Wireless technology essay

Business, E-Commerce

It’s a beautiful day in the park, and you are enjoying the sunshine and the company of your friends.

Then you remember. You have to do research for your science project. Hey, no problem. Your laptop is right next to you. There in the grass, you are searching the internet for ideas as birds chirp in the background. Wireless technology puts information at your fingertips from practically anywhere in the world.

It allows you to connect with friends, family, and others with ease-even if there isn’t a telephone line for miles around. Wireless technology set you free, so you can create a workspace or fun space from practically anywhere. Modern technology has given us easy, convenient ways to transfer information, communicate and entertain ourselves. With wireless technology, we can do all these things on devices that work without wires or cables. Wireless technology includes cell phones, wireless internet connections, and handheld devices such as PDAs, Medical devices such as cardiac pacemakers rely on wireless technology to correct heard rhythms.

A global positioning system (GPS) uses satellites and wireless technology to help people know where on earth they are and how to get where they’re going. Not long ago, if you wanted privacy for a phone call, you needed a long cord to pull the phone into another room. If you wanted to surf the internet, you had to do it in your home, your office, or on a public computer at the library. Not too long ago you had to stand up and turn a knob on the TV to change the channel. That’s all changed.

In the modern times, you can chat with your friends on a wireless Bluetooth handset, send emails on your Blackberry, and download new songs to your Ipod and you can do it all without leaving that sunny spot in the park. What is wireless technology? Wireless technology lets you send and receive information without using wires. It can be said to include simpler, older devices like car radios and baby monitors – even garage door openers and TV remotes. But when we talk about wireless technology, we mean electronic devices that are linked, or networked, together. These devices can send and receive large amounts of information over radio waves. Radio Waves Radio waves are energy waves that move through space at a certain frequency or wavelength.

Other kinds of waves travel the same way. These include microwaves, visible light, and X-rays. Different kinds of waves travel at different frequencies. A wave’s frequency is how often it goes up and down in one second. Nearly any information can be transmitted wirelessly, including sounds, text, images and video. To do this you need three basic parts. 1.

a transmitter 2. a receiver 3. a carrier wave the transmitter and receiver are electronic devices. They use wires and hardware to function.

The carrier wave begins as a continuous wave pattern. But to carry information, it has to be modulated or changed. For example, the sounds in a telephone conversation produce movements called vibrations. These are combined in the transmitter with a constant radio wave, or carrier wave. When they’re combined, the radio wave has been modulated. The two

signals travel together through the air. Modulation changes information on the wave into codes a receiver can understand.

Wi-fi routers, antennas, and cell phone towers are transmitters. They modulate sounds and images over radio waves. Computers, cell phones and other devices are the receivers. History of wireless communication. Electromagnetic waves were first described by a physicist named James Clerk Maxwell. He published a paper in 1864 explaining how light waves and radio waves move through space.

At the time, people could communicate by electrical telegraph. Telegraphs send messages over wires, using Morse code. A practical telephone wasn’t invented until 1876. Maxwell’s theory was proven by physicist Heinrich Hertz.

In the 1880s, hertz did experiments with a simple transmitter and receiver set apart from each other. When the transmitter produced a spark, the receiver responded with a smaller spark. This experiment showed that electrical energy had traveled across the room wirelessly. Remarkable innovation has been occurring in the wireless category of net centric technologies, facilitated by that hourglass architecture that puts few restrictions on the actual means of transmission. If we can use telephone wires, coaxial cable, or fiber to transmit information using TCP/IP, then why not electromagnetic waves? Despite the obvious disadvantage of tiny screen size, some analysts predict that the cell phone will become the most prevalent means of accessing the internet, outstripping the microcomputer in a short time. In some ways, the mobile internet access market be in the

same phase that land-line internet access was in, in 1995, poised on the brink of an explosive growth phase. The internet enabled cell phone may also be in a position similar to the telephone, which was initially conceived as a “ speaking telegraph”.

Although PCs abound in industrialized countries, they are far less common in many parts of the world, and certainly more difficult to use and expensive to buy compared to a phone. The cell phone with internet capabilities may be a means to distribute internet access far wider than has been possible in the past. The kind of optimism may have prompted the billions spent by network operators around the world to obtain licenses to run third-generation (3G) wireless networks, which involves advantage technology that supports much greater data speeds than the current wireless networks do.

Wireless technologies are in a very fragmented state now, with many types of devices on the market using a variety of connection strategies, often incompatible with one another. They can be grouped into three general categories, based largely on the distance the signal needs to travel: personal area, local area and wide area. In the wireless personal area network arena, a key goal is to develop ways for devices to synchronize and interact with one another without short run cables. A technology called Bluetooth is an important ingredient here, and many predicts that it will replace a good portion of the cabling infrastructure that clutters office desks, connecting computers to printers, personal digital assistants, and cell phones. For local area networks, wireless technologies offer another set of attractions, especially for laptop users. Wireless access points can be placed in various

locations of a building, and those with laptops and wireless LAN cards can log in to the network from any nearby location. This is becoming very popular for public spaces that would be difficult to configure with data jacks, such as large conference rooms, libraries, airports, and outdoor patios or garden. Office workers can take their laptops to the balcony and enjoy some sunshine as they continue to access the network.

Wireless LANs are also becoming popular in homes, particularly for people who have a high-speed internet connection and more than one computer, but don’t want to punch holes in their walls for the wiring. Wire area wireless networks offer many different opportunities for the workplace, including the internet-enabled cell phones and personal digital assistants. Retrieving your email from your PDA while waiting in the line at the airport is not difficult with these devices. The speed of connection is typically slow, but these devices work well for simple text. The “ last mile” has been an obstacle to the delivery of high-speed internet access, especially to remote areas. Wireless wide area networks offer opportunities here as well. It is very expensive to deploy new wiring to every office or residence, but constructing towers with transmitters that can service wider areas is more feasible. Satellites can also be used to serve large geographical areas.

In Alaska, for example, satellites are being used to provide Internet connectivity to libraries, schools, and municipalities in remote areas of the state. Wireless systems have been especially vulnerable to intrusion, and they illustrate the tense balance between the desire for openness and the concern for security. For example, employees give rave reviews to the

development of the wireless network in which they can use their laptops any place near a corporate access point. Corporations have happily set those points up in cafeterias, in the outside gardens, in the auditoriums, and in the conference rooms to workers from their desktops and make it easy for people and teams to log in to the network from anyplace on the corporate campus.

Yet securing those networks is extraordinarily difficult, and people out in the parking lot or on the street can also access the network with their own laptops. Also “ rogue access points” have been hung without the knowledge of the corporation, thus adding unauthorized “ doors” into the network. Security threats are so common that is easy enough to launch a hoax that frightens people into harming their own computers, under the guise of helping them remove a threat. One such hoax, sent to addresses in the victim’s address book, warned that a virus has been infecting all of them and gave precise instructions on how to remove it. There was no virus, but the file that would be removed if the victim followed the instructions was critical to the computer’s operating systems. Standards As implied earlier, wireless technology are currently being deployed for personal, home, local and wide area networks. Standardization is important in order to support interoperability and reduce costs.

Now we look at key WLAN, WPAN, WWAN standards. IEEE 802. 11 specifications are focused on the physical layer (PHY) and medium access control (MAC) sublayer of WLANs. The MAC is consistent with the IEEE 802. 3 Ethernet standard.. The IEEEE standard developed by working group 802.

11 was accepted by the IEEE board in 1997 and became IEEE standard 802. 11-1997. the standard defines three different WLAN physical implementation (signaling techniques and modulations), MAC function, and a management function. All of the implementations support data rates of 1 Mbps and optionally, 2Mbps.

Security, roaming, and QoS are also considered, although major improvements to the security apparatus have been shown to be necessary. The three physical implementations are as follows: 1. Direct sequence spread spectrum radio (DSSS) in the 2. Ghz – the most commonly deployed technology 2. Frequency hopping spread spectrum radio (FHSS) in the 2.

4Ghz band 3. Infrared light (IR) GPRS is a packet switched wireless data network operations in the GSM environment that enables data to be sent and received using GPRS devices in a more cost efficient and quicker way than was possible over the GSM cellular system. users can secure data download rates up to 53. 6 kbps over GPRS compared to 14.

4 Kbps via circuit – switched data over GSM. GPRS is a 2. 5G wireless technology standard that was expected to improve the data services that can be added to GSM.

ETSI defined GPRS in 1997 with the goal of providing packet-mode data services in GSM. GPRS is an over the air system for transmitting data on GSM networks that converts data into standard IP packets, enabling interoperability between the Internet and GSM network. In GPRS a single time slot may be shared by multiple users to transfer packet data. GPRS

wireless technology employs authentication and encryption via standard GSM algorithms. One of the key gain from 802. 11 standard is the ability for products from different vendors to interoperate with each other.

This was not the case with WLAN products available throughout the 1990s. his means that as a user, one can purchase a wireless LAN card from one vendor and a wireless LAN card from another vendor and they can communicate with each other, independent of the brand of access point utilized. This gives the user the choice to choose the system that best meets the needs for each application. As a supplement to the 11-Mbps interoperability testing that will be performed through WECA, a number of vendors have successfully tested interoperability together at the University of New Hampshire Interoperability.

Security Considerations for WLANs. IEEE 802. 1 provides for security via two mechanisms: authentication and encryption. Authentication is the process by which one station is verified to have authorization to communicate with other stations or APs in a given coverage area.

In the infrastructure mode, authentication is established between an AP and each station. Authentication can be either open system or shared key. In the open system, any STA may request authentication. The STA receiving the request may grant authentication to any request or only to those from stations on a user-defined list.

In a shared key system, only stations that posse a secret encrypted key can be authenticated. Shared key authentication is available only to systems

having the optional encryption capability. Encryption is intended to provide a level of security comparable to that of a wired LAN. Without question, a variety of extremely positive services have been made available to users around the globe with the development and rapid growth of the internet over the last decade. These very useful functions range from communications services, such as instant messaging and telephony, to rapid, real time online transactions, such as e-commerce, internet banking, online gaming, political activism, and online voting. Also, within the past few years, physicians have been able to access over the internet and through handheld wireless devices patients' health histories and diagnostic records without having to rely on time delaying courier services. Not only have young billionaires have made with the creative development of " Google-like" search engines, but in addition, government around the globe have made use of the internet to collect homeland security intelligence as a means of keeping their citizens safe.