The challenge of High Density Heterogeneous Wi-Fi Networks

Definition, Analysis, Recommendations
Contents

Introduction ........................................................................................................................................... 3

Problem Definition ................................................................................................................................. 3

Distributed Medium Access Control .................................................................................................... 3

Implications for HDH networking ........................................................................................................... 4

Numerical Analysis ................................................................................................................................. 5

Sources of heterogeneity .......................................................................................................................... 5

Analysis ................................................................................................................................................... 7

Impact Assessment .................................................................................................................................. 8

Coverage ................................................................................................................................................ 8

Throughput ............................................................................................................................................ 8

Reliability .............................................................................................................................................. 8

QoS ........................................................................................................................................................ 8

Recommendations for high Density Wi-Fi Networking ........................................................................... 9

Network Configuration and Management ................................................................................................. 9

Dynamic RF parameter control ............................................................................................................... 10

Summary ................................................................................................................................................ 11

References ............................................................................................................................................. 12
Introduction

Wi-Fi technology has seen a meteoric rise since its breakthrough in the late 1990’s. In the early years it was envisioned as a low-cost cable replacement but soon its suitability as a means to connect the emerging laptop computers to wired Ethernet became apparent. It was leveraged initially by Apple as a means to push the sales of its new notebook computers and the industry as a whole rapidly followed suit.

Today the dominance of the smartphone and tablet computers are moving Wi-Fi up another level of usage and ubiquity – thanks, in part, to the inability of the mobile networks to carry the vast amounts of internet traffic generated by these devices.

The result is that Wi-Fi is entering a new territory – that of High Density, Heterogeneous (HDH) networking. “High Density” refers to the number of devices per area, “heterogeneous” refers to the variety of operating modes and device properties of Wi-Fi devices on the market. The IEEE 802.11 standard is one source of variation: it evolves continuously and adds new operating modes and new protocol details. In addition, vendors tailor the RF properties of their Wi-Fi devices to typical applications. For example, a smartphone does not need a powerful transmitter but working at a low power level saves cost and improves battery life, advantages that users appreciate.

However, the potential impact of device property spread was not foreseen by the engineers that devised the original IEEE 802.11 standard that underlies all Wi-Fi equipment. This short white paper defines the problem, analyses its severity and consequences and recommends ways to deal with it. Since the problem space is both rich and complex, a single paper would not suffice and therefore this document concentrates on the root causes and the basic approaches to addressing their consequences.

Problem Definition

Distributed Medium Access Control

Wi-Fi owes much of its success to its flexibility and robustness in practical use. Unlike mobile telecom network technology which relies on base stations, Wi-Fi devices have the means to share the RF channels available. This obviates the need for complex coordination procedures.

---

1 A more in-depth treatment of spectrum sharing is given the Kruys&Qian, Sharing RF Spectrum with Commodity Wireless Technologies, Springer 2011.
2 The IEEE 802.11 standard on which Wi-Fi is based defines a second mode of medium access based on a “Point Coordination Function”. This allows the access point to control its clients, in a way similar to a mobile telecom system. This mode has never received much support because of the lack of RF channels in the 2.4GHz band and the complicated coordination between access points that would be required.
while preserving the ability to function in the face of unfavorable deployment conditions and high density of use.

Wi-Fi networks consist of access points connected to a wired backbone – typically Ethernet – and (mobile) client devices. All share the same RF medium or RF channel. The mechanism underlying Wi-Fi’s medium access control is the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. This protocol is basically a politeness protocol: Wi-Fi devices listen before transmitting and apply a few simple rules of contention to avoid stomping on each other’s transmissions:

1) listen if the channel is free for a defined period of time, if so transmit;

2) if the channel is not free, start a counter at a random value and down count that while the channel is free;

3) once the channel is free, transmit.

The minimum time the channel must be free has been chosen such that the Acknowledgement received in response to a frame transmission is also covered. In effect, the contention process (the down counting), the transmission of a frame and receiving its Ack are bound together in one “atomic” operation. The figure below depicts this for a Wi-Fi access point sending a frame to a client device.

The key elements of this protocol are common values for the detection of channel occupation, for the transmitter output power and for the contention window size.

**Implications for HDH networking**

Although extremely flexible and resilient, this distributed medium access control has a price: it spends part of the channel capacity on sharing procedures and it assumes device homogeneity: all participating devices have the same RF properties: notably bandwidth, RF power output and receiver sensitivity.

The cost of medium sharing varies with the size of the contention window (the counter). A large window makes collisions unlikely but wastes time; a small window is efficient but risks wasteful collisions. Careful management of the window size assures optimal efficiency. Even in high density conditions, the time that the channel is idle because of the contention process is limited
to a few multiples of the interval between frame and Ack transmissions. Practice shows that the medium sharing process is quite efficient in distributing the available channel capacity over all devices – access point and clients.

The cost of device parameter spread is more difficult to assess. The CSMA/CA protocol works fine when all devices have the same detection threshold and the same output power level in the same bandwidth. Ideally all devices that share a channel should hear each other so that costly collisions on the channel are avoided. However, mixed low power and high power devices makes this “all hear all” impossible and therefore collisions are unavoidable. This is further aggravated by some devices being in exposed locations whereas others are worn on the body or carried in bags and other gear. The result is not only a wide variety of properties between devices but also, for each device, a large variation in the sensitivity and RF power output for a given direction. Some devices may hear each other, some may not. This asymmetry will result in collisions on the medium that reduce its capacity. Practice proves that, at high densities, such collisions can make it impossible for low power clients to communicate effectively or to complete the association process that precedes actual communications. Other consequences of a high collision frequency range from the blocking of TCP traffic to temporary blockage of an RF channel.

The reason this subject has not emerged earlier is that in most Wi-Fi networks, certainly in the vast majority of home networks, the actual loading of the RF channel is but a fraction of the potential capacity and therefore inefficiencies caused by collisions go mostly unnoticed. In HDH networking this benign situation is no longer the case and the problem emerges in all its complexities and unpredictability.

**Numerical Analysis**

This section gives a quantitative analysis that indicates the potential damage that spread of RF parameters (i.e. the heterogeneity) and environment may cause in high density Wi-Fi networks.

**Sources of heterogeneity**

**RF parameter spread**

The RF parameters concerned are transmitter output power, transmitter bandwidth, receiver sensitivity and contention threshold. Of these, transmitter power is the most important. Bandwidth mostly has a statistical effect – it affects the number of devices affected more than it impacts their transmissions. Receiver sensitivity and contention threshold tend to have much lower spreads than transmitter power because most chipsets are roughly comparable in this respect. However, actual receive conditions always affect the strength of the received signal.

---

3 This condition also underlies the “hidden node” syndrome that is recognized in the literature but for which no effective solution has been developed to date. The IEEE 802.11 defines a mechanism to reduce the impact of hidden nodes by means of a probe by the transmitter (called RTS) and a response by the intended receiver (called CTS) prior to the transmission of a frame. In HDH networks, these short RTS/CTS frames are equally subject to interference and therefore do not solve the problem.

4 See Reference 2] for a detailed analysis of
Transmitter output power varies widely between devices, in some cases even within the same brand. Whereas the typical laptop generates 50 to 100mW RF power, the typical smartphone may not exceed 1 mW. Similar values have been seen for such different devices as handheld scanners and RF ID tags. The reasons are primarily reduced device cost and reduced power consumption. Expressed in dBs the observed spread is 20dB but it can be more or less in practice. For the purposes of this document the conservative value of 17dB will be used.

RF propagation conditions

RF propagation conditions vary with the environment and the relative position of devices. In large open spaces, the variations are limited but in offices, schools and similar buildings propagation paths can be very variable and complex, as shown below.

The actual variation depends on the obstacles and the materials they are made of between sender and receiver. The range of variation observed lies between 3 and 20 dB; the latter reflects highly isolating walls or floors of e.g. concrete. For the purposes of this document, a conservative 13 dB will be used as the typical delta in propagation conditions.

Usage patterns

Portable devices are ported in many ways – people carry their smartphones in a (short) pocket, attached to a belt or in a briefcase stuffed with other things. Scanners and personal monitoring devices are typically body worn or in close proximity to the body and therefore the orientation of the body relative to the transmission path between client and access point becomes a major factor. Depending on the actual device position and distance to the body of the wearer, the RF impact varies between 0 and 13dB. For the purposes of this document a conservative value of 7dB will be used and applied only to client devices, not to access points.
**Analysis**

A crucial factor in the operation of the Wi-Fi protocol is the detection of other transmitters. Any Wi-Fi signal that exceeds the contention threshold\(^5\) – which is typically -85dBm – is taken as a sign that the channel is occupied.

Taken together the above spreads in RF power and RF propagation factors adds up to 37dB or a factor 5000. This should be compared to the 60dB range of signal attenuation between a 17dBm transmitter and the contention threshold of a distant receiver. The implication is that detection range varies widely. For a benign propagation environment the spread in detection range could be between 150m and 16m. In a highly attenuating environment such as a factory of hospital, the spread in detection range can easily range from a high value of 64m to a low value of 10m.

In a high density network these differences translate directly into number of potential interferers: low power devices or devices in unfavorable conditions will not be heard by many other devices whose transmissions will cause collisions. In general, the potential for collisions rises rapidly with the increasing spread in RF parameters, and divergence in propagation conditions. The impact depends on the overall structure of the environment: a high density network in a transparent environment will experience more problems than a network deployed in an “isolating” environment.

The following figure gives a schematic representation of the above discussion: number of access point operate on the same channel and their coverage areas overlap in some way. Because they detect each other, their transmissions will not collide. However the low power client device is not visible to AP1 and AP3. Therefore, the transmissions from the client to AP2 are subject to interference from the other two access points\(^6\) as well as from all high power clients that share this area and this channel.

\(^5\) For simple energy detection, this threshold is 20dB higher (=less sensitive).
\(^6\) In addition, AP2 must contend with the two other access points and therefore its throughput will be reduced.
In this example the detection ranges differ by a factor three. Assuming a homogeneous distribution of clients, and every third client being a high power client, every low power client is subject to potential interference from at least three high power clients. Whether this has effect on the communications of the low power clients depends very much on the traffic load of the channel. At high loads, the channel is almost continuously occupied and the change of collisions is high. Another effect of parameter spread is that the low power clients will have difficulty gaining access to the channel: because their contention threshold is similar to that of other devices, they will see a very busy channel. Combined with the high probability of collisions, the result is very poor network performance as seen from the low power devices.

This example gives a somewhat optimistic view of things because the chosen delta in detection distance is small – a factor 3. In many cases this factor will be 6 or more and the probability of collisions will be correspondingly higher and addressing the problem effectively will be more difficult.

**Impact Assessment**

The impact of RF variability on Wi-Fi networks becomes visible in 4 aspects:

**Coverage**
The usual models and programs for Wi-Fi network planning assume a certain pathloss model – for example exponent 2 (=free space) up to 4m, exponent 3 between 4 and 16m and exponent 4 beyond that. As the preceding discussion shows, such models give rough approximation at best and provide no certainty of coverage.

**Throughput**
Throughput various with range but it also depends on the number of devices sharing a given RF channel and the amount of traffic they put on the channel. The worst case throughput – disregarding hidden nodes and other network degradation factors – is therefore determined by the number of access points which operate on the same channel and are in contention detection range

**Reliability**
A major cause of network performance degradation is the occurrence of hidden node situations: devices that are not visible to other devices operating on the same RF channel. Depending on the nature of the hidden node effect and the relative traffic loads of the devices concerned, temporary but severe reductions in medium access and/or throughput may occur.

**QoS**
Even if overall network reliability is reasonable, good QoS, necessary for VoIP and video services, may be not be possible. The degree of degradation will vary with location and traffic loads and the cause hard to localize.

All of the above effects are amenable to proactive and or corrective treatment. This is discussed in more detail below.

---

7 Note that this effect is independent of the ratio between downlink and uplink traffic loads.
Recommendations for high Density Wi-Fi Networking

The main cause of network degradation in high density networking is RF variability caused by differences of devices, the environment and usage.

The degrees of freedom available to address these problems depend on the degree of control one has over the acquisition and use of client devices, the placement of access points and the predominant mode of client devices usage. In practice, the network operator has very little freedom of action if only because of the Bring Your Own Device policy that is gaining popularity rapidly. Any organization that serves the general public in one sense or another with find its options similarly restricted. Operational considerations may demand operation in complex RF environments. Further, users want to be free to use their pet devices in whatever way they want and this limits the opportunities for reducing heterogeneity as well. This leaves the reduction of the impact of RF parameters spread as the only option.

There are three ways to limit the impact of RF parameter spread: passively through (a) network configuration or actively through (b) dynamic RF parameter control. Both come down to reducing the spread during operations.

The following sections assume that the usual means of maximizing network reliability and performance are in place. These include spreading the client population over the available access points - this is also known also load balancing - and RF channels as well as auditing of the network's performance to identify and address short term or localized performance issues.

Network Configuration and Management

Wireless Network Configuration provides many opportunities to reduce the impact of device parameter spread by careful planning of access point location and channel choice. The goal is to achieve a small cell size to accommodate the low power clients while maximizing the attenuation between cells operating at the same frequency channel. This does require an increase in the number of access points to serve a given area. Avoiding that access points have to share the same channel requires putting them on different RF channels. In the 2.4GHz band, the number of channels is limited, typically 3 or at best 4. In the 5GHz band with its 19 channels, this strategy is more easily realized except when preference is given to using MIMO over 40MHz channels to achieve high transmission rates.

An added benefit is the opportunity to reduce the transmitter power of the access points so as to balance the operating range of the low power clients. By increasing the contention threshold as well, the size of Wi-Fi cells is reduced. This downsizing in effect increases the capacity of the RF channel occupied: more non-interfering cells can be deployed in the same area. A judicious choice of data rates will help to minimize inter-cell interference.

Reducing the power level of the access points reduces the ability of the network to deal with the asymmetry in traffic levels between downstream (=higher) and upstream (=lower). More traffic requires more throughput and therefore a higher modulation rate. The higher SNR required is served by a higher output power of the access points. The downside is the increased interference...
potential of the higher output power. This, in turn can be compensated to a degree if lower modulation rates with better interference resistance are used by clients.

Maximizing the benefits of isolating walls and objects is not easy and requires the use of powerful planning software that can accurately model the environment as well as clients with different properties. Further, access points can control the maximum RF power output of client devices so that high power clients can be throttled.

During operation, the network load varies with time and location and therefore it may advantageous to dynamically re-configure the RF plan of the network to optimize local capacity. Given a real time network performance audit capability, such reconfiguration can be largely automated.

Whereas the benefits of proactive network configuration described above are clear, there may be cases where this is not sufficient and additional means are needed. Isolation is one option. Isolation requires the grouping of similar devices on a specific RF frequency band or on specific RF channels. The effect is to reduce the de facto parameter spread so that its impact is largely reduced or even eliminated. This approach is easily implemented by allowing only certain access points to serve clients of a certain kind. A simple example is to reserve one RF channel in the 2.4GHz band for low power clients such as smartphones – e.g. those with a power level in the range of 1 mW.

Which of the above best serves a given network depends on its users and operating conditions and the degree of control one has over the types of client device being used on the network.

**Dynamic RF parameter control**

Whereas the benefits of the pro-active network configuration described above can be sufficient, dynamic RF power control offers the best possibilities to negate the reduce of RF parameter spread and to compensate to some degree for variation in the environment and usage patterns.

This form of control requires that access points control the main RF parameters of clients: their output power, their uplink data rate and their contention threshold. The IEEE 802.11 standard in its 2007 version provides the means to achieve that but implementation by vendors varies. The principle of this approach is to reduce the variation in the operational values of the RF parameters of all devices that have joined the network. This necessarily leaves devices that have not joined the network out but this is unavoidable.

Dynamic RF parameter control requires that the network keeps track of the power output levels of all clients and access points and to adjust them as necessary to avoid interference among access points and clients in the uplink as well as in the downlink. By adjusting the contention threshold of all devices and the data rates in the uplink as well as downlink, the network can optimize frequency re-use and therefore maximize capacity under the given conditions. All of this assumes that access points and client devices implement the necessary RF parameter management functions and related protocol. The price paid for this high level of control is

---

8 Through the Spectrum Management elements of the beacon and related protocol elements
twofold a) the overhead of management messaging - also on the RF medium - and the cost of the powerful controllers required to manage the RF “landscape” in near real time. Due to the dependence on these controllers, hot standby back-up may be considered necessary.

The following table summarizes the above and indicates how the various approaches affect Wi-Fi network performance.

<table>
<thead>
<tr>
<th>Performance factor</th>
<th>Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Detailed RF Planning</td>
</tr>
<tr>
<td>Coverage</td>
<td>Necessary</td>
</tr>
<tr>
<td>Throughput</td>
<td>Necessary</td>
</tr>
<tr>
<td>Reliability</td>
<td>Necessary</td>
</tr>
<tr>
<td>QoS</td>
<td>Necessary</td>
</tr>
</tbody>
</table>

**Summary**

The introduction of large numbers of low power WI-Fi devices such as smartphones and other personal devices changes the Wi-Fi landscape permanently, raising new challenges and opportunities. Wi-Fi technology, nor its underlying IEEE 802.11 standard take the mixed use of high power and low power devices into account. The variability of the environment and extensive portable use add to the difficulty of achieving and maintaining efficient network operation. Unless addressed thoroughly, this leads to significant user dissatisfaction that parallels the increasing ubiquity of these and similar devices.

The root cause of the problems occurring is the disparity between the narrow range of device parameters that underlies the design of the IEEE 802.11 standard and the very wide range of those parameters in practice.

The ways to address the problems vary from careful network planning and real-time optimization to separating different populations of devices and/or dynamic management of the client RF parameters. Which of these is appropriate depends on actual conditions and demands placed on the network. This short white paper may prove useful for those grappling with this complex subject.
References


4] Zach Epstein: “IDC Smartphone sales hit an all time high in Q4 led by Apple and Samsung.”