DATE OF EXPERIMENT : 13/03/2020
DATE OF SUBMISSION:03/04/2020

WIRELESS NETWORKS
EXPERIMENT 6

Aim : To compare different IEEE 802.11 standards and observe their performance metric in EXata simulations

Intro to wireless standards:
The wireless networking equipment available supports varying levels of industry communication standards. At present, the IEEE 802.11b/g standard is widely accepted throughout the industry and provides the necessary balance of range, network throughput, and support for device mobility to effectively serve most needs of the University community. As newer standards emerge, such as IEEE 802.11 enhancements they will be evaluated and deployed should they offer security and throughput improvements over 802.11b/g.

It is the University's goal to offer the most advanced technology available while ensuring that the University Community benefits from stable and reliable service. Pitt IT will continue to evaluate available wireless network industry standards and equipment to ensure that the University meets this goal.

Wireless Access Point

A wireless communications hardware device that creates a central point of wireless connectivity. A wireless access point behaves much like a "hub" in that the total bandwidth is shared among all users for which the device is maintaining an active network connection.

Wireless Port

A network port that has been installed to connect a wireless access point to the University's wired network. Wireless ports provide both data and power service to the wireless access point and are clearly distinguished from ordinary network ports by an affixed yellow warning label. Because wireless ports carry both data and electrical power, ordinary end-user devices could be severely damaged if they are connected to this type of port.

Wireless client software or built in 802.1x supplicant

Pitt IT provides client software client that allows a computer to utilize 802.1x authentication to the wired and wireless networks. Some operating systems have built-in support for 802.1x and can be used for accessing the University's networks. The University-provided client software will be preconfigured to support the specific setup for PittNet Wi-Fi.

Coverage Area

The geographical area in which acceptable wireless service quality is attainable. Coverage areas for similar devices can vary significantly due to the presence of building materials, interference, obstructions, and access point placement.

Interference

Degradation of a wireless communication radio signal caused by electromagnetic radiation from another source including other wireless access points, cellular telephones, microwave ovens, medical and research equipment, and other devices that generate radio signals. Interference can either degrade a wireless transmission or completely eliminate it entirely depending on the strength of the signal generated by the offending device.

Privacy

The condition that is achieved by successfully maintaining the confidentiality of personal, student, employee, and/or patient information transmitted over a wireless network.

Security

Security is particularly important in wireless networks because data is transmitted using radio signals that, without implementation of specific data encryption mechanisms, can easily be intercepted.

Wireless Network Infrastructure

The collection of all wireless access points, antennas, network cabling, power, ports, hardware, and software associated with the deployment of a wireless communication network.

Wired Equivalent Privacy (WEP)

A security protocol for wireless networks defined within the 802.11b standard. WEP is designed to provide the same level of security as that of a wired network. Recent reports indicate that the use of WEP alone is insufficient to ensure privacy unless used in conjunction with other mechanisms for data encryption.

WPA

Short for Wi-Fi Protected Access, a Wi-Fi standard that was designed to improve upon the security features of WEP. This technology features improved data encryption through the temporal key integrity protocol (TKIP) and user authentication through the extensible authentication protocol (EAP), PEAP – MSChapV2. PittNet Wi-Fi utilizes the WPA protocol.

Types of wireless standards:

802.15

802.15 is a communications specification that was approved in early 2002 by the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) for wireless personal area networks (WPANs). The initial version, 802.15.1, was adapted from the Bluetooth specification and is fully compatible with Bluetooth 1.1.

Bluetooth is a well-known and widely used specification that defines parameters for wireless communications among portable digital devices including notebook computers, peripherals, cellular telephones, beepers, and consumer electronic devices. The specification also allows for connection to the Internet.

The IEEE 802.15 Working Group proposes two general categories of 802.15, called TG4 (low rate) and TG3 (high rate). The TG4 version provides data speeds of 20 Kbps or 250 Kbps. Additional features include the use of up to 254 network devices, dynamic device addressing, support for devices in which latency is critical, full handshaking, security provisions, and power management.

802.16

Commonly referred to as *WiMAX* or less commonly as *WirelessMAN* or the *Air Interface Standard*, IEEE 802.16 is a specification for fixed broadband wireless metropolitan access networks (MANs) that use a point-to-multipoint architecture. Published on April 8, 2002, the standard defines the use of bandwidth between the licensed 10GHz and 66GHz and between the 2GHZ and 11GHz (licensed and unlicensed) frequency ranges and defines a MAC layer that supports multiple physical layer specifications customized for the frequency band of use and their associated regulations. 802.16 supports very high bit rates in both uploading to and downloading from a base station up to a distance of 30 miles to handle such services as VoIP, IP connectivity and TDM voice and data.

802.11

In 1997, the Institute of Electrical and Electronics Engineers created the first WLAN standard. They called it *802.11* after the name of the group formed to oversee its development. Unfortunately, 802.11 only supported a maximum network bandwidth of 2 Mbps — too slow for most applications. For this reason, ordinary 802.11 wireless products are no longer manufactured. However, an entire family has sprung up from this initial standard.

The best way to look at these standards is to consider 802.11 as the foundation, and all other iterations as building blocks upon that foundation that focus on improving both small and large aspects of the technology. Some building blocks are minor touch-ups while others are quite large.

The largest changes to wireless standards come when the standards are "rolled up" to include most or all small updates. So, for example, the most recent rollup occurred in December 2016 with 802.11-2016. Since then, however, minor updates are still occurring and, eventually, another large roll-up will encompass them.

Below is a brief look at the most recently approved iterations, outlined from newest to oldest. Other iterations — 802.11ax, 802.11ay, and 802.11az — are still in the approval process.

Types of 802.11x wireless standards:

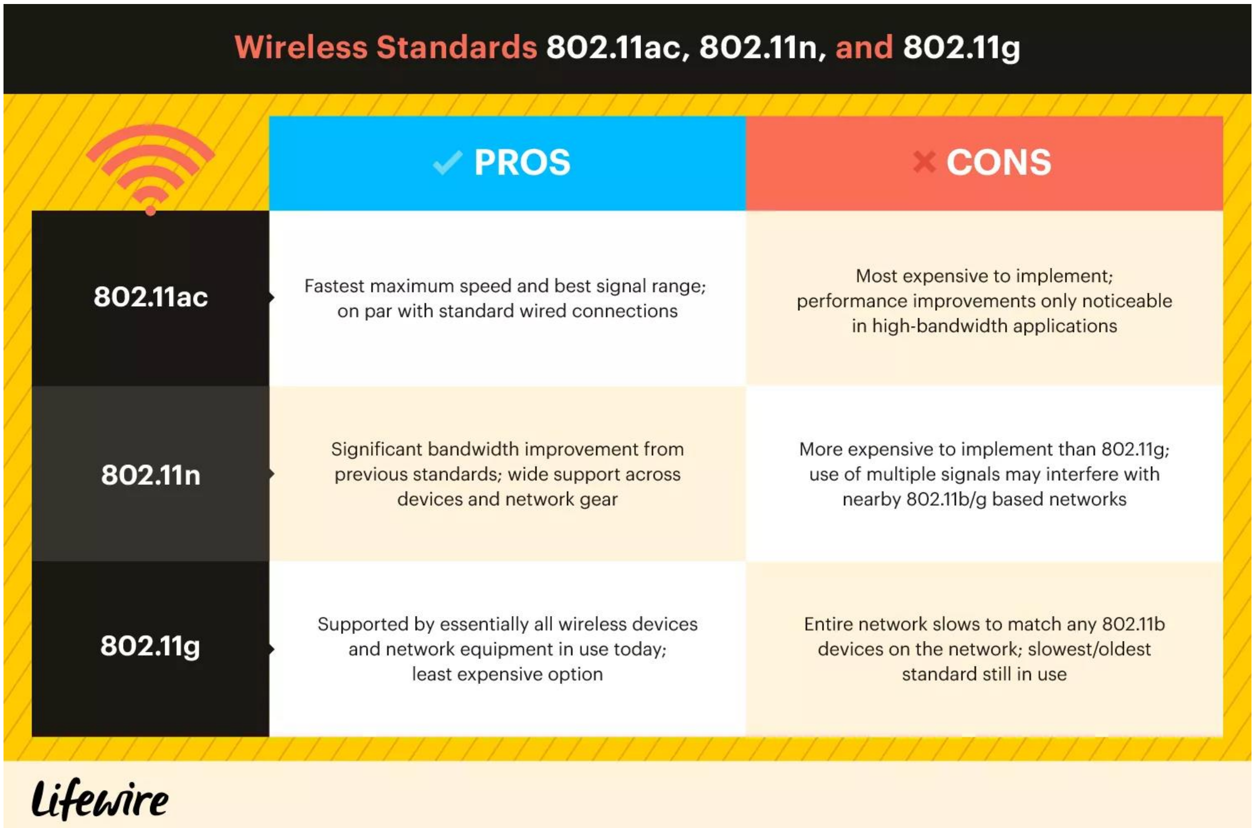

Figure: comparison of wireless standards

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Year Released	1999	1999	2003	2009	2014	2019
Frequency	5Ghz	2.4GHz	2.4GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz
Maximum Data Rate	54Mbps	11Mbps	54Mbps	600Mbps	1.3Gbps	10-12Gbps

Figure. Types of 802.11x standards

802.11aj

Known as the China Millimeter Wave, this standard applies in China and is basically a rebranding of 802.11ad for use in certain areas of the world. The goal is to maintain backward compatibility with 802.11ad.

802.11ah

Approved in May 2017, this standard targets lower energy consumption and creates extended-range Wi-Fi networks that can go beyond the reach of a typical 2.4 GHz or 5 GHz networks. It is expected to compete with Bluetooth given its lower power needs.

802.11ad

Approved in December 2012, this standard is freakishly fast. However, the client device must be located within 11 feet of the access point.

802.11ac

The generation of Wi-Fi that first signaled popular use, 802.11ac uses dual-band wireless technology, supporting simultaneous connections on both the 2.4 GHz and 5 GHz Wi-Fi bands. 802.11ac offers backward compatibility to 802.11b/g/n and bandwidth rated up to 1300 Mbps on the 5 GHz band plus up to 450 Mbps on 2.4 GHz. Most home wireless routers are compliant with this standard.

Pros of 802.11ac: Fastest maximum speed and best signal range; on par with standard wired connections

Cons of 802.11ac: Most expensive to implement; performance improvements only noticeable in high-bandwidth applications

802.11ac is also referred to as *Wi-Fi 5*.

802.11n

802.11n (also sometimes known as Wireless N) was designed to improve on 802.11g in the amount of bandwidth it supports, by using several wireless signals and antennas (called *MIMO* technology) instead of one. Industry standards groups ratified 802.11n in 2009 with specifications providing for up to 300 Mbps of network bandwidth. 802.11n also offers a somewhat better range over earlier Wi-Fi standards due to its increased signal intensity, and it is backward-compatible with 802.11b/g gear.

Pros of 802.11n: Significant bandwidth improvement from previous standards; wide support across devices and network gear

Cons of 802.11n: More expensive to implement than 802.11g; use of multiple signals may interfere with nearby 802.11b/g based networks

802.11n is also referred to as *Wi-Fi 4*.

802.11g

In 2002 and 2003, WLAN products supporting a newer standard called *802.11g* emerged on the market. 802.11g attempts to combine the best of both 802.11a and 802.11b. 802.11g supports bandwidth up to 54 Mbps, and it uses the 2.4 GHz frequency for greater range. 802.11g is backward compatible with 802.11b, meaning that 802.11g access points will work with 802.11b wireless network adapters and vice versa.

Pros of 802.11g: Supported by essentially all wireless devices and network equipment in use today; least expensive option

Cons of 802.11g: Entire network slows to match any 802.11b devices on the network; slowest/oldest standard still in use

802.11g is also referred to as *Wi-Fi 3*.

802.11a

While 802.11b was in development, IEEE created a second extension to the original 802.11 standard called *802.11a*. Because 802.11b gained in popularity much faster than did 802.11a, some folks believe that 802.11a was created after 802.11b. In fact, 802.11a was created at the same time. Due to its higher cost, 802.11a is usually found on business networks whereas 802.11b better serves the home market.

802.11a supports bandwidth up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz. This higher frequency compared to 802.11b shortens the range of 802.11a networks. The higher frequency also means 802.11a signals have more difficulty penetrating walls and other obstructions.

Because 802.11a and 802.11b use different frequencies, the two technologies are incompatible with each other. Some vendors offer hybrid *802.11a/b* network gear, but these products merely implement the two standards side by side (each connected device must use one or the other).

802.11a is also referred to as *Wi-Fi 2*.

802.11b

IEEE expanded on the original 802.11 standard in July 1999, creating the *802.11b* specification. 802.11b supports a theoretical speed up to 11 Mbps. A more realistic bandwidth of 5.9 Mbps (TCP) and 7.1 Mbps (UDP) should be expected.

802.11b uses the same *unregulated* radio signaling frequency (2.4 GHz) as the original 802.11 standard. Vendors often prefer using these frequencies to lower their production costs. Being unregulated, 802.11b gear can incur interference from microwave ovens, cordless phones, and other appliances using the same 2.4 GHz range. However, by installing 802.11b gear a reasonable distance from other appliances, interference can easily be avoided.

802.11b is also referred to as *Wi-Fi 1*.

Implementation:

1. Create a topology with 10 nodes.
2. Connect source and destination using CBR.

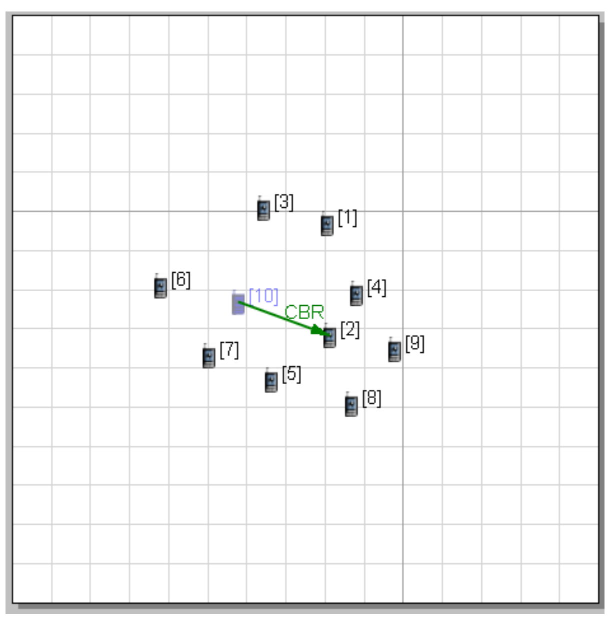

Figure: A topology with 10 nodes

3. Set the node mobility to random way point.
4. Go to the Physical layer by clicking on interface, set the radio type as 802.16.

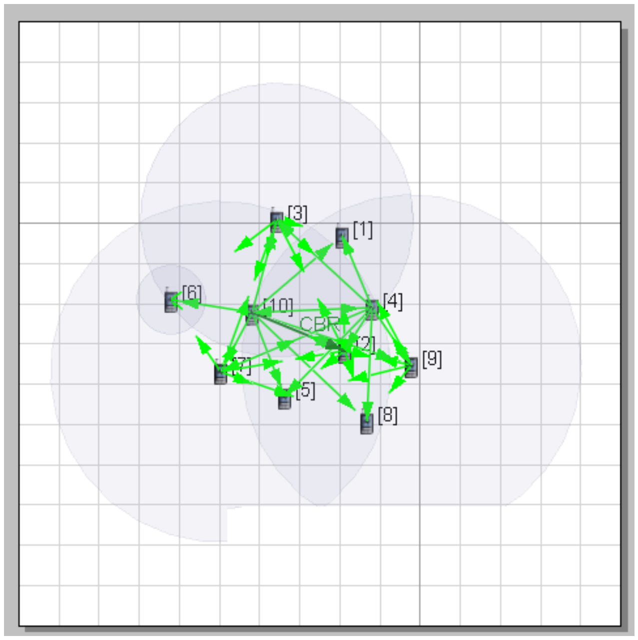

Figure: The simulation running

5. Run the simulation.
6. Now click on the analyzer to get the resultant graphs.
7. Now get the graphs for the various parameters like the packet delivery ratio,end-to end delay,average jitter and throughput.
8. Import the results into a text document and analyze them.

Now, repeat the procedure by changing the radio type to

a) 802.16
b) 802.11

Interpret and compare the results for the same.

Conclusion: Multi-hop topology for wireless sensor network has been built and studied.