Sensorless Sensing with WiFi device free human detection

[1]M.Prashant, [2]Ramesh Krishnan
[1]Internship Trainee,
Polaris India Pvt. Ltd.,
Chennai, India.
Email: prashantmuralidharan@gmail.com
Research Scholar
Department of ECE
Easwari Engineering College, Anna University
Email:eswaranphd@gmail.com

ABSTRACT:
Can WiFi signals be used for sensing purpose? The growing PHY layer capabilities of WiFi has made it possible to reuse WiFi signals for both communication and sensing. Sensing via WiFi would enable remote sensing without wearable sensors, simultaneous perception and data transmission without extra communication infrastructure, and contactless sensing in privacy-preserving mode. Due to the popularity of WiFi devices and the ubiquitous deployment of WiFi networks, WiFi-based sensing networks, if fully connected, would potentially rank as one of the world's largest wireless sensor networks. Yet the concept of wireless and sensorless sensing is not the simple combination of WiFi and radar. It seeks breakthroughs from dedicated radar systems, and aims to balance between low cost and high accuracy, to meet the rising demand for pervasive environment perception in everyday life. Despite increasing research interest, wireless sensing is still in its infancy. Through introductions on basic principles and working prototypes, we review the feasibilities and limitations of wireless, sensorless, and contactless sensing via WiFi. We envision this article as a brief primer on wireless sensing for interested readers to explore this open and largely unexplored field and create next-generation wireless and mobile computing applications.
Key words: Channel State Information (CSI); sensorless sensing; WiFi; indoor localization; device-free human detection; activity recognition; wireless networks; ubiquitous computing

I INTRODUCTION

Wi-Fi, or Wireless Fidelity is freedom :it allows you to connect to the internet from your couch at home, in a hotel room or a conferance room at work without wires . Wi-Fi is a wireless technology like a cell phone. Wi-Fi enabled computers send and receive data indoors and out; anywhere within the range of a base station. And the best thing of all, it is fast . However you only have true freedom to be connected anywhere if your computer is configured with a Wi-Fi CERTIFIED radio (a PC card or similar device). Wi-Fi certification means that you will be able able to connect anywhere there are other Wi-Fi CERTIFIED products – whether you are at home ,office , airports, coffee shops and other public areas equipped with a Wi-Fi access availability. Wi-Fi will be a major face behind hotspots , to a much greater extent.More than 400 airports and hotels in the US are targeted as Wi-Fi hotspots. The Wi-Fi CERTIFIED logo is your only assurance that the product has met rigorous interoperability testing requirements to assure products from different vendors will work together. The Wi-Fi CERTIFIED logo means that it is a "safe" buy.

Wi-Fi certification comes from the Wi-Fi Alliance, a non-profit international trade organisation that tests 802.11 based wireless equipment to make sure that it meets the Wi-Fi standard and works with all other manufacturer's Wi-Fi equipment on the market. The Wi-Fi Alliance (WELA) also has a Wi-Fi certification program for Wi-Fi products that meet interoperability standards. It is an international organisation devoted to certifying interoperability of 802.11 products and to promoting 802.11as the global wireless LAN std across all market segment.

IEEE 802.11 ARCHITECTURES
In IEEE's proposed standard for wireless LANs (IEEE 802.11), there are two different ways to configure a network: ad-hoc and infrastructure. In the ad-hoc network, computers are brought together to form a network "on the fly." As shown in Figure 1, there is no structure to the network; there are no fixed points; and usually every node is able to communicate with every other node.

A good example of this is the aforementioned meeting where employees bring laptop computers together to communicate and share design or financial information. Although it seems that order would be difficult to maintain in this type of network, algorithms such as the spokesman election algorithm (SEA) [4] have been designed to "elect" one machine as the base station (master) of the network with the others being slavesAnother algorithm in ad-hoc network architectures uses a broadcast and flooding method to all other nodes to establish who's who.
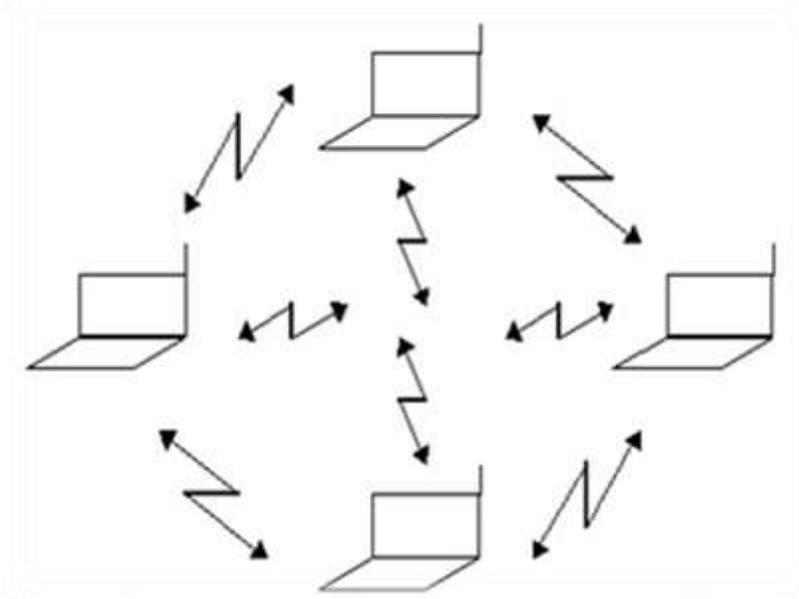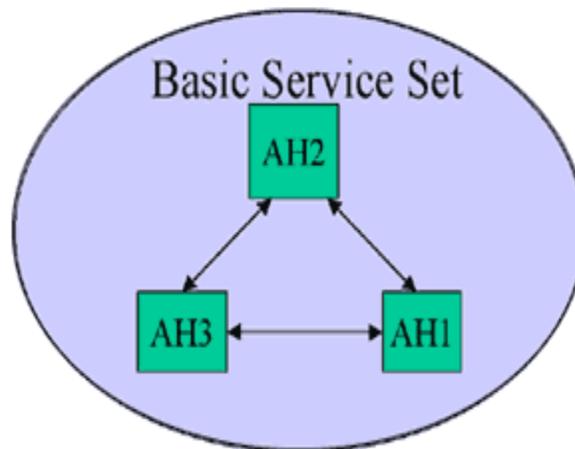
Fig.1: Ad-Hoc Network

Figure 1a: The ad-hoc network structure in the 802.11 protocol.

The ad-hoc network (**Figure 1a**) is one formed from a collection of peer nodes all using RF links. This network has no formal structure; all nodes can communicate with all other nodes. Several algorithms are available to prevent this from being total chaos, however, including a spokesman election algorithm that selects a master from the collective and makes all others slaves. Another possibility is to use broadcast and flooding to all other nodes to establish an addressing scheme.

A good example of an ad-hoc network is one that is formed when a group gets together at a meeting and everyone has WLAN-enabled PCs. They can form an ad-hoc network at the meeting to share data.

As shown in figure 2 the network structure used in wireless LANs is the infrastructure. This architecture uses fixed network access points with which mobile nodes can communicate. These network access points are sometime connected to landlines to widen

the LAN's capability by bridging wireless nodes to other wired nodes. If service areas overlap, handoffs can occur. This structure is very similar to the present day cellular networks around the world.

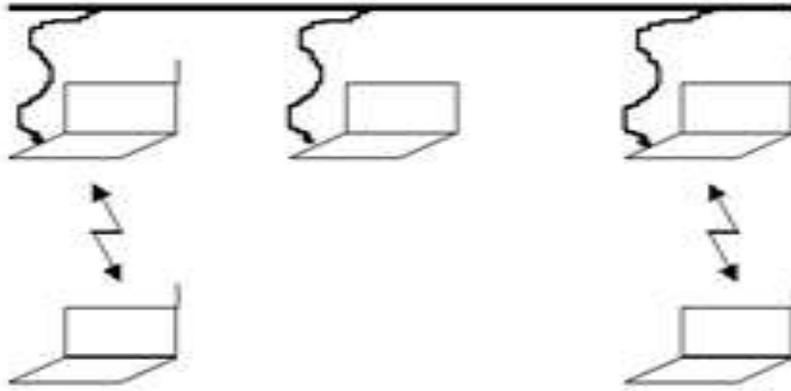They can form an ad-hoc network at the meeting to share data.
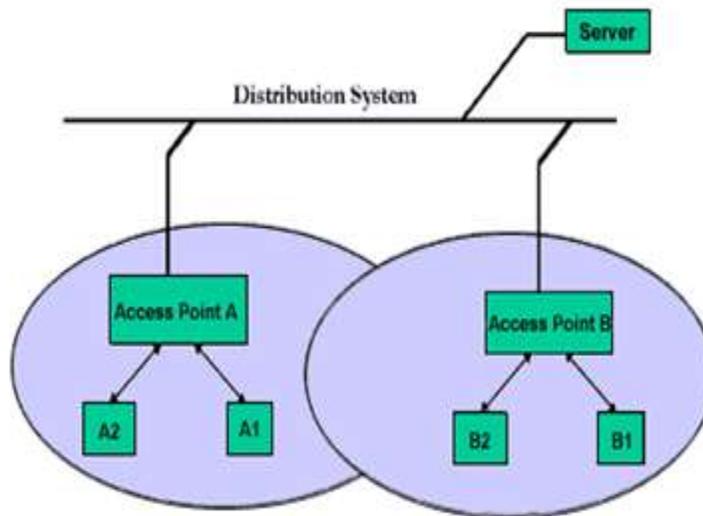

Fig.2: Infrastructure Network

Figure 2b: The infrastructure network structure in the 802.11 protocol.

The infrastructure network has a formal structure (**Figure 1b**). It uses fixed access points (AP), which are RF-enabled nodes on a hard-wired LAN. The structure allows mobile nodes to communicate with the access points to join the network. Mobile units can move freely within the area covered by the access point radios, typically a range of 100 meters for the 2.4 GHz band. The RF link is intended to operate with units moving at pedestrian or vehicular speeds.

The ABCs of IEEE 802.11

At the beginning the IEEE802.11 was an extension technology for conventional or wired LANs.Nowadays it has grown in to something much more capable, complex and confusing. With growth, new issues have arisen such as security, roaming among multiple access points, and even quality of services. These issues are dealt by extensions to the standard identified by the letters of the alphabet derived from the 802.11 task groups that created them:

802.11a

The 802.11a supplement to 802.11 was published in 1999. It uses Orthogonal Frequency Division Multiplexing (OFDM) to provide data rates to 54 Mbps in the 5 GHz U-NII licensed National Information Infrastructure)

802.11b

Commercially trademarked in 1999 by Wireless Ethernet Compatibility Alliance (WECA)as Wi-Fi , this is the extension that made 802.11a a house hold world

802.11g

The 802.11g task group is working on a supplement to the 802.11 standard that defines a technology for operation at 2.4 GHz that offers higher data rates (up to 22 Mbps) using OFDM, while remaining backwards compatible to 802.11b.

BASIC COMPONENTS

IEEE 802.11b wireless networking consists of the following components:

- Stations

    A station (STA) is a network node that is equipped with a wireless network device. A personal computer with a wireless network adapter is known as a wireless client. Wireless clients can communicate directly with each other or through a wireless access point (AP). Wireless clients are mobile.

- Wireless APs

    A wireless AP is a wireless network node that acts as a bridge between STAs and a wired network. A wireless AP contains:

    o   At least one interface that connects the wireless AP to an existing wired network (such as an Ethernet backbone).

    o   A wireless network device with which it creates wireless connections with STAs.

    o   IEEE 802.1D bridging software, so that it can act as a transparent bridge between the wireless and wired networks.

        The wireless AP is similar to a cellular phone network's base   station. Wireless clients communicate with both the wired   network   and other   wireless clients through the wireless AP. Wireless APs are not mobile and act as peripheral bridge devices that extend a wired network.

- Ports

    A port is a channel of a device that can support a single point-to-point connection. For IEEE 802.11b, a port is an association, a logical entity   over which a single wireless connection is made. A typical wireless client   with   a   single wireless network adapter has one port and can support only   one wireless connection. A typical wireless AP has multiple ports and can   simultaneously support multiple wireless connections. The logical   connection between a port on the wireless client and the port on a wireless   AP is a point-to- point bridged LAN segment—similar to an Ethernet-based network client that is connected to an Ethernet switch

OPERATION BASICS

When a wireless adapter is turned on, it begins to scan across the wireless frequencies for wireless APs and other wireless clients in ad hoc mode. Assuming that the wireless client is configured to operate in infrastructure mode, the wireless adapter chooses a wireless AP with which to connect. This selection is made automatically by using SSID and signal strength and frame error rate information. Next, the wireless adapter switches to the assigned channel of the selected wireless AP and negotiates the use of a port. This is known as establishing an association.

If the signal strength of the wireless AP is too low, the error rate too high, or if instructed by the operating system (in the case of Windows XP), the wireless adapter scans for other wireless APs to determine whether a different wireless AP can provide a stronger signal or lower error rate. If such a wireless AP is located, the wireless adapter switches to the channel of that wireless AP and negotiates the use of a port. This is known as reassociation.

Association with a different wireless AP can occur for several reasons. The signal can weaken as either the wireless adapter moves away from the wireless AP or the wireless AP becomes congested with too much traffic or interference. By switching to another wireless AP, the wireless adapter can distribute the load to other wireless APs, increasing the performance for other wireless clients. You can achieve contiguous coverage over large areas by placing your wireless APs so that their signal areas overlap slightly. As a wireless client roams across different signal areas, it can associate and reassociate from one wireless AP to another, maintaining a continuous logical connection to the wired network.

TECHNOLOLGY

Wi-Fi uses radio technology called IEEE 802.11b to provide secure ,reliable,fast wireless connectivity.A Wi-Fi network can be used to connect computers to each other, to the internet and to the wired networks. Though WLANs are easy to deploy, the network administrator or IT professional will benefit from some basic knowledge about radio wave propagation. Although it is possible to utilize infrared technology (which always requires line of sight between elements of the network), this paper deals only with Radio Frequency (RF) wireless networks, which have become the industry accepted standard for WLANs.

The reason for using RF is simple. It can pass through solid objects such as office walls. However, radio waves do not go on forever in all directions without weakening or being affected by physical barriers. The user needs to have some understanding of their propagation characteristics, as well as the relationship between power levels and data rates, before a wireless network can be designed.

Propagation Characteristics Must Be Considered

Reflection - Radio waves can be reflected by some materials. This phenomenon is often used to steer microwave signals between stations that are not line-of-sight, but in an office environment it can create multipath (see below).

Absorption - Radio waves can be absorbed by many materials such as water, plastic, sheetrock, and carpet.

Geometric Spreading loss - Radio waves, like light waves, get weaker as they expand outward away from their source. This loss grows as the square of the distance. This means that if a device is moved twice as far away, the signal power drops by one fourth.

Path loss - The above phenomena lead to path loss, or an unavoidable weakening of the signal's power as it propagates outward. In an office environment, the placement of furniture and walls, and even the movement and location of people, will contribute to the amount of path loss.

Multipath - If a received signal is made up of radio waves from the same signal that has dispersed and arrived from different paths, i.e. some of the original energy was often exhibit this as ghosting. Network users may likewise experience its digital counterpart - referred to as *intersymbol interference*. This is caused when the difference in time between radio waves arriving from the same signal, referred to as *delay spread*, is enough to cause symbol overlap in the digital data. As the data transmission speed gets faster, the time between received data bits get smaller and more susceptible to intersymbol interference, so multipath places an upper limit on data transmission   speed.

Propagation characteristics are frequency dependent:

At *lower frequencies (longer wavelengths)*, less RF energy is absorbed by obstructions. Signals can pass through solid objects   (walls)   more   readily. At *higher frequencies (shorter wavelengths)*, smaller antennas can be used. However, if antennas are scaled down proportionately with wavelength, the received signal power will decrease as a function of frequency squared, due to less signal energy being intercepted by the smaller antenna. This shortcoming can be overcome by using higher gain antennas.

How the properties of radio waves affect networking capabilities?

When used in wireless technologies, the ideal radio wave should have high speed, use little energy and travel far distaces.This type of radio wave would let us transfer information in few milliseconds, require little battery power and send signals at

whatever range we needed. In reality however, it is impossible to achieve all three of these characteristics at the same time. It is established fact that the further and faster that a radio wave travels, the more energy it needs. Because it is impossible to simultaneously achieve high speed, low power consumption and long range in radiowave, product designers and developers have instead selected specific characteristics to optimize in certain conditions while creating wireless technologies. This approach has led to the concepts of wireless area networks of different magnitudes, (ie., personal ,local metropolitan, global, etc.) Each type of wireless area network signifies a specific combination of radio characteristics that in turn translate into specific applications and usage scenarios.

WirelessArea Network	Range	Power Drain	Transmit Speed*	Example	Primary Application/ Usage Scenario
Wireless Personal Area Network (WPAN)	10 m	Low	800 Kbps	Bluetooth	Cable replacement between nearby devices
Wireless Local Area Network (WLAN)	100 m (to an access point)	Medium	11 Mbps	Wi-Fi (IEEE 802.11b)	Accessing an existing Ethernet network run on cables
Wireless Wide Area Network (WWAN)	2-3 km (to a base station)	High	14.4-56 Kbps	GSM, CDMA, GPRS, CDPD, TDMA	Voice and data communications
Wireless Metropolitan Area Network (WMAN)	30 km	Very High	1.5 Mbps	Sprint fixed wireless	Replace ISDN DSL, cable modem
Wireless Global Area Network (WGAN)	500-1500 km (to a satellite)	High	64 Kbps	Iridium GlobalStar satellite phones	Military

*Note: With overhead and other variables, actual throughput will be less.

For example, while developing applications for a wireless personal area network (WPAN), the wireless area network with the shortest range , product designers and developers need to consider what scenarios demand low power more than they do high speed or great range. Conversely, while developing uses for the wireless local area network (WLAN), product designers and developers must determine in which situations users would value moderate range and moderate speed more than they would low power consumption.

Similarly, the energy levels demanded by Wi-Fi render it impractical for small battery –powered devices like mobile phones, personal gadgets , and most PDAs. For example, typical Wi-Fi compact Flash and PC cards use 110-140 mA during idle mode and 200-300 mA during transmission, each atleast twice the amount of power required by Bluetooth cards. As a result, most manufacturers today are implementing Wi-Fi into notebook and desktop computers and serves, whose power resources are better suited for high power requirements of Wi-Fi.

SECURITY

Putting Wi-Fi Security in Perspective

Before this issue is explained in detail, the reader needs to keep in mind that Wi-Fi (IEEE 802.11) only attempts to provide security for the wireless portion of a network. It is not end-to-end security, and it was never intended to do more than prevent casual eavesdropping, which is what un-encrypted wired Local Area Networks (LANs) provide.

The user must, however, keep in mind that wireless networks cannot provide the same level of inherent security at the physical level that wired networks do. Radio waves pass through walls and can be intercepted from a distance. Even though a standard Wireless LAN (WLAN) card in a laptop may indicate a marginal or even non-existent signal, specialized equipment may be able to receive the signal from a much greater distance. More security is often required, whether the network is wired or wireless.

There are many components to effective network security, including the following:

Authentication - assurance that a packet comes from where it claims
Confidentiality - protection from disclosure to unauthorized persons
Access control - keeping unauthorized users out
Integrity - ensuring that data is error-free

Network security is generally implemented in layers, utilizing all of the above components and built around the seven-layer OSI Reference Model . Unlike the common saying "strong as the weakest link," layered network security is just the opposite. It is as strong as its strongest link. For example, end-to-end security can be achieved by a strong mechanism in the application layer only, even if link-layer security is broken or non-existent. However, that solution only provides security for that particular application. The advantage to applying security at progressively lower levels is that it becomes generally available to more applications.

Also, remember that corporate Wi-Fi usually attached to a wired LAN. So even if 802.11 link-level security was very strong, it only applies to the wireless portion of the network. Higher-level layers of security may still need to be employed, even if a firewall is utilized for the wired portion.

Wi-Fi Security Options

IEEE 802.11 contains an encryption option intended to provide confidentiality. The Wired Equivalent Privacy (WEP) option is defined in the 802.11 standard as "protecting authorized users of a Wi-Fi from casual eavesdropping." Recently, this security scheme has come under a great deal of criticism, accompanied by a number of papers which uncover weaknesses and outline how WEP can be defeated. Additionally, tools to exploit these weaknesses are now freely available over the Internet.

The Problem with WEP

WEP utilizes a *symmetric algorithm* known as a stream cipher, for encryption. A symmetric algorithm is one that relies on the concept of a single *shared key* (as opposed to a public key) that is used at one end to encrypt *plaintext* (the data) into *ciphertext* (the encrypted data), and at the other end to decrypt it - convert the ciphertext back to plaintext. Thus, the sender and the receiver share the same key, and it must be kept secret.
Stream ciphers encrypt data as it is received, as opposed to *block ciphers* that collect data in a buffer and then encrypt it a block at a time. Stream ciphers are tempting to use for applications requiring hardware implementation (i.e. wireless LAN cards), because they can be implemented very efficiently in silicon. However, care must be taken to ensure that the application is well suited for the proper implementation of a stream cipher, or for that matter, whatever encryption algorithm is being used.

Proper Use of Stream Ciphers

Stream ciphers are very simple and operate in theory by expanding the shared key into an infinite pseudo-random *key stream* which is logically combined (XORed) with the plaintext to produce ciphertext. Being a symmetric cipher, the user employs the shared key at the receiving end to regenerate the identical key stream, which is then XORed with the ciphertext to reproduce the plaintext. In practice, of course, an infinite key stream is never produced; it is only as long as the data stream being encrypted.

Once a key has been used to generate a key stream, the same key can never be reused again because it will generate the same key stream. If an attacker can obtain two different ciphertexts encrypted with the same key stream, the encryption process can be broken and the contents of the shared key determined. An important consequence of this is that if an encrypted transmission is interrupted and the encryption and decryption algorithms lose synchronization, and there is no means to resynchronize the process, then the entire message must be resent again, but with a different key.

The RC4 stream cipher has no mechanism to resynchronize the encryption process if an interruption occurs. Thus, it is not well-suited to applications where there is a possibility of a transmission being interrupted, unless provision is made to restart the session with a new key. For example, the RC4 stream cipher is successfully used to provide encryption for Secure Socket Layer (SSL) services for Internet transactions. An SSL session typically lasts a relatively short period of time and operates over a reliable channel where it is unlikely that a packet will be dropped. If it is, the session is started over, but with a different key. The new key is exchanged during a secure authentication process (using RSA public key cryptography) before the encrypted transaction is begun.

Improper Use of a Stream Cipher by WEP

The problem arises when the RC4 stream cipher is being used to encrypt data being sent over a channel, such as a wireless link, where it is highly likely that packets will be dropped. If there is no provision for key management (802.11 currently has none), then there is no way to create and exchange a new key with an authenticated user so that a packet can be resent.

The designers of WEP tried to get around this by appending a unique key. The effect is that instead of having only one 40-bit shared key available for use, there are now 2^{24} different 64-bit shared keys. The receiver only needs to know the secret shared 40-bit portion which is common to all of them. The unique 24-bit IV vector, which is transmitted unencrypted with each packet, determines which of the keys was used to encrypt a particular packet. The key stream is generated with this unique 64-bit "packet" key and the packet key and the key stream change for every packet. One of the problems with this scheme is that there are only a finite number of IVs available for use, and there is no mechanism in place for changing the shared key when all of the available unique IVs get used up. Another is that the simple process of concatenating the IV onto the shared key produces unique keys that are too similar. These fundamental weaknesses proved to be WEP's initial undoing. So… WEP is now generally considered to do no more than "discourage casual eavesdropping," which is all it was ever intended to do..

Providing Additional Security

Virtual Private Networks (VPNs)

It provide the most robust security solutions for corporate LANs and are already widely used for intranets and remote access. A VPN typically utilizes a dedicated server that provides both authentication and confidentiality. Wireless Access Points are also beginning to include VPN technologies within their devices, allowing simplified VPN deployment.A VPN works through the VPN server at the company headquarters, creating an encryption scheme for data transferred to computers outside the corporate offices.The special VPN software on the remote computer uses the same encryption scheme, enabling the data to be safely transferred back and forth with no chance of interception.

The following steps to insure that wireless networks are secure:

For home users and small offices:
- Use all of the 802.11 security options, including WEP.
- Use any other security features specific to your vendor's products.
- Change default passwords.
- Don't use the default key. Change it immediately and then repeatedly on a regular basis.

Additional steps for corporate users:
- Install the WLAN outside the firewall.
- Use a VPN with a physical authentication token such as a SmartCard or SecureID card.

SPECIAL FEATURES OF Wi-Fi

Unlike today's wired network, a Wi-Fi network requires little more than an access point(AP). Access to a Wi-Fi- network does not require an expensive connection to each user. Wi-Fi technology is also far less expensive to deploy than the limited wireless technologies of currently existing cellular servicing providers.

Access to a Wi-Fi broad band can be provided both outdoors and indoors. Whether from an outdoor café or a park bench a person can access the Internet if they are in range of a service station. Such a Wi-Fi broadband is much power full and can transmit data at a rate of 11Mbps which is sufficient for all types of multimedia.Many schools and businesses have unsuitable building layouts or walls that cannot be wired for various reasons making it difficult or impossible to build a wired network. Wi-Fi is a very cost effective alternative in these environments.A Wi-Fi network can provide many benefits for the society. It can provide local hospitals.

Though the radio waves are of relatively high frequency, they are not powerful enough to pass through multiple layers of building materials. Specifically radio waves are completely blocked by steel. For this reasons the factors deciding performance are proximity to access point and the degree to which the signal is blocked by the surroundings.As more computers begin to communicate with the same access point ,a bottleneck occurs. An access point has a finite amount of network bandwidth to which it is physically linked. As a result, all computers that are associated with a specific access point must share the same bandwidth.

More computers mean the possibility for a slower network connection. Since Wi-Fi technology is constantly improving these shortcomings will get removed soon.

CONCLUSIONS

Wireless and sensorless sensing seeks breakthroughs in the contradiction between the limitation of WiFi and the growing demand for environment perception in daily life, seeks a balance between low cost and high accuracy, explores solutions via frequency diversity and spatial diversity, and creates applications that are previously infeasible in wireless communications and mobile computing.We envision technological advances would boost the capability of wireless sensing to finer granularity and higher sensitivity, which will in turn foster various new applications. This article only serves as an introduction on the concept of wireless and sensorless sensing.

we refer interested readers to the corresponding references for in-depth information. If we considerWiFi as a side sensor, thenWiFi-based sensorless sensing can be regarded as one of the world's largest wireless sensor networks, spreading over office buildings, shopping malls, other public places and homes, and silently watching the activities of humans therein. Living inside such a network, every individual in the physical world has been bestowed with unique being in the digital world. So the next time you want a secret meeting, after shutting the doors, pulling down

the curtains, and even checking for wiretaps beneath the table, do not forget to turn off the WiFi!

REFERENCES

[1] T. Ralston, G. Charvat, and J. Peabody, Real-time Through-wall Imaging using an Ultrawideband Multiple Input Multiple-Output (MIMO) phased array radar system, in Proc. of 4th IEEE Int. Symposium on Phased Array Systems and Technology, Boston, USA, 2010, pp. 551–558.

[2] M. Youssef, M. Mah, and A. Agrawala, Challenges: Device-free passive localization for wireless environments, in Proc. of 13th ACM Annual Int. Conf. on Mobile Computing and Networking, Montreal, Canada, 2007, pp. 222–229.

[3] J.Wilson and N. Patwari, Radio tomographic imaging with wireless networks, IEEE Trans. Mobile Comput., vol. 9, no. 5, pp. 621–632, 2010.

[4] Z. Zhou, Z. Yang, C. Wu, L. Shangguan, and Y. Liu, Towards omnidirectional passive human detection, in Proc. of 32nd IEEE Int. Conf. on Computer Communications, Turin, Italy, 2013, pp. 3057–3065.

[5] W. Xi, J. Zhao, X.-Y. Li, K. Zhao, S. Tang, X. Liu, and Z. Jiang, Electronic frog eye: Counting crowd using WiFi, in Proc. of 33rd IEEE Int. Conf. on Computer Communications, Toronto, Canada, 2014, pp. 361–369.

[6] Q. Pu, S. Gupta, S. Gollakota, and S. Patel, Whole-home gesture recognition using wireless signals, in Proc. Of 19th ACM Annual Int. Conf. on Mobile Computing and Networking, Miami, USA, 2013, pp. 27–38.

[7] Y. Wang, J. Liu, Y. Chen, M. Gruteser, J. Yang, and H. Liu, E-eyes: Device-free location-oriented activity identification using fine-grained WiFi, in Proc. of 20th ACM Annual Int. Conf. on Mobile Computing and Networking, Maui, USA, 2014, pp. 617–628.

[8] G. Wang, Y. Zou, Z. Zhou, K. Wu, and L. M. Ni, We can hear you with Wi-Fi! in Proc. of 20th ACM Annual Int. Conf. on Mobile Computing and Networking, Maui, USA, 2014, pp. 593–604.

[9] P. Melgarejo, X. Zhang, P. Ramanathan, and D. Chu, Leveraging directional antenna capabilities for finegrained gesture recognition, in Proc. of 2014 ACM Int. Joint Conf. on Pervasive and Ubiquitous Computing, Seattle, USA, 2014, pp. 541–551.

[10] X. Liu, J. Cao, S. Tang, and J.Wen, Wi-Sleep: Contactless sleep monitoring via WiFi signals, in Proc. of 35th IEEE Real-Time Systems Symposium, Rome, Italy, 2014.

AUTHORS

Prashant.M received B.E degree in computer science and engineering from Anna University, Tamil Nadu, and India in 2015 respectively. Currently he is doing the full time internship Trainee in Polaris India Pvt. Ltd. He has published one international journal.
His research interests focus on the area of Network Security analytics, dynamic adaptation of MapReduce computations, data mining.

Ramesh Krishnan received Bachelor of Engineering and Master of Engineering degrees from Anna University, India in 2007 and 2010 respectively. Currently he is pursuing the full time Ph.D Degree at Anna University. He has published papers in four international journals and three international conferences. His research interests focus on the area of low-power, high-performance VLSI architectures and circuit design for digital communications and digital signal processing.