Open access Journal International journal of Emerging Trends in Science and Technology

Wireless Networks

Authors
Kimmi Makkar*, Meenakshi Janghu, Poonam Tanwar*****

*Student, Dept. of Information Technology,Dronacharya College of Engineering , Gurgaon, Haryana, India
Email: *kimmimakkar111@gmail.com*

**Student, Dept. of Information Technology, Dronacharya College of Engineering , Gurgaon, Haryana, India
Email: *janghu.meenakshi@gmail.com*

***Student, Dept. of Information Technology,Dronacharya College of Engineering , Gurgaon, Haryana ,India
Email: *tanwarpoonam26@gmail.com*

Abstract : The arrival of wireless technology has reduced the human efforts for accessing data at various locations by replacing wired infrastructure with wireless infrastructure and also providing access to devices having mobility .Since wireless devices need to be small and bandwidth constrained, some of the key challenges in wireless networks are Signal fading, mobility, data rate enhancements, minimizing size and cost, user security and (Quality of service) QoS. Speaking of Wireless LAN, the general thought is about data transfer while using applications such as web browser, e-mail client, etc. As the technology is advancing, Wireless LANs are now also capable of supporting time-sensitive services such as voice and video. These services have stringent service requirements from the network infrastructure. These requirements supersede the requirements of general data. The wireless industry is undergoing a change. We see the evolution from cellular 2G to 3G standards, the migration from circuit to packet applications, and the procession of voice to data. We also see the industry incorporating new wireless access technologies such as WiFi and WiMAX. All of this is happening in a market place where voice subscriber penetration levels in many parts of the world are saturating and there is incredible pressure to reduce network capital and operating costs. These conditions present signicant technology challenges to increase customer demand and further increase network capacity to lower network costs .This paper is intended to provide the reader with an overview of the Research Issues and Challenges in wireless networks.
Keywords :Wireless Local Area Networks (WLANs), IEEE 802.11, Quality of Service (QoS), Frequency Hopping Spread Spectrum (FHSS), Wired corresponding privacy (WEP)

I. INTRODUCTION

The hazardous increase in wireless networks from the last some years resembles the speedy increase in the growth of the internet within the last ten years. Wireless communication abide to enjoy exponential increase in the mobile phones, wireless internet and wireless home networking arenas. With custom of Wireless LAN (WLAN)

technology, computer networks could achieve the connection with a useable amount of bandwidth without being networked via a wall socket. The generations of devices which are hold by hands allowed the users right to stored data even while travelling. Users could set their laptops down anywhere and immediately be granted the right to all the networking equipments. This was, the ability to see the future of wireless networks, and what they are capable of giving or delivering. Nowadays, wireless networks have seen existing in many places in the home user markets, widely reported and treating unfairly to get some benefits of themselves in the standard security system have not able to grow to normal size wireless deployment rate in business company environments. Over time, it became understand that some form of safety was needed to stop outsiders from exploiting the connected resources. We believe that the recent wireless access points gives a large safety problems than the earlier Internet connections. As many wireless advanced machines or equipments , this will be a good step in a process that helps us to move forward to another part of it for providing a good secure solution to any wireless solution.

The rest of this research paper is planned as follows;

Firstly we will present the taxonomy of wireless networks and will provide the discussion of the two operating modes of the IEEE 802 .11 . Then we will provide a short description about the Research Challenges and Issues of Wireless Networks .A new technology namely cognitive radio is described and in last the conclusion of the whole paper is given.

II. TAXONOMY OF WIRELESS NETWORKS

The distinguishing features of wireless networks is that segments are passed with the existence of wireless links. A machine can send messages in a wireless network via the wireless way of communicating information, air, to another device provided that the receiver is within the transmission range of the sender. This adds the ability to move easily , how a wireless network is formed and organized. And it also supports the ability to move the part of the device or can also say it a device mobility.

IEEE 802.11

IEEE 802.1 is a necessary standard for Wireless Local Area Network (WLAN) communication. This standard was first popularized in 1997. It was predictable for home and office conditions for wireless local area connectivity and guide three types of transmission technologies named

i) Infrared (IR),

ii) Frequency Hopping Spread Spectrum (FHSS),

iii) Direct Sequence Spread Spectrum (DSSS). In 1999 two other transmission components were involved and they are, Orthogonal Frequency Division Multiplexing (OFDM) and High Rate Direct Sequence Spread Spectrum (HR-DSSS). The next OFDM modulation design was introduced in 2001 for high data amounts . The standard suggests two operating techniques of wireless networks, namely, the infrastructure networks and the ad hoc networks.

A. Infrastructured Networks

The infrastructure operating technique is a network with an Access Point (AP), in which all STAs ought be combined with an AP to contact the network. STAs relate with each other through the AP. An infrastructure one with prospective, permanent network gadget installations. It can be set up with a solid topology, to which a wireless moderator can attach via a fixed point, which is known as a base station or an access point. The following is associated to the backbone network, often via a wired link. Cellular networks and many of the wireless local area networks (WLANs) compel as the constant infrastructure networks. All wireless moderators within the transmission scope of the base station can connect through it and then use it for the communication with the backbone network. This means that all communications proposed from or intended to a wireless moderator have to pass through the base station to which the moderator connects straight. In addition, an infra-structured network is also be rooted with a quasi-static or an aggressive topology. A satellite network is related to this section. It contains two segments and they are a space segment and a ground segment. This space segment contains satellites and the ground segment contains a lot of for base stations which are also known as gateway stations (GSs), through which

all communications via long-haul satellite junction takes place. The base station, or access point, is a discriminating component for communication. When a mobile owner moves away from the scope of its base station, then for maintaining an ongoing connection, a terminal handoff appear such that a mobile owner hands over its representative for communication from one base station to the other one. Whenever the scopes of distinct neighbouring base stations overlap with each other, a mobile owner may connect to one of the attainable base stations based on positive fact.

B. Ad Hoc Networks

The second operating mode is the independent mode or the ad hoc mode and it is used if there are no Access Points (APs) in the system or network. In this operating mode, Stations (STAs) form an Ad hoc network straight with each other. A packet radio network is an ad hoc network, which is without a fixed topology. A wireless host can openly connect with another host straight whenever the acceptor is in its communication scope. If a wireless owner would like to send messages to another owner which is not in the coverage area, it will first deliver them to a owner in its transmission area. The host tasks as a transfer to lead the messages on its way to the target. The main advantage of this composition is flexibility. An ad- hoc network can be togethered smoothly, without the use of any preset, fixed infrastructure. In addition, an ad hoc network is usually more potent than an infrastructure network because it does not contain any complementary device to control the network connectivity. In other words, it is rarely an ad hoc network will be subdivided due to the breakdown of a wireless host, but the malfunction of a base station may seperate an infrastructure network, blocking the transmission between all wireless hosts attaching to the flop base station and all other hosts in the network. However, there are many obstacles for ad hoc networks. First, it is much more troublesome and complicated to perform revolting ad hoc networks because of periodic differences in the network topology due to host mobility. Second, it is more tough to equalize or restraint appropriate operation of an ad hoc network, as each wireless host may have its own conclusions to execute activities like time synchronization, power management, and packet scheduling. In an infra structured network, these conclusions are mostly resolved in and thus unified by the base stations or access points.

III. RESEARCH CHALLENGES OF WIRELESS NETWORKS

After all wireless devices need to be small in size and wireless networks are bandwidth limited, some of the primary objections in the wireless networks are shortifying the size, user security, data rate enlargements, cost, low power networking and Quality of Service (Qos).

A. Signal Fading

Signals transmitted over a wireless medium contrasted wired media, may be perverted or exhausted because they are inseminated over a free or open, unprotected, and ever dynamic medium with uneven boundary. Likewise, the same signal may scatter and travel on various paths due to diffraction, reflection and scattering generated by hindrances before it reaches at the target. The scattered signals on various paths may take different times to reach the destination. Thus, the resultant signal after adding up all propagated signals may have been extremely distorted and constricted when related with the transmitted signal. The acceptor may not perceive the signal and hence the transmitted data cannot be accepted. This uncertain nature of the wireless medium causes a generous number of damages of the packets.

B. Mobility

Beyond the pressure established by the wired connections among devices, all devices in a wireless network can move freely. To guide mobility, a continuing connection should be kept conscious as a user drift around. In an infrastructure network, a handoff appears when a mobile owner moves from the scope of a base station or access point to that of other one. A protocol is hence prescribed to assure flawless transition during a handoff. This contains deciding when a handoff should developed and how data is repulsed at the time of the handoff process. In some seasons, packets are missed during a handoff. The topology changes when a mobile host moves in an ad hoc network. This means that, for an ongoing data communication, the transmission route may need to be recomputed to, cater for the topological changes. Since an ad hoc network may subsist of a huge number of mobile hosts, this established a powerful challenge on the sketch of an impressive and profitable routing protocol that can work well in an environment with repeated topological changes.

C. Power and Energy

A mobile phone is a gadget which is generally handy, small in size, and devoted to operate a positive set of functions; its potential cause may not be able to transfer power as much as the one established in a fixed apparatus. When an equipment is preferred to move openly, it would normally be difficult to receive a continued supply of power. To save energy, a mobile device must be capable of operating in a practical and profitable manner. To be strange, it should be capable of transmitting and receiving in an observant manner so as to diminish the number of transmissions and receptions for assertive communication operations.

D. Data Rate

Elaborating the present data rates to guide future high geared applications is necessary, specially, if multimedia services are to be implemented. Data rate is an objective of individual circumstances such as the interference mitigation through error-resilient coding, data compression algorithm, power control, and data transfer protocol. Thus, it is essential that builders implement a well thought out composition that recognized these aspects in order to accomplish more advanced data rates. Data compression plays a very important function when the multimedia applications like video conferencing are to be promoted by a wireless network. Presently, compression standards such as MPEG-4 gives a production of compression ratios of the order of 75 to 100. Now the challenge is to upgrade these data compression designs for producing good and high quality audio and video even at these compression rates. Unsuccessfully, highly compressed multimedia data is more responsive to network glitches and obstructions and this requires the need of algorithms to preserve perceptive data from getting perverted . Economical error control conclusions with deep overhead must be scrutinized. And the other way to improve the data rates would be to occupy original data transfer protocols that alter to the time- varying network and traffic aspects.

E. Security

Security is a enormous transaction in wireless networking, specifically in m-commerce and e-commerce applications . Mobility of customers raises the safety concerns in a wireless network. Modern wireless networks apply confirmation and data encryption procedures on the air interface to give safety to its customers. The IEEE 801.11 standard represents wired corresponding privacy (WEP) that explains a process to authorize users and encode the data between the PC card and the wireless LAN access point. In extensive firms , an IP network level security solution could ensure that the corporate network and proprietary data are safe. Virtual private network (VPN) is an option to make access to fixed access networks reliable.

ACKNOWLEDGMENT:

Sincere thanks to our guide for his help and assistance towards the successful completion of this research paper.

REFERENCES:

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

[2] V.O.K. Li and X. Qiu, ―Personal Communication Systems (PCS),‖ Proc. IEEE, vol. 83, no. 9, Sept. 1995

[3] 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.

[4] J.H. Schiller, Mobile Communications, 2nd ed., Addison-Wesley, 2003.

[5] Y. HU and V.O.K. Li, ―Satellite-Based Internet: A Tutorial,‖ IEEE Comm. Mag., vol. 39, no. 3, Mar. 2001, pp. 154–62.