WIRELESS SENSOR NETWORK IN NIGER DELTA OIL AND GAS FIELD MONITORING: THE SECURITY CHALLENGES AND COUNTERMEASURES

Fidelis C. Obodoeze[1], Hyacinth C. Inyiama (PhD)[2] and V.E. Idigo (PhD)[3]

[1] Doctoral Research student, Department of Electronic and Computer Engineering, Nnamdi Azikiwe University, P.M.B 5025, Awka, Nigeria
All correspondence to fidelisobodoeze@gmail.com
[2] Professor, Department of Electronic and Computer Engineering, Nnamdi Azikiwe University, P.M.B 5025, Awka, Nigeria
drhcinyiama@gmail.com
[3] Associate Professor and Head, Department of Electronic and Computer Engineering, Nnamdi Azikiwe University, P.M.B 5025, Awka, Nigeria
vicugoo@yahoo.com

ABSTRACT

The IEEE 802.15.4 specification has enabled low-power, low-cost and smart wireless sensor networks (WSNs) capable of robust and reliable multi-hop communications. By January 2005, an International Oil and Gas Company (IOC), Shell Petroleum Development Company (SPDC), became the first multinational Oil and Gas Company operating in the Nigeria Niger Delta region to switch from wired to wireless sensor technology eliminating the need for cables thereby allowing data collection in remote, swampy areas and enabling new applications. However, there are concerns related to the use of these smart wireless sensor networks such as reliability, standardization, energy consumption and general operational, data and physical security issues especially in the monitoring of mission-critical oil and gas installations and infrastructure such as pipelines, oil wells, oil rigs and flow stations in a region characterized by rampant vandalisation and sabotage of oil pipelines and other oil installations by militants and oil thieves. High cases of vandalisation of oil and gas pipelines and other oil installations were identified even when there is evidence of wireless sensor deployment. This paper introduced practical deployment architectures and mechanisms that can secure oil facilities and the wireless sensors from being physically attacked so that they can successfully monitor and report incidences of pipeline and equipment vandalisation easily and on time while at the same time maintain data security of the WSN.

KEYWORDS

Wireless Sensor Network WSN, Niger Delta Region, Nigeria, oil pipelines, CCTV, cyber physical systems, security triad, multi-hop communication.

1. INTRODUCTION

Wireless sensor networks are IEEE 802.15.4 enabled devices capable of robust and reliable multi-hop communications [1],[2]. Wireless sensors can be deployed in unattended environments and can enable collection of data from there to distant base stations and then to control room [3],[4].

Wireless sensors have found useful applications in varying number of civilian and military applications because of their low-cost and ease of deployment [2],[5],[6]. Because of these inherent and other advantages, wireless sensor networks have found useful applications in

environmental monitoring applications especially in oil and gas fields. Prior to January 2005, International Oil and Gas Companies(IOC) operating in Nigeria Niger Delta region made extensive use of conventional wired network technologies such as fiber optics and wireless technologies such as satellite and radio communications for monitoring of vast oil wells and facilities but due to prohibitive high cost of deployment and maintenance, delayed detection of pipeline problems and leakages, Ineffective reservoir management and optimization due to the need to obtain data primarily from conventional and non-timely well tests and coupled with frequent stealing and vandalisation of the components of these technologies, Shell Petroleum and Development Company (SDPC), the first International oil and gas company(IOC) to berth in Nigeria, made a paradigm shift to wireless sensor networks (WSNs) for monitoring of her over 1,000 oil wells and other oil and gas facilities scattered all over the dense jungle and swampy/riverine Niger Delta region. Figure 1 depicts the model of vMBusX-SP microwireless sensor installed by Shell in most of her oil wells in Niger Delta [6]. Shell shifted to microwireless sensors because of their following inherent advantages:

- It is small enough so that they attracted less attention,
- It has low power and it is battery operated, without solar panels required by the conventional satellite communication,
- It has long-range wireless communication capabilities, greater than 4-5 miles in a dense jungle,
- It has low-cost, almost at a price that would make it disposable and maintenance free unlike the conventional technologies wired and wireless technologies,
- above all, it is easy to deploy and install and does not require daily maintenance[6].

This shift by Shell to wireless sensors helped her to reduce the operational difficulties and cost hitherto encountered in the deployment and maintenance of monitoring devices of the previous conventional technologies. Apart from this Shell was able to increase her production, maintain safety and increased reservoir life [7]. Since then WSN has been helping other International oil and gas companies (IOC) and other local firms operating in the Niger Delta region such as NNPC, Chevron Texaco, Exxon Mobil, Total and so on and in other oil and gas regions elsewhere by offering great opportunities for production optimization in the areas of remote monitoring of pipelines, oil wells, oil rigs, flow stations, natural gas leaks, corrosion, H_2S, equipment condition, and real-time reservoir status. Data gathered from wireless sensor nodes enables new insights into plant operation and innovative solutions that improve platform safety, optimize operations, prevent problems, tolerate errors, and reduce operating expenses (OPEX). Figure 2 shows the aerial photograph of one of Shell's over 1000 oil wells in Niger Delta field where these micro wireless sensor units were installed. According to [8], the applications of wireless sensor networks(WSNs) and other wireless technologies in oil and gas industries include process monitoring, asset management, plant management, productivity enhancements, Health, Safety and environmental(HSE) monitoring and applications for meeting regulatory requirements.

Figure 1. A model of vMBusX-SP battery-powered Smart Wireless Sensor installed by SPDC in her over 1000 oil wells and other oil facilities in the fields of Niger Delta [6]

All these are some of the enormous benefits WSN can offer to oil and gas prospecting but the greatest obstacle or challenge to utilizing these benefits is the issue of security. Because of ad-hoc wireless communication and unattended deployment nature of wireless sensor network an adversary or attacker can enter the radio frequency of the WSN, intercept and hijack the WSN to eavesdrop the WSN data, modify it or worse still disrupt the entire network. An attacker can equally, due to the unattended deployment nature of the WSN and lack of tamper resistance capability of the sensor nodes, attack the sensors physically, remove the security keys and disrupt the entire network. The implication of these security challenges is that data gathered from these wireless sensors can be intercepted and modified by an attacker and this can affect the confidentiality and integrity of the data, more so, in mission-critical applications such as oil and gas pipeline and reservoir monitoring. The disruption of the smooth functioning of the WSN by an attacker can defeat the entire goal of remote-monitoring of oil and gas installations and infrastructure using wireless sensors. These kinds of attacks are obtainable in the Niger Delta region where militant activities and sabotage, oil bunkering and theft, pipeline vandalisation and all sorts of criminality are the order of the day [9].

Figure 2. A vMBusX-SP wireless sensor units installed in an oil well in the Niger Delta by Shell to help prevent theft and sabotage [6]

Battery powered energy of these wireless sensors does not help matter; the inefficient provisioning of security solutions to the wireless sensors equally leads to the increased energy consumptions of the sensors and thereby reduces the WSN lifespan [8]. Also lack of insights and the provision of technical requirements for WSN in the oil and gas prospecting can lead to the defeat of the smooth functioning of the WSN.

The dominant security challenges in Niger Delta Region ranges from pipeline vandalisation, illegal oil bunkering, kidnapping of oil an gas workers by militants and criminals, vandalisation and destruction of oil and gas facilities such as oil wells, flow stations, oil rigs and even theft and destruction of oil and gas installed equipment and wireless sensors that are supposed to monitor these facilities. According to [11], vandalisation is the most serious challenge out of these whole lots.

Many International Oil and Gas Companies(IOCs) operating in Niger Delta Region have put up much efforts to reduce incidences of these security challenges outlined above but despite these efforts cases of oil and gas pipelines vandalisation and the inability to detect oil and gas pipeline vandalisation on time or at all still remains a very serious security challenge[10].

1.1. Our Contributions

The paper investigates and highlights the security and technical challenges facing the deployment and utilization of IEEE 802.15.4 based WSN devices used to facilitate remote oil and gas field monitoring in the oil-rich Niger Delta region. Equally, this paper introduced deployment architectures and mechanisms that can facilitate easy and fast detection and reporting of vandalisation of oil and gas facilities and the wireless sensors using Wi-Fi base stations, Cyber Physical System (CPS) and digital Close-Circuit Television (CCTV) low-cost cameras. This paper equally proposes an algorithm for the provision of WSN data security for wireless sensors deployed to monitor oil and gas facilities.

2. OVERVIEW OF SECURITY CHALLENGES AFFECTING WSN DEPLOYED IN OIL AND GAS FIELDS NIGER DELTA REGION

The security challenges affecting the successful deployment and utilization of Wireless Sensor Networks (WSNs) in oil and gas field monitoring are quite enormous and are categorised into three major types as follows.

2.1. Major Attack types against Wireless Sensor Network in Niger Delta Region

In Ad-hoc networks, such as Wireless Sensor Network (WSNs), malicious nodes can enter in radio transmission range on the routing path and disrupt network activity. Therefore, protecting from intrusion of malicious nodes to enhance data security is an important issue on Ad-hoc networks especially WSN.

The major attack types or security challenges against Wireless Sensor Networks (WSNs) deployed in oil and gas fields are as follows:

1. *Denial-of-Service (DoS) attacks,*
2. *Compromised or Malicious node attacks and*
3. *Physical attack against the wireless sensor nodes*.

We indentified Physical attack to be the most serious and rampant type of attack against Wireless Sensor nodes deployed in oil and gas fields in the vast and swampy Niger Delta region. The International Oil and Gas Companies (IOCs) operating in the region have made extensive investments in the provisioning of data security to ensure that the data coming from the WSN are confidential and have great amount of integrity but despite these efforts vandalisation of oil and gas pipelines and equipment still persists. This could be as a result of attacks/vandalisation on the wireless sensor nodes themselves which are supposed to do the monitoring and send data report to the base station and finally to the control room about the status of the oil and gas pipelines and equipment. It is a well established fact that once the wireless sensor nodes are compromised physically the security cryptographic solutions inside

them can be extracted and the keys used to compromise the entire WSN. Consequently, the oil and pipelines and facilities they suppose to monitor will be at the mercy of the vandals.

2.2. Security Triads in oil and gas field using Wireless Sensor Networks (WSNs)

There are three types of security required to totally protect and enhance wireless sensor networks used in any field, most especially in oil and gas field. There are as follows:

1. *Operational/Communication Security,*
2. *Information/Data Security, and*
3. *Physical Security.*

The most important of these security triads as identified in the Niger Delta Region is the physical security because once the sensor nodes are compromised physically the entire WSN can be compromised and the oil and gas pipelines and equipment will be entirely at the mercy of the vandals who destroyed the wireless sensor monitors.

3. OVERVIEW OF TECHNICAL CHALLENGES AFFECTING WSN DEPLOYED IN OIL AND GAS FIELDS NIGER DELTA REGION

Apart from security, technical challenges or difficulties are faced on daily basis in the oil and gas industry especially in the Niger Delta Region during deployment and utilization of Wireless Sensor Network (WSN).

The following technical challenges were identified to pose technical difficulties to Plant managers and operators of WSN in Niger Delta oil and gas fields:

1. **Interoperability and scalability issues**: Wireless sensor products from different vendors and of different protocols and standards are difficult to be made to work together or be scaled. WSNs have to co-exist with other wireless technologies such as Wireless LAN (WLAN), Wi-Fi, Bluetooth, etc. Research efforts are yielding good results in finding solution to these challenges. Spread-spectrum Frequency Hopping is a good research effort that can resolve the issues of interoperability.
2. **Technical Knowledge and know-how:** Highly skilled manpower is needed for the effective and efficient deployment, installation and maintenance of the technologies of WSN and other wireless technologies and their interoperability. Training and retraining of technical staff are required to address the challenge of lack of technical know-how.
3. **Energy issues and challenges:** Energy issues such as sensor node battery usage, utilization and maximization pose some technical challenge to the WSN utilization. The energy issues such as battery energy preservation and maximization are of present receiving great research attention.
4. Latency Concerns, Redundancy of WSN nodes, Node failures, Network performance concerns etc, pose another form of technical challenge. Mesh or star network topology deployment in conjunction with Spread Spectrum Frequency Hopping mechanism can help out to reduce energy consumption and at the same time help to maintain an efficient network after node failure.

4. OUR PROPOSED SOLUTIONS

Our proposed solutions cover four main areas to facilitate:

(1.) Easy detection of vandalised oil and gas facilities and wireless sensor nodes,

(2.) Fast reporting of incidences of vandalisation to the nearest base station and then to the control room where SCADA is installed, and

(3.) Proactive prevention of vandalisation of oil and gas facilities by hoodlums.

(4.) Protection of WSN data and communication links

To enable fast detection and reporting of incidences of vandalisation of oil and gas facilities as well as proactively prevent or deter vandalisation of oil and gas facilities and the installed WSN, we propose the following practical deployment architectures:

(1.) Deploying and interconnecting WSN together with Wi-Fi/WiMax network,

(2.) Installing miniaturised wireless Close-circuit Television Circuit (CCTV) cameras around the vicinity where the oil and gas facilities installed to provide 24-hour surveillance, and

(3.) Installation of a Cyber-Physical System (CPS) having WSN and installed actuators integrated with an intelligent decision system,

(4.) Camouflaging or hiding the wireless sensors installed in oil and gas prospecting equipment

In the following section, we will briefly examine the three proposed solution.

4.1. Deploying and interconnecting WSN together with Wi-Fi network.

Wi-Fi wireless sensor connects to the Wi-Fi network automatically as any other Wi-Fi network device. Wi-Fi sensors' settings can be managed wirelessly via Wi-Fi network. Wi-Fi networks are easily available in the Nigerian Niger Delta region and are completely compatible to the mesh architecture which is the defacto deployment topology for WSN in oil and gas industry. Mesh topology deployment of WSN prolong energy of the battery by utilizing shortest path routes and removing redundant paths.

Data transmission from wireless sensors can be pointed directly to the SQL database through personal computer connected to Ethernet LAN[14] as shown in Figure 3 and from the database measured or detected data can be directed to other programs for analysis, for example SCADA systems for fast analysis of WSN data. Incidences of vandalisation of oil and gas facilities or even the vandalisation of some of the wireless sensor nodes can easily be detected by the remaining wireless sensor nodes and routed to the fast Wi-Fi base station and then to SCADA systems installed at the control room.

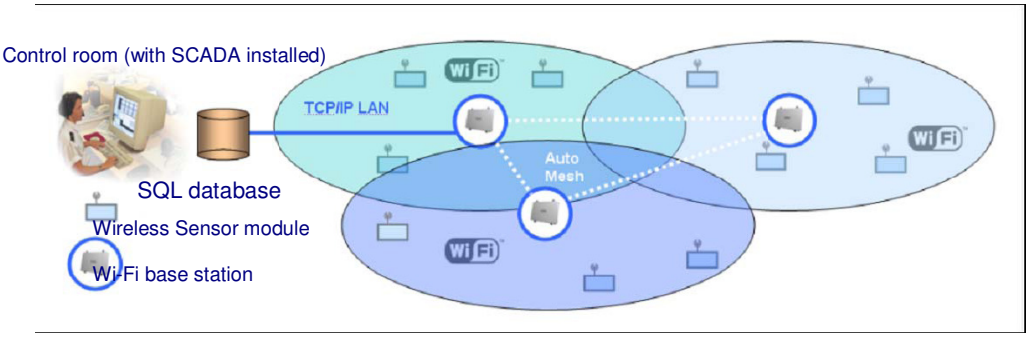

Figure 3. *Direct connection between wireless sensor network and SQL database using Wi-Fi network base station to facilitate easy and fast reporting of vandalisation to the control room (Source from [14])*

4.2. Installing miniaturised wireless Close-circuit Television Circuit (CCTV) cameras around oil and gas facilities

Installing miniaturised wireless digital Close-circuit Television Circuit (CCTV) cameras around the vicinity where the oil and gas facilities installed can provide 24-hour surveillance and expose instantly incidences of vandalisation. One or few wireless CCTV camera can be adequate to provide surveillance for a large area where oil facilities are installed. This preventive mechanism can help record the video footages of oil thieves and vandals and alert nearby Joint Military Task Force (JTF) that operates in Niger Delta region to apprehend and arrest the culprits on the spot. Figure 4 depicts the proposed deployment architecture of wireless digital CCTV cameras in oil and gas facility in the Niger Delta region.

Suggested operations of wireless CCTV cameras around oil and gas facilities:

1. Provide 24-hour surveillance of oil and gas facilities and transmit real-time video data/footage to Joint Military Task Force (JTF) patrol vehicles or stationary stations in the Niger Delta region.

2. Provide physical security cover or surveillance for the installed/deployed wireless sensor nodes so that they can be protected from vandalisation from vandals.

Figure 4 depicts a typical scenario of deployment architecture of wireless CCTV cameras monitoring oil and gas facilities and installed WSN.

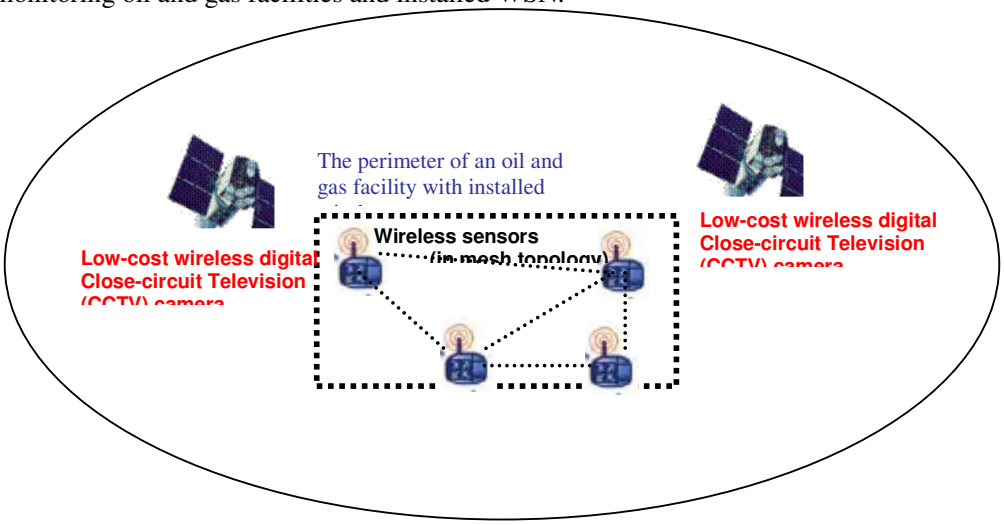

Figure 4. Deployment architecture for wireless digital Close-Circuit Television Circuit (CCTV) to provide surveillance for an oil facility in Niger Delta region

4.3. Installation of a Cyber-Physical System (CPS) to bridge between WSN and actuators integrated under intelligent decision system

As part of proactive and preventive mechanism to stop or deter vandalisation of oil and gas facilities as well as the monitoring WSN, a Cyber-Physical System (CPS) can be installed in an area with vast oil and gas facilities. A CPS may consist of multiple static/mobile sensor and actuator networks integrated under an intelligent decision system [15]. For each individual WSN, the issues such as network formation, network/power/mobility management, security, etc. would remain the same. However, CPS is featured by cross-domain sensor cooperation, heterogeneous information flow, and intelligent decision/actuation. The wireless sensors monitor the oil and gas facilities, the roles of the actuators is to instigate or initiate the intelligent decision systems (such as a robot) to take action immediately WSN detects a vandalisation of oil and gas facility. The intelligent decision system such as a robot can fire a warning shot, raise a very audible alarm or even physically apprehend the vandals or culprits. The practicality of such systems is possible but can be costly at the moment. Robotic actuators are introduced in [16] in details.

Figure 5 depicts the concept of CPS deployment to prevent oil and gas facilities vandals from having their way.

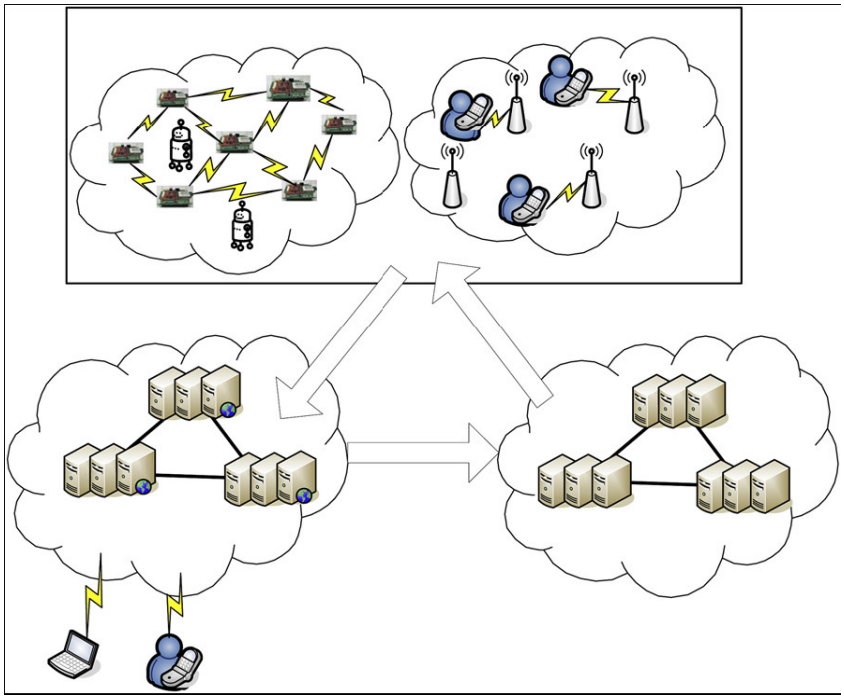

Figure 5. A CPS architecture model for deterring vandalisation of facilities during WSN deployment in oil and gas fields (Source from [16])

4.4. Camouflaging or hiding the wireless sensors installed in oil and gas facility

Another preventive or deterrent mechanism of protecting oil and gas facilities from vandalisation is camouflaging of the oil and gas facilities as well the wireless sensors. Camouflaging or hiding the wireless sensors

Conventional cryptography-based security solutions described above cannot alone provide satisfactory solutions to all the security challenges facing WSN in oil and gas field monitoring. This is because, by definition, once a node is compromised or captured, the adversary or attacker can always acquire the encryption/decryption keys of the node, and thus can intercept any information/data passed through it [12]. Extra security mechanism or scheme is therefore needed to ensure total security for the WSN.

Figure 6 depicts the proposed algorithm for WSN that will ensure WSN data security by applying encryption/decryption using encryption engine such as AES to provide data confidentiality and Message Authentication Codes (MAC) to ensure data integrity in data packets broadcast amongst WSN cluster head (CH) and other sensor nodes.

4.6. Protection of WSN communication links

Operational security ensures that there is continuous availability of WSN at all times. Operational security takes care of attacks on the physical layer of the network protocol stack. For operational/communication security of the WSN the following measures are suggested:

1. Protection of communication links of the WSN against jamming attacks and all sorts of Denial-of-Service (DoS) attacks targeted to exhaust the battery energy of the network in order to disrupt the availability of the network. Encryption of all communication links to wade of malicious nodes from attacking the network in order to enter into the operating frequency of the network to disrupt it.
2. The use of spread spectrum frequency hopping to stop most of the malicious nodes from attacking the network in order to ensure availability of the network so that it will recover and continue to operate even after attack.
3. The use geographic path hopping to protect the routing protocol layer of the network in order to wade off routing attacks against the operational capacity of the network.

4.7. Need to conserve the battery energy of the wireless sensors

Because of the battery energy constraints and memory size of the wireless sensor nodes, combining all these suggested security solutions into one solution especially for data/information and operational/communication security will be a great challenge. The cost of providing security must not exceed the security objective that is to be solved [13]. Some of the suggested solutions can be integrated depending on how critical the WSN application that requires the security. For instance, providing security for WSN monitoring oil and gas pipelines carrying millions of barrels of crude oil or liquefied natural gas is a mission-critical application and will require complete security solution to protect it. The application that is not so critical can make do with some of the suggested solutions in order to conserve the sensor battery energy and elongate the lifespan of the network.

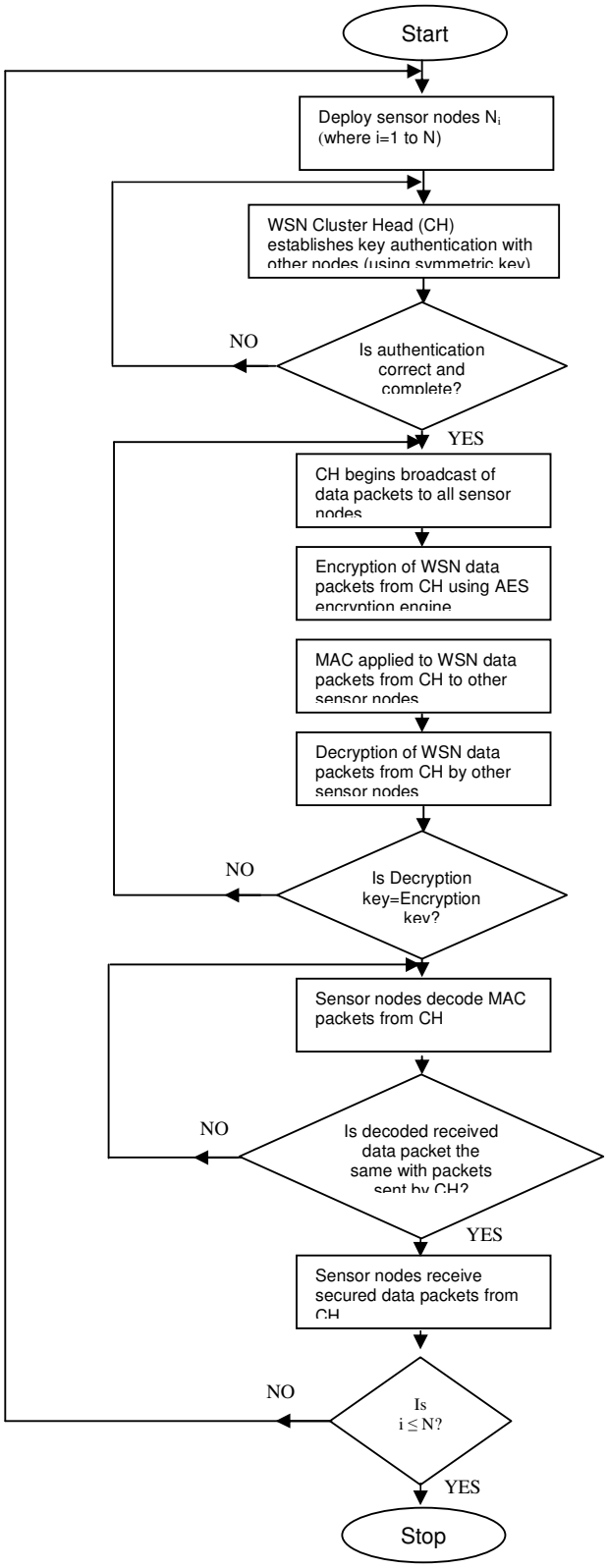

Figure 6. A process flowchart depicting the flow of securing WSN data packets from WSN cluster head (CH) to other nodes using authentication keys, encryption and MAC

5. CONCLUSIONS

In this paper, the security and technical challenges facing the deployment and utilization of wireless sensor Networks (WSNs) in the Niger Delta oil and gas field monitoring have been identified. For WSN to perform optimally and reliably in mission-critical oil and gas infrastructure and facility monitoring, the security challenges facing them must be tackled and resolved successfully. The three-tier security triad: operational, data/information and physical security of the wireless sensor network have been identified as the key security issues affecting WSN deployed for oil and gas field monitoring. This three-triad security must be provided for reliable and efficient operation of the WSN in field monitoring; the data emanating from the WSN nodes to the base stations and control room must be made to be confidential and reliable. The communication links of the WSN must be secured against eavesdropping and denial-Of-Service attacks to protect the WSN from being hijacked and its services disrupted by criminal-minded elements; most importantly, pre-emptive and proactive physical security measures should be provided at the oil and gas fields to deter or apprehend criminals who may want to vandalise oil facilities in order to steal crude oil. Efforts, also, must be made to protect the sensors installed in unattended and hostile environments such as obtainable in the Niger Delta region from being physically captured and attacked. This paper proposed deployment architectures and mechanisms to protect oil and gas facilities as well as wireless sensors from being physically vandalised using novelty technologies such as Cyber Physical Systems(CPS), Wireless Fidelity(Wi-Fi) and low-cost digital Close Circuit Television(CCTV) cameras.

Technical challenges such as inoperability of different WSN standards, issues relating to preservation of battery energy of the wireless sensors, Network performance etc. must be considered in order to ensure the smooth functioning and energy preservation of the wireless sensors. It is after these countermeasure solutions are provided that WSN can provide an efficient and reliable oil and gas field monitoring for an oil region full of security challenges as the Nigerian Niger Delta.

5.1. Suggestion for further work

We suggest more research work to be carried out on how Cyber-Physical System (CPS) can be used to practically safeguard and protect remotely installed oil and gas facilities from vandals and crude oil thieves.

REFERENCES

[1] I.F.Akyildiz, W.Su, Y.Sankarasubramaniam and E.Cayirci (2002) "A Survey on Wireless Networks", IEEE Communications Magazine, pp.102-114.

[2] S.Petersen, P.Doyle, S.Vatland, C.S.Aasland, T.C.Andersen and D.Sjong (2007) "Requirements, Drivers and Analysis of Wireless Sensor Network Solutions for Oil and Gas Industry", IEEE Communications Magazine, pp.219.

[3] G.Sharma, S.Bala, A.K.Verma and T.Singh (2012) "Security in Wireless Sensor Networks using Frequency Hopping", International Journal of Computer Applications (0975-8887), pp.1.

[4] C.Bisdikian (2012). "An Overview of the Bluetooth Wireless Technology", IEEE Communication Magazine, vol.39.

[5] C.O.Iwendi and A.R Allen (2011) "Wireless Sensor Network Nodes: Security and Deployment in Niger-Delta Oil and Gas Sector", International Journal of Network Security and Its Applications (IJNSA), Vol.3, No.1, pp.68.

[6] T.Fasasi, D. Maynard and H.Nasr (2005) "Sensors remotely monitor wells in Nigeria swamp*s",* Oil and Gas Journal, pp.2.

[7] T.Fasasi, D. Maynard and H.Nasr (2005) "Sensors remotely monitor wells in Nigeria swamps", Oil and Gas Journal, pp.4.

[8] J.G.Bhatt (2007) "Wireless Networking Technologies for Automation in Oil and Gas Sector", Electrical Engineering Department Indian Institute of Technology Roorkee, India, pp.15.

[9] K.N.Aroh, I.U.Ubong, C.L.Ezeh, I.M.Harry, J.C.Umo-Otong, A.E.Gobo (2010) "Oil Spill Incidents and Pipeline Vandalisation Incidents in Nigeria: Impact on Public Health and Negation to the Attainment of the Millennium Development Goal", Disaster Prevention and Management Journal, Vol. 19 Issue 1, pp.70-87, ISSN 0965-3562.

[10] T.John (2012) *TUC backs NUPENG on alleged JTF's connivance with bunkerers,* Daily Sun, Thursday, 16, August, 2012, pp.10.

[11] E.F. Idachaba (2011) "Remote Operation of Oil and Gas production installations in the Niger Delta" Asian Transactions on Engineering (ATE ISSN: 2221-4267) Vol. 01 Issue 03, pp. 58.

[12] T. Shu, M. Krunz and S. Liu. "*Secure Data Collection in Wireless Sensor Network Using Randomized Dispersive Routes",* Department of Electrical and Computer Engineering University of Arizona, pp.14.

[13] A.K.Pathan, H.Lee and C.S.Hong (2006) "Security in Wireless Sensor Networks: Issues and Challenges", Proceedings from ICACT2006, February 20-22, 2006, pp.1047

[14] AutoLog, "Wi-Fi Wireless Sensor Networks", Accessed online @ http://www.ff-automation.com on November 8, 2012, pp.3.

[15] Fang-Jing Wua, Yu-Fen Kaob, Yu-Chee Tseng, "From wireless sensor networks towards cyber Physical systems", Elsevier Journal of Mobile Computing, March 2011, pp.7-8.

[16] I.F. Akyildiz, I.H. Kasimoglu, Wireless sensor and actor networks: research challenges, Ad Hoc Networks 2 (4) (2004) 351–367.

Authors

Fidelis C. Obodoeze is a Doctoral Research Student in the Department of Electronic and Computer Engineering Nnamdi Azikiwe University Awka. He is currently lecturing Computer Science and Engineering at Renaissance University Agbani Enugu. His PhD work is on Data and Operational Security of Wireless Sensor Network (WSN) in Oil and Gas industry Niger Delta Region. He had his Masters Degree in Control Systems and Computer Engineering at Nnamdi Azikiwe University and B.Sc Degree in Computer Engineering at Obafemi Awolowo University Ile-Ife. He has authored several conference and research journal publications. He has about seven years experience in ICT industry which included holding forth as Chief Technical Officer (CTO) in an IT firm based in Wuse, FCT Abuja.

Prof. Hyacinth Chibueze Inyiama is a Professor in the Department of Electronic and Computer Engineering Nnamdi Azikiwe University Awka. He holds PhD (University of Manchester, UK), MEngr, BEng in Computer Engineering. He has taught and supervised several PhD and Masters Research students in Computer Engineering, Telecommunications, Control Systems and Computer Science that spans over three decades. He is a visiting professor and external examiner to a number of universities in Nigeria and abroad. He is a member of NSE, COREM, NCS, etc. He has authored several publications in reputed local and International journals and presented several conference papers both at home and abroad.

Dr. V.E Idigo is an associate Professor holds a Ph.D, M.Eng, BEng in Communication Engineering, a Member of IAENG, MNSE and COREN, with about two decades in the Lecturing Profession and a recipient of many academic awards he is presently the Head of Department of Electrical Electronics in Nnamdi Azikiwe University Awka Anambra State, Nigeria. He has much Publication to his credit both locally and internationally.