Advantages of Broadband Fixed Wireless Systems over 802.11 LANs

Redline Communications
90 Tiverton Court
Markham, Ontario
www.redlinecommunications.com

The demand for broadband services is growing at a rapid pace for both the residential and enterprise market. Existing wireline technologies, such as DSL and cable, are often not an option, either because they are simply not available in a given geographical area or lack the necessary performance to fulfill the requirements for high-speed connectivity – as such operators are turning to alternative means, such as broadband fixed wireless (BFW) technology, to provide a cost effective solution that can be deployed quickly and easily. Fixed wireless systems have been designed specifically for outdoor operations, to address environmental anomalies such as multipath and power fluctuations, and to provide high spectral efficiency for multi-user deployments. Some operators, in the hopes of reducing capital and operational spending, have turned to wireless local area network (LAN) solutions, based on the IEEE 802.11a/b standard, to fulfill their fixed wireless requirements. Wireless LANs are competitively priced, due to their relatively simple design and wide availability (multi-vendor sourcing cost advantage), and are easy to install (self-install). In some cases, operators have successfully demonstrated WLAN operation in an outside environment, making the proposition attractive for small operators such as Wireless Internet Service Providers (WISPs). However, as will be examined in this paper, there are several shortcomings of wireless LAN systems for delivering broadband fixed wireless services relating to issues such as multipath, throughput performance, interference, regulatory compliance, Quality of Service (QoS), and security.

Multipath

Wireless LANs are designed to operate indoors over relatively short ranges, i.e. < 500 ft. In a typical enterprise or residential setting, the signal from the wireless LAN access point (AP) to the modem can reflect off of several fixed objects including walls, furniture and cabinets, creating echoes that trail the direct signal on the order of tens of nanoseconds. These echoes overlap with the direct signal in the receiver, creating a problem known as Inter Symbol Interference (ISI). The wireless LAN system comprises processing to effectively address ISI, providing the delay is relatively short. However, if the echoes trail the direct signal with greater delay (>500 ns), then the LAN receiver will begin to detect errors, invoking frequent re-transmissions, which will cause severe data throughput degradation. In a fixed wireless environment, where end-users are deployed several hundreds of feet to tens of miles away from the base station, multipath arising from distant buildings, trees, etc., will produce echoes on the order of 100’s to 1000’s of nanoseconds, well beyond the capability of the wireless LAN system to process and correct. Additionally, the BFW environment is highly dynamic (e.g. tree leaves moving from the wind) creating echoes that fluctuate in amplitude and phase well beyond what is typically processed by a WLAN system. BFW systems, on the other hand, are designed specifically to address these propagation anomalies.

It should be noted that some operators have deployed WLAN systems in a fixed wireless scenario over ranges of 6 to 10 miles with some success. The operator may have achieved First Fresnel zone clearance[1] (by installing the radio/antenna at very high altitudes) or most likely the prevailing climatic conditions were such that multipath reflections were not predominant at the time of installation. In either case, multipath is a time-variant phenomenon, which can change characteristics over different weather patterns and seasons – and hence, a favorable condition observed at deployment time is not representative of the propagation conditions that can and will likely prevail over the subsequent months. Many operators learned first hand the long-term effects of BFW deployments; having installed a wireless LAN system over several miles, successfully operating it for months, and then having to replace it with a dedicated BFW system because changing propagation conditions rendered the LAN solution inoperable. This is the 'hidden' cost of a WLAN system deployed outside of its intended environment.

A similar phenomenon was observed with cable modems in the past. Operators believed that a DOCSIS-based cable modem, attached to a radio transverter, would meet their fixed wireless deployment needs – after all, they had experienced success in deploying cable modems over the air for several months in a multipoint setting and at great distances, hence, it was difficult to argue the need for a dedicated BFW solution. Within a year from initial deployment, however, a disturbing trend developed – the modems began to fail one after another. It was discovered that the changing weather conditions caused multipath disturbances to become more prevalent, rendering the cable modems completely ineffective with their simple equalizers. Additionally, the temperature extremes caused the radios to alter their RF parameters, beyond what the cable modem could correct with its compensation circuitry. This turned out to be a very expensive lesson for operators who had hoped a simpler alternative solution would suffice.

Security

WLAN systems are known for their security deficiencies, which are only exasperated when they are operated outdoors in a BFW deployment scenario where the opportunity for breach is potentially greater. Although a WLAN system features wired equivalent privacy (WEP), there are several shortcomings with this scheme including: a) it has many theoretical security limitations, b) the encryption keys are widely known and shared, c) it does not provide end-system/end-user authentication, and d) when invoked, the system loses flexibility with regards to portability and ubiquitous coverage, which are the key attributes of a WLAN solution. Most BFW systems, on the other hand, have implemented algorithms to address security over a wide wireless network, with an efficient proprietary or commercial encryption scheme such as the data encryption standard (DES) II and III

Regulatory Emissions

Wireless LANs transmit at low output power levels, lower than what is typically needed to operate over the larger distances associated with fixed wireless deployments. To improve reach, operators are attaching high-power radios, amplifiers, and in some cases upconverters to their LAN devices, along with a high gain antenna. These augmented configurations are typically not approved by the regulatory agency, and often create serious out of band emissions and spurious noise that can spill into parts of the spectrum used by sensitive equipment including navigation systems associated with commercial air traffic. These modified LANs, known as rogue systems, have become a great concern with regulatory agencies worldwide, and steps are being taken to rectify the situation, such as banning outdoor use of WLAN systems.

[1] First Fresnel zone clearance is a mathematically specified distance that objects need to be from the direct path to ensure signal propagation is not affected by multipath disturbances.

Concatenation

WLAN systems do not include concatenation; a feature, which allows an end-station to send multiple packets in a single large burst on the upstream direction. Significant spectral efficiencies can be realized when a station is permitted to transport larger data payloads using the same overhead typically associated with the smaller packet sizes. Minimizing overhead promotes greater overall data throughput within the network. BFW systems typically feature concatenation, and hence offer the advantage of greater throughput and higher bandwidth efficiencies over WLAN solutions.

Fragmentation

Fragmentation is essentially the opposite of concatenation, in which a large upstream data frame is sliced into smaller grants or allocations to facilitate real-time applications such as voice. Without fragmentation, a long data stream could use up the entire bandwidth for a period of time, causing the voice traffic to be momentarily delayed, and in turn creating jitter, degradation in performance, which is unacceptable to the operator. BFW systems feature fragmentation to ensure real-time services can co-exist with data traffic over the same air interface by creating smaller data frames when necessary.

Adaptive Modulation

Most WLAN products currently offered in the market do not feature adaptive modulation, which adjusts the modulation index (spectral efficiency) in response to challenging channel conditions to ensure optimal transmission. Consequently, when intermittent signal fades occur due to multipath or diffractive losses, the WLAN system simply drops packets, affecting overall throughput. BFW systems, on the other hand, with adaptive modulation, can continue to sustain the communication link during channel degradation, providing up to five nines (99.999%) of availability, which is critical for carrier class operations.

ARQ

WLANs do not possess automatic repeat and request (ARQ) schemes found in many BFW systems to deal with errors that can occur from propagation effects associated with over-the-air BFW deployments. ARQ is a physical layer attribute, which involves retransmitting one to a few bits of data that have been adversely affected by propagation anomalies during a communication session. By retransmitting the individual bits, the signal is recovered well before the TCP/IP stack is involved – note bit recovery at the RF layer is significantly more efficient than IP recovery at Layer 3.

Dynamic Range

WLAN devices are designed to operate over relatively short distances (<500 ft), and hence, do not have to deal with the considerable dynamic ranges associated with the near-far phenomenon of fixed wireless systems, i.e., a typical BFW base station may have a user at 100 ft away and 20 miles away simultaneously operating within the same sector. BFW systems possess robust automatic gain controls to deal with this dynamic range effectively.

Medium Access Controller (MAC)

The wireless LAN MAC is based upon carrier sense multiple access collision avoidance (CSMA/CA), which is well suited for a limited number of users in an in-building network installation, however, throughput performance suffers greatly when a larger number of users (>20 users) over longer distances (>500 ft) is deployed, as is typical with BFW deployments. CSMA, originally designed for wireline applications, assumes that end user stations can hear each other to avoid collisions. With a WLAN deployment, end-stations will not hear each other (primarily due to directive antennas), resulting in multiple collisions that will severely degrade throughput performance (this is known as the hidden node problem). More specifically, when a collision occurs, a communication error will result, forcing the station to attempt a re-transmission (usually after a certain period of time defined by a back-off algorithm). It only takes a few systems on the network to create multiple collisions, resulting in repeated transmissions that dramatically reduce the effective data throughput of the network.

BFW systems, on the other hand, are based on time division multiple access (TDMA), in which a MAC scheduler is used to allocate time slots or bandwidth in an efficient and orderly manner to each end-user. Since a common scheduler is employed, bandwidth can be allocated on a pre-defined basis depending on the profile of each customer. This represents the basis for quality of service (QoS) where different services can be provided to each user in accordance with their respective service level agreements (SLAs). This is an important service offering that an 802.11x based system does not support.

Interference

Interference can be a significant issue with 802.11 based systems operating in their native deployment environments, particularly in traditional bands such as 2.4 GHz, where other commercial systems operate including cordless phones, Bluetooth systems, Industrial microwave ovens, and other competing wireless LANs providing in-building connectivity. As discussed previously, 802.11 MACs are designed to be 'interference adverse' such that the moment they detect interference in the channel, they immediately stop transmitting until the interference dissipates. The net result is severe degradation to throughput performance. Fixed wireless systems, on the other hand, are designed for outdoor deployments, and hence, comprise a host of features to address interference.

Conclusion

WLAN systems are ideal for indoor applications, in which they were originally designed to operate. However, they lack the critical features and system architecture necessary to operate effectively in the outdoor environment. Fixed wireless systems, such as the Redline AN-50 system, are specifically designed to address outdoor deployments, featuring a host of techniques to provide optimal throughput, robustness, and range for broadband applications.

Table 1. Summary of BFW System over 802.11x.

Item	Benefits of BFW Systems over 802.11x
Multipath	Better compensation against long delay multipath to avoid ISI
Security	Higher level of security – DES encryption, safer keys
Regulatory Emissions	Regulated out of band emissions and spurious noise
Concatenation	Higher spectral efficiency for larger data packets
Fragmentation	Support real time applications such as voice
Adaptive Modulation	Dynamic modulation index in response to challenging channel conditions
ARQ	Over the air error correction for greater efficiency
Dynamic Range	Greater power control for extreme near-far challenge
MAC	TDMA over CSMA for significantly greater spectral efficiency
Interference	Designed specifically to address potential interference in the outdoor environment from such equipment as cordless phones, bluetooth, microwave ovens, other WLAN devices, etc.