Data Transfer With Wireless Technology: A Review

Aushmin Lodh
B.E.(Electronics & Inst)
IIITM-Kerala
Mobile- 9020694821
aushminlodh@ymail.com

Abhishek Samrat
B.Tech(IT)
IIITM-Kerala
Mobile-7736856919
abhisheksamrat02@gmail.com

Abstract—We review the latest developments in the leading wireless access technologies and we assess the ability of those technologies to meet the future requirements of the wireless devices for the consumer. Wireless Communication is an application of science and technology that has come to be vital for modern existence. From the early radio and telephone to current devices such as mobile phones and laptops, accessing the global network has become the most essential part of our lifestyle. Wireless communication is an ever-developing field, and the future holds many possibilities in this area. One expectation for the future in this field is that, the devices can be developed to support communication with higher data rates and more security. Research in this area suggests that a dominant means of supporting such communication capabilities will be through the use of Wireless LANs. As the implement of Wireless LAN increases well around the globe, it is increasingly important for us to understand different technologies and select the most appropriate one. This paper provides a detailed study of the available wireless LAN technologies and the concerned issues. This is followed by a discussion evaluating and suggesting a feasible standard for future.

New generations of handheld devices allowed users access to store data even when they travel. Users could set their laptops down anywhere and instantly be granted access to all networking resources. This was, and is, the vision of wireless networks, and what they are capable of delivering. Today, while wireless networks have seen widespread adoption in the home user markets, widely reported and easily exploited holes in the standard security system have stunted wireless deployment rate in enterprise environments. Over time, it became apparent that some form of security was required to prevent outsiders from exploiting the connected resources. We believe that the current wireless access points present a larger security problem than the early lntemet connections. As more wireless technology is wireless technology, this will be a good stepping-stone for providing a good secure solution to any wireless solution.

Keywords: wireless Internet, Wi-Fi, 802.11, WLAN, Geographic Information Systems

I INTRODUCTION

Classical abstractions used in software engineering leave out "nonfunctional" aspects, such as cost, efficiency and robustness. In particular in the field of embedded software, there is a growing awareness that these abstractions no longer suffice to arrive at dependable design .Embedded software is subject to complex and permanent interactions with its, mostly physical, environment via sensors and actuators. Wireless sensor and actuator networks such as Wireless HART are setting new standards in this domain. Regardless if wireless or wired, the possibilities of user intervention with such systems are usually very limited and high requirements are therefore put on performance and dependability as the embedded nature complicates tuning and maintenance. At the same time, embedded software permeates safety and mission critical applications in a spectrum ranging from pace makers to chemical plant control. The future will likely bring an increase in wireless technology also in the context of safety-critical control applications. Wireless communication is known to be inherently unreliable and often is characterized by relatively high message loss rates. When hard real time requirements are to be met despite wireless communication, it becomes even more difficult to come up with safety guarantees. The central problem is that consecutive failures in message transfer may affect the correct functioning. WiFi is becoming a common urban service like any other, electricity or land-phonesas an example. The popularity of WiFi is further enhanced by its capacity to handle multiple types of communication over the same protocol like text, voice, images and video all can be streamed over WLAN networks instantaneously and globally. As we anticipate that complete Wi-Fi coverage in many cities will come about soon, there is an urgent need to explore the spatial impact of this powerful new communication network for an architect

A. Wireless

Recent year witnessed a great increase in 802.11 wireless local-area networks (WLAN) around the world. Wireless Internet, which only a few years ago began as a tool in corporate offices, has come a long way forward, now covering entire urban blocks with uninterrupted networks. According to www.jiwire.com_there are over 20,000 public 'hotspots' already available in the U.S. today. In Europe, London has the largest concentration of public and private wireless networks. While several forward-looking cities like San Jose CA and Philadelphia PA have launched projects to provide free wireless Internet for all citizens, WiFi is becoming a common urban service like any other, electricity or land-phones for example. The popularity of WiFi is further enhanced by its capacity to handle multiple types of communication over the same protocol: text, voice, images and video can all be streamed over WLAN networks instantaneously and globally. As we anticipate that complete WiFi coverage in many cities will come about soon, there is an urgent need to explore the spatial impact of this powerful new communication network, from the point of view of the architect or urban planner. Real world example at the MIT campus around 16,000 students, faculty and staff attend the Institute every day. In the year 2000, when laptops were still expensive and wireless Internet new, MIT decided to undertake a vast operation of building a campus-wide wireless network. Today, this 168 acre campus has over 2300 wireless access points (APs), providing full coverage of WiFi in nearly all buildings on campus.

B. GIS (Geoinformatics) Technology over wireless technology

A new technology is to use a Geographical Information System (GIS) and wireless LOG files, obtained from the to construct an on-line map server, which will allow the huge acre established campus community to observe the real-time WiFi activity on a webpage. Simultaneously, we canl collect the generated maps and traffic data into a database, which will allow comprehensive analyses to be carried out at a later date, exploring behavioral trends in a longer time frame. Thanks to the fusion of GIS data about the campus and the relative precision of WLAN logs, the analysis can range from an individual user's point of view to a multilayered analysis of the campus as a whole. Eventually, we hope that the web page can accumulate different layers
of real-time information about the campus, including data about WiFi activity, the amount of bytes transferred, a spatial reference to the real- time events calendar, parking availability, etc. which could evolve into a standard tool for understanding the natural complexity of the campus on a real-time website.

The second stage of this project will enable students to voluntarily make their personal data log files and movement patterns of their MAC addresses accessible to others on the web. This would allow friends who have reciprocally agreed to share their movement patterns, to track their device locations on the campus map. In order to participate and expose one's MAC or I.P. location on the webpage, participants will register an agreement on-line and use an opt-in system to set up an identification profile that will characterize them to other participants. Only participating students can track each other's locations on the webpage. The profile identification will be similar to many existing internet communities like MSN Messenger, Skype and others. Besides providing a new tool of interaction, this project will also allow us to perform a social analysis of the campus use based on individual profile tracking with the wifi enabled campus surplussing wireless technology. By understanding how a given type of people use the campus spatially, we can for the first time understand the urban environment as set of quantifiable processes of inter-relationships in real-time.

C. A Wireless Bike Break

This section discusses the principal aspects of a wireless bike brake, as an example of a safety critical wireless sensor network system that, despite making use of wireless communication, has hard real time requirements.

1) Problem Statement

We consider a bike brake, where the communication between the brake handle and the brake shoe is wireless. The wireless design has led us to use a number of components, the force sensor, sender, replicator(s), receiver, actuator and the alarm system.

The bike brake system has very strict real time timing requirements. The time between the rider applying the brake by pressing the handle to the braking mechanism actually being applied, has to be short enough to ensure the safety of the rider. The time for applying the brake includes the time for the force sensor to notice the difference in the force being applied which is being conveyd to the sender, the sender transmitting these values wirelessly to the receiver and then its informing the actuator to apply the braking force. The timings of all these steps in the braking process are also limited by the hardware being design or used

Example of above statement

A regular bike-rider may ride at 20 km/h. We have decided that the communication between handle and shoe cannot exceed 140 ms, based on the fact that the actuator mechanics takes 120 ms to react and that adding both intervals leads to 240 ms, which is equivalent to 3 meters

2) Principal Design

Replacing only the connecting wire between the brake handle and the brake shoe with a wireless connection does not result in a wireless electric brake. We identified the following basic components and their functionalities.

Force Sensor: This sensor is an apparatus which replaces the brake handle and produces a digital or analog signal which represents the pulled force.

Sender: The sender is located near to the Force Sensor and has a wire connected to it. It reads the signal and sends it using a wireless connection to the Receiver.

Actuator: Actuator produces the brake force based on the control signal of the Receiver

Receiver: This component receives values from the Sender and modulates a control signal for the Actuator to a wire.

Replicator(s): To increase reliability we study the op- tion to introduce a network of node(s) for redundancy. A Replicator component acts as a Sender and a Receiver combined, it listens to the Sender (or all Replicators) and echoes the last value obtained to the Receiver (or to all Replicators). A scenario with 3 replicators is depicted below.

Alarm System: If any problem occurs, the Alarm System has to notify the rider that the brake is not working in this moment.

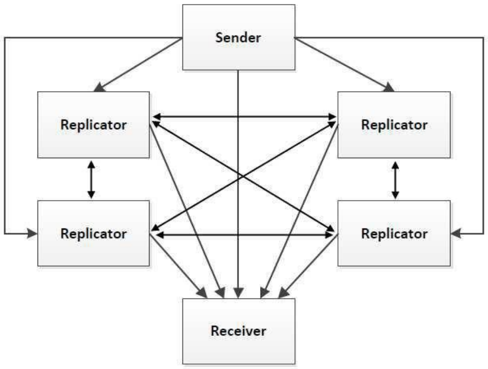

Fig 1 :- Block Diagram Of Wireless Bike Break

D. Bluetooth**:** Bluetooth is an industry specification for short-range RF-based connectivity for portable personal devices with its functional specification released out in 1999 by Bluetooth Special Interest Group [6]. Bluetooth communicates on a frequency of 2.45 gigahertz, which has been set aside by international agreement for the use of industrial, scientific and medical devices (ISM). One of the ways Bluetooth devices avoid interfering with other systems is by sending out very weak signals of 1 milliwatt. The low power limits the range of a Bluetooth device to about 10 meters whivh cuts the chances of interference between a computer system and a portable telephone or television. Bluetooth makes use of a technique called spread-spectrum frequency hopping. In this technique, a device will use 79 individual, random frequencies are chosen within a designated range, changing from one to another on a regular basis. Bluetooth devices essentially come in two classes, both using point-to-point communication to speak. Class 3 devices operate at 0 dBm range and are capable of transmitting 30 feet, through walls or other objects and the other class is termed as class 1 products.

Fig 2:-List & Range Of Wireless Sensors

Standard	**IEEE 802.11**	**802.11a/802.11b**	**HiperLAN/2**	**Bluetooth**	**HomeRF**
Mobile Range (GHz)	N.A/E 2.4 – Japan 2.47 – 2.499	**a** Aimed at 5.15 – 5.25 5.25 – 5.35 5.725 – 5.825 **b** NA/Europe 2.4 – 2.483 Japan 2.47 – 2.499	Aimed at 5.15 – 5.47 – 5.725	NA/Europ 2.4 – Japan 2.47 – 2.499	NA/Euro 2.4 – Japan 2.47 – 2.499
Multiple Access Method	CSMA /CA	CSMA/CA	TDMA	TDMA	TDMA/ CSMA
Duplex Method	TDD	TDD	TDD	FDD	TDD
Number of IndeX XXpendent Channels	FHSS*: 79 DSSS*: 3-5	**a** 12 **b** 3 to 5	12	FHSS*: 79	FHSS*: 79

1) HomeRF:

Homo RF was a wireless networking specification for home devices. It was developed in 1998 by the Home Radio Frequency Working Group, a consortium of mobile wireless companies that included Proxim Wireless, Intel, Siemens AG, Motorola, Philips and more than 100 other companies.[1] The group was disbanded in January 2003 after other wireless networks became accessible to home users and Microsoft began including support for them in its Windows operating systems. As a result HomeRF fell into obsolescence but later on home rf gain its importance and now HomeRF is an open industry specification developed by Home Radio Frequency that defines how electronic devices such as PCs, cordless phones and other peripherals share and communicate voice, data and streaming media in and around the home. HomeRF-compliant products operate in the license-free 2.4 GHz frequency band and utilize frequency hopping spread spectrum RF technology for secure and robust wireless communications with data rates of up to 1 Mbps (HomeRF 1). Unlike Wi-Fi, HomeRF already has quality-of-service support for streaming media and is the only wireless LAN to integrate voice. HomeRF may become the worldwide standard for cordless phones. In the year 2001, the Working group unveiled HomeRF 2.0 that supports 10 Mbps (HomeRF 2.0) or more.

II CLASSIFICATION OF WIRELESS LAN

Wireless LANs can be broadly classified into two categories: ad hoc wireless LANs and wireless LANs with infrastructure. In ad hoc networks, several wireless nodes join together to establish a peer-to-peer communication. Each client communicates directly with the other clients within the network. Ad-hoc mode is designed such that only the clients within transmission range (within the same cell) of each other can communicate. If a client in an ad-hoc network wishes to communicate outside of the cell, a member of the cell MUST operate as a gateway and perform routing. They typically require no administration. Networked nodes share their resources without a central server. In wireless LANs with infrastructure, there is a high-speed wired or wireless backbone. Wireless nodes access the wired backbone through access points. These access points allow the wireless nodes to share the available network resources efficiently. Prior to communicating data, wireless clients and access points must establish a relationship, or an association. Only after an association is established can the two wireless stations exchange data.

A. Issues over Wireless LAN:

Since wireless devices need to be small and wireless networks are bandwidths limited, some of the key challenges in wireless networks are:

a. Data Rate Enhancements.
b. Low power networking.
c. Security.
d. Radio Signal Interference.
e. System Interoperability.

1) Enhancing Data Rate: Improving the current data rates to support future high speed applications is essentially special, if multimedia service are to be provided. Data rate is a function of various factors such as the data compression algorithm, interference mitigation through error-resilient coding, power control, and the data transfer protocol. Therefore, it is imperative that manufacturers implement a well thought out design that considers these factors in order to achieve higher data rates.

2) Low Power Design: The size and battery power limitation of wireless mobile devices place a limit on the range and throughput that can be supported by a wireless LAN. The complexity and hence the power consumption of wireless devices vary significantly depending on the kind of spread spectrum technology being used to implement the wireless LAN. Normally, direct sequence spread spectrum (DSSS) based implementations require large and power-hungry hardware compared to frequency hopped spread spectrum (FHSS). They require to consume about two to three times the power of an equivalent FHSS system. But, the complex circuitry provides better error recovery capability to DSSS systems compared to FHSS. The right time has come for the researchers and developers to approach these issues in all the wireless LAN technologies together and from a global perspective point of view.

3) Security: Security [10] is a big concern in wireless networking, especially in m- commerce and e-commerce applications. Mobility of users increases the security concerns in a wireless network. Current wireless networks employ authentication and data encryption techniques on the air interface to provide security to its users. The IEEE 802.11 standard describes wired equivalent privacy (WEP) that defines a method to authenticate users and encrypt data between the PC card and the wireless LAN access point. In large enterprises, an IP network level security solution could ensure that the corporate network and proprietary data are safe. Virtual private network (VPN) is an option to make access to fixed access networks reliable. Since hackers are getting smarter, it is imperative that wireless security features must need frequent upgradation

B. Radio Signal Interference**:**

Interference can take on an inward or outward direction. A radio-based LAN for example, can experience inward interference either from the harmonics of transmitting systems or from other products using similar radio frequencies in the local area. Microwave ovens operate in the S band (2.4GHz) that many wireless LANs use to transmit and receive. These signals result in delays to the user by either blocking transmissions from stations on the LAN or causing bit errors to occur in data being sent. Newer products that utilize Bluetooth radio technology also operate in the 2.4GHz band and can cause interference with wireless LANs, especially in fringe areas not well covered by a particular wireless LAN access point. The other issue ,indicationg outward interference, occurs when a wireless network's signal disrupts other systems, such as adjacent wireless LANs and navigation equipment on aircraft.

C. System Interoperability

With wireless LANs, interoperability is taken as a serious issue. There are still pre-802.11 (proprietary) wireless LANs, both frequency-hopping and direct sequence 802.11 versions, and vendor-specific enhancements to 802.11- compliant products that make interoperability questionable. Toensure interoperability with wireless LANs, it is best to implement radio cards and access points from the same vendor.

III SECURITY ISSUES IN 802.11

During the beginning of the commercialization of the Internet, organizations and individuals connected without concern for the security of their system or network. Overtime, they realized that some form of security was required to prevent others from exploiting the connected resources. Deployment of Wireless LAN as a medium of communication to connect mobile devices with the wired infrastructure has paved a new path in the networking technology. Security should also be taken as an important factor while considering this way of communication. In contrary to their wired counterparts, a wireless network is more difficult to secure since the transmission medium is open to anyone within the geographical range of a transmitter. Data privacy is usually accomplished over a radio medium using encryption. While encryption of wireless traffic can be achieved, it is usually at the expense of increased cost and decreased performance. Organizations are rapidly deploying 802.11 standard based wireless infrastructures. For most WLAN users, there are three basic issues

- Data Compromise is any form of disclosure to unintended parties of information. Data compromise can be inappropriate access to have payroll records by company employees, or industrial espionage whereby marketing plans can be disclosed to a competitor.

- Denial of Service is an operation designed to block or disrupt normal activities of a network or facility. This can take the form of false requests for login to a server, whereby the server is too distracted to accommodate proper login requests.
- Unauthorized access is any means by which an unauthorized party is allowed access to network resources or facilities. Unauthorized access can lead to compromise, for example, if access is gained to a server with unencrypted information, or destruction in the case that critical files, although encrypted on the server, may be destroyed.

IV RESEARCH CHALLENGES OF WIRELESS NETWORK:

Since wireless devices need to be small and wireless networks are bandwidth limited, some of the key challenges in wireless networks are data rate enhancements, minimizing size, cost, low power networking, user security and Quality of Service (QoS).

A. Signal Fading

Unlike wired media, signals transmitted over a wireless medium may be distorted or weakened because they are propagated over an open, unprotected, and ever changing medium with irregular boundary. Besides, the same signal may disperse and travel on different paths due to reflection, diffraction, and scattering caused by obstacles before it arrives at the receiver. The dispersed signals on different paths may take different times to reach the destination.Thus, the resultant signal after summing up all dispersed signals may have been significantly distorted and attenuated when compared with the transmitted signal. The receiver may not recognize the signal and hence the transmitted data cannot be received. This unreliable nature of the wireless medium causes a substantial number of packet losses

B. Power and Energy

A mobile device is generally handy, small in size, and dedicated to perform a certain set of functions; its power source may not be able to deliver power as much as the one installed in a fixed device.When a device is allowed to move freely, it would generally be hard to receive a continuous supply of power. To conserve energy, a mobile device should be able to operate in an effective and efficient manner. To be specific, it should be able to transmit and receive in an minimize the number of transmissions and receptions for certain communication operations .

C. Data Rate

Improving the current data rates to support future high speed applications is essential, especially, if multimedia service are to be provided. Data rate is a function of various factors such as the data compression algorithm, interference mitigation through error-resilient coding, power control, and the data transfer protocol. Therefore, it is imperative that manufacturers implement a well thought out design that considers these factors in order to achieve higher data rates. Data compression plays a major role when multimedia applications such as video conferencing are to be supported by a wireless network. Currently, compression standards such as MPEG-4 produce compression ratios of the order of 74 to 100. The challenge now is to improve these data compression algorithms to produce high quality audio and video even at these compression rates. Unfortunately, highly compressed multimedia data is more sensitive to network errors and interference and this necessitates the use of algorithms to protect sensitive data from being corrupted. Efficient error control algorithms with low overhead must be explored. Another way to enhance the data rates would be to employ intelligent data transfer protocols that adapt to the time- varying network and traffic characteristics.

D. Security

Security is a big concern in wireless networking, especially in m-commerce and e-commerce applications [8]. Mobility of users increases the security concerns in a wireless network. Current wireless networks employ authentication and data encryption techniques on the air interface to provide security to its users. The IEEE 801.11 standard [2] describes wired equivalent privacy (WEP) that defines a method to authenticate users and encrypt data between the PC card and the wireless LAN access point network. We presented an overview of a comprehensive list of research issues and challenges of the wireless network like signal fading problem , mobility problem ,power and Since hackers are getting smarter, it is imperative that wireless security features must be updated constantly [10]. A low interruption frequency implies that handoffs do not occur too often. Applications may accept a larger maximum connection interruption time in exchange for a low interruption frequency. For example, it may be more desirable to have infrequent long breaks in a video connection, rather than frequent smaller breaks. The IEEE 801.11 standard describes wired equivalent privacy (WEP) that defines a method to authenticate users and encrypt data between the PC card and the wireless LAN access point.

V CONCLUSIONS

This paper identifies and describes the various research issues and challenges available in the wireless domain. We first presented an overview of the taxonomy of wireless energy , data rate enhancement, security and the quality of service issues problems of the wireless networks .In addition the popularity of wireless networks growing at a exponential rate, the data rate enhancements, minimizing size, cost, low power networking, user security and the best requirement to obtain the required QoS problems becomes more challenging.

REFERENCES

[1] V.O.K. Li and X. Qiu, ―Personal Communication Systems (PCS),‖ Proc. IEEE, vol. 83, no. 9, Sept. 1995,
[2] J.H.Schiller, Mobile Communications, 2nd ed., Addison-Wesley, 2003.
[3] Y. Hu and V.O.K. Li, ―Satellite-Based Internet: A Tutorial,‖ IEEE Commun. Mag., vol. 39, no. 3, Mar. 2001, pp. 154–62
[4] A.Gupta, I. Wormsbecker, and C. Williamson―Experimental Evaluation of TCP Performance in Multi- Hop Wireless Ad Hoc Networks,‖ Proc. IEEE MASCOTS 2004, Volendam, The Netherlands, 4–8 Oct. 2004, pp. 3–11.
[5] H. Singh and S. Singh, ―Energy Consumption of TCP Reno, Newreno, and SACK in Multi-Hop Wireless Networks,‖ ACM SIGMETRICS Perf. Evaluation Rev., vol. 30, no. 1, June 2002, pp. 206-216.
[6] Chip Craig J. Mathias Principal, Farpoint Group COMNET 2003 ―Wireless Security: Critical Issues and Solutions‖ 29 January 2003
[7] Sandra Kay Miller ―Facing the Challenge of Wireless Security‖ July 2001
[8] E.A. Lee Embedded Software. In M. Zelkowitz, editor,Advances in Computers, vol. 56, Academic Press, 2002.
[9] MyriaNed R : large wireless sensor and control network. http://wsn.chess.nl/ – accessed on Apr 28, 2011