J. Appl. Environ. Biol. Sci., 7(6)126-134, 2017
© 2017, TextRoad Publication

ISSN: 2090-4274
Journal of Applied Environmental and Biological Sciences
www.textroad.com

Efficient Use of Wireless Sensor Network in Explosive Material Detection

Fareeha Zafar[1*], Faisal Hameed[2], Muhammad Ahmed Dar[3]

[1]Assistant Prof Dr., Government College University, Lahore, Pakistan,
[2]M. Phill. Computer Science, Government College University, Lahore, Pakistan,
[3]M. Phill. Computer Science, Government College University, Lahore, Pakistan,

Received: January 30, 2017
Accepted: April 11, 2017

ABSTRACT

The research illustrates efficient use of wireless sensor network in explosive detection. With the surge of terrorism activities around the world, it is important to limit these hazardous activities. There are many systems used to detect the presence of explosive materials. But there is an immense need to upgrade the technology with the usage of latest tiny sensors having enhanced detection capability which can prevent disclosure from human eye. The document suggests the fault tolerant network of wireless tiny sensors which can be emplaced in public places like airports, railway stations, universities, etc. The research suggests that 'Tiny sensor'; latest wireless sensor which in not commercialized yet, can be effectively used in distributed cluster based network. The suggested network is simulated in network simulator(NS-2) and response time is calculated which is 20 micro seconds that is less than detection with old technologies and can play important role in limiting terrorism. Technique to reduce false alarm rate is also discussed which will help the sensor to be practically implemented in public sector.

***KEYWORDS**:* Wireless Sensor Network; Detection of Explosives; Distributed Clustering; Ad Hoc Sensor Networks; Limiting Terrorism.

1 INTRODUCTION

In the past few years, terrorism is much more alarming issue all over the world. Terrorist are using latest explosive material with latest techniques to damage governmental assets, military installations and even now a days it is used to create harassment in civil society. Recently, terrorist activities had set their targets to blast in public rushed areas like parks, markets, and universities in Egypt, Lebanon, France, Pakistan, Belgium, Turkey and many more countries. Consequently, we have lost thousands of precious lives in such terrorist activities. So, there is an immense need for technology workers to come up with a positive solution because forces cannot be deployed everywhere especially in rushed areas. Moreover we cannot afford to risk the precious lives of forces personnel.

During 2014, 32727 fatalities occurred [1]. According the statistics, total 80% of global fatalities due to terrorism are in four countries around the world. Iraq is having a largest record number of fatalities which is 9929 deaths which is 30.4% of global fatalities caused by terrorism all over the world in 2014. Nigeria, Afghanistan and Pakistan are having 23.0%, 13.8% and 5.4% of global fatalities respectively as shown in figure 1 [2].

***Corresponding Author:** Fareeha Zafar, Assistant Prof Dr., Government College University, Lahore, Pakistan, dr.f.zafar@gcu.edu.pk

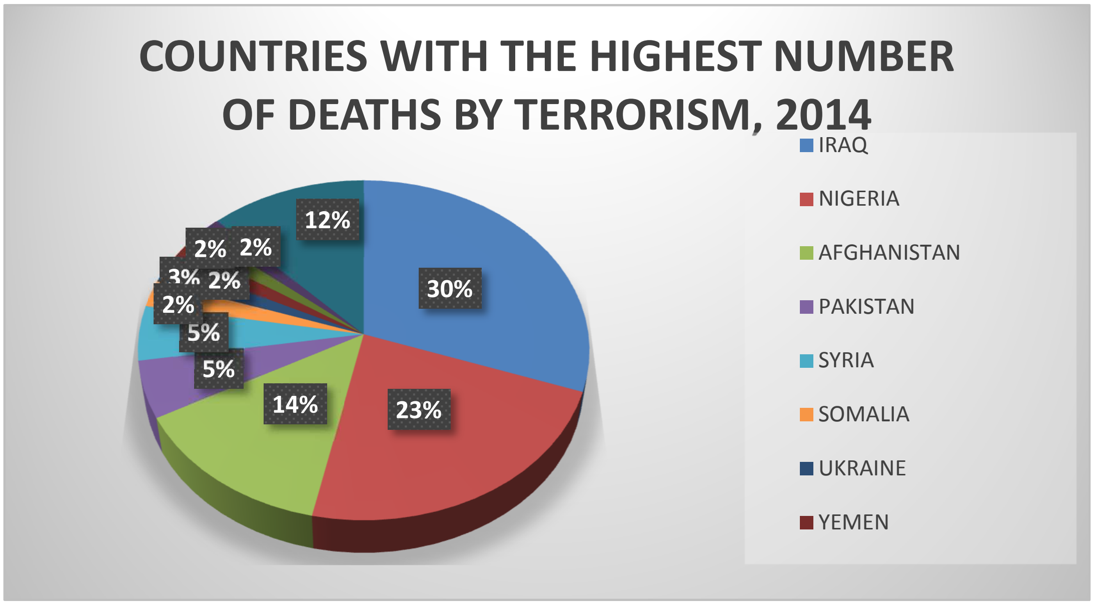
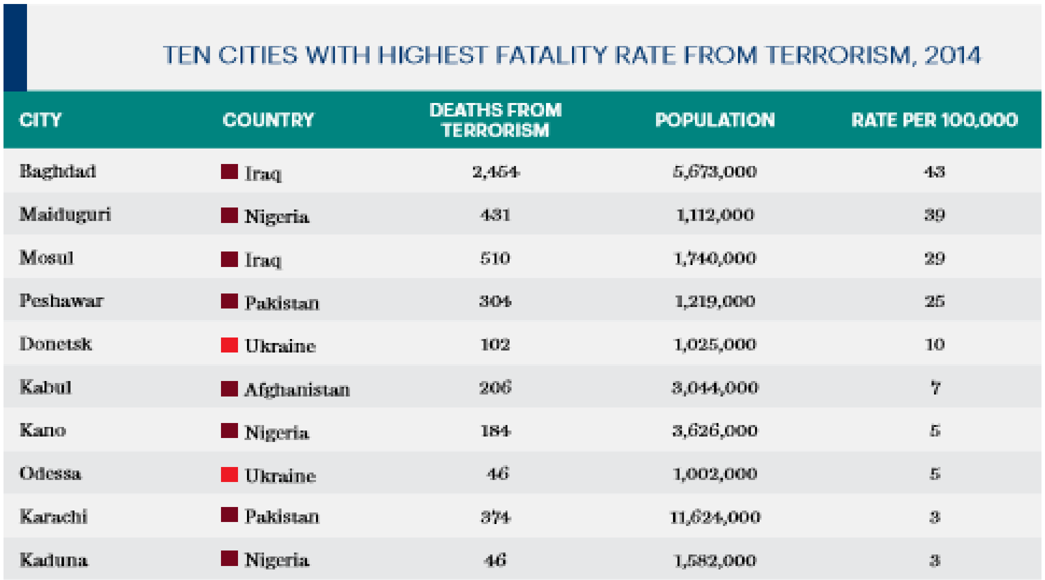


Figure 1: Countries with highest number of death rate by Terrorism, 2014

Table 1 describes that in 2014, Baghdad in the city with highest deaths from terrorism [2]. Mosul comes at number 3. Peshawar at number 4 and Karachi comes at number 9. The two main cities of Pakistan come in top ten cities in world who have highest fatalities rate from terrorism during 2014.Consequently, industry moves to safe countries and effects economy [3][4].



TEN CITIES WITH HIGHEST FATALITY RATE FROM TERRORISM, 2014

CITY	COUNTRY	DEATHS FROM TERRORISM	POPULATION	RATE PER 100,000
Baghdad	🟥 Iraq	2,454	5,673,000	43
Maiduguri	🟥 Nigeria	431	1,112,000	39
Mosul	🟥 Iraq	510	1,740,000	29
Peshawar	🟥 Pakistan	304	1,219,000	25
Donetsk	🟥 Ukraine	102	1,025,000	10
Kabul	🟥 Afghanistan	206	3,044,000	7
Kano	🟥 Nigeria	184	3,626,000	5
Odessa	🟥 Ukraine	46	1,002,000	5
Karachi	🟥 Pakistan	374	11,624,000	3
Kaduna	🟥 Nigeria	46	1,582,000	3

Table 1: Ten Cities with Highest fatality rate from terrorism, 2014

Past few decades reveal that the terrorist activities are performed with Integrated Explosive Device (IED). IED is homemade bomb and have a variety of explosive material like trinitrotoluene (TNT), detonating material, nitrate and various systems which could be used to explode various hazardous chemicals[5]. North Atlantic Treaty Organization (NATO) defines IED as “a device planned in an improvised manner incorporating destructive, noxious, lethal chemicals and designed to incapacitate, harass or destroy”. The devices can be used as mines or it can be attached with vehicle or building to destroy the targets. These are the types of explosives:

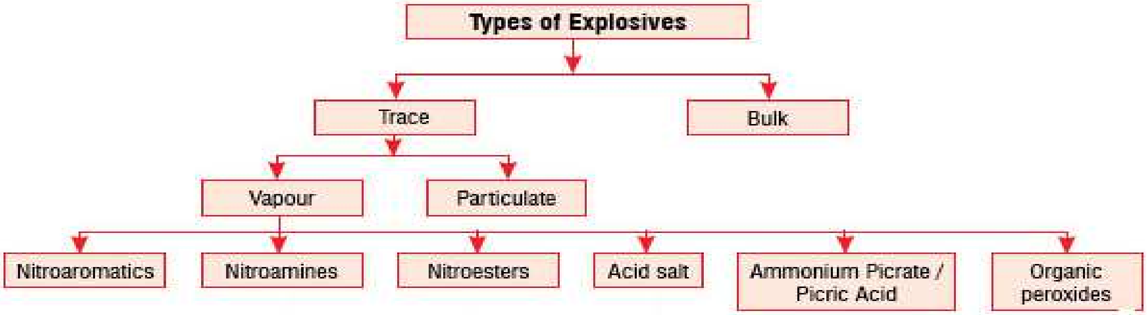


Figure 2: Types of Explosives

There are many types and forms of munitions, TNT and PE4 are being used by military and also in commercial explosives. The same is used in IEDs. To enhance effect of the explosive, many hardware items like ball bearings, bolts, solid iron pieces and even fuel tanks are being used by terrorist. There are three major groups of explosive:

- Nitro aromatic explosives
- Chlorate based explosives
- Peroxide based explosives

Many techniques have been used to limit these terrorist activities and to somehow these efforts are not proved appreciable because the traditional techniques for detection of explosive material are having large size and terrorists can easy change their route by having a look upon the detection devices like walk-through gates or police checking posts. So there is a need to use detection devices which can dodge human eye and also which are economical because if the devices are costly then it would be difficult to set a large network even in public places.

The document describes historical evolution in detection devices that have been used in explosives detection. Trained dogs are natural and efficient sensors to trace the presence of explosive material. They are special types of dogs and highly trained to smell the presence of particle of explosive material. They remember the fragrance of special substance and whenever they smell the fragrance again, they let their handler aware of the presence of explosive material. But there are some limitations as the practice can only be implemented at special occasions. Moreover, terrorist can see the dogs and from a distance, he can change his route. Moreover, when dogs are tired of smelling, then the dogs cannot effectively smell the presence of fragrance.

2nd most effective sensors are honey bees and the phenomena behind the technique is same like trained dogs. In this technique, their training is being held advance software for strategic reaction. The bees serve for two days and then they returned to their hive. Biotechnology firm Inessential claims that the bees are effective than the sniffer dogs. The technique is good but it's not commercially available.

X-ray machines can detect explosives by looking at density of items which are being scanned [6]. So the operator can see all the items in a package/ bag without opening it. The technique is effective but limited in its usage as the machines are heavy and cannot be operated in rush areas. Moreover terrorist can see the machines and easily can change his route.

A wireless sensor network (WSN) is a collection of sensor nodes that are used into a cooperative network [7]. They are ad-hoc systems connected by wireless links between sensor nodes having a small amount of power bank. To get effective use of the power, various algorithms are experimented [8]. WSN has numerous applications, ranging habitat monitoring to environmental control. WSN is also used in explosive detection. Efforts have been implemented in various techniques using WSN.

Wireless sensors are being used for explosive detection [5]. The sensors are most effective way to sense the molecules of explosive material in the air and frequently used in military [9]. The sensors are used in a wireless network to be operated in public areas. The presence of explosive material can easily be detected in public rushed area like civil market, schools, universities, railway station, airports, etc.

The research uses wireless sensors which are penny sized and they can easily dodge the terrorist eye. The sensor is much economical and its cost is in cents: not even in dollars. The sensors are used in a network to transmit the info to tag reader (sink) and then to server room and anti-terrorism action can be taken by law enforcement agencies. Moreover the network is reliable and robust. The sensor has capability to selfheal if it loses the network as the routing algorithm used in the network is smart enough to detect the alternate path if it gets disconnected with primary route [10].

2.**LITERATURE REVIEW**

Trammell Hike [11] advocated approach to detect explosive ordnance by using magnetic sensor. The sensor works on magnetic properties that are contained in most unexploded ordnance and IEDs. Magnetic sensors are configured as a tensor magnetic gradiometer that sense magnetic targets using magnetic moments. Magnetic sensors in a sensor network could be effective for protecting communal areas such as airports and busy urban areas.

Another approach is to detect explosive material using chemical sensors. The sensors detect the traces of the particular chemical. Sensor contains a thin layer of the chemical to match and hence when the chemical is matched, the sensor lets us know the presence of the material. But problem with this technique is that it has lack of sensitivity, accuracy and false alarm rates. However the technique is ever growing and scientists are doing their best in finding out some new advancement in chemical sensors.

One of the technology in the market today is “CrossBow technology”. It is the leading wireless sensor end-to-end solution provider and the largest manufacturer of Smart Dust wireless sensors. One of the best security mote is model number MPS410 which has capability to detect the traces of explosive material. They are easily deployed by just switching them ‘ON’ and they are set in a mesh topology. The sensors detect the material and send the information automatically that can be vied in MOTE-VIEW(TM) application. They are self-healing and easily find the multi-hop network. The MPS410 security motes are powered by a pair of AA batteries and additional security motes can be added to a network without any configuration or maintenance.

The size of MPS410 has the size 3.5’’ x 3.5’’ x 2.4’’ and each security mote is powered by five low-power sensor elements. So the sensor is still large to be easily caught by human eye from a hundreds of meter. The processor radio engine continuously monitors and combine the five sensors’ elements and then transmit the info to server. Detection data from multiple MSP410 Motes is communicated and then the data is aggregated across the sensor network to form tracking data [12].

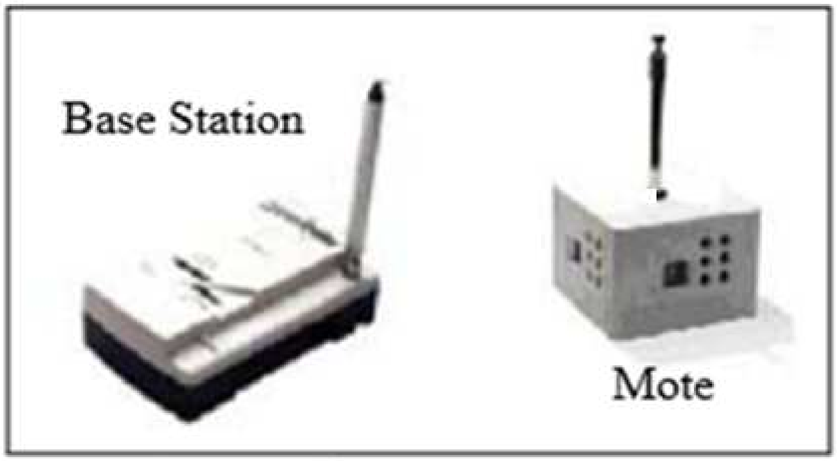


Figure 3*:* MPS410 Base Station with Mote

The technology is efficient and is in commercial use now a days. But it has also some limitations:

a) Its size is large and terrorist can change their route if the sensors are not properly concealed. We need the sensors that can be easily hide their presence.
b) False alarm rate is high. We need the sensor with much less false alarm rate than this.
c) The technology is old now, and cannot detect some types of IEDs. So evolution in sensor technology is of much importance.

Zahraa Abdul Hussein Jaaz [13] discussed the MPS410 Mote in detail in his MS Thesis and performed emulation. He integrated the sensor network with internet of things (IoT) and passed the detection info to main server. He calculated the time delay from end-to-end which is 0.28 seconds. And hence he suggested the network to effectively use in detection of explosive material. He mentioned an immense need of fault tolerant network design in his future work.

The research uses a sensor which is introduced in January 2015 by scientist working in GE lab. It is a penny-sized radio sensor that is built by engineers at GE lab. The author of [14] claims that the sensor has the capability to detect faintest traces of chemical and explosives. And the special thing is that it needs only a tiny amount of power to operate. The main phenomena behind the detection process is that the device has a special film a tenth the thickness of human hair to spot the compound.

Tomas Kellner [14] explained that the sensor costs only a few cents to produce which is 300 times smaller than conventional detectors. The second attractive aspect of the sensor is that it uses a tiny amount of power which is 100 times less than the desktop detectors usually we use at airports and other important areas. It's a very attractive device – reliable, robust, cost-effective, low power and high performance.

The sensor is combination of radio frequency identification (RFID) tag and an advance thin layer of chemical detection film. The chemical detection film plays a vital role in detection of the explosive material. Even the chemical detection film is combination of many chemicals which are usually used in explosive devices. The scientists designed the film by combining their study of chemistry, nanotechnology and data analytics.

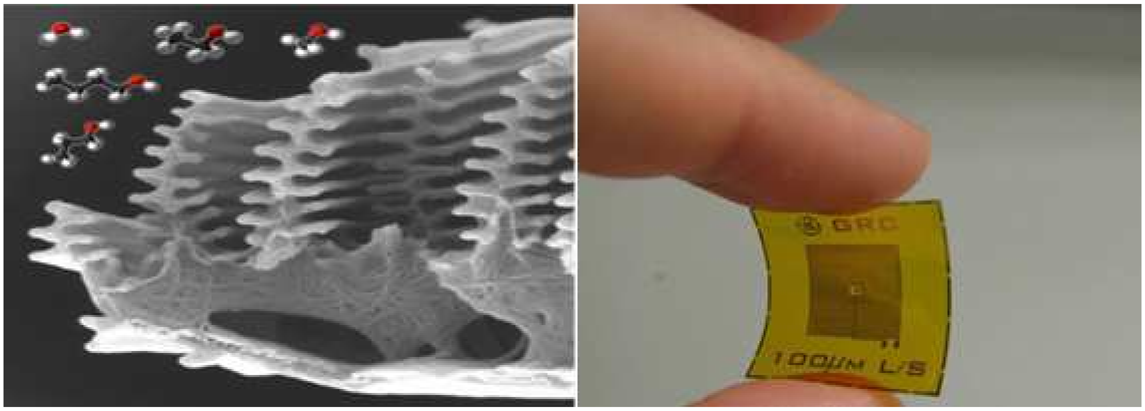


Figure 4: A battery-free RFID sensor tag for detection of chemicals such as explosives and oxidizers

The whole detection process utilize two parts: the RFID sensor tag and a cellphone sized handheld tag reader (TR). The sensor tag is composed of a flat antenna which is attached with a microchip mounted on tag. The antenna harvests power from the cellphone sized reader nearby. To detect the molecules of explosive material is basically work of antenna and the chip mounted on the tag. Whenever the tag detects presence of explosive material, it will alter the radio frequency spectrum and the change is radio frequency spectrum is read by the reader nearby and the signal may forward to server for counter measures.

3. MATERIAL AND METHODS

3.1. The Proposed Sensor. The tiny sensor, mentioned in [14], is basically formed to detect explosive material in a confined space where only one sensor is sufficient to secure the place like container, etc. That is the main reason that the sensor tag, which senses the explosive material, do not use battery power in processing and the maximum power is consumed in transmission and sensing explosive material. The processing is performed at tag reader (TR) which is powered by an external battery. So sensors are just small, thin and overcome the size limitation of previously used sensors.

The research suggests that instead of MPS410 of CrossBow technology, the tiny sensor [14] can be effectively used in WSN for explosives detection but with a slight change. Tag reader (TR) is designed to read just one sensor tag's signal but in the proposed architecture, tag reader should receive and read sensors detection signal from multiple sensor tags. Sensor tag detection range is considered the same which is 20 feet. Tag reader range can be extended up to 100 meters as it is powered by external battery. The readers have ability to create a link with other readers as well as with server room. In this way, the sensors tag can replace MPS410 and also overcomes the limitation of MPS410. The proposed sensor tag is very small and thin to be un-noticed from terrorist eye as well as it is robust, economical, sensitive with low false alarm rate.

3.2. The Network Model. The network model is based on distributed clustering ad hoc network [15]. Each senor tag senses explosive material and passes the signal to a specific tag reader (Cluster Head). TR performs aggregation and discards redundant data. Then the TR sends data to next TR and so on and finally to Base Station.

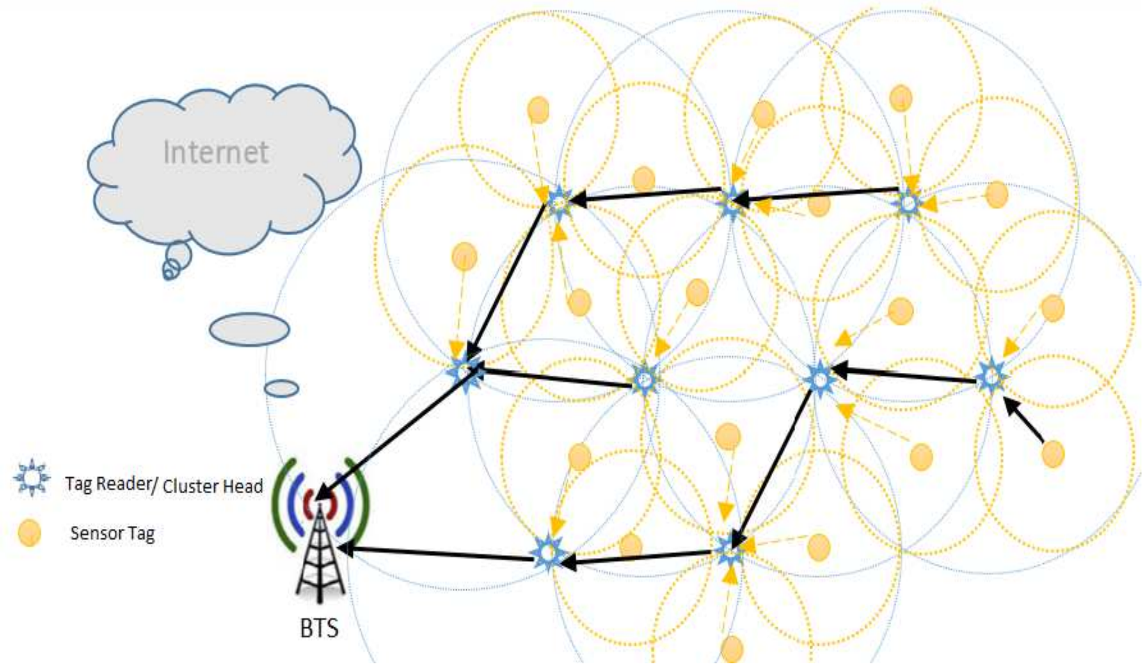


Figure 5: The network model

Sensor tag just senses and transmits data without processing at sensor tag within the range of 20 feet. The sensor tag does not receive the signal of other sensors. Sensors are placed around tag reader with the distance of 20 feet. It is normally enough to place 04 sensors around a sensor tag as shown in the figure 5(b). However 03 sensor tags can be placed for economic reasons as shown in figure 5(a). A single tag reader reads the data of multiple sensor tags and distinguishes them by identifying sensor id. Here the data aggregation is also performed and redundant data is discarded. It is to be noted that in the proposed architecture, only sensor tags are needed to be concealed while sensor tags are so small and thin that they can hide their physical presence due to their small size. The TR should be in range of tags which transmits information and the reader gets the information and further transmits to next TR or server room. Usually every sensor tag has at least 2 TR in its range.

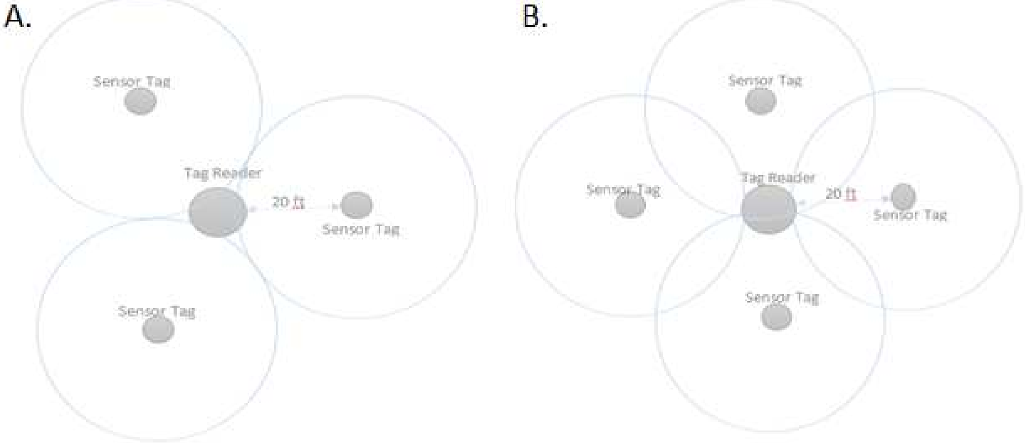


Figure 6. (A): reader with three sensor tags and**(B):** reader with four sensor tags

To understand the selection of TR process, first look at network session. Network session is divided into two sections; setup section and sleep section. In setup section, a hope count packet is forwarded to each sensor tag as well as TR to determine their distance with base station in terms of hopes. Sensor tag selects TR with lowest hope count for speedy transmission. The 2nd section is sleep section in which transmitter goes off. Sensor Tag does not perform extra processing. It just remains in sleep mode and keep on sensing. Then upon receipt of signal, it switches on transmitter and sends to a specific TR. Thus it saves energy and life time. Processing occurs at TR because it is powered by external battery.

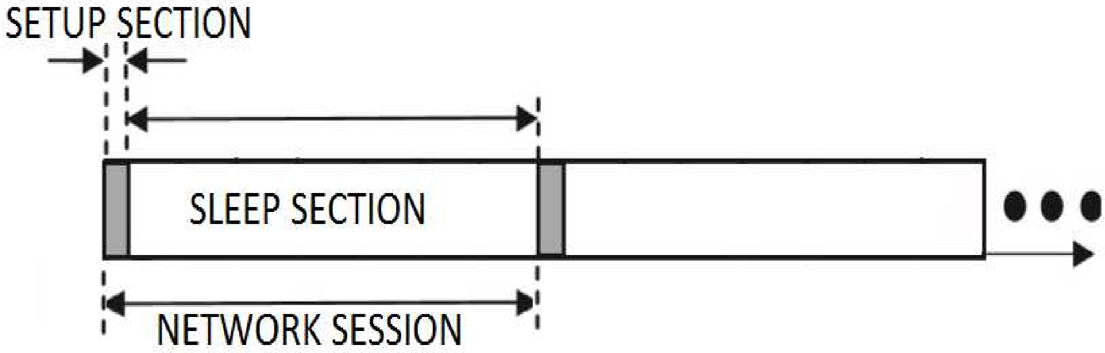
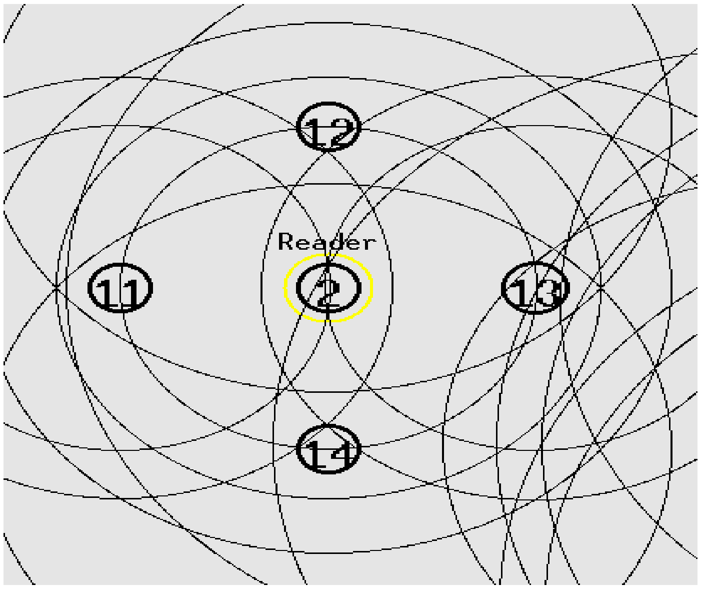


Figure 7. The network session

3.4. Simulation. The network is simulated in NS-2 to determine the performance factors under these basic parameters:



Channel type: Wireless Channel
Propagation Model: Two Ray Ground
Interface type: Phy/ Wireless Phy
MAC Type: Mac/802_11
Antenna Model: Omni Antenna
Routing Protocol: AODV
Sensor sensing range: 20 feet
Sensor communication range: 20 feet
TR communication range: 100 feet
Distance between Sensor tags: 20 feet

Figure 8: Tag reader with four sensor tags

In the proposed network, sensor nodes are placed 20 feet apart from reader as shown in the figure 6. When explosive material comes in the range of sensor tag, the sensor senses the presence of explosive material and transmits 23 bytes of signal including 1 byte of sensor id and uses UDP protocol. The reader receives the signal, processes the signal, performs aggregation, discard redundancy and distinguishes its location based on sensor id. Meanwhile transmitter of sensor tag remains in sleeping mode and in this way we can increase life span of the sensor tag. Whenever it receives the signal, then the signal is transmitted to TR where TR processes the data and transmits the positive signal to nearby TR or server room.

The proposed network has a back-up path between tag readers and server. If TR loses a connection with server room, it transmits the information to other tag readers nearby. And then the second TR passes the info to server room. Even the 2ndTR is passing the information, still there is no confusion in determining the exact targeted location as the signal contains the sensor id of the detecting sensor. Here there is a back-up path for reader to server room transmission. And if a TR down sudden, then in the upcoming network setup section, the sensor node will select any other alive TR based on lowest hope count. Hence the network is fault tolerant.

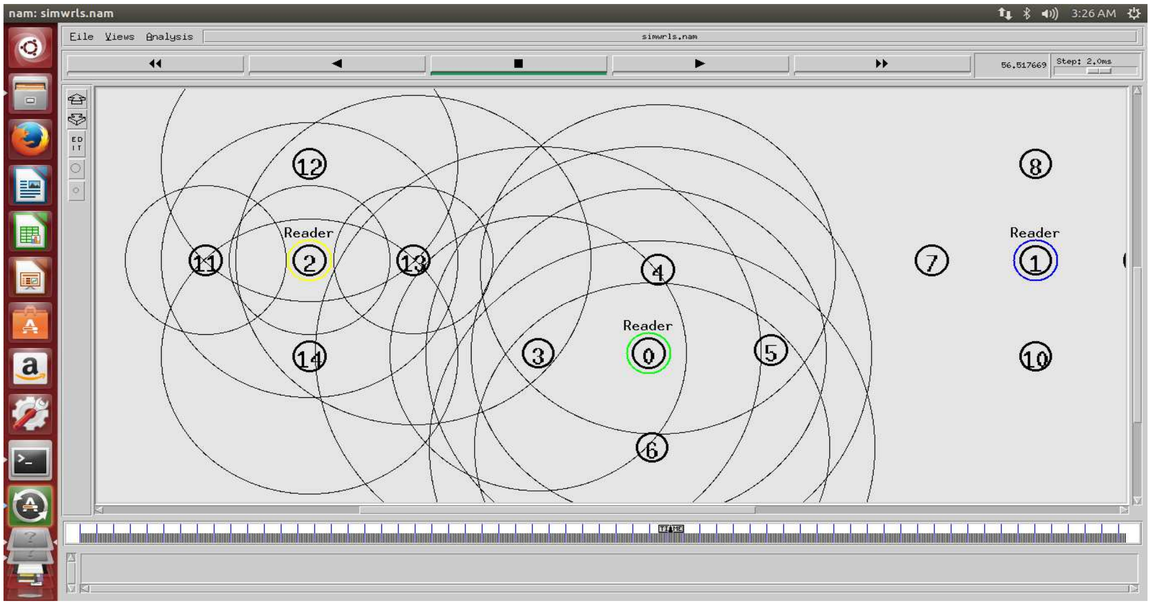


Figure 9: Sensors and TRs used in network

The research enhanced the scope of tiny sensor as in this way, the sensor can be used in public areas in the network to limit terrorism. The second objective is achieved: to dodge the terrorist eye as sensor tags are small enough to hide their physical presence. The third objective is achieved as the sensor costs a few cents so the proposed system is economical. So by using the sensor in the topology, we can save money as well as enhance efficiency because the sensor tags are robust and efficient.

3.5. Simulation Results.

- Real time detection of explosive material and speedy passing the information to server room.
- Detection time is calculated which is 20 micro seconds.
- Total time required to process and pass the signal to server room is 0.20 second.

3.6. Technique to reduce false alarm rate. Efficiency is achieved by increasing sensitivity of the tag and reducing false alarm rate. As the sensor is much sensitive; it can sense a tiny amount of explosives passing nearby. The main limitation of wireless sensors in explosives detection is false alarm rate which is normally low but even then minor false alarm ratio creates hindrance in practical implementation. However we can also reduce false alarm rate by making a tradeoff between first alarm time and false alarm ratio. In the simulation, a single detection of explosive material is occurred in 20 micro second. And time calculated to reach the server room is 0.20 seconds. It means in a single second, 5 times a signal reaches the server room if the signal is positive. At application level, we can make our first alarm system active after receiving the detection signal consecutive three times. After receiving the signal three times, the application will generate alarm and we can activate our counter measures. After the alarm is generated once, then the application will generate alarm on every single positive signal. So, the only first alarm time is compromised and in this way, false alarm rate is minimized to negligible level.

4. CONCLUSION

To overcome the threat of terrorism, the research emphasizes on the wireless sensor network of new tiny sensors because of its small tiny sensor size, less cost and better efficiency. It has low false alarm rate and high robustness than conventional sensors. The tiny size sensor tag can cut off easily from sight due to its small size. The proposed network is having the secondary network path between tag readers and server room which might be used in case the primary path is unreachable. The network is simulated in NS-2 and detection time is calculated which is 20 microseconds. The research also suggests the tradeoff between first alarm time and false alarm rate to reduce false alarm rate to negligible level. Hence the proposed WSN may be helpful in limiting terrorist attacks and could be used commercially.

5. FUTURE WORK

- There is need to work on the practical Implementation and its worst case studies.
- There is a need to enhance the sensing range of the sensor and to more reduce sensing time.
- Energy model of sensor and reader tags needs consideration and improvement techniques.

REFERENCES

1. Bureau of Counterterrorism. 2014. *National Consortium for the Study of Terrorism and Responses to Terrorism: Annex of Statistical Information*, United State: U.S Department of State. Available at: http://www.state.gov/j/ct/rls/crt/2014/239416.htm (Accessed 06 June 2016).
2. Global Terrorism Index. 2015. New York: Institute for Economics and Peace. Available at: http://economicsandpeace.org/wp-content/uploads/2015/11/Global-Terrorism-Index-2015.pdf (Accessed: 25 June 2016).
3. Zada, K. Tariq, M. Ullah, I. Jan, S. Khan, Z. and Malik., 2016. The Impact of Terrorism on Foreign Remittances Inflows in Pakistan. J. Appl. Environ. Biol. Sci,6 (11), pp.123-32.
4. Ali, S., Waqas, H. and Asghar, M., 2015. Bearing the Brunt: The Effect of Terrorism on Foreign Direct Investment in Pakistan. *J. Appl. Environ. Biol. Sci*, 5(5), pp.312-320.
5. Rowe, N.C., Singh, G. and O'Hara, M., 2009. Wireless Sensor Networks for Detection of IED Emplacement/*14th ICCRTS*: C2 and Agility.
6. Armistead, R.A., Advanced Research and Applications Corporation, 1998. *Single beam photoneutron probe and X-ray imaging system for contraband detection and identification*. U.S. Patent 5,838,759.
7. Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D. and Pister, K., 2000. System architecture directions for networked sensors. *ACM SIGOPS operating systems review*, 34(5), pp.93-104.
8. Mohammadi, P. Jamali, S. and Analoui, M., 2013. Decrease Number of Bit ID in Wireless Sensor Network by Using Huffman Algorithm. *J. Appl. Environ. Biol. Sci*,3(12), pp.127-36.
9. Đurišić, M.P., Tafa, Z., Dimić, G. and Milutinović, V., 2012, June. A survey of military applications of wireless sensor networks. In *2012 Mediterranean conference on embedded computing (MECO)* (pp. 196-199). IEEE.
10. Hosseinpoor, M. J., 2013. Analysis, Simulation and Compare Two Routing Algorithms SMORT and DAR in Ad-Hoc Networks. *J. Appl. Environ. Biol. Sci*,3(12), pp.8-14.
11. Trammell III, H.S., Perry, A.R., Kumar, S., Czipott, P.V., Whitecotton, B.R., McManus, T.J. and Walsh, D.O., 2005, May. Using unmanned aerial vehicle-borne magnetic sensors to detect and locate improvised explosive devices and unexploded ordnance. In *Defense and Security* (pp. 963-971). International Society for Optics and Photonics.
12. Sundram, J. and Sim, P.P., 2007. *Using Wireless Sensor Networks in Improvised Explosive Device Detection*. NAVAL POSTGRADUATE SCHOOL MONTEREY CA.
13. Jaaz, Z.A.H., 2014. *Integrating Internet of Things and Wireless Sensor Networks for Metropolitan Explosive Detection* (Doctoral dissertation, Middle East University).
14. Tomas Kellner (9 Feb 2015) Tiny Sensors Inspired by Butterfly Wings Could Improve Bomb Detection, Available at: http://www.gereports.com/post/110183245875/tiny-sensors-inspired-by-butterfly-wings-could(Accessed: 25 April 2016).
15. Younis, O. and Fahmy, S., 2004. HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. *IEEE Transactions on mobile computing*, *3*(4), pp.366-379.