Framework for Integrated Oil Pipeline Monitoring and Incident Mitigation Systems

Johnson Eze[1], Christopher Nwagboso, and Panagiotis Georgakis

Faculty of Science and Engineering
University of Wolverhampton
Wolverhampton, WV1 1LY, United Kingdom

ABSTRACT

Wireless Sensor Nodes (motes) have witnessed rapid development in the last two decades. Though the design considerations for Wireless Sensor Networks (WSNs) have been widely discussed in the literature, limited investigation has been done for their application in pipeline surveillance. Given the increasing number of pipeline incidents across the globe, there is an urgent need for innovative and effective solutions for deterring the incessant pipeline incidents and attacks. WSN pose as a suitable candidate for such solutions, since they can be used to measure, detect and provide actionable information on pipeline physical characteristics such as temperature, pressure, video, oil and gas motion and environmental parameters. This paper presents specifications of motes for pipeline surveillance based on integrated systems architecture. The proposed architecture utilizes a Multi-Agent System (MAS) for the realization of an Integrated Oil Pipeline Monitoring and Incident Mitigation System (IOPMIMS) that can effectively monitor and provide actionable information for pipelines. The requirements and components of motes, different threats to pipelines and ways of detecting such threats presented in this paper will enable better deployment of pipeline surveillance systems for incident mitigation. It was identified that the shortcomings of the existing wireless sensor nodes as regards their application to pipeline surveillance are not effective for surveillance systems. The resulting specifications provide a framework for designing a cost-effective system, cognizant of the design considerations for wireless sensor motes used in pipeline surveillance.

Keywords: Pipeline Monitoring; Critical Infrastructure Protection (CIP); Wireless Sensor Networks (WSN); Wireless Sensor Node (Mote); Data Fusion; Pipeline Surveillance

1. INTRODUCTION

Following increasing terrorism, militancy and cyber-attacks, the need for Critical Infrastructure Protection (CIP) was demonstrated on February 12, 2013 when President Obama issued an executive order for cyber security critical infrastructure protection. Oil pipelines as critical infrastructures need adequate layered security for proper protection. Recent events show that pipeline threats are no longer mere corrosion and operational errors as witnessed two decades ago. Concerns for pipelines are now terrorists, militants and cyber-attackers who hack into Supervisory Control and Data Acquisition (SCADA) and other pipeline monitoring systems.

Common pipeline monitoring techniques include fiber optics, satellite systems, Unmanned Aerial Vehicles (UAV), Seismic sensors, patrol teams, mass balance and Wireless Sensor Network (WSN) techniques. WSN technique is very promising and has attracted a lot of interest as evident in Al-Kadi et al. [1] and Yu and Guo [2]. Due to wide application of WSN, designers have always designed generic WSN motes that could fit various purposes. However, in order to achieve better efficiency for specific tasks, it is sensible that analysis of optimization factors for such system design is done. Zilan and Tavli [3] as well as Augusto, Vieira and Di [4] discussed existing WSN motes and Microcontrollers but none of these is adequate for pipeline monitoring. With rising global pipeline insecurity, there is need for WSN mote designed for pipeline

[1] Corresponding author: Tel.: (+44) 7504758364; E-mail: Johnson.Eze@wlv.ac.uk

surveillance. This work discusses the requirements and features of a WSN mote for pipeline surveillance.

In pipeline surveillance, satellite method discussed in Peng, Yun and Honghong [5] is widely used in USA and Canada because majority of their pipeline incidents are due to excavation damages. In Europe however, Unmanned Aerial Vehicles (UAV) method is attracting some interests since they could be used in mission critical tasks that present high safety risks for people [6]. Also fiber optics method is often used owing to high sensitivity of fiber optic sensors as applied to leakage detection. WSN comprises motes otherwise known as wireless sensor nodes that are interconnected wirelessly to measure and detect physical quantities like temperature, pressure, sound, video, etc. WSN offer many benefits over other techniques. It is low cost, reliable, available, functional in adverse conditions and compatible with other methods thus providing redundancy and reliability [2]. Pipelines by nature span wide geographical areas and therefore need robust real-time monitoring for adequate security. The low-cost nature of WSN makes it very adequate for this task. However, power sustainability and multimedia transmission are among some challenges of WSN in meeting wide area coverage and real-time demands of pipeline surveillance. Implementing distributed architecture and data fusion in WSN design as well as choosing high resource motes and good topology effectively enhances pipeline surveillance systems.

The rest of the paper is structured as follows: Section 2 discusses threats to pipelines and forms of attacks. Section 3 presents related work and WSN applications, while Section 4 elaborates on their requirements. Section 5 proposes a framework for pipeline monitoring and the research methodology is given in section 6. Finally, several propositions are presented in section 7, while section 8 concludes the paper.

2. BACKGROUND

Most literature identify as causes of pipeline failure, corrosion, operational failures, material and construction defects, external interference and natural disasters. External interference dominates others and encapsulates third party interference, such as construction work, or malicious attacks like theft, vandalism and sabotage [7]. This paper discusses causes of pipeline failure under human and natural threats since there is an observable trend showing that leak detection systems are more suitable for natural threats while external interference monitoring systems are more suitable for human threats.

2.1. PIPELINE THREATS AND DETECTION

Human threats could come in the form of vandalism, sabotage, operational error, and construction works. Some attacks on pipelines are caused by groups of people who are in dispute with Government, or pipeline operators. This could be militant groups that attack pipelines as in the case of Niger Delta, in Nigeria [8]. Also, due to sheer greed or poverty, people resort to tampering with pipelines for personal gains. Instances include the case of theft from a pipeline passing underneath Deputy Prime Minister’s house in London [9], and persistent cases of pipeline sabotage in Nigeria [8]. Moreover, there have been growing concerns that terrorists might begin to use oil and gas pipelines as weapons of mass destruction [10]. Operational errors contribute considerably to pipeline failure either due to system failure, or technicians and pipeline operators at work [11]. Also, systems put in place to monitor corrosion as well as Supervisory Control and Data Acquisition (SCADA) systems could fail leading to pipeline failure. Concluding the discussion of human threats, construction work is a major cause of pipeline failure in the developed countries. In USA, pipeline incidents through construction work are mitigated using pipeline right-of-way surveillance, satellite surveillance, public awareness activities and one call system. Other methods are acoustic monitoring and fiber-optic sensors buried along the pipeline.

Deterrence of terrorists, vandals and thieves can be achieved by detecting common weapons used by these groups including explosives, guns, knives and other sharp objects. Vandals use axes, explosives and other sharp objects while thieves are likely to use drills, and containers or tanks to siphon fuels. Technologies used to detect metallic and non-metallic weapons and explosives include Terahertz imaging, Neutron scattering, X-Ray scattering and Millimeter Wave (MMW) imaging. Terahertz detection has about 10 times better spatial resolution compared to MMW systems since THz radiation electromagnetic wavelength is about 10 times shorter than MMW radiation [12]. Terahertz imaging can detect objects from a distance of 0.5km which is deemed sufficient for proactively initiating defensive actions.

Natural threats to pipelines are mainly corrosion and natural disasters such as earthquakes and landslides. Pipeline corrosion is an electro-chemical process that changes metal back to ore as a result of a difference in potential between two points having a path for the flow of current which results in one of the points losing metal [13]. Different types of corrosion have been identified such as uniform attack, pitting, inter-granular or exfoliation, crevice, filiform, galvanic corrosion and stress corrosion. Coating prevents corrosion in pipelines, and in most cases cathodic protection is also used to further protect pipelines. Intelligent or smart pigs are used to gather pipeline data and detect leakages and metal loss. Corrosion detection technologies available include Visuals, Eddy Current, Ultrasonic, Radiography, Thermography, Robotics and Automation, Data Fusion and Sensor Fusion. In pipeline systems, pigging and eddy current are widely used to detect corrosion. Natural disasters such as earthquakes and landslides, due to their unpredictability, also constitute threats to pipelines. Scientists have reported the potentials of using seismic data to predict earthquakes and landslides but accurate predictions are still not possible.

2.2 FORMS OF ATTACKS

Often, pipeline operators make new connections to pipelines to expand or modify their existing system. This usually involves a shutdown (3 days or more) of the pipeline system and purging the oil or gas to ensure a safe atmosphere. Hot tapping is an alternative process used to establish pipeline connections while the pipeline remains in service. It involves attaching a branch connection and valve on the outside of an operating pipeline, then cutting out the pipeline wall within the branch and removing the wall section through the valve [14]. It is used for corrosion repairs, upgrade work or other modification works on pipelines with no downtime. Alas, this industrial technical process is now being used by thieves to siphon fuel from pipelines.

Explosive attack is carried out using explosives such as dynamites, C-4, HMX, RDX, and TNT. These attacks are carried out by militants, vandals, saboteurs' terrorists or thieves. Most attacks on pipelines using explosives are done when the pipeline is not in operation. Explosive attacks carried out while pipelines are in operation result in fire and could claim the attackers' lives.

Tampering attacks, as used in this article, refer to attacks by third parties which neither involves hot taps nor explosives, still they are aimed at stealing fuels from the pipeline. This often involves drilled holes on the pipeline, cutting the pipeline with hacksaw, or third party tampering with well head, clamps, valve settings and flanges [15].

3. RELATED WORKS AND WSN APPLICATIONS

Pipeline surveillance is an important research field owing to the economic importance of pipelines as well as the health and safety implications of pipeline incidents. WSN has been identified as a cost-effective solution for pipeline surveillance. Besides pipeline surveillance, other applications of WSN in the oil and gas sector include leakage detection, Tank Level Monitoring, Equipment Condition Based Monitoring (CBM), Pipeline Pressure Relief Value Monitoring (PRV), Refineries Pressure Relief Value Monitoring (PRV) and Wellhead Automation and Monitoring. Although most pipeline surveillance systems have focused on leak detection [1];[16], few pipeline surveillance systems have tried to address threat detection in pipelines. Sun and Wen [17] investigated pipeline threat detection and security by developing a pre-warning system for pipeline security using multi-seismic sensors. Liang et. al [18] studied risk assessment of pipelines based on malicious and accidental threats. The authors used fault tree to determine the risk assessment index and thereafter used Self Organizing Maps (SOM) to classify sections of pipelines into various risk levels. Jawhar et al. [19] presented an ideal WSN architectural model for pipelines while Seema and Reisslein [20] developed Node architectures for Wireless Video Sensor Networks Platforms (WVSNP). The authors discussed hardware/software requirements for WVSNP. Various models of WSN have been developed, with the dynamic linear configuration model being the most suitable for pipelines due to its linear nature Mohamed and Jawhar [21] and Jawhar et. al [19].

Wireless sensor networks have wide range of applications in the present-day technology. WSN used for intelligent transportation will differ from that used for telemedicine in various ways. Effective WSN for pipeline surveillance should detect leakages and threats to pipelines and localize such events with certain degree of accuracy. Three key design features to consider while designing effective WSN for pipeline surveillance, include adequate wireless mote, deployment topology and data mining technique. Oil and gas pipelines by nature traverse large geographical areas. As such, wireless motes used for pipeline surveillance should employ power optimization strategies to conserve energy while being able to transmit over a considerable distance. In WSN design, factors considered depend on the specific task at hand even though a lot of factors are generic for various tasks.

4. GENERAL REQUIREMENTS FOR WSN

In general, some factors to consider while designing a sensor node are as discussed below:

***Power Considerations* -** Power source is a crucial factor to consider while designing Wireless Multimedia Sensor Network (WMSN) motes. As these devices are wireless, they either need some stored energy in form of battery or generate their own power. They could generate energy through solar cells. However, due to size requirements, integrating solar cell is presently a challenge. Inter-sensor communications require a lot of energy. WMSN motes should use less power to enable their batteries last at least a year. As a rule of thumb, Seema and Reisslein [20] recommended that wireless motes should utilize less than 500 mW instantaneous power and less than 100 mW power during idle times. To sustain energy for the WMSN, it is recommended that energy harvesting (a process by which energy is derived from the environment) should be adopted. Although there are many energy harvesting technologies such as thermal, magnetic, radio frequency, vibration based, and under-water, solar energy harvesting has proved more efficient and more widely used. Also, energy optimization approaches should be adopted in WMSN designs. Three energy optimization techniques in WSN discussed by Boudhir et al. [22] including sensing, processing and communication energies.

Sensing Energy – Most WSNs sense physical quantities such as temperature, humidity, pressure, radiation etc. These sensing activities utilize power, so regulating the frequency of activities by these WSNs conserves energy.

Processing Energy – In a computer system, the three units that utilize most of the energy are the processor, display and hard disk units. The processor and radio transceiver use most of the energy in WSNs. Dynamic Voltage Scaling, an emerging technology for reducing power utilization in hand held devices is good for WMSN energy optimization.

Communication Energy – Media Access Control (MAC) is a technique used in both computer and sensor networks to control and manage data transmission. One of the fundamental tasks of MAC is to control data transmission in Networks so that two competing nodes do not transmit at the same time. Different MAC protocols have been used for optimizing energy utilization in wireless environments[23]. Sensor – MAC (S-MAC) is a MAC protocol designed to reduce energy utilization in WSN [24]. It reduces energy utilization by dividing the node time into periodic sleep and listening time. Timeout-MAC (T-MAC) has also been proposed [25]. This improves on S-MAC by reducing the listening time and transmitting the data in bursts of packets within the small listening time. Also, *IEEE 802.15.4* is the standard MAC protocol for low power, low data rate wireless networks. It is the standard in most motes at present. It achieves low power utilization via low power transmission, small frame size and energy-efficient Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) algorithms.

Another energy optimization technique in WSN is the wireless charging system presently being developed. Qi standard was developed by Wireless Power Consortium (WPC) and is a good solution for WSN energy issues [26].

Partitioning System Approach - There is a need to find the right balance in the trade-off between processing data at the sensor node and processing at the base station. When data is processed at the base station, it saves the sensor node a lot of power since the base station has more computational capability and no power constraint. On the other hand, transmitting unprocessed data require more energy than processed data which is less in size.

Routing Protocols –Various routing protocols used in WSN have been designed to optimize energy during data transmission. Some hierarchical protocols such as Low-Energy Adaptive Clustering Hierarchy (LEACH), **T**hreshold-Sensitive **E**nergy **E**fficient Sensor **N**etwork protocol (TEEN) and Adaptive Periodic Threshold-sensitive Energy Efficient sensor Network (APTEEN) minimize energy utilization during data processing and transmission [22] and [27]. Figures 2 and 3 are comparisons of energy utilization and longevity for these protocols respectively [27].

Communication Standards and Bandwidth Issues **-** In wireless communication, bandwidth is a critical factor for consideration. Presently, Wi-Fi, ZigBee, Bluetooth and Ultra-Wideband (UWB) are the four protocols used for wireless communication. Lee et al. [28] carried out a comparative study of the four wireless technology standards. Table 1 shows an extract. While ZigBee is the best for WSN due to its low power utilisation, Wi-Fi is the best for mobile devices and other computer networks due to better signal rate and improved bandwidth transmission. Although Bluetooth, UWB and Wi-Fi have signal rate of 1Mb, 110Mb and 54Mb respectively, ZigBee has only 250Kb/s, a big limitation to the use of ZigBee for Multimedia transmission. Yet, researchers are optimistic that low cost nature of ZigBee as a motivating factor could spur researchers to develop this technology for effective video transmission. A comparison of the power utilisation of these wireless technology standards is discussed in details in [28].

Processing Speed and Memory / Storage Capacity **-** Processing speed is a major factor in rating the performance of a WMSN mote. Ordinary WSN motes deal with data like temperature, light, pressure, humidity etc. while WMSN involves voice, images and videos that are usually bulky and take more storage space. WSNs need moderate-speed CPUs but bulky data associated with WMSN require more processing power for capturing, processing and transmission. As more processing speed is required for WMSN motes, more storage space is also needed for storage.

Cost **-** Wireless sensors are low cost in nature due to the availability of cheap Complementary metal oxide semiconductors (CMOS). WSN solutions must maintain low cost to remain competitive among other solutions. According to Seema and Reisslein [20], the cost of an ideal WSN mote should be much less than $50.00 or £33.00 as at 2011. Table 2 shows the Comparison of Size, Weight and Cost of latest Motes in 2012 [29].

Table 1: Comparison of Wireless Technology Standards

Wireless Standard				
Attributes	**Bluetooth**	**UWB**	**Wi-Fi**	**ZigBee**
IEEE Spec	802.15.1	802.15.3	802.11a/b/g	802.15.4
Max Signal Rate	1Mb/s	110Mb/s	54Mb/s	250Kb/s
TX Range	10m	10m	100m	10 -100m
Nominal TX Power	0-10 dBm	-41.3 dBm	15-20 dBm	-25 - 0 dBm
Max No. Of Nodes	8	8	2007	> 65000

Table 2: Comparison of Size, Weight and Cost of Latest Motes in 2012

S/No	**Name of Motes**	**Size in (mm)**	**Weight (g)**	**Cost per node**
1	MicaZ [8]	58*32*7	18	US$99
2	TelosB [9]	65*31*6	23	US$99
3	IRIS [10]	24.23*24.23*7.5	3	US$115
4	SHIMMER [11]	44.5*20*13	10	US$262
5	TinyNode [12]	30*40	--	US$180
6	Sun SPOT [13]	41*23*70	54	US$750
7	Cricket [14]	~58*32*7	~18	US$225
8	LOTUS [15]	76*34*7	18	US$300

4.1 Considerations factors for WSN motes for Pipeline Surveillance

The main purpose of any network is to integrate and share information. Sensors are specific to the physical quantities they detect and no single sensor can detect all physical quantities. It is therefore important that WSN motes are able to integrate data from various sensors for the purpose of data mining. Effective motes should be able to integrate various sensors capable of detecting various physical quantities for the purpose of data mining to confirm leakages or threats to pipelines. Thus, key selection parameters for WMSN mote for pipelines surveillance are sensing modality, power optimization, localization capability, transmission range and security technology employed. Having extensively discussed power optimization strategies in section 4.1, we dedicate the rest of this section to discussing the remaining selection parameters for WMSN motes.

4.1.1 Sensing Modality

Sensors are devices that receive physical quantities and convert them to electrical energy. The physical quantities received vary in different sensors. The sensing modalities chosen or considered for WSN or mote design depend on the physical information required. There are various sensors in existence [30] but the ones that have been commonly used for pipeline leak monitoring include; acoustic, chemical, magnetic, optical, piezoelectric, thermal and ultrasonic sensors. Multi-modal sensing is an interesting but challenging research area since no single sensor can detect all physical quantities as mentioned earlier. Multi-modal sensing ability of motes will ensure that false alarms are avoided. In this regard, WSN motes with multimedia capability are more adequate for pipeline surveillance. Micro-Electromechanical Systems (MEMS) is one of the most promising technologies of the 21st century that enables various sensors to be combined into a single Integrated Circuit (IC) chip [31]. Traditional pipeline monitoring using sensors according to Owojaiye and Sun [32] are done either with steady-state detection methods or transient detection method. Steady-state detection work with the concept that most pipeline parameters such as pressure, flow, temperature, and vibration remain constant unless there is an anomaly such as leakage or third-party damage. This method uses pre-defined thresholds to detect pipeline incidents and attacks. Unlike the former, transient detection methods are used where the pipeline parameters change rapidly over time. The Real-Time Transient Model (RTTM) also known as dynamic model based system, mathematically models the one-dimensional hydraulic behaviours of pipelines. They work with the principle of conservation of mass, momentum, energy as well as the equation of state for the fluid Bai Yong [33]. The conservation laws are described by non-steady partial differential equations in which hydraulic parameters such as pressure, temperature and flow of liquid are functions of time and distance along the pipeline. This method requires that pipeline parameters readings be taken at both the inlet and outlets of pipelines. Preferably, taking measurements of pipeline parameters at designated points along the pipeline will increase efficiency of the system.

As early as 1987, Billmann and Isermann [34] demonstrated the use of this method to detect leakage in pipeline. Since then, researchers including Colombo et al [16]; Giustolisi et al [35]; Vitkovsky et al [36] and Egyptian et al [37] have done remarkable work on transient method of pipeline leak detection which is known for its high sensitivity.

4.1.2 Event localization

Event localization capability is an important design consideration for motes. As discussed in section 5 below, motes are able to localize pipeline incidents using GPS sensors. Various localization techniques are used but it has been shown that using GPS in every mote may not be cost effective. Some motes could therefore determine their positions relative to GPS enabled motes [19].

4.1.3 Transmission Range

Adopting a good deployment topology for pipeline WSN ensures that the network can cover the geographical area spanned by the pipeline system while conserving transmission energy. Common topologies used for WSN design are tree/cluster, mesh, ring and star topologies. However, pipelines are linear in nature and none of these topologies would give optimum performance for pipeline surveillance. Accordingly, Jawhar et al. [19] proposed a linear topology for pipelines considering power, transmission range, security and other factors. Also, the design should establish if direct access or multi-hop is used. While direct access requires only one transmission for the receiving node to be accessed, multi-hop requires that the packets are forwarded by one or more node before the receiving node. Generally, good deployment topology results in high performance of the WSN.

4.1.4 Security Technology

The importance of security in WSN cannot be over-emphasised. A breach in the security of WSN could result in the breakdown of the entire WSN. Notable security technologies that are employed to secure WSN were summarised by Yang et al. [38] as encryption / key management, certification and routing protocol security. Encryption is indispensable in WSN since network data travel from one place to another and could be intercepted by an adversary. In WSN cryptography, numerous key management mechanisms are employed to encrypt data. The performances of five popular encryption schemes used in WSN were evaluated in Ganesan et al. [39] as seen in Perrig [40] and it was concluded that MD5 and SHA-1 incur more overhead than RD4, RD5 and IDEA algorithms. Moreover, Zhang et al. [41] presented a classification and comparison of key management protocols used in WSNs as seen in [40]. No key management protocol can be selected as the best over others, however protocols employing pairwise key management showed best results in power consumption and communication overhead as well as high security [42].

Certification in network security could be identity authentication or message authentication. It is a way of confirming the integrity of the party or message received. Certification could be implemented using symmetric or asymmetric encryption algorithm. From the energy conservation perspective, symmetric cryptosystem is preferred to asymmetric method in WSN because less power is required. However, considering network security, asymmetric cryptography perform better [38].

In routing protocol security, categories employed include Data-centric secure routing protocols, Location-based secure routing protocols, Hierarchical-based security routing protocol and Multipath transmission-based routing protocols. As discussed in section 4, hierarchical routing protocols such as LEACH, TEEN and APTEEN perform very well in terms of energy conservation. Multipath routing protocols on the other hand are known for higher security resistance than others.

4.2 Data Fusion

Data fusion is a design strategy used to achieve two important design goals; (i) to optimize energy in wireless motes (ii) to implement data mining and extract useful information from data for decision making. Although implementation of data fusion for the purpose of energy optimization is expected to occur at various senor nodes (especially Aggregation and Forwarding Nodes (AFN) [43]), majority of data fusion implementation for data mining should occur at sub-stations or the base station. For the former's design goal, routing algorithms are designed such that data fusion reduces the amount of network communication, and thus the amount of power consumed for data transmission. The latter's design goal however, aims at acquiring complimentary information from various sensors to increase the accuracy of the overall decision making process. This is because no single sensor can capture all information about the surroundings and sensor information are most times uncertain, inaccurate and sometimes conflicting [44].

Popular technologies that have been used to realize data fusion include Ambient Intelligence (AmI), Service Oriented Architecture (SOA), Multi-Agent System (MAS) and Enterprise Application Integration (EAI). These are distributed architectures aimed at integrating subsystems to improve performance. Tapia et.al [45] developed FUSION@ based on SOA in order to integrate multi-agent systems and build AmI based system. FUSION@ provides better integration with services and applications which is lacking in previous frameworks for MAS. It also offers computational capability and intelligent computation which are lacking in most SOA frameworks. Although FUSION@ provides integration with services and applications, it was not developed for heterogeneous system. Services laYers over Light PHysical devices (SYLPH) [46] on the other hand is developed to integrate heterogeneous WSN based on various radio technologies. Hardware-Embedded Reactive Agents (HERA) [47] just like SYLPH employs heterogeneous devices with reduced resources to save CPU time, memory size and power consumption. HERA however, has an edge over SYLPH since it adds reactive agents and reasoning mechanism to make it context aware. HERA embeds agents directly into WSN nodes and their services can be invoked from other nodes. It also uses Case-Based Planning model [48] that solves problems using previous solutions to similar problems.

Although these platforms discussed employ distributed systems to implement data fusion for better decision making, they are not developed for multimedia applications and are therefore not suitable for WMSN applications.

5. REQUIREMENTS FOR PIPELINE SURVEILLANCE AND MONITORING

Efficient and effective pipeline monitoring is the dream of any pipeline operator as this prevents wastage through leakages and forestalls pending pipeline incidents. However, such monitoring system is hard to come by as a lot of resources are needed to actualize it. To protect the environment and the people while forestalling economic loss, the pipeline operators put series of protections in place. Among these according to PHMSA [49] are "customized leak detection technology deployment; periodic risk-based assessment and defect repair prioritized by environmental and safety consequences; corrosion management; pipeline right-of-way surveillance; public awareness activities; emergency preparedness and coordinated response, liaison efforts with emergency responders; and a review and incorporation of lessons learned from accident analysis and investigations". Thus, for good pipeline monitoring system, the resources and factors discussed below should be considered.

Information Communication System/Flow Computers **-** A Robust Information Communication System is a sine qua non of pipeline inspection. Computer systems are needed, to receive, analyse, store and retrieve pipeline information regarding leakages. To detect leakages, these computers process flow pressure, volume and temperature difference between two reference points then generate alerts if the value is more than certain threshold.

Location Detection/GPS – Event localisation is very important in pipeline surveillance. Global Positioning Systems (GPS) are used to identify positions of incidents when patrol teams collate pipeline data for analysis. They offer instant communication for incidents in pipeline system. GPSs are often integrated into sensor nodes to enable them give accurate positions of pipeline incidents.

GIS for Pipeline Route Information **-** Geographic Information System (GIS) database or data are needed for pipeline route information preferably in a map or table dividing the pipeline routes into sections. With pipeline routes categorised into sections, it is possible to assign different levels of risks or threats to different pipeline sections. GIS-based map enables us to tell if data or population distribution in a certain geographical region is clustered, dispersed, or randomly distributed. Also, it enables response team to trace reported pipeline incidents easily. It is a resourceful tool used by National Pipeline Mapping System (NPMS) of USA for pipeline management [50].

Round – the – Clock Availability **-** Thieves and vandals would attack pipelines when no one will notice and this could be day or night. As such, Pipeline monitoring systems should be operational both day and night. To achieve such availability, power efficiency and reliability are crucial factors to be considered as earlier discussed.

Low Cost System **-** Most pipeline systems cover a wide area and require great efforts and resources to monitor. For instance, USA has about 2.6 million miles pipeline transportation system which is capable of going round the earth more than 100 times [51] while Nigeria has about 5,120 Kilometres of pipeline. Therefore, effective monitoring of such area of infrastructure would require low cost devices to cover the infrastructure at reasonable cost.

Compatibility with other systems **-** A lot of solutions for pipeline monitoring systems are in existence today. The ability of a system therefore to work with other products for pipeline monitoring purpose is considered as an advantage. This not only compliments the other system but also provides needed redundancy. Modular design of motes as in the case of CITRIC mote where image processing unit is separated from the networking unit promotes compatibility [20]. In the same vein, designers could design motes that work with standard Wi-Fi cameras such that video signals could be received wirelessly and processed before being transmitted to base station.

Others (Sensors) - Sensors are indispensable in pipeline monitoring. Some sensors used for this task include motion, seismic, acoustic, fibre optic and camera sensors. Cameras are very useful in monitoring threats and could be used to detect leakages as well. Motion sensors could be used to design smart motes which are only triggered by specific events. Individuals and moving vehicles approaching pipelines as well as pipe leakages generate seismic waves that could be detected with seismic sensors. Fibre optics is widely used in communication industries and offers numerous advantages including immunity to electromagnetic interference, high temperature performance, large bandwidth, high sensitivity, environmental ruggedness and distributed sensing.

6. METHODOLOGY

In this work, literature search was conducted on related researches with the keywords pipeline surveillance, pipeline monitoring, wireless sensor networks, wireless sensor network motes, critical infrastructure protection and wireless multimedia sensor networks and relevant articles reviewed accordingly. Following the literature review, a survey was conducted in the pipeline industry to ascertain the level of third-party interference (TPI) on pipelines. The survey revealed that TPI or external interference constituted majority of the pipeline failures. In a bid to model a system to manage and mitigate TPI and external interference on TPI, Universal Modelling Language (UML) was used to develop Use Case Scenarios for each type of pipeline attack using the Case-based Planning model concept. Thereafter, a framework and architecture for WMSN for pipeline monitoring termed IOPMIMS was developed. Finally, data collected from CONCAWE website were simulated to investigate the performance of the proposed system. Three machine learning algorithms including Neural Network (NN), Support vector Machine (SVM) and Decision Tree (DT) were investigated. Results obtained shows that SVM gave the best performance with 91.2% accuracy while NN and DT gave 63% and 57% accuracy respectively.

7. PROPOSITIONS

Extensive study of pipeline attacks has been carried out and various use case scenarios were developed for each type of pipeline attack using the Case-based Planning model concept. Due to limited space required for this publication, only one example of many use cases developed, “general use case scenario” is given.

7.1 General Use Case Scenario for Pipeline Monitoring System

7.1.1 Description: The general use case scenario shown in Figure 1 describes how an attacker (Vandal or Thief) is detected before damage to the pipeline takes place. This is irrespective of the means of transportation, or mode of attack on the pipeline.

7.1.2 Actors: The actors include; (1) Attacker (2) System Administrator (3) Security officer

7.1.3 Basic Event Flow:

1. The attacker approaches the pipeline
2. The sensors (seismic and motion sensors) detect the presence of the attacker
3. Signal is generated and video camera is initialised
4. Video recording starts as well as transmission to the internet and base station
5. Video analysis is done by the Decision Support System (DSS)
6. Other sensor data such as pressure and volume (rate of flow) are collated and fused
7. Threat and location of threat to the pipeline is confirmed and threat level assigned
8. Alert is generated and sent to the security officers or various stakeholders.

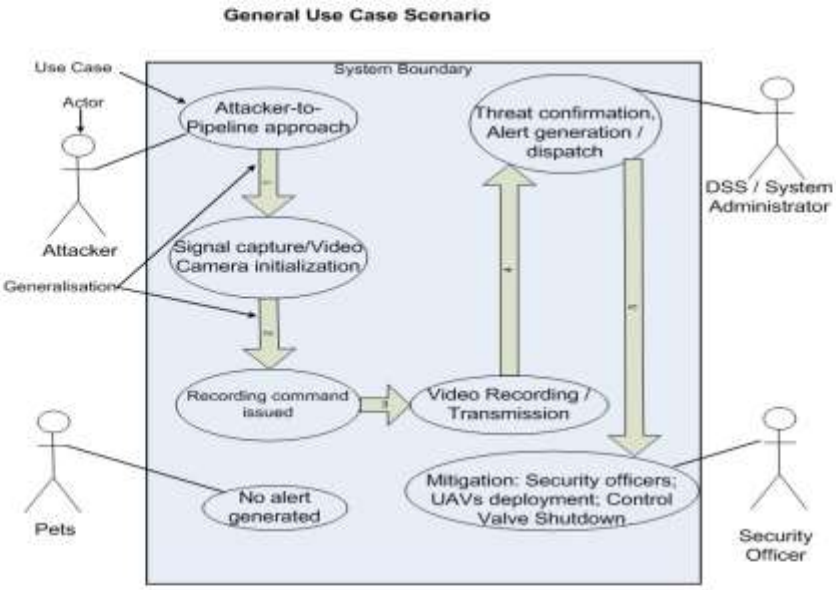
General Use Case Scenario
Use Case
Actor
System Boundary
Attacker-to-Pipeline approach
Threat confirmation, Alert generation / dispatch
DSS / System Administrator
Attacker
Signal capture/Video Camera initialization
Generalisation
Recording command issued
Video Recording / Transmission
Pets
No alert generated
Mitigation: Security officers; UAVs deployment; Control Valve Shutdown
Security Officer

Figure 1: General Use Case Scenario for Pipeline Monitoring Using WSN

7.2 Proposed WMSN Node Architecture

An ideal WMSN Node comprises Power Supply Unit (PSU), Processing, memory, transceiver and sensing units [4] and [29]. PSUs are usually batteries, designed to sustain motes for long period of at least a year. A mote's processing unit, the microcontroller unit (MCU) is responsible for controlling sensors, gathering and processing sensed data, executing WSN applications, and managing communication protocols and algorithms. The MCU consists of the processor, memory, non-volatile memory and interfaces such as SPI, UART, GPIO, counters and timers[4]. Merits of MCU over microprocessors are faster speed, more reliability and lower cost. MCUs attributes include number of bits, memory size, flash memory, operating voltage, current, power mode, number of ADC and timers. It is recommended that at least 32 bit MCU should be used in order to meet the high computation requirement of WMSN. Based on the requirements discussed in sections 4 and 5, we have designed a conceptual architecture of an ideal WMSN mote for pipeline monitoring as seen in figure 2 below.

The communication or transceiver unit of a mote is used for the transmission and reception of signal in a WSN. IEEE802.15.4 is the technology of choice for WSN and uses ZigBee technology. Wi-Fi would have been a great option for WMSN considering the huge bandwidth required. However, the power usage of Wi-Fi is a serious limitation to this. Most common chips employed in WSN today such as CC1000, CC2420, CC2500, and CC2480 from Texas Instruments use the IEEE802.15.4 ZigBee standard. We advocate dual Wi-Fi-ZigBee radio integration as recommended by Seema and Reisslein [20] for effective multimedia transmission. Some advantages of ZigBee over other wireless technologies include low power usage, and low cost. Major limitations of ZigBee include low data rate and lack of interoperability with existing devices unlike Bluetooth technology. Though Mohamed and Jawhar [21] provided redundancy using a combination of wired and wireless connections, our work provides redundancy using dual ZigBee/Wi-Fi transceiver radio.

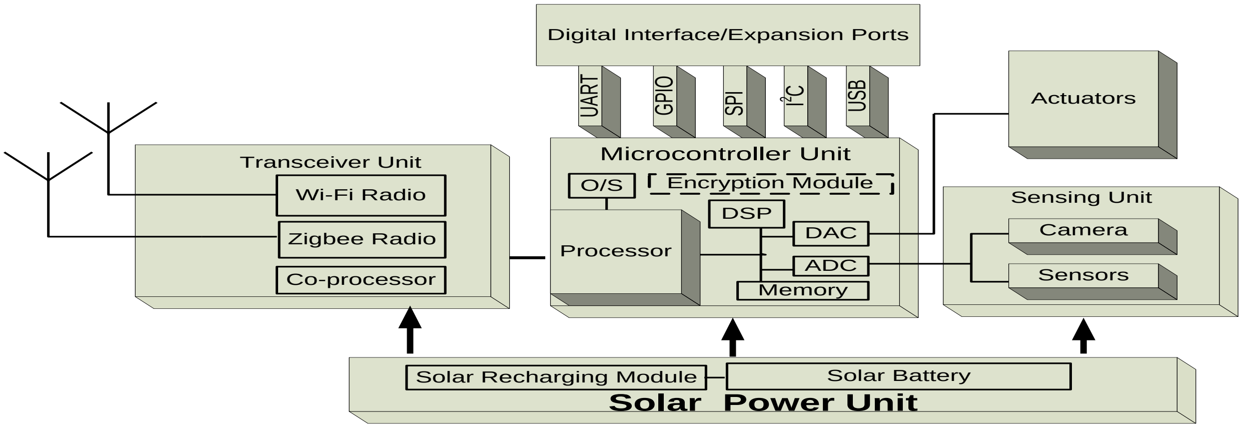

Figure 2: Conceptual architecture of an Ideal WMSN Mote for Pipeline Monitoring.

7.3 PROPOSED INTEGRATED OIL AND GAS PIPELINE MONITORING AND INCIDENT MITIGATION SYSTEM (IOPMIMS)

The basic concept of IOPMIMS is to use MAS to integrate heterogeneous sensors for pipeline surveillance. Prospective sensor nodes for IOPMIMS would use the architecture depicted in figure 2 to effectively process and transmit high resource intensive data such as multimedia data. The WMSN architecture presented has the capability to acquire signals from various sensors such as seismic, motion and cameras sensors. The dual radio composition improves efficiency in multimedia transmission via Wi-Fi and power usage via ZigBee. Thereafter, an MAS embedded in AFN nodes performs data fusion on these signals at designated sub-station and the base station to confirm if certain events constitute a threat to the pipeline. With the concept of distributed system, the AFNs at sub-stations aggregate the data and fuse them before uploading them online or forwarding to base station. The general architecture for IOPMIMS is shown in figure 3 below.

In addition to the preliminary aggregation of data at the substation, the MAS at the base station collates information from other devises such as GPS, wireless camera equipped drones, pipeline flow meters and pressure sensors for threat and leakage detection. Upon detection of threat or leakage in the pipeline system, decision is taken by the system and actionable information or alerts are sent to security personnel or pipeline operators.

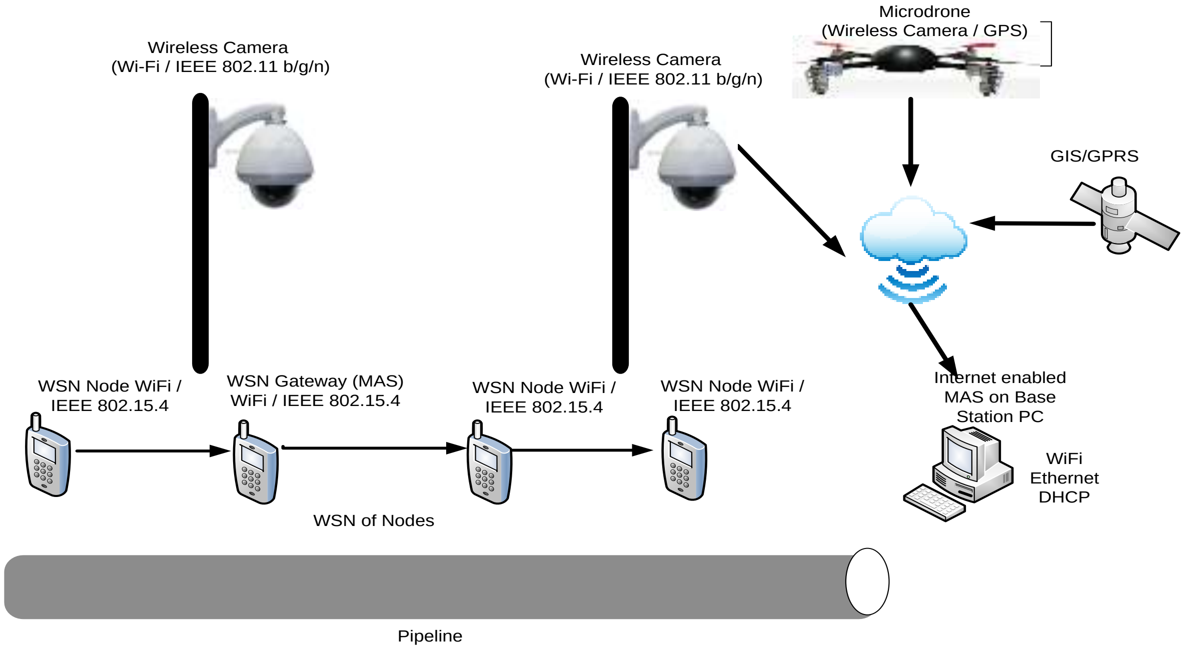
Wireless Camera
(Wi-Fi / IEEE 802.11 b/g/n)
Wireless Camera
(Wi-Fi / IEEE 802.11 b/g/n)
Microdrone
(Wireless Camera / GPS)
GIS/GPRS
WSN Node WiFi / IEEE 802.15.4
WSN Gateway (MAS) WiFi / IEEE 802.15.4
WSN Node WiFi / IEEE 802.15.4
WSN Node WiFi / IEEE 802.15.4
Internet enabled MAS on Base Station PC
WiFi
Ethernet
DHCP
WSN of Nodes
Pipeline

Figure 3: Conceptual architecture for IOPMIMS

Shortcomings of existing motes and suggestions to address them

The data analysis above highlights the need for effective pipeline monitoring against intrusion. WSN motes though widely used for monitoring have some shortcomings limiting their usage for pipeline monitoring as discussed below:

Most existing WSN motes have batteries that cannot last for more than one year. It is recommended that WMSN motes use solar power, wireless rechargeable batteries or both to sustain the motes for longer duration. Low bandwidth problems experienced in multimedia communication could be addressed with the integration of ZigBee and Wi-Fi transmitters in WMSN motes. These two technologies were tested and confirmed to have negligible interference with each other[52]. With this design, small data for physical quantities are transmitted via ZigBee while large volumes of multimedia data are transmitted via Wi-Fi.

Video recording and analysis is essential for pipeline monitoring to confirm remote incidents thereby avoiding false alarms. Thus, integration of Cameras be it standalone or built-in are crucial for WMSN. Though WSN motes are generally low cost in nature, a lot of these are needed to cover lengthy pipelines traversing a geographical region. Thus, WMSN motes must be very cheap in order to cover lengthy pipelines.

8. CONCLUSION

Security experts have advocated for layered security for CIP and an integrated approach as provided by WSN is a great means of providing layered security. The requirements for effective pipeline surveillance have been critically reviewed in this paper. Based on the review focusing on the need for proactive protection of pipeline, IOPMIMS has been proposed. This proposition is unique because IOPMIMS is a concept that uses distributed systems, MAS and Case-based reasoning to provide proactive protection to pipelines. Distributed system concept enables AFNs at sub-stations to interact with one another as well as the base station to share information. The MAS feature on the other hand enables the system to collate data from heterogeneous wireless devices for more informed decision. Moreover, through case-based reasoning, the system can use previous trained data to detect pipeline threat and leakages.

This paper demonstrated how effective WSN for pipeline surveillance could be realized by selecting appropriate wireless sensor node, adequate deployment topology and adequate data mining technique. Such system should implement MAS and SOA to integrate heterogeneous sensors so that data from cameras, pressure sensors, flow meters and other sensors could be used to detect pipeline threats and leakages. We have identified some shortcomings of existing WSN motes in terms of pipeline monitoring and given some measures to address them. The requirements and components of motes that make them adequate for pipeline surveillance have been discussed. Due to the nature of this task, an ideal mote for pipeline surveillance should be a WMSN mote that could deal with resource intensive data associated with multimedia data processing. Thus, this should be a mote with at least 32 bit MCU since these utilize less power than 16-bit and 8-bit MCUs in the order of about half of 8-bit MCU power. Also to overcome issues associated with transmission of resource intensive multimedia data, researchers should put more efforts in designing an MCU with dual ZigBee and Wi-Fi transmitters. With this, multimedia data could easily be sent to the internet through Wi-Fi while taking advantage of ZigBee's low power utilization for other communication. Thus, motes designed with the WMSN architecture presented will have improved power efficiency as well as improved multimedia data transmission. Integration of heterogeneous multi-agent sensors, application of case-based reasoning and implementation of data fusion on the output of various sensors will ensure that there is no false alarm experienced.

Simulation of the proposed WMSN architecture for Pipeline Monitoring motes to find the best machine learning algorithm for data fusion and decision support system indicates that SVM gives the best performance with an accuracy of 91.2% over NN and DT.

REFERENCE

[1] T. AL-Kadi, Z. AL-Tuwaijri, and A. AL-Omran, "Wireless Sensor Networks for Leakage Detection in Underground Pipelines: A Survey Paper," *5th Int. Symp. Appl. Ad hoc Sens. Networks*, vol. 21, no. 0, pp. 491–498, 2013.

[2] H. Yu and M. Guo, "An efficient oil and gas pipeline monitoring systems based on wireless sensor networks," in *Information Security and Intelligence Control (ISIC), 2012 International Conference on*, 2012, pp. 178–181.

[3] R. Zilan and B. Tavli, "Available Mote Platforms for Wireless Image Sensors I . Literature Survey," pp. 1–24, 2008.

[4] M. Augusto, M. Vieira, and O. Di, "BEAN : Uma Plataforma Computacional para Rede de Sensores Sem Fio," 2004.

[5] Z. Peng, H. Yun, and D. Yonghong, "Application of Satellite Monitoring Technology to Prevent the Third-Party Damage of Pipeline 3 Application of GPS Satellite Positioning Technology in Pipeline Inspection Management," 2012.

[6] D. Hausamann, W. Zirnig, and G. Schreier, "Monitoring of Gas Transmission Pipelines– A Customer Driven Civil UAV Application," in *5th ONERA - DLR Aerospace Symposium*, 2003, pp. 1–15.

[7] P. K. Dey, "Decision support system for inspection and maintenance: a case study of oil pipelines," *Eng. Manag. IEEE Trans.*, vol. 51, no. 1, pp. 47–56, 2004.

[8] O. Okpo and R. C. Eze, "Vandalization of Oil Pipelines in the Niger Delta Region of Nigeria and Poverty: An Overview," *Stud. Sociol. Sci.*, vol. 3, no. 2, pp. 13–21, 2012.

[9] R. Standard, "Police probe theft of oil from pipeline under Nick Clegg's country residence - Crime," *London Evening Standard*, 2014. [Online]. Available: http://www.standard.co.uk/news/crime/police-probe-theft-of-oil-from-pipeline-under-nick-cleggs-country-residence-9659184.html. [Accessed: 11-Sep-2014].

[10] P. W. Parfomak, "Keeping America ' s Pipelines Safe and Secure : Key Issues for Congress," *Congressional Research Service*, 2013. [Online]. Available: http://fas.org/sgp/crs/homesec/R41536.pdf.

[11] C. H. Achebe, U. C. Nneke, and O. E. Anisiji, "Analysis of Oil Pipeline Failures in the Oil and Gas Industries in the Niger Delta Area of Nigeria," in *International Multi-Conference of Engineers and Computer Scientists.*, 2012, vol. II.

[12] J. F. Federici, D. Gary, R. Barat, and D. Zimdars, “THz Standoff Detection and Imaging of Explosives and Weapons,” *Soc. Photogr. Instrum. Eng.*, vol. 5781, pp. 75–84, May 2005.

[13] P. K. Dey, “Integrated project evaluation and selection using multiple-attribute decision-making technique,” *Int. J. Prod. Econ.*, vol. 103, no. 1, pp. 90–103, Sep. 2006.

[14] P. A. Environmental, “Lessons Learned Using Hot Taps For In Service Pipeline Connections,” 2006.

[15] SPDC, “Shell Incident Report Sheet.pdf,” 2014.

[16] A. F. Colombo, P. Lee, and B. W. Karney, “A selective literature review of transient-based leak detection methods,” *J. Hydro-Environment Res.*, vol. 2, no. 4, pp. 212–227, 2009.

[17] J. Sun and J. Wen, “Research on Monitoring and Pre-warning System for Security of Pipelines Based on Multi-Seismic Sensors,” *Int. Conf. Electron. Meas. Instruments*, pp. 1–5, 2009.

[18] W. Liang, J. Hu, L. Zhang, C. Guo, and W. Lin, “Assessing and classifying risk of pipeline third-party interference based on fault tree and SOM,” *Eng. Appl. Artif. Intell.*, vol. 25, no. 3, pp. 594–608, Apr. 2012.

[19] I. Jawhar, N. Mohamed, and K. Shuaib, “A framework for pipeline infrastructure monitoring using wireless sensor networks,” in *Wireless Telecommunications Symposium, 2007. WTS 2007*, 2007, pp. 1–7.

[20] A. Seema and M. Reisslein, “Towards Efficient Wireless Video Sensor Networks : A Survey of Existing Node Architectures and Proposal for A Flexi-WVSNP Design,” *IEEE Commun. Surv. Tutorials*, vol. 13, pp. 462–486, 2011.

[21] N. Mohamed and I. Jawhar, “A Fault Tolerant Wired/Wireless Sensor Network Architecture for Monitoring Pipeline Infrastructures,” in *Sensor Technologies and Applications, 2008. SENSORCOMM ’08. Second International Conference on*, 2008, pp. 179–184.

[22] A. BOUDHIR, M. BOUHORMA, and M. BENAHMED, “Energy Optimization Approaches In Wireless Sensor Networks: A Survey,” *Int. J.*, vol. 1, no. 1, 2012.

[23] J. Polastre, J. Hill, and D. Culler, “Versatile Low Power Media Access for Wireless Sensor Networks Categories and Subject Descriptors,” *ACM J.*, pp. 95–107, 2004.

[24] W. Ye, J. Heidemann, and D. Estrin, “An Energy-Efficient MAC Protocol for Wireless Sensor Networks,” *IEEE Conf. Comput. Commun.*, vol. 0, no. c, pp. 1567–1576, 2002.

[25] T. van Dam and K. Langendoen, “An adaptive energy-efficient MAC protocol for wireless sensor networks,” *Proc. first Int. Conf. Embed. networked Sens. Syst. - SenSys ’03*, p. 171, 2003.

[26] W. P. Consortium, “Qi: The global standard-The best user experience,” 2013. [Online]. Available: http://www.wirelesspowerconsortium.com/what-we-do/qi/.

[27] A. Manjeshwar and D. P. Agrawal, “APTEEN : A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks ∗,” 2002.

[28] J.-S. Lee, Y.-W. Su, and C.-C. Shen, “A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi,” in *Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE*, 2007, pp. 46–51.

[29] M. Maurya and S. R. N. Shukla, “Current Wireless Sensor Nodes (Motes): Performance metrics and Constraints,” *Int. J. Adv. Res. Electron. Commun. Eng.*, vol. 2, no. 1, 2013.

[30] J. Fraden, *Handbook of Modern sensors*. 2010.

[31] L. University, *An Introduction to MEMS (Micro-electromechanical Systems)*, no. January. 2002.

[32] G. Owojaiye and Y. Sun, “Focal design issues affecting the deployment of wireless sensor networks for pipeline monitoring,” *Ad Hoc Networks*, vol. 11, no. 3, pp. 1237–1253, 2013.

[33] Y. Bai and Q. Bai, *Subsea Pipeline Integrity and Risk Management*. Amsterdam, 2014.

[34] L. Billmann and R. Isermann, “Leak detection methods for pipelines,” *Automatica*, vol. 23, no. 3, pp. 381–385, May 1987.

[35] O. Giustolisi, D. Savic, and Z. Kapelan, “Pressure-Driven Demand and Leakage Simulation for Water Distribution Networks,” *J. Hydraul. Eng.*, vol. 134, no. 5, pp. 626–635, 2008.

[36] J. Vitkovsky, M. Lambert, A. Simpson, and J. Liggett, “Experimental Observation and Analysis of Inverse Transients for Pipeline Leak Detection,” *J. Water Resour. Plan. Manag.*, vol. 133, no. 3, pp. 218–229, 2007.

[37] T. (Egyptian D. R. I. El-Shiekh, “Leak Detection Methods in Transmission Pipelines,” *Energy Sources Part A Recover. Util. Environ. Eff.*, vol. 32, no. 8, pp. 1–12, 2010.

[38] Q. Yang, X. Zhu, H. Fu, and X. Che, “Survey of Security Technologies on Wireless Sensor Networks,” *J. Sensors*, vol. 2015, 2014.

[39] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, “Analyzing and modeling encryption overhead for sensor network nodes,” *Proc. 2nd ACM Int. Conf. Wirel. Sens. networks Appl. - WSNA ’03*, p. 151, 2003.

[40] A. Perrig, J. A. Stankovic, and D. Wagner, “Security in Wireless Sensor Networks,” *Commun. ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[41] Y. Zhang, J. Zheng, and H. Hu, *Security in Wireless Mesh Networks*. CRC Press Taylor & Franscis group, 2008.

[42] O. B. Melhem, Q. Abu Al-Haija, and A. Al-Badawi, “Performance Evaluation of Probabilistic Key Management Approaches for Wireless Sensor Networks,” *1st Int. Conf. Inf. Commun. Syst. ICICS*, no. November 2015, pp. 91–96, 2009.

[43] D. Gupta, “A Review on Wireless Sensor Networks,” *Netw. Complex Syst.*, vol. 603, no. 1, pp. 18–23, 2013.

[44] S. Rodríguez, J. F. De Paz, G. Villarrubia, C. Zato, J. Bajo, and J. M. Corchado, “Multi-Agent Information Fusion System to manage data from a WSN in a residential home,” *Inf. Fusion*, vol. 23, pp. 43–57, 2015.

[45] D. I. Tapia, R. S. Alonso, C. Zato, O. Gil, and F. De Prieta, “Analysis and Design of a SOA-Based Multi-agent Architecture,” *Trends Pract. Appl. Agents Multiagent Syst. Adv. Intell. Soft Comput. Adv. Intell. Soft Comput.*, pp. 183–190, 2010.

[46] D. Tapia and R. Alonso, “SYLPH: An Ambient Intelligence Based Platform for Ingegrating Heterogeneous Wireless Sensor Networks,” *IEEE Int. Conf. Fuzzy Syst. (FUZZ), 2010*, pp. 1–8, 2010.

[47] R. S. Alonso, D. I. Tapia, J. Bajo, Ó. García, J. F. de Paz, and J. M. Corchado, “Implementing a hardware-embedded reactive agents platform based on a service-oriented architecture over heterogeneous wireless sensor networks,” *Ad Hoc Networks*, vol. 11, no. 1, pp. 151–166, 2013.

[48] J. M. Corchado, J. Bajo, Y. de Paz, and D. I. Tapia, “Intelligent environment for monitoring Alzheimer patients, agent technology for health care,” *Decis. Support Syst.*, vol. 44, no. 2, pp. 382–396, 2008.

[49] PHMSA, “Pipeline Safety: Leak Detection on Hazardous Liquid Pipelines,” 2010.

[50] D. NPMS, “National Pipeline Mapping System (NPMS) – Home,” *NPMS Website*, 2015. [Online]. Available: https://www.npms.phmsa.dot.gov/. [Accessed: 05-Jan-2015].

[51] R. Observer, “2013 annual report: Consumer Energy Alliance,” *Consumer Energy Alliance*, 2013. .

[52] G. Thonet and P. Allard-jacquin, “ZigBee – WiFi Coexistence,” *White Pap. Test Rep.*, vol. 1, no. 38, pp. 1–38, 2008.

Authors

Johnson Eze is presently pursuing his PhD at the Faculty of Science and Engineering University of Wolverhampton. Having obtained his Master’s degree from same University, Johnson has been working for several years as a Wireless Network Administrator and recently as Visiting Lecturer at the University of Wolverhampton. Prior to his MSc programme, he worked in various capacities such as System Engineer, Network Administrator and Head of IT department in the field of Information Technology. Johnson has managed many projects both as Network Administrator in Peugeot Automobile Nigeria (PAN) Ltd and as a head of IT department in Ibeto Microfinance Bank Ltd. Johnson holds a B.Tech (Physics) degree from Federal University of Technology, Owerri, in Nigeria. Though, formerly a professional member of Institute of Electrical and Electronics Engineers (IEEE), Johnson is now a student member of IEEE as well as Society of Petroleum Engineers (SPE) owing to his status as a PhD student. Upon graduation, he proceeded to teach Physics as a Graduate Assistance in Nigerian Defense Academy (NDA) during National Service assignment. He has received several awards, of which the last is the University of Wolverhampton' s Best Researcher Award for the 2013 Annual Researchers' Competition.

Prof. Christopher Nwagboso, was the Chairman of the Society of Automotive Engineers (SAE) – UK. He has worked on and led various futuristic transport systems related research and development projects funded through European Research Programmes, various UK government and industry research programmes. He was the leading investigator of FRETSET (EPSRC – Foresight Vehicle) and has published well over 140 research papers and four books on Intelligent Transportation Systems.

Dr. Panagiotis Georgakis, B.Sc. (Hons), M.Sc., MBA, Ph.D, Senior Lecturer, University of Wolverhampton. Dr. Georgakis obtained his PhD from Wolverhampton University for the development of a platform for the integration of Intelligent Transport Systems. Part of his postdoctoral worked examined systems design integration for marine applications as part of the EU-FP VRShips Project. He has numerous (more than 40) publications in peer reviewed journals and conferences, as well as chapter contributions in books. His areas of interest are ITS system design and development, in- vehicle networking and integration, AI techniques for urban planning, multi-criteria evaluation for logistical operations and others.