Integrating Internet of Things and Wireless Sensor Networks for Metropolitan Explosive Detection

تكامل انترنت الاشياء وشبكات الاستشعار اللاسلكية للكشف عن المتفجرات على نطاق جغرافي واسع

By

Zahraa Abdul Hussein Jaaz

Supervisor by

Dr. Maamoun Khaled Ahmed

A Thesis Submitted in Partial Fulfillment of the Requirements for the Master Degree in Computer Science

Department of Computer Science

Faculty of Information Technology

Middle East University

Amman, Jordan

April, 2014

اقرار التفويض

أنا زهراء عبد الحسين جعاز، افوض جامعة الشرق الاوسط بتزويد نسخ من رسالتي للمكتبات أو المؤسسات أو الهيئات أو الافراد عند طلبها.

التوقيع : 

التاريخ : ٢٠١٤/٤/٢٧

Authorization Statement

I'm Zahraa Abdul Hussein Jaaz, authorize the Middle East University to supply a copy of my thesis to libraries, establishments or individuals upon their request.

Signature: 

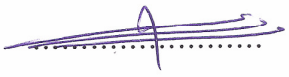
Date: 27/4/2014

Examination committee decision

This is certifying that the thesis entitled "Integrating Internet of Things and Wireless Sensor Networks for Metropolitan Explosive Detection" was successfully defended and approved on 27/4/2014.

Examination Committee Member Signature

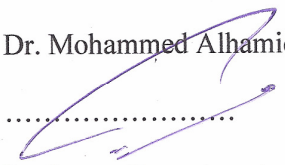
1- Dr. Maamoun Ahmed Khaled



Assistant Professor, Assistant Dean of the Faculty of Information Technology

Middle East University

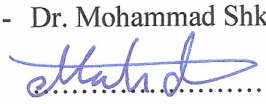
2- Dr. Mohammed Alhamid



Professor, Department of Computer Information Systems

Middle East University

3- Dr. Mohammad Shkoukani



Associate Professor, Department of Software Engineering

Applied Science Private University

Dedication

I dedicate this work to my father, my mother, my brothers and sister for their love, understanding and support; they were the light in my path. Without them, nothing of this would have been possible. Thank you for everything.

Acknowledgments

In the name of Allah the Most Gracious the Most Merciful My guidance cannot come except from Allah, in Him I trust; to Him I repent, and to Him I praise and thanks always go.

I am heartily thankful to my supervisor, Dr. Maamoun Khaled Ahmed, whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of the subject.

I am grateful of my parents and my family who are always providing help and support throughout the whole years of study. I hope I can give that back to them.

I sincerely acknowledge and express my appreciation to Prof. Dr. Reyadh Shaker Naoum the ex-dean of the faculty of Computer and Information Sciences, Dr. Hussein Al-bahadili Department of Computer Science Faculty of Information Technology Petra University, Dr. Hussein H. Owaied Department of Computer Science Faculty of Information Technology MEU University and Dr. Ahmad Kayed the dean of the faculty of Information Technology for their support, concern and thankful help.

I offer my regards and blessings to all of those who supported me in any respect during the completion of the project.

Finally, I would thank my friends and all people who gave me support and encouragement.

Abstract

By the time of writing this thesis, a lot of conflicts are happening around the world, harvesting the lives of thousands of innocent people using different types of weapons and explosives. In the guerilla and urban warfare, explosives are being delivered to target locations using vehicles forcing the authorities to come up with different techniques to stop the bloodshed in public places such as airports, shopping malls, and others.

Such techniques include employing people to do the task of scanning entering vehicles using handheld sensing devices, which may cost money as salaries, threaten the employees' lives directly, and the response time could be late due to the human factor delay. Other techniques involve building a Wireless Sensor Network (WSN) in which every sensor node detects any suspicious materials within its range and report that to a local monitory station through the sensor network, an effective technique; however it may not cover large areas due to the wireless transmission range of wireless sensor nodes.

In this thesis, a model of integration between WSN and Internet of Things (IoT) that combines the advantages of using the WSN for explosive detection with the advantages of wide coverage of internet.

The proposed technique has shown promising results in terms of end-to-end delay of response time between sensors and the metropolitan-wide management which have not exceeded the value of 0.28 seconds. The system also has shown that the management can take action based on different measures such as received traffic at each local location, and radio state of sensors.

Keywords: Wireless Sensor Nwtwork, Internet of Things, OMNet++, MiXiM

الملخص

في وقت كتابة هذه الرسالة ، الكثير من النزاعات التي تحدث في جميع أنحاء العالم تحصد أرواح الآلاف من الأبرياء باستخدام أنواع مختلفة من الأسلحة والمتفجرات. في حرب العصابات و حرب المدن ، يجري استهداف المواقع بالمتفجرات باستخدام المركبات مما اضطر السلطات للتوصل إلى تقنيات مختلفة لوقف اراقة الدماء في الأماكن العامة مثل المطارات ومراكز التسوق وغيرها.

وتشمل هذه التقنيات توظيف الناس للقيام بمهمة المسح اليدوي للمركبات حيث تستخدم أجهزة الاستشعار المحمولة ، والتي قد تكلف المال لبذي يدفع كرواتب للموظفين ، وتهدد حياة الموظفين مباشرة ، و زمن الاستجابة يمكن أن يكون في وقت متأخر بسبب العامل البشري. تتضمن تقنيات أخرى بناء شبكة الاستشعار اللاسلكية حيث يقوم كل جهاز تحسس بالاستشعار للكشف عن أي مواد مشبوهة في نطاقها وتقديم تقرير إلى أن محطة رقابية محلية من خلال شبكة أجهزة الاستشعار. تقنية فعالة ؛ ومع ذلك فإنه قد لا تغطي مساحات كبيرة نظرا للمجال الذي تغطيه الاجهزة المكونة للشبكة. في هذه الأطروحة ، نموذج للتكامل بين شبكة الاستشعار اللاسلكية و إنترنت الأشياء الذي يجمع بين مزايا استخدام شبكة الاستشعار اللاسلكية للكشف عن المتفجرات مع مزايا التغطية الواسعة من الإنترنت.

وقد أظهرت هذه التقنية المقترحة نتائج واعدة من حيث تأخير زمن الاستجابة بين أجهزة الاستشعار و الإدارة والتي لم يتجاوز 0.28 ثانية. وقد أظهرت أيضا أن نظام الادارة يستطيع أن يتخذ إجراءات بناء على قيم مستلمة من اجهزة الاستشعار مثل حالة الراديو او قراءات المعلومات المارة عبر اجهزة الاستشعار .

Table of Contents

List of figures

List of Tables

List of Abbreviations

Abbreviations	Meaning
WSN	Wireless Sensor Network
IoT	Internet of Things
AM	Active Messages
GPS	Global Positioning System
PDA	Personal Digital Assistant
SMP	Sensor Management Protocol
TCP	Transfer Control Protocol
UDP	User Datagram Protocol
MAC	Medium Access Control
NED	Network Description
ECG	EleCtrocardioGram
ADC	Analog to Digital Convertor
CPU	Central Processing Unit
RFID	Radio Frequency Identification
ED	Event Detection
IED	Improvised Explosive Device

Chapter one

Introduction

1.1 Introduction

Nowadays the world is going through difficult times for everyone and security has become a critical issue. The development of modern technologies has led to the development of weapons and explosives of various kinds, and by the spread of explosives everywhere the world needs modern and sophisticated techniques help in detecting such explosives in order to prevent disasters and casualties among innocent people. Currently, most of the explosive detection methods employ human factor, and if the methods used automated techniques such as wireless sensor networks, these automated techniques cover local area coverage in most cases. Such coverage plays an important role in determining response time to any incident. In other words, covering a small area with sensors will only alert people within that area, and if an incident happened in different area, those locals will get alerted by that and hence, the reaction time for both locations will differ depending on the human factor, again.

In this thesis we discuss the current methods used in detecting explosives, in particular, the use of WSN in detecting explosives. Then we propose a new method that involves centralizing the process of detection though connecting wireless sensor networks to the Internet of Things (IoT) reducing the response time between the detection of explosive and the reaction by the authorities dramatically and removing the need of the human factor in the detection mechanism.

Compared with traditional computer networks, WSNs are based on small smart nodes with very limited processing power, small footprint, and especially limited autonomous power supply (Lin C, et al, 2009). When a node's power supply is exhausted, it loses capacity to transmit or to receive information disappearing from the network. As a

result network lifetime depends on node lifetime, which depends on node energy, resulting in a major difference from traditional computer networks.

IoT was coined some 10 years ago by the founders of the original MIT Auto-ID Center, with special mention to Kevin Ashton in 1999(Kevin Ashton et al. 2009) and David L. Brock in 2001(David L. Brock et al 2001). Internet of things is defined as an integrated part of Future Internet and could be defined as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network. (Harald Sundmaeker et al, 2010). It is based on RFID (radio frequency Identification).

1.2 Wireless Sensor Network (WSN)

Wireless Sensor Networks (WSN) is a network consisting of a set of sensors that are characterized as self- controlled distributed in different places to monitor environmental conditions, such as temperature, sound, pressure, and others also needs corporate or physical, and cooperation to pass data through the network to the site Parent. More modern networks are bi-directional, and can enable control of the activity sensor. The motivation behind the development of wireless sensor networks was by military applications such as battlefield surveillance, and today these networks are used in many industrial and consumer applications, such as monitoring and control of industrial processes, machine health monitoring, and so on.

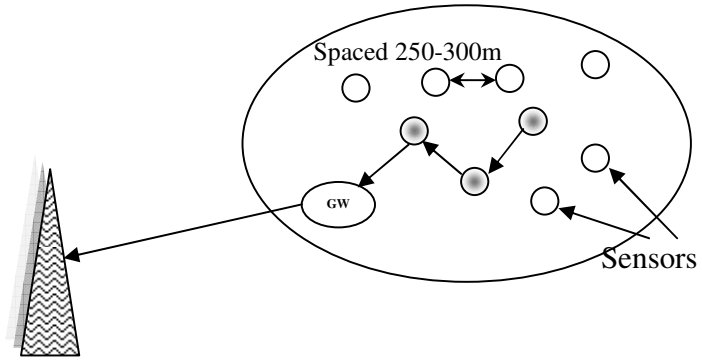


Figure 1.1 WSN

WSN is based on a small to a large number of nodes, where each node is connected to one and sensors. Each sensor node has typically several parts: a radio transceiver with an internal antenna or external antenna connection, microcontroller, and an electronic circuit to interact with the sensors and an energy source, usually a battery or form an integral part of the energy harvest. In some cases, the sensor node may vary in size down to the size of a grain of dust, although the genuine microscopic dimensions have yet to be created (LEWIS.F. L., 2004)

The cost of sensor nodes ranging from a few dollars to hundred dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth of communication. Topology of the WSNs can vary from a simple star network multi -hop network to advanced wireless network. Propagation mode between hops of the network can be routing or flooding.

1.2.1 WSN node Architecture:

In this section we summarize main components of the composition of a node for a wireless sensor network, Understand energy consumption aspects for these components and Operating system support for sensor nodes.

The Main components of a Sensor node are made up of four basic components: a sensing unit, a processing unit, a transceiver unit and a power unit. Any additional depended on application such as a localization unit, a power generator and a mobility unit (Akyildiz, I. F. et al, 2002)

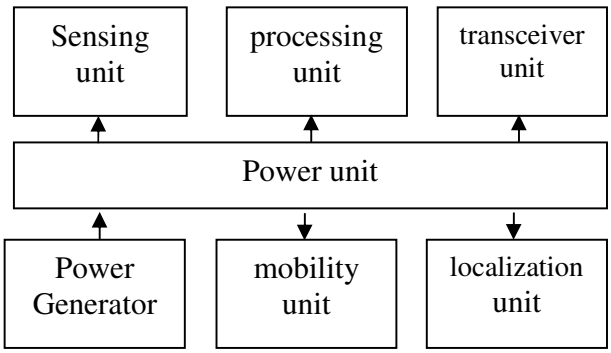


Figure1.2 WSN node Architecture

Sensing units are usually composed of two subunits: sensors and analog to digital converters (ADCs). The analog signals produced by the sensors based on the observed phenomenon are converted to digital signals by the ADC, and then fed into the processing unit. There are diverse types of sensors however they can be categorized into; passive and active sensors. Passive sensors can measure a physical quantity at the point of the sensor node without actually manipulating the environment by active probing – in this sense, they are passive. Typical examples for such sensors include thermometer, light sensors, vibration, and microphones.

Active sensors probe the environment, for example, a sonar or radar sensor or some types of seismic sensors, which generate shock waves by small explosions. These are quite specific and require quite special attention (Karl H., et al, 2005)

The processing unit or the controller manages the procedures that make the sensor node collaborate with the other nodes to carry out the assigned tasks. The controller is the core of a wireless sensor node. It collects data from the sensors, processes this data, decides when and where to send it, receives data from other sensor nodes, and decides on the sensor's behavior. It has to execute various programs, ranging from time-critical signal processing and communication protocols to application programs; it is the Central Processing Unit (CPU) of the node. Such a variety of processing tasks can be performed on various controller architectures, representing trade-offs between flexibility, performance, energy efficiency, and costs. Along with the controller, a memory is always associated with the controller in the processing unit. Evidently, there is a need for RAM to store intermediate sensor readings, packets from other nodes, and so on. Program code can be stored in ROM, EEPROM or flash memory to be preserved even in the absence of the power (Karl H., et al, 2005).

A transceiver unit is a combined transmitter and receiver that connect the node to the network. Its essential task is to convert a bit stream coming from the processing unit and convert them to and from radio waves. Usually, half-duplex operation is realized since transmitting and receiving at the same time on a wireless medium is impractical in most cases (the receiver would only hear the own transmitter anyway). A range of low-cost transceivers is commercially available that incorporate all the circuitry required for transmitting and receiving – modulation, demodulation, amplifiers, filters, mixers, and so

on. The choice of the suitable transceiver depends on many characteristics such as power consumption in different states (idle, sleeping, transmitting, or receiving), state change time, data rates, modulation and coding, and coverage range (Karl H., et al, 2005).

One of the most important components of a sensor node is the power unit which provides all other parts by the required energy. Power units may be supported by a power scavenging unit such as solar cells. However, the most common case is that the power unit is not chargeable and so other units have to reduce its power consumption as much as possible.

There are also other subunits, which are application dependent such as localization and mobility units. In many circumstances, it is useful or even necessary for a node to be aware of its location in the physical world. For example, tracking or event detection functions are not particularly useful if the WSN cannot provide any information where an event has happened. To do so, usually, the reporting nodes' location has to be known.

Manually configuring location information into each node during deployment is not an option. Similarly, equipping every node with a Global Introduction 10 Positioning System (GPS) receiver fails because of cost and deployment limitations (e.g. does not work indoors). Thus, there are various techniques of how sensor nodes can learn their location automatically, either fully automatically by relying on means of the WSN itself or by using some assistance from external infrastructure (Karl H. Karl et al 2005).

A mobility unit may sometimes be needed to move sensor nodes when it is required to carry out the assigned tasks. Mobility can appear in three forms. First, node mobility is used where the application requires individual nodes to be mobile in its area. In the face of node mobility, the network has to reorganize itself frequently enough to be able to function

correctly. Second, sink mobility is a special case of node mobility but sinks can be considered as a separate part from sensor network, for example, a human user requested information via a PDA while walking in an intelligent building. Finally, in applications like event detection and in particular in tracking applications, the cause of the events or the objects to be tracked can be mobile. This is called event mobility which the nodes and sinks are stationary but the tracked objects or events are mobile.

1.2.2 Sensor characteristics:

When choosing the right sensors for an application it is important to understand the basic characteristics of sensors. While there are many characteristics associated with wireless sensor networks as outlined by (Cayirci E. et al 2007), characteristics important to IED detection are:

- Minimal intrusiveness (especially when sensors are sited in public areas such as shopping malls and airports).
- Distributed data collection (permitting self-healing when a node failure occurs).
- Energy efficiency (necessary to maintain as long an operational life as possible, particularly when regular battery renewal is infeasible).
- Security (sensor nodes are usually sited in accessible areas, risking of physical sabotage).
- Minimal human interaction (using ideas such as a highly adaptive network topology and properties of self-organization and self-maintenance to reduce the need for human interaction other than data processing).

1.2.3 WSN Classification

There are two basic ways to categorize sensors. First is based on the principal by which they function, and the second is based on the function the sensor performs. Most sensors act like passive devices (i.e. capacitors or resistors). These sensors require external circuitry for biasing and amplification of the output signal. Resistive sensors are devices whose resistance changes with the value of input signal being measured. These sensors can be used in a simple voltage divider configuration. For more precise measurements a variety of configurations can be used (e.g. the Whetstone bridge circuit).

Capacitive sensors produce a change in capacitance proportionate to the value of the measured input signal. Detection of this change is done quite similarly as with the resistive sensors, only in this case the impedance of the capacitor is observed, which means that an AC bias must be provided. Inductance based sensors can be observed in much the same way (Rakočević, Goran, 2009).

1.2.4 WSN protocols:

When designing network protocols for wireless sensor networks, several factors should be considered. First and foremost, because of the scarce energy resources, routing decisions should be guided by some awareness of the energy resources in the network.

Thus, communication in sensor networks is typically referred to as data-centric, rather than address-centric, and data may be aggregated locally rather than having all raw data sent to the sink(s) (Pattem S., et al, 2004).

The protocol stack for WSNs consists of five protocol layers: Physical layer, Data link layer, Network layer, Transport layer, Application layer.

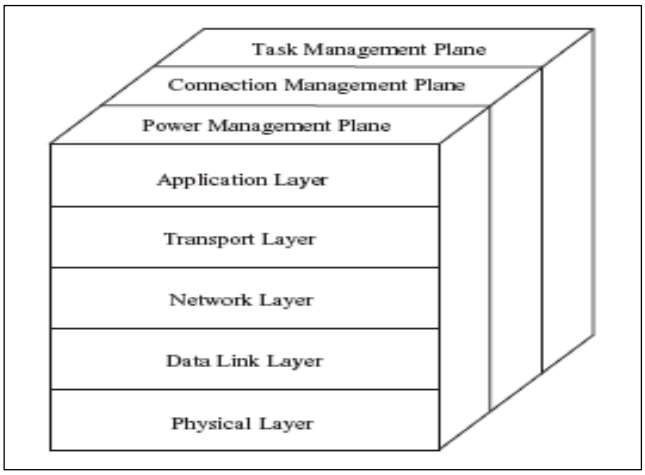


Figure1.3Protocol Stack for WSNs (Zheng Jun et al, 2010)

The application layer contains a variety of application – layer protocols to generate various sensor network applications. The transport layer is responsible for reliable data delivery required by the application layer. The network layer is responsible for routing the data from the transport layer. The data link layer is primarily responsible for data stream multiplexing, data frame transmission and reception, medium access, and error control. The physical layer is responsible for signal transmission and reception over a physical communication medium, including frequency generation, signal modulation, transmission and reception, data encryption, and so on.

On the other hand, the protocol stack can be divided into a group of management planes across each layer, including power, connection, and task management planes. The power management plane is responsible for managing the power level of a sensor node for sensing, processing, and transmission and reception, which can be implemented by employing efficient power management mechanisms at different protocol layers. For

example, at the MAC layer, a sensor node can turn off its transceiver when there is no data to transmit and receive.

At the network layer, a sensor node may select a neighbor node with the most residual energy as its next hop to the sink. The connection management plane is responsible for the configuration and reconfiguration of sensor nodes to establish and maintain the connectivity of a network in the case of node deployment and topology change due to node addition, node failure, node movement, and so on. The task management plane is responsible for task distribution among sensor nodes in a sensing region in order to improve energy efficiency and prolong network lifetime. Since sensor nodes are usually densely deployed in a sensing region and are redundant for performing a sensing task, not all sensor nodes in the sensing region are required to perform the same sensing task. Therefore, a task management mechanism can be used to perform task distribution among multiple sensors.

1. Application Layer:

The application layer includes a variety of application – layer protocols that perform various sensor network applications, such as query dissemination, node localization, time synchronization, and network security. For example, the Sensor Management Protocol (SMP) is an application – layer management protocol that provides software operations to perform a variety of tasks, for example, exchanging location – related data, synchronizing sensor nodes, moving sensor nodes, scheduling sensor nodes, and querying the status of sensor nodes.

2. Transport Layer

In general, the transport layer is responsible for reliable end – to – end data delivery between sensor nodes and the sink(s). Due to the energy, computation, and storage constraints of sensor nodes, traditional transport protocols cannot be applied directly to sensor networks without modify action. For example, the conventional end – to – end retransmission – based error control and the window – based congestion control mechanisms used in the transport control protocol (TCP) cannot be used for sensor networks directly because they are not efficient in resource utilization.

3. Network Layer

The network layer is responsible for routing the data sensed by source sensor nodes to the data sink(s). In a sensor network, sensor nodes are deployed in a sensing region to observe a phenomenon of interest. The observed phenomenon or data need to be transmitted to the data sink. In general, a source node can transmit the sensed data to the sink either directly via single – hop long – range wireless communication or via multihop short – range wireless communication. However, long – range wireless communication is costly in terms of both energy consumption and implementation complexity for sensor nodes. In contrast, multihop short – range communication can not only significantly reduce the energy consumption of sensor nodes, but also effectively reduce the signal propagation and channel fading effects inherent in long – range wireless communication, and is therefore preferred. Since sensor nodes are densely deployed and neighbor nodes are close to each other, it is possible to use multihop short – range communication

in sensor networks. In this case, to send the sensed data to the sink, a source node must employ a routing protocol to select an energy- efficient multihop path from the node itself to the sink.

4. Data Link Layer:

The data link layer is responsible for data stream multiplexing, data frame creation and detection, medium access, and error control in order to provide reliable point – to – point and point – to – multipoint transmissions. One of the most important functions of the data link layer is Medium Access Control (MAC). The primary objective of MAC is to fairly and efficiently share the shared communication resources or medium among multiple sensor nodes in order to achieve good network performance in terms of energy consumption, network throughput, and delivery latency.

5. Physical Layer:

The physical layer is responsible for converting bit streams from the data link layer to signals that are suitable for transmission over the communication medium. For this purpose, it must deal with various related issues, for example, transmission medium and frequency selection, carrier frequency generation, signal modulation and detection, and data encryption. In addition, it must also deal with the design of the underlying hardware, and various electrical and mechanical interfaces.

1.2.5 WSN applications:

WSNs may consist of many different types of sensors including seismic, magnetic, thermal, visual, infrared, acoustic, and radar, which are able to monitor a wide variety of ambient conditions that include the following: temperature, humidity, pressure, speed, direction, movement, light, soil makeup, noise levels, the presence or absence of certain kinds of objects, and mechanical stress levels on attached objects. As a result, a wide range of applications are possible. This spectrum of applications includes:

- Military: Battle field surveillances (Sarjoun S. et al, 2002).
- Emergency situations: Disaster management (Ian F. Akyildiz et al, 2002).
- Physical world: Environmental monitoring of water and soil (Al-Karaki,J.N, 2006).
- Medical and health: Sensors for blood flow, respiratory rate, ECG(electrocardiogram),pulse ox meter, blood pressure and oxygen measurement (Wendi B. Heinzelman et al, 2004).
- Industrial: Factory process control and industrial automation (Chien-Chung Shen et al, 2001).
- Home networks: Home appliances, location awareness (blue tooth (José A. et al, 2001).
- Automotive: Coordinated vehicle tracking (Chien-Chung Shen, 2001).

The above applications can be categorized into four categories:

1- Event detection in which the sensors detect an event they send messages to the sinks. An event could be a single value, for example, an above threshold humidity, or a complicated type

2- Periodic measurements in which the sources periodically send messages to the sinks
3- Function approximation and edge detection" in which the WSN system, based on specific finite values, approximates an "unknown function."
4- Tracking in which the event producer is mobile, and thus a WSN is used to detect the object's position and possibly its speed and direction

1.2.6 WSN Traffic:

Because the data traffic dynamics in different WSN scenarios are quite different, the data traffic modeling and analysis in WSNs will be quite application dependent. In (Demirkol I. et al 2006) it is suggested that WSN applications can be categorized as event-driven or periodic data generation. For periodic data generation scenarios, constant bit rate (CBR) can be used to model the data traffic arrival process when the bit rate is constant (Cui, S et al 2005). When the bit rate is variable, a Poisson process can be used to model the data traffic arrival process as long as the data traffic is not bursty (Ma Y. et al 2004).

For event-driven scenarios such as target detection and target tracking, bursty traffic can arise from any corner of the sensing area if an event is detected by the local sensors. A Poisson process has also been used to model the traffic arrival process in an event-driven WSN (Tang, S. 2006)

However, there is no solid ground to support the use of a Poisson process in this case. Actually, the widely used Poisson processes are quite limited in their burstiness (Paxson, V. et al 1995, Øverby, H. et al 2004). Instead of using Poisson processes, the author of this article proposes to use an ON/OFF model to capture the burst phenomenon in the source data traffic of an event-driven WSN [Wang, Q. et al 2008). Further, the

distributions of ON/OFF periods are found to follow the generalized Pareto distribution in his considered WSN scenario (Wang, P. et al 2009). Studies a different WSN scenario - a mobile sensor network (MSN). In an MSN, the node mobility introduces new dynamics to network traffic. In (Wang, P. et al 2009), the authors find that the mobility variability of humans (in this case, sensor nodes are attached to humans) and the spatial correlation of the collected information lead to the pseudo-LRD (i.e. long range dependent) traffic, which exhibits characteristics significantly different to that of Markovian traffic.

1.3 Detection classification

We can classify these detection techniques or equipment in to:

1.3.1 Passive detection:

Means trace detection such as vapor or microscopic elements emitted from the explosives like chemical signature-based detection technique with a vapor sensor “Fido” (Nomadics Inc., 2004) It is reported that this system can detect a wide range of Improvised Explosive Device (IED), even those concealed in vehicles.

1.3.2 Active Detection:

Means stimulating a response from explosives or the device using radiation such as x-rays or radio frequencies like MMW radiometers are sensors used for monitoring soil moisture and other geophysical data. (XyTrans Inc., 2006). Proposes using MMW radiometers to detect signatures from disturbed soil and vegetation stress that are caused by buried IEDs; images of buried IEDs can be constructed by using “MMW active illumination” method.

1.4 Example of explosive detection sensors:

One example of a commercial explosive detection is a Crossbow Technology Inc. is a solution supplier for wireless sensor networks and inertial sensor systems[1]. A good overview of MSP410 and other Crossbow's sensor systems is provided in (Vlasios Salatas, 2007).

We must understand the representation of data field in crossbow sensor because the sensor's detection mechanism will be emulated. The Crossbow sensor uses the Active Message (AM) format, which is encapsulated data from the sensor network forwarded to the base station. The format is presented in figure 1.4.

Generally, the packet contains 2 main fields, the control and data fields. The control field will be neglected for now; the data field is the one that contains information about detected objects, such as its ferrous radiation pattern values, magnetic values, traces values, and any other indications that could be compared to a fixed threshold and alert if the values exceeded the threshold.

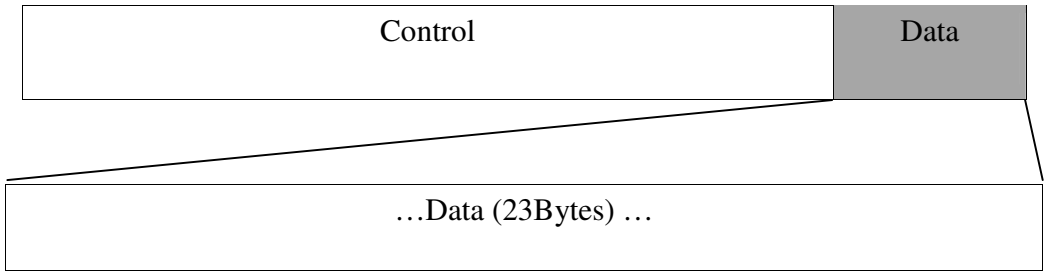


Figure 1.4 Format packet of Crossbow

[1] www.xbow.com

Figure 1.4 shows the breakdown of the “data” segment of the AM structure. The Node ID is contained in the data field and represented by 1 Byte and the rest of the 23 Bytes are used to contain the mentioned detection information.

1.5 The Problem Definition

An increase interest in explosive detection methods in present era has boosted the need to have a continuous monitoring of explosives in public places. Recent terrorist and guerilla warfare countermeasures require distributed networks of sensors that can be deployed and have self-organizing capabilities to provide more reliability and make the right decision. The selection of WSNs in explosive detection process provides capabilities of real-time data collection and data communication with central security office in less time and delay. Wireless sensors have become insufficient to cover a large area as a city, for example, this led us to think about an efficient and reliable manner for “sense and deliver” sensor data (warning) without delay to the concerned authorities. In this research we propose connection between IoT and WSNs for this purpose. The problem in the current explosives detection methods can be concluded as follows:

1. Explosives detection using WSNs alone is not capable of covering large geographical areas and that because of the nature of physical layer of wireless sensors, where the range of transmission of wireless sensors may not exceed 300 meters according to Institution of Electrical and Electronic Engineering (IEEE) .
2. Decentralized management of explosive detection using WSN. Every WSN is located in different geographical area, and each of them is managed by local security units that lack the collaboration during threats alerts. In order for those

units to warn for a threat, this will take more time, delay, and sometimes false alarms caused by human errors.

Proposed approach in this thesis is to integrate WSNs with IoT for explosives detection process to achieve higher connectivity, higher fault-tolerance, and less delay when integrating WSNs with the IoT and evaluate the overall performance of the process of centralized explosives detection compared the decentralized one to achieve easy deployment of WSN while keeping the overall design reliable and tolerant to faults and generalize the finding of this study on other domains.

1.6 Objectives:

The main objective of this research is to enhance connectivity by using IoT with WSN for fast transmission of collected data from sensor nodes in any location to security offices in wide area. The aim is to save many people's lives and secure the country.

Simplifying the process of explosives detection by centralizing it. Centralization of this operation means that the data of detection, processing of the data, and different types of reactions should be done at one place. Additionally, centralizing the process means that the data harvested from distributed sensors should be transmitted to the security head office through a global medium. One of this research's objectives is to utilize the concept of IoT and use it as the mentioned global medium.

Generally, the integration process between the IoT and WSNs should achieve more reliability, ease of deployment, and early warning and notification. The end result means a more efficient, cost-effective tool that readily detects hazardous products, providing an early warning capability in a large geographical area.

1.7 Motivation

Nowadays, the researchers and developers are giving more attention to explosives detection systems, and it has become their priority because of the high proportion of terrorism and vandals. Additionally, it is a governments' first priority to search for the best techniques for detecting explosives to maintain security of their countries and the lives of human beings.

The IoT's abilities of high performance, connection speed and precise geographic location of a any "thing" plays an important role in several areas. This motivated us to connecting it with WSNs to detect explosives for monitoring and controlling security in metropolitan or large geographical areas.

1.8 Significance:

The significance of this thesis can be an optimizing approach for save people life and Infrastructure of Institutions and all the important centers in real time.

1.9 Limitations:

As for many studies; there have been some limitations in the research, such as time limitation for the research that restricted the development of realistic explosive detection sensor. However, emulation of explosive detection mechanism was done to walk-around this limitation.

1.10 Thesis Organization

This thesis consists of six chapters organized as follows:

Chapter 1: Introduction: overview of the current explosive detection mechanism, the problem identification, the objectives of the study, the motivation, the significance of the study, and the limitation of the research.

Chapter 2: literature review: this chapter focuses on the related work in the field of explosive detection using WSN and summary of literature reviews that have been published by other researches.

Chapter 3: Methodology: outlined research methodology used by this thesis was described. Overview of the software that was used for the evaluation of our proposed method. Additionally, dataset that were used for experiments in this study was shown.

Chapter 4: The implementation details of the proposed technique and details of simulation environment and parameters.

Chapter 5: Evaluation and experiments results, discussion and analysis of results, and comparison with current techniques.

Chapter 6: Conclusions and future work.

Chapter two

Literature Review

2.1 Introduction

There are many methods and technologies used for detection of explosives that help securing communities and public places where response time to operate in high throughput must be as low as possible, such as in airports, ministries, universities, shopping malls, and other public places. The WSN research field has been having a huge amount of attention by research individuals and organizations for its important applications in many fields.

The chapter is categorized into four parts: Explosive Detection Sensors, WSN, IoT, and the integration between WSN and IoT.

2.2 Explosive Detection Sensors:

Detection of explosives is very important in countering terrorist threats. In this section present types of sensors for explosive detection.

2.2.1 Magnetic sensors:

Driven by the need for improved sensitivity, smaller size, and compatibility with electronic systems.

Measuring magnetic fields is usually not the primary intent of magnetic sensors. desired parameter dependent on what application want to sense such as wheel speed, presence of a magnetic ink, vehicle detection, or heading determination. These parameters can not be measured directly, but can be extracted from changes, or disturbances, in magnetic fields. First, the enacting input has to create, or modify, a magnetic field. The output of these sensors will directly report the desired parameter. This makes magnetic sensing a little more difficult to apply in most applications, but it also allows for reliable

and accurate sensing of parameters that are difficult to sense otherwise (Michael J. Caruso et al, 1998).

2.2.2 Ion-mobility spectrometry (IMS)

The most public technique is Ion mobility spectrometry (IMS) used for commercial applications (Abu B. Kanu et al,2008). Is an analytical technique used to separate ionized molecules and determine in the gas phase depends on their ability to navigate in the buffer carrier gas. Although working heavily for military or security purposes , such as detecting drugs and explosives , has also many technical laboratory and analytical applications , recently being coupled with mass spectrometry and high performance liquid chromatography . IMS devices come in a wide variety of sizes (often designed for a specific application), it is able to work within a wide range of circumstances. Operating systems is accompanied by a high pressure (i.e. weather conditions, 1 ATM or 1013 mbar) is also of high temperature (above 100 degrees Celsius), while the lower- pressure systems (1-20 mbar) does not require heating.

Its main disadvantage is that it contains a small quantity of radioactive material as an ionizing source which poses health risk to the operator.

2.2.3 Chemiluminescence Method:

Chemiluminescence (CL) method works by producing directly proportional Infrared (IR) light to the amount of Nitro-Oxide (NO) present figure 2.1. There may also be limited emissions of heat. Given reagents A and B with medium excited. A significant drawback of CL systems is their inability to detect explosives that are not nitro-based (Stefano GIROTTI, 2008)

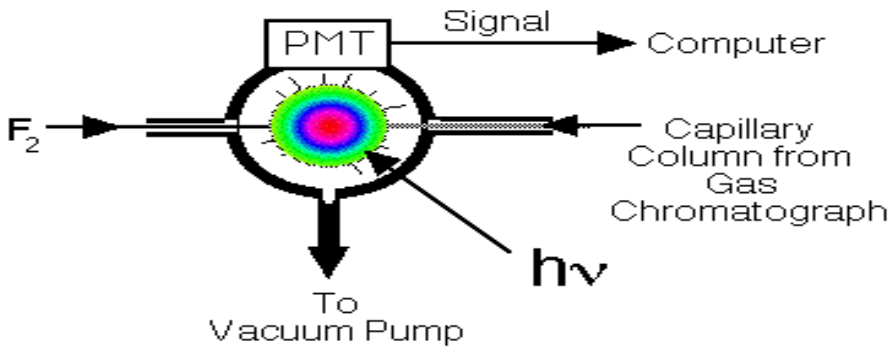


Figure 2.1 Chemiluminescence [2]

2.2.4 Surface Acoustic Wave (SAW):

Surface acoustic wave (SAW) is the sound wave traveling along the surface of the material and show flexibility, with amplitude that typically decays exponentially with depth into the substrate (Lisa Theisen et al, 2008).

Surface Acoustic describes the situation from spreading characteristics predicted in his classic paper. Named after its discoverer, Rayleigh waves have longitudinal and vertical shear component that can couple with any media in contact with the surface. This coupling strongly affects wave amplitude and speed, allowing SAW sensors directly on the sense of mass and mechanical properties.

Regardless the methods and techniques used for explosives detection, the term "explosives detection" will be used throughout the thesis without specifying the level of details in the chemical or otherwise mechanism used for the detection process itself, rather it will focus on the level of connectivity and whatever relates to it.

[2] http://www.shsu.edu/chm_tgc/chemilumdir/CLUMIN.html

Chemical detection using sensor systems that are facing a major challenge of selectivity (Potyrailo RA et al, 2012). In this review, we provide a brief summary of chemical threats and the importance of home security; focusing in detail on the modern concepts in the field of chemical sensor; study the origins of the unmet needs in the most important in chemical sensors exist, and analysis of the opportunities and the specific requirements and challenges facing chemical sensors and WSNs.

We review a new approach to the selective chemical sensors which involves a combination of sensor materials that have different mechanisms in response to different types of interest, with an adapter that has the capability multi- variable signal transduction. Have realized this approach selective chemical sensor using the new platform is attractive everywhere from passive radio frequency identification free battery (RFID) tags adapted for chemical sensors. We illustrate the performance of the sensor developed and interact in measurements of toxic industrial and humidity independent detection of toxic fumes, and the detection of simulated chemical agent and explosives, and strong oxidizers.

The Perimeter Intrusion Detection System (PIDS) based on WSN. The main purpose is to detect an open field across the perimeter intrusions, self-contained power, and the contract is based on a very small acceleration sensor (Davis, A. 2012). The proposed system is inexpensive, and easy to deploy and maintain self- configurable and self-recovery. Through the presence of any single point of component failure, this system is also highly reliable. The proposed system is designed specifically to detect the vicinity of infiltration, and preferably to complement the already existing physical protection such as

chain link fences. While our system addresses the security concerns at the airport, and can be extended to include other vital infrastructure such as railway stations and ports the ship.

Increase in bomb attacks in present era and its contribution to the need to have a continuous monitoring of explosives in public places (S. Simi & Maneesha V. Ramesh, 2010) proposes an effective warning mechanism for security threats in public places such as railway stations so that security corps can take immediate action against bomb threats. Using a multi- phase wireless sensor network, the system provides a technique to reduce, control, and warning of terrorist activity coming through the rapid and accurate detection of explosives. It uses wireless sensor nodes integrated with multiple different types of sensors to determine the chemical composition of explosives. Based on different orthogonal techniques, the system will collect data from the sensor nodes dynamically assemble and transmit data to the sink node for further analysis. Authors have introduced a mobile node to confirm the suspected objects, thus contributing to the goal of strengthening the tracking mechanism that reduces the number of false alarms.

Researchers say that in recent years, remote monitoring of the environment has improved significantly with the wireless sensor networking technology (Simi S & Joshua D Freeman, 2011). This paper presents a real - time streaming of the indoor environment using wireless sensor network and a group of self - mobility robots. Will mobile robots with sensors installed on the self- navigate through the interior space with unknown obstacles the robots will be able to avoid obstacles and move across the region Robots sense of environmental parameters in the area, and send that data to the remote monitoring

stations using wireless sensor network infrastructure. This design is applicable to networks where some may not be of sufficient sensors for sensing data more accurate and closer monitoring is required, and achieved an effective path planning for mobile robot by combining a map of the area, and sensor readings and the power of radio to the sensor network. E-mail alerts can be sent to officials sensed if the data goes above a predetermined threshold level, and thus successfully detects the presence of explosives in a certain area. This system streams data in real time to the Internet, which makes it possible for authorized personnel to view the state of the environment on the Internet.

Proposed automatic explosive detection system automatically detects the IED without any human intervention (Avinash.Vanimireddy et al, 2012). There are many advantages with the proposed system when compared with the traditional detection techniques. The advantages include less cost, low power consumption and less analysis time. By this proposed system the exact location of the IED can Radar unit Paper sensor& Communication easily located which will deactivated immediately so that many lives can be saved.

Researchers proposed an efficient autonomous system for standoff explosive detection (Hariharan Balaji et al, 2011). While comparing with traditional systems, iWEDS have lot of advantages. The main advantages are its miniature size, low power consumption, distributed operation, and easy implementation. iWEDS is organized in such a manner that only security officials know about the presence of the system. For common

public it is visible only as a solar road reflector. So we overcome the problem of bypassing the security mechanism by intruders.

2.3 Internet of Things (IoT) :

In this section we present the definition of Concept of IoT and the time of writing the thesis.

The phrase "Internet of Things" was coined some 10 years ago by the founders of the original MIT Auto-ID Center, with special mention to Kevin Ashton in 1999 and David L. Brock in 2001. The term "Auto-ID" refers to any broad class of identification technologies used in industry to automate, reduce errors, and increase efficiency. These technologies include bar codes, smart cards, sensors, voice recognition, and biometrics. But since 2003 the Auto-ID technology on the main stage has been Radio Frequency Identification (RFID).

- "The Internet of Things", by Sean Dodson, The Guardian, 9 October 2003.5
- "Toward a Global Internet of Things", by (Steve Meloan, 2003). It heralded that With the official release of the Electronic Product Code Network, we are about to see the Internet of Things paradigm enter the big time – the world of mainstream commerce". Sun Microsystems argued of course that with its notion that "The Network is the Computer", it was uniquely positioned to play a leading role in the Auto-ID revolution, especially with respect to security, scalability and cross-platform compatibility. Figure 2.2.
- "A Machine-to-Machine Internet of Things", Business Week, 26 April 2004.
- "The principles that gave rise to the Internet are now leading to a new kind of network of everyday devices." by (Neil Gershenfeld et al,2004)

- "Start-ups jump into next big thing: tiny networked chips", by (Weisman Robert, 2004)

In fact, when considering the spectrum of possibilities for the Internet of Things in the 2020-2025 timeframe, little can be said at this stage since the technology is still being refined, the industry is in a process of reconfiguration, and the market is embryonic. The main uncertain ties can be grouped around two axes: the timing of developments (slow versus fast) and the depth of penetration (niches versus ubiquity). (Vision and Challenges for Realising the Internet of Things, (Harald Sundmaeker, Patrick Guillemin, Peter Friess, Sylvie Woelfflé, March 2010)).

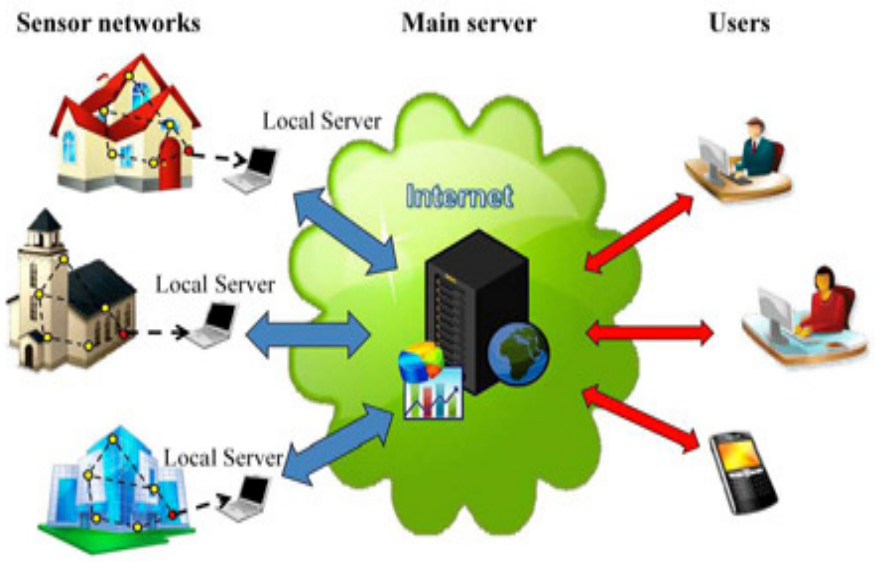


Figure 2.2 Internet of Things[3]

Clear potential of the WSN paradigm will be fully unleashed once it is connected to the Internet (Alcaraz Cristina et al, 2010), becoming part of the IoT. However, it is

[3] http://www.liu.se/forskning/forskningsnyheter/1.428680?l=en

necessary to discuss whether a full integration at the network level (i.e. using direct TCP/IP connections) should be advisable for every application. Authors conclude that some applications should not connect their nodes directly to the Internet (e.g. SCADA systems), but other applications can benefit from using TCP/IP directly (e.g. first responder systems).

Researcher first analysis step to integrate WSNs into the Internet of Things (Delphine Christin et al, 2009), have considered selected application scenarios presenting a high diversity in terms of monitored subjects and environments. By taking into account their main characteristics, we have analyzed three integration approaches and demonstrated that they were inappropriate in their current state to allow sensor nodes joining dynamically the Internet of Things.

Authors consider applying the IP to the Field paradigm, which implies assigning additional responsibilities to the sensor nodes as an adequate solution to integrate WSNs with the Internet. We have selected three important task assignments in order to highlight the challenges emerging from the paradigm adoption: Security, Quality of Services (QoS), and configuration management. Their analysis revealed that the solutions currently deployed in the Internet are not suitable for the limited sensor node resources and consequently, novel mechanisms have to be developed to adapt to the capabilities and constraints of WSNs. We plan to investigate existing approaches and find suitable modifications for resource-constrained sensor platforms to tackle these challenges.

(Marco Z. Z. et al 2003) propose an application -level gateway to integrate WSNs with internet. The proposed technique is applicable in homogenous networks. (i.e. all nodes

have the same capabilities). In simple sensor networks where nodes are providing information continuously, the gateway acts as a web server and the collected data can be displayed in dynamic web pages.

In more sophisticated networks, the gateway acts as an interface to a distributed database where users can issue queries to the sensor network. In heterogeneous WSN, they recommend to use an overlay IP network instead figure 2.3.

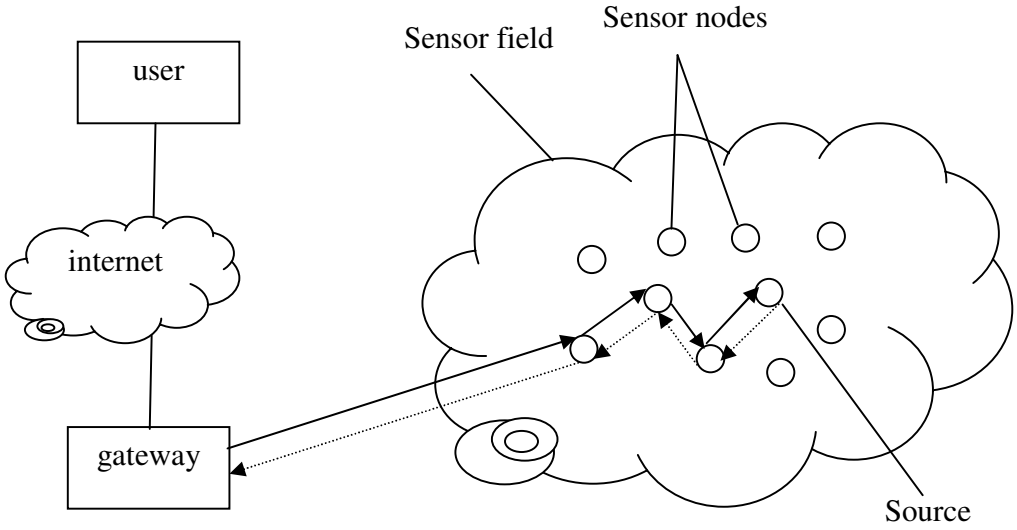


Figure 2.3 Communication Architecture using a gateway

Another framework uses gateways is proposed in (Mohanty et al, 2007). Where each SN is identified by an IP address (the gateway IP) as shown in Figure 2.4 Sensor nodes are identified by node ID and endpoint ID (endpoint ID identifies the application within a node). IP hosts can access a sensor node through the IP address of WSN and a specific port number assigned to it at the gateway.

Packets from each side are reformed when reach the gateway to the destination network as shown in figure 2.5 When the gateway receives an UDP message from IP network, it creates a packet confirming to the protocol used in that WSN.

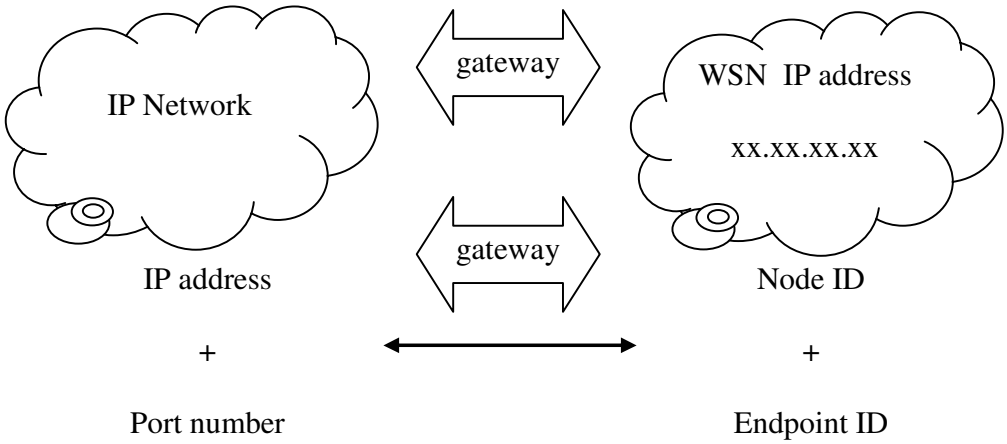


Figure 02.4 A WSN identified by a single IP address

The UDP payload maps to the payload of this new packet and its header is constructed using mapped WSN addresses.

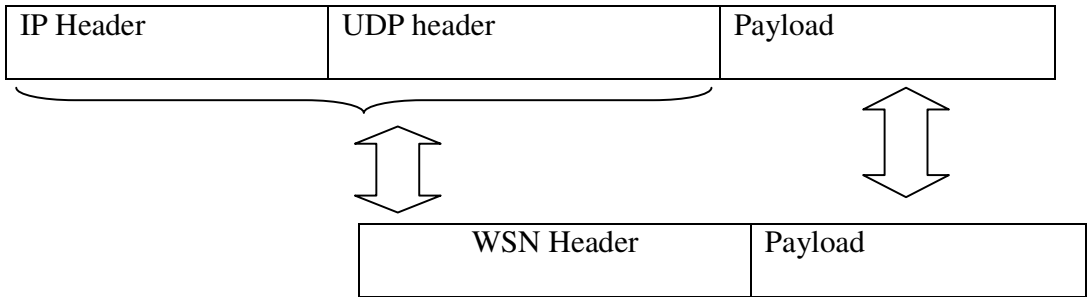


Figure 2.5 Packet mapping in single IP framework

Similarly, when gateway receives a packet from WSN destined to an IP destination, it creates a UDP packet. The packet payload maps to the UDP payload. UDP and IP header is constructed using mapped IP addresses and port numbers too.

Chapter three

Methodology

3.1 Introduction:

In this chapter, an overview of the simulation environments used for simulation of WSN is described, and then examples of WSN simulators are investigated and compared. Additionally, an overview and an example on the concept of emulation are shown, finally, a comparison between the terms: simulation and emulation is discussed.

3.2 Simulation of WSN

There were two options for the implementation of the proposed technique; using a hardware WSN test-bed or using a network simulator. The test-bed option requires multiple sensor nodes along with a gateway node which can be connected to internet. This option costs a lot .Therefore the work is implemented using a simulator. However, there are several network simulators for WSN. Each simulator has advantages and disadvantages and the most suitable was selected carefully.

"Simulation is the process of designing a model of a real system and conducting experiments with this model for the purpose of either understanding the behavior of the system and/or evaluating various strategies for the operation of the system"

(Chhimwal Mrs. Poonam, et al, 2013).

The simulation result depends upon on the environment and physical layer assumption which may not be accurate to predict the real behavior of wireless sensor network. Simulation is necessary to test the application and protocols in this field. The correctness of the model and Suitability of model for the implementation are necessary factors of WSN simulations. The key properties of good Simulator:-

* Reusability and availability

* Performance and scalability.

* Support for rich-semantics scripting languages to define experiments and process results.

* Graphical, debug and trace support.

Generally, a simulator is more useful when looking at things from a high view. The effect of routing protocols, topology, and data aggregation can be seen best from a top level and would be more appropriate for simulation. Emulation is more useful for fine-tuning and looking at low-level results. Emulators are effective for timing interactions between nodes and for fine tuning network level and sensor algorithms (Lessmann Johannes, et al 2008).

In this thesis before choose any simulator we most set a factors that to be able to fit in the implementation.

1- Simulator must support protocols of both WSN and IP network. It is a crucial feature as the gateway node needs to be connected to a WSN and an IP network to integrate them together.
2- Simulator should have realistic wireless channel and radio models for WSN to ensure valid results that are near to those produced by real hardware test beds.
3- Should be recognizable in research to indicate its accuracy, open source to support adding new protocols and well-documented to facilitate its learning.

We excluded simulators that do not support IP networks from these surveys and compared the rest to select the most suitable one.

3.3 Simulators used for WSN modeling:

3.3.1 NS-2:

NS-2[4] is the most popular simulation tool for networks in general and sensor networks too. Back in 1996 when the first version of ns-2 was released. NS-2 is an object-oriented discrete event simulator; its modular approach has effectively made it extensible. Simulations are based on a combination of C++ and Object Oriented Tool Command Language (OTcl). In general, C++ is used for implementing protocols and extending the NS-2 library. OTcl is used to create and control the simulation environment itself, including the selection of output data. Simulation is run at the packet level, allowing for detailed results (Curren David, 2007).

NS-2 sensor network simulation is a modification of the mobile ad hoc simulation tools, with a small number of add-ons. Support is included for many of the features that make sensor networks unique, including limited hardware and power. An extension developed allows for external phenomena to trigger events. NS-2 extensibility is perhaps what has made it so popular for sensor networks. In addition to the various extensions to the simulation model, the object-oriented design of NS-2 allows for straightforward creation and use of new protocols; however it is hard according disorganization or relationships among extensions.

The popularity of NS-2 has ensured that a high number of different protocols are publicly available, despite not be included as part of the simulator's release. Its status as the

[4] The Network Simulator – NS-2. http://www.isi.edu/nsnam/ns.

most used sensor network simulator has also encouraged further popularity, as developers would prefer to compare their work to results from the same simulator.

NS-2 does not scale well for sensor networks. This is in part due to its object-oriented design. While this is beneficial in terms of extensibility and organization, it is a hindrance on performance in environments with large numbers of nodes. Every node is its own object and can interact with every other node in the simulation, creating a large number of dependencies to be checked at every simulation interval, leading to an n2 relationship. Another drawback to NS-2 is the lack of customization available. Packet formats, energy models, MAC protocols, and the sensing hardware models all differ from those found in most sensors. One last drawback for NS-2 is the lack of an application model. In many network environments this is not a problem, but sensor networks often contain interactions between the application level and the network protocol level.

3.3.2 OPNET:

OPNET (Junhong Wu et al, 2004) is another discrete event, object oriented, general purpose network simulator. It uses a hierarchical model to define each aspect of the system. The top level consists of the network model, where topology is designed. The next level is the node level, where data flow models are defined. A third level is the process editor, which handles control flow models. Finally, a parameter editor is included to support the three higher levels. The results of the hierarchical models are an event queue for the discrete event simulation engine and a set of entities representing the nodes that will be handling the events. Each entity in the system consists of a finite state machine which

processes the events during simulation. OPNET is capable of recording a large set of user defined results.

OPNET supports the use of modeling different sensor-specific hardware, such as physical-link transceivers and antennas. OPNET can also be used to define custom packet formats. The simulator aids users in developing the various models through a graphical interface. The interface can also be used to model, graph, and animate the resulting output. Additionally, OPNET is only available in commercial form.

3.3.3 OMNeT++ framework:

OMNeT++[5] Objective Modular Network Testbed in C++ is an object-oriented modular discrete event network simulator. OMNeT++ is a discrete event simulation environment**.** Its primary application area is the simulation of communication networks, but because of its generic and flexible architecture, is successfully used in other areas like the simulation of complex IT systems, queuing networks or hardware architectures as well.

OMNeT++ provides component architecture for models. Components *(modules)* are programmed in C++, then assembled into larger components and models using a high-level language Network Description *(NED)*. Reusability of models comes for free. OMNeT++ has extensive Graphic user interface (GUI) support, and due to its modular architecture, the simulation kernel (and models) can be embedded easily into your applications.

Although OMNeT++ is not a network simulator itself, it is currently gaining widespread popularity as a network simulation platform in the scientific community as well as in industrial settings, and building up a large user community.

[5] http://www.omnetpp.org/

	NS-2	OPNET	OMNeT++
Programmability	Strong Programmability C++	Strong Programmability C++	Strong Programmability C++
Available Protocols and Models	large number of protocol models, but mostly centered around TCP/IP, that limit NS2 in WSN simulation	lots of protocol models, including TCP/IP,ATM, Ethernet, etc., but it is so expensive to get the licenses	Has TCP/IP, SCSI and FDDI models. Along with the fast increase of users, the model library also rapidly consummates and it can satisfy the large-scale sensor network simulation the demand
Network Topology and Hierarchical Models	insufficient in this kind of ability	allows hierarchical models with arbitrarily deep nesting but models always use fixed topology , has too many limits	allows hierarchical models with arbitrarily deep nesting by NED and its graphical editor allow customize topology and parameterized topologies
Programming Model and Simulation Library	library provides less function,	Simulation library is based on C	supports both thread/coroutine-based programming model, or FSMs built upon a message-receiving function and more powerful
Debugging and Tracing	not very good, it needs a long time and lots of memories to simulate	powerful command-line simulation debugger, but it did not have a graphical runtime environment	automatic animation, module output windows and object inspectors
Source Opening	fully open-sourced	Commercial source	fully open-sourced

Table 3.1 Comparison between simulators

In this research, design WSN for explosive detection using OMNeT++ 4.3.1 framework with simulator MiXiM 2.3 for WSN and the INET 2.2.0 Framework for IP network.

3.4 Simulation Environment:

OMNet++ can installed on linux and windows. In our work installed in windows to improve compatibility with the latest operating system and compilers releases provided by version 4.3.1. It also introduced features that help you debug and verify your simulation models more efficiently.

MiXiM[6] is an OMNeT++ modeling framework created for mobile and fixed wireless networks (wireless sensor networks, body area networks, ad-hoc networks, vehicular networks, etc.). MiXiM concentrates on the lower layers of the protocol stack, and offers detailed models of radio wave propagation, interference estimation, radio transceiver power consumption and wireless MAC protocols

The INET[7] Framework contains models for several Internet protocols: UDP, TCP Ethernet and several other protocols. Protocols are represented by simple modules. These modules can be freely combined to form hosts and other network devices using script language called NED language. Not all modules implement protocols though. Protocol headers and packet formats are described in message definition files which are translated automatically into C++ classes by OMNeT++'s special tool

[6] http://mixim.sourceforge.net/

[7] http://inet.omnetpp.org/

G++ is a compiler, not merely a preprocessor. G++ builds object code directly from C++ program source.

3.5 IEEE 802.11p standard:

Standard for information technology local and metropolitan area network specific requirements Wireless LAN medium Access Control (MAC) and Physical Layer (PHY) Specification Amendment Wireless Access in Vehicular Environments[8].

At the communication link between the vehicles and the roadside infrastructure might exist for only a short amount of time, the IEEE 802.11p amendment defines a way to exchange data through that link without the need to established a basic service set (BSS), and thus, without need to wait for the association and authentication procedures to compete before exchanging data. For that purpose, IEEE 802.11p enable stations uses the wildcard of the frames they exchange, and may start sending and resaving data frames as soon as they arrive on the communication channel.

Use 802.11p for WSN offer several advantages:

1- Infrastructure cost the infrastructure cost attached to sensor data distribution can be essentially eliminated, thus greatly improving the wireless sensor network total cost of ownership (TCO).

2- Network efficiency capacity can be monitored and additional access points and infrastructure can be installed as network load grows.

3- faster deployed in large or small numbers without modifying the data distribution infrastructure that could enable use of sensors in remote locations, including

[8]Standards.ieee.org, IEEE STANDARD ASSOCIATION, 2010

outdoor environments and easily relocated to meet changing operating conditions or set up in remote or temporary locations,.

4- knowledge base consumer network operators are familiar with managing 802.11 networks
5- scalability is directly related to the maximum data rate of a particular network architecture that ability to add new sensors and utilize higher data rate sensors is directly proportional to the maximum data rate supported by the physical channel so can to a greater number of nodes and faster data rates
6- 802.11 operate in the 5.9GHz unlicensed Radio Frequency (RF) band. The maximum isotropic transmission power in this band allowed by FCC in US is 1Wt, but 802.11 devices are usually limited to the 100mWt value.
7- The establishment of 802.11 as a dominant worldwide standard guarantees technical advancement and on-going support for a complete range of critical enhancements necessary for reliable, robust network operation.
8- Battery life achieving 5-10 years of battery life using one AA battery. Such performance is achieved by designing silicon from the ground up specifically for low power consumption applications.

3.6 Emulation:

Imitation of behavior of a computer or other electronic system with the help of another type of computer/system or means mimic the behavior[9]. We benefit from this approach in our work that emulate the explosive detection Mechanism because we haven't enough to

[9] http://academic.research.microsoft.com/Keyword/27380/Network-Emulation

make a simulation for sensor itself that's need to make many change in OMNet++ functionalities. For example are designed to emulate Hewlett-Packard LaserJet printers because so much software is written for HP printers. If a non-HP printer emulates an HP printer, any software written for a real HP printer will also run in the non-HP printer emulation and produce equivalent printing.

In our work we benefit from emulation approach by explosive detection mechanism. We will use a sensor system from Crossbow Technologies because it can apply in to magnetic and infrared, commercial, and many studies wrote about it.

The emulation was based on two assumptions:

1- Building traffic on the cars to emulate bizarre car behavior (indicating car has explosives)

2- Traffic's packets have 2 types, 1Byte data field to indicate car has no explosives and 23Bytes to indicate the opposite (according to reference above).

Testing the emulation of explosive detection, and loading a vehicle out of 30 with bizarre traffic.

3.7 Differences between simulation and emulation:

Simulation is the imitation of another device and its functionalities, but emulation is the imitation of the behavior of some device rather than the device itself.

Emulation allow different software/hardware to be experienced or employed on a single platform without the original system requirements; therefore, allowing cheaper alternatives in many digital level scenarios[10]. Even though the initial development costs

[10] http://hemantcnb.blogspot.com/2013/08/what-is-difference-between-emulator-vs.html

may be high, an emulator can be very cost efficient over a long term due to its versatility. Even though the emulators are very useful in modern digital environment. Benefit from this feature for emulation explosive detection Mechanism.

In a simulation, the operation of a targeted system is recreated to the best possible. The underlying mechanisms used to recreate the scenario may be the same or different from the original.

Chapter four

Implementation

4.1 Introduction:

One of the most important elements in the IoT paradigm is wireless sensor networks (WSN). The benefits of connecting both WSN and other IoT elements go beyond remote access, as heterogeneous information systems can be able to collaborate and provide common services.

Implementation process was straightforward in the simulation part; however, the part in which the sensors should sense explosives was treated differently. The sensing process was emulated for time-related reasons that prevented the researcher from developing a fully working explosive detection sensor.

The following sections describe the integration process, the configuration of the simulation, and settings for the simulation runs.

4.2 Overview of Integration Approaches

From a network perspective, if we want to know whether a WSN should be completely integrated into the Internet or not, it is first necessary to know what kind of integration approaches can be used to connect both infrastructures.

Approaches can be classified into two different ways:

1- **Stack-based**: the level of integration between the Internet and a WSN depends on the similarities between their network stacks (Roman R., et al, 2009) classification :

- Front-End: A WSN can be completely independent from the Internet
- Gateway solution: be able to exchange information with Internet hosts
- TCP/IP solution: share a compatible network layer protocol (*TCP/IP*).

2- **Topology-based**: level of integration depends on the actual location of the nodes that provides access to the Internet. (Christin D. et al, 2009) classified.

- Hybrid solution approach: These nodes can be a few dual sensor nodes (e.g. base stations) located on the root of the WSN
- Access point solution approach: a full-fledged backbone of devices that allow sensing nodes to access the Internet in one hop.

Stack-based approach was used in this research with fixed number of 24 sensors, 8 for each local location. One of 8 sensors acts as a gateway, connected to sensors on one side via wireless access and on the other side it is connected to the local location via Ethernet access.

The size of the simulation area was fixed to 50 x 50 km for the whole metropolitan network. 3 different locations were distributed over the network with distance between them, each location is connected to a centralized management through internet.

Sensors and gateways are configured to have Better Approach To Mobile Ad hoc Networking (B.A.T.M.A.N.) protocol which a proactive routing protocol that detects other nodes and finds the best way (route) to them. It also keeps track of new nodes and informs its neighbors about their existence[11].

Configuration of routing information on sensors and gateways as set on omnet++:

***.sensor*[*].routingProtocol = "Batman"*

***.gwHost*.routingProtocol = "Batman"*

[11] http://ntnu.diva-portal.org/smash/record.jsf?pid=diva2:453358

The main feature of this protocol is that it does not try to determine the whole path from source to destination, but it rather uses the originator-messages, only the package's first step in the right direction. The data is handed over to the next neighbor in that direction, who in turn uses the same mechanism. This process is repeated until the data reaches its destination. Sensors within the WSN have no mobility, hence link breakage due to mobility is rare to happen, and therefore the routes update interval was set to 10000 milliseconds to preserve more power.

30 were deployed to roam the city with random mass mobility[12] and with a uniformly random speed between 5 and 20 meters per second (mps) which is assumed to be approximate representation of the speed in a city. The starting location for each of the cars' mobility is random, however, they have been put in a way that guarantees the presence of the cars around the sensors at most of the time, by fixing the initial value of cars' mobility to be uniform for the X coordination (5km,40km) and the Y coordination (25km, 38km).

Virtual Private Network (VPN) extends a private network across a public network[13], such as the Internet. VPN was set in the network by using static IP addresses for all nodes in the network to limit access from outside, on the form 10.0.0.x, and with a subnet mask 255.255.255.x

The internet itself was represented using a cloud, which represents the infrastructure for the internet. The cloud's most important feature is the delayer, which delays the traffic

---

12

http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1624340&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1624340

13 http://searchenterprisewan.techtarget.com/definition/virtual-private-network

that passes through it in a realistic random fashion, through functions that were set prior to setting up the simulation.

Rather than building explosive detection sensors from scratch, which could have took more time than the dedicated for this research, the traffic for the explosive detection sensors was emulated (Vlasios Salatas,2005 and Joshua Sundram Phua Poh Sim, 2007)

Where all cars were equipped with traffic source that is periodically sent to sensors (representing the scenario where sensors detect no bizarre behavior), and in the cases where cars may carry explosives, the car was equipped with traffic source that sends packets with the size of 23 Bytes, the 23 Bytes represents the payload of the Active Message (AM) format used by explosive detection sensors, the AM format which is encapsulated data from the sensor network forwarded to the base station. In the scenario, one car (out of 30) was equipped with explosives.

All locations of the network were connected using Ethernet with 0.1 μs channel delay data rate of 100Mbps except the infrastructure of the internet which was configured as in Appendix 1.

For the transport layer, the User Datagram Protocol (UDP)[14] protocol was used for the traffic between entities of the network, the UDP was chosen because of the nature of the WSN itself, where sensor nodes may go on sleep mode, breaking an open connection if the Transport Control Protocol (TCP) was chosen. The UDP is a connection-less protocol which does not require opening and closing connections between source and destination as in the case of the connection –oriented TCP. UDP provides checksums (used for error-

[14] http://searchsoa.techtarget.com/definition/UDP

checking of the header and data) for data integrity, and port numbers (along the computer's IP address, completes the destination address for communication between source and destination) .

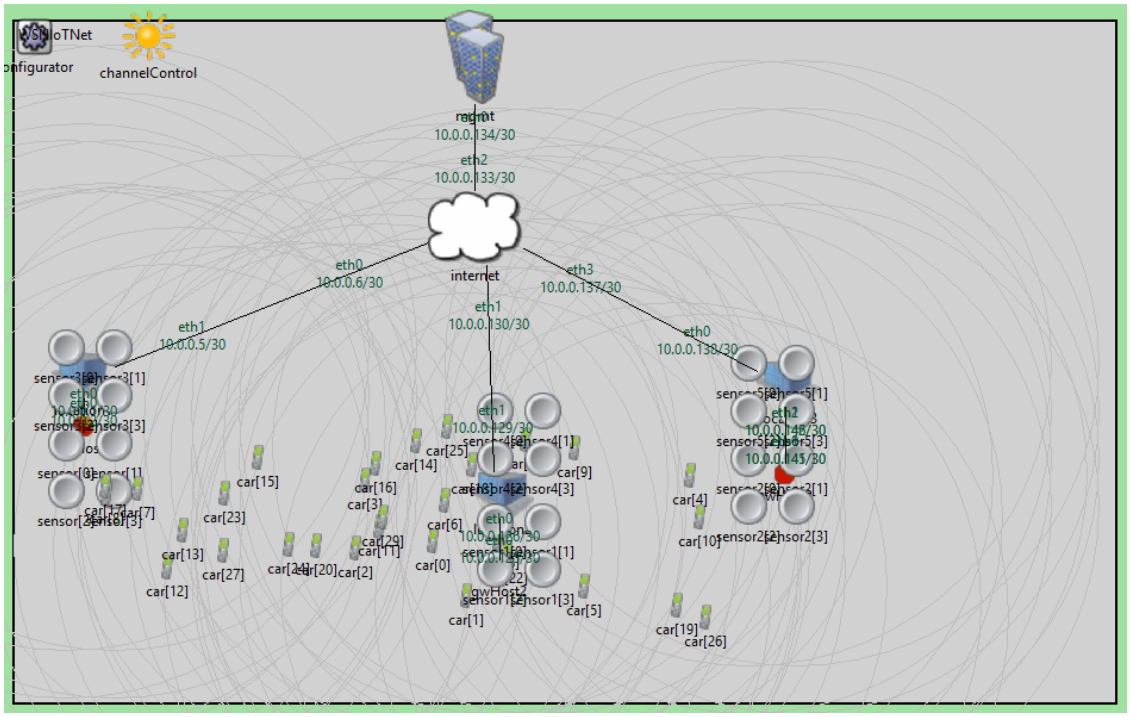


Figure 4.1 Model representation in OMNet++

4.3 Sensors:

The sensors were represented by 802.11p “AdhocHost” module. A wireless host that contains routing, mobility and battery components, it supports IPv4 IP protocol, and TCP and UDP as transport protocols. This is a typical mobile node which can participate in ad hoc routing and may have TCP/UDP applications installed.

The Mobile Ad-Hoc Network (*manetrouting*) sub-module is responsible of controlling MANET related control information and routing protocols.

By default it contains a single wireless card; however it can be configured by the numRadios parameter. Figure 4.2

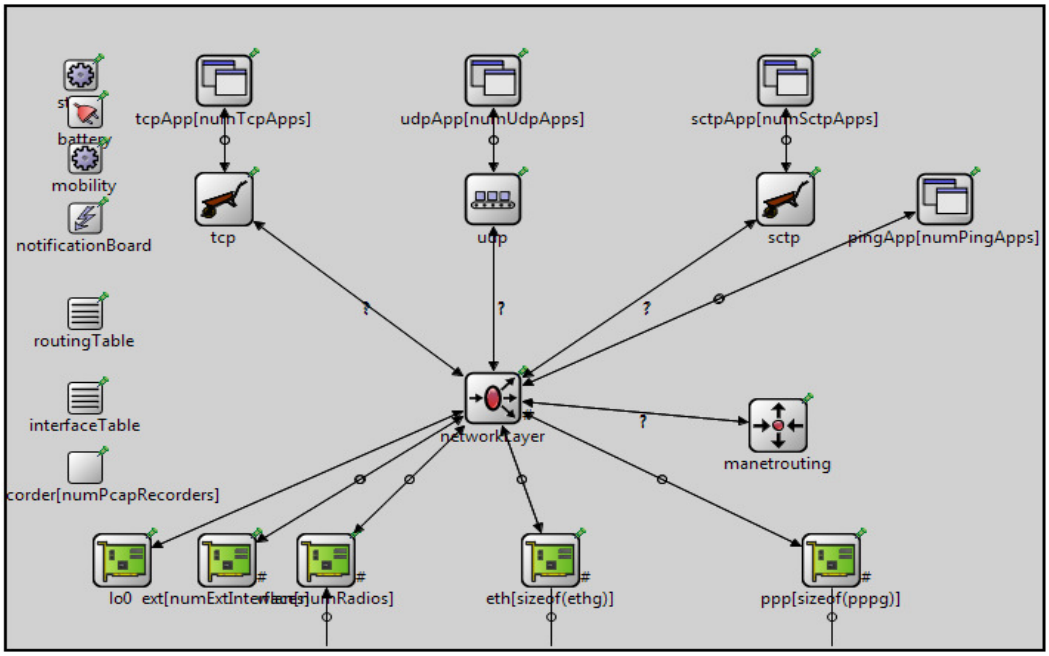


Figure 4.2 Adhoc model represent sensors

4.4 Management:

Represent by Standard Host (compound module) IPv4 host with TCP, UDP layers and applications, it can be connected via Ethernet interface to other nodes using the ethg gate. By default full-duplex connections are supported only (twisted pair).

In this research, the management is the key alerting node (or number of nodes if extended), this node receives traffic from all around the network through the 3 locations connected to it and detect when to alert and when not to.

The mechanism of detecting bizarre behavior at the management side is explained in chapter 5

4.5 Internet:

Represented by Internet Cloud (compound module) this module is an IPv4 router with the ability to delay or drop packets based on which interface card the packet arrived on and on which interface it is leaving the cloud.

In this research, the internet cloud was employed to represent the internet infrastructure implicitly. The implicit employment of infrastructure was using the delayer sub-module which adds realistic random delay and data rate values that are used in real-life scenarios as shown in figure 4.3, example:

<traffic src="location1" dest="mgmt" delay="20ms+truncnormal(200ms,60ms)" datarate="uniform(100kbps,1Mbps)" drop="uniform(0,1) " />

The above line – for example – is to set the delay between location 1 and the management by 20ms (for initialization delay) plus a random value based on the truncated normal distribution of 200ms and 20ms.

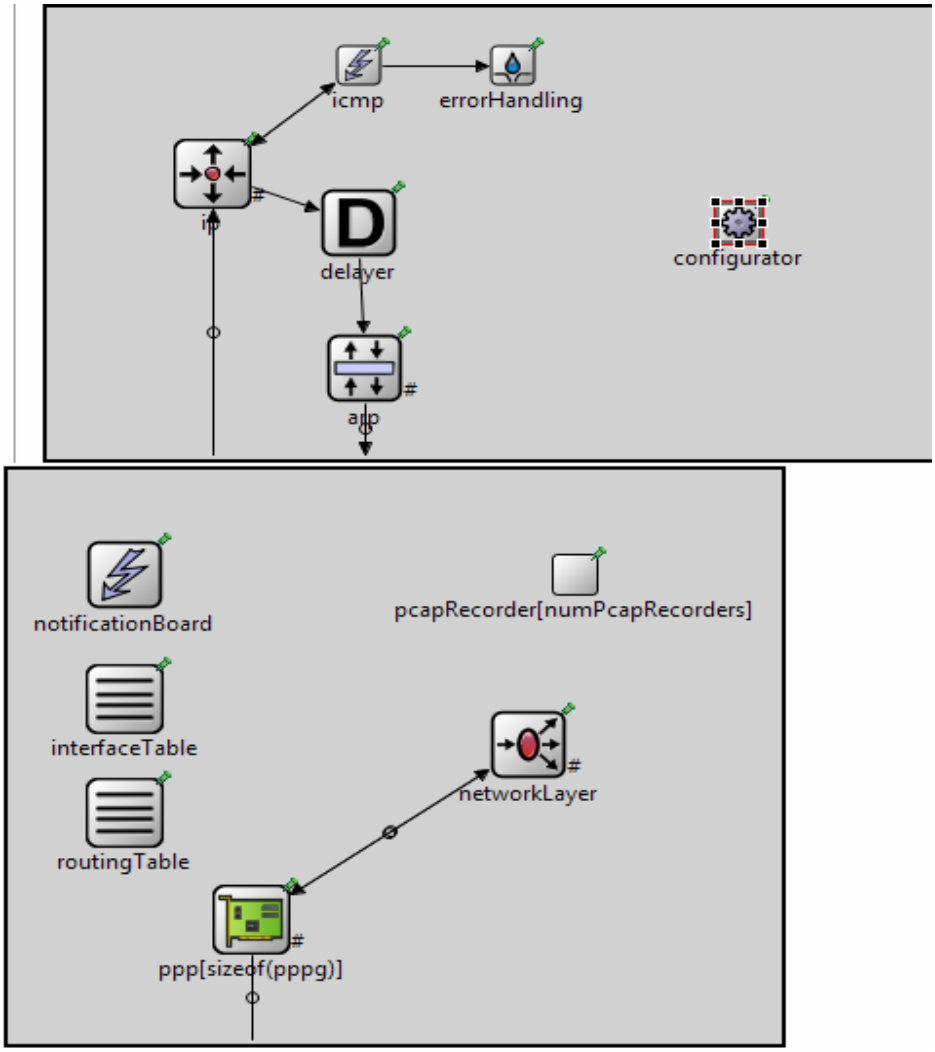


Figure 4.3 Component of internet cloud

4.6 Control channel:

Has exactly one instance in every network model that contains mobile or wireless nodes. This module gets informed about the location and movement of nodes, and determines which nodes are within communication or interference distance. This info is then used by the radio interfaces of nodes at transmissions.

4.7 IP4NetworkConfigurator:

This module assigns IP addresses and sets up static routing for an IPv4 network. It assigns per-interface IP addresses, strives to take subnets into account, and can also optimize the generated routing tables by merging routing entries.

4.8 Emulation of explosive detection mechanism:

In order to emulate the explosive detection mechanism, an assumption was considered, which states that vehicles will be equipped with traffic sources (although vehicles do not have traffic sources in reality), yet the traffic sources will periodically send data to sensors, emulating the physical characteristics of loaded versus unloaded vehicles.

In reality and in magnetic detection mechanism, unloaded vehicles have no abnormal radiation patterns for the ferrous materials that they contain (the fact that cars are ferrous materials for the iron they contain). On the other hand, loaded cars show abnormal radiation patterns.

"Magnetic sensors measure magnetic flux or the strength and direction of a magnetic field; a variation in the magnetic field is caused by an input which creates or alters the magnetic field such as a ferrous object moving within the earth's magnetic field"[15]. Shows in figure 4.3.

[15] http://www.dtic.mil/dtic/tr/fulltext/u2/a475908.pdf

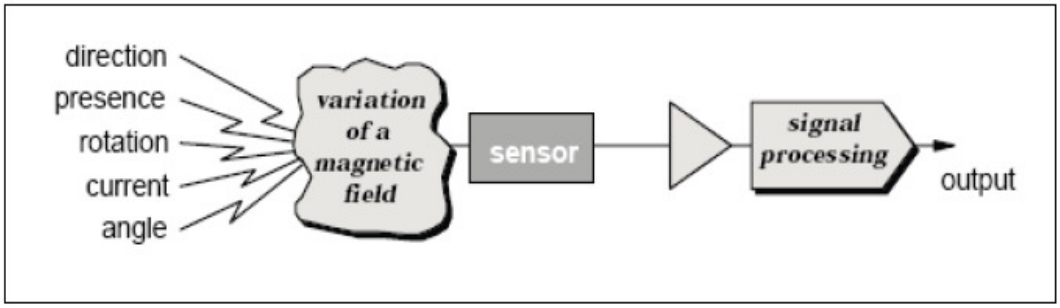


Figure 4.4 Schematic of magnetic sensing *(*Michael J. Caruso et al, 2007*)*

Based on that, loaded versus unloaded vehicles have different values of magnetic field characteristics, therefore, the assumption was as follows:

$$\textit{Alert (traffic)} = \begin{cases} \textit{Unloaded: 1 Byte of UDP from car to sensor} \\ \textit{Loaded: 23 Bytes of UDP from car to sensor} \end{cases}$$

In other words, abnormal magnetic field data assumed to fill the 23Bytes of data field in the AM packet, while the normal one was assumed to fill 1Byte enough to store the node ID (car's). These assumptions were used to emulate the explosive detection mechanism rather than simulating the sensor itself since it would be out of this research's scope.

In order to verify the model, one car (out of 30) was equipped with a bizarre traffic source (23 Bytes of UDP traffic) to emulate an abnormal magnetic field characteristics around the car, while other cars were equipped with 1B UDP traffic to emulate the normal magnetic field characteristics.

Chapter five

Experiments and Evaluation

5.1 Introduction:

In this chapter experimental results that were taken represent two phases of research work: validation results and verification results.

The validation results are those which reflect the correctness of the built model, such as average end-to-end delay for the network, which indicates that the network was built correctly and that traffic was transceiver between sensors and management nodes successfully. While the verification results are those indicating that the built model was designed to deliver the objectives of the research. Verification results varied in their meaning, such as “received packets at each sensor node” which shows the relation between the number of received packets at each sensor and the distance of cars to clusters of sensors. Such result shows which area the loaded vehicle is approaching.

5.2 Validation phase:

In the validation phase, the aim was to show if the system is working, that is, to show if the WSN was integrated with IoT and data is being transceiver between the two parties successfully regardless whether the system can detect explosives or not.

Figure 5.1 shows the integration between the WSN and IoT using sensor gateways placed in the middle of the sensors cluster. The number of sensors was picked according to the size of the covered area, the more the size of the covered area the more the number of sensors deployed. This has been done by assigning an integer number to the vector size of the sensors, and this number is equal to the size of the covered area multiplied by itself as follows:

```
int netSize;
```

```
sensor3[netSize * netSize]
```

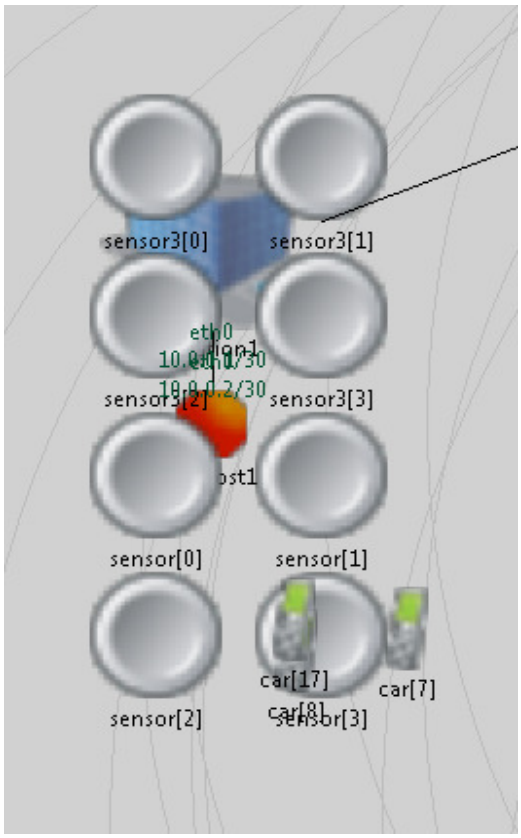


Figure 5.1 Integration between the WSN and IoT

Three locations were used, with a longitude distance of approximately 20 – 25km between each of them. The three locations represent the management at each local place of interest, such as malls, shopping places, police stations, etc… the three locations are connected to a centralized management through internet. Internet was represented in OMNET++ using internet cloud, which contains virtual infrastructure. The OMNET++ considers the delay and data rate values of any traffic passing through internet by deploying the delayer module, which can be configured to give realistic random values of delay and data rate values that exist on real scenarios. In this research, the delayer was configured to use delay of uniform(100kbps,1Mbps), while using the value

20ms+truncnormal(200ms,60ms), the 20ms is the initial delay for setting up the connection, while the truncated normal distribution that gives random values between 200ms and 60ms as a maximum a minimum delay values respectively.

In order to validate the system, UDP traffic generators were set up on each sensor (total number of 24 traffic sources, one for each sensor) with one UDP sink application on the management. UDP traffic settings for each sensor are shown in table 5.1.

Parameter	Value
Number of UDP applications	1
Application Type	UDP Basic Burst Application
Destination Hostname	"mgmt"
Local Port	1234
Destination Port	1234
Message Length	1Byte
Send Interval	0.5s + uniform(-0.001s,0.001s)
Burst Duration	0.01 Seconds
Sleep Duration	0 Seconds
Start Time	5 Seconds
Delay Limit	10 Seconds

Table 5.1 UDP traffic settings for each sensor

The basic measure to validate the system and whether it is successfully delivering traffic from sources to destination considering the impairments is the end-to-end delay.

The delay is the measured time between sending a packet from a source and receiving it at another node, or:

Delay (in seconds) = distance between source and distension (meters) / speed (meter/second)

The average end-to-end delay for the network as measured, results of the delay for the 24 sources of UDP traffic is shown in figure 5.2

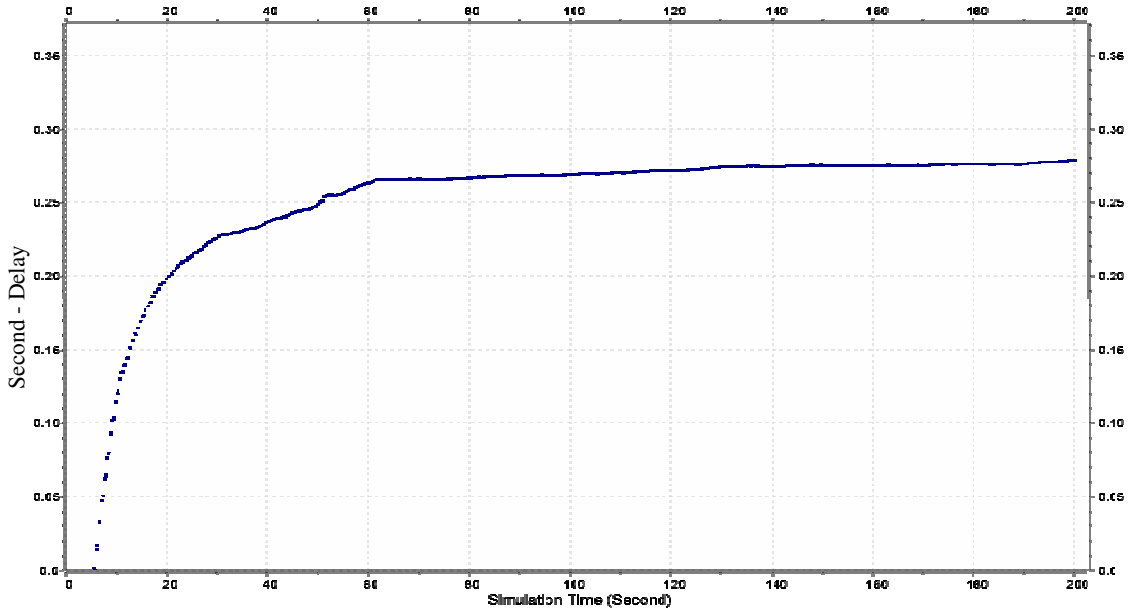


Figure 5.2 Average end-to-end delay

The figure is an indicator that the system is working properly, stabilizing the delay at a value less than 0.28 seconds. There are many others representations of the validation process, such as throughput, SNR, etc.. that will be shown in the next phase, which is the verification.

5.3 Verification phase:

This phase is the core of this research, which gives an indication whether or not the system is achieving the objectives which the system was built to achieve. The main

objective of this research was to integrate both WSN and IoT to use in explosive detection (and to be generalized on other domains of sensors applications), therefore, this phase included assumptions to emulate the explosive detection mechanism rather than simulating the explosive detection sensors themselves.

The reason behind that is after investigating the used simulation framework, OMNET++, and the simulation packages (MiXiM and Inet), developing an explosive detection sensor from scratch would take more time than the time dedicated for this research, hence, a commercial explosive detection sensor (CROSSBOW) was studied (Salatas Vlasios, 2005), and the detection mechanism was generally investigated.

The Crossbow sensor uses Active Message (AM) packet format, which consists of control information fields (sensor ID, next hop, etc..) and Data fields. The size of the data field is 23B and it consists of data that represents the magnetic field values (in case of magnetic detection mechanism), and other data fields in case of other detection mechanism, in addition to the Node ID which is also stored in the data field.

Simulation scenario was run 10 times using random seed for each run, each run for 200 simulation seconds in order to achieve reliable results.

5.4 Results:

A- Detection of explosives in real time:

The main goal of this research is to alert the management of any threats in real time, in order to avoid any consequences resulting from manual alerting mechanism used nowadays.

In order to achieve that, the system has to show real-time detection of loaded vehicles. Figure 5.3 shows the times where the loaded vehicle approached the sensors and the closeness to the sensor through the density of traffic from car to sensors.

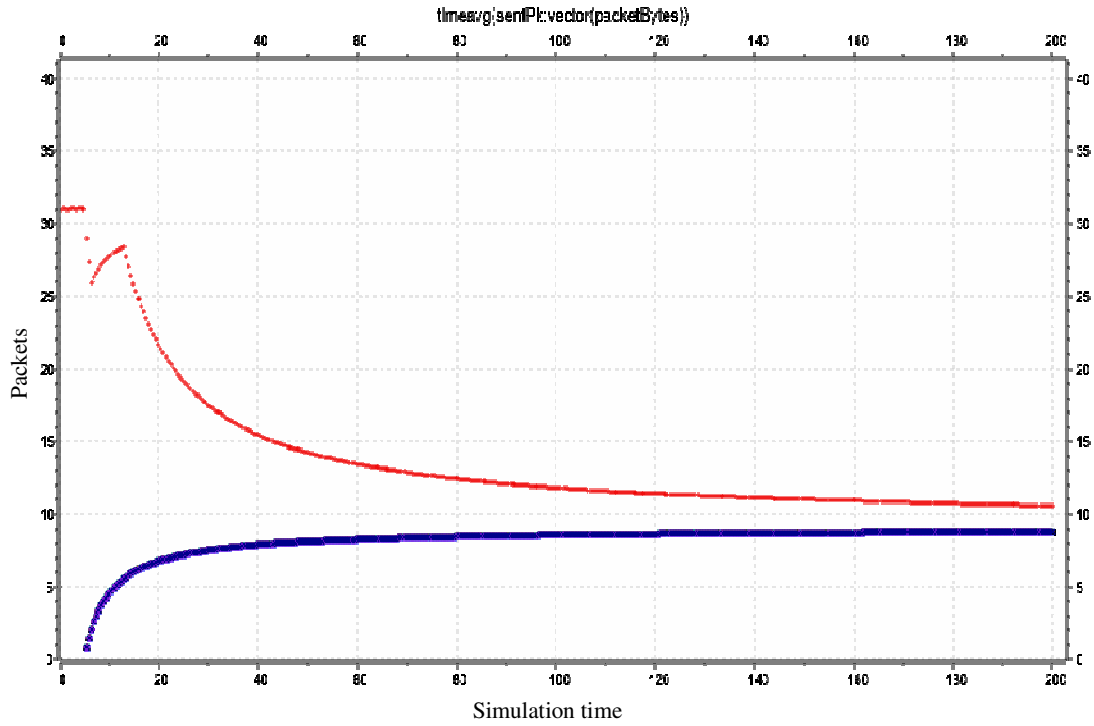


Figure 5.3 Average packets received from each vehicle

Figure 5.3 shows the average number of packets received from each vehicle, including the loaded vehicle. The graph shows clearly that the loaded vehicle's traffic is higher than the unloaded vehicles, since the former is loaded with 23Bytes of data while the others are not. However, the graph does not show "when" the loaded car is detected which required to manipulate the graph in a way that approximates it to the closest discrete form using Difference Quotient[16] as shown in figure 5.4.

[16] http://www.mathwords.com/d/difference_quotient.htm

In figure 5.4 the straight blue line on the 0 x-axis indicates the unloaded vehicles while the red dots show the loaded vehicles and the times of detection. The y-axis indicates the density of detection, the higher (and lower since the Difference Quotient is calculated using difference equation and results could be in minus) the dots the closer to sensor the car is. That is, the exact time of detection can be determined, so can be the closeness to the sensor.

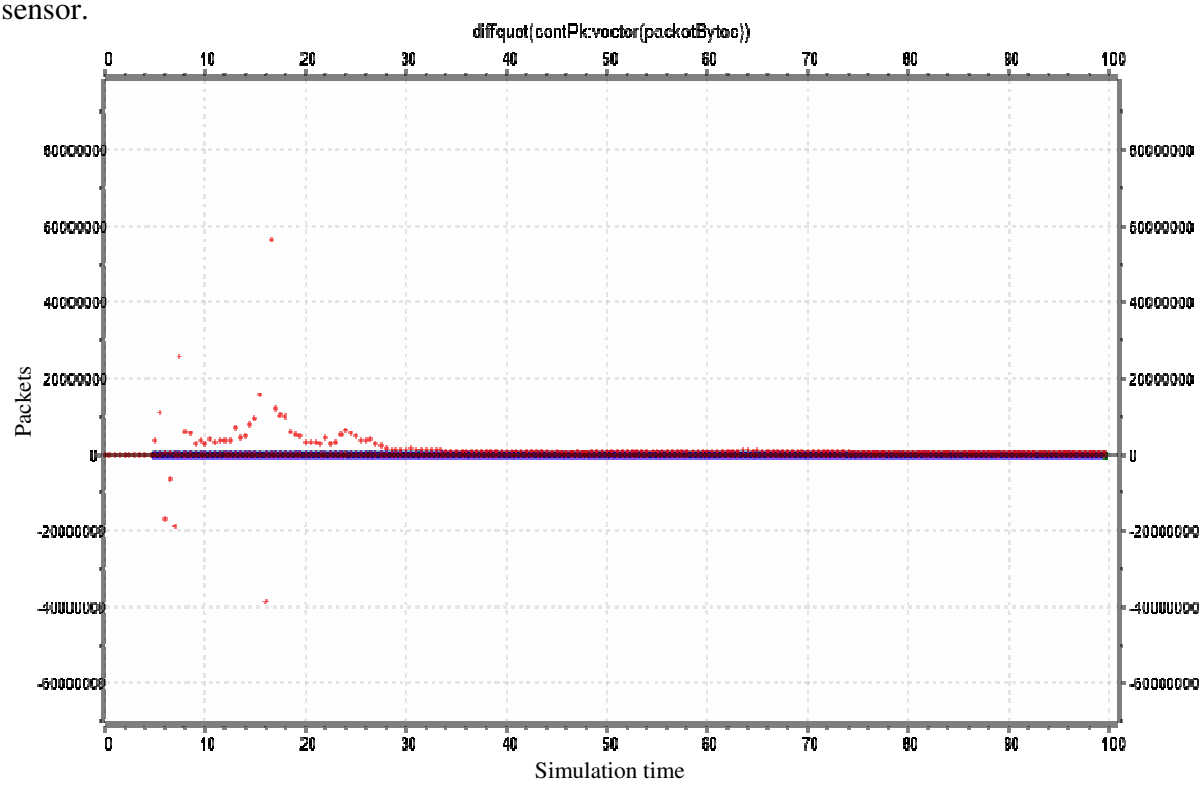


Figure 5.4 Average packets received from each vehicle using Difference Quotient

One may ask about how the management could determine the location of the detected vehicle. The received packets at the managements contain node ID field, and upon comparing the ID with its database the management can locate the location of the deployed sensor.

B- Received traffic at each sensor:

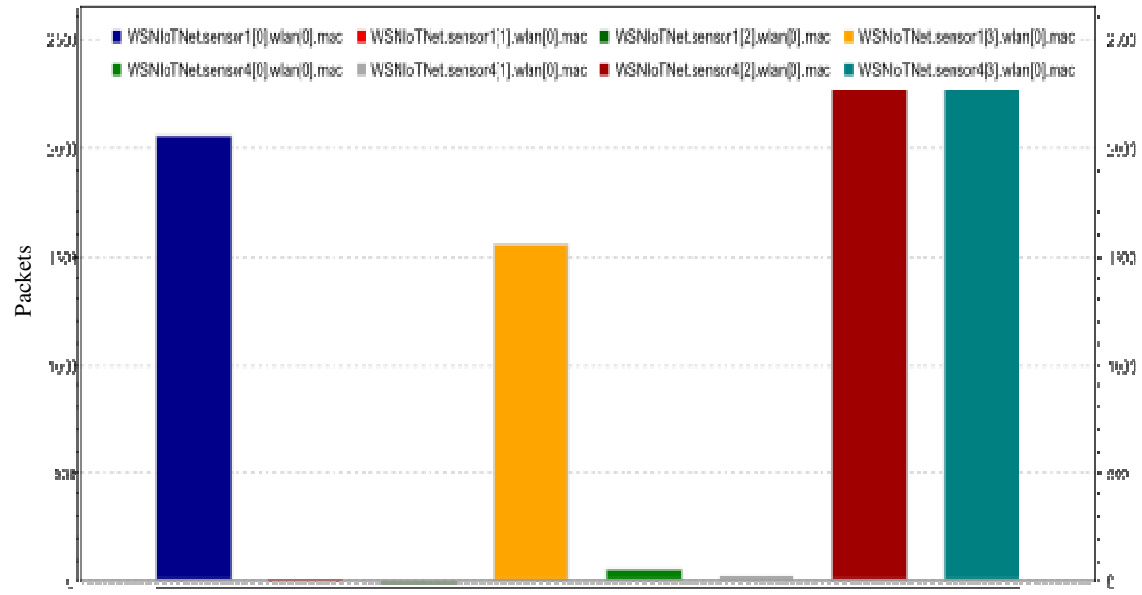


Figure 5.5 Received traffic at sensors in no detection scenario

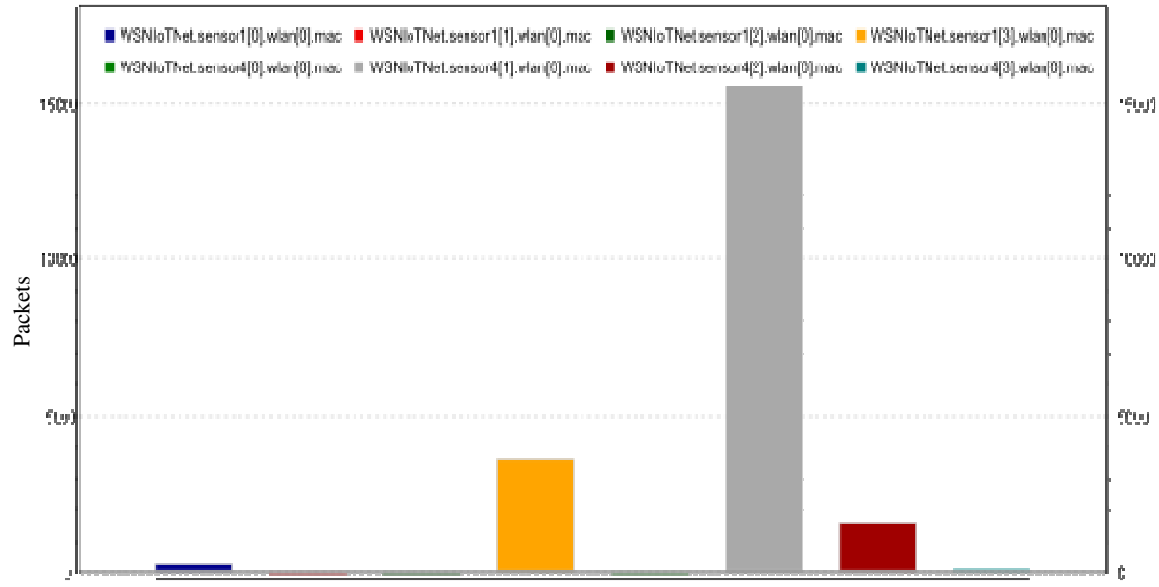


Figure 5.6 Received traffic at sensors in detection scenario

Figures 5.5 and 5.6 show which sensor detected the loaded vehicle. The first figure shows the traffic coming from sensors where there was no detection of explosives, while the second shows that the second sensor of the cluster 4 is receiving high traffic, and according to our assumption, the sensor is detection explosives. Location of the sensor can be shown on the map.

C- Radio State for close cluster

This also can be shown in the radio state of the sensors, where it is clear that the radio of same sensor (sensor 1 of the 4th cluster) has been in send and receive modes more than the other modes (idle, sleep) in the detection scenario (Figure 5.7), while it is showing normal behavior compared to other sensors in the other scenario. (Figure 5.8).

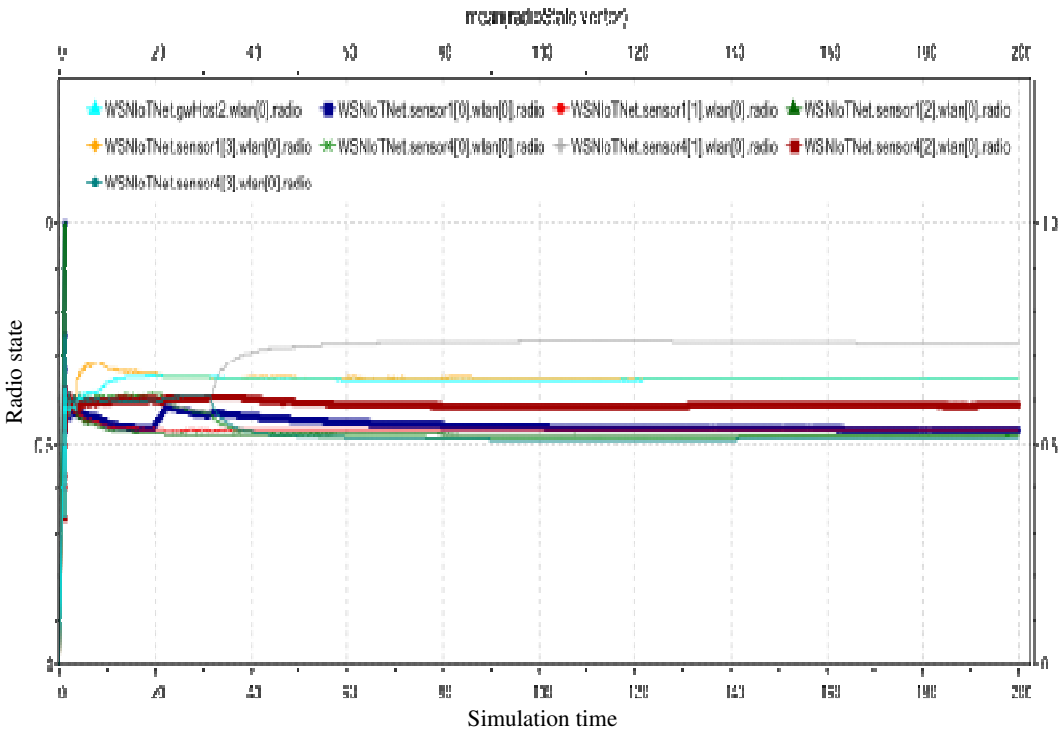


Figure 5.7 Radio state in detection scenario

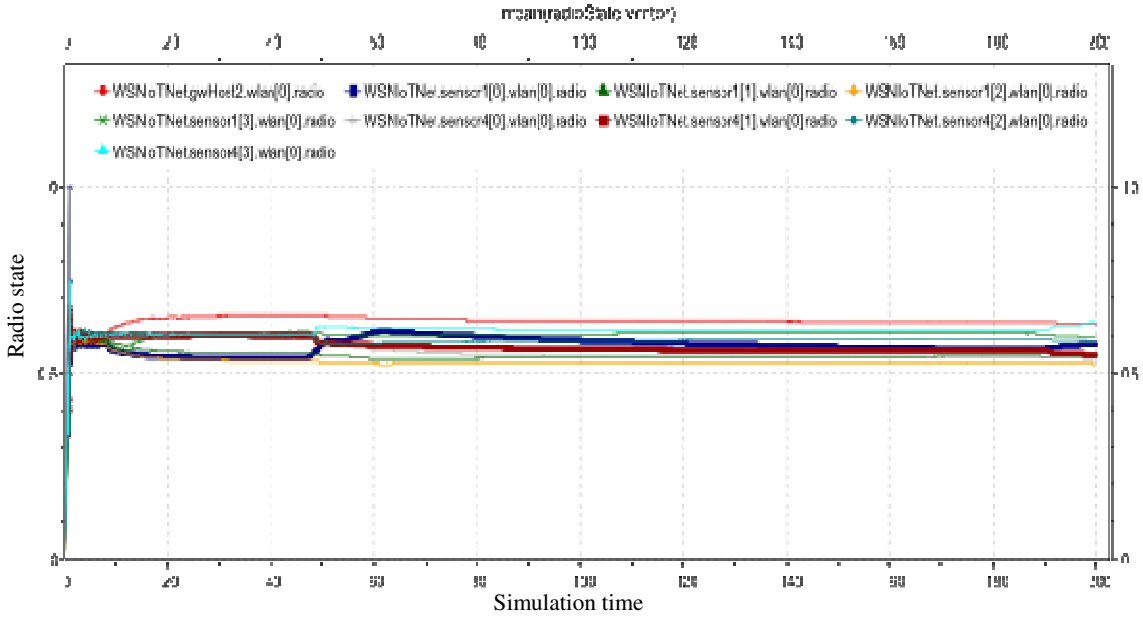


Figure 5.8 Radio state in no detection scenario

D- Bit rate at each gateway:

Additionally, the management can determine the location of the detected vehicle based on determining bit rate of traffic coming from each location, the following shows the difference between bit rates values of traffic from the gateway sensors to management. Figure 5.9 represents normal traffic from the 3 gateways (a gateway for each location), while Figure 5.10 represent the high bit rate of gateway number 2 (of color red in the graph), which is the gateway of the location through which the loaded vehicle pass.

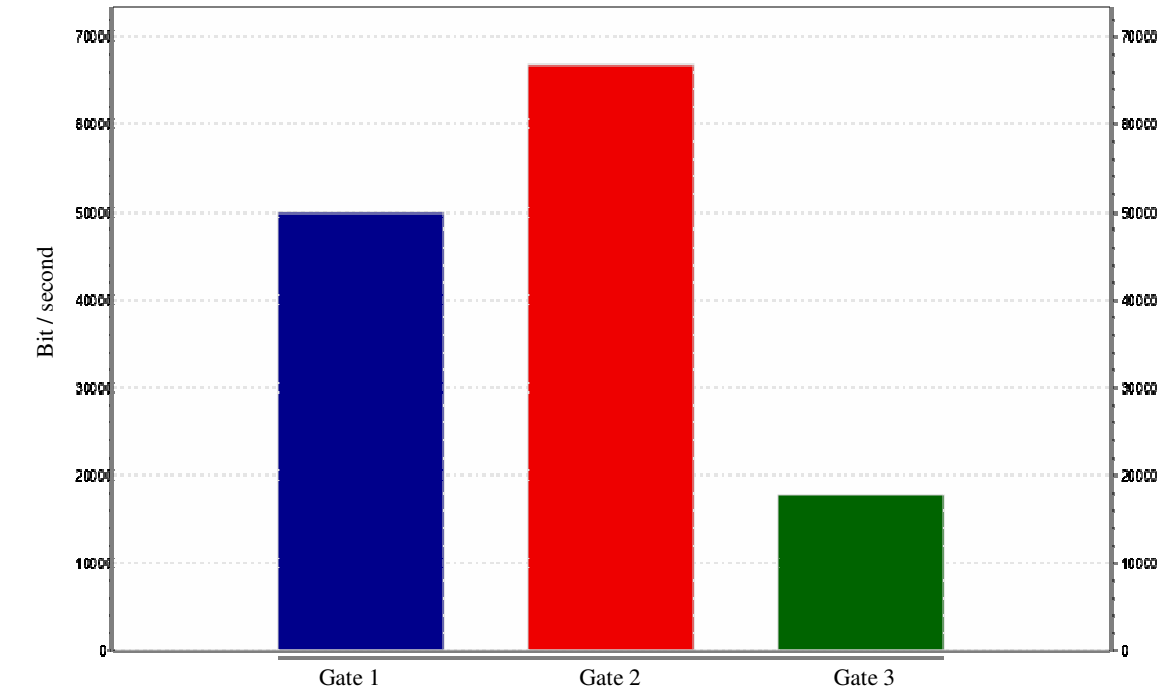


Figure 5.9 Traffic from 3 gateways

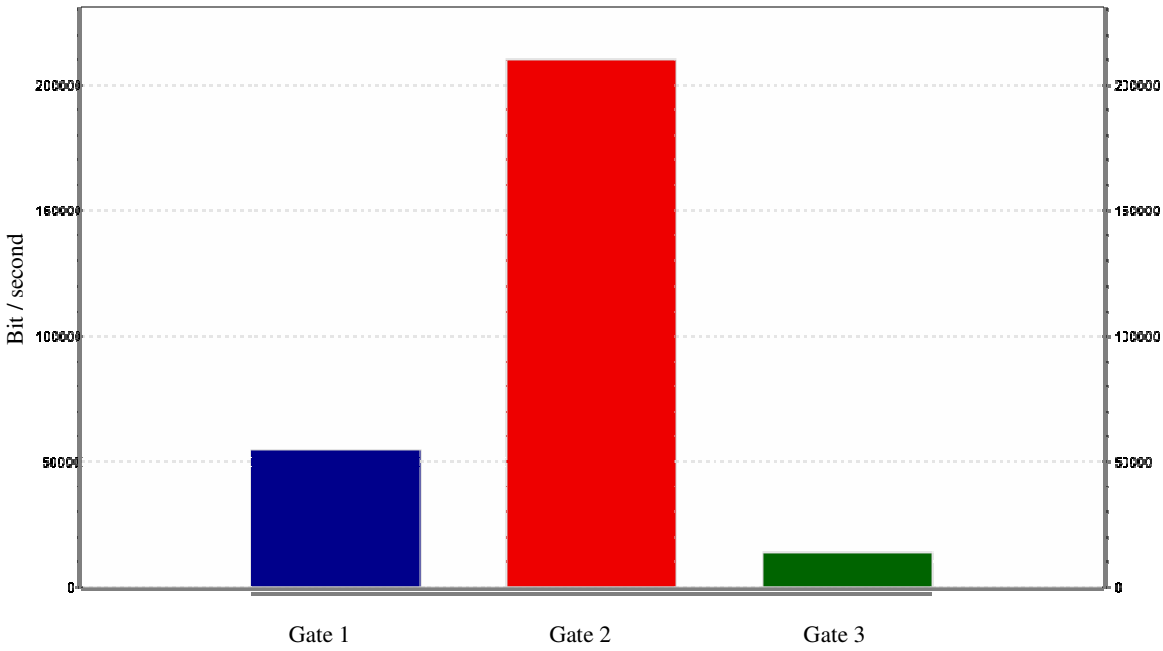


Figure 5.10 Bizarre traffic at gateway 2

E- Energy consumption:

It is vital to show the sustainability of battery for sensors and gateways battery lifetime is one important characteristic of sensors.

In the following two graphs, it is clear that the energy consumption of batteries is linear with time, however, it is important to show that for the scenario where a loaded vehicle was approaching the clusters 1 and 4, sensors in these clusters were active more than others, therefore, the energy consumption was more than in the case of no loaded vehicle for the same clusters.

The sensor batteries were configured to consume current as follows:

State of sensor	Value of current reduction consumption (mA)
Send	0.450
Receive	0.390
Idle	0.19
Sleep	0.010

Table 5.2 Sensor batteries parameters

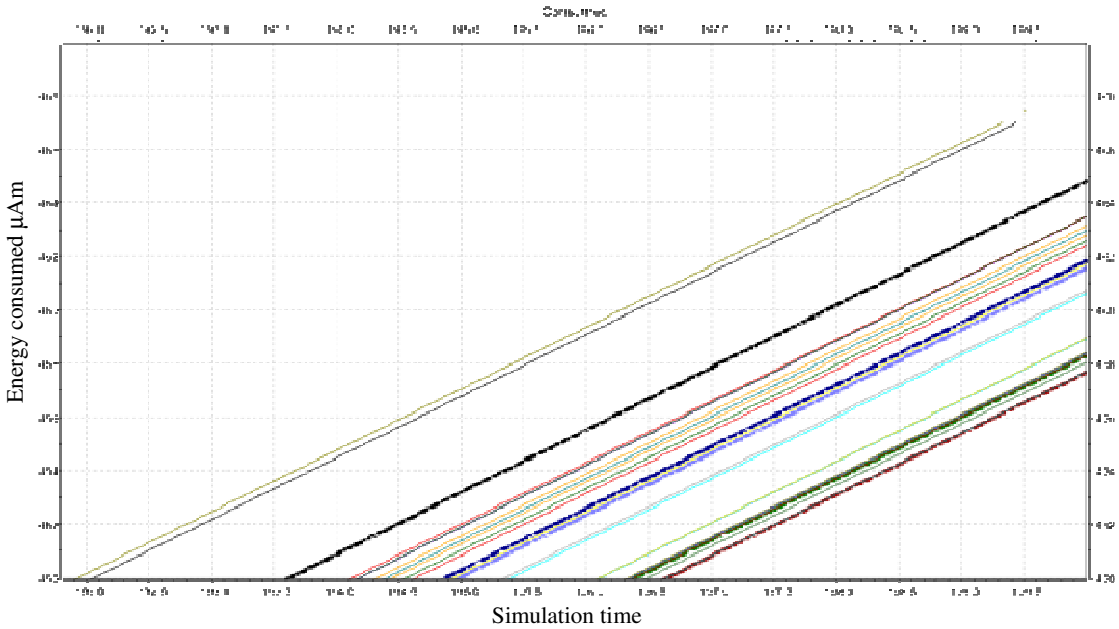


Figure 5.11 Energy consumption in detection scenario

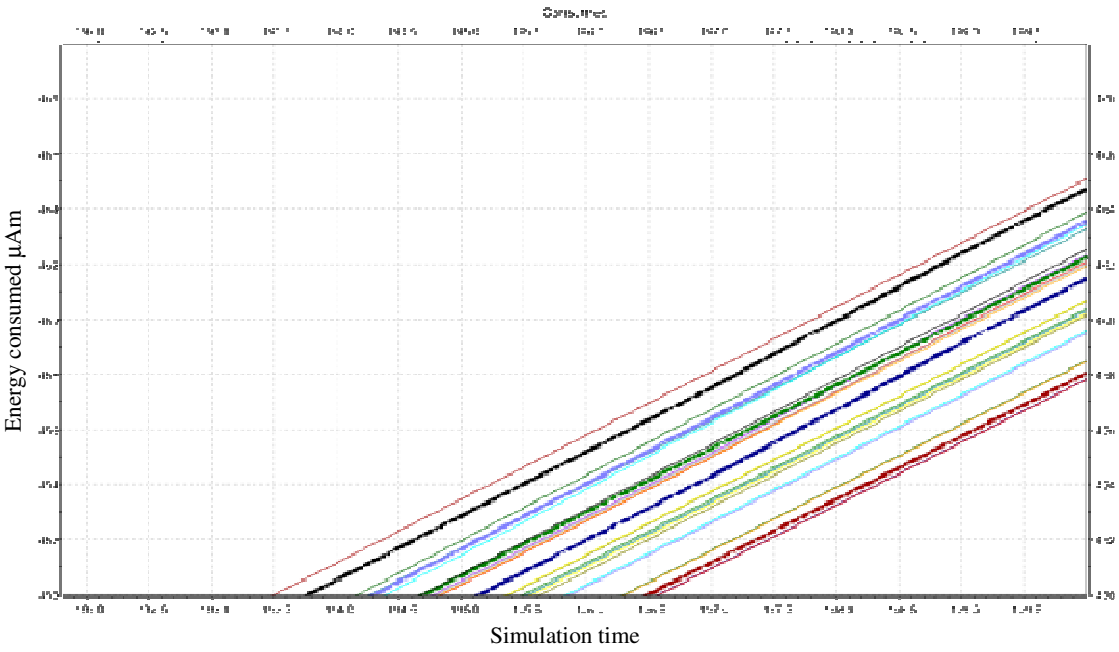


Figure 5.12 Energy consumption in no detection scenario

A figure 5.11 and 5.12 was truncated since the effect on energy consumption and values started to show differences approximately after the last quarter of simulation time.

Figures 5.13 shows that more energy was consumed by sensors closed to the loaded vehicle since those sensors work on “send” mode more than other sensors, and hence they consume more energy because of the relative excessive usage of current, the voltage was fixed for all sensors (12Volts). The energy is calculated using the following electrical energy equation:

$$Energy\ (Watts) = Voltage\ (Volts)\ x\ Current\ (Amps)$$

F- Comparison with Current Mechanism:

Nowadays, malls – for instance – require the management of the mall to employ people who keep scanning entering cars for any explosives using handheld scanning devices, and this would cost the management more money as salaries for those people. Such device alerts the person who is carrying it about any suspicious packages in a car. By the alert, the employee would stop the car, threatening his own life in case of resistance of car driver, and in the case of car being stopped it would take time for the employee to call the police or the security in order to inform them about the situation, and their reaction would take time too.

Assuming that a device alerts the employee carrying it, the employee would take a minimum of 5-10 seconds to pull the “walkie-talkie” and dial the security, security would take same time to answer, and then it could take variable time for the security to react, considering their location from the incident, assuming that they are next to the incident, it would take at least a minute to ask the driver to pull down, or ask him for an ID, hence the total time would be from 70 to 80 seconds, approximately.

Based on that, by comparing the time of detection and informing the security, which is approximately 10-20 seconds in the case of nowadays mechanism, and the proposed model's mechanism, which takes 0.28 seconds, it is useless to do a real comparison between the two mechanisms.

Chapter six

Conclusion and Future Work

6.1 Conclusion

The use of internet and in particular IoT as a medium to help in centralizing the management of explosive detection mechanism and alerting was proposed in this research. Results have shown that the model has successfully alerted the centralized management in average of 0.28 seconds end-to-end delay through the IoT as a medium.

The sensor's explosive detection mechanism was emulated rather than simulated because of the time required to develop the sensor which may exceed the time frame given for this research.

The emulation was based on a commercial sensor (Crossbow) and an assumption was being considered, which is to equip the vehicles with traffic sources to mimic the radiation patterns of ferrous surface. It was assumed that the vehicle that has no explosives would send traffic of size 1Byte while the loaded vehicle has a 23Bytes of data in the data field of its transmitted packet.

By assuming the above, the detection mechanism was emulated successfully and results of detection in real-time were shown.

The management can use different sources to compare with its database for alerting purposes, such as received traffic at each gateway or at each sensor, sensor's radio state, and other indicators. If these values exceeded some threshold that has been investigated and fixed, a reaction would be automatically taken from the management.

6.2 Future work:

1- Simulation of the sensor itself rather than emulating the detection mechanism

2- Make a realistic reaction to explosives' detection, such as locking mall, alerting people to exit, etc…

3- Make reaction management locally and proposing Fault-tolerance mechanism using alternative medium in case of internet failure.

References:

- Akyildiz I. F., W. Su, Y. Sankara subramaniam, and E. Cayirci, "Wireless sensor networks: a survey" Computer Networks, IEEE, vol. 38, pp. 393-422, 2002.
- Cayirci E., et al., "Wireless sensor networks: a survey." *IEEE Computer*, vol. 38, no. 4, pages 393-422. Mar 2002. Available from http://www.ece.gatech.edu/research/labs/bwn/sensornets.pdf, last accessed 23 Aug 2007.
- Cui, S., Madan, R., Goldsmith, A. J., and Lall, S. Joint routing, mac, and link layer optimization in sensor networks with energy constraints. In Proc. of IEEE International Conference on Communications (ICC'05), pages 725—729, 2005.
- David L. Brock, MIT Auto-ID Center, MIT-AUTOID-WH-002, "The Electronic Product Code", January 2001.
- Demirkol, I., Alagoz, F., Delic, H., and Ersoy, C. Wireless sensor networks for intrusion detection: Packet traffic modeling. IEEE Communications Letters, 10(1):22—24, 2006.
- John A. Stankovic, "Research Challenges for Wireless Sensor Networks." Available from www.cs.virginia.edu/sigbed/archives/stankovic.pdf, last accessed 7 Sep 2007.
- Karl H. and A. Willig, Protocols and architectures for wireless sensor networks, 1st ed. Wiley, June 2005.
- Ma, Y. and Aylor, J. H. System lifetime optimization for heterogeneous sensor networks with a hub-spoke topology. IEEE Transactions on Mobile Computing, 3(3):286—294, 2004.
- Michael J. Caruso et al, A new perspective on magnetic field sensing, 1998.

- MSP410 User Manual. Available from www.crossbow.com, last accessed 8 Oct 2007.
- Nomadics Inc., Final technical report "Explosive Chemical Signature-Based Detection of IEDs." Dec 2004. Available from http://stinet.dtic.mil/cgi-bin/GetTRDocAD=ADA430111&Location=U2&doc=GetTRDoc.pdf, last accessed 6 July 2007.
- Øverby, H. and Stol, N., Effects of bursty traffic in service differentiated optical packet switched networks. Optics Express, 12(3):410—415, 2004.
- Paxson, V. and Floyd, S., Wide-area traffic: The failure of poisson modeling. IEEE/ACM Transactions on Networking, 3:226—244, 1995.
- S. Pattem, B. Krishnamachari, and R. Govindan. The impact of spatial correlation on routing with compression in wireless sensor networks. In Proceedings of the Third International Symposium on Information Processing in Sensor Networks (IPSN) , 2004.
- Tang, S. An analytical traffic flow model for cluster-based wireless sensor networks. In Proc. of 1st International Symposium on Wireless Pervasive Computing, 2006.
- Wang, P. and Akyildiz, I. F., Spatial correlation and mobility aware traffic modeling for wireless sensor networks. In Proc. of IEEE Global Communications Conference (Globecom'09), 2009.
- Wang, Q. and Zhang, T., Source traffic modeling in wireless sensor networks for target tracking. In Proc. of the 5th ACM International Symposium on Performance Evaluation of Wireless Ad-Hoc, Sensor, and Ubiquitous Networks (PE-WASUN'08), pages 96—100, 2008.

- XyTrans Inc., “Longer Stand-off Distance for IED Detection.” Jul 2006. Available from www.xytrans.com/pdf/IED%20Detection%20White%20Paper.pdf, last accessed 8 Sep 2007.
- Abu B. Kanu, Prabha Dwivedi, Maggie Tam, Laura Matz and Herbert H. Hill Jr. Ion mobility–mass spectrometry Article first published online: 16 JAN 2008.
- Alcaraz Cristina et al, Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration?, 2010.
- Al-Karaki,J.N,Al-Mashagbeh: Energy-Centric Routing in Wireless Sensor Networks Computers and Communications, ISCC 06 Proceedings, 11th IEEE Symposium (2006).
- Avinash.Vanimireddy, Detection of Explosives Using Wireless Sensor Networks, 2012.
- Buratti Chiara, An Overview on Wireless Sensor Networks Technology and Evolution, 2009
- Chhimwal Mrs. Poonam, Dhajvir Singh Rai, Deepesh Rawat, “ Comparison between Different Wireless Sensor Simulation Tools”, Mar. - Apr. 2013, PP 54-60 www.iosrjournals.org.
- Chien-Chung Shen, Chavalit Srisathapornphat, Chaiporn Jaikaeo: Sensor Information Networking Architecture and Applications, IEEE Personal Communications, pp. 52-59 (August 2001).
- Christin D., A. Reinhardt, P.S. Mogre, R. Steinmetz. Wireless Sensor Networks and the Internet of Things: Selected Challenges. 8th GI/ITG KuVS Fachgesprch “Drahtlose Sensornetze”, 2009

- Christin Delphine et al, Wireless Sensor Networks and the Internet of Things: Selected Challenges, 2009.
- Curren David, "A Survey of Simulation in Sensor Networks", Technical Report, Department of Computer Science, University of Binghamton, 2007.
- Davis, A., Airport protection using wireless sensor networks, 2012.
- Gershenfeld Neil, Raffi Krikorian and Danny Cohen, Scientific American Magazine, October 2004.
- Harald Sundmaeker, Patrick Guillemin, Peter Friess, Sylvie Woelfflé, march 2010, Vision and challenges for realising the IoT, CERP-IoT – Cluster of European Research Projects on the Internet of Thing.
- Hariharan Balaji and Arjun Sasidharan ,iWEDS - An Intelligent Explosive Detection and Terrorist Tracking System Using Wireless Sensor Network , July 2011.

  http://www.magneticsensors.com/datasheets/am.pdf, last accessed 15 Sep 2007.
- Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, Erdal Cayirci: A Survey on Sensor Networks, IEEE Communications Magazine, pp. 102-114 (August 2002).
- José A. Gutierrez, Marco Naeve, Ed Callaway,Monique Bourgeois,Vinay Mitter, Bob Heile, IEEE 802.15.4: A Developing Standard for Low-Power Low-Cost Wireless Personal Area Networks, IEEENetwork, pp. 12-19 (September/October 2001).
- Junhong Wu, Yang Yang, etc., “Network Simulation Method and OPNET's Simulation”, Technology Computer Engineering, 2004, 30(5): 106-108.

- Kevin Ashton, RFID Journal, 22 June 2009. I could be wrong, but I'm fairly sure the phrase 'Internet of Things' started life as the title of a presentation Imade at Procter & Gamble (P&G) in 1999".
- Lessmann Johannes, Peter Janacik, Lazar Lachev, Dalimir Orfanus, "Comparative Study of Wireless Network Simulators," ICN, pp.517-523, Seventh International Conference on Networking (ICN 2008), 2008).
- LEWIS.F. L., Wireless Sensor Networks, 2004.
- Lin C, Xiong N, Park JH, Kim T-H. Dynamic power management in new architecture of wireless sensor networks International Journal of Communication Systems 2009; 22(6):671–693.]
- Lisa Theisen, Ph.D. David W. Hannum Dale W. Murray John E. Parmeter, Ph.D., November 2004, Survey of Commercially Available Explosives Detection Technologies and Equipment 2004, The National Law Enforcement and Correction Technology Center, a Program of the National Institute of Justice, U.S. Department of Justice.
- Meloan Steve, Sun Microsystems, 11 November 2003.
- Michael J. Caruso & S. Lucky, "Vehicle Detection and Compass Applications using Magnetic Sensors," Honeywell Inc. Available from
- Mohanty, Pradeep K., "A FRAMEWORK FOR INTERCONNECTING WIRELESS SENSOR AND IP NETWORKS", Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium.
- Neil C.Rowe, Matthew O'Hara,and Gurminder singh, Wireless sensor networks for detection of IED Emplacement Networks and Networking, 2009

- Potyrailo RA et al, Wireless sensors and sensor networks for homeland security applications, 2012.
- Potyrailo RA, Nagraj N, Surman C, Boudries H, Lai H, Slocik JM, Kelley-Loughnane N, Naik RR, Wireless sensor networks for homeland security applications new selective chemical-sensing approach was realized using an attractive ubiquitous platform of battery-free passive Radio-Frequency Identification (RFID) tags adapted for chemical sensing, 2012.
- Rakočević, Goran,Overview of Sensors for Wireless Sensor Networks, 2009.
- Roman R., J. Lopez. Integrating Wireless Sensor Networks and the Internet: a Security Analysis. Internet Research, Vol. 19, no. 2, pp. 246-259, 2009.
- S. Simi & Maneesha V. Ramesh, Real-time monitoring of explosives using wireless sensor networks, 2010.
- Sarjoun S. Doumit, Dharma P. Agrawal: Self-Organizing and Energy-Efficient Network of Sensors, IEEE, pp. 1-6 2002.
- Simi S & Joshua D Freeman, Robot Assisted Wireless Sensor Network for Monitoring and Detection of Explosives in Indoor Environment, 2011.
- Stefano GIROTTI, Elida N. FERRI, Pasquale CAPUTO, Gianluca GUARNIERI, Sergei A. EREMIN Angel MONTOYA , Maria J. MORENO, and Marcello D'ELIA, Development of chemiluminescent methods for explosives detection Elisabetta MAIOLINI.
- Vlasios Salatas, "Object Tracking Using Wireless Sensor Networks," Masters Thesis, Naval Postgraduate School. Sep 2005. Available from

http://stinet.dtic.mil/cgibin/GetTRDoc?AD=ADA439599&Location=U2&doc=GetTRDoc.pdf, last accessed 25 Aug 2007.

- Vlasios Salatas, "Object Tracking Using Wireless Sensor Networks," Masters Thesis, Naval Postgraduate School. Sep 2005
- Weisman Robert, The Boston Globe, 25 October 2004.
- Wendi B. Heinzelman, Amy L. Murphy, Hervaldo S. Carvalho, Mark A. Perillo: Middleware to Support Sensor Network Applications, IEEE Network, pp. 6-14, (January/February 2004).
- Z. Z. Marco, K. Bhaskar, in "Integrating Future Large-scale Wireless Sensor Networks with the Internet", USC Computer Science Technical Report CS 03-792, 2003.
- Zheng Jun, Abbas Jamalipour, WIRELESS SENSOR NETWORKS A Networking Perspective Book, August 13, 2010.

APPENDIX 1:

```
<internetCloud symmetric="true">
  <parameters name="good">
    <traffic  src="mgmt"  dest="mgmt"  delay="20ms+truncnormal(200ms,60ms)"
datarate="uniform(100kbps,1Mbps)" drop="uniform(0,1) &lt; 0.01" />
    <traffic               src="location1"               dest="location1"
delay="20ms+truncnormal(200ms,60ms)"    datarate="uniform(100kbps,1Mbps)"
drop="uniform(0,1) &lt; 0.02" />
    <traffic                  src="location1"                  dest="mgmt"
delay="20ms+truncnormal(200ms,60ms)"    datarate="uniform(100kbps,1Mbps)"
drop="uniform(0,1) &lt; 0.03" />
    <traffic                  src="mgmt"                  dest="location1"
delay="20ms+truncnormal(200ms,60ms)"    datarate="uniform(100kbps,1Mbps)"
drop="uniform(0,1) &lt; 0.04" />
    <traffic               src="location2"               dest="location2"
delay="20ms+truncnormal(200ms,60ms)"    datarate="uniform(100kbps,1Mbps)"
drop="uniform(0,1) &lt; 0.05" />
    <traffic                  src="location2"                  dest="mgmt"
delay="20ms+truncnormal(200ms,60ms)"    datarate="uniform(100kbps,1Mbps)"
drop="uniform(0,1) &lt; 0.06" />
    <traffic                  src="mgmt"                  dest="location2"
delay="20ms+truncnormal(200ms,60ms)"    datarate="uniform(100kbps,1Mbps)"
drop="uniform(0,1) &lt; 0.07" />
     <traffic               src="location3"               dest="location3"
delay="20ms+truncnormal(200ms,60ms)"    datarate="uniform(100kbps,1Mbps)"
drop="uniform(0,1) &lt; 0.08" />
    <traffic                  src="location3"                  dest="mgmt"
delay="20ms+truncnormal(200ms,60ms)"    datarate="uniform(100kbps,1Mbps)"
drop="uniform(0,1) &lt; 0.09" />
    <traffic                  src="mgmt"                  dest="location3"
delay="20ms+truncnormal(200ms,60ms)"    datarate="uniform(100kbps,1Mbps)"
drop="uniform(0,1) &lt; 0.1" />

    <traffic   src="**"   dest="**"   delay="10ms+truncnormal(100ms,20ms)"
datarate="uniform(100kbps,500kbps)" drop="uniform(0,1) &lt; uniform(0.01,
0.05)" />

  </parameters>
</internetCloud>
```