International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011

Wireless Sensor Network Nodes: Security and Deployment in the Niger-Delta Oil and Gas Sector

Iwendi, C. O. Allen, A. R.

Communication & Optical Engineering Research Group, University of Aberdeen, Scotland, UK (ciwendi@abdn.ac.uk, a.allen@abdn.ac.uk)

Abstract

Wireless sensor networks (WSN) is tending towards becoming a complete solution in communication protocols, embedded systems and low-power implementations. However, the resource constraints which includes, limited communication range, limited energy, limited computing power, limited bandwidth and the fear of intruders have limited the WSN applications. Since lightweight computational nodes that are currently being used in WSN pose particular challenge for many security applications, the whole research therefore, is the investigation of new security techniques and appropriate implementation for WSN nodes, including various trade-offs such as implementation complexity, power dissipation, security flexibility and scalability. The goal of this research is to develop a network that has efficient and flexible key distribution scheme secured enough to prevent algorithmic complexity and denial of service attacks as well as the network able to conserve energy. A review of previous research to date in the area of security for WSNs was carried out and proposals are made based on security schemes that gather data in an energy-efficient mechanism through secured pre-allocation of keys, faster clustering routing algorithm and dynamic based rekeying implementation.

Keywords

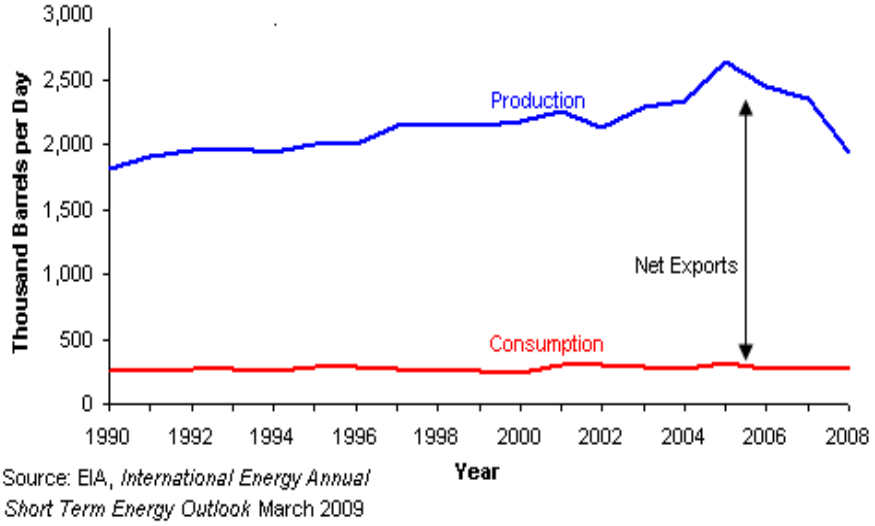
Blom, Judy Array, Clustering Routing, Niger-Delta

1. Overview

Improvements in the latest electronic technology has brought about the idea of deploying small, low power, low-cost sensor devices in the Oil and Gas Industries. Wireless sensor network (WSN) is one of the world's most emerging technologies that comprise a good range of practical applications like environmental monitoring, smart spaces, medical systems, robotic exploration, military surveillance etc. The fact that many countries depends on Oil and Gas as resources for welfare, development and social stability is a thing of interest to this proposal. Like in Nigeria, the hydrocarbon resources are the stronghold of the country's economy but production and growth of the oil and natural gas sectors are often constrained by insecurity in the Niger Delta. The Nigerian economy is heavily dependent on the oil sector which, according to the World Bank accounts for over 95 percent of export earnings and about 85 percent of government revenues. The industry has been blamed for pollution that has damaged air, soil and water leading to losses in arable land and decreasing fish stocks. Local groups seeking a share of the oil wealth often attack the oil infrastructure and staff, forcing companies to declare force majeure on oil shipments. At the same time, oil theft, commonly referred to as "bunkering" leads to pipeline damage that is often severe, causing loss of production, pollution, and forcing companies to shut-in production [1]. Figure 1.0 shows the Nigeria oil production from 1990- 2008 [2].

DOI : 10.5121/ijnsa.2011.3105

Fig. 1.0 **Nigeria's Oil Production and Consumption, 1990-2008**



Source: EIA, *International Energy Annual*
Short Term Energy Outlook March 2009

This research goes a long way in addressing safety-critical Microsystems and robust smart miniature systems for transport applications [3], detection of abnormal vibrations offshore in the oil and gas industry [4] as well as advanced sensor and actuator based systems for safety and security. The detail of the research involves wireless sensor nodes deployment with security key management scheme attached, secured routine with minimal energy using the clusterhead formation and rekeying mechanism using Judy array key system. It could also apply to many other applications in communication system [5, 6, and 7].

WSN nodes consist of a large number of distributed miniscule devices that arrange themselves into a multi-hop wireless network. These devices or nodes are equipped with one or more sensors, embedded processors and a wireless transceiver [8]. These nodes are deployed into a specific area to perform a desired task of collecting and processing data. There is considerable research activity in WSNs, in such areas as node architecture, energy efficient data gathering and routing, security and trust, and software infrastructure. It is important that sensor networks implement robust protocols, and that individual nodes can support concurrent processes without deadlock or other problems. This is particularly the case where the sensors are in relatively inaccessible places, must work reliably for months or even years. Therefore, to achieve energy efficiency is also very important because of sensor nodes' remote location [9]. Figure 2.0 illustrate the idea of security in wireless sensor network node in mind.

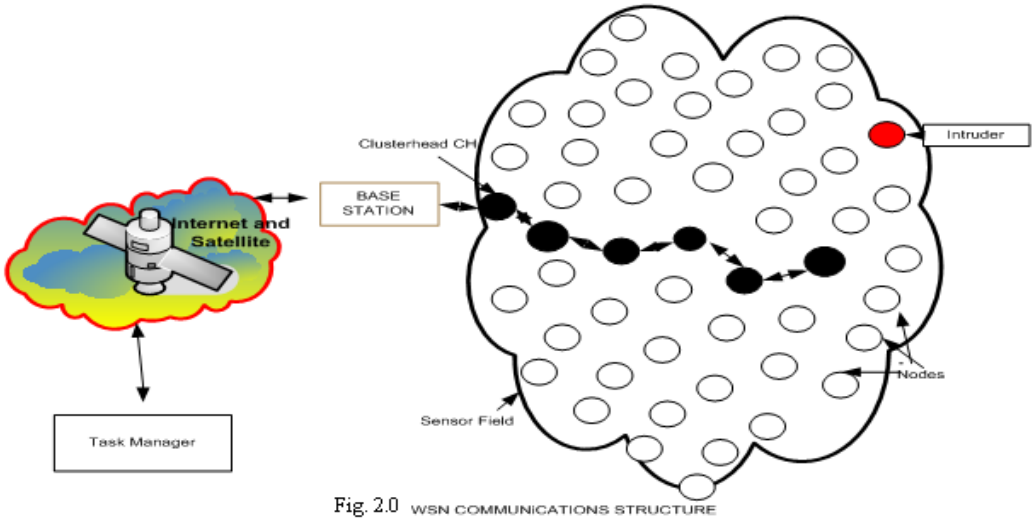
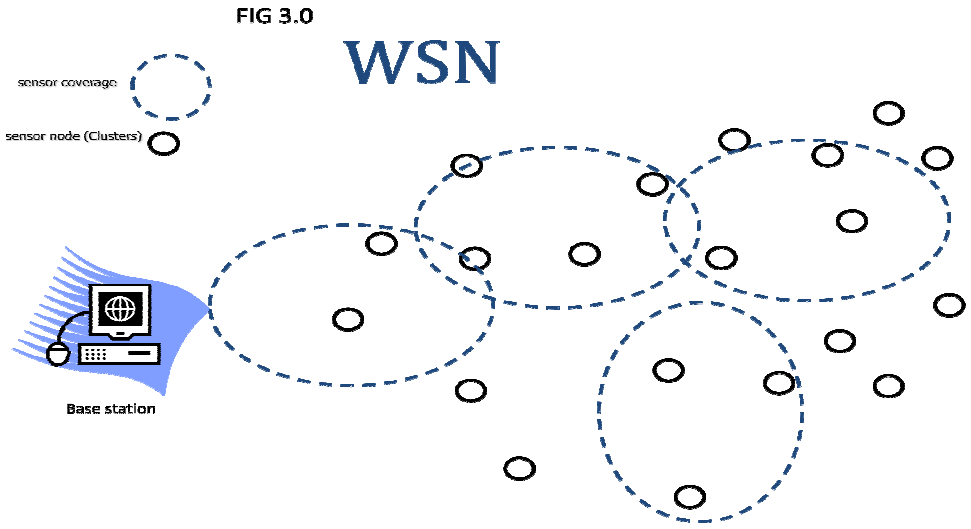


Fig. 2.0 WSN COMMUNICATIONS STRUCTURE

Security in wireless sensor network encompasses the characteristics of authentication, integrity, privacy, non-repudiation, and anti-play back [10]. The greater the dependency of information sent or received in the network, the greater the security risk. Various security issues that have been considered in ad hoc networks ([11], [12]) are not applicable to WSN because of the architectural disparity of the two networks [13]. Also, quite a number of other security schemes are already being proposed [14]. In the cluster formation design currently being investigated to be effective in saving energy, there is need to look at the security between the individual nodes, neighbouring nodes and the base station. There are numerous constraints affecting the performance of a wireless sensor network. These restraints includes, low memory and low energy resources. Attacks on network availability also arise when considering that wireless sensor networks (WSN) are more vulnerable to denial-of-service (DOS) attacks and algorithmic complexity attack as shown in Fig. 3.0. Majority of current security applications proposed is not viable due to low memory to run complicated algorithm after running the Operating System (OS) and other applications. Since all security services are ensured by cryptography, security in WSN corresponds to a large amount of energy consumption for cryptographic functions [13].



2. Review of Relevant Literature

The need to provide an effective security mechanism as wireless sensor network application grows is the motivating factor for this research. A good number of studies are ongoing on the best possible way to achieve the desired methods in adding security to a resource constrained wireless sensor network. Many WSN deployments are security sensitive and attacks against them may lead to damage to health and safety of people. Denial of service are conditions for hardware failures, resource exhaustion, bugs, malicious attacks and environmental conditions that could reduce the functionality or totally eliminating a networks ability to perform as expected [15]. Also, the best possible way to achieve effectiveness in the area of Denial-of-service attacks and countermeasures, techniques for WSN nodes deployment, key management protocols, energy reduction, formal verification method, and performance evaluation and security enhancement has been studied.

3. Group Objectives

The research in wireless sensor networks (WSN) has been intensified during the last few years. Security issues have become a central point of concern for achieving secured communication in the network. Safeguarding data authentication in a hostile environment, where the sensor nodes may be compromised has become an essential security issue particularly in the Oil and Gas Industries where the sensor nodes maybe deployed. In a compromised network, detecting a real event by an intruder can disrupt, destabilize or destroy the data. The end product of such attack can lead to exhaustion of network energy and bandwidth resources, triggering false alarms and undesired reactions to the nodes in the network.

We intend to develop a network that has efficient and flexible key distribution schemes secured enough to prevent algorithmic complexity attacks and denial-of-service attack as well as the system capable of saving energy. The platform should also exhibit high authentication, full authorization, maximum confidentiality, freshness and secrecy of message received or been transmitted.

4. Justification of the Research

Several industry like oil and gas, automobile, textile etc are approaching towards the benefit of WSN, the current market projected for Wireless Sensor Networks is due to reach US$1.75 Billion by 2019 [16]. Some industry consortiums have emerged to develop WSN innovations for pipeline corrosion monitoring, wellhole drilling and completion, seismic sensors, and nanotechnologies in oil and gas industry [17]. Environmental monitoring and pipeline destruction is also significant reasons to apply security to the wireless sensor nodes deployed in the field. Oil spill incidents and the vandalization of the pipelines create multiple problems. The run-off and sedimentation of this pollutant in fresh water systems severely degrade water quality; affect fish spawning and aquatic invertebrates' habitats, thus lowering food web productivity. Incidentally the spill-over effect on humans who directly depend on fish and other aquatic food as an alternative protein supplement is quite inundating. The effects on humans include irritation, dermatitis, cancer, occurrence of abortion, organ failure and genetic disorder [18]. On the other hand, with the increased interest in security applications such as under water surveillance, dealing with the connectivity, coverage and detection of intruders in 3-Dimensional detection (3D) using wireless sensor network has totally become a necessity [19].

5. Relevance of the Research to the Niger-Delta Oil and Gas Sector

In general, the relevance of the research will include a contribution to the government research effort, towards pipeline destruction, underwater surveillance, environmental monitoring, and opportunity to collaborate with foreign researchers in the latest area of technology. Similarly, the research can be utilized by indigenous oil and gas companies towards better exploitation of petroleum resources and detection of crude oil and leakages in the rural communities. Acquired skills can similarly be applied in the development and training of young Nigerians on the use of advanced 3D visualization machines used in detection of wormhole attacks and other geological uses. More importantly, there will be an overall contribution to world research community of developing new security method that is not currently exploited in wireless sensor network nodes. The value of the research is that oil spill and pipeline vandalization if not secured devastate the environment, pollute dependable potable water sources such as streams and rivers and should be seen as a serious threat and negation to the attainment of the United Nations Millennium development goals [20].

6. Methodology

In this regard, the vulnerability of the broadcast session key (BROSK) [21] and self key establishment (SKEW)[22, 23] protocols is taken into consideration in formulating the new security technique as well as using formal method to argue about the correctness of these protocols that were virtually simulated. Moreover, the research is also centre on solving one of the biggest attacks in secure routing and using a 3D visualization technique with sets of wireless sensors deployed in the field to detect the anomalies by wormhole attack usually witnessed in the Oil and Gas Industries.

6.1 Preliminary Simulation Results

This section describes the preliminary simulation results to date. The idea and concern in this stage was to adequately identify an appropriate scheme to use. The scheme should also readily provide a data source that can fit into the different levels of the entire project. The source is needed to reproduce both a normal and malicious network activity for later analysis and classification.

6.1.1 Key Generation using Blom's Scheme

The basic part of the first proposal was implemented here, not the whole scheme but in a way that the key exchange protocol makes use of a very trusted sensor ID pre-allocated in each sensor.

Protocol set up

An MDS-code matrix is chosen in a random scenario over a finite field $\mathrm{GF}(\mathrm{p})$, where p is a prime number. This is a trusted master key as pointed out in the assumption. Considering scalability as trade off, let n represent the number of nodes. Let $\mathrm{CH}(\mathrm{A})$ and $\mathrm{CH}(\mathrm{C})$ be two nodes in the network. Sensor ID is required when new nodes or CH is to be added to the key sharing group.

Let P = 17

Let's assume the following values

Symmetric matrix ID_{xxx} implies the following conditions.

a = a = 1
b = d = 6
c = g = 2
f = h = 8
e = e = 3
i = i = 2

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \equiv \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & i \end{bmatrix}$$

$$\therefore ID_{xxx} = \begin{bmatrix} 1 & 6 & 2 \\ 6 & 3 & 8 \\ 2 & 8 & 2 \end{bmatrix} \equiv \begin{bmatrix} 1 & 6 & 2 \\ 6 & 3 & 8 \\ 2 & 8 & 2 \end{bmatrix} \mathrm{mod}\, 17$$

To allow a new CH to join the network, a k-element vectors on nodes $\mathrm{CH}(\mathrm{A})$ and $\mathrm{CH}(C)$ is form for public identifiers represented as $\mathrm{ICH}(A)$ and $\mathrm{ICH}(C)$

The private key will now become

$$\mathrm{g}(\mathrm{CH}(\mathrm{A})) = \mathrm{ID}_{\mathrm{A}} * \mathrm{ICH}(A)$$

$$g(CH(C)) = ID_C * ICH(C)$$

It is expected that each CH will use these private keys generated to compute shared keys with other CH in the network.

For example

$$\text{Let } CH(A) = \begin{bmatrix} 3 \\ 10 \\ 11 \end{bmatrix}$$

And

$$ICH(C) = \begin{bmatrix} 1 \\ 3 \\ 15 \end{bmatrix}$$

The secret keys will thus be generated by the trusted party as follows:

$$g(CH(A)) = \begin{bmatrix} 1 & 6 & 2 \\ 6 & 3 & 8 \\ 2 & 8 & 2 \end{bmatrix} * \begin{bmatrix} 3 \\ 10 \\ 11 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 6 \end{bmatrix} \bmod 17$$

$$g(CH(C)) = \begin{bmatrix} 1 & 6 & 2 \\ 6 & 3 & 8 \\ 2 & 8 & 2 \end{bmatrix} * \begin{bmatrix} 1 \\ 3 \\ 15 \end{bmatrix} = \begin{bmatrix} 15 \\ 16 \\ 5 \end{bmatrix} \bmod 17$$

Therefore a shared pairwise key between the two CHs will become:

$CH(A)$ will computes shared key to become

$$K_{CH(A)/CH(C)} = gCH(A)^t * ICH(C)$$

Where t denotes transpose

Also,CH(C) will compute its own pairwise key as

$$K_{CH(C)/CH(A)} = gCH(C)^t * ICH(A)$$

Substituting for the given values

$$K_{CH(A)/CH(C)} = \begin{bmatrix} 0 \\ 0 \\ 6 \end{bmatrix}^t * \begin{bmatrix} 1 \\ 3 \\ 15 \end{bmatrix} = 0x1 + 0x3 + 6x15 = 5 \bmod 17$$

$$K_{AC} = \begin{bmatrix} 15 \\ 16 \\ 5 \end{bmatrix}^t * \begin{bmatrix} 3 \\ 10 \\ 11 \end{bmatrix} = 15x3 + 16x10 + 5x11 = 5 \bmod 17$$

The Blom's method therefore proves that

$$K_{CH(A)/CH(C)} = K_{CH(C)/CH(A)}$$

Therefore, k-keys must be compromised before every shared key can be computed by an intruder. More work on this area is meant to be done using the MDS- CODE matrix in the area of increasing the speed the key use in the formation.

6.1.2 Clustering Routing Algorithm

The second phase in ensuring the routing is shorter in transmission as to reduce the energy consumption and also the risk of attack from an intruder through the CH routing. Since the BS was located the origin (0, 0), the simulator program deploys the nodes randomly, since each node has a unique ID assigned to it which also depend on the node at x-axis. The nodes according to the proposal will communicate with each other using the average neighbour distance. The traditional multi hop routing scheme where each CH tends to relay the data received to its nearest neighbours has been compared as shown in Figure 4.0. The proposed routine saves a lot of space, speed, energy and reduces the risk of a security attacked from an intruder. Since the route are not static.

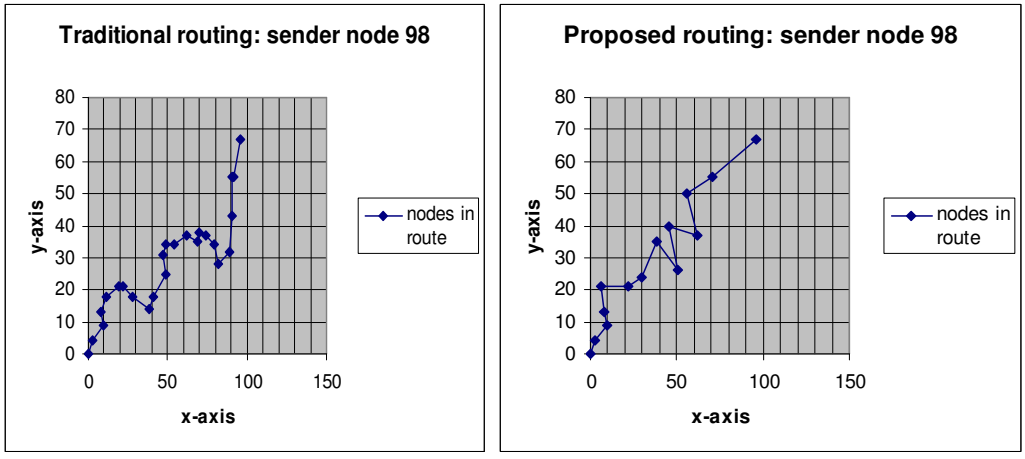


Figure 4.0 Traditional and Proposed Node 98 sending data to Base Station

Sender node ID: 98.

Route (Traditional routing scheme): 98-->93-->92-->91-->90-->86-->85-->81-->76-->74-->66-->59-->54-->51-->55-->45-->43-->32-->23-->19-->15-->11-->13-->3-->BS

Route

(Proposed): 98-->78-->62-->66-->49-->57-->42-->35-->23-->7-->11-->13-->3-->BS

Making the routing to be dynamic will change a lot in this cluster formation. We intend to deploy mobile nodes in the coming months and witness the different scenario.

6.1.3 Judy Array based Re-keying

Node A wants to communicate to Node C which is the cluster head, it can do so independently even if one of the node or cluster is compromise and the network will still remain intact. Consider the following symbols:

- A, B, C represents communicating nodes
- ID_A, ID_B, ID_C represents sensor Identifier for nodes, A, B and C
- N_A, N_B, N_C denotes nounce generated (Unpredictable bit string generated)
- J_A, J_B, J_C Judy Array generated
- K_{AB}, K_{AC} K_{ABC} denotes secret pairwise key shared between A and B, A and C, and A, B and C.
- M_K indicates the encryption of message M with key K
- MAC (K, M) represents the computation of the message authentication code of message M with key K.
- A → B denotes A unicast A message to B
- A → * indicates A broadcasts a message to its neighbours

$A \rightarrow *: ID_A \backslash J_A$, MAC (K, $ID_A \backslash J_A$)

$C \rightarrow *: ID_C \backslash J_C$, MAC (K, $ID_C \backslash J_C$)

K_{AC} = MAC (K, J_A/J_C)

It implies that node A and the cluster head C will receive the broadcast message. They can also verify the message that was sent using the master key, and both of them can as well calculate the shared session key.

7. Conclusion

The research of an effective Wireless Sensor Networks node security idea is increasing [10]. Without a clear perspective of the risk involved in WSN and options available to manage the risks by intruders, it is unfeasible to have a defensible network. Therefore, developing a security protocol can be quite challenging, and requires a wide range of skills manipulation as will be demonstrated in this research. The protocols and routings must be well-suited, flexible, energy reduced compliant, operationally appropriate and should be practicable in real sensor world. The successful implementation of security protocols demands serious attention compared to the neglects wireless sensor network nodes have had in the past in terms of deployment. It is therefore noted that irrespective of the resource constraints in WSN, it is still possible to have a WSN security scheme that maintain energy efficient data gathering, total protection using 3D visualization technique to act in detecting the anomalies in the network and the future application of a WSN mobile nodes deployable in any environment including the Oil and Gas Industries where pipeline vandalism has become the other of the day. These schemes if properly managed and implemented can bring total significant change to the scope of WSN and increase its usefulness in this industry.

References

[1] Nigeria Energy Data: EIA International Annual, Short Term Energy Outlook, EIA. May 2009. http://www.eia.doe.gov/cabs/Nigeria/Oil.html

[2] Nigeria Energy Data: EIA International Annual, Short Term Energy Outlook, EIA. March 2009. http://www.eia.doe.gov/emeu/steo/pub/

[3] J. Tavares, F. J. Velez., and J. M. Ferro, "Application of Wireless Sensor Networks to the Automobile" Measurement Science Review, Volume 8, Section 3, No. 3, 2008.

[4] Y. U. Yan and O. U. Jinping "Wireless sensing experiments for structural vibration monitoring of offshore platform. Journal: Frontiers of Electrical and Electronic Engineering in China. Publisher: Higher education press, co-Published with Springer-Verlag GmbH. ISSN 1673-3460. Issue Volume 3 Number 3, September 2008. Pages 333-337

[5] V. A. Petrushin, G. Wei, O. Shakil, D. Roqueiro, V. Gershman, " Multiple-sensor indoor surveillance system," in, Proceedings of the 3rd Canadian Conference on Computer and Robot Vision (CRV '06), Quebec city, June 2006.

[6] D. R. Raymond and S. F. Midkiff, "Denial-of-Service in wireless sensor networks: Attacks and Defences," IEEE Pervasive Computing Magazine. Volume 7, Issue 1, Jan. – March 2008. Page(s):74 – 81.

[7] A. D. Wood and J. A. Stankovic, "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, 2002, pp. 54 – 62.

[8] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and Cayirci E., "A Survey on Sensor Networks" IEEE Communication Magazine, Aug. 2002.

[9] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," Proceedings of the 33rd Annual Hawaii International Conference on Systems Sciences Jan 4-7, 2000 Page(s): 10pp. vol 2

[10] J. Undercoffer, S. Avancha, A. Joshi, and J. Pinkston, "Security for sensor networks", CADIP Research Symposium, 2002.

[11] L. Zhou and Z. J. Haas, "Securing ad hoc networks", IEEE Network, Volume 13, Issue6, Nov. – Dec. 1999, pp. 24 – 30.

[12] B. Strulo, J. Farr, and A Smith, "Securing mobile ad hoc networks – A motivational approach", BT Technology Journal Volume 21 Issue 3, 2003, pp. 81 -89

[13] A. S. K. Pathan; Hyung-Woo Lee; Choong Seon Hong; "Security in wireless sensor networks: Issues and challenges" The 8th International Conference on Advanced Communication Technology, ICACT 2006. Volume 2, 20-22 Feb. 2006. Page(s):6 pp.

[14] X. Du and H. Chen, "Security in Wireless Sensor Networks" IEEE Wireless Communications. Aug. 2008.

[15] S. Kaplantzis, "Security models for wireless sensor networks". PhD Conversion Report March 2006

[16] Energy Harvesting & Storage and RTLS & WSN conference summary. Energy Harvesting Journal , November 2009

[17] Mareca Hatler, Darryl Gurganious, and Charlie Chi."Wireless Sensor Networks for Oil & Gas**".** May 2008 ON World Inc**.** San Diego, California

[18] K.N. Aroh, I. U. Ubong, C. L. Eze, I. M. Harry, J. C. Umo-Otong, A. E. Gobo "Oil spill incidents and pipeline vandalization in Nigeria: Impact on public health and negation to attainment of Millennium development goal" Disaster Prevention and Management Journal, 2010 Volume 19 Issue 1 Page 70-87 ISSN 0965-3562

[19] V. Ravelomanana, "Extremal properties of three-dimensional sensor networks with applications," IEEE Transactions on Mobile Computing Volume 3, Issue 3, July-Aug 2004 Page(s) 246 – 257

[20] United Nations "The Millennium Development Goals Report New York, 2009

[21] B. Lai, S. Kim, and I. Verbauwhede, "Scalable Session Key Construction Protocols for Wireless Sensor Networks," IEEE Workshop. Large Scale Real Time and Embedded Systems, 2002

[22] M. Sharifi, S. P. Ardakani, S. S. Kashi, "SKEW: An efficient self key establishment protocol for wireless sensor networks," International Symposium on Collaborative Technologies and Systems (CTS'09). 18- 22 May 2009 Page(s):250 – 257.

[23] F. Hu, J. Ziobro, J. Tillett, N. K. Sharma, "Secure wireless sensor networks: Problems and Solutions," Journal of Systemics, Cybernetics and Informatics vol. 1 number 4

Authors

Celestine Iwendi obtained a BSc and MSc in Electronics and Computer Engineering from Nnamdi Azikiwe University Nigeria, MSc Communication Hardware and Microsystems from Uppsala University Sweden and is currently a PhD student at the University of Aberdeen, Scotland. He has carried out many Independent and supervised designs that apply knowledge of Signal processing and Communications engineering to analyze and solve problems at Nnamdi Azikiwe University, Awka Nigeria, and Nigerian Telecommunication, Uppsala University Sweden, Norwegian University of Science and Technology, and University of Aberdeen, Scotland

Dr Alastair Allen graduated BSc, DPhil in physics, and has lectured in physics and information technology. He has a wide knowledge of a range of computational techniques and interdisciplinary applications. He is an expert in embedded instrumentation (including Wireless Sensor Networks), distributed computing, and image processing. His research has been supported by research council, European and industrial funding. For example, his group was involved in a recent EC FP6 project, working on aspects of Wireless Sensor Networking. His research group is currently working on the development of wireless sensor applications for physiological, industrial, and environmental monitoring.
He is currently a senior lecturer at the University of Aberdeen, Scotland.