Designing Robust Hybrid Wireless Sensor Network: Dual Technology Aspect

Ajay Jangra[1], Rajesh Verma[2], Priyanka[3]

[1] CSE department, U.I.E.T. Kurukshetra University, Kurukshetra, INDIA
[2]CSE [3]ECE department, Kurukshetra Institute of Engineering & Technology, INDIA

er_jangra@yahoo.co.in, vermar.rajesh1974@gmail.com , priyanka.jangra@gmail.com

***Abstract*:** Wireless Sensor Networks are infrastructure less network characterized by dense node deployment, low power, unreliable sensor node, frequent topology change, and severe power, computation and memory constraints because the nodes will often operate with finite battery resources. Because of their wide range of applications, both research community and industry focus on the deployment of wireless sensor networks. In this paper we proposed a framework for hybrid wireless sensor networks using two popular wireless standards deployment. This paper elaborates the sensor network architecture and different wireless technologies. The co-existence behavior is also analyzed with respect to cases of interference occurrence in hybrid model.

Keywords: wireless sensor network, co-existence, interference, network security

1. Introduction

Sensor networks are composed of a large number of sensing nodes, which are equipped with limited computing, radio communication capabilities characterized by dense node deployment, unreliable sensor node, frequent topology change, and severe power, computation and memory constraints because the nodes will often operate with finite battery resources. A typical network configuration consists of sensors working unattended and transmitting their observation values to some processing or control center, the so-called sink node, which serves as a user interface. Due to the limited transmission range, sensors that are far away from the sink deliver their data through *multihop* communications, i.e., using intermediate nodes as relays. In this case a sensor may be both a data source and a data router. Most application scenarios for sensor networks involve battery-powered nodes with limited energy resources. Recharging or replacing the sensors battery may be inconvenient, or even impossible in harsh working environments. Thus, when a node exhausts its energy, it cannot help but ceases sensing and routing data, possibly degrading the coverage and connectivity level of the entire network. A widely employed energy-saving technique is to place nodes in sleep mode, corresponding to low-power consumption as well as to reduce operational capabilities. [5, 6]

WSN is an emerging technology that promises a wide range of potential applications in both civilian and military areas, and has therefore received tremendous attention from both academia and industry in recent years. Depending on the application the large, sudden, and correlated synchronized impulses of data sent to a small number of sinks or base station without significantly disrupting the performance (i.e., fidelity) of the sensing application. This high generation of data packets is usually uncontrolled and often leads to congestion. One of the major challenges wireless sensor networks face today is security. While the deployment of sensor nodes in an unattended environment makes the networks vulnerable to a variety of potential attacks, the inherent power and memory limitations of sensor nodes makes conventional security solutions unfeasible. The sensing technology combined with processing power and wireless communication makes it profitable for being exploited in great quantity in future. The wireless communication technology also acquires various types of security threats[4,6,7]

2. Architecture of WSN

As shown in figure architecture of WSN consists of various components (Sensor, Sensor Unit, Memory, Processing Unit Power supply, Communication Unit, Radio, Mobilizer, Power Generator and Location Finding System). Each component has its own relative task that helps nodes to communicate with each other in WSN. Sensors sense the information from the environment and transfer it to Sensor Unit for further processing. After taking sensed information transfer it to processing unit that apply some calculation on it and make that raw information into a compatible format of given network. Processing unit is directly connected with Memory and Power Supply, Memory is used to store the processed information so that it may be further used and Power supply provides essential power so that all components work well. After that all processed information transfer to the Communication Unit (media) through which the requested information could easily transfer to the client through radio signals or by some other means. Power Supply is also directly connected with Power Generator that generates required power for all the components.

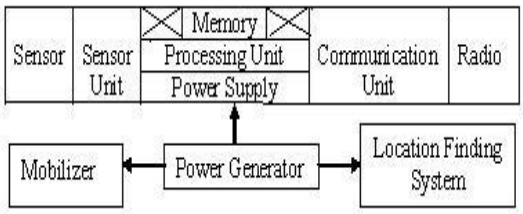

Figure.1 WSN Architecture

Mobilizer is used to move sensor node when assigning any task to the node. A Location finding/detection system is used for finding the location with high accuracy [4, 5,8]

3. Applications of Wireless Sensor Network

Depending upon the requirement and characteristics of system, wide variety of application are there which require constant monitoring and detection of specific event. [5,8]

3.1 Military Applications

like military command & control communications, computing, intelligence, surveillance, reconnaissance & targeting systems, monitoring & Reconnaissance enemy forces, Targeting, Battle damage assessment and Military situation Awareness

3.2 Environmental Applications

like Habitat monitoring, Agriculture research-include sensing of pesticide, soil moisture, PH levels, Habitat Exploration of Animal, Forest Fire and Flood detection and Ocean Monitoring.

3.3 Structural health monitoring

like i) *Heavy industrial monitoring*: In warehouse monitoring to improve inventory control system, Manufacturing monitoring and Industrial automation and factory process control ii) *Health or Medical Applications* : monitor patient physiological data such as blood pressure or heart rate.

3.4 Home Application

Switch on/off, Monitoring product quality, Managing and Monitoring Inventory system, music, and lighting can be set automatically and Control of temperature and airflow adjustment.

4. Communication Technologies (WSN)

In this section we elaborate the various wireless technologies used for deploying a wireless sensor network. Characteristics and features of these technologies are explained below.

4.1 Infrared

Infrared is a wireless communication medium for aligned nodes. It has limited radius of communication and works on ISM band. It has limited processing capabilities as compare to other wireless technologies used in WSN. For a short distance and small data it is reliable to communicate and economic as well.[13]

4.2 Bluetooth (IEEE 802.15)

Bluetooth is wireless LAN technology design to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, coffee makers, ad so on. Bluetooth follows two types of networks: piconet and scatternet. *Piconet:* A small network and can have up to eight nodes, among them one of which is called master; the rest are called slaves. In order to between master and slave can be one-to-one or one-to-many. The maximum numbers of slaves in a piconet can have seven. *Scatternet:* Two or more piconet combined together to form a scatternet. A slave node in one piconet can be the master in another piconet. This node can receive messages from both the piconets and act as master/slave at the same time and they can communicate by mans of multi-hopping [3,1,11,13]

4.3 Wireless Fidelity (Wi-Fi, IEEE 802.11)

Wi-Fi is the transmission of radio signals. In order to define data transmission and manages location independent network access using radio signals on the bases of that we can call it as a packet protocol. The structure of physical/link layer interface of Wi-Fi is similar to Ethernet. The layers above the physical and data link layers include TCP/IP. By the above introduction we can clearly see all programs and applications for TCP/IP that can run on an Ethernet can also be run on Wi-Fi interface. [1, 2, 10]

4.4 ZigBee (IEEE 802.15.4)

ZigBee technology (similar to Bluetooth) provides low data rate and low power connectivity for gadgets that follows low battery life as long as several months to several years. ZigBee has low cost and built to perform wireless networking protocol targeted towards automation and remote control application. The main features of ZigBee are developed for application with relaxed throughput requirements which cannot handle the power consumption of heavy protocol stack, very low power consumption, low data rate in an ad hoc self-organizing network among inexpensive fixed, low cost, network flexibility moving and portable devices. [12, 13]

4.5 WiMax (Worldwide Interoperability for Microwave Access, IEEE 802.16)

As we know in the modern era of broadband wireless access, WiMAX (IEEE 802.16) is an outstanding, well suitable, useful connection oriented protocol to which access fixed and mobile with low cost, high reliability, very high data rate and better efficiency. WiMAX standard defines the formal speciation for deployment of broadband wireless metropolitan area networks (wireless MANs) and with the help of WiMAX (802.16) we can access broadband anytime, on virtually any device and anywhere. While moving at a speed of approximate 125 kmph, in that speed we can also be able to access broadband. WiMAX (802.16) has data rate up to 70 mbps and can be able to work in both license free and licensed band and have high efficiency. WiMAX can have coverage area approximately is up to 50 km. [9, 10]

4.6 Mobile-Fi (IEEE 802.20):-

Mobile-Fi (IEEE 802.20) is the youngest IEEE standard. In order to access fully mobile broadband, it is the first standard designed to carry native IP traffic with licensed airwave

below 3.5 GHz and provides symmetrical wireless rates over long distance (~15km). If we compare all the factors with other technologies for ad hoc network, it has lower power than WiMax but has high mobility and has latency of 10 ms. This features can pursue even with fast moving vehicles and we can also compare it with 3G has 500ms and for optimization of packets uses small antennas.[12,13]

5. Comparison of Wireless Standards

Now it is better to check the performance of Bluetooth and Wi-Fi and analyze them. We are comparing *(as shown in table 1)* the two widely used wireless technologies i.e. Bluetooth and Wi-Fi and check how they are different and compatible to each other. On the bases of some crucial wireless parameter as in table we analyze which one is reliable for what kind of network.

Wireless Parameter	Bluetooth	Wi-Fi
Frequency band	2.4 GHz	2.4 GHz
Physical/MAC layers	IEEE 802.15	IEEE 802.11
Protocol stack size	250 KB	1 MB 32 KB
Minimum quiet bandwidth required	15 MHz (dynamic)	22 MHz (static)
Number of channels	19	13
Maximum number of nodes per network	7	32 per access point
Raw data rate	1 Mbps	11 Mbps
Range	9 m	75 to 90 m
Current consumption	60 mA (Tx mode)	400 mA (Tx mode) 20 mA(Standby mode)
Typical network join time	>3 sec	variable,1 sec typically
Interference avoidance method	FHSS	DSSS

Table 1 Comparison of Bluetooth and Wi-Fi Technologies

6. Co-existence scenario

This paper presents the coexistence scenario of Wi-Fi and blue-tooth wireless technology. Researchers claims that Wi-Fi and Bluetooth do not compete, because of high data rate and high power of the former. Wi-Fi used DSSS instead of FHSS and is a very high power, high cost scheme than Bluetooth with much greater range (45m indoor, 300m outdoors) let's take a look at the actual capabilities of these two technologies, as well as the corresponding requirements of the applications and real world considerations that affect the performance of the systems. [1, 2, 11, 13]

7. Hybrid wireless sensor network modal *(Co-existence aspect)*: The Proposed Model

In this paper we present a hybrid wireless sensor network modal which deploy both Bluetooth and Wi-Fi enable wireless devices. Wi-Fi nodes having communication range more then Bluetooth nodes so, in presented modal Wi-Fi node communicate each other with covering large geographic area and region between Wi-Fi node is covered by Bluetooth nodes. Network using Bluetooth nodes is characterized as low power requirement, low installation/maintain cost, small size, easy to install, secure, small range, multi-hop communication network. Its better to construct a low cost network rather then deploying high cost/power required Wi-Fi devices and Bluetooth nodes provides more information/data of a region *(i.e. more Bluetooth node in same area)*. Bluetooth forms scatter net to cover great area.

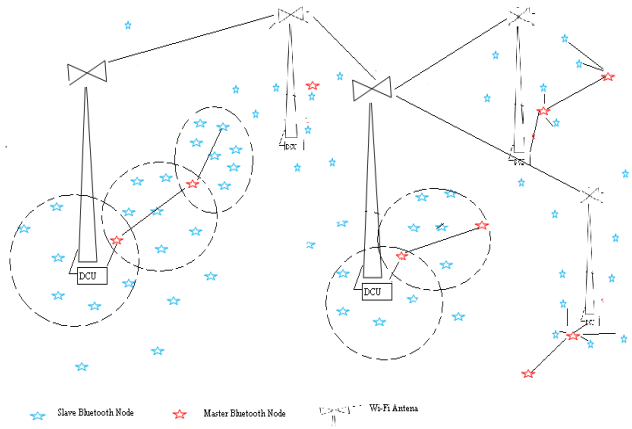

Figure.2 hybrid wireless sensor network

As modal shown in fig.2 where BLUE nodes represents the slave Bluetooth node and RED nodes represents the master Bluetooth node. There is one master node in every piconet. Any slave node in a piconet can behave as a master node for other piconet this process leads a scatter net. There is a DCU (Data Compatible Unit) which works as an interfacing device between Wi-Fi and Bluetooth devices. DCU receives the data from scatter net , process that data in to useful information (removal of redundant data) and convert that data in the form as required by Wi-Fi devices and vice-versa. The DCU contain buffers to store un-processed and processed data, controls the flow of data, cancel the duplicate data (bandwidth utilization). Bluetooth devices separated by short distance which provides accurate and high degree of information. This proposed model could also be feasible and reliable for both stationary and mobile node.

Routing and relaying are the two approaches to provide multi-hop connectivity in wireless ad hoc networks. In relaying, the switching or forwarding decisions take place at the MAC layer, while routing schemes make these decisions at the network layer. Routing is a widely researched and practiced solution, whereas relaying has not been adequately explored in wireless ad hoc networks. The IEEE 802.11 MAC protocol is the standard for wireless LANs; it is widely used in test beds and simulations for wireless multi-hop ad hoc networks. However, this protocol was not designed for multi-hop networks. Although it can support some ad hoc network architecture, it is not intended to support the

wireless mobile ad hoc network, in which multi-hop connectivity is one of the most prominent features.

7.1 Power management

Power consumption is a critical consideration as it directly affects device battery life specially in case of wireless sensor networks. This consideration is obviously most crucial for devices that spend most or all their operating hours on battery power. Bluetooth was designed to be a small-form factor, low-cost, low-power technology. The Bluetooth specification incorporates a number of power saving features in order to keep power use to a minimum. These features include a *standby mode* as well as four connected modes – (*parked, hold, sniff and active*). An adaptive transmission power feature further minimizes power use. Wi-Fi offers a power save mode in which STAs "*sleep*," then *reawaken* periodically to check for messages. Table 2 shows the power requirement for both technologies. [3, 10, 11]

Power required in	Bluetooth	Wi-Fi
Transmit (mA)	50-100	340-450
Receive (mA)	50-80	250-310
Idle/Sleep (mA)	1.5-2	10 - 32

Table 2. Typical Bluetooth and Wi-Fi power requirements comparison

Bluetooth devices required very less amount of power as compared to Wi-Fi. The implication is that Bluetooth will drain the battery less quickly than will Wi-Fi, making Bluetooth a more attractive option for users with smaller devices.

7.2 Security

Security threats to any network include the physical security of the network, unauthorized access, eavesdropping and attacks from within the network's authorized user community. Wireless sensor networks are more susceptible to threats due to the fact that signals from the network are more accessible to potential hackers. Nevertheless, both Bluetooth and Wi-Fi are highly resistant to security threats based on the security procedures implemented in the protocols as well as commonly used adjunct security procedures. Some of the basic security concepts addressed by the technologies include: [3, 4,]

i) Authentication – verifying who is at the other end of a link between devices;

ii) Authorization – the process of determining what a device or user is *allowed to do*;

iii) Encryption – disguising information to make it *inaccessible to unwanted listeners*.

7.3 Interference

Wi-Fi WLAN installations and the anticipated growth in the use of Bluetooth-enabled devices ensure that the two technologies will find themselves sharing space because both use 2.4GH spectrum (ISM band). The question naturally arises as to how these two technologies will get along. Interference between Bluetooth and Wi-Fi will occur any time there is an overlap of both time and frequency between transmissions associated with each technology.

7.4 Cases of interference occurrence

Case-I Wi-Fi receiver senses a Bluetooth signal at the same time when a Wi-Fi signal is being sent to it.

Case-II Bluetooth receiver senses a Wi-Fi signal at the same time when a Bluetooth signal is being sent to it.

7.5 Discussion

Bluetooth is considered less susceptible to interference because of its frequency hopping capability. It has the ability to "hop away" from interfering signals and does so pseudo-randomly. Wi-Fi is considered more susceptible to interference because it inhabits a specific 22 MHz pass band and cannot "hop away" from interference as Bluetooth can. Its collision avoidance mechanism also results in retransmission following Bluetooth interference events, leading to successful transmission but reduced throughput. [2]

8. Interference reduction methods

To minimize any potential interference between Wi-Fi and Bluetooth systems can follow a few simple guidelines to help ensure optimal coexistence between the two technologies.

i) Ensure adequate spacing between Wi-Fi APs and Bluetooth APs to minimize the probability of interference b/w the two types of devices most likely to be transmitting.

ii) Do not deploy any devices that are simultaneously equipped with both Bluetooth and Wi-Fi.

iii) Increase the number of Wi-Fi APs deployed in order to yield a shorter average distance between wireless LAN STAs and APs.

9. Conclusion

Low cost, performance and security are remains the major objectives of a sensor network. The hybrid sensor network framework proposed in this paper deployed Bluetooth and Wi-Fi in a same network model. Bluetooth nodes perform low cost and short distance scatternet based communication, which can enhanced the sensor networks performance by deploying heterogeneous nodes for observing different parameters for a common network, co-existed with Wi-Fi. It is also claim that both Bluetooth and Wi-Fi technologies are complementary to each other but not competing.

References

1. Shoemake, M., *Wi-Fi (802.11b) and Bluetooth: Coexistence Issues and Solutions for the 2.4 GHz ISM Ban*d, February 2001.
2. Mobilian Corporation, *Wi-Fi (802.11b) and Bluetooth: An Examination of Coexistence Approache*s, 2001.
3. Jakobbson, M. et al., *Security Weaknesses in Bluetoot*h, February 2001
4. Schenk, R. et al., *Wireless LAN Deployment and Security Basic*s, ExtremeTech.com, August 2001

5. .F. Akyildiz, W.Su, Y.Sankarasubramaniam, E. Cayirci, "Wireless Sensor Networks: A Survey", IEEE commun. Mag., published by Elsevier Science B.V. in 2002.
6. Abdul-Halim Jallad and Tanya Vladimirova,"Data-centicity in wireless sensor network", springer-Verlag London limited 2009.
7. Raymond Mulligan, Habib M. Ammari," Coverage in Wireless Sensor Network: A Survey" , network protocol and algorithm, Vol 2, published in 2010
8. Chiara Buratti, Andrea conti, Davide Dardari, Roberto Verdone," An Overview on Wireless Sensor Network Technology and Evolution", ISSN 1428-8220, published on 31August 2009.
9. N. Gupta and G. Kaur, "WiMAX: Applications," ser. The WiMAX Handbook, S. Ahson and M. Ilyas, Eds. CRC Press (Taylor and Francis Group), 2008, ch. 3: WiMAX Technology for Broadband Wireless Communication, pp. 35 – 54, ISBN 9781420045474.
10. "An Introduction to Wi-Fi" 019-0170 • 090409-B USA 2007-2008, Caroline Gabriel, "WiMax", ARCchart ltd., London EC2A 1LN
11. Ajay Jangra, Sunita Beniwal, Anil Garg, "Co-existence behavior study of Bluetooth & Wi-Fi for 2.4 GHz ISM band"2006
12. Sinem Coleri ,Ergen, ZigBee IEEE 802.15.4" September 10, 2004
13. Ajay Jangra, Nitin Goel, Priyanka , Komal Kumar Bhatia, "IEEE WLANs Standards for Mobile Ad-hoc Networks (MANETs): Performance Analysis" global Journals of Computer Science and Technology (GJCST) Volume 10 Issue 14 Version 1.0 november 2010.

Author Biographies

Er. Ajay Jangra (11th March 1979) received his B.Tech. in 2001 from kurukshetra university, kurukshetra india, M.Tech. Computer Engineering (with honour) in 2004 from YMCA institute of engineering & technology *(now YMCA university of science & technology)*, faridabad india & M.B.A.(information technology) from guru jambheshwar university, hisar, india in 2008. Presently working as *Assistant Professor* in CSE department UIET, kurukshetra university, kurukshetra,india. He has published 21 research papers repute journals/conference. His area of interest is smart sensors, Ad-hoc & sensor networks, digital & data communication, Mobile computing, software engineering, testing etc.

Dr. Rajesh Verma (May 1974) received his Bachelor degree in 1994 from UCK, kurukshetra university, kurukshetra india, Masters in Computer Application in 1999 and Ph.D in Computer Science & Engg. In 2009 from Department of Computer Science and Applications from kurukshetra university, kurukshetra india. Presently he is *Professor and Head* in CSE department Kurukshetra Institute of Technology and Management, Kurukshetra, INDIA. He has published 30 research papers repute journals/conference. His area of interest is smart sensors, Ad-hoc & sensor networks, AI, Computer Architecture, Simulation, software engineering, testing etc.

Ms. Priyanka (18th October1980) received his B.Tech. (Electronics & communication engineering) in 2002 from kurukshetra university, kurukshetra india, M.Tech. (electronics & communication engineering) with honour from N.I.T. kurukshetra ,india in 2006 & M.B.A.(information technology) from guru jambheshwar university, hisar, india in 2008.Presently working as *Sr. Assistant Professor* in ECE department, kurukshetra institute of technology & management, kurukshetra, india. She has published 10 research papers reputed international journals. Her area of interest is Ad-hoc & sensor networks, Mobile computing, analog & digital communication, antenna & wave propagation etc.