World Journal of Innovative Research (WJIR)
ISSN: 2454-8236, Volume-10, Issue-1, January 2021 Pages 29-33

Wireless Sensor and Mobile Ad-Hoc Networks for the Internet of Things: A Survey

Raphael Agong

***Abstract*— Mobile Ad hoc Networks (MANETs) and wireless sensor networks (WSNs) are a type of network that belong to an ad hoc network. An Ad hoc network is a peer to peer networks involving wireless technology using radio frequency ranges to communicate to nodesfor MANETs or motes WSN with the correct identification (user id). These networks can be used in places where access is difficult or dangerous like war fields. Some of these networks can be used to monitor long events or behaviors. In this paper twenty-four journals published between 2007 and 2020 on Mobile Ad Hoc Networks, Internet of things (IoT), and Wireless Sensor Networks reviewed with their futuristic technology and trends identified. Sensors and wireless technologies are taking centre stage in modern communication, control, and management of equipment. The future of wireless network is very bright emerging from 2G to cellular then to IoT.**

WSNs and MANETs have unlimited progression in modern technologies. Most communication equipment, entertainment, error detection, prediction equipment, and many more base their input from sensed signals. This places them at greater heights in modern technology usage.

***Index Terms*— wireless sensor networks, Ad hoc networks, IoT, WSN implementation, MANET.**

I. Introduction

The network is the art of communicating through an interconnected set of devices. These devices are capable of communicating with each other (machine to machine communication). Communication between people to machine (P- to – M) is also possible. Devices connection can be through cable and air referred to as guided and unguided channels respectively. The guided channel also called wired channels or cabled channels includes LAN, MAN, WAN, and many others [1]. Cables used in wired networking are unshielded twisted pair (UTP), Shielded twisted pair (STP), Coaxial, and Fibre cables. Unguided channels also called wireless to utilize air as a communication channel. One of the characteristics of a channel is its capacity to carry the load called the bandwidth. The bandwidth of a cable is limited depending on the type of cable compared to that of air. Fiber cables have bigger bandwidth than their counterparts copper and coaxial [1]. The rates at which information will travel through these guided channels depend on the bandwidth. This rate is the bit rate or data rate in data communication. Air has a bigger bandwidth and therefore carries huge traffic than the cable networks. For information to travel from one point to the other point (point to point communication), there must be an identification of both points. The sender must identify the receiver and vice versa. These communicating points are the nodes (data terminal equipment and MANETs). Each node is identified with a unique address or number called internet protocol address (IP address) [2]. Networks are formed to allow nodes to communicate or share information. Networks of low bandwidth may connect to networks of higher bandwidth using a bigger bandwidth channel called backbone cable. In the case of two similar LANs, the connection can only be though a bridge and in case the two have different protocols then they can be linked through a router. If a single device is used to combine both functions of the bridges and the router, it will be called a bridge router device or just B-router [2]. The purpose of a network is to offer communication between two or more nodes transferring or sharing information. In this paper, major emphasis is placed on mobile ad hoc and wireless sensors which are in the class of wireless networks. Detailed functions of nodes and motes are not discussed in this paper. Most communication equipment, entertainment, error detection, prediction equipment, and many more base their input from sensed signals. This places them at greater heights in modern technology usage.

Raphael Agong, Faculty of Computer and Information Management KCA University

II. Types of wireless networks

There are so many types of networks falling within the two categories wireless network and wired network.

i. Ad hoc networks (wireless)
ii. Wireless sensor network (wireless)
iii. Infrastructure networks (wired)
iv. Distributed networks (wired or wireless)
v. Cellular networks (wireless)

This paper did not discuss the last three types of networks.

Ad hoc networks

Ad hoc is derived from a Latin word meaning ‘for this only’ [3]. Several communication devices can communicate with each other without central management. One requirement to allow this communication is the identification of both sender and receiver unique numbers that identifies them. An ad hoc network can, therefore, be defined as peer unguided network devices that directly communicate with each other. There is no device in between the communicating devices and the medium is air [3], [4]. This network is organized impulsively when the communicating devices communicate directly. There are some restrictions in this type of network ranging from but not limited to distance, environment, equipment, number of devices within the communication range, and speed. Some of the characteristics worth mentioning here are:

i. The capability of a node moving out/in of communication range or moving into the communication range
ii. Well defined communication range
iii. A defined number of nodes
iv. There is no central point in an ad hoc network
v. All the devices have an equal right within the communication range
vi. The mode of operation is based on the IEEE 802.11 wireless network standard
vii. Ad hoc network is self-organizing and self-managing

Because of its capability to change network topology, an ad hoc network lack reliability [3].

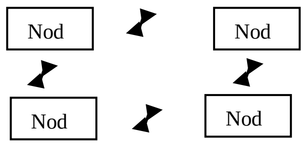


Figure 1 block diagram of ad hoc network

Types of Ad hoc network

i. Wireless Mesh Network
ii. Wireless Sensor Network
iii. Mobile Ad hoc Network

Wireless Mesh Network

Wireless Mesh Network (WMN) is an organized radio node arranged in a mesh topology where the name is derived. Generally, WMN infrastructure is a router networking without physical channel giving it a low cost and flexible hefty bandwidth within a coverage region [4].

Wireless Sensor Network (WSN)

Wireless Sensor Networks is an automatic configuring ad hoc network with capabilities of monitoring, communicating, computing, and tracking. This means it has the capability of physical and non-physical activities [6]. WSN is linked to the main storage also called Base Station where the data collected are transferred for analysis. This base station is the interface between the user and the network. The stored data can be retrieved by sending a question to the interface.

In WSN, the communication between thousands of sensors is through electromagnetic waves simply known as radio signals [7]. The main components of WSN are:

i. Sensors
ii. Computing Components (microprocessors, microcontrollers)
iii. Transmitters
iv. Receivers
v. A power source (usually DC)

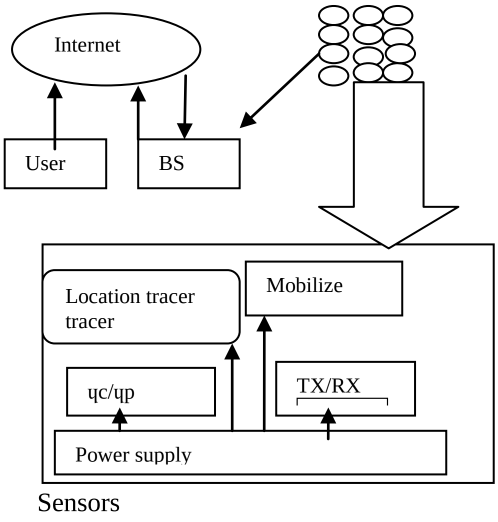


Figure 2 components of wireless sensor node

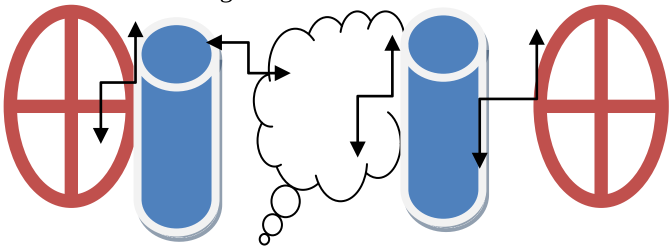
Sensor nodes are the main players in receiving signals in wireless sensor networks and can be in two states, continuity and event-driven. With this in mind, the main application of this network has been strictly on data monitoring [5]. This is not holding as per the current trend towards the development of wireless networks. It is possible to have a different energy level of sensors in the same network [6]. Wireless sensor networks (WSN) are distributed automatic sensor networking system that monitors physical activities like warmth, resonance, force, etc. Wireless sensor networks (WSN) also called wireless sensor and actor-network (WSAN) [8]. In modern networks, WSNs are two-directional and there is a possibility of controlling sensor works in both directions. The WSN is constructed from several nodes and each node is connected to one sensor. The possibility of connecting several sensors to one node is also possible [8]. The parts of WSN, the node, are radio transmitter, radio receiver, an antenna, and microprocessor controller unit [6], [9].

Architecture of WSN

As mention above, the architecture of WSN composed of a processing unit, acquisition unit, transceiver unit (transmitter and receiver), and power supply unit [10], [6], [11]. The design of WSN is in a way that information can be collected and disseminated to one point or several points (broadcasted). Looking at the processor unit or section, two subsystems can be implemented in this section for WSN. A microprocessor or Microcontroller can be implemented in this section. Implementing a microprocessor in the processing area will enlarge the whole structure because the microprocessor doesn't have memory and therefore an external memory must be added. The microcontroller has microprocessor and memory within a single wafer. Most processing units in a wireless sensor network were single microcontroller units. Brey (2000) said that the microcontroller unit used to double up its functions as processing activities and networking activities. In this book by Brey, the activities of the microprocessor are all encapsulated in microcontroller systems. The major problem with this design using microcontroller is size, speed, performance, and flexibility. The solutions to some of these problems were addressed by the Digital Signal Processing (DSP). With the DPS issues of mathematical calculations are handled. Digital filtering

Algorithms and Fourier series analysis are managed by DSP without human intervention [12]. This places DSP above the traditional Microcontroller units (MCU) in the application of WSN. The limitations of DSP are processing speed and allowable bandwidth which overrides its other advantage of doing basic signal processing without a dedicated approach. With the limitation of DSP, Application Specific Integrated Circuit (ASIC) comes into the design and implementation to overcome some of the weaknesses of microcontroller and DSP limitations. An integrated circuit is an electronics component placed in a single wafer. These components are discrete components like transistors, FETs, JFETs, etc connected and placed in a single unit (wafer) [7]. ASIC has been emphasized by several researchers due to its high performance, low energy utilization, and its miniature type compared to microcontrollers and DSPs. ASIC has within its construction of energy management unit, upgradable sensor interfaces, integrated non-active radio frequency (RF) receiver energized to capture power thereby the ability to remain active for a long time. This allows the RF receiver to offer a time-specific quality of service (QoS) [13]. The inclusion of camera, TX, RX, Power supply, and charging unit into the ASIC improved the functionality of the WSN. The limitations of ASIC ranges from duration to advertise, design anomalies, adaptability, testing, and removal of programming errors contributed to its avoidance in the market design. To avoid the issues of ASIC, a better approach was proposed that uses fast switching electronic components called gates. Gates are digital electronic components that have a higher switching speed than transistors [14]. The approach to reducing the limitations of ASIC forced the researcher to look into field programmable logic gates (FPLG) as a fast solution to issues with ASIC. This architecture has the capability of being programmed after production, dynamic configuration, good bandwidth, and better processing speed. It can adapt to other systems and not surpassing its flexibility. This technology comes with its counterpart, the complex programmable logic devices (CPLD). The CPLD and FPLG encompass variable logic designs with a great range of logic circuits. The design includes operational area, input, and output area good interconnectivity. Its main advantage is in energy utilization at the expense of flexibility due to few logic gates used [10]. The same researchers found that mixing the FPLG and CPLD to form the Hybrid CPLD. This HCPLD could be implemented in three different architectures: standalone, modular, and subsystem in a single wafer improving processing speed to over 96% (F. Karray et al, 2014).

The trend to move technology to digital format forced the mixing of the analogy technology to be mixed with the digital technology in a single unit. In WSN, the Field Programmable Analogue Array (FPAA) has been adopted. The word programmable has brought in strongly the digitalization of the WSN. The FPAA has few analogy configurations work than digital giving it advantages like reliability and efficiency [15]. Some sensor nodes base their design on one programmable chip simply referred to as System on one programmable chip (SOPC) [14]. It is now evident that WSN designers consider power utilization and its source, bandwidth, speed, suppleness (flexibility), interfaces (operating system), cost of production, reliability, programmability, heterogeneity, robustness, medium, sensitivity and integration as paramount in design characteristics[5], [10], [15]. WSN adopts Over the Air programming paradigm in most components like set-top boxes (commonly known as Decoders). This network paradigm has a wide range of applications from short ranges like a blue tooth to a global sensing infrastructure. It doesn't mean that the global wireless sensor network is an infrastructure network but it uses infrastructure in the whole network as shown in figure 2.



Sensors BS infrastructure BS sensors

Figure 3 Global sensor infrastructure networks

Two communication styles exist in WSN as push and pull collection styles. When WSN collects samples of data in a continuous approach in a design fashion (programmed), it is called a push pattern. Push pattern or style has a problem with continuously sampling the data although the time between the placement of request and the time the results from the request are available is low (latency time) [16]. The WSN motes in the pull style will have to wait for an open command from the BS or link before beginning the sampling process. The Pull style has long latency compared to push style but has an advantage of good power utilization and message accommodation during the querying process. These advantages are due to non-continuous sampling.

WSN Data delivery

Infrastructure base communication rules exist in four specific groups: - unicast-one to one transfer of information between distinct motes groups, broadcast where data is transferred between one -to- many motes one communication radius. When motes spread the information to a group, it is a multicast model. The motes in multicast are clustered by an application and packets are processed by clusters that bear the identification number of the cluster. In a multiple storage media in WSN "the sink or base station" accesses the data or information is many to many delivery approaches [17].

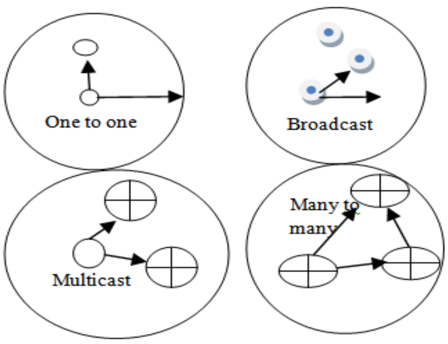


Figure 4 Wireless sensor network delivery approaches

Mobile Ad hoc NETwork (MANET):

A Mobile Ad hoc NETwork is a type of network that identifies the communication path and the nodes without human intervention. It can be referred to as identity-forming or self-forming. MANET, in general, can send non-traffics to another node thereby becoming a router on its own. This implies that it can generate spurious information thereby misusing bandwidth [12], [3], [25]. MANET is a Mobile Ad hoc network without a dedicated path. They don't have any infrastructure. Its activities are dynamical in nature and every node in the network can act as a router to another node. The participating nodes are none dependent. The path or channel is air and the signal transmitted is in the spectrum of radio waves. In MANET, a node can act as a router to another node even if the node is not within the network range. This node that acts as a router to another node will perform routing protocols. A router is a device that connects devices of dissimilar protocols. The node that performs this routing function at that time must be in both network ranges.

Mobile Ad hoc Networks has subclasses.

i. VANET

ii. IMANET

iii. InVANET

VANET: vehicular ad hoc networks are networks that use vehicles as the nodes. Every vehicle participating as a wireless device covering a given range are in high mobility or low mobility. When a car is out of range, another will be identified by the network automatically [18].

IMANET:

This stands for Internet Mobile Networking and is internet-based networking. IMANET connects mobile nodes and permanent internet gateway nodes. This mobile network can establish a link between a mobile network and a fixed network.

INVANT:

An intelligent ad hoc vehicular network (IVANET) is a type of MANET based on artificial intelligence. It defines an intelligent way of vehicle networking usage. It is used to integrate on several ad hoc networks technology ranging from IEEE802.11 to ZigBee [19].

Services offered by mobile Ad hoc networks (MANETs)

In a business environment, MANETs will offer a link between business communities in places where the communication infrastructure is compromised by avoidable forces. Mobile Ad hoc network is used in military war tone areas by embracing unified working place technology. MANETs can be used to monitor applications in places with little access like earthquakes, intrusion detection, and hot areas [10], [21].

Wireless networks and IoT

There exist physical environments that require monitoring and recording of their behavior including anomalies. These environments can be found in enclosed places or open places. Monitoring can be through a closed-loop or open loop. For example, war tone areas, wildlife parks, plant installations, animal or bird's migration can be monitored using wireless networks. The process of getting the patterns is to describe the nodes used in each situation or similar conditions, either singly or as parts of the wireless network. [11], [23]. The graph below is the expected wireless network usage in the internet of things with a projection of 5 years changes.

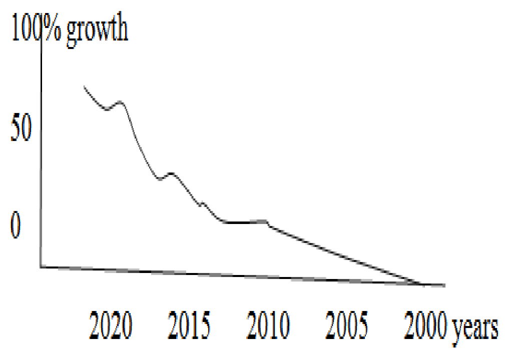


Figure 5 wireless network and IoT

Besides this expected growth and vast usage of modern technology, IoT network naturally includes several devices with inhibited resources and devices including extremely deployed services over large areas like smartphones and cities, engineering plants, un-accessible areas like war tone areas. The perfect management of IoT networks requires considering wireless networks and their associated networks [23].

IoT's main characteristics are shown by an increasing number of connected devices through unique homogeneity, heterogeneity, and the presence of resources coined in wireless technology. To ensure the perfect performance of those network devices, these devices must be able to: connect remotely, over air programming, configure remotely, and monitor their status remotely. A perfect automation management IoT network is achieved through wireless technology [24].

Challenges of WNs

The channel used in wireless network is the air. The limitation WNs is the network impairments like attenuation, inter-modulation, and distortion. Others are there but not severe as the three. Using time specific transmission will eradicate most of these impairments i.e. the use of time division multiplexing.

Future of wireless networks

Wireless networks are perceived to be huge scale development with advanced technology. WNs will provide several interfacing software and devices powered by several other networking interfaces. These interfaces will help the user to be fast in networking usage and supporting mobility in most topographies and topologies. The main limitations lying in the bandwidth is the distance and time (not discussed in this paper). The future of WNs is towards the use of IoT and other advanced technologies like smart cities with over the air programming.

III. Results

The implementation of wireless technology is taking shape in modern technology. Most places that were risky to access the data can be accessed through wireless sensor networks. The trend towards this technology and the advancing microprocessor technology is a result of fast-moving to IoT. Cabled technology has limited usage in IoT due to bulkiness and maintenance costs.

IV. CONCLUSION

Due to the bulkiness of space, unsafe to collect data and sensitivity of data collected there is a need to embrace wireless sensors and mobile ad hoc networks in most fields of trade. Because of their abilities to be programmed directly and over the air programming capability, the two are entering into dynamic and upcoming places like the internet of things and the 5G Networks. Internet of things (IoT) network naturally includes several devices which exhibit highly scalable types of equipment. These devices can be programmed over the air and pre-programming is also possible making these devices to be the center of network technology. The recent management of IoT networks requires considering wireless networks and their associated networks to embrace other technologies like smart cities, smartphones, etc. A perfect automation management IoT network is achieved through modern wireless technology and dynamic programming paradigms. n some areas, a static sensor node needs to be placed to monitor the activity. In some situations, a sensor network that can use several applications like monitoring war, the behavior of wild animals, high fluctuating temperatures will require a good amount of static sensor nodes to be placed. A well-designed algorithm to settle on the positions of devices or nodes in such areas helps to utilize the network power perfectly.

REFERENCES

[1] Dordal, P. L. (2000). *An Introduction to Computer Networks.* New York: Pullmans.
[2] 1Inam Ullah Khan, 2Faheem Numan, 3Shaheen Ahmad. (2016). Mobile ad hoc network challenges. *IJSEAT.*
[3] Flammini, E. S. (2014). Wireless Sensor Networking in the Internet of Things and Cloud Computing Era. *Elsevie*r, 7.
[4] Ernesto Estrada (2010).Quantifying network heterogeneity. Elsevier.
[5] Marcos A.M. Vieira, Adriano B. da Cunha, and C. da Silva Jr. (2018). Designing Wireless Sensor Nodes. *researchgate*, 3.
[6] M.A. Matin and M.M. Islam. (2015). Overview of Wireless Sensor Network. *Researchgate*, 2.
[7] Theraja. (2014). *electrical telecommunication engineering.* New Delhi: Pullmans.
[8] Yadav, D. K. (2018). Optimization of Anchor Nodes in Wireless Sensor Network. *Researchgate*, 7.
[9] Seifedine Kadry, Wassim Hassan. (2015). Design and implementation of the system and network security for an enterprise with worldwide branches. *Researchgate*, 4.
[10] F, Karay, 2017 wireless sensor network: a survey. *Rsearchgate.*
[11] Anupama Sahu (2010). A pattern for sensor nodes. *Researchgate*
[12] Ghorale, M. G. (2016). automated digital filtering algorithm. *researchgate*, 4.
[13] Manoranjani, A Chandrasekar & S Jothi. (2019). Improve QoS of black hole attack in MANET using a trust detection framework. *jCMECC*, 5.
[14] Mano, M. (2015). *Digital Electronics.* New York: Pullmans.
[15] Muhammad Bilal, Moonsoo Kang. (2017). Future Mobile Network Architecture: Challenges and Issues. *IJSEAT.*
[16] Rumanyika, J. (2016). Contemporary Challenges Facing Mobile Networks Operators: *IJEW.*
[17] SAHU, A. (2015). A Pattern for a Sensor Node. *Researchgate*.
[18] Zille Huma Kamal and Mohammad Ali Salahuddin. (2015). *Wireless Sensor and Mobile Ad-Hoc Networks: Vehicular and Space Applications.* New York: Springer.
[19] Paolo Bellavista. (October 2013). Convergence of MANET and WSN in IoT Urban Scenarios . *IEEE*, 9.
[20] Inam Ullah Khan, (2017). Mobile Ad hoc Network challenges
[21] Ankur O. Bang, Prabhakar L. Ramteke. (September 2013). MANET: History, Challenges, And Applications. *Researchgate*, 4.
[22] Manoranjani, A Chandrasekar & S Jothi. (2019). Improve QoS of black hole attack in MANET using a trust detection framework. *jCMECC*, 5.
[23] Parvaneh Asghari, Amir Moumud Rahmani. (2018). Internet. *Elsevie*r, 5.
[24] Pietro Danzi, Anders E. Kalør, Ren´e B. Sørensen. (2019). Communication Aspects of the Integration of Wireless IoT Devices with Distributed Ledger Technology. *IEEE*, 6.
[25] Sadiya Mirza, Sana Zeba Bakshi. (2018). Introduction to MANET . *IRJET.*
[26] So-In, C., Jain, R., Paul, S. and Pan, J. (2012) 'Future wireless networks: key issues and a survey (ID/locator split perspective)', Int. J. Communication Networks and Distributed Systems, Vol. 8, Nos. 1/2, pp.24–52.