In this chapter we discuss the various issues and approaches for AP selection in 802.11 WLAN. Further, in this chapter we describe the challenges, merits and demerits of legacy AP selection strategies and load balancing techniques in IEEE 802.11 WLAN.
3.1 Introduction

When IEEE 802.11 WLAN is deployed in infrastructure mode, the mobile stations send and receive frames through an Access Point. The selection of an Access Point has been encountered as a very much critical and complex problem in a way to obtain satisfactory performance. The traffic load of wireless LANs is often, unevenly distributed among the access points (APs), which results in unfair bandwidth allocation among Mobile Users. In a large scale wireless networks with multiple co-located Access Points (AP), a load balancing policy or optimal AP selection procedure is required for the distribution of the Mobile User (MU) to the AP's, in a way to maximize the network performance. The existing algorithms, which are considering the Received Signal Strength Indicator (RSSI) value as metrics, does not utilizes the radio resources properly and as a result more STAs associates with a single AP due to strongest signal and affects on the overall network performance degradation.

WLAN is widely used in office and public areas. In these large WLAN networks, Radio Resource Management is very important for the efficient use of wireless medium. As an example, since three channels (1, 6 and 11) can be used simultaneously in IEEE802.11b WLANS, APs
have to be installed to reduce the overlaps between the same channels and to reduce interferences between STAs using the same channel. When a STA enters an 802.11 WLAN, it scans all the 802.11 channels and sends association request to the APs. If the AP authenticates the STA then the STA gets associated with the selected AP.

3.2 AP Selection Strategies

The AP selection strategies concerns two primary issues. The first is how to the measure the traffic loads in an access point. Secondly how to select an AP so that balance or load in a wireless LAN is optimally distributed. In the literature various kinds of AP selection mechanisms have been proposed. Depending on which part of the network is responsible for such managements, these protocols could be classified into two categories Centralized and Decentralized approach.

3.2.1 Decentralized Strategy

In a decentralized approach, STAs learns the load status in an AP somehow and, accordingly, select an AP that maximizes potential bandwidth [5]. An AP acts passively in the whole selection process. Most of the centralized AP selection mechanisms are not designed to balance
load system wide rather STA selects AP for their own interests. The load in an AP can be realized in several ways. A STA may know the channel utilization or the delay between the scheduled and actual transmission time of periodic Beacon frames [5]. In such approach, the AP may let the STA to know about channel load by simply broadcasting its current STA population and traffic level in Probe Response or Beacon frames [5], preferably with a QBSS Load element if the AP supports IEEE 802.11e. In [9], a STA briefly connects to each available AP for performance test and select the best eventually. The STA-AP association management can be carried out either in a static or dynamic fashion. In static cases, a STA performs AP selection prior to its association with the target AP and does not re-associate to other APs as long as the association holds. A drawback of static AP selection is the inflexibility to adapt to network dynamics. With dynamic AP selection, a STA may re-associate with another AP even if the current association still holds. Dynamic AP selection shows better performance in a network which is highly dynamic. But this technique may cause the WLAN unstable (ping-pong effect) state. To avoid ping-pong effects, either static AP selection should be used or there should be a way to distribute re-associations in the temporal domain. For instance, in [10] a STA periodically searches for the best AP that has the least load. When the best AP found is
different from the previous one, the WS does not switch to that AP immediately but generates a random value. The STA can switch to the best AP only after the AP has been identified the best for the successive times. As in centralized approach STA select APs for their own interests, these approaches generally do not lead to a network-wide load balance. An alternative is to distribute load by a network-side entity.

### 3.2.2 Centralized strategy

In a centralized approach [8 11], STAs behave passively in modifying AP-STAs associations. It is a network-side entity (could be an AP, a switch, or a dedicated server) that controls the distribution of AP’s load. There are three basic techniques for APs to control their own load level

#### 3.2.2.1 Coverage Adjustment

Heavily loaded APs can reduce the transmission power of their beacon signal so that new STAs are less likely to discover them. APs may contribute each other in adjusting their radio range patterns in a way that less-loaded APs cover maximum area than heavily-loaded APs; and there is no coverage hole to ensure continuous coverage [14].
3.2.2.2 Admission Control

In this mechanism each AP contains an admission [15 16 18] controller which is responsible for accepting new connections or not. An AP may simply reject or accept new connections to the STA depending on the network load conditions. The request can be granted only when the predicted load level after the association does not exceed some threshold.

3.2.2.3 Association Management

A crowded AP may issue explicit de-association frame to selected STAs which are associated with it so that notified STAs would re-associate with other lightly-loaded APs. Theoretically, the best disassociation candidate is the one for which there exist an optimal association in another AP and balances the load among APs in the WLAN.

3.3 Centralized Vs Decentralized approach

In centralized approach, the association and re-associations are controlled by a centralized entity which can be a switch, AP or some dedicated server. If the centralized entity ever becomes malfunctioning then the entire process of association and de-association is affected. Moreover the link between STA and central node may become...
bottleneck potentially and resulting affect in the whole process of AP selection. In centralized approach the STA behaves passively.

But in decentralized strategy the selection procedure is located within the STA itself hence no central control is there. The STA makes the optimal association or de-association based on various information conveyed in beacon frames. Therefore there is no distributed affect in the decision making process of AP selection. In decentralized approach STA behaves actively.

When centralized servers are used for association then the latency taken during the HO (Hand-Over) procedure will increase and significant delay may affect on the performance of the WLAN. But in decentralized strategy, the STA itself makes HO decision, and thus the latency is greatly reduced.

The decentralized approaches do not have a global view of the WLAN and therefore it does not have a customized association, de-association and balancing load among APs in the WLAN, but they have the potential advantage of exploiting off the-shelf APs without much modification. On the other hand the centralized strategies do not require
modification in STAs. Centralized strategies AP selection can provide system wide load balance at the time of high traffic congestions. But deploying AP selection mechanism centrally produces an overhead in the system installation and also it may create problems when the central controlling server ever becomes malfunctioning.

Both centralized and decentralized strategies have their own advantage and disadvantages. As studied in literature, it is an open debatable issue.

3.4 Challenges in AP Selection

In IEEE 802.11 WLAN a station has the right to select an AP to which it will associate. But the selection of the AP is a complex issue due to the following challenges. The challenges are outlined and explained below.

1. **Distance**: Station near from the AP communicates in higher data rate. The common approaches for assignment of AP are based on RSSI value. As shown in figure 3.1 the stations get associated with the AP nearby it from which it getting strongest signal and as a result spatial non uniformity causes traffic convergence in a particular AP. As shown in the figure 3.1
2. **Number of STA:** Considering number of STA associated with an AP does not always lead to the better channel utilization because the required data rate for various traffics are different. As shown in figure 3.2, more stations are associated with AP1 but the traffic load is less in AP1 than AP2 because the required data rate of STAs is less than the data rates of the STAs associated in AP2.

3. **Mixed WLAN environments:** with the wide popularity of real time traffic applications like video conferencing and VOIP has got many attentions. The real time applications are very much delay and bandwidth sensitive. For ensuring QoS, the MAC layer has to provide adequate support for providing services to real time traffics. The challenge is that the legacy AP treats each traffic as best effort traffic
Figure 3.1: Congestion due to maximum association

Figure 3.2: Load imbalance
3.5 Prior Works

The basic and preliminary AP selection mechanisms for load balancing among APs consider only RSSI (Received Signal Strength Indicator) and the number of STAs connecting to an AP. But considering only RSSI [5] for load balancing leads to traffic congestion and produces lower performance. In this section we describe the important and relevant research works that we have come across during the literature survey related to this PhD work.

In [7], the authors have presented a decentralized AP selection mechanism by considering the control metric Signal Strength, throughput, and AP's load. In the proposed mechanism they have derived a function namely Eligibility of Access Point, (EoAP), which is a function of signal strength, throughput, and channel speed, considered in appropriate AP selection by the stations. For each discovered AP, in particular WLAN the signal strength and channel speed is computed and when the association between STA and AP is established then the throughput is estimated actually by transmitting TCP/IP packets. When a mobile node starts up, the algorithm for AP selection is operated, and function EoAP is automatically evaluated.
EoAP = SS% × TP × LF. SS%

Where SS% is the signal strength of the received AP which is usually converted into a percentage, while TP means the network throughput when transmitting data. Loading Factor (LF), defined as LF = TP / channel speed, reflects the current load of the access point. Channel speed is the transmit rate of the current channel between the mobile node and associated AP. Finally, the access point with the largest EoAP is selected for association.

As very advantage of this AP selection mechanism is that it considers the load factor and channel speed as control metric and thus achieves efficient utilization of radio resources.

The weak point we have observed in this mechanism is that it considers only best effort traffic only. Therefore traffics with real time traffic experience lower throughput and bad QoS.

In [5] the authors have designed a new AP selection mechanism to overcome the problems as shown in figure 3.2. and figure 3.3. The proposed new mechanism for AP selection is called HRFA (High Rate First Association) [5]. In this mechanism the authors have considered three metrics Transmission Rate, Channel Load in AP and real-time traffic load in an AP. Transmission rate is used to communicate with an AP is determined by LA (Link Adaptation) algorithm implemented in
STAs. Channel load and real-time traffic load in an AP are conveyed to STAs through the QBSS [5] load element in beacon frame.

Their proposed strategy considers both real-time traffic and non real-time traffics. Traffics from STAs with real time are accepted by admission controller implemented in the AP. In this mechanism STA with real-time traffic selects an AP whose real-time traffic load is less. But if there is a difference in load among various APs, the STA selects an AP, with which it can communicate using higher transmission rate, in order to efficiently utilize radio resource.

The first advantage of this proposed mechanism is that, by considering transmission rate and channel load level, this strategy justifies to the utilization of radio resources. Moreover this AP selection mechanism also provides a way for justifying real time application from non real time application.

The weak point we have observed in this mechanism is that it is a decentralized AP selection mechanism. The STAs do not have a global view of the WLAN. In certain situations the frequent association and de-association mechanism may result in ping-pong behavior in to the WLAN.
In [17] the authors have represented two mechanisms for improving QoS in a WLAN for both real and non real time traffic. They have first derived an analytical model for specifying upper bounds for both delay means and variations for services of different priorities in the non-saturated 802.11e WLAN. Their proposed mechanisms include one admission control mechanism and a rate control mechanism to ensure that QoS requirements of real-time traffics are statistically guaranteed and at the same time the best effort traffics can effectively utilize the residual bandwidth.

Their admission control mechanism namely CAC (Call Admission Control) uses the concept of imposing quota on the channel utilization due to the real-time traffic [5 17]. They have given maximum channel utilization for real time traffic but leaving some portion of the bandwidth for best effort traffic so that the best effort traffic is operational all the time.

The transmission rate of the best effort traffic is determined by Rate control algorithm which is conducted basically at the wireless nodes.

Their proposed mechanism [17] clearly shows an improvement in the QoS of real time traffic but the weak point of this algorithm is that it does not consider the greedy station problem; where upon the stations
with higher priority always gets more opportunity for packet transmission due to reservation in channel utilization. Reservation in channel access does not ensure efficient channel utilization directly because traffics of higher category may not exist in particular situations and also by accommodating more traffics of higher category can affect other traffics QoS.

In [18] the authors have proposed an adjustment method for QoS parameter by dynamically adjusting the CW values. Their proposed scheme adjusts the QoS parameters in the AP. The AP distributes the changed QoS parameters in wireless LAN within transmission range. Two-way handshaking mode of EDCA is good for real-time traffic, and by using the RTS/CTS helps resolving the hidden/exposed terminal problem. Proper adjustment of maximum CW value of real-time traffic produces efficient channel access for higher priority ACs and at the same time the non real-time traffics get better chances to access the residual channel bandwidth.

The advantage of their proposed mechanism is that the default EDCA parameters alone don't sufficiently improve the QoS performance of real-time traffic; rather it produces increased data drops. So with their proposed scheme [17] for adjusting the CW values dynamically
depending on the network conditions they have achieved better throughput from simulation.

But the dynamic tuning of CW values may increase the overhead in a QAP when there are a significantly large number of real time transactions and frequent association and de-association and it may lead to some unstable state of the WLAN.

3.6 The 802.11 MAC Sub-layer Protocol

The IEEE 802.11 MAC defines three types of messages: data, management and control. Management messages are used to support the services described in section 2.6. Control frames are used to support the delivery of data and management messages. Data frames carry higher layer information. The general MAC frame format is depicted in Figure 3.3. Each frame consists of a MAC header, a variable length frame body and a Frame Check Sequence (FCS), which contains an IEEE 32-bit CRC. The MAC header comprises several fields:
Frame Control: consists of several subfields and flags that contain relevant information for STAs in power save mode. It also includes information about the frame type, fragmentation, etc.

Duration/ID: vary with frame type, but it is usually set to the time (in $\mu$s) required to complete the current transmission.

Address Fields 1 to 4: used to identify the BSSID, the source address, the destination address, the transmitting STA address and receiving STA address. The contents of the address fields are dependent upon the values of the To DS and From DS flags in the Frame Control field.
**Sequence Control:** used to number a MAC Service Data Unit (MSDU) and to identify fragments of a given MSDU.

**Data:** The MAC frame may contain arbitrary data (maximum 2,312 bytes) which is transported transparently from a sender to a receiver.

**Checksum (CRC):** A 32 bit checksum is used to protect the frame.

The frame control field shown in figure 3.3 consists of the following fields.

**Protocol version:** The 2 bit filed indicates the current protocol version and it is fixed to 0 in current standards (802.11).

**Type:** The type filed specifies the type of the frame: management (=00), control (=01) or data (=10). 11 is reserved.

**Subtype:** Indicates frame sub type. It's a 4 bit filed. Example subtypes for management frames are: 0000 for association request, 1000 for beacon. RTS and CTS control frames are coded with 1011 and 1100 respectively. User data is transmitted as data frame with subtype 0000 and etc.
**ToDS:** When this bit is set it indicates that destination frame is for DS

**FromDS:** When this bit is set it indicates that frame coming from DS

**Retry:** This bit is set in case of retransmission of a frame. With this bit set it is possible for the receiver to eliminate duplicate frames.

**Power Management:** This bit is set when station goes in Power Save mode (PS). If this bit is set to 0 this station remains active.

**More fragments:** This filed is set when all data or management frames that have another fragment of the current MSDU to follow.

**More Data:** This bit is set when frame is followed by other fragments. This can be used by an Access point to indicate to a station in power save mode that more packets are buffered.

**WEP:** This filed indicates that the standard security mechanism of 802.11 is applied. However due to the drawbacks of WEP algorithm some higher layer security should be used to secure an 802.11 network.
**Order:** This bit is set to indicate that the received frame must be processed in strict order.

The 802.11 MAC [4] protocol is quite different from 802.3 due to the property of wireless links. In wired Ethernet connections a user is able to detect when a collision has taken place because a network card is setup to be able to transmit and receive on different physical wires that make up the actual Ethernet cable. This is not possible in wireless Ethernet because, when a wireless LAN card is transmitting it can not listen to detect if packets collide. With Ethernet, a station just waits until the ether goes silent and starts transmitting. If it does not receive a noise burst back within the first 64 bytes, the frame has almost assuredly been delivered correctly. With wireless, this situation does not hold.

To partially cope with the inability to detect a collision, the IEEE 802.11 standard attempts to avoid collisions using carefully designed waiting periods that allow multiple users to defer access to the shared wireless channel to one another. That is, IEEE 802.11 clients will always ensure a channel has been idle for a certain period of time before transmitting. The Wireless MAC protocols falls under two categories: Decentralized and centralized.
The decentralized MAC protocols are not based on some central controlling policy. These protocols are simple in terms of implementation, because it does not require much overhead and relatively less complex. DCF is one of the examples of distributed protocol in IEEE 802.11 standard. The basic mechanism of distributed protocol is based on the principles of CSMA [4], which is explained in the following sections.

In contrast to decentralized protocols, centralized protocols like Time Division Multiple Access (TDMA), polling or scheduling schemes have got more importance as domain of good research as they ensures QoS guarantees to some level. PCF is one of the examples of centralized MAC protocol in IEEE 802.11 standard. The working principle of DCF and PCF is explained in the following sections,

3.6.1 DCF (Distributed Coordination Function)

When DCF is employed, 802.11 uses a protocol called CSMA/CA [4, 20] (CSMA with Collision Avoidance). CSMA/CA uses both physical carrier sensing and virtual carrier sensing.

In physical carrier sensing, when a data packet is ready for transmission, a client will first sense the medium. If the medium is idle
for a period of time defined as the Interframe Spacing (IFS) period [4]. There exist four kinds of IFS frame spacing.

- **SIFS** (Short IFS): Is the time waited between packets in an ongoing dialog (RTS, CTS, data, ACK, next frame)

- **PIFS** (PCF IFS): when no SIFS response, base station can issue beacon or poll.

- **DIFS** (DCF IFS): when no PIFS, any station can attempt to acquire the channel.

- **EIFS** (Extended IFS): lowest priority interval used to report bad or unknown frame.

When the IFS period expires, the packet can be immediately transmitted. If this transmission is not successful the user again defers its transmission. This is done using a Network Allocation Vector (NAV) [4 20] that is nothing but a timer. To initiate NAV the sender extracts the field in the header of the packet which is currently being transmitted.
indicating how long the sender uses the medium for the current transmission. In this way the client does not need to continue to sense the state of the channel until the NAV timer has expired.

When the NAV timer expires or the sender senses the medium no longer to be busy, the sender will backoff. In backoff, a sender chooses a random number. This random number is chosen from the interval between 0 and the value of the Contention Window (CW) using binary backoff exponential algorithm.

When the backoff interval is chosen between 0 and CW value and if the medium found idle for IFS period, then the sender starts decrementing from that random number. While decrementing the station or sender also listens to the carrier if it becomes busy then the backoff counter is frozen and the sender enters a defer state.

If the medium is free for IFS period and remain so while the backoff counter reaches to zero then the sender transmits its data frame. If the client discovers that the transmission has failed then the client must exponentially increase the value of CW using binary exponential backoff algorithm [20]. The DCF implementation of IEEE 802.11 does not handle a problem referred to as the hidden terminal problem [20].
The hidden terminal problem occurs when all wireless stations do not belong within the radio range of each other. The transmissions going on in one part of a cell may not be sensed elsewhere in other part of the same cell. In the example shown in figure 3.4, station A is transmitting to station B. If C senses the channel, it will not hear transmissions from A because it is not in the radio range of A, and falsely conclude that it may now start transmitting to B. And as a result collision occurs at station B.

![Figure 3.4: Hidden-Terminal problem](image)

**Affect of Hidden Terminal**

- More collisions
- Wastage of resources

The exposed terminal problem as illustrated in figure 3.5 is the inverse of hidden terminal problem, Here B is transmitting to A. C is not
within the radio range of A but in the range of B and D. Now C wants to send to D so it listens to the channel. Then it hears a transmission, and falsely assumes that it may not send to C and C prohibits its transmitter from transmission. Where upon C could easily transmit to D.

Figure 3.5: Exposed-Terminal problem

Moreover the wireless links are mostly half duplex, meaning that they cannot transmit and listen for noise bursts at the same time on a single frequency. As a result of these problems, 802.11 does not use CSMA/CD, as Ethernet does.

**Affect of Exposed Terminal**

- Underutilization of channel
- Lower effective throughput
To solve the problem of hidden and exposed terminal problem, IEEE 802.11 adds optional RTS/CTS mechanism. In this technique instead of immediately transmitting a data packet after waiting for an IFS period, STA will transmit a short Ready To Send (RTS) packet to access the medium for a fixed period of time. If this succeeds, the receiver quickly responds with (after a SIFS period) a short Clear To Send (CTS) packet. After the successful exchange of an RTS/CTS pair the actual transmission takes place. With this method any station who gets a RTS or CTS know how to access the medium using the NAV functionality described above.

Figure 3.6: Resolving Hidden-Terminal problem with RTS/CTS

The hidden terminal problem is revisited in the presence of RTS/CTS as shown in Fig 3.6. When A wants to transmit to B then it
starts with by sending a RTS packet to B. B responses by sending a CTS. The CTS is over heared by C also. C inhibits its own transmitter to the time given in CTS. And as a result A successfully sends DATA to B.

![Diagram](image)

Figure 3.7: Resolving Exposed-Terminal problem with RTS/CTS

In figure 3.7 we have revisited the exposed terminal problem in the presence of RTS/CTS. When B wants to send to A it starts out by sending RTS to A. The RTS is also received by C. A sends CTS to B but C cannot hear the CTS because it is not within the radio range of A. C assumes A is either down or out of range and hence C does not inhibit its transmissions to D.
The RTS/CTS mechanism reduces the chances of collision but cannot eliminate entirely as RTS packets can collide itself. But collisions of RTS frames are not regarded to be costly as compared to the collisions of data frame in CSMA due to the fact that RTS frames are much smaller (30 bytes) than DATA frames. Therefore wireless mediums are very much unreliable because of collisions. To ensure reliability, DCF uses positive Acknowledgments after each successful reception of data frame by the receiver. If the ACK is not received in the SIFS window, then transmitter concludes that there was some collision and goes in to retry procedures. The DCF channel access is illustrated in Figure 3.8.
3.6.2 PCF (Point coordination function)

Another optional protocol that is part of the IEEE 802.11 standard is the Point Coordination Function (PCF). In DCF mode, there is no central control, and stations compete for the medium, just as they do in Ethernet. The other preferred mode is PCF [4 20], where the base station polls other stations, asking them if they have any data to send. The basic mechanism is for the base station to broadcast a beacon frame periodically (10 to 100 times per second). The beacon frame bears system parameters, like hopping sequences and dwell times (for FHSS), clock synchronization, etc. It also asks new nodes to get in polling service. As transmission sequence is completely controlled by the base station in PCF mode, therefore no collisions ever occur.

When a station has signed up for polling service at a certain data rate, it is effectively entertained with a certain fraction of the bandwidth, thus making it possible to provide QoS guarantees. More over PCF and DCF can coexist within the same cell. At the very first sight, it might seem impossible to have central control and distributed control operating simultaneously, but 802.11 provides a means to accomplish this goal. It functions by carefully defining the inter frame time interval or inter framing space. After a frame has been transmitted, a certain amount of idle time is required before any station starts sending a
frame. Four different intervals are defined, each for a specific purpose. The four intervals are described in the previous section.

The major advantage of the centralized protocol, PCF is that it assures QoS guarantee once associated with a network. But from the literature it is also observed that, that the adoption of these mechanisms is confined due to several drawbacks like overhead, relatively more complex to implement and issues of expandability.

### 3.7 Limitations of PCF and DCF

The DCF mode has many advantages because of its simple in terms of implementation and suitability for data applications. But DCF has some serious drawbacks as it only supports best effort traffics. Real-time traffics are not supported in DCF. Real Time applications are sensitive to some attributes like bandwidth, delay, and jitter guarantees. The point is explained in the previous sections that with DCF, all the STAs compete for the channel with the same priority. There is no differentiation policy among the traffics for providing guaranteed QoS for real-time multimedia applications. It seen in the literature that DCF shows high variation of throughput, delay and relatively poor performance for audio transmission.
As PCF was designed to support Real Time applications, but it has been experienced inflexible for doing the same due to some major drawbacks and as a result it leads to poor QoS. PCF defines a single-class round-robin scheduling algorithm, and hence it cannot tackle the claimed QoS requirements from various types of traffics. Moreover it is very much difficult for PCF to control the transmission time of a polled STA. When a STA is polled then it is allowed to send a frame segment of any size in between 0 and 2304 bytes, and as a result variable transmission time is needed. In addition to this, the PHY data rate of an already polled STA may change according to variable channel situations. And hence the AP is not able to determine the transmission time exactly. This forbids the AP from providing guaranteed delay and jitter performance for other STAs engaged in the polling list during the rest of the CFP interval.

Both DCF and PCF do have a common QoS [18] problem as no admission control mechanism is specified in the 802.11 legacy MAC. When traffic load is very high, the performance of both functions can be degraded and QoS requirements are not satisfied.
3.8 QoS

In the literature various mechanisms have been proposed for improving the QoS performance in a WLAN. From the literature we have gathered the following QoS issues and adequate properties for QoS support mechanisms in a WLAN. From the observations it is seen that there exist some differences among the various properties of QoS. While some QoS performance is achieved others are scarified. There should be a sort of balance required to get optimal QoS support in such WLANs.

3.8.1 QoS Characteristics

The QoS mechanisms should have a certain amount of fairness, specifically when it comes for improving throughputs. Without fairness various traffic classes may experience unjustified bandwidth distribution.

The QoS mechanisms should be designed with minimal or no changes to the existing MAC standards of IEEE 802.11/11e [5 16 17 18] so that the proposed mechanisms are easily compatible with the current standard and thus easy to implement and adopt.

The QoS mechanisms must be designed to support high scalability. That means the QoS performance should not be affected when more active connections having different data rates exist at the same time.
The QoS mechanisms must provide throughput services with minimal variation. Because the performance of real-time applications strictly relies on the stability of the available channel bandwidth.

The QoS mechanisms must be carried out with minimal computational complexity. We know that without simplicity it is not possible to get wide acceptance of any mechanisms.