IOSR Journal of Mobile Computing & Application (IOSR-JMCA)
e-ISSN: 2394-0050, P-ISSN: 2394-0042.Volume 3, Issue 4 (Jul. - Aug. 2016), PP 17-22
www.iosrjournals.org

Critical Study of Wireless Ad-Hoc Sensor Networks and Their Applications

Onu Fergus U. (Ph.D), Ikporo Stephen C.
Department of Computer Science, Ebonyi State University, Abakaliki – Nigeria

Abstract: *The attention of many researchers have been attracted by Wireless Ad-hoc Sensor Networks (WASN). The WASN is formed by a large number of sensor nodes which are commonly known as motes. This paper presents a critical study of wireless ad-hoc sensor network as well as its application areas. In particular, the paper evaluates the various applications of wireless ad-hoc sensor networks, its advantages and disadvantages as well as the security mechanisms for countering attacks on wireless sensor networks. Data were collected from secondary sources and a critical detailed study was carried out. The paper deduced that wireless ad-hoc sensor networks were used daily by millions of people. The technology is predominantly deployed for wireless Internet access with laptops, PDAs, Tablets, Android phones and the likes for data transfer between the devices, for monitoring purposes and even to play games with portable game consoles. The application areas for WASN has grown due to ease of the network acquisition and configuration.*

Keywords: *PDA, Sensor Nodes, Electromagnetic Waves, Guided Media, Tranceivers, Signal Processors.*

I. Introduction

Hong *et al* (2004) wrote that a wireless ad-hoc sensor network is a collection of nodes organized into a cooperative network. Each node has processing capability (i.e one or more microcontrollers, central processing units (CPUs) or digital signal processing (DSP) chips, multiple types of memory), have a radio frequency (RF) transceiver (usually with a single Omni-directional antenna), have a power source (e.g., batteries and solar cells), and accommodate various sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an ad-hoc fashion. The nodes sense environmental changes and report them to other nodes over flexible network architecture. According to Anderson *et al* (2002) "Sensor nodes are great for deployment in hostile environments or over large geographical areas".

A wireless ad-hoc sensor network has important applications such as remote environmental monitoring and target tracking. This has been enabled by the availability of sensors that are smaller, cheaper, and intelligent; particularly in recent years. These sensors are equipped with wireless interfaces with which they can communicate with one another to form a network. The design of a wireless ad-hoc network depends significantly on the application, and it must consider factors such as the environment, the applications design objectives, cost, hardware, and system constraints.

II. Literature Review

Wireless Network: According to [1], unguided or wireless media transport electromagnetic waves without the use of physical conductors. In this type of network, signals are usually broadcast through the air and thereby making it available for anyone that has the device capable of receiving them. A wireless network enables people to communicate and access applications and information without wires. This provides freedom of movement and the ability to extend applications to different parts of a building, city, or nearly anywhere in the world. Wireless networks allow people to interact with e-mail or browse the Internet from a location that they prefer [2]. Many types of wireless communication systems exist, but a distinguishing attribute of a wireless network is that communication takes place between computing devices which may include personal digital assistants (PDAs), laptops, personal computers (PCs), servers, and printers. Computer devices have processors, memory, and a means of interfacing with a particular type of network. The information shared in a network can take the form of e-mail messages, web pages, database records, streaming video or voice.

Wireless Sensor Network: Wireless sensor networks consist of distributed, wirelessly enabled embedded devices capable of employing a variety of electronic sensors according to [3]. Each node in a wireless sensor network is equipped with one or more sensors in addition to a microcontroller, wireless transceiver, and energy source. The microcontroller functions with the electronic sensors as well as the transceiver to form an efficient system for relaying small amounts of important data with minimal power consumption.

Wireless Ad-hoc Network: A wireless ad-hoc network is a decentralized type of wireless network [4]. The network is ad-hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or

access points in managed (infrastructure) wireless networks. Each node in the network participates in routing by forwarding data to other nodes, and so the determination of which nodes to forward data is made dynamically based on the network connectivity. In addition to the classic routing, ad-hoc networks can use flooding for forwarding the data. An ad-hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad-hoc network devices in link range.

Wireless Ad-hoc Sensor Networks: A wireless ad-hoc sensor networks consists of a number of sensors spread across a geographical area [3]. Each sensor has wireless communication capability and some level of intelligence for signal processing and networking of the data.

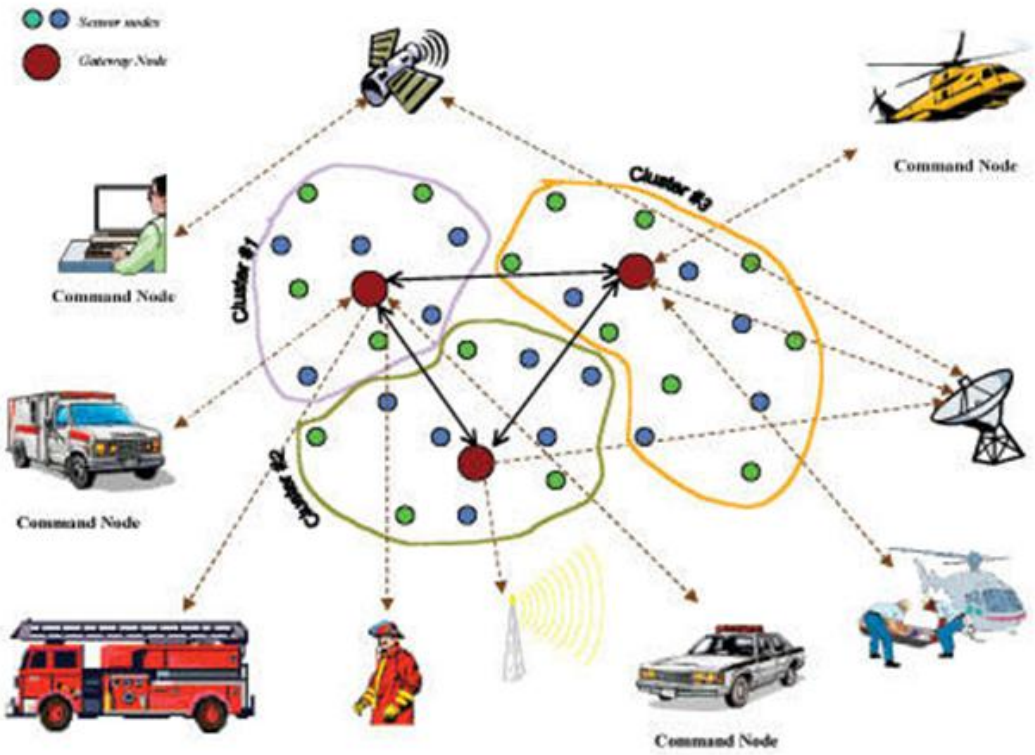

Figure 1: Structure of wireless ad-hoc sensor networks

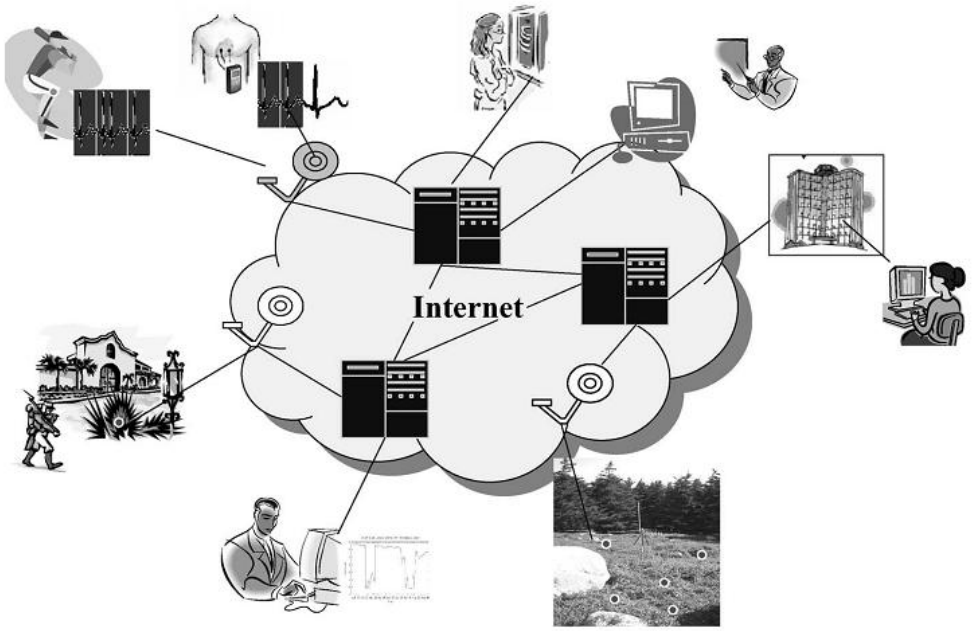

Figure 2: Wireless sensor network applications. [5]

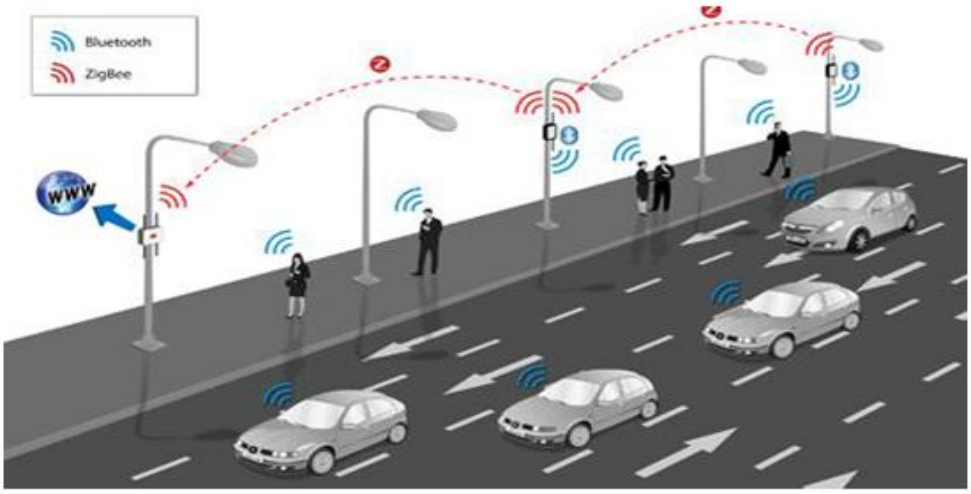

Figure 3: Traffic monitoring with wireless traffic sensor network

Figure 4: Cardiac implanted device to monitor the heart rhythm or beat.
(*http://www.ercim.org/publication/Ercim_News/enw51/bielikova.html*)

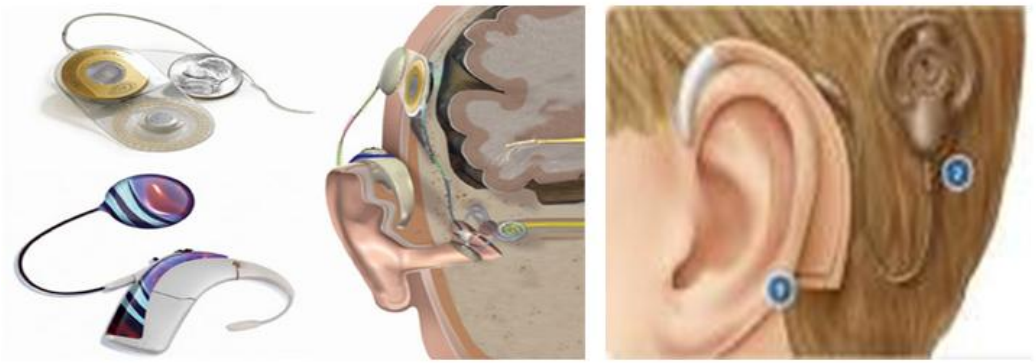

Figure 5: Cochlea implants.

Figure 6: Forest fire detection

Requiements Of Wireless Ad-Hoc Sensor Networks:
Wireless ad-hoc sensor network requirements include the following:

- **Large number of (mostly stationary) sensors:** Aside from the deployment of sensors on the ocean surface or the use of mobile, unmanned, robotic sensors in military operations, most nodes in a smart sensor network are stationary. Networks of 10,000 or even 100,000 nodes are envisioned, so scalability is a major issue.
- **Low energy use:** Since in many applications the sensor nodes will be placed in a remote area, service of a node may not be possible. In this case, the lifetime of a node may be determined by the battery life, thereby requiring the minimization of energy expenditure.
- **Network self-organization:** Given the large number of nodes and their potential placement in hostile locations, it is essential that the network be able to self-organize; manual configuration is not feasible. Moreover, nodes may fail (either from lack of energy or from physical destruction), and new nodes may join the network. Therefore, the network must be able to periodically reconfigure itself so that it can continue to function. Individual nodes may become disconnected from the rest of the network, but a high degree of connectivity must be maintained.
- **Collaborative signal processing**: Yet another factor that distinguishes these networks from MANETs is that the end goal is detection/estimation of some events of interest, and not just communications. To improve the detection/estimation performance, it is often quite useful to fuse data from multiple sensors. This data fusion requires the transmission of data and control messages, and so it may put constraints on the network architecture.
- **Querying ability**: A user may want to query an individual node or a group of nodes for information collected in the region. Depending on the amount of data fusion performed, it may not be feasible to transmit a large amount of the data across the network. Instead, various local sink nodes will collect the data from a given area and create summary messages. A query may be directed to the sink node nearest to the desired location.

III. Application Of Wireless Ad-Hoc Sensor Networks

Wireless ad-hoc sensor networks are very versatile and can be used in a variety of application areas. Some of these areas include: healthcar and environmental monitoring, target/device tracking, military surveillance, etc. Wireless sensor networks are usually made of hundreds of thousands of sensor nodes and can gather information from an unattended location and transmit the gathered data/information to a particular user, depending on the application they are deployed to handle. Some more specific areas of wireless ad-hoc sensor network applicatios are:

- **Traffic Sensor Network:** Detect the occurrence of events of interest and estimate parameters of the detected event or events: In the traffic sensor network shown in figure 3, one would like to detect a vehicle moving through an intersection and estimate the speed and direction of the vehicle. One can as well need to c**lassify a detected object;** for instance, is the detected vehicle in a traffic sensor networks a car, a mini-van, a light truck, a bus, etc.The objective of the Traffic monitoring is (1) to calculate the average speed of the vehicles which transit over a roadway by taking the time mark at two different points. (2) Understand the flow and congestion of vehicular traffic for efficient road systems in cities such as reduce journey times, reduce emissions and save energy.
- **Process Management or Area monitoring:** Process management is a is a common application for wireless ad-hoc sensor network. In area monitoring, the wireless ad-hoc sensor networks is deployed over a region where some phenomenon is to be monitored. A military example is the use of sensors to detect enemy intrusion; a civilian example is the geo-fencing of gas or oil pipelines. Area monitoring is a vert important application area for WASNs.
- **Healthcare monitoring:** Wireless sensor networks can be used to monitor and track elders and patients for healthcare purposes. This significantly reduces the severe shortage of healthcare personnel experienced in developing countries. In addition, it would reduce the healthcare expenditures in the current healthcare systems. For example sensors can be deployed in a patient's home to monitor the behaviours of the patient. It can alert doctors when the patient falls and requires immediate medical attention. The medical applications can be of two types: wearable and implanted. Wearable devices are used on the body surface of the patient or just at close proximity to the user. The medical implant devices shown in figures 4 and 5 are inserted or placed inside the body. There are many other applications like body position measurement and location of the person, overall monitoring of ill patients in hospitals and at homes. Body-area networks can collect information about an individual's health, fitness, and energy expenditure.
- **Environmental monitoring:** There are many applications in monitoring environmental parameters. Some examples are air pollution, forest fire detection, landslide detection, water quality monitoring, natural disaster prevention, etc. These areas share a common challenging feature of harsh environments and

reduced power supply. Also WASNs can be deployed to determine the value of some physical parameter at a given location. In an environmental work, one might want to know the temperature, atmospheric pressure, amount of sunlight and relative humidity at a number of locations. This example shows that a given sensor node may be connected to different types of sensors each with a different sampling rate and range of allowed values.

- **Military Applications:** Wireless sensor networks are used for establishing communication among a group of soldiers for tactical operations and coordinating of military object moving at high speeds such as fleets of airplanes or ships. Wireless ad-hoc sensor networks are also becoming an integral part of military command, control, communication and intelligence systems. Sensors can be deployed in a battle field to monitor the presence of forces and vehicles, and track their movements, enabling close surveillance of opposing forces.
- **Emergency Operations:** WASNs are also used in emergency applications such as rescue mission, and crowd control.

IV. Threats And Attacks/Security Mechanisms On Wireless Ad-Hoc Sensor Networks

Threats and Attacks:

WASNs are prone to the following types of attacks:-

- **Common Attack:** The first common attack is eavesdropping [6] i.e., an adversary can easily retrieve valuable data from the transmitted packets. The second common attack is Message modification i.e., the adversary can intercept the packets and modify them. The third common attack is message replay ie.., the adversary can retransmit the contents of the packets at a later time.
- **Denial of service (DoS) Attack:** In the opinion of [7] a DoS attack on WSN may take several forms. The first one is node collaboration, in which a set of nodes act maliciously and prevent broadcast messages from reaching certain sections of the sensor networks. The second one is jamming attack, in which an attacker jams the communication channel and avoids any member of the network in the affected area to send or receive any packet. The third one is exhaustion of power, in which an attacker repeatedly requests packets from sensors to deplete their battery life.
- **Node compromise Attack:** A sensor node is said to be compromised when an attacker gains control or access to the sensor node itself after it has been deployed. Various complex attacks can be easily launched from compromised nodes, since the subverted node is a full- fledged member of the sensor network.

Security Mechanisms

The security mechanisms adopted for the various attacks according to [8] listed earlier are:

- To counter common attacks like eavesdropping, message modification, message replay attacks, strong encryption techniques and time stamps are to be used.
- The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.

V. Discussion And Conclusion

A wireless ad-hoc sensor network is a wireless network consisting of spatially distributed autonomous devices or nodes. These nodes use sensors to monitor physical or environmental conditions such as temperature, sound, pressure, etc. and cooperatively pass their data through the network to a control location. These technologies led to the implementation of wireless sensor networks, allowing easily configured, adaptable sensors to be placed almost anywhere, and their observations similarly transported over large distances via wireless networks. This has been enabled by the availability of sensors that are smaller, cheaper, and intelligent, particularly in recent years. These sensors are equipped with wireless interfaces with which they can communicate with one another to form a network. It is a collection of nodes organized into a cooperative network. Each node consists of processing capability which, may contain multiple types of memory (program, data and flash memories), have a RF transceiver (usually with a single Omni-directional antenna), have a power source (e.g. batteries and solar cell). The development of WASNs has made a lot of impact in human existence.

Advantages:

- Wireless communications allow monitoring an environment remotely, without being in that location.
- Ideal for the non-reachable places such as across the sea, mountains, rural areas or deep forest. That is, it can collect, aggregate, and analyze diverse and distributed data, and detect patterns that would be otherwise very hard to identify.
- It can be deployed without requiring any pre-existing infrastructure and very quickly.
- It can be distributed also on wide areas at limited costs.

Disadvantages:

- Less secure because hackers can enter the access point and get all the information.
- Lower speed compared to a wired network.
- More complex to configure than a wired network.
- Easily affected by surroundings (walls, microwaves, large distances due to signal attenuation,

VI. Conclusion

It is certain from this study that unlike other networks, Wireless Ad-hoc Sensor Networks (WASNs) are designed for specific applications. Applications include, but are not limited to, environmental monitoring, industrial machine monitoring, surveillance systems, and military target tracking. Each application area differs in features and requirements, but they have some common features of challenging and human unfriendly environments. Today, disasters are predicted and prevented through the use of several types of sensor detectors. These detectors have the capability of sensing impending dangers such as flood, wild fire outbreak, fire disasters, and air pollution. Smoke Detectors are now installed in most buildings, used for residential and business purposes. Medical science is also utilising the technology to monitor and boost the healthcare delivery efficiency.

References

[1]. Onu F. U., Ugwu I. O., Okpara C., (2007), "Fundamentals of computer studies". Revised edition, Larry and Calab: copycraft Int'l Comp., pp. 231 – 234.
[2]. Stallings W. (2002), "Wireless Communications and Networks". Prentice Hall, Upper Saddle River, NJ.
[3]. Culler D. E and Hong W., (June 2004) "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, pp. 30-33.
[4]. Jan Suwart. (2008) "Wireless Ad-hoc Networks: Limitations, Applications and Challenges". Available at https://www.cs.tu-bs.de/theses/rehman/Report_WANsLAC.pdf retrieved 10/2/2016
[5]. Kazem S, Daniel Mi, and Taieb Z. (2007) Wireless Sensor Networks: Technology, Protocols, and Applications, by John Wiley & Sons, Inc.
[6]. Douceur J. R, (2002) "The Sybil Attack," in 1st International Workshop on Peer-to-Peer Systems (IPTPS ″02).
[7]. Wood A.D. and Stankovic J.A., (2002) "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, 2002, pp. 54– 62
[8]. Undercoffer J., Avancha S., Joshi A., and Pinkston J., (2002) "Security for Sensor Networks", CADIP Research Symposium, retrieved on 10/02/2016 from: http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf.