Multiuser Transmitter OFDM Using IP Mobile in VPNs

M. C. NICULESCU, Elena NICULESCU and I. RESCEANU
Dep. of Mechatronics and Electronics and Instrumentation
University of Craiova
Al. I. Cuza Street, No. 13, Craiova, RO-200585
ROMANIA

Abstract:- In this paper we try to present advantages of multiuser OFDM and a hardware implementation, this include adaptive frequency hopping, adaptive modulation, and multiple transmitter cells. An overview of several new which techniques improve the safety of system and the enlargement efficiency.

Key-Words: - OFDM, IFFT , WLAN, Mobile IP, Networks, Authentication, VPN.

1 Introduction

OFDM has been widely used in broadcast systems. It is being used for Digital Audio Broadcasting (DAB) [1] and for Digital Video Broadcasting (DVB) in Europe. It was selected for these systems primarily because of its high spectral efficiency and multipath tolerance. OFDM transmits data as a set of parallel low bandwidth (100 Hz - 50 kHz) carriers. The frequency spacing between the carriers is made to be the reciprocal of the useful symbol period. The resulting carriers are orthogonal to each other provided correct time windowing at the receiver is used. The carriers are independent of each other even though their spectra overlap. OFDM can be easily generated using an Inverse Fast Fourier Transform (IFFT) and received using a Fast Fourier Transform (FFT). High data rate systems are achieved by using a large number of carriers (i.e. 2000-8000 as used in DVB). OFDM allows for a high spectral efficiency as the carrier power, and modulation scheme can be individually controlled for each carrier. However in broadcast systems these are fixed due to the one way communication.

In most communication systems two-way communications is required and multiple users must be supported. OFDM can be applied in a multiuser application producing a highly flexible, efficient communications system. Little work has been previously done on multiuser OFDM. It was first presented by Wahlqvist [2] who suggested one possible implementation. The system design of a multiuser OFDM system is dependent on the intended application and hardware complexity.

This paper presents multiuser OFDM in a more general form and outlines some of the potential techniques that could be used to make it a highly efficient and reliable communication system. Additionally a test hardware solution is presented using SHARC® Digital Signal Processors (DSP) demonstrating the feasibility of a simple multiuser OFDM system.

2 Adaptive modulation

Most OFDM systems use a fixed modulation scheme over all carriers for simplicity. However each carrier in a multiuser OFDM system can potentially have a different modulation scheme depending on the channel conditions. Any coherent or differential, phase or amplitude modulation scheme can be used including BPSK, QPSK, 8PSK, 16QAM, 64QAM, etc. Each modulation scheme provides a trade off between spectral efficiency and the bit error rate. The spectral efficiency can be maximised by choosing the highest modulation scheme that will give an acceptable Bit Error Rate (BER). In a multipath radio channel, frequency selective fading can result in large variation in the received power of each carrier. For a channel with no direct signal path this variation can be as much as 30 dB in the received power resulting in a similar variation in the SNR. Using adaptive modulation the carrier modulation is matched to the SNR, maximising the overall spectral efficiency.

In systems that use a fixed modulation scheme the carrier modulation must be designed to provide an acceptable BER under the worst channel conditions. This results in most systems using BPSK or QPSK. These give a poor spectral efficiency (1-2 bits/s/Hz) and provide an excess link margin most of the time. Using adaptive modulation, the remote stations can use a much higher modulation scheme when the

radio channel is good. Thus as a remote station approaches the base station the modulation can be increased from 1 bits/s/Hz (BPSK) up to 4-6 bits/s/Hz (16QAM - 64QAM), significantly increasing the spectral efficiency of the overall system. Preliminary results show that for a cellular network the system capacity can potentially be doubled using adaptive modulation. There are several limitations with adaptive modulation. Overhead information needs to be transferred, as both the transmitter and receiver must know what modulation is currently being used. Also as the mobility of the remote station is increased, the adaptive modulation process requires regular updates, further increasing the overhead. There is a trade off between power control and adaptive modulation. If a remote station has a good channel path the transmitted power can be maintained and a high modulation scheme used (i.e. 64 QAM), or the power can be reduced and the modulation scheme reduced accordingly (i.e. QPSK). The received power for neighbouring carriers must have no more than 15-30 dB variation at the base station, as large variations can result in strong signals swamping weaker carriers. Intermodulation distortion (IMD) results from any non linearites in the transmission. This IMD causes a higher noise floor in the transmission band, limiting the maximum SNR to typically 30-60 dB. Frequency errors in the transmission due to synchronisation errors and Doppler shift result in a loss of orthogonality between the carriers. A frequency offset of only 1% of the carrier spacing results in the effective SNR being limited to 30 dB [4]. The limited SNR restricts the maximum spectral efficiency to approximately 5-7 bits/s/Hz. Adaptive modulation requires accurate knowledge of the radio channel. Any errors in this knowledge can result in large increases in the BER, due to the small link margin used. For a multiuser OFDM system, transmitting pilot tones or reference symbols can perform channel characterisation. Transmitting a symbol with known data allows the phase error to be estimated, giving the SNR of each carrier. This SNR can then be used to select the modulation scheme.

2.1 User allocation

There are several methods for allocating carriers to users. The main three groups are grouped carriers, spread out carriers and adaptive carrier allocation.

2.2 Carriers

The simplest scheme is to group the carriers allocated to each user. Grouping carriers minimises inter-user interference due to distortion, power level variation and frequency errors. However, grouping the carrier makes the transmission susceptible to fading, as the whole group of carriers can be lost in a null in the spectrum. This problem can be partly overcome by frequency hopping the carriers. In user allocation scheme described by [2], groups of carriers are transmitted in short time blocks. These blocks were randomly frequency hopped to ensure that the time period spent in a null would is relatively short, approximately 11 symbols. To recover data lost during a null, time interleaving and forward error correction was used. These come at the cost of reduced capacity and an increased delay.

2.3 Spread Carriers

Carriers can be allocated in a comb pattern, spreading them over the entire system bandwidth. This improves the frequency diversity, preventing all the carriers used by a user being lost in a null in the spectrum. However, this allocation scheme may be susceptible to inter-user interference. This type of user allocation is useful in applications that can not use adaptive hopping. Figure 1 shows an example of a comb user carrier allocation.

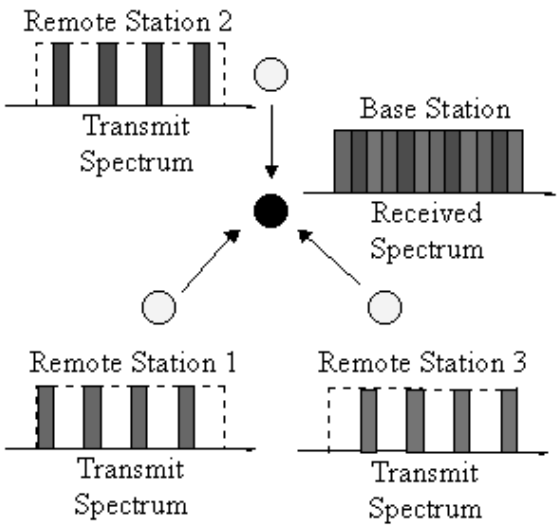

Fig. 1 Reverse link of a multiuser OFDM system

3 Multiple Transmitter

ODFM signals are intrinsically multipath robust due to the low symbol rate used and the addition of a time domain guard period [3]. Multipath reflections

that have a delay spread less than the guard period cause no inter-symbol interference. This allows for Single Frequency Networks (SFN) to be used in broadcast OFDM systems [1]. A single frequency can be used for all transmitters in a country wide broadcast. For DAB the transmitter can be spaced up to 75 km apart. Normally each transmitter must use a different frequency from neighbouring transmitters, as they would appear as strong multipath if the same frequency were used. A SFN greatly reduces shadowing as multiple signals are received from different directions resulting in spacial diversity.
The concept of a SFN can be applied to a multiuser OFDM system. The base station would consist of multiple repeaters transmitting the same signal. Each signals received by the repeaters can either be combined and decoded with a single central receiver, or each repeater could have its own receiver. Using a multiple transmitter cell will significantly reduce shadowing due to the increased spacial diversity, as shown in figure 2.

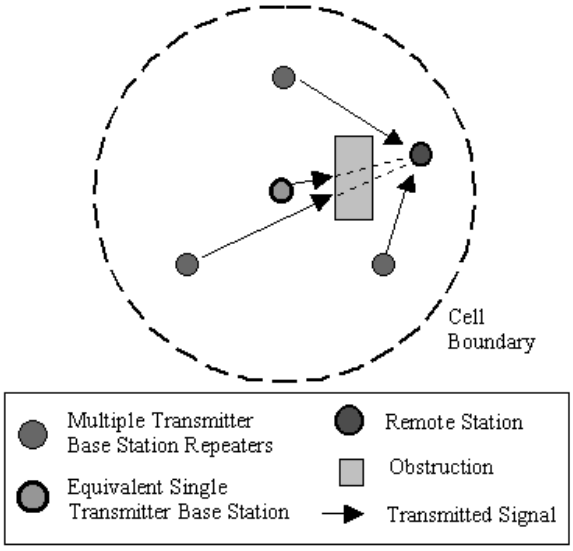

Fig. 2 Reduced shadowing with a multiple transmitter cell

Multiple transmitter cells are particularly suitable for wireless LAN applications. Shadowing makes it difficult to achieve good coverage of a building. Repeaters are often required, except that in conventional systems these repeaters cause multipath problems. In a multiuser OFDM system repeaters could be added where needed, with no additional problems. A multiple transmitter cell could be as simple as a coax running the length of a building corridor with multiple tap off points (see figure 3).

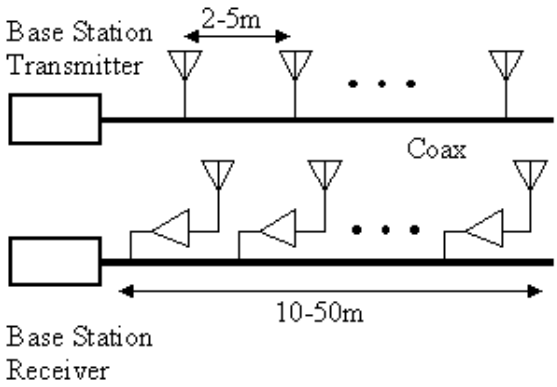

Fig. 3 Simple Multiple Transmitter Set up for Wireless LAN

3.1 Hardware implementation

A small-scale test system was made using Analog Devices Ez-Kit evaluation boards. This board includes a 40 MHz SHARC® DSP processor, a 16 bit stereo CODEC, bootloader kernel, and a serial interface. A baseband multiuser OFDM system was implemented using the on- board CODECs. The maximum sample rate for the CODECs was 48 kHz. A 512 point real FFT was used for signal generation, of which 196 carriers were active, giving a bandwidth of 18 kHz. A guard period of 32 samples was used. Each transceiver was made using two Ez-kit boards. Figure 4 shows one of the multiuser OFDM transceivers.

Fig. 4 Example Multiuser OFDM transceiver

3.2 User Allocation

A three user system was made consisting of a base station and two remote stations. The forward link transmission was subdivided into 2 groups of 96 carriers, one group for each user. The reverse link transmission from each remote station was a group

of 96 carriers. One remote station used the lower 96 carriers, the other the upper 96 carriers. No adaptive frequency hopping was used.

3.3 Errors in reception

The input data for each user was an audio signal sampled at 8 kHz at 8 bits. This data was modulated with 256 PSK, using a linear mapping from the 8 bit audio data. Due to the linear mapping errors in reception have only a small effect. The modulation was fixed to simplify the system.

3.4 Time Synchronisation

Multiuser OFDM requires strict time and frequency synchronisation. In the reverse link the signals from all users are combined in the channel and are received as a complete OFDM signal. All remote stations must be frequency and time synchronised in order for the transmitted signals to remain orthogonal to each other. All signals in the forward channel originate from the base station, and thus synchronisation techniques developed for broadcast OFDM can be used [3, 4].

The remote stations were synchronised to the base station using a null symbol frame synchronisation. The base station transmitted a null symbol at the start of each frame (36 symbols). The remote stations synchronised to the null using a moving average envelope detector.

3.5 Results

The mobile system was found to work, with no apparent cross talk between the two users. The forward link synchronisation was found to be stable, with an error of ~1-2 samples/frame at a high SNR, degrading to 8-32 samples at a SNR of 1dB. Reverse link synchronisation was slightly worse caused by difference in forward synchronisation of the two users.

4 Mobile IP Worldwide

In the previous section Mobile IP Deployment for an Intranet, security implications of this deployment as well as the protections against these threats have been described. In this section security threats of the intranet being extended with attack to the mobile node outside of the intranet, a protection for this mobile node as well as how this mobile node can securely access to the intranet are presented. The scenario for mobile IP worldwide however is first introduced.

4.1 Internet-wide Mobility Deployment

Mobile IP can allow a user to move anywhere through the entire Internet without exposing his Intranet to additional security threats over the attacks that face any network connected to the Internet. Fig. 9 represents an Internet-wide mobile IP deployment scenario. In the figure, we visualize the part of the Intranet with confidential data connected to the global Internet through a firewall to ensure connectivity of authorized mobile nodes. The figure also shows a public area of this Intranet that provides access for mobile nodes.

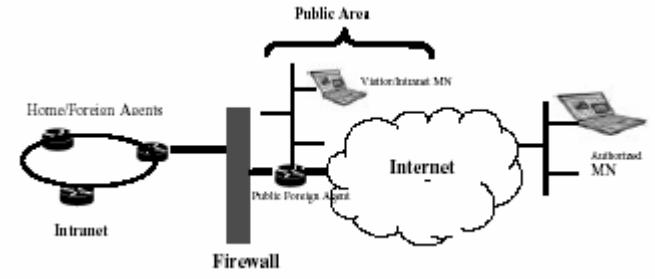

Fig. 5 - Mobile IP deployment Scenario

The mobility on Internet scenario is characterized by a topological placement of home agents and foreign agents with respect to the firewall and the mobile nodes. Although the home agents are protected by the firewall, all foreign agents can not be under the firewall. The public foreign agent that is non-protected has to provide service to the public area's mobile nodes. Therefore this agent can support passive or active eavesdroppings. This scenario is used in the rest of this section to show how a mobile node can reach his home agent securely.

4.2 Mobile Node Protection

Although the deployment adds no security risks over and above those faced by any network that connects to the Internet, the vulnerability of the intranet with internet access introduce security threats over the network's mobile nodes that are "on the Internet" with no firewall to protect them against attacks. The protection against these threats can be a method based upon Virtual Private Networks (VPNs) technology. Fig. 10 shows VPNs for protection of Intranets. A VPN consists of two or more physical private networks that are separated by a public network and behaves as a single private network.

The VPNs are built from authenticated and encrypted tunnels between secure tunneling firewalls at the border of each physical network. The firewall protects its network by admitting only those packets that have been authenticated and encrypted by one of the other firewalls.

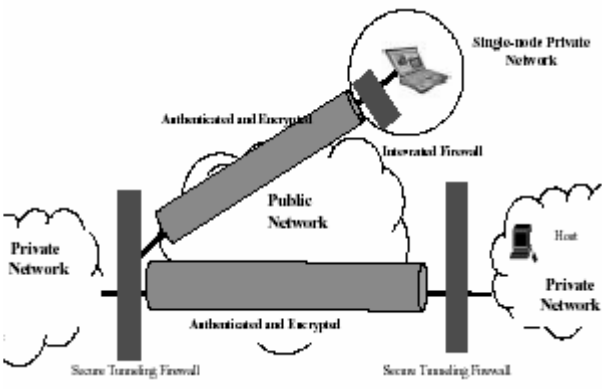

Fig. 6 - Virtual Private Network ensuring secure firewall traversal

The application of VPNs technology for a mobile node protection is also shown in this figure. In the figure the mobile node is presented as a single-node private network protected by the integrated firewall. This solution protects a mobile node through a secure tunneler. Therefore the secure tunneler is a firewall of the application-layer relay type (see fig. 6) that provides a cryptographically-protected path for authorized users to access a private network across a public network. The solution must provide a way by which the mobile node is able to communicate with all hosts and routers within the rest of the VPN (any of the physical, private networks) without compromising the security of those networks. Simple Key-Management protocol (SKIP) [9] is an implementation of the method to traverse the firewall securely. How this protocol protects the mobile node is shortly introduced in the following section.

5 Conclusion

We addressed the mobile IP security issues in campus Intranet and in the Internet. We firstly examined the ESP, the AH and the IKE protocols defined in the IETF's IPSec architecture. Based on these protocols, protection against denial of service, passive eavesdropping, session stealing and other active attacks in campus intranets were discussed. These discussions were further extended to the Internet-wide context, where the use of the secure tunneler as a main protection mechanism was examined. The recurring pattern in the counter measures against all of these attacks is that security mechanisms and services concern authentication and encryption techniques to prevent security attacks. Security mechanisms, services and protocols to provide communications throughout the Internet with confidentiality, authentication and integrity are under elaboration within the IETF. The works cover both IPv4 and IPv6 and ranges from the link layer up to the application layer.This paper has presented an overview of multiuser OFDM and some of the new techniques that can enhance system performance. Multiuser OFDM allows for highly flexible communications, thus can be made to adapt to radio channel conditions. This adaptability results in a high spectral efficiency and reliability.

References

[1] Thibault L. and Le M.T., "Performance Evaluation of COFDM for Digital Audio Broadcasting, Part I: Parametric Study", *IEEE Transactions on Broadcasting*, Vol. 43, No. 1, pages 64-75, March 1997

[2] Wahlqvist M., Östberg C., Beek J., Edfors O., Börjesson P., "A Conceptual Study of OFDM-based Multiple Acess Schemes", Technical Report Tdoc 117/96, ETSI STC SMG2 meeting no 18, Helsinki, Finland, May 1996, http://www.sm.luth.se/csee/sp/publications/

[3] Lee D., Cheun K., "A new symbol timing recovery algorithm for OFDM systems", *IEEE Transactions on Consumer Electronics*, Vol. 43, No. 3, pages 766-775, August 1997

[4] Moose P., "A Technique for Orthogonal Frequency Division Multiplexing Frequency Offset Correction", *IEEE Transactions on Communications*, Vol. 42, No. 10, pages 2908-2914, October 1994

[5] S. Kent and R. Atkinson. IP Encapsulating Security Payload (ESP). RFC 2406, December 2005.

[6] S. Kent and R. Atkinson. IP Authentication Header. RFC 4303, December 2005.

[7] Eastlake, D., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4305, December 2005.

[8] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[9] Hardjono, T. and B. Weis, "The Multicast Group Security Architecture", RFC 3740, March 2004.

[10] Krawczyk, H., "The Order of Encryption and Authentication for Protecting Communications (Or: How Secure Is SSL?)", CRYPTO' 2001.

[11] Kaufman, C., Ed., "The Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.
[12] Hardjono, T. and B. Weis, "The Multicast Group Security Architecture", RFC 3740, March 2004.
[13] Communications 2100 Network Camera, AXIS 2002, http://www.axis.com
[14] C. Luna, Y. Eisenberg, R. Berry, T. Pappas, A. Katsaggelos, Transmission Energy Minimization in Wireless Video Streaming Applications," Proc. of Asilomar Conf. on Signals, Systems, and Computers, Nov. 2001.