Robotics and Computer--Integrated Manufacturing (xxxx) xxxx–xxxx

Contents lists available at ScienceDirect

Robotics and Computer–Integrated Manufacturing

journal homepage: www.elsevier.com/locate/rcim

Framework for integrated oil pipeline monitoring and incident mitigation systems

Johnson Eze*, Christopher Nwagboso, Panagiotis Georgakis

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

ARTICLE INFO

Keywords:
Pipeline monitoring
Critical infrastructure protection (CIP)
Wireless sensor networks (WSN)
Wireless sensor node (Mote)
Data fusion
Pipeline surveillance

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.

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 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

* Corresponding author.
E-mail address: jceze2002@yahoo.com (J. Eze).

http://dx.doi.org/10.1016/j.rcim.2016.12.007
Received 7 December 2015; Received in revised form 26 November 2016; Accepted 26 December 2016

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 0.5 km 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.