Oil Pipeline Vandalism Detection and Surveillance System for Niger Delta Region

Obodoeze Fidelis Chukwujekwu
Department of Computer Science, Renaissance University
Enugu, Nigeria

Asogwa Samuel Chibuzor
Department of Computer Science, Michael Okpara
University of Agriculture, Umudike, Nigeria

Ozioko Frank Ekene
Department of Computer and Information Science, Enugu
State University of Science and Technology (ESUT),
Enugu, Nigeria

***Abstract* - Oil pipeline vandalism is on the increase in the oil rich Nigeria Niger Delta region with over 400,000 barrels of crude oil lost to crude oil bunkerers as a result of rampant rupturing and vandalisation of pipelines transporting crude oil and refined products from one point to another in the region. In this paper automated electronic pipeline vandalism detection and surveillance system with the capacity to detect intrusion into pipeline system before vandalisation takes place and send SMS and email alerts to plant operators. The system is also integrated with a surveillance camera so as to capture the video footage needed in tracking and prosecuting the criminals in court of law.**

Keywords - Pipeline monitoring, surveillance, video camera, SMS, Waspmote, 3G/GPS, SCADA, security, FTP Server, cloud storage,HSPDA

I. INTRODUCTION

Pipeline system as a medium of transportation is usually attributed to very sensitive products such as crude oil, natural gas and industrial chemicals, in which unattended problems in their operation results in unimaginable catastrophe. These problems include terrorism attacks, vandalism and theft of the pipeline content. The need for implementing adequate security systems for pipeline management has been addressed from time immemorial. While some of these attempts have recorded some level of success, others have contributed insignificantly to this outstanding challenge that is currently giving mankind sleepless nights. Vandalism refers to illegal or unauthorized activities that result in the destruction of petroleum, gas and chemical pipelines. It is a negative activity aimed at getting products for personal use or for sale in the black market especially in developing countries of the world where they are rampant. About 40% of the world's oil flow through pipelines which run thousands of kilometers across some of the most volatile areas of the world [1,2].

Shell Petroleum and Development Company (SPDC), one of the many International Oil Companies (OICs) operating in the Niger Delta region in a bid to protect its vast array of oil pipelines and other oil facilities scattered in the Niger Delta, in January 2005, introduced the use of micro wireless sensor network (WSN) which was supposed to help her to detect drop in pressure once an oil pipeline is ruptured by vandals and alert her on the exact location of the vandalisation. Despite this latest efforts of Shell to combat pipeline vandalism, pipeline vandalism and subsequent crude oil theft as reported by [3,4] has been on the increase as a result of obvious collaboration and collusion of security officers with oil thieves who are supposed to race to the scene of vandalisation, make arrest of the vandals and bring them to face the law. This obvious economic sabotage and corruption has compounded the menace of pipeline vandalism and crude oil theft which has left the Nigerian Federal Government aghast on how to tackle the problem.

The level of oil theft in Nigeria is becoming alarming and will continue to increase if no radical action is taken by the government and the IOCs. Many security and technological measures have already been implemented to stop oil pipeline vandalism and detect leakages and failure in oil pipelines but due to obvious human factor none of these wonderful measures and technologies had yielded the desired results. The design presented in this study is to enable oil pipeline and plant operators monitor the safety of oil pipelines installed remotely (especially oil pipelines above the ground and buried underneath). This proposed system should be able to detect an intrusion into the pipeline system early enough and alert the pipeline operators via SMS and email before the pipeline is vandalized and also be able to capture a video/photo footage of the vandalisation scene in case the vandals go ahead to vandalize the pipelines to steal crude oil . This will go a long way in reducing the theft of pipeline products, environmental degradation and also accidental deaths which often result from the explosion of those flammable substances when leakage occurs.

II. THE CHALLENGE OF PIPELINE VANDALISM TO NIGERIA

Pipeline networks are important parts of the national energy transportation infrastructure vital to the national economy. It is an indispensable means for conveying water,

gas, oil and all kinds of products. Undoubtedly, the pipeline project is one of the most important infrastructures in Nigeria as it stretches several thousands of kilometers and passes through cities, villages and rural communities across the country. These pipelines are operated at high pressure and any failure or damage poses a great danger to human health and properties, environmental and ecological disaster and interruption of gas or oil supplies [2]. The pipelines are prone to losing their functionality by any internal or external corrosion, cracking, third party intrusion and manufacturing flaws, thereby leading to damage, leakage and failure with serious economic and ecological consequences [2]. Third party mechanical damage has proven to be the most serious problem encountered by pipeline industries on their facilities located onshore [2]. Oil spill incidence through pipeline vandalism appears to be peculiar to Nigeria and has become rampant in recent times and if no urgent measures are taken by the relevant Nigerian agencies, the frequent pipeline cuts that continue to spill for weeks and months has the capacity of undermining Government's efforts at meeting its obligations in spill management. Pipeline vandalism and disruption of oil production activities regrettably are now integral part of oil and gas operations in Nigeria.

The enormous oil installations deployed in the Niger Delta region explains their vulnerability to vandalism. Presently, the Niger Delta region plays host to 600 oil fields of which 360 fields are onshore while 240 are offshore with over 3000 kilometers of pipelines crisscrossing the region and linking some 275 flow stations to various export terminals. It is pertinent to note that oil spills resulting from pipeline vandalism has continued to be a challenge, with most incidents along major pipelines and manifolds [5].

Table1 shows that for the period 1995-2005 for instance, Shell Petroleum Development Company one of the major oil operators in Nigeria recorded a total of 2944 oil spill incidents. The data reveals a noticeable increase from 235 oil spill incidents in 1995 to 330 in 2000. The least number of 224 oil spill incidents was observed in 2005. Also it was reported that about 250,000 barrels of crude is stolen daily for sale on the local and international black markets, reportedly costing the country about $6bn to $12bn annually. From 2002 to 2011, records show that about 18,667 incidences of vandalism occurred [6].

Table 1. Oil Spill Data: SPDC 1995-2005 [6]

Year	***Number Of Spills***	***Volume In Barrels (bbl)***
1995	***235***	***31,000***
1996	***326***	***39,000***
1997	***240***	***80,000***
1998	***248***	***50,000***
1999	***320***	***20,000***
2000	***330***	***30,100***
2001	***302***	***76,960***
2002	***262***	***19,980***
2003	***221***	***9,916***
2004	***236***	***8,317***
2005	***224***	***11,921***

Table 2 shows the most recent statistics of quantity of crude oil lost as result of pipeline vandalism from Oil Producers Trade Section (OPTS). From the table, you can see that a total of over 5 million barrels of crude oil was lost due to illegal bunkering facilitated by pipeline vandalism. The recent jetty explosion in Lagos was as a result of pipeline vandalism [6,7]. Furthermore, Nigeria National Petroleum Corporation (NNPC) posited that Nigeria lost about N163billion in three years to pipeline vandalism [2,8,9]. Pipeline vandalism has crippled fuel supply and incurred over N174billion in product losses and pipeline repairs [9].

Many lives have been lost as a result of explosions and fire coming from vandalized pipelines carrying crude oil and refined products when they become vandalized. The environment has also been degraded and many farmlands completely destroyed.

Table 2. Volume of Crude oil lost due to illegal bunkering as a result of vandalism: Oil Producers Trade Section (OPTS) January 2014 – March 2014 [10]

2014		
Month	*Security Related Deferment (bbls)*	*Loss Due to Oil Theft / Illegal Bunkering (bbls)*
Jan.	***4,679,301***	***2,172,341***
Feb.	***4,153,114***	***1,679,874***
Mar.	***9,534,642***	***1,253,825***
TOTAL	*18,367,057*	*5,106,040*

III. MATERIALS AND METHODS

A. Component Design

1.) Hardware Sub-System

The design and development of the system has both hardware and software requirements. The hardware sub-systems include the hardware modules used to realize the physical test-bed for the oil pipeline vandalism surveillance and monitoring system. The software sub-systems include the software modules used to realize the sensor initializations and communication, data transfers from the deployed test-bed to an online FTP Server, designated email addresses, and mobile phone numbers, data visualization from the FTP Server to web-based SCADA Server and clients at the Control room of the IOC so that the personnel of the IOC can view videos/photos captured from a vandalisation scene at the oil pipeline infrastructure.

The hardware sub-system is categorized into five (5) modules and they are as follows:

i. The Controller Module,

ii. The Sensors, Actuator and Surveillance Module,

iii. The Communication and Gateway Module,

iv. The SCADA Module, and

v. The Power Supply Module.

The block diagram describing the entire Hardware Sub-system is depicted in Fig. 1.

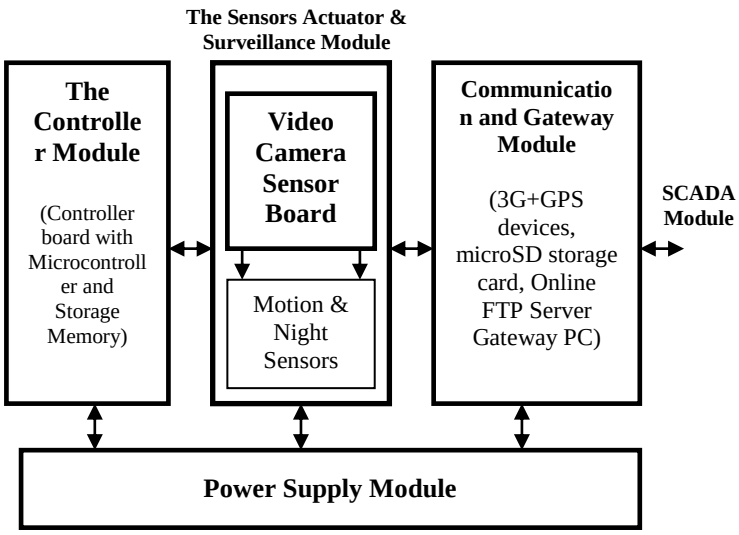

Fig. 1. The block diagram of the proposed system

3.1.1.1 *The Controller Module*

The Controller module is implemented using Libelium Waspmote™ wireless integrated circuit board referred to as Waspmote Pro v1.2 that works with different communication protocols (ZigBee, Bluetooth and 3G/GPRS) and frequencies (2.4GHz, 868MHz, 900MHz) and create links up to 12Km. Using the hibernate low power mode (0.06μA) it can save battery energy when not transmitting and be able to work even for years. In this project Waspmote controller board is connected to two other electronic boards - the Video Camera Sensor board and the 3G+GPS communication board. Fig. 2 shows the Waspmote controller board (top view) while Fig. 3 shows Waspmote controller board (bottom view). The three electronic boards connected together and powered by a Power Supply module (Lithium Rechargeable battery) as depicted in Fig.4.

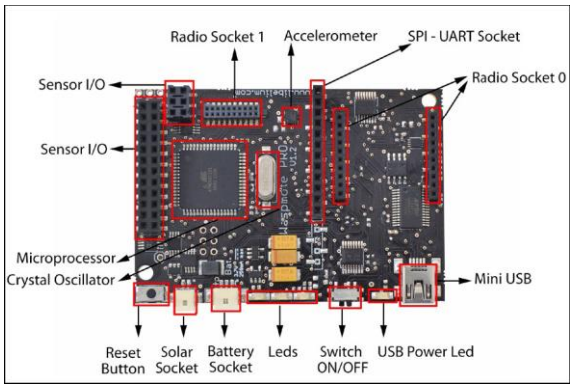

Fig.2. The Waspmote board top view[11]

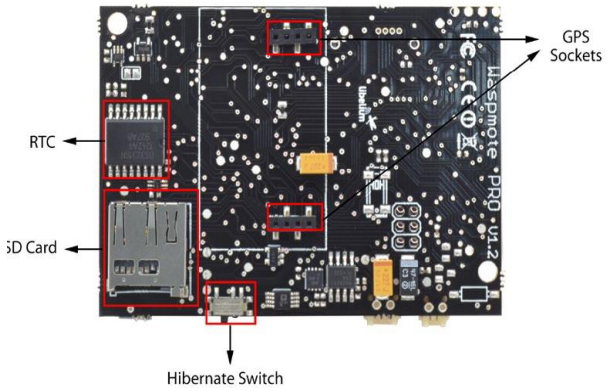

Fig.3. The Waspmote board bottom view[11]

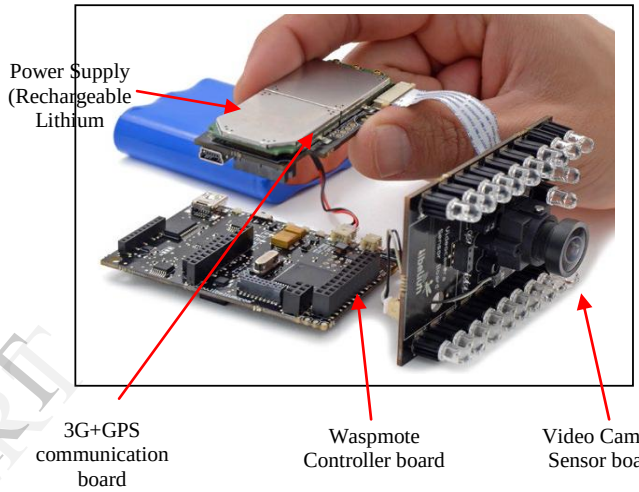

Fig.4. The Assembled three electronic boards used in the project

Waspmote board is implemented using ATmega microcontroller. The functions of microcontroller include powering the system automatically, initializing the 3G/GPS module, interpreting the received signals and sending the required signal to the 3G/GPS module. Waspmote is based on a modular architecture. The idea is to integrate only the modules needed in each device optimizing costs. For the reason, all the other modules (radios, sensor boards, etc) plug in Waspmote through sockets.

The modules that can be integrated in Waspmote are categorized as the following:

- 3G Module,
- Sensor Module (Sensor boards),
- GPS Module,
- Storage Module (SD Memory card), and
- ZigBee (802.15.4 modules).

3.1.1.2 *The Sensors Actuator and Surveillance Module*

This module contains the design and integration of the following components or sub-modules:

- The Sensors,
- The Actuator (i.e. the PIR motion/presence detector which detects the presence of a mammal within the defined perimeter (10-15 meters) of an oil pipeline) and,
- The Surveillance IP video camera board which houses the sensors (including the IP camera sensor), the actuator and 22 IR Light Emitting Diodes (LEDs)

The Sensors:

There are four (4) sensors altogether in this module:

1. The camera sensor,
2. The visible light (luminosity) or LDR sensor,
3. An IR Sensor, and
4. A presence sensor, which is Passive Infra-Red (PIR) sensor (this equally acts as the actuator sub-module).

Fig. 5 shows the camera sensor used in this module to record video and photo snapshot of the oil pipeline infrastructure when an intruder, mostly vandals, intrude into the defined perimeter of the pipeline. Fig. 6 shows the other remaining sensors used in this module; on the left is a luminosity sensor, which is a light-dependent resistor (LDR) with a 20 MOhm dark resistance and 5 to 20 kOhm light resistance. It has a spectral range of about 400 to 700 nm. It is used mainly to determine whether to power on the illumination LEDs. In the center is an IR sensor which acts as a current source, and outputs from 100 nA to around 70 mA over its full range. This sensor, which has maximum sensitivity at 860 nm, is used to determine when to use an IR cut filter in the camera to avoid pink washout in the images. The visible light (luminosity or LDR) and IR LEDs Sensors were chosen because they aid the module to work both day and night; this feature is required for continuous monitoring and surveillance of oil pipelines at both day and night, especially in the Niger Delta region where most of the reported cases of vandalisation occurred in the night[b].

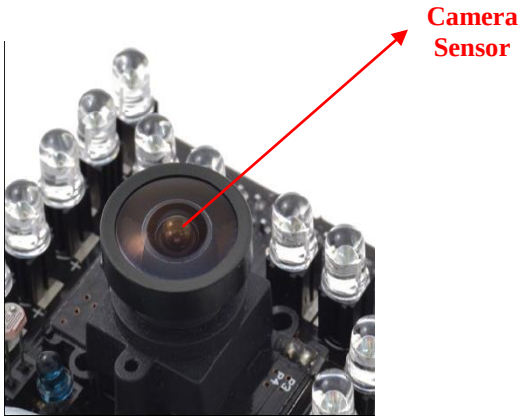

Fig.5. Camera Sensor with IR cut filter and lens

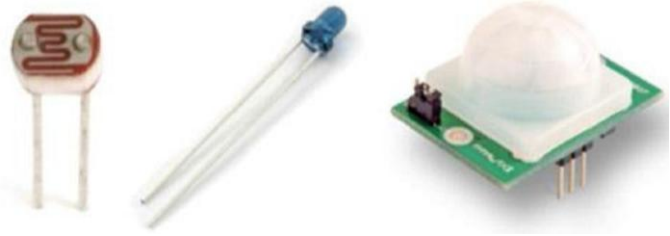

Fig.6. The Sensors

On the right is the PIR sensor (which equally acts as the actuator to trigger the camera to record scene of vandalisation) which is used to detect presence of people or animals. It is optimized to sense emissions from mammals around 36°C, and can generate an interrupt sent to the communications board to alert the system to record information.

Tables 3, 4, 5 and 6 show the general specifications of the Camera sensor, Luminosity sensor, IR sensor and PIR presence sensor respectively.

Table 3. Specifications of the Camera Sensor[11]

Width (min.):	21mm
Height:	21mm
Length:	17mm
Max resolution:	610x180 for pictures, 320x210 for video
Image Sensor Analog Voltage:	3.3V
Image Sensor Digital I/O Voltage:	2.8V (from Waspmote 3G/GPRS board)
Temperature range:	
Operating temperature**:**	-30^0C to 70^0C junction temperature
Stable image**:**	0^0C to 50^0C junction temperature
Consumption current (active):	18mA
Angle of View:	70^0

Table 4. Specifications of the Luminosity Sensor[11]

Resistance in darkness:	20MΩ
Resistance in light (10lux):	5~20 KΩ
Spectral range:	400 ~ 700nm
Operating Temperature:	-30ºC ~ +75ºC
Minimum consumption:	0uA approximately

Table 5. Specifications of the IR Sensor[11]

Peak sensitivity wavelength:	860nm
Collector dark current (Ee=1mW/cm^2):	100nA
Operating Temperature:	-25ºC ~ +85ºC

Table 6. Specifications of the Presence Sensor (PIR)[11]

Height:	25.1mm
Width:	21.3mm
Length:	28.0mm
Consumption:	100µA
Range of detection:	6 ~ 7m
Spectral range:	~ 10µm

The Actuator:

This Actuator is the Passive Infra-Red (PIR) presence sensor depicted in Fig. 6 (right). This component or sub-module is necessary to prevent vandalism through pipeline intrusion detection. Any threat to the oil pipeline infrastructure is preemptively detected by this actuator device by triggering an interrupt which starts up the surveillance IP camera mounted on the video surveillance board to record video/snapshots of the area within the vandalisation. The interrupt can also trigger an SMS alert or alarm to be sent to the SCADA Control Station or designated mobile phone for necessary action to be taken to arrest the vandals apart from the video/snapshots taken by the IP surveillance camera.

The Surveillance IP camera on board:

The Surveillance IP camera is housed by the Waspmote™ Video camera Sensor board depicted in Fig. 7 alongside other sensors. The IP camera is a camera sensor sitting on board the Waspmote Video camera Sensor board shown in Fig.4.5. The Video Camera Sensor Board allows to Waspmote to take pictures and record video along with the Waspmote 3G+GPS board. The board includes 22 IR LEDs, divided in two blocks controlled each one by transistors, to give extra illumination and record with few light or in the night. To eliminate the IR distortion when the board is used with natural light, the board has a filter exchanger with an IR light filter.

The board has two sockets for a LDR and an IR photodiode. With the information of these sensors the users can select the proper filter and, if is necessary, to use the IR LEDs.

The Video Camera Sensor Board also includes a presence sensor (PIR), to generate an interruption on Waspmote and take a picture or record a video when a person passes by; this feature is specially designed for security and surveillance applications such as oil pipeline vandalism monitoring and surveillance.

Fig. 7. Waspmote Video Camera Sensor board[11]

Libelium Waspmote video camera board was chosen for the Surveillance module because it has the capability to house all the sensors (including the IP camera sensor, the actuator and can be integrated with other modules - Communication module such as the 3G+GPS sub-modules in a single housing along with a rechargeable lithium ion battery and external solar panel.

Secondly, Libelium Waspmote video camera board was chosen because it can allow the transfer of the captured video/snapshot data from the vandalized oil fields to a safe online FTP Server for onward transfer to the SCADA Module (Server and Client devices) for data visualizations to provide Common Operational Picture (COP) for the IOC personnel.

Specifications for Waspmote Video Camera Sensor Board:
The general specifications for the Waspmote Video Camera Sensor board that houses all the sensors and the IP surveillance camera is shown in Table 7. Table 8 depicts the electrical characteristics of the Waspmote Video Camera Sensor board.

Table 7. Specifications for the Waspmote Video Camera Sensor board[11]

Weight (with sensors):	13g
Dimensions:	73x53x1.3mm
Temperature range:	-25 ^{0}C – 70 ^{0}C

Table 8. Electrical Characteristics of the Waspmote Video Camera Sensor board[11]

IR LED power voltages:	3.6V – 1.2V (from battery)
IR cut filter exchanger power voltages:	3.6V – 1.2V (from battery)
Image Sensor Analog Voltage:	3.3V
Image Sensor Digital I/O Voltage	2.8V (from Waspmote 3G/GPRS board)
LDR and IR photodiode Sensor Voltage:	3.3V
PIR Sensor Voltage:	3.3V
Maximum admitted current (continuous) for sensors:	200mA
IR LED maximum current (continuous) for block 1:	1A
IR LED maximum current (continuous) for block 2:	1A

3.1.1.3 The Communication and Gateway Module

The Communication and Gateway module is very critical for the successful transmission of the captured data from the remotely deployed oil pipeline vandalism surveillance monitoring system to a safer storage location such as an online File Transfer Protocol (FTP) Server located on the internet. This is necessary to prevent tampering or destruction of the captured video/image file from the vandalisation scene. The Communication sub-module is the 3G/GPRS communication sub-module while the Gateway sub-module is the FTP Server computer which is located remotely on the internet. This module in details is broken down into the following sub-modules or components:

1. The 3G module, its antenna, a GSM SIM module and microSD storage card,
2. The GPS module and its antenna, and
3. FTP Server PC on the internet

The 3G sub-module:

The 3G sub-module for Waspmote allows sensor networks and M2M devices to connect to the Cloud by using high speed Wideband Code Division Multiple Access (WCDMA) and High Speed Packet Access (HSPA) cellular networks in the same way as Smartphones do. This makes possible sensor

nodes send not only discrete sensor information such as temperature or humidity (which can be encoded using just a single number) but also complex streams of information such as photos and videos as required in this research project where real-time videos and photos captured from vandalized oil pipelines can be used to trace and apprehend the criminals and oil thieves to face justice. The 3G sub-module for the Waspmote sensor platform offers speed rates of 7.2Mbps in

Table 9. Comparative difference between the 3G and the GPRS sub-modules for Waspmote[11]

Model	3G (SIM5218)	GPRS (SIM900)
Download speed:	7.2Mbps	0.02Mbps
Upload speed:	5.5Mbps	0.01Mbps
FTP:	Yes	Yes
FTPS (Secure) :	Yes	No
HTTP:	Yes	Yes
HTTPS:	Yes	No
TCP/UDP Sockets:	Yes	Yes
Electronic Mail (Email) :	Yes	No
GPS:	Yes (A-GPS + S-GPS + NMEA)	No
Video Camera:	Yes (Photo + Video)	No
Video Calls:	Yes	No
Protocols:	3G, WCDMA, HSPA, UMTS, GPRS, GSM	GPRS/GSM
Frequency Bands:	850,900,1800,1900,2100MHz	850,900, 1800,1900MHz
SD Card:	Yes (up to 32GB)	No

download mode and 5.5Mbps when uploading information to the Cloud. This is an incredible increase compared with previous cellular technologies such as GPRS which rates were of 0.02Mbps and 0.01Mbps respectively [11]. Table 9 shows the comparative difference between 3G and GPRS sub-modules for Waspmote. Each Waspmote sensor node may integrate at the same time a medium range radio such as 802.15.4/ZigBee/Bluetooth/Wi-Fi and one long range 3G radios. This 3G sub-module comes also with an internal GPS what enables the location of the device outdoors and indoors combining standard NMEA frames with mobile cell ID triangulation using both assisted-mobile (A-GPS) and mobile-based (S-GPS) modes.

The 3G communicating sub-module is specially oriented to work with Internet servers implementing internally several application layer protocols which make easier to send the information to the cloud. We can make HTTP and HTTPS (secure mode) navigation, downloading and uploading content to a web server. In the same way FTP and FTPS (secure).

The captured images/video from the video camera board IP camera can be sent or transmitted to the recipient at the SCADA module using any or the combination of the following four (4) approaches or methods:

1. Via 3G sub-module to its microSD card to an internet FTP Server,
2. via 3G sub-module to an email as an attachment,
3. via XBee DigiMesh device to a Meshlium Router for onward transmission to a WAN connection, and,
4. Via Wi-Fi device to an internet FTP Server

In this research project, the first and second methods were chosen because of two reasons: (1.) it is the fastest approach and (2.) it is the cheapest approach. Table 10 shows the sending time (in seconds) for the four (4) approaches.

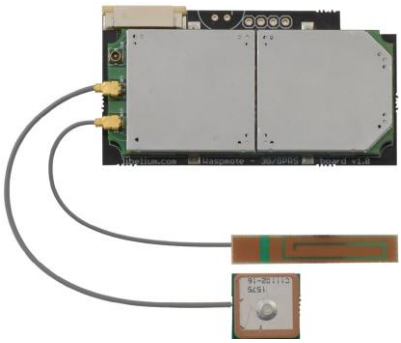

Fig. 8 The 3G and GPS sub-modules integrated with their antennae

Table 10. Sending time of the four approaches to send captured image/video file [11]

Radio	Destination	Time (s)
3G	Upload to FTP Server	16
	Attach in an email	18
XBee DigiMesh	Send to Meshlium Router	150
Wi-Fi	Upload to FTP Server	90

GPS sub-module:

The Waspmote 3G board is equally attached a GPS receiver using Assisted GPS (A-GPS), which is capable to geotag captured data (video/photo) from the remote oil pipeline infrastructure using information from the cell tower. Fig. 8 shows the GPS sub-module attached with the 3G sub-module on Waspmote 3G+GPS board. Fig. 9 shows the GPS sub-module with antenna separately.

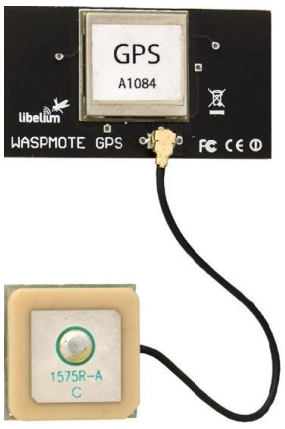

Fig. 9. The Waspmote GPS sub-module with its antenna

The GPS module gives us information about the following parameters with respect to the location on oil pipeline where vandalism has occurred:

- Latitude,
- Longitude,
- Height,
- Speed,
- Direction,
- Date/time, and
- Ephemeris.

Secure Digital (SD) card for the 3G sub-module:

A Secure Digital (SD) card is a tiny memory card used to make storage portable among various devices, such as car navigation systems, cellular phones, eBooks, PDAs, Smartphones, digital cameras, music players, camcorders, and personal computers. An SD card features high data transfer rate and low battery consumption, both primary considerations for portable devices. It uses flash memory to provide nonvolatile storage, which means that a power source is not required to retain stored data.

An SD card is about the size of a postage stamp and weighs approximately two grams. It is similar in size to a multimedia card, but smaller than older memory card types such as the Smart Media card and the Compact Flash card. Both MMC and SD cards provide encryption capabilities for protected content to ensure secure distribution of copyrighted material, such as digital music, video, and eBooks. SD cards are available with storage capacities as high as 2 GB, 4G and up to 32 GB.

SD cards are more rugged than traditional storage media. They have an operating shock rating (basically, the height you can drop them from and still have them work) of 2,000 Gs, compared to a 100-200 G rating for the mechanical drive of the typical portable computing device. This translates to a drop to the floor from 10 feet, as compared to a single foot for the mechanical disk drive. Both MMC and SD cards use metal connector contacts, instead of the traditional pins-and-plugs, so they aren't as prone to damage during handling.

The SD card was jointly developed by Matsushita, SanDisk, and Toshiba. Fig. 10 shows the Transcend microSD™ 2G card used in the project being inserted into the Waspmote 3G sub-module.

Storage Requirement for the 3G sub-module:

The required amount of SD storage for the 3G sub-module is dependent on camera's following parameters:

1. image resolution,
2. frame rate and
3. compression ratio and
4. days of retention.

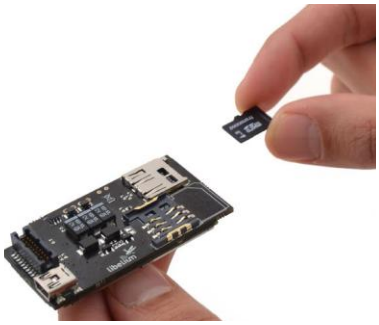

Fig. 10. The Transcend microSD™ 2G card used in the project being inserted into the Waspmote 3G sub-module

A security camera might typically be set up at 320x240 image resolution, one frame every 2 seconds, and 7 days of image retention. The required storage space is about 3.5 GB:

12 KB x 86400/2 x 7 = 3.5 GB.

Increasing the image resolution to 640x480 will quadruple the storage usage to 14GB. However, setting up motion detection may significantly lower the storage usage.

Setting up IP camera to use motion detection can significantly reduce storage usage, that is the reason PIR motion/presence sensor or detector was used in this project to reduce capturing images/video real-time (at all time) but only captures images/video when an interruption is generated by the PIR motion/presence sensor when an intruder/vandal intrudes into the crude oil pipeline system in order to vandalize it.

Protective enclosure for the integrated Oil pipeline vandalism monitor and surveillance system:

The Waspmote integrated circuit boards from Libelium are open and not protected with special protective casings such as IP65, IP66 and so on; so the electronic components inside the boards could be damaged if deployed outdoor as a result of exposure to environmental conditions such as water, light, dust, humidity or sudden changes in temperature. In this project, an IP65 protective design was designed using aluminum metal casing measuring 162 x 171 x 91 cm, one side of the casing used transparent plastic material to allow the IP camera sensor to take photo/video. The integrated circuit boards was positioned such that that the Waspmote video camera sensor board is positioned perpendicular to the base of the Aluminum protective enclosure. This will allow the PIR motion/presence sensor to obtain maximum signal and the camera to obtain video/image in correct positions.

Also two (2) perforations were made in the metal area to allow the two (2) antennae of 3G+GPS sub-modules to obtain wireless aerial signals without obstructions. The flexible solar panel was included inside with a transparent plastic material to enable it obtain solar energy from the external environment. Fig. 11 shows a typical IP65 enclosure targeted in this design.

Fig.11 The typical IP65 aluminum and transparent protective casing used in this project

FTP Server PC (Database and Web Server):

FTP (File Transfer Protocol) is a popular method of transmitting or transferring multimedia files from a client device or machine to a server using the so-called FTP Client software. FTP stands for File Transfer Protocol, which is basically a network protocol used to transfer files from one computer or host to another within a network (TCP-based network) through internet. The first FTP client applications were command-line applications that were developed before operating systems had graphical user interfaces but are still in use with most of the operating system such as Windows, UNIX, and Linux. Since then, number of FTP clients and automation utilities has been developed for computers, serves, hardware and also for gadgets like mobile devices.

FTP or File transfer protocol can be used for exchange and transfer of files between computer accounts, between an account and a desktop computer.

To initiate transfer of files with FTP, a program is used called the 'Client', which establishes a connection to the remote computer which runs the FTP 'server' software. Once the remote connection is established, the client is free to choose any file to send or receive the copy of files. To establish a successful connection to a FTP server, the client requires a username and password that has been set by the administrator of the server.

FTP works on a client-server architecture in which the server component is known as FTP daemon that is responsible for listening to the FTP requests from the remote clients. Once a request is received, the FTP server executes the login and establishes the connection. Within the duration of the entire session, the FTP server executes any of commands sent by the FTP client.

An internet or online FTP Server or PC was chosen in this research project to receive and store the captured video/photo from the remote oil pipeline field.

The importance of using FTP Server is as follows:

(1.) to act as gateway between the deployed surveillance monitoring system and the SCADA module,

(2.) to store the captured file for later viewing at the SCADA module and,

(3.) to protect the captured data/file from destruction or tampering in the event the camera is detected and destroyed by the pipeline vandals.

The stored data/file in the FTP Server can be used later to trace, apprehend and arrest the suspected vandals. In this research project a CPANEL internet hosting account was purchased at a yearly lease because an internet CPANEL account has a FREE FTP Server with unlimited storage space for a minimal yearly fee of N2500.00 (less than 16 US dollars per year); this is far cheaper than one setting up his own FTP Server. Also, this CPANEL account has a web server (Apache) which can be used to process the captured video and photo file/data and display them at SCADA module for visualization by the personnel of the oil company.

The following parameters or settings are needed for an FTP account before an FTP Server can communicate with the Waspmote video camera board and 3G+GPS sub-modules:

1. FTP Server name (DNS) or Internet Protocol (IP) Address,
2. FTP Server Port (which is usually TCP port 21),
3. FTP mode which can either be proactive or passive (Most IP cameras use passive which set at 1, and proactive is set at 0; so we choose passive, i.e. 1)
4. Username which is usually the same with the CPANEL *account username, and*
5. *Password, which is usually the same with the CPANEL account password.*

The FTP Server is equally in this same CPANEL hosting account with MySQL database Server and Apache Web Server on the internet, so information such as captured video/photo location, name, time/date captured can be stored in the MySQL database Server while the Apache Server can help to process SCADA user requests by accessing to the captured data/information stored in the FTP Server and MySQL Server and send same to the requesting SCADA users via SCADA web interface. Fig. 12 depicts the interaction amongst the FTP Server, the MySQL database Server, the Apache Web Server and the SCADA requests/queries from users.

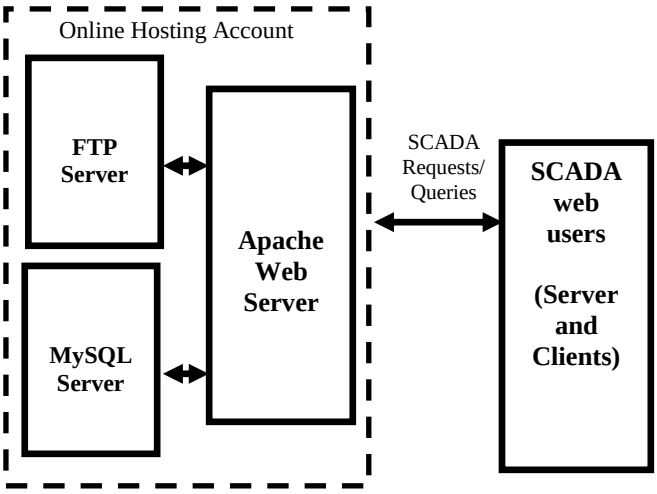

Fig.12. The functional block diagram showing interactions amongst FTP, MySQL and Apache Web Servers with SCADA users

3.1.1.4 The SCADA Module

Supervisory Control And Data Acquisition (SCADA) is a combination of standardized protocols and technologies used to view or visualize the captured data from a remote field and also to effect some control functions over the deployed remote surveillance monitoring system. SCADA is needed by the oil companies that installed the pipelines so that its personnel can monitor the captured data (video/photo) sent by the 3G sub-module in the event of a generation of interrupt by the PIR presence sensor or actuator. SCADA module includes the following:

1. *Server PC with a broadband internet connection, and*
2. *Client PCs or portable devices such as PDAs, Smartphones.*

Fig.13 depicts the typical SCADA module envisaged for this research project integrated with internet-based FTP Server gateway PC and other modules. The SCADA Module is also needed by the personnel of the oil company to be able to affect some control on the pipeline surveillance monitoring system either to force the Waspmote video IP camera to disable the PIR interrupt in order to capture video or take photo snapshot of what is happening at a particular period of time. For this to be possible, the PIR interrupt of the PIR sensor/actuator must be disabled.

The SCADA Server and clients must be internet-ready and should be able to connect to the internet 24/7 using broadband internet connectivity such as HSPA or other networks to be able to view captured video/photo data from the FTP Server gateway PC.

Fig.13. The functional block diagram showing interactions amongst FTP, MySQL and Apache Web Servers with SCADA users

3.1.1.5 The Power Supply Module

The power Supply module includes the 6600mAh rechargeable battery model with an external solar panel power source to recharge it in case the battery energy gets drained. The 6600mAh will last for approximately 16-18 hours when deployed outside to provide power backup for the other modules. The Solar panel is needed to recharge the 6600mAh rechargeable battery since pipeline surveillance and monitoring system will be deployed remotely for several days. Fig. 9 depicts the 6600mAh rechargeable battery used to power the pipeline surveillance and monitoring system while Fig. 14 is the 7.2V-100mA flexible solar panel as an external power source to recharge the battery.

Fig.14. The 6600mAh rechargeable battery used to power the entire hardware sub-system

The functional block for the proposed oil pipeline vandalism surveillance monitoring system is depicted in Fig.4.15.

2.) Software Sub-System

The software sub-system is needed for the successful implementation of the proposed pipeline vandalism detection and surveillance system. The following operations will be utilized using the software sub-system:

1. Coding of commands for data acquisition from the remote qualitative sensors and actuator;
2. capturing of the vandalisation photo/video from the remote oil field using the wireless surveillance video camera, storing of the captured video file into the SD card of the video camera and transmitting the captured video/image file to the wireless Sensor Gateway (FTP Server or Router);
3. storage and management of the sensed and captured data from the sensors and video camera into the local storage of the Sensor Gateway (FTP Server or Router) and synchronizing the data into an external database or File system;
4. Configuration of all the qualitative sensors on the sensor boards;
5. Configuration of all the parameters for the communication interfaces (3G/GPRS, GPS);
6. Management of battery power of sensors, sensor boards and Sensor Gateway using different power-saving modes;
7. Management of the protocol stack to handle all protocols used for communication;
8. Configuration of operating microkernel which allows the wireless sensor actuator network to have access to the operating system;
9. The Server-Client web-based visualization interface to enable the SCADA Server and client users to connect and visualize real-time the sensed data from

the remote qualitative sensors and actuator.

The software sub-system for the entire project is divided into three major segments or modules:

- **Module 1**: This software module handles the Monitoring/Surveillance of oil pipelines by Waspmote video camera board and sensors (including the actuator) and the eventual transfer and storage of the captured photo and video files to a remote online FTP Server;
- **Module 2**: This is an online web-based application to handle the visualization of the captured photo and video files stored in online FTP Server using a web-based SCADA application in PHP and HTML and,
- **Module 3**: This software module will handle the intercommunication protocols and Control System that will enable SCADA users (from the web-based application) control the operations of the remotely deployed Waspmote video camera board and sensors from SCADA Control Room.

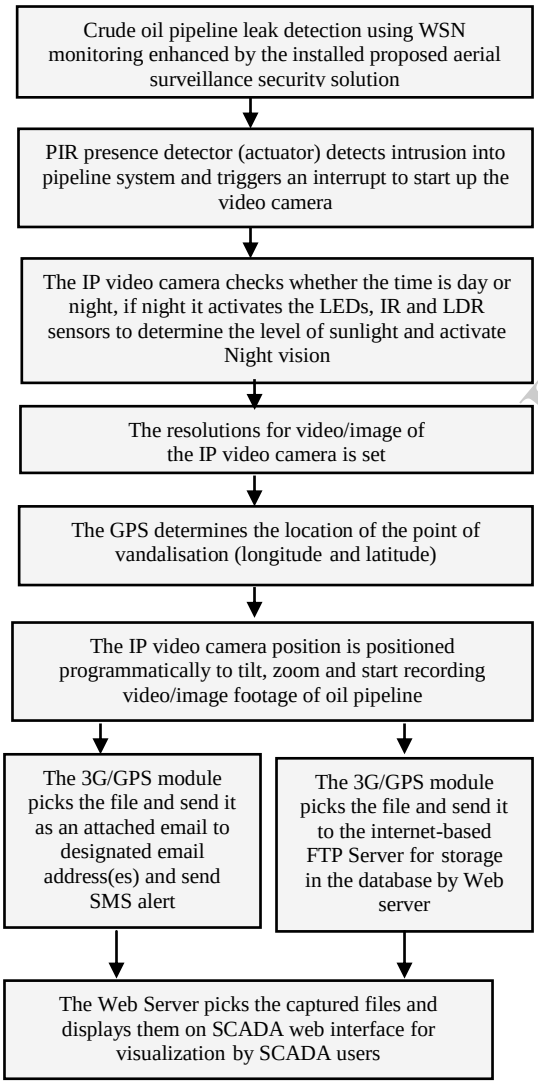

Fig.4.15. The functional process block diagram of the oil pipeline vandalism surveillance monitoring system

IV. CONCLUSION

This paper provides insights on the way an automated electronic surveillance and monitoring system can be used to detect, alert and dispatch video/photo footage of an oil pipeline vandalisation incident from a remote location to oil pipeline operators at the control station.

A method for providing automated detection for pipeline with remote monitoring and location specification was achieved. A PIR sensor was used to detect early intrusion of vandals into the pipeline system in order to communicate to the pipeline operators via SMS and email alerts so that a proactive action such as shutting down the pipeline valves or calling in the security patrol team can be initiated to mitigate loss. The major benefits of this study include early detection of pipeline intrusion before pipeline is damaged which can lead to reduction in financial losses and alleviation of environmental degradation as well as the possibility of the system to take action towards successful arrest and prosecution of the culprits by a way of capturing the vandalisation video footage which can serve as exhibit in the court of law.

V. FUTURE WORK

We will continue work in this research towards successful completion of the building of the prototype, the deployment to real oil pipeline system in the Niger Delta region and finally carry out performance evaluation of the project via simulations and comparison of simulated data and data from previously deployed oil vandalism detection systems. We sincerely believe our contributions will help fight crude oil bunkering and pipeline vandalism that has become the order of the day in the Nigerian oil rich Niger Delta region.

REFERENCES

[1] Saharareporters, “A nation in search of pipeline safety ”, Accessed online at http://www.saharareproters.com/nigeria on June 18, 2014.
[2] G.N Ezeh,N. Chukwuchekwa,J .C. Ojiaku and E. Ekeanyawu, "Pipeline Vandalisation Detection Alert with Sms", Int. Journal of Engineering Research and Applications Vol. 4, Issue 4(Version 9), April 2014, pp.21
[3] T.John, “TUC backs NUPENG on alleged JTF’s connivance with bunkerers”, Daily Sun, Thursday, 16, August, 2012, pp.10.
[4] B. Ojediran, and J. Ndibe, “Oil Spill Management: SPDC and the Environment, 2005.” Unpublished.
[5] Bakpo, F. S.and Agu, M. N, "Automatic Data Collection Design For Real-Time Detection Of Oil-Spillage Disasters In Nigeria",Nigerian Journal Of Technology, vol. 28 No.1, pp. 54, March 2009.
[6] L.P.E YO-ESSIEN, "Oil Spill Management In Nigeria:Challenges Of Pipeline Vandalism In The Niger Delta Region Of Nigeria",pg.16. Accessed Online at http://Ipec.Utulsa.Edu/Conf2008/Manuscripts%20&%20presentations%20received/Eyo_Essien_2.Pdf On June 23, 2014.
[7] Lagos Jetty explosion caused by pipeline vandalization. Accessed online at http://www.informationng.com on June 13, 2014
[8] Thisday, “NNPC lost about N163billion in the space of three years to pipeline vandalism”, accessed online at http://www.thisdaylive.com on June 13, 2014.
[9] NNPC, “How pipeline vandals cripple fuel” supply”, Accessed online at http://www.nnpcgroup.com/public relation on June 24, 2014.
[10] OPTS,"Suspects Arrested, 60 Convicted for Oil Theft, Vandalism", Accessed online at Suspects Arrested, 60 Convicted for Oil Theft, Vandalism on June 23, 2014.
[11] Libelium, “Video Camera Technical Guide”, Document version: v4.1, April 2013, pp.34.G. Eason, B. Noble, and I.N. Sneddon, “On certain

integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955.

AUTHORS' PROFILES

Engr. 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 Enugu, Nigeria. His PhD work is on Security of Wireless Sensor Network (WSN) in Oil and Gas field monitoring Niger Delta Region. He had his Masters Degree in Control Systems and Computer Engineering at Nnamdi Azikiwe University in 2010 and B.Sc Degree in Computer Engineering at Obafemi Awolowo University Ile-Ife in 2001. He has authored several conference and research journal publications

Mr. Samuel Chibuzor Asogwa is a Ph.D research scholar in the Department of Computer Science Nnamdi Azikiwe University Awka, Nigeria. He is currently lecturing at the Department of Computer Science Michael Okpara University of Agriculture Umudike, Nigeria. He had his Masters (MSc.) in Computer Science at Ebonyi State University Abakaliki, Nigeria in 2011 and Bachelor of Engineering (BEng.) in Computer Science and Engineering at Enugu State University of Science and Technology (ESUT), Nigeria in 1999. He was the former Acting Head of Department of Computer Science, Renaissance University, Enugu, Nigeria. He has several years of teaching and research experience.

Engr. Frank Ekene Ozioko is the Director of ICT office Enugu State University of Science and Technology (ESUT) and Lecturer Department of Computer and Information Science, ESUT, Nigeria. He had several years of experience in university ICT administration and engineering as well as in teaching and research.