FRAMEWORK OF WIRELESS SENSOR NETWORK (WSN) FOR OIL AND GAS INFRASTRUCTURE PROTECTION WITH EMPHASIS ON NIGER DELTA REGION OF NIGERIA

Nwabueze, C. A. and Nzeife, I. D.
Department of Electrical/Electronic Engineering,
Chukwuemeka Odumegwu Ojukwu University, Uli, Anambra State, Nigeria.
Email: canwabueze@yahoo.com and nzeifeid@gmail.com

ABSTRACT

This paper studied and highlights the security and technical challenges facing the deployment and utilization of IEEE 802.15.4 based Wireless Sensor Network (WSN) devices used to facilitate remote oil and gas field monitoring in the Niger Delta region of Nigeria. The underlining crises were also highlighted and a solution framework was proffered. The framework includes suggestion for amicable resolutions between parties, putting in place a proactive WSN structure for monitoring infrastructure to facilitate easy and fast detection and reporting of vandalized oil and gas facilities. A designed data encryption algorithm to secure the validity of information using symmetric encryption was also presented. This paper also presents an overview of sensor devices, the advantages of WSN over the wired monitoring system for pipeline monitoring and application environment. Overview of conflicts and security challenges in oil and gas exploration fields in the Niger Delta region are also discussed. Encryption as a standard method for protecting WSN data from possible attacks, advantages and disadvantages of the two classes of encryption methods and the System's framework for the monitoring the infrastructure and designed encryption algorithm of the system are presented.

Keywords: Wireless Sensor, Network, Monitoring, Pipeline, Infrastructure.

1.0 INTRODUCTION

A wireless sensor network (WSN) [1] [2] is a network formed by a large number of sensor nodes where each node is equipped with a sensor to detect physical phenomena. It is a natural battery operated sensing technology that processes collected data, transmits and communicates with other nodes through radio frequency (RF) channel [3]. WSN consist of hundreds, even thousands of nodes. The sensor node collects information from the environment and sends it to main the node called sink node or base station (BS) which can be one or more [4]. As depicted in figure 1, the BS is referred to as a gateway. A base-station maybe a fixed node or a mobile node capable of connecting the sensor network to an existing communication infrastructure or to the Internet where a user or an observer can have access to the reported data. The network is self-configuring and capable of reorganizing at all times and that they can be deployed in unattended environments still enabling collection of data from there to distant base stations and then to control room [5, 6].

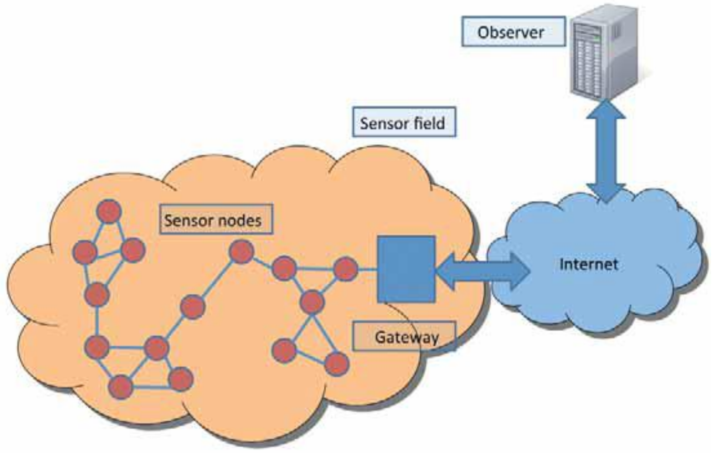

Figure 1: Wireless Sensor Network (WSN) [1].

1.1 Sensor Devices

Sensor devices are basically formed by a computational part responsible for storing and transmitting data, and a sensing portion which can be formed by one or more sensors, such as acoustic, seismic, infrared video camera, heat temperature and pressure. In general, two modulation formats are available: Frequency-Shift-Keyed (FSK) operating at 433 MHz and 868-915 MHz and direct sequence spread spectrum (DSSS) operating at 2.4 GHz band that transmit IEEE 802.15.4 and ZigBee standards. The reach of the radios varies from 10 to 100 meters [7, 8]. Currently, the sensor nodes can vary between mode activity, inactivity (idle) and low consumption (sleep) in order to save energy [7, 8]. The main sensor nodes available are LOTUS, IRIS, MICAz, Mica2, and TELOSB CRICKET. IEEE 802.5.14 is the most relevant communication standard for the WSN. IEEE 802.5.14 defines the physical and link layer for short-range wireless transmission with low power consumption, low complexity and low cost and is the foundation for other standards like ZigBee®, WirelessHart, WIA-PA and ISA.100.11a which define regional or market specific versions [8, 9].

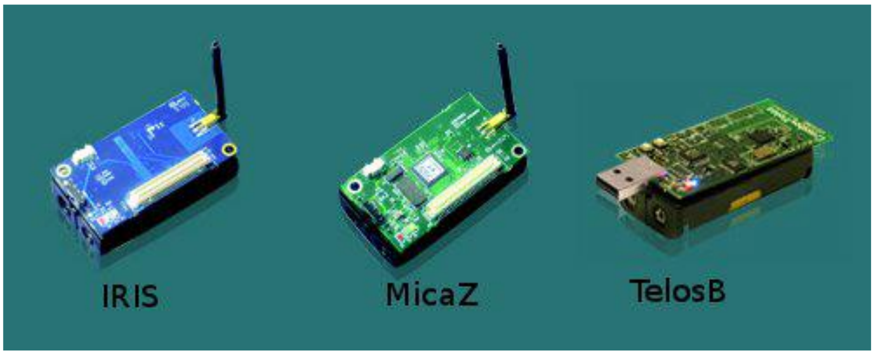

Figure 2: IEEE 802.15.4 Standard Sensors [7].

1.2 Advantages of WSN over Wired Network

In recent years, availability of low cost wireless sensor nodes makes WSNs to be a more viable choice in pipeline monitoring than their wired counterparts. Compared with the wired solution [1], WSNs feature easier deployment and better flexibility of devices. The following advantages of a WSN over a traditional wired network in monitoring a large pipeline infrastructure are identified [10], elaborating that the traditional wired protection method incurs the follow:

1. That the tiniest damage in any part of the long wiring structure may render the whole monitoring system useless.
2. Surveillance across a long network is a very difficult task, it is easier for a human attacker to disable a wired monitoring system by cutting the network wires in an unprotected part.
3. Also, determining the point of failure in a wired network requires a thorough scanning across the entire network length in the worst case.

It is believed that Shell Petroleum Development Company (SDPC) shifted to micro wireless sensors because of the following inherent advantages of WSN nodes [9]:

- It is small enough that they attracted less attention,
- It has low power and it is battery operated, without solar panels required like in 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 wired and wireless technologies, above all, it is easy to deploy and install and does not require daily maintenance (figure 2).

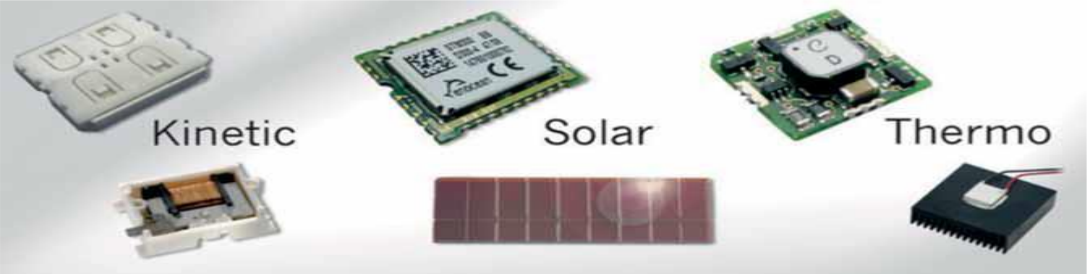

Figure 3: Sensor Nodes Configured with Ambient Energy Harvesting Devices [1].

Figure 3 depicts three different sensors which could operate using kinetic (micro-electromechanical vibrations), solar or thermo as battery energy source. Any of these sensors could be applied where their source of energy is considered cheaper.

2.0 Overview of Application Environment

2.1 Application

WSNs can be applied in various areas such as [7]:

• Environment **-** Monitoring of environmental variables such as in buildings, residences and external locations such as oceans, volcanoes, deserts, etc..

• Traffic **-** Monitoring of vehicle traffic on highways, railroads, rivers, oceans, etc.

• Security **-** To provide security in homes, shopping centers, farms, among others.

• Military **-** To detect the presence of enemies, explosions, presence of hazardous materials as poison gas and radiation.

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 [11]. Typically, sensor nodes are deployed randomly (e.g., via aerial deployment), and are expected to be self-organize to form a multi-hop network and such a system has the potential to reduce the casualties that incur in surveillance of hostile environments [12]. The recent integration of sensors with microcontroller and embedded microprocessors had made this dream come true where integration of physical world with digital technology is possible [4]. Hence, this diversity has resulted in a complex standardized environment.

2.2 Overview of Conflicts and Security Challenges in Oil and Gas Exploration Fields in Niger Delta

Pipeline infrastructure is considered to be a very critical component for any nations' economy and is vastly used to distribute oil, natural gas, water, sewage etc. across the country. Therefore, protecting and monitoring pipelines is a mission critical job for a thriving economy [8][10]. Lack of monitoring, on the other hand, may result in loss of critical natural resources. Long list of accidents arose in one form or the other from pipeline malfunction. Apart from the loss of valuable natural resources, most of these accidents were also responsible for human casualties. One such notable example was the *1998 Jesse pipeline explosion* in Nigeria. This explosion was reported to have cost the life of nearly 700 villagers as quoted in [8] and over one 1000 villagers. Hence, these incidents clearly underscore the importance of implementing a robust pipeline monitoring and protection system [8, 13 and 14].

The Niger delta scenario unlike any other part of the world is complicated with socio-economic and political conflicts and interests.

These conflicts in the region are based on the following classifications [15]:

- ❖ Conflicts within the oil bearing communities arising from divide and rule policy of the oil companies.
- ❖ Conflicts between the host oil communities and the government.
- ❖ Conflicts between the host oil communities and the oil companies.
- ❖ Conflicts between two different communities or states.

The challenges can be classified into Accidental, Malicious (Sabotage), Incidental and Acts of Vandalism. *Terrorist attacks* pose a significant threat to the safety of pipeline infrastructure [8, 16]. There are at least 497 accounts of oil pipeline vandalism within a single calendar year in Nigeria alone, and *Pipeline sabotage* has been reported as a very common occurrence in Nigeria. Several of such sabotages have caused pipeline explosion and resulted in human casualties. Sabotage is currently the leading cause of oil spillage in Nigeria and pipeline vandalism and disruption of oil activities regrettably are now integral part of oil and gas operation in Nigeria [14].

There are concerns related also to the use of wireless sensor networks with regards to its reliability, standardization, energy consumption and general operation. Also, 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 vandalism and sabotage of oil pipelines and other oil installations by militants and oil thieves even when there is evidence of wireless sensor deployment. Quite a few protocols have been proposed to monitor pipelines using wireless sensor networks over the last few years. However, it should be noted that these protocols were not designed to take into account the presence of human adversary. Most of the existing protocols are primarily designed to sense device malfunctions such as leakage, blockage, rupture etc. in the pipelines. Also, most of these protocols are able to detect direct attacks like that of *pipeline vandalism* because these attacks always result in device malfunction regardless of the attack type [8, 17].

2.3 Security Vulnerabilities of WSN

Attacks on WSNs can be divided into three main types:

(1) Attack of authentication and confidentiality: Consists of attacks intended to change, cause repetition or modification of packages.

(2) Availability network Attack: Generally known as Denial-of Service (DoS) attacks or negation of service, this involves the application of techniques that make the network unavailable.

(3)Attack on integrity (compromise or malicious attack): in this type of attack, the attacker’s goal is to inject false data into the network, keeping the network available with fictitious data. The most common types of attacks in WSN depending on the network layer in which they operate are [7, 18]:

- ❖ **Physical** Layer. They stated that at the physical layer, jamming and tampering can occur. Jamming results to interference on radio frequency signals of the sensor nodes hampering communication. The tampering attack occurs due to physical vulnerability of sensor nodes spread over large areas and being susceptible to damage. Hence, 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 vandalism and all sorts of criminality are the order of the day [9].
- ❖ At **link** layer attacks can be of the collision, when two sensor nodes attempt to transmit while at the same frequency, in this case the packet is discarded and must be retransmitted. Setting modification or even replacement of a network node by a malicious sensor node [7, 11].

According to them, the attacker may cause intentional collisions by a malicious sensor node and that repeated collisions can lead to exhaustion of resources, resulting to death of sensor nodes. Also in the link layer exists the Denial of Service (DoS) attacks which floods the receiver with no other requests for communication thereby cutting off the involved nodes out of communication.

- ❖ In the **network** layer attacks can occur of type Spoofed Routing Information, where the attacker modifies routing table information causing the packets not to reach the desired destination, or even make the referral to consume more resources than normal.

The following problems are associated with the use of WSN [1]:

1**. Interoperability, scalability, energy and architectural divergence problems** as noticeable in lowered “horizontal recycling” of functions, modules and concepts from one domain to another as the main challenges to effective use of WSN nodes. Similarly, these are identified as the technical challenges posing difficulties to Plant managers and operators of WSN in Niger Delta oil and gas fields. Both believe that products should be of universal standards and adoptable to other wireless technologies and that best method of energy management in WSN should be applied [9].

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 [9].

3. **Latency Concerns**: Redundancy of WSN nodes, Node failures, Network performance concerns etc., pose another form of technical challenge. Proffering solutions, Mesh or star network topology deployment in conjunction with Spread Spectrum Frequency and improving on inter-node and node-CH communications using effective scheduling plan would reduce latency. Energy consumption also can be minimized by using multipath routing mechanism and hierarchical routing [3, 9].

3.0 ENCRYPTION

3.1 Standard Method for Defending WSN data of Most Possible Attacks

Encryption system is an art that consists of distorting the information that is being transported, so that only the authorized recipient can decipher it. Encryption is the standard method for defending a WSN of most possible attacks, even though various levels of encryption implies variations in overhead in the form of growth in the size of package data, code size, processor usage, memory, etc. In this regard, a cryptographic algorithm can be set as a function that converts encrypted message in clear messages and vice versa, making use of a cryptographic key. Currently encryption ensures [7, 19]:

• Confidentiality: ensuring that only the sender and receiver have the ability to understand the message being exchanged.

• Integrity: Ability to check if a message was altered during transmission.

• **A**uthentication: Medium to prove the identity of an individual communication.

3.2 Classes of cryptographic algorithms

Cryptographic algorithms are an essential part of the security architecture of WSNs, using the most efficient and sufficiently secure algorithm which is an effective means of conserving resources of tiny sensors. Most existing cryptographic algorithms can be classified as symmetric or asymmetric. Symmetric encryption involves the use of a key called the symmetric key. This key will be used to encrypt a message and decrypt same message. Asymmetric uses two keys, a private key and a public key. The public key is used to encrypt a message and the private key is used to decrypt same message. Different keys are used on each end of an encrypted communication between two parties [19, 21].

ADVANTAGES OF SYMMETRIC

A symmetric cryptosystem is faster.

• In Symmetric Cryptosystems, encrypted data can be transferred on the link even if there is a possibility that the data will be intercepted. Since there is no key transmitted with the data, the chances of data being decrypted are null.

• A symmetric cryptosystem uses password authentication to prove the receiver’s identity.

• A system only which possesses the secret key can decrypt a message.

DISADVANTAGES

• Symmetric cryptosystems have a problem of key transportation. The secret key is to be transmitted to the receiving system before the actual message is to be transmitted. Every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So the only secure way of exchanging keys would be exchanging them personally.

• Cannot provide digital signatures that cannot be repudiated

ADVANTAGES

• In asymmetric or public key, cryptography there is no need for exchanging keys, thus eliminating the key distribution problem.

• The primary advantage of public-key cryptography is increased security: the private keys do not ever need to be transmitted or revealed to anyone.

• Can provide digital signatures that can be repudiated

DISADVANTAGES

• A disadvantage of using public-key cryptography for encryption is speed: there are popular secret-key encryption methods which are significantly faster than any currently available public-key encryption method.

Secure data aggregation of WSNs

Secure data aggregation is to ensure each node data is secured. The general processes of secure data aggregation are as follows: first, it should be possible for the nodes to provide reliable data and securely transmit them to the higher aggregation nodes. The higher aggregation nodes judge the credibility of data and do aggregation calculation based on redundancy. Each aggregation nodes select the next safe and reliable hop, and then transmit data to the central node. The central nodes judge the credibility of data and do the final aggregation calculation. Secure data aggregation is mostly realized by authentication and encryption based on the theory of cluster and hierarchy [11].

Many secure **routing** networks have been specifically designed for WSNs, they can be divided into three categories according to the network structure: flat-based routing, hierarchical based routing, and location-based routing [5]. Hierarchical is adopted in this framework because of its advantages over others in energy conservation [3].

4.0 SYSTEM FRAMEWORK

Our preferred solutions cover two major areas:

1. Proactive preventive /detective measures (a) Human Angle and (b) Scientific Angle
2. Data and data link security using symmetric encryption algorithm.

4.1 The human aspect could be the key factor that leads to most of the trouble especially in the Niger Delta scenario. From the quoted sources, it seems most of these oil companies for some reasons have not fully realized that they run their business where people live and owned and whose habitat it is no longer news that these exploration activities had affected negatively and not much caution had been taken to forestall further occurrences. The people feel neglected and poorly compensated and hence, the feud. On the other hand, the concerned communities (when issues are resolved) should be made to understand that it is important that the Federal government accrue revenue through these oil firms to sustain the nation. They should not overbear on the firms with their demands that sometimes seemed outrageous and impracticable. There should be an environment based on clear mutual understanding of each party's stance for a sustainable relationship based on give and take to exist, in other to avoid the protracted wanton destruction of infrastructures by the community due to some misunderstanding between the host communities and the firms. The community representatives should be transparent and honest with their people too.

4.2 (b) Scientific angle to proactive measures includes:

Proactive monitoring and surveillance of facilities within the premises and Pipelines can be achieved using the network arrangement as shown in figure 4. Solution for monitoring such expanse of infrastructure entails using a relatively high density WSN node. The first component consists of inexpensive off-the-shelf wireless sensor devices, such as MicaZ motes. Specially trained management staff will supervise the protection system by Internet at any time. This paper adopts the WSN architecture shown as Figure 4, to furnish the monitoring system framework (distances of course will vary according to topography and area). Clustered wireless sensor network is used to collect protection potential data; communication subnet take responsibility for long-distance data transmission; and the Internet service network is responsible for data processing, analysis and system control. This monitoring system chooses General Packet Radio Service (GPRS) network for remote communication, which has the merit of spread coverage, high data transmission rate, effective real-time processing, good correspondence quality, continued online and low expense [17]. GPRS technology can support bi-direction long-distance data transmission by intercommunicating with the Internet following TCP/IP protocol; and high traffic capacity to satisfy the needs of sudden data transmission for so many sampling points.

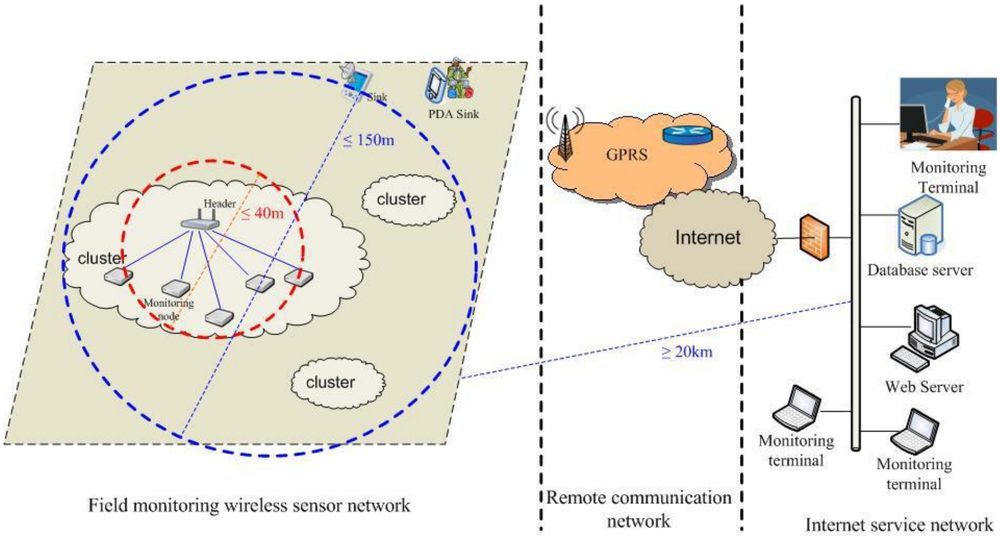

Figure 4: Network Structure of Monitoring System [17].

In figure 4, the Wireless sensor network (WSN) uses cluster scheme to realize energy conservation. The grouped sensors collect information within the monitoring zone of their cluster and send to their respective cluster heads (CH). There are two CHs acting as gateways between the WSN and the Internet.

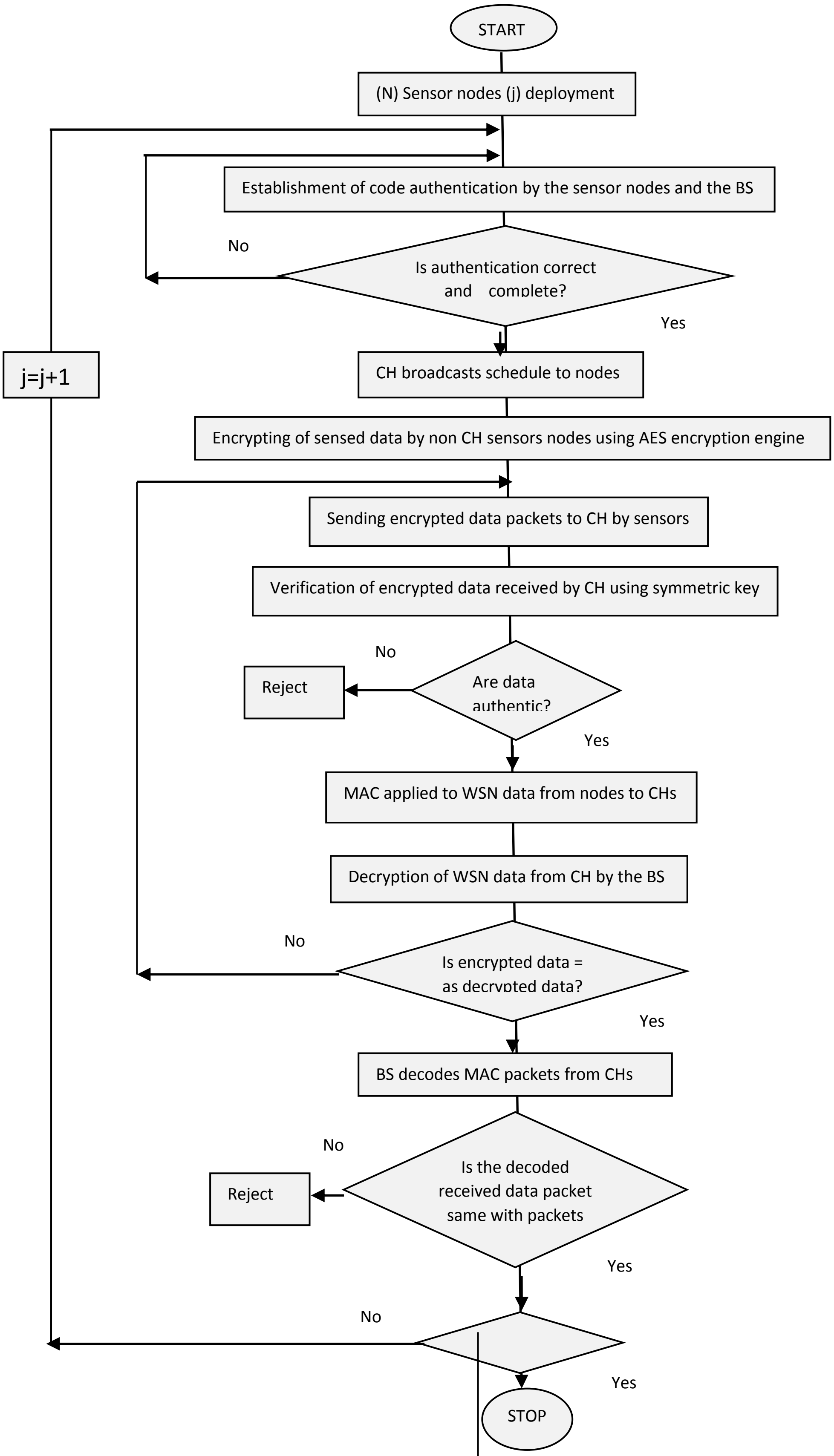
START
(N) Sensor nodes (j) deployment
Establishment of code authentication by the sensor nodes and the BS
No
Is authentication correct and complete?
Yes
j=j+1
CH broadcasts schedule to nodes
Encrypting of sensed data by non CH sensors nodes using AES encryption engine
Sending encrypted data packets to CH by sensors
Verification of encrypted data received by CH using symmetric key
No
Reject
Are data authentic?
Yes
MAC applied to WSN data from nodes to CHs
Decryption of WSN data from CH by the BS
No
Is encrypted data = as decrypted data?
Yes
BS decodes MAC packets from CHs
No
Reject
Is the decoded received data packet same with packets
Yes
No
Yes
STOP

Figure 5: Data and Data Link Security Symmetric Encryption Algorithm.

Another kind of Sink integrated in Personal Digital Assistance (PDA) compatible with CompactFlash (CF) card can provide on-site maintenance by sending not only query command to wake up the monitoring node to collect information, but also control commands to adjust operating parameters of WSN. The web server in the Internet with a dynamic or static Internet Protocol (IP) address communicate with Sink through GPRS network to collect potential information from WSN in time, check network working state and store data in the database server [17]. Link could be made interconnecting the BS, Control Room (CR) and the State Security Services (SSS) for a quicker response.

2. Data and data link security using symmetric encryption algorithm
Figure 5 depicts the proposed data and data link security algorithm using symmetric encryption. It has the ability to check at some crucial stages the validity of transmitted data before they get to the user. Though the recommended framework may go a long way in solving most of the identified shortcomings in oil and gas infrastructure protection in Niger-Delta region of Nigeria, it is however recommended that other systems of data security should be incorporated as no particular measure would be able to completely solve the issue of network data invasion in the present world.

CONCLUSION

Problems of security and pipeline vandalization can broadly be divided into two major issues: Host community/company clashes and scientific/technology security problems. This paper calls for understanding and amicable resolution of issues bothering on oil and gas exploration activities in the concerned communities. It has also looked at security and technical challenges' being experienced in the use of IEEE 802.15.4 based WSN sensors in this region and proffered a network structured solution for surveillance using node clustering, GPRS, internet and servers. It also presented a symmetric encryption algorithm that will take care of security, confidentiality, authentication and integrity of data transmission.

REFERENCES

[1] Yinbiao et al (2014), *Internet of Things*: Wireless Sensor Network International Electrotechnical Commission, 3 rue de Varembe CH-1211 Geneva 20 Switzerland, pp-3-78

[2] Archana, B., Vijay, A. and Sai, P. (2004), *Sensor Networks: An Overview*, International Journal of Sensors and Sensor Networks; Vol. 2(3), pp 22-32

[3] Nzeife, I. (2016*). Enhancing Energy Efficiency of Wireless Sensor Networks Using HierarchicalRouting Technique*, Unpublished M. Eng. Dissertation in the Department of Electrical/Electronic Engineering, Faculty of Engineering, Chukwuemeka Odumegwu Ojukwu University,Uli, Nigeria.

[4] Iqbal, J. and Moughal, F. (2010), *Wireless Sensor Network Setu*, Master's Thesis in Computer Systems Engineering, School of Information Science, Computer and Electrical Engineering, Halmstad University, Technical Report, IDE1043, (June 2010).

[5] Al-Karaki, J. N. and Kamal, A. E. (2004), *Routing Techniques in Wireless Sensor Networks: A Survey,* Wireless Communications, IEEE, Vol. 11, No. 6, pp. 628.

[6] Olafsen, H. K. (2007), *Wireless Sensor Network Localisation Strategies*, Master Thesis, Department of Informatics, University Of Oslo.

[7] Quirino, G. S., Ribeiro. A. R. L. and Moreno, E. D. (2007), *Asymmetric Encryption In Wireless Sensor Networks Wireless Sensor Networks,* Technology and Protocols INTECH, Vol.10, pp 217-231.

[8] Mohammad, S. I., Nix, R. and Kantarcioglu, M. (2012), *A Game Theoretic Approach for Adversarial Pipeline Monitoring using Wireless Sensor Networks*; IEEE IRI, Las Vegas, Nevada, USA.

[9] Obodoeze, F. C., Inyiama, H. C. and Idigo, V. E. (2012), *Wireless Sensor Network in Niger Delta Oil and Gas Field Monitoring: The Security Challenges and Countermeasures*, International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.6.

[10] Mohamed, J. N. and Shuaib, K. (2007). *A Framework for Pipeline Infrastructure Monitoring using Wireless Sensor Networks*, Wireless Telecommunications Symposium, pp 7.

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

[12] Bokareva, T., Hu, W., Kanhere, S., Ristic, B., Gordon, N., Bessell, T., Rutten, M. and Jha, S. (2006), *Wireless Sensor Networks for Battlefield Surveillance*, Land Warfare Conference, Brisbane.

[13] Demirkol, C., Ersoy, E. and Alagoz, F. (20001). *MAC Protocols for Wireless Sensor Networks: A Survey*, IEEE Communications Magazine, Vol. 44, No. 4, pp. 115-121.

[14] YO-Essien, L. P. E., *Oil Spiill Management in Nigeria: Challenges of Pipeline Vandalism in The Niger Delta Region of Nigeria*, National Oil Spill Detection and Response Agency (NOSDRA) Abuja, Nigeria

[15] Akpan, P. U. (2014), *Oil Exploration and Security Challenges in the Niger-Delta Region: A Case of Akwa Ibom State*, *Nigeria*, A Ph.D. Thesis of the Department of Political Science & Public Administration, Faculty of Social Science, University of Uyo, Uyo, Akwa Ibom State, Nigeria. IOSR Journal of Research & Method in Education (IOSR-JRME), Vol. 4, Issue 2. Pp. 41-48.

[16] Achebe, C H., Nneke, U. C., and Anisiji, O.A. (2012), *Analysis of Oil Pipeline Failures in the Oil and Gas Industries in the Niger Delta Area of Nigeria*. Proceedings of the International Multi Conference of Engineers and Scientists, (IMECS), Hong Kong, Vol 2.

[17] Liu, P., Huang, Z., Duan, S. , Wang, Z. and He, J. (2015), *Optimization for Remote Monitoring Terrestrial Petroleum Pipeline Cathode Protection System Using Graded Network*; International Journal of Smart Home, Vol. 9, No. 6, pp. 51-64.

[18] Wang, Y., Attebury, G. and Ramamurthy, B. (2006), *A Survey of Security Issues in Wireless Sensor Networks*, IEEE Communications Surveys and Tutorials, Vol. 8(2), pp 2–23.

[19] Patel, B. N., and Pandya, N. (2013), *Secure Data Transfer using Cryptography with Virtual Energy for Wireless Sensor Network*, International Journal of Engineering Trends and Technology (IJETT), Vol. 4., Issue 8, pp. 3468- 3473.

[20] Boyle, D. and Newe, T. (2008), *Securing Wireless Sensor Networks: Security Architectures*, Journal of Networks, Vol. 3(1), pp. 65–77.

[21] KetuFile White Papers (2004), *Symmetric vs Asymmetric Encryption*, KetuWare, a Division of Midwest Research Corporation, pp.1-7.