An Assessment of Wireless LAN Intended For System Monitoring

Dr. Shailendra Singh Sikarwar[1] Mahesh Bansal[2]

[1]Assistant Professor, P. G. V. College, Gwalior

[2]Assistant Professor, P. G. V. College, Gwalior

Abstract – 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 and indispensable 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 deployment of Wireless LAN increases well around the globe, it is increasingly important for us to understand different technologies and to select the most appropriate one.

This paper provides a detailed study of the available wireless LAN technologies and the concerned issues ,will give a brief description of what wireless LANs are ,the need of Wireless LAN ,History of wireless LAN , advantages of Wireless Networks ,with summarizing the related work on WLAN in academic area , Wireless LAN technologies , some risks attacks against wireless technologies , suggesting some recommendations to protect wireless LAN network from attack , Finally we propose some research issues should be focused on in the future.

----------♦----------

INTRODUCTION

Computer technology has rapidly growth over the past decade, Much of this can be attributed to the internet as many computers now have a need to be networked together to establish an online connection. As the technology continues to move from wired to wireless, the wireless LAN (local area network) has become one of the most popular networking environments.

Wireless local area network (LAN) technology are widely deployed and used in organisations today. A wireless LAN is a flexible data communications system implemented as an extension to, or as an alternative for, a wired network. Using radio frequency (RF) technology, wireless LANs transmit and receive data over the air, minimising the need for wired connections. Thus, wireless LANs combine data connectivity with user mobility.

Today wireless LANs are becoming more widely recognized as a general-purpose connectivity alternative for many organisations and home users. Wireless LAN users can access shared information without looking for a place to plug in, and network administrators can set up networks without installing physical cables. However, organisations should be aware of threats in wireless LANs, and learn how to manage information security risks in wireless LANs effectively.

Using the characteristics of a wireless network, these issues might be determined. In this postulation, a WLAN will be utilized for a device checking provision. The perpetual plausible outcomes of wireless advances should be utilized to screen the variables included in printers, fax machines, scanners, and different devices. Using a WLAN, a device might be surveyed for information without meddling with the network spine, the device does not must be fastened to a solitary area and it could be gained entrance to in a remote area that can't be associated with a wired network.

Wireless innovation permits the capacity of making a network that works independently from the client's underlying wired network -the device checking requisition might be produced to utilize its own particular divide network. A comparative technique for wireless wide area

networking for device checking seems to be produced in parallel with the advancement of this local area networking result . The point when these two techniques are mixed together, the device checking requisition will be equipped for checking devices from a remote area, i.e. from the company database server.

This postulation offers an extensive variety of commitments to the wireless conveyances investigate field. It started with a complete survey of the regular WLAN protocols. From this research, an extensive examination of these protocols was performed with a decision of which order fits into the DCS technique the "best". When this methodology has been chosen equipment building design was produced to bring about the methodology into the DCS technique, with programming advanced to work on top of the devise that runs the WLAN methodology. This advancement leaves the supporting organization with a complete answer for changing over the DCS technique from a wired technique to a wireless system. At last, the proposition introduces fittings structural engineering for incorporation of this WLAN result with the wireless wide area networking answer for the formation of a completely wireless device checking solution.

WIRELESS TECHNOLOGY : AN OVERVIEW

Wireless LANs are everywhere – at the office, at home, in the hotel, in the coffee shop or at the airport. The wireless concept that we take for granted now has its roots in the wireless modem of the early 90's. Early wireless modems were designed for single peripheral devices that needed a way to allow devices to send and receive computer data. The modem speeds that we had grown accustomed to were more than adequate for the task.

Industry professionals drawn to this new emerging field are typically from the Information Systems Networking field with a strong background in the concepts of wired LAN, MAN and WAN or from the Radio Telecommunications field with an in-depth experience in wireless communication. This Wireless LAN field requires some degree of expertise in both. The hardware is typically added to an existing system as an extension of the Access Layer requirements of the network and managing the Air Interface requires another set of skills entirely. One of the best things about WLANs is that they operate in a license-free band allowing the market to develop products and technologies through open competition. One of the drawbacks with WLANs is that they operate in unlicensed bands, which results in increasing radio interference from other devices such as cordless phones. Industry Canada determines the frequency bands that WLANs operate in and the Institute of Electrical and Electronics Engineers (IEEE) develops the standards that describe how the technology will work in that spectrum.

Wireless local area networks (LAN) are groups of wireless networking nodes within a limited geographic area, such as an office building or building campus, that are capable of radio communication.

Wireless LANs are usually implemented as extensions to existing wired local area networks to provide enhanced user mobility and network access. This enables organisations to offer its employees the mobility to move around within a broad coverage area and still be connected to the network. The most widely implemented wireless LAN technologies are based on the IEEE 802.11 standard and its amendments. The original 802.11 standard was published in June 1997 as IEEE Std. 802.11-1997, and it is often referred to as 802.11 Prime because it was the first WLAN standard. The standard was revised in 1999, reaffirmed in 2003, and published as IEEE Std. 802.11-1999 (R2003).

To know WLAN we need first to know the definition of LAN, which is simply a way of connecting computers together within a single organization, and usually in a single site (Franklin, 2010). According to Cisco report in 2000 wireless local-area network (WLAN) does exactly what the name implies: it provides all the features and benefits of traditional LAN technologies such as Ethernet and Token Ring without the limitations of wires or cables. Obviously, from the definition the WLAN is the same as LAN but without wires.

Clark et al, (1978) defined WLAN as a data communication network, typically a packet communication network, limited in geographic scope.' A local area network generally provides high-bandwidth communication over inexpensive transmission media.

While (Flickenger, 2005) see it as a group of wireless access points and associated infrastructure within a limited geographic area, such as an office building or building campus, that is capable of radio communications. Wireless LANs are usually implemented as extensions of existing wired LANs to provide enhanced user mobility. Wireless Local Area Network (WLAN) links two or more devices using a wireless communication method. It usually provides a connection through an Access Point (AP) to the wider internet (Putman, 2005). This gives users the ability to move around within a local coverage area while still be connected to the network. Just as the mobile phone frees people to make a phone call from anywhere in their home, a WLAN permits people to use their computers anywhere in the network area.

In WLAN Connectivity no longer implies attachment. Local areas are measured not in feet or meters, but miles or kilometers. An infrastructure need not be buried in the ground or hidden behind the walls, so we can move and change it at the speed of the organization.

WIRELESS COMPONENTS OF CONCERN

The WLAN is made by utilizing an existing wireless order that has recently been produced to make the configuration and usage of the result proficient and convenient. A choice was be made between 802.11, 802.11a, 802.11b, 802.11g, Bluetooth, Homerf, and Ultrawideband. The decision between these protocols was made dependent upon their capacities to handle the numerous criteria required for the device checking system. The criteria for this system incorporate network topology, limit, range, information rates, adaptability, power, require, unwavering quality, security, and accessibility. A case of the network topology is indicated in Figure.

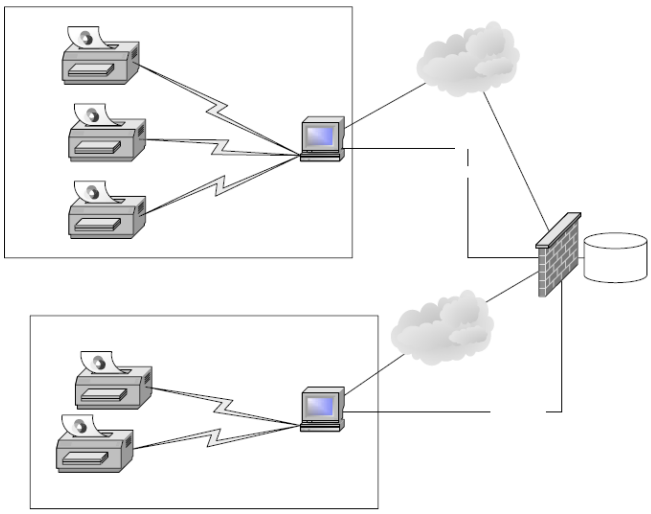

Figure : Proposed Device checking Application

Figure shows two Lans at a site where there are five devices to be supervised. The device administrations requisition depicted in this proposal is just concerned with effectively making a set of local area networks that can unite all devices to a local area network host. A major concern of the WLAN system is the amount of Wlans sent at a

area. It is craved that the amount of Wlans at an area is minimize to lessen unpredictability in the association of the WLAN to the WAN system. This will lessen the expense of the system since the WAN system has the potential for a high expense. Minimizing the number of Wlans is straight identified with the limit and transmission extend of the order.

The information being exchanged on the network is required to be low so the limit won't have an in number influence in the beginning device checking provision. Then again, the reach is of extraordinary concern since the devices at an area are required to be divided by substantial separations. This implies that the bigger the extent of the picked methodology, the more devices it will be capable to handle with a solitary WLAN host. Likewise, the limit of the system is affected by the information rates of the methodology. The information rates are not a preeminent concern at first given that wanted information on the network are low and speed is of negligible concern.

MANAGEMENT CONTROLS

Management controls are very much required to ensure that a secure wireless LAN is implemented in organisations. To ensure this, roles and responsibilities for wireless LAN planning and implementation are to be clearly defined. Security policies and procedures related to wireless LANs need to be developed and endorsed. Senior management has to ensure that risk assessment on wireless LANs and wireless network assessments are conducted periodically and in accordance to organizational policies and procedures, as well as other security requirements.

ROLES AND RESPONSIBILITIES - Security is not a task; it is a continuous process that every employee in organisations should understand and undertake in their job functions. To ensure adequate security in wireless LANs, senior management should play significant roles in network security especially related to wireless networks. The following tasks should be used as guidance in identifying the roles and responsibilities in ensuring wireless LAN security:

1. Senior management should provide support for planning and implementing security for wireless LANs through clear direction and demonstrated commitment.

2. Senior management should ensure risk assessment is performed before implementing wireless LANs.

3. The Human Resources (HR) department (together with senior management) should engage a dedicated employee (e.g. CISO) who is independent of the Information Technology (IT) department to oversee the organisation's

information security, especially wireless network security.

4. The HR and IT departments (together with senior management) should define roles and responsibilities of each employee allowed to use wireless devices, network, and facilities, in an employee's terms and conditions.

5. All employees should be aware of technical and security implications of wireless and handheld device technologies by attending training and awareness sessions held by organisations.

POLICIES AND PROCEDURES - Security policies and procedures related to wireless LANs should be developed, documented, approved and maintained based on security requirements, best practices and agreed fundamental guidelines set forth by organisations. A policy is typically a document that outlines overall intention and direction as formally expressed by management. Comprehensive wireless security policies and procedures for organisations, and compliance therewith, is the minimum requirement needed in organizations to plan and implement wireless LANs. Its main purpose is to inform employees on what is deemed as allowable and what is not with regards to wireless LANs.

The IT department should develop policies and procedures related to wireless LAN security; and ensure they are approved and endorsed by senior management. The endorsed policies and procedures should be communicated accordingly to all employees. In addition, these policies

and procedures should be reviewed periodically to ensure its effectiveness and suitability. The following statements should be included in a wireless LAN's security policy (Note: this is not an exhaustive list):

1. Identify who may use wireless LAN technology in the organization.

2. Identify whether Internet access is required.

3. Describe who is responsible to install wireless access points and other wireless equipments for the organisation.

4. Provide limitations on the location of physical security for wireless access points.

5. Describe the type of information that may be sent over a wireless network.

6. Describe conditions under which wireless devices are allowed.

7. Define standard security settings for wireless access points.

8. Describe hardware and software configurations for all wireless devices.

9. Provide guidelines for the protection of wireless clients to minimise/reduce theft. (This is because an employee is responsible to protect their wireless clients.)

10. Provide guidelines on the use of encryption and key management for wireless clients.

RISK ASSESSMENT OF WIRELESS LANs - A risk assessment is the process of identifying, quantifying and prioritising risks against criteria for risk acceptance and objectives relevant to the organisation.The primary goal of a risk assessment for wireless LANs is to mitigate impacts of possible threats in a wireless network. A risk assessment of wireless LANs should be performed periodically or when there are any changes that impact an organisation's wireless LAN. Organisations should define the approach, scope and methodology on conducting risk assessments for wireless LANs and perform risk assessments on wireless LANs periodically to fully explore the security

posture of their wireless network. A risk assessment report should then be produced which identify risks and security controls to be implemented in mitigating them.

WIRELESS NETWORK ASSESSMENT - A wireless network assessment highlights vulnerabilities found in current wireless LAN implementations in organisations. The wireless network assessment can be performed either randomly or on fixed schedules. To maintain the independence of the assessment results, wireless network assessments shall be performed by an independent and trusted third party. This assessment can and should be part of the periodic risk assessment effort to ensure potential wireless LAN threats and vulnerabilities are mitigated.

WIRELESS LAN TECHNOLOGIES

When making a decision about the best protocol or standard to use. We need to consider its features and our needs. Weight the features and compare the advantages and disadvantages of each one to make the final decision. There are several wireless LAN solutions available today, with varying levels of standardization and interoperability. Many solutions that currently lead the industry, IrDa,

Bluetooth, HomeRF and IEEE 802.11. These technologies enjoy wider industry support and targeted to solve Enterprise, Home and public wireless LAN needs.

Infrared (IrDa) - The appearance of portable information terminals in work and living environments is increase the introduction of wireless digital links and local area networks(LAN's). Wireless LANs can use either radio frequencies or infrared light to transmit signals. While it is considerably cheaper to install infrared networks, as many devices already have infrared (IrDA) ports (Franklin, 2010).

Portable terminals should have access to all of the services that are available on high-speed wired networks. Unlike their wired counterparts, portable devices are subject to severe limitations on power consumption, size and weight. The desire for inexpensive, high-speed links satisfying these requirements has motivated recent interest in infrared wireless communication.

Wireless infrared communications refers to the use of freespace propagation of light waves in the near infrared band as a transmission medium for communication (Carruthers, 2002). The Infrared Data Association (IrDA) is another trade association, which defined standards for infrared communication for many years. It has some advantages; notably that it is cheap and there are many devices which already include infrared including most laptops and PDAs as well as some printers. Before the advent of radio frequency LANs people were building infrared LANs, with some success. (irda.org, 2011)

Bluetooth - Bluetooth is an industry specification for short-range connectivity for portable personal devices with its functional specification released out in 1999 by Bluetooth Special Interest Group. 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) (Chandramouli, 2005). It is a worldwide license free band that any system can use (Goldsmith, 2004).

Using this band allows the Bluetooth protocol to become a standard around the world for interfacing devices together wirelessly.

Communications protocol developed to allow the devices using Bluetooth to transfer data reliably over their wireless network.

Bluetooth has a range of less than 10 meters. The range is increased when a scatternet is used because each unit only has to be within 10 meters of one other unit. The range can also be increased if the data is transmitted in a high power mode which offers transmissions up to 100 meters. Bluetooth also offers a cipher algorithm for security. This is most useful in the high power mode because when data is being transmitted further there is a greater possibility of an unwanted device receiving the network's data (Goldsmith, 2004).

HomeRF - In early 1997, several companies formed the Home RF working group to begin the development of a standard designed specifically for wireless voice and data networking in the home. (Goldsmith, 2004). HomeRF is an open industry specification developed by Home Radio Frequency Working Group 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.

The development of this working group was motivated by the widespread use of the internet and the development of affordable PCs that can be used in most homes. This protocol allows PCs in the home to have greater mobility, providing a connection to the Internet, printers, and other devices anywhere in the home. With all this potential, many members of industry worked to develop the Shared Wireless Access Protocol-Cordless Access (SWAP-CA) specification (Goldsmith, 2004).

IEEE 802.11 - The vendors joined together in 1991, first proposing, and then building, a standard based on contributed technologies. In June 1997, the IEEE released the 802.11 standard for wireless local-area networking. This initial standard specifies a 2.4 GHz operating frequency with data rates of 1 and 2 Mbps. With this standard, one could choose to use either frequency hopping or direct sequence. Because of relatively low data rates as, products based on the initial standard did not flourish as many had hoped.

In late 1999, the IEEE published two supplements to the initial 802.11 standard: 802.11a and 802.11b (Wi-Fi). The 802.11a (Highly Scalable Wireless LAN Standard , 2002), standard (High Speed Physical Layer in the 5 GHz Band) specifies operation in the 5 GHz band with data rates up to 54 Mb/s. The 802.11 WLAN standard allows for transmission over different media. Compliant media include

infrared light and two types of radio transmission within the unlicensed 2.4-GHz frequency band: frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS). Spread spectrum is a modulation technique developed in the 1940s that spreads a transmission signal over a broad band of radio frequencies.

CONCLUSION

The future of wireless local-area networking is now, and it is the solution for communication problems in organizations or any place that need a wide spread of internet connection, interoperability became reality with the introduction of the standards and protocols and prices have dramatically decreased. These improvements are just a beginning. Organizations who use WLANs networks can eliminate many of wireless LAN's security risks with careful education, planning, implementation, and management. WLAN brings out not only advantages, but also some Specific security problems, although development of wireless standards and security protocols may enhance the WLAN security.

A wireless local area networking system has been created for the utilization in a device checking requisition. The IEEE 802.11b methodology was resolved to be the best fit WLAN order to use in the provision dependent upon its cost, range, information rates, and networking topology. The 802.11b order makes information networking straightforward on account of its utilization of the Tcp/ip order. Along these lines, the network is effortlessly interfaced with wired Lans and the wireless WAN. The 802.11b order was then used to outline an equipment arrangement to be utilized as a part of the device checking requisition. 802.11b has a vast transmission run and exceptional information rates, so it combines well onto an area where it can handle numerous devices to minimize the WAN expenses.

REFERENCES

1. AirDefense,Inc, *Wireless LANs: Risks and Defenses,* 2002. http://www.itsec.gov.cn/webportal/download/73.pdf , 11/02/2008.

2. Batra, A., et. al., "Physical Layer Submission to 802.15 Task Group 3a: Time-Frequency Interleaved Orthogonal Frequency Division Multiplexing," Texas Instruments, Inc., Dallas, Texas, 2003.

3. Carruthers, Jerrey B., (2002). Wireless Infrared Communications. Wiley Encyclopedia of Telecommunications.

4. Chen, James C., "Meassured Performance of 5-GHz 802.11a Wireless LAN Systems." Atheros Communications. Sunnyvale, CA.

5. Clark, David, Pogran, Kenneth T. & Wed, David p. (1978). An Introduction to Local Area Networks. Proceedings of the IEEE, Vol. 66, 11, November 1978.

6. Flickenger, Roger Weeks. (2005). Wireless Hacks, 2nd Edition, O'Reilly, 2005

7. Franklin, Tom, (2010). Wireless Local Area Networks. TechLearn, The Network Centre, Innovation Close,

8. Goldsmith, Colin, (2004). Wireless Local Area Networking For Device Monitoring, Master thesis, University of Rochester Rochester, New York

9. Kraemer, R., "Bluetooth Based Wireless Internet Applications for Indoor Hot Spots: Experience of a Successful Experiment During CeBIT 2001," *Computer Networks: The International Journal of Computer and Telecommunications Networking*, Volume 41 , Issue 3, February 2003, pp. 303-312.

10. Negus, K. J., Stephens, A. P., and Lansford, J., "HomeRF: Wireless Networking for the Connected Home," 2000.

11. O'Hara, B. and Petrick, A., IEEE 802.11 Handbook: A Designer's Companion, Standards Information Network, IEEE Press, New York, New York, 1999.

12. Putman, Byron W.(2005). WLAN Hands-On Analysis. AuthorHouse, 2005.

13. Wireless LAN Security, 802.11/Wireless LAN Wardriving & Warchalking. http://www.wa drive.net, 11/02/2008.