WIRELESS SENSOR NETWORKS FOR METROPOLITAN SCALE EXPLOSIVES DETECTION

Maamoun Ahmed, PhD
Radwan Abu Jassar, PhD
Zahraa Jaaz
Middle East University, Jordan Al Nahrain University

Abstract

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.

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 is was proposed.

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: WSN, IoT, Explosives Detection, Omnet++

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 research we discuss the current methods used in detecting explosives, in particular, the use of Wireless Sensor Networks 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).

WSN Integration Types:

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.

Emulation of Detection Mechanism:

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

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

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

In other words, abnormal magnetic field data assumed to fill the 23Bytes of data field in the Active Message (AM) packet format, 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 develping the explosive detection sensor for simulation purposes.

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.

Implementation

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” (the central management host)
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

Results:

- Validation

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.

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

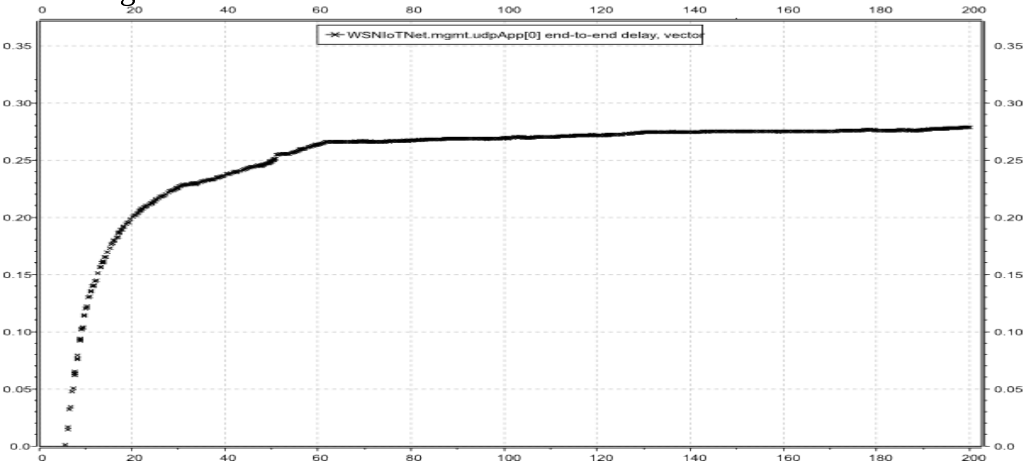

Figure 5.2 average end-to-end delay

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 verification phase.

- Verification

- 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 5.4 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.

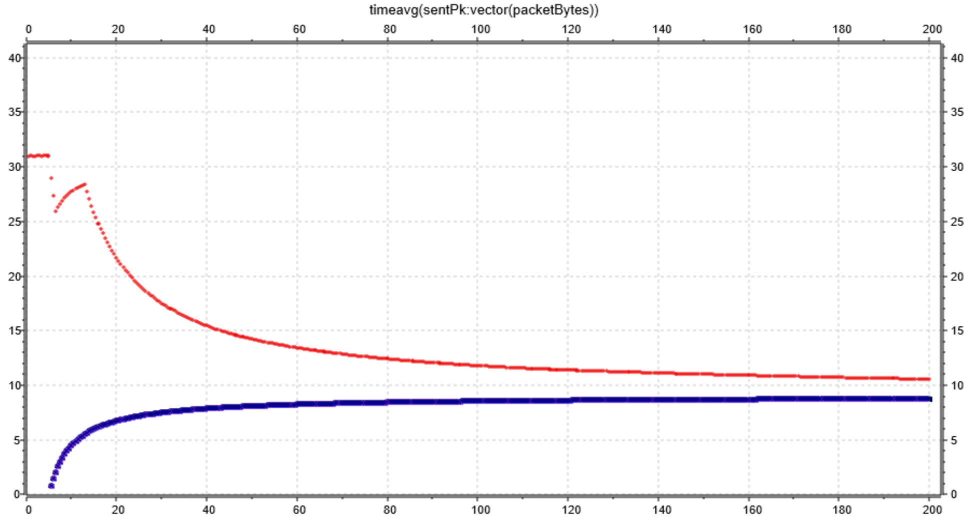

Figure 5.4- Average packets received from each vehicle

Figure 5.4 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[1] as shown in figure 5.5.

In figure 5.5 the straight blue line on the 0 x-axis indicates the unloaded vehicles while the red dots show the loaded vehicles and the times

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

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.

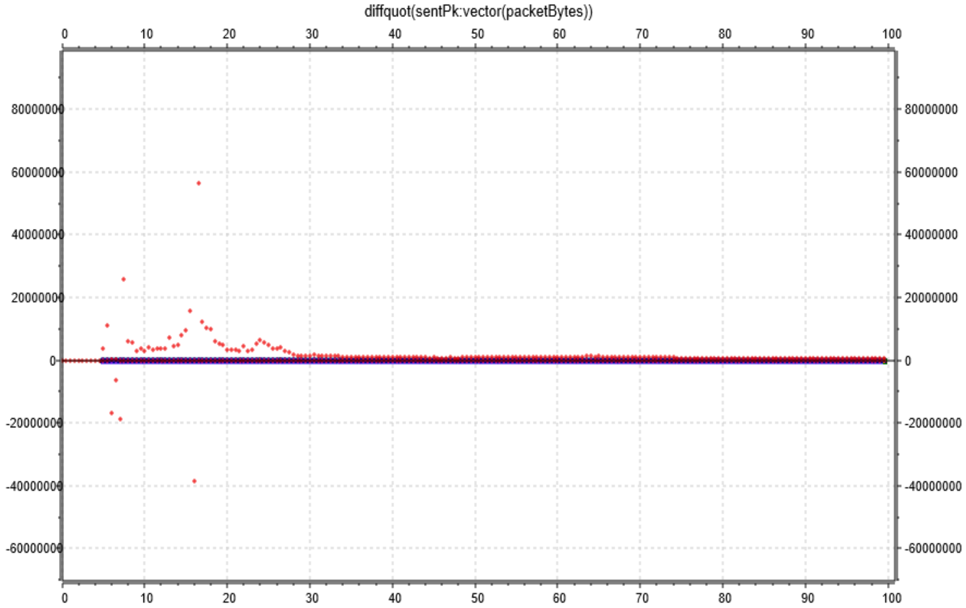

Figure 5.5- Average packets received from each vehicle using Difference Quotient

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.

A- 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 5.8), while it is showing normal behavior compared to other sensors in the other scenario. (Figure 5.9)

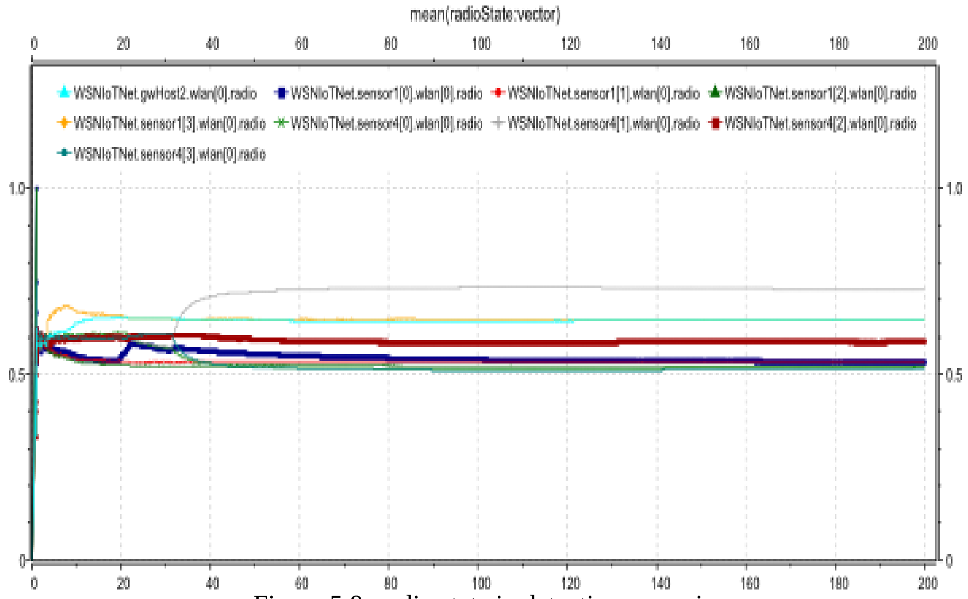

Figure 5.8- radio state in detection scenario

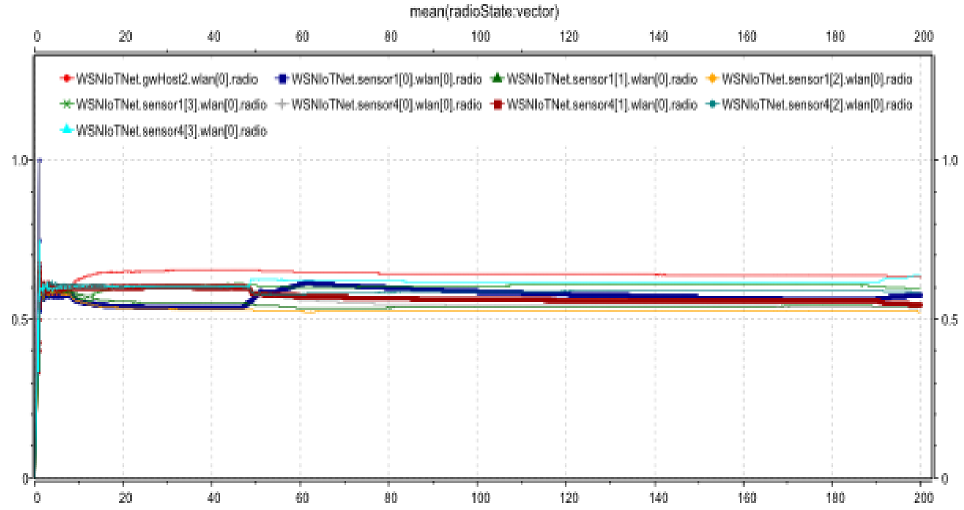

Figure 5.9- radio state in no detection scenario

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.

References:

Clancy, Tom, Carl Stiner, and Tony Koltz. Shadow Warriors: Inside the Special Forces. New York: Putnam, 2002.

Cohen, Andrew, and J.L. Granatstein, eds. Trudeau's Shadow: The Life and Legacy of Pierre Elliott Trudeau. Toronto: Random, 1998.

Meidenbauer, Jorg, ed. Discoveries and Inventions: From Prehistoric to Modern Times. Lisse: Rebo, 2004.

Puzo, Mario. The Family: A Novel. Completed by Carol Gino. New York: Harper, 2001.

Rowling, J.K. Harry Potter and the Chamber of Secrets. New York: Scholastic, 1999