryptography," CRC Press, Boca Raton, FL, 1997.