Achieving Improved Performance at Access Point in WLAN Infrastructure Mode

Irfan Siddavatam
Department of Information Technology
K J Somaiya College of Engineering
Mumbai, India
irfanasv@gmail.com

***Abstract*—In recent years WLAN is projecting itself as alternate solution to carry out enterprise's network traffic. The basic mode of WLAN is classified as ad-hoc mode and infrastructure mode. Infrastructure mode use wired network as backbone. The enterprise WLAN network design preferred infrastructure mode which assume as extension to wired network. The wireless access point is major component of infrastructure mode. As demand for every type of traffic increases in WLAN, how access point handles this traffic grabs equal attention. Study of access point varies at different layers such as location of access point at physical layer, queuing mechanism of access point at Mac layer. In this paper we discus role of access point in handling WLAN traffic and shortcoming of existing approach. In this paper alternative approach for access point is suggested to approve network performance using learning method.**

Keywords- Access point, Access Point Management, Access Point Firmware

I. INTRODUCTION

Enterprises are deploying wireless LANs for larger numbers of users with needs for providing flexibility for corporate applications that involve e-mail, Web browsing, and access to various server-based databases. Due to easy deployment in existing infrastructure of enterprise, WLAN gains popularity in last little years.The primary purpose of deployments of WLAN is to satisfy user demands for high bandwidth, mobility, and reliability.

The IEEE 802.11 defines two basic WLAN architectures:

- Ad hoc Based and
- Infrastructure Based

The Ad hoc mode also called Independent Basic Service Set (IBSS) or peer to peer, allows two or more clients to establish connectivity between them and the wire line network without the involvement of any central point. It is commonly used to form small networks set up for a specific purpose.

Infrastructure mode is differing from ad-hoc mode in following manner: need an access point, need an administration and need wire line support. The Infrastructure mode also called the Basic Service Set (BSS) relies on a central point called the Access Point (AP) through which the 802.11 clients communicate with each other and the wire line network. The most important function of the AP is bridging as shown in figure 1. It converts the 802.11 frames to another type for delivery to the Wide Area Network (WAN). To cover a large area, two or more APs normally connected through a wired backbone are deployed. The wired backbone is called the Distribution System (DS). The DS is a logical component of the 802.11. Its main function is to relay frames among APs. In infrastructure mode, an access point is typically connected using an Ethernet (IEEE 802.3) link to a wired network and all wireless nodes communicate to this network through the access point. Access points are often combined with network function. The AP acts as a bridge between the wired and wireless networks and can perform basic routing functions. Workstations with client radio cards reside within a basic service set, while multiple basic service sets create an extended service set..

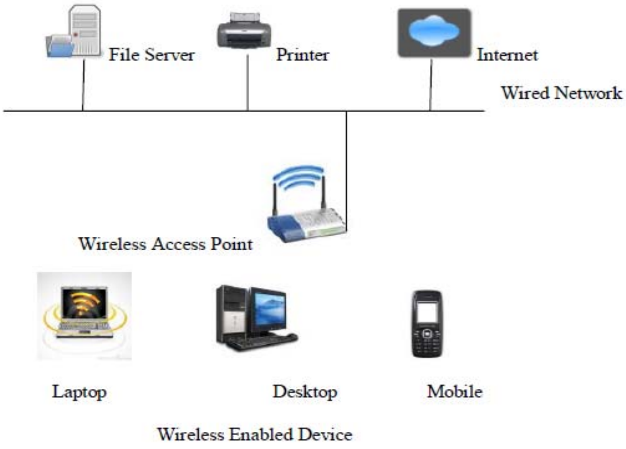

Figure 1. WLAN Infrastructure Mode

There are two types of access points: Dedicated hardware access points (HAP) normally termed as Wireless Routers. Access points allow wireless clients access to a single network, while WLAN routers allow clients to browse a number of different networks. Software Access Points which run on a computer equipped with a wireless network interface card as used in an ad-hoc or peer-to-peer wireless network. With appropriate networking software support, users on the wireless LAN can share files and printers located on the wired LAN and vice versa.

The access point (AP) assigns timely throughputs to clients under the delay and reliability constraints. Performance studies of IEEE 802.11 access points are becoming increasingly important since it is the predominant choice for high-speed wireless access to Internet. The AP has the physical capacity to handle 2048 MAC addresses, but, because the AP is a shared medium and acts as a wireless hub, the performance of each user decreases as the number of users increases on an individual AP. Ideally, not more than 24 clients can associate with the AP because the throughput of the AP is reduced with each client that associates to the AP. So when deploying a wireless LAN, it is important to know how many users the access points will support. This helps in determining whether the WLAN will bear a specific application. For example, the WLAN may need to handle twenty users accessing the Internet from an airport concourse. Or, hundreds of users may need access to the WLAN from a convention center.

Following Figure 2 shows simplified block diagram of 802.11 Access Point [1].

Block diagram of access point consists of Transmitter and receiver buffer along with buffer manager. It contains physical layer of Ethernet and 802.11 and MAC layer of both. Transmitter and Receiver block transmits and receives Ethernet frame including address checking, cyclic redundancy checking (CRC) and carrier sense multiple access with collision detection (CSMA/CD). Buffer manager stores frame to be transmitted and received frames. CPU and Ethernet MAC calculates checksum and TCP/IP header.

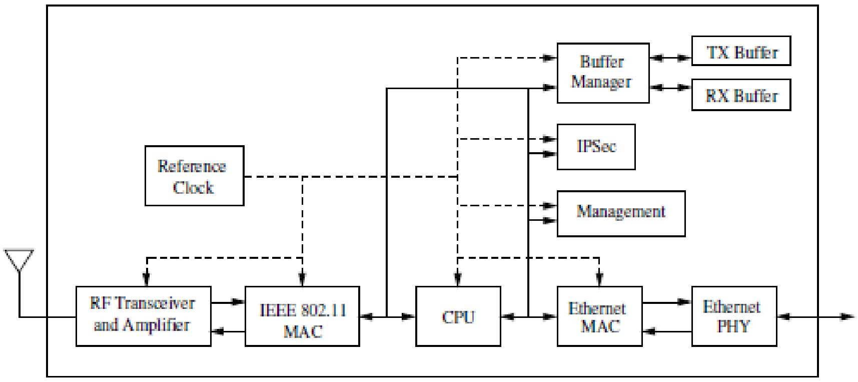

Figure 2 Block diagram of 802.11 Access Point

With wired IEEE 802.11 AP uplink capacities greater than or equal to 100 Mbps and wireless IEEE 802.11g downlink capacities of 54 Mbps, the wireless AP can often become the bottleneck for downstream Internet traffic.

The MAC layer of 802.11 works on logical function, these logical functions are also known as coordination functions. The 802.11 standard defines two forms of medium access, distributed coordination function (DCF) and point coordination function (PCF).Point coordination function is centralized protocol and optional. In PCF, as it is centralized, no collision will occur. The pooling mechanism is used by PCF for gaining the access of channel. DCF is mandatory and based on the CSMA/CA (carrier sense multiple access with collision avoidance) protocol. There are two access methods of DCF .The access point uses DCF protocol to handle traffic at enterprise level.

II. Access Point Arrangement

WLANs typically consists of Access Points (APs) distributed across the enterprise. Initially, the implementation of WLAN is achieved with individual AP, also called as FAT AP. An Access point extends the capability of an existing Ethernet network to devices on wireless network. Wireless device can connect to a single access point, or they can move between multiple access points located within same vicinity. As wireless client move from one coverage cell to another, they maintain network connectivity. These distributed access point provide different types of coverage such as hot spot coverage. Access points provide a WLAN connection in specific areas, such as conference rooms and other common areas. Distributed access points implements the complete 802.11 specification. They provide the wireless to Ethernet layer 2 bridging function. User traffic goes from the wireless network to the Ethernet where the access point is connected. These APs are designed to have everything on-board that is needed so that they can be connected to any Ethernet switch. An access point contains both a radio circuit supporting required frequency band for 802.11 WLAN Standards and on-board intelligence capable of processing 802.11 control and management information plus the ability to encrypt and decrypt frames as well as a capability to communicate to an authentication server to confirm the identity of user trying to access the network. This implementation is low cost and simple to deploy. But as WLAN to begin ramp up in enterprises, the initial deployment models typically used large number of independent access points. When configuring a network based on this approach, each device must be individually manipulated.

However, as networks grow and become more complex, the deployment of standalone WLAN APs can become very time consuming and expensive. Access points cannot easily convey configuration or security information to each other since no standard protocols exists to perform these functions. Each access point operates as an independent device. These APs often provide high speed wireless connectivity but access the internet via independent, relatively low-speed DSL or cable modem links. The independent AP architecture suffers from scalability and management problems. Large infrastructure may have 100, 1000 access points to deploy and manage. With thousands of access points, it simply isn’t possible to configure and alone manage such a large wireless network. On the other hand, the scarcity of APs in conventional enterprise WLANs limits their performance in variety of ways. The WLAN is unable to fully utilize the available spectrum at each location with less number of APs. Managing scalability and managerial issues of independent AP is first step to centralized management of WLAN. A centralized wireless controller manages number of access points as one. This centralized approach is also called as Thin AP or dependent AP architecture. A thin or controller based access point is usually part of a centrally managed enterprise WLAN. This type of access point requires an external controller to manage network traffic [3]. Centralized architecture is that all traffic either to or from the wireless network must pass through the switch. This allows controller to have complete control over the traffic management and security issues. Centralized wireless controllers not only ease the burden of deploying new access pints, but they also simplify the day to day management of them. Centralized management allows changes to be made once, from a central location. Controller becomes the single point of configuration, management, security troubleshooting for all access points and wireless users.

Access point management not only has to take care of managing network with effective but also have to look after interference avoidance such as co-channel interference. . Each AP is assigned fixed channel with supported data rate of 11Mbps. A total of 14 channels are defined in 802.11b/g channel set. The optimal WLAN deployment makes the maximum number of non-overlapping channels available in both 802.11b/g. Each channel is 22 MHz wide and channel separation is of 5 MHZ. In 14 channel system, there are non overlapping channels 1, 6, 11 to use compared to 802.11a has 12 non-overlapping channels. This channel spacing governs use and allocation of AP in environment where multiple APs. More non overlapping channel more bandwidth is allocated to users.

III. THROUGHPUT IMPROVEMENT APPROACHES AT ACCESS POINT

Author S. Vasudevan et.al estimated bandwidth between Access Point and Host for upstream and downstream traffic. Author proposes measurement of delay of the periodic Beacon frames sent from an access point [4]. An access point schedule Beacon interval at regular interval which is typically of 102.4ms. The time instant at which the access point schedules the next beacon message is referred to as the Target Beacon Transmission Time (TBTT). As per the 802.11 standard, time zero is defined to be a TBTT. Given the value of the beacon interval, the end-host knows the exact time instants when beacon messages are scheduled for transmission.

Once a beacon message is scheduled, it is transmitted According to the normal frame transmission rules. Author assumes that beacon frames are not prioritized over other frames, as implemented in the APs used in experimentation. The time difference between the instant when a beacon message transmission begins (as obtained from the timestamp field of the Beacon frame) and the TBTT yields an estimate of the beacon delay, TB, which is the total time spent by a beacon frame at the access point waiting for transmission. Since author assumes that beacon frames are not prioritized over other frames, TB provides an estimate of the total queuing delay plus the contention delay that will be experienced by a data frame transmitted by the AP. Downstream bandwidth estimated in absence of RTS/CTS mechanism is as follows:

The contention and transmission delay of the data frame plus the respective ACK delay.

$$T = T_D + T_A$$

Where T_D is estimated form beacon delay

If the AP has multi-rate support, then the current sending rate R of the AP can easily be inferred from the duration fields in the data frames transmitted by the AP, then T_D can be computed as

$$T_D = T_B + DATA/R$$

Upon receiving the data frame, the receiver sends an ACK frame after a delay of SIFS. ACK frames are fixed in length and are typically sent at the same rate as the data frame. Hence, knowing the sender rate, TA can be easily determined as:

$$T_A = SIFS + ACK/R$$

The potential bandwidth B from the AP to the end-host is then given by:

$$B = DATA/T$$

Experimentation result perform with Netgear MA 311 wireless PCI card to function as an access point shows following result for 552µs. For a packet of size L bytes and data rate R, the potential downstream bandwidth is then given by

$$B = 8L/552 + 8L/R + T_A$$

Where T_A = 213µs. For instance, when L = 640 and R =11 Mbps, the potential downstream bandwidth yields an estimate B = 4.16 Mbps. Results are obtained for contention free environment.

The upstream bandwidth estimating requires that the end-host sends data frames to an access point in the unaffiliated state and records the time elapsed between the instant when a frame is scheduled for transmission and the time when the end-host receives an ACK message.

If a wireless AP supports many flows, the queuing requirements of an AP may decrease. A typical home AP will not carry anywhere near 250 flows. However, a commercial AP deployed at a corporation or university may have a significant number of flows. If the Access Point queue capacity is too small, a flow's throughput can be significantly below the available bandwidth of the wireless link. If the wireless AP is handling UDP traffic, such as found in some online games and streaming applications, that is unresponsive to congestion and sends at a rate higher than the wireless link capacity, then the AP queue will fill to capacity regardless of the queue capacity. During periods of bursty packet arrivals or when the AP nears a saturating offered load due to a high speed wired link into the access point, the AP queue will fill and produce undesirable droptail packet losses that will cause intolerable delay for applications such as VoIP or computer gaming. Author Feng Li et.al. proposed deploys the Access Point Queue (APQ) methodology for externally estimating the queue capacity for a wireless access point [5] . The basic steps in the Access Point Queue technique for measuring wireless AP queue capacities are to fill the AP queue, to measure the queuing delay and to compute the queue capacity using the measured delay and throughput. APQ uses a two step process that first determines the saturation offered load for a given AP configuration before carefully measuring the maximum queuing delay at saturation and thereby determining a blackbox estimate of the internal AP downstream queue capacity. Employing a controlled Host AP, the APQ method was validated to provide solid evidence that APQ accurately measures AP queue capacity. Let D_h be the delay measured with a full queue, D_l be the delay measured with an empty queue and T be the saturation throughput measured by sending packets of size s (including IP headers). Then the queue capacity in packets, q_p, is:

$$q_p = (D_h - D_l) \times T/s$$

To fill the AP queue, the downlink offered load must be greater than the effective wireless link capacity.

A fundamental APQ concept is to measure the delay when the queue is full compared to the delay when the queue is empty.

802.11e access point achieves admission control based on either of two approaches measurement based admission control or analytical model based admission control. The measurement based approaches does not required complex numerical computation. Simple computation of additional loads that can be generated by the activation of the new flow is necessary. These additional loads are then compared to the measured residual capacity of the channel. But it is very hard to precise the measurement interval value. Analytical model predict the performance metrics using numerical computation before making any decision.

The other proposed approach to achieve QoS with help of 802.11e access point is model-based admission control algorithm that is located within the QoS Access Point (QAP) [6]. Author Nada Chendeb Taher et.al propose an admission control mechanism which is based on the analytical model which was developed for two main objectives:

1) To provide a sufficient degree of accuracy and precision and

2) To have a low computational overhead in order to be suitable for the usage in access control algorithm.

Author considers analytical model is a four dimensional discrete Markov chain drawn for each AC. The transition probabilities are based on p_c (collision probability), p_b (channel busy probability) and p_e (probability of empty queue).A lot of efforts were put to develop an accurate analytical model, that predicts on the best the correct values of the achievable performance metrics. By using these predicted value algorithms are designed to which is to be implemented in the QAP and which is responsible for the decision making at the arrival of new flow.

IV. PROPOSED FRAMEWORK

After discussing mechanism and working of access point, here we suggest alternative approach to improve performance of WLAN at access point. After going through literature review for access point role in network, one can conclude that most of the work in direction of improvement is based on protocol mechanism. In contrast to this here we suggest improvement in access point firmware which can be achieved in with any types of protocol network implement. There are several projects focused on building quality third-party software for access point. Access point contains built-in programmable logic called firmware. This firmware is written in NAVRAM. This NAVRAM is of few Kbps. The proposed approach suggests that access point firmware should be updated such that it has supervisor module which supervise the connected client to it.

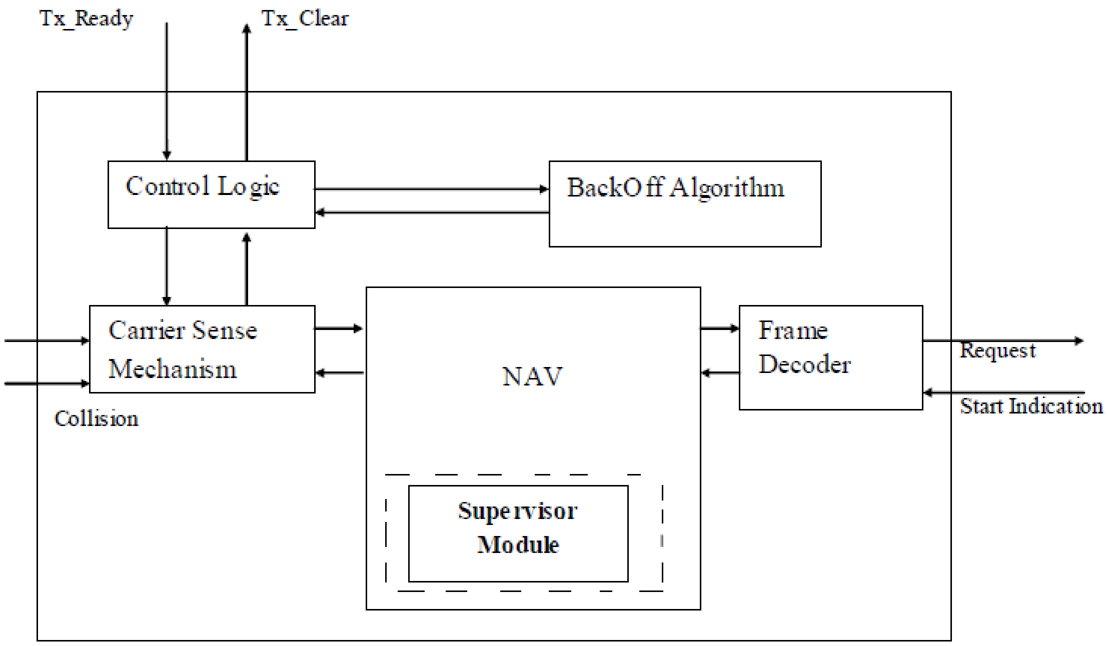

Figure 3 Modified Access Point Firmware

By applying learning process, this module records usage of particular IP which is frequently get connected in network. From reading of this supervisor module network administrator can be able to take decision whether network should be continued with number of connected client or any of the clients should be disconnected to achieve satisfactory performance. Learning rules can be set depending upon need of network environment. For example if network administrator want maintain satisfactory throughput limit for all the connected user at any given time with any given types of network services, then learning parameter for supervisor module can be set as throughput of individual connected user. The supervision module will learned the delivered throughput of every user at dynamic network condition. Rules can be set by using learned information to set privilege for specific user for maintaining constant throughput irrespective of dynamic load of network. This privileged user can be categorized under premium user of network. This scenario explains how supervisor module of access point can be used to maintain required performance of network using access point as per need of network administrator rather than every time making changes to protocol.

Depending on the specific access point, third-party software can be uploaded either by the web interface and/or tftp from a command line prompt. Even existing software can be updated at vendor place. But updating access point firmware with third party software gives privilege to user for setting learning parameter as per his needs.

CONCLUSION

Enterprises deploying WLAN rapidly to achieve advantages of it such as mobility, ease of deployment, economical etc. The popular form of WLAN deployment is infrastructure mode. In infrastructure mode, access point plays major role in providing connectivity among wireless users. An association between a wireless access point and a wireless access device is simple which makes it predominant choice for high-speed wireless access to Internet. So when deploying a wireless LAN, it is important to know how many users the access points will support. This helps in determining whether the WLAN will bear a specific application or not. But study observed that access point become bottleneck in high speed and high usage networks. Managing network traffic at access point is researched extensively in literature. The most of the approaches suggested change in either queue capacity of access point to buffered incoming and outgoing traffic or enhancement in protocol which is implanted in access point. In this paper we proposed approach which offers more flexibility than the approaches suggested in literature. Approach is independent of either queue capacity of access point or protocol implementation. The proposed approach suggests making firmware of access point intelligent to handle traffic across it. Supervisor module is written in firmware of access pint such that it observes traffic across access point and applying learning rule. The learning rules can be set and decide by network administrator to meet specific requirement of network.

The firmware changes can be done either in company firmware directly at the time of flashing original firmware or can be later updated by third party firmware. The latter option provides flexibility to network administrator to set and change rule for dynamic network condition.

REFERENCES

[1] Biplab Sikdar. "Environmental Impact of IEEE 802.11 Access Points: A Case Study"

[2] Benny Bing, ""Emerging Technologies in Wireless LANs: Theory.

[3] www.cisco.com/.../wireless_lan_switches.html

[4] S. Vasudevan, K. Papagiannaki, C. Diot, J. Kurose and D. Towsley, "Facilitating Access Point Selection in IEEE 802.11 Wireless Networks", Internet Measurement Conference, USENIX Association, 2005.

[5] Feng Li, Mingzhe Li, Rui Lu, Huahui Wu, Mark Claypool and Robert Kinicki , "Measuring Queue Capacities of IEEE 802.11 Wireless Access Points"

[6] Nada Chendeb Taher, Yacine Ghamri Doudane1, Bachar El Hassan, Nazim AGOULMINE, "An Accurate Analytical Model for 802.11e EDCA under Different Traffic Conditions with Contention Free Bursting"

[7] IEEE 802.11 standard for Wireless Local Area Networks, http://standards.ieee.org/getieee802/802.11.html

[8] http://wirelesse2e.wordpress.com/2010/09/07/why-wifi-is-still-needed-to-supplement-lte/

AUTHORS PROFILE

Irfan Siddavatam received the B.E. degree in Electronics in 1999 and M.E. degree in Computer Science in 2007. Since 2005 he is an Assistant Professor with the Department of Information Technology at K J Somaiya College of Engineering. His interest includes Artificial Intelligence, Computer Networks, Wireless Networking, Programming Languages.