ISSN 2277-3061

Demand of Wireless Network and Security in Current Research

Abhishek Prabhakar, Amod Tiwari, Vinay Kumar Pathak
Dr. Ambedkar Institute of Technology for Handicapped, Kanpur
abhishekprabhakar.aith@gmail.com
Bhabha Institute of Technology, Kanpur
amodtiwari@gmail.com
VC Vardhman Mahaveer Open University, Kota

ABSTRACT

Wireless security is the prevention of unauthorized access to computers using wireless networks .The trends in wireless networks over the last few years is same as growth of internet. Wireless networks have reduced the human intervention for accessing data at various sites .It is achieved by replacing wired infrastructure with wireless infrastructure. Some of the key challenges in wireless networks are Signal weakening, movement, increase data rate, minimizing size and cost, security of user and QoS (Quality of service) parameters... The goal of this paper is to minimize challenges that are in way of our understanding of wireless network and wireless network performance.

Indexing terms/Keywords

wireless network, Ad Hoc networks, crypto security.

Academic Discipline And Sub-Disciplines

Computer Science and Engineering

SUBJECT CLASSIFICATION

Wireless Network

TYPE (METHOD/APPROACH)

Survey

Council for Innovative Research
Peer Review Research Publishing System

Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Vol.14, No.6

www.ijctonline.com, editorijctonline@gmail.com

ISSN 2277-3061

INTRODUCTION

In wireless networks, computers are connected and communicate with each other not by a visible medium, but by emissions of electromagnetic energy in the air.The growing trends in wireless networks over the last few years are same as growth of the internet. Wireless communication is showing exponential growth in the cellular telephony, wireless internet and wireless home networking arenas. With help of Wireless LAN (WLAN) technology, computer networks could achieve connectivity with optimal bandwidth utilization. New generations of devices allowed users access to stored data even when they are travelling. Users use their laptops anywhere and instantly are granted access to all networking resources. Wireless network was developed keeping in mind what they are capable of delivering. Today, while wireless networks [1] have seen multiple uses but there are many disadvantages which can be exploited by attackers. Some form of security was required to prevent attackers from exploiting the wireless networks.

RELATED WORK

Researchers at Stanford have performed a number of studies of wireless network usage. Of late Tang and Baker [2] analyzed a 12-week trace collected from the wireless network used by the Stanford Computer Science department; this study built on earlier work involving fewer users and a shorter duration [3]. Users are divided into distinct location-based communities, each with its own movement, activity, and usage characteristics. Most users exploit the network for web-surfing, session-oriented activities and chat-oriented activities. Their study provides a good qualitative description of how mobile users take advantage of a wireless network, although it does not give a characterization of user workloads in the network. Earlier, Tang and Baker [4] also characterized user behaviour in a metropolitan area network, focusing mainly on user movement. The network spread over a larger geographical area and had very different performance characteristics. IEEE 802.11 is a basic standard for Wireless Local Area Network (WLAN) communication.

TYPES OF WIRELESS NETWORK

The IEEE standard introduces two types of wireless networks, namely, the infrastructure networks and the ad hoc networks.

Infrastructure Networks

The infrastructure type of wireless network (Fig 1) is a network with an Access Point (AP), in which all stations (STAs) must be associated with an AP to access the network. Stations communicate with each other through the AP. In infrastructure wireless network device installations can be set up with a fixed topology to which a wireless host can connect via a fixed point known as a base station or an access point. The latter is connected to the backbone network often via a wired link. Cellular networks [5] and most of the wireless local area networks (WLANs) [6] operate as static infrastructure networks. All wireless hosts within the transmission coverage of the base station can connect to it and use it to communicate with the backbone network. The communications initiated from or destined to a wireless host have to pass through the base station to which the host connects directly.

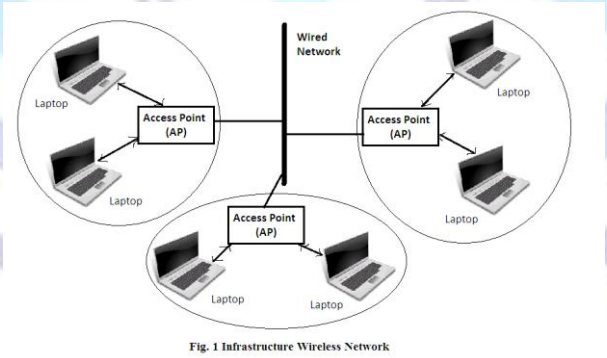

Fig. 1 Infrastructure Wireless Network

Fig 1

Ad Hoc Networks

The second type of wireless network is the ad hoc mode (Fig 2) is used if there are no Access Points (APs) in the network. In this mode, Stations (STAs) form an Ad hoc network directly with each other. An ad hoc network, such as a packet radio network, is one without a fixed topology. A wireless host can freely communicate with another host directly whenever the receiver is in its transmission coverage. If a wireless host would like to send messages to another host which is not in the coverage region, it will first relay them to a host in its transmission range. The host functions as a relay to forward the messages on its way to the destination. The major advantage of this configuration is flexibility. An ad- hoc network can be built easily without the need of any preset, fixed infrastructure. In addition, an ad hoc network is generally more robust than an infrastructure network as it does not have any critical device to maintain the network connectivity. In other words, it is unlikely that an ad hoc network will be partitioned due to the failure of a wireless host, but the malfunction of a base station may partition an infrastructure network, blocking the communication between all wireless hosts connecting to the failed base station and all other hosts in the network. There are some disadvantages for ad hoc networks. It requires more system

resources as the physical network layout will change as devices move around, while an access point in infrastructure mode generally remains stationary. If many devices are connected to the ad-hoc network, there will be more wireless interference. Each computer has to establish a direct connection to each other computer rather than going through a single access point. If a device is out of range of another device it wants to connect to, it will pass the data through other devices on the way. Passing the data through several computers is just slower than passing it through a single access point. Ad-hoc networks don't scale well. It is much more difficult and complex to perform routing in ad hoc networks because of frequent changes in the network topology due to host mobility.

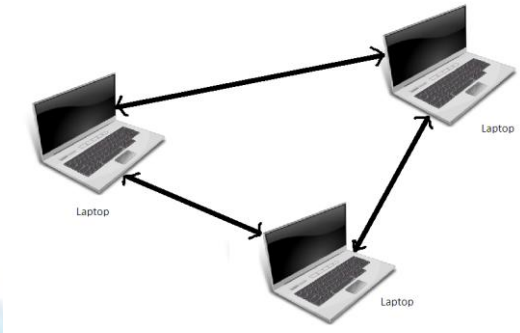

Fig 2. Ad Hoc Wireless Network

Fig 2

WIRELESS NETWORK SECURITY

With continual advances in technology, coupled with increasing price/performance advantages, wireless accessibility is being deployed increasingly in office and public Environments. To protect the wireless LAN network from attack, the following best practices are recommended:

1. Training to employees about WLAN risks, especially about how to recognize an intrusion or suspicious behaviour.
2. Stop unauthorized attachment of wireless access points.
3. Deploy strong authentication (X.509 digital certificate, USB token, smart card and/or biometric) for all of your IT resources, wireless and wire line alike.
4. Stop use of 802.11x WLAN cards in ad hoc mode, especially when in public areas or any building with a perimeter less than the WLAN broadcast range.
5. Change passwords and, where possible, administrator account names on WLAN access points.
6. Change the default SSID on all access points, and allow the access points to broadcast their SSIDs.
7. Use strong security for other data resources such as laptop or desktop data files and e-mail messages and attachments

RESEARCH CHALLENGES OF WIRELESS NETWORKS

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

Weak Signal strength

The strength of the radio signal weakens (with the square of the distance), hence the machines have a limited radio range and a restricted scope of the network. Signals transmitted over a wireless medium may be distorted or weakened because they are propagated over open and unprotected medium with irregular boundary.

Movement

Even when machines are not mobile a wireless network avoids cables between machines .Setting a wireless network is simple. Wireless network are free to move Where as wired network are bounded. As user roams around the connection is always kept alive.

Increase Data Rates

Improving the current data rates is required in wireless networks .To support multimedia applications high data rates are required.

Security

Security is really a big concern in wireless networking, especially in e-commerce [7, 8].and internet banking applications. wireless networks uses authentication and data encryption techniques to provide security to its users.

(Quality of Service) QoS

While the effective cost of small wireless network (cost of network cards) may be higher than the wired ones, extending the network is cheaper. As there are no wires there is no cost for material installation and maintenance. Quality of Service is a measure of network performance. It reflects the network's quality of transmission and service. For each flow of network traffic, QoS can be characterized by four parameters: Reliability, Delay, Jitter, and Bandwidth. It indicates network performance.

PROPOSED CONTROL IN CHALLENGES

The main challenges in current wireless technology is to minimize signal fading and network signal key if the signal related to x_i where the parity bits are $x_{1i}, x_{2i}, \cdots\cdots\cdots x_{ni}$

The parity bits should pass in odd serial order using Hamming code [9].

Hence the all parity bits can be represented as

$$\sum_{j=1}^{n} x_{ji} = x_{1i} + x_{2i} + x_{3i} + \cdots\cdots + x_{ni}$$

Where n is odd no of bits with positive integer. Let a specific function by which to improve the bandwidth data rate of geographical area networks. Where K is represent base of signal length. Hence

$$\sum_{i=1}^{n} x_i = a_n k^n + a_{n-1} k^{n-1} + \cdots\cdots\cdots + a_1 k + a_0$$

And $s = n+1$ it is apparent that $x \geq k^n$, where S is parity bits count number

$$x \leq (k-1)k^n + (k-1)k^{n-1} + \cdots + (k-1)k + (k-1) \qquad = k^{n+1} - 1 \prec k^{n+1}$$

Since $k^{s-1} \leq x \prec k^s$

Then $S - 1 \leq \log_k x \prec S$ and so.

$$S = \lfloor \log_k x \rfloor + 1$$

Now $k^{s-1} \prec x + 1 \leq k^s$ where

$$S - 1 \prec \log_k (x+1) \leq S$$

Where $S = \lceil \log_k (x+1) \rceil$ is strong signal

Wireless Sequenced Networks (WSNs) plays a vital role in military Command, Control, Communications, Computing, Intelligence, Surveillance, reconnaissance and geographic Targeting systems. Few challenges have been faced by WSNs on the battlefield are addressed in [10]. In the battlefield, the WSNs are prone to the attacks, where either the data or corrupting control devices are attacked, leading to large amount of energy consumption and finally to the exit of nodes from work. The energy efficiency of sensor nodes and the correct modelling of energy consumption are the research issues yet to be explored. WSN based collaborative target detection with reactive mobility has been presented . A sensor movement scheduling algorithm was developed and its effectiveness was proved using extensive simulations. WSNs have found application in very critical applications such as object detection and tracking. These applications require high detection probability, low false alarm rate and bounded detection delay.

CONCLUSION

The main advantage is that a wireless network allows the machine to be fully mobile as long as they are in radio range. If such networks are to succeed in the commercial world, the security aspect naturally assumes paramount importance.Wireless LANs are not either in secure that some people predict, nor are they secured enough in exactly the same way as conventional wireline LANs. But because this technology is rapidly increasing, it is required that the organization roll out its WLAN(s) in a secured way according to their need.

In conclusion, wireless networks are rapidly gaining popularity, and demand for wireless network applications is increasing.

REFERENCES

[1] http://en.wikipedia.org/wiki/Wireless_network

[2] D. Tang and M. Baker. Analysis of a Local-Area Wireless Network. In Proceedings of ACM MobiCom'00, pages 1–10, August 2000.

[3] K. Lai, M. Roussopoulos, D. Tang, X. Zhao, and M. Baker. Experiences with a Mobile Testbed. Worldwide Computing and Its Applications, Lectures notes in Computer Science, pages 222–237, 1998.

[4] D. Tang and M. Baker. Analysis of a Metropolitan-Area Wireless Network. In Proceedings of ACM MobiCom'99, pages 13–23, August 1999.

[5] V.O.K. Li and X. Qiu, ―Personal Communication Systems (PCS),‖ Proc. IEEE, vol. 83, no. 9, Sept. 1995, J.H.Schiller, Mobile Communications, 2nd ed., Addison-Wesley, 2003.

[6] Chip Craig J. Mathias Principal, Farpoint Group COMNET 2003 ―Wireless Security: Critical Issues and Solutions‖ 29 January 2003.

[7] IEEE 802.11-1999, IEEE Standard for Local and Metropolitan Area Networks Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 12, 1999.

[8] Symposium on Modeling and Optimisation in Mobile adhoc and Wireless Networks and Workshops, April 2008, pp.192-196

[9] En. Wikipedia.org/wiki/hamming_code.

[10]N. Alsharabi, L. R. Fa, F. Zing, and M. Ghurab, "Wireless sensor networks of battlefields hotspot: challenges and solutions," WIOPT 2008Sixth Intl.ICST symposium on modeling and optimization.