

Indoor Geolocation using OFDM Signals in HIPERLAN/2 Wireless LANs

Xinrong Li and Kaveh Pahlavan
Center for Wireless Information Network Studies
Worcester Polytechnic Institute, USA
{xinrong, kaveh}@ece.wpi.edu

Matti Latva-aho and Mika Ylianttila
Centre for Wireless Communications
University of Oulu, Finland
{matla, ylianttila}@ees2.oulu.fi

ABSTRACT

With the finalization of new series of IEEE 802.11 and ETSI HIPERLAN standards, it becomes very important and interesting to study the methods to integrate geolocation functionalities into the next generation wireless LANs. In this paper we investigate geolocation methods and system architectures using OFDM signals in HIPERLAN/2 wireless LANs. We propose a novel method to measure geolocation metrics by exploiting the HIPERLAN/2 MAC frame structure. Computer simulation results are presented to show the performance of the geolocation systems using OFDM signals.

I. INTRODUCTION

Providing geolocation services and integrating context awareness is becoming one of the future trends of wireless data communication systems. As a result of FCC ruling concerning the enhanced wireless E911 services, considerable interests have been attracted to geolocation techniques. Similar to the geolocation applications in cellular systems, there are increasing needs in indoor environments (e.g. hospital, warehouse and emergency site) to locate expensive equipments or people (e.g. patients, children, firefighters, soldiers and policemen) [1][2]. These incentives have led to research in designing accurate geolocation systems in indoor environment where the severe multi-path radio propagation and lack of line-of-sight signal makes it very difficult for traditional GPS systems and cellular geolocation systems to provide adequate accuracy.

Geolocation information can be extracted either from a dedicated infrastructure and signaling system (e.g. GPS systems) or from an existing infrastructure and signaling system designed for wireless voice or data communications (e.g. providing geolocation services within existing cellular systems) [2]. Compared to the method of using dedicated systems, extracting geolocation information from existing signaling systems is more challenging. However, exploiting existing infrastructures and signaling system for geolocation purpose is more attractive because by using this method, geolocation related services can be easily integrated into existing wireless communication systems without significant changes in both mobile terminals and network infrastructures. With the finalization of new series of IEEE 802.11 and ETSI BRAN HIPERLAN standards, new features are being integrated into the next generation wireless LANs and it becomes very important

and interesting to study the methods to integrate geolocation functionality into wireless LANs.

During the past decade, geolocation methods in DSSS (Direct Sequence Spread Spectrum) systems have been well studied. The autocorrelation properties of PN sequences make DSSS systems very suitable for ranging and geolocation applications. More recently, OFDM has been adopted by ETSI HIPERLAN/2 and IEEE 802.11a as physical layer standard for next generation wireless LANs. However, no similar studies of using OFDM systems for geolocation applications have been reported in the literature. In this paper, we investigate geolocation methods and system architectures using OFDM signals in HIPERLAN/2 wireless LANs. We propose a novel method to measure geolocation metrics TOA (Time of Arrival) and TDOA (Time Difference of Arrival) by exploiting the HIPERLAN/2 MAC frame structure.

The paper is organized as follows. In Section 2, we review those aspects of HIPERLAN/2 standards that are relevant to geolocation considerations. Then in the following section, we investigate geolocation methods and architectures in HIPERLAN/2 wireless LANs. In Section 4, we present a burst synchronization method in HIPERLAN/2 OFDM systems that can be used to extract geolocation metrics from OFDM signals. In Section 5, simulation results are presented to show the performance of OFDM based geolocation systems.

II. REVIEW OF HIPERLAN/2

The HIPERLAN is a collective reference to High Performance Radio Local Area Networks standards developed or been developing by ETSI (European Telecommunications Standards Institute) project BRAN (Broadband Radio Access Networks) [4][5]. The HIPERLAN/2 network operates in 5 GHz band, and it supports short-range broadband wireless access, 30m in typical indoor environment and up to 150m in typical outdoor or large open indoor environment.

A HIPERLAN/2 network typically has a configuration as shown in Figure 1. A number of Access Points (AP), each of which covers a certain area, are connected to a core network and form together a radio access network. The mobile terminal (MT) associates with one of the APs and communicate with the associated AP over the radio channel. Handoff between APs will be performed for the roaming MTs when necessary. HIPERLAN/2 defines two basic operation modes, the mandatory

Centralized Mode and the optional Direct Mode. In the Centralized Mode, APs are connected to a core network that serves MTs associated to it. All traffic must pass through AP even if the data exchange is between two MTs in the same serving area of the AP. In the optional Direct Mode, the medium access is still controlled by a central controller but this controller needs not necessarily be connected to a core network. The MTs may communicate directly between each other. In a HIPERLAN/2 network, data transmission between MT and AP is connection-oriented. There are two types of connections, bi-directional point-to-point and unidirectional point-to-multipoint (from AP to MT). The connections between MTs and AP, which are time-division multiplexed over the air interface, are established prior to the transmission using signaling functions.

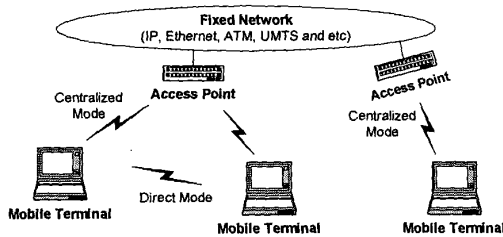


Figure 1: The HIPERLAN/2 network.

HIPERLAN/2 protocol has three basic layers: Physical (PHY) layer, Data Link Control (DLC) layer, and Convergence layer (CL). The PHY layer defines basic data transmission functions via radio channel. The DLC layer consists of Medium Access Control (MAC) function, Error Control (EC) function and Radio Link Control (RLC) function. The Convergence layer works as an intermediate component between the DLC layer and a variety of fixed networks, e.g. IP, Ethernet, ATM, UMTS and etc., to which HIPERLAN/2 network is connected.

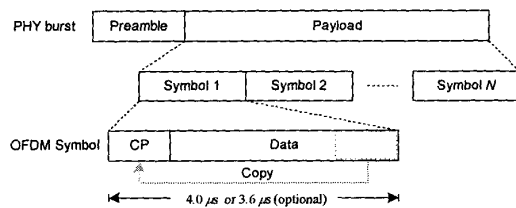


Figure 2: HIPERLAN/2 physical layer burst format with OFDM signaling.

The PHY layer of HIPERLAN/2 is based on a multicarrier modulation scheme OFDM (Orthogonal Frequency Division Multiplexing). The basic idea of the OFDM is to divide a wideband selective channel into a number of independent narrowband sub-channels so that the narrowband sub-channels can be viewed as non-selective or flat fading. OFDM can be efficiently implemented using FFT (Fast Fourier Transform) and

IFFT (Inverse FFT) at the receiver and the transmitter respectively. In such a scheme, to avoid inter-symbol-interference (ISI) and to combat multipath effects, a cyclic prefix (CP), which is a copy of the ending part of OFDM symbol, is added at the beginning of each symbol as temporal guard interval as illustrated in Figure 2. As shown in Figure 2, the basic signal format on the PHY layer is a RF burst started with a preamble that is followed by a payload data part. Five different types of PHY bursts are defined with different burst preamble formats to distinguish between each other: Broadcast Burst, Downlink Burst, Uplink Burst with Short Preamble, Uplink Burst with Long Preamble and Direct Mode Burst.

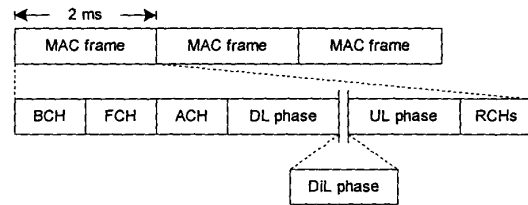


Figure 3: MAC frame structure for HIPERLAN/2.

The Data Link Control layer constitutes the logical link between AP and MTs. The functional entities in DLC layer are Medium Access Control function, Error Control function and Radio Link Control function. In HIPERLAN/2, the MAC protocol is based upon a dynamic TDMA/TDD scheme with centralized control. The Basic MAC frame structure is shown in Figure 3. The duration of each MAC frame is 2ms. Each MAC frame consists of transport channels BCH (Broadcast Channel), FCH (Frame Channel), ACH (Access Feedback Channel), a DL (Down-Link) and UL (Up-Link) phase, and one or many RCHs (Random Channel). A DiL (Direct Link) phase is also contained between DL phase and UL phase if Direct Mode is used. The duration of the BCH is fixed while the duration of the FCH, DL phase, DiL phase, UL phase and the number of RCHs are dynamically adapted by the AP according to the current traffic condition. The BCH (downlink only) contains control information that reaches all the MTs. It provides information about transmission power levels, starting point and length of the FCH and RCH, wake-up indicator, and identifiers for identifying both the HIPERLAN/2 network and the AP. The FCH (downlink only) contains an exact description of how the DL phase, UL phase and RCH are configured in the current MAC frame. The ACH (downlink only) contains information on previous access attempts made in the RCH. The DL and UL phase (bi-directional) is for the traffic of PDU (Protocol Data Unit) trains to and from the MTs respectively. The RCH (uplink only) is used by the MTs to request transmission resources for the DL or UL phase in upcoming MAC frames, and to convey some RLC signaling messages. Collisions may occur in RCH and the results from RCH access will be reported to MTs in ACH.

III. HIPERLAN/2 GEOLOCATION METHODS AND ARCHITECTURES

As we noted in the last section, HIPERLAN/2 MAC protocol is based upon dynamic TDMA/TDD scheme with centralized control. Each MAC frame of fixed length (2ms) is divided into a number of transport channels of varying length. The MAC frame synchronization between AP and MTs is established with the aid of physical layer Broadcast Burst that is transmitted at the beginning of transport channel BCH (i.e. the beginning of each MAC frame). The starting time points of other transport channels are determined with time offset from the starting point of MAC frame and are known to both AP and mobile terminals. These features of MAC frame structure can be exploited in measuring geolocation metrics TOA and TDOA from OFDM burst signals. In this section, we examine different geolocation methods in light of different geolocation architectures in HIPERLAN/2 wireless LANs.

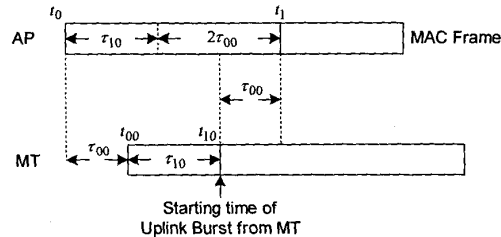


Figure 4: AP-based TOA geolocation method.

Geolocation system architectures can be roughly grouped into two categories, mobile-based and network-based architectures. In both cases, more than three Geolocation Base Stations (GBS) are needed to geometrically locate MT using multiple TOA/TDOA measurements [2]. In mobile-based architecture, MT extracts geolocation metrics from received radio signals that are transmitted by GBSs. The location information can be relayed to a Geolocation Control Station (GCS) if necessary. In network-based architecture, GBS measures radio signals transmitted by MT and then GBS or GCS extracts geolocation metrics from the measurements. The selection of geolocation system architecture depends on where the geolocation information is needed, i.e. in MT or in GCS, and some other implementation considerations in specific application scenarios. In this paper, we only focus on geolocation methods for network-based architecture. The functionality of GBS can be either implemented in AP or in a separate Geolocation Reference Point (GRP). The selection of implementation methods between AP-based and GRP-based approaches also depends on the specific application scenarios and implementation considerations. For example, in some application scenarios, only one AP is available and thus we need a few separate GRPs operating around AP to provide geolocation services. As we will discuss later in this section, different approach requires different geolocation

methods and results in different signaling requirements in HIPERLAN/2 networks.

In AP-based architecture, TOA from MT to AP can be measured basing on round-trip time of flight as illustrated in Figure 4, where t_0 and t_1 are the times (measured at AP) of transmitting Broadcast Burst and receiving Uplink Burst from MT respectively, while t_{00} and t_{10} are the times (measured at MT) of receiving Broadcast Burst from AP and transmitting Uplink Burst respectively. The delay τ_{10} is the offset of UL phase within the MAC frame, which is known to both MT and AP, and the delay τ_{00} is the TOA to be measured. The request for location services can be initiated either from GCS, which is connected to the network through wired or wireless connection, or from MT through AP (or GCS). AP assigns UL phase in current MAC frame to the target MT and the MT sends a signal within UL phase. The MT determines the starting time t_{00} of current MAC frame by measuring the receiving time of the Broadcast Burst from AP, and AP determines t_1 by measuring the receiving time of the Uplink Burst from the MT. Since the delay τ_{10} is known to both AP and MT, the TOA from MT to AP can be calculated at AP as follows:

$$\tau_{00} = \frac{1}{2} [(t_1 - t_0) - \tau_{10}]. \quad (1)$$

To perform geolocation function at GCS, TOA measurements from MT to at least three APs are required. But it should be noted that to measure TOA from MT to multiple APs, forced handoffs are needed to associate MT to different APs, which requires significant coverage overlap between adjacent APs. This is the major drawback of AP-based geolocation method.

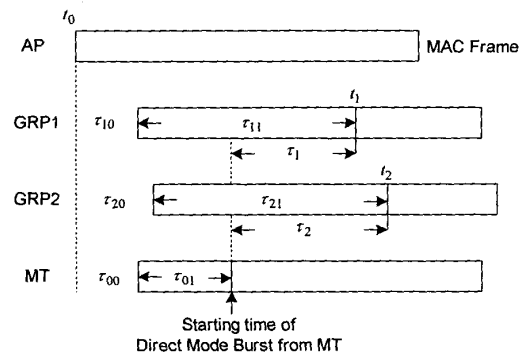


Figure 5: GRP-based TDOA geolocation method.

If the functionality of GBS is implemented in a separate Geolocation Reference Point (GRP) instead of in AP, TDOA method can be used as illustrated in Figure 5, where t_0 is the starting time of a MAC frame at AP while t_1 and t_2 are the times of receiving Direct Mode Burst at GRP1 and GRP2 respectively. The delay τ_{01} is the offset of DiL phase within MAC frame; delays τ_{00} ,

τ_{10} and τ_{20} are transmission delays from AP to MT, GRP1 and GRP2 respectively. In this method, after the request for geolocation services is initiated by MT or GCS, AP assigns the optional DiL phase in the current MAC frame to the MT and the MT transmits a Direct Mode Burst within the DiL phase. Then GRP measures the receiving time of the Direct Mode Burst from the MT. The TOAs from AP to GRPs τ_{10} and τ_{20} can be accurately estimated at GCS since the distances between each GRP and AP are known. Consequently, the TDOA from MT to GRP1 and GRP2 can be calculated as follows:

$$\begin{aligned} TDOA_{21} &= \tau_2 - \tau_1 \\ &= [(\tau_{20} + \tau_{21}) - (\tau_{00} + \tau_{01})] \\ &\quad - [(\tau_{10} + \tau_{11}) - (\tau_{00} + \tau_{01})] \\ &= (\tau_{20} + \tau_{21}) - (\tau_{10} + \tau_{11}) \end{aligned} \quad (2)$$

Using this method, GCS acts as a master that collects measurements of receiving time of Direct Mode Burst from multiple GRPs and calculates TDOAs as well as estimating position of MT basing on TDOAs. As a result, after measuring receiving time of Direct Mode Burst, GRPs have to request a UL phase to report the measurement to GCS. Using the GRP-based TDOA method, only one AP is needed to perform geolocation function and no forced handoff between APs are needed.

IV. BURST SYNCHRONIZATION METHODS IN HIPERLAN/2 OFDM SYSTEMS

Using the geolocation methods discussed in the preceding section, we need to determine the receiving time of physical layer burst signals at MT and AP (or GRP) that is also known as symbol timing synchronization. Symbol timing for OFDM signals is very different from that of a single carrier signals because no eye-opening point, which is the best sampling time, can be found [6]. In this section, we present burst synchronization methods in HIPERLAN/2 OFDM systems that can be used for geolocation purpose.

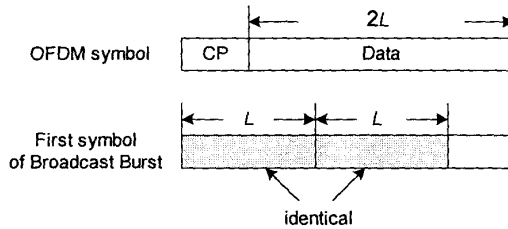


Figure 6: Training symbol in HIPERLAN/2 burst preamble.

In burst transmission mode, receiver must continuously scan for incoming data and the symbol synchronization time is required to be as short as possible. In HIPERLAN/2, the burst preamble consists of special training symbols that are used to accomplish the timing synchronization and frequency offset correction within the duration of several OFDM symbols. The first

symbol in the Broadcast Burst preamble consists of two identical parts in the time domain as illustrated in Figure 6. The timing synchronization can be performed by searching for the training symbol with two identical halves. A timing metric M is formed by performing sliding correlation of two consecutive parts of the received signal $r(k)$ (each of which has a length of L) as follows [6]:

$$M(d) = \frac{|P(d)|^2}{[R(d)]^2}, \quad (3)$$

where

$$\begin{aligned} P(d) &= \sum_{m=0}^{L-1} r^*(d+m) \cdot r(d+m+L) \\ R(d) &= \sum_{m=0}^{L-1} |r(d+m+L)|^2 \end{aligned} \quad (4)$$

and $*$ denotes complex conjugate operation. Figure 7 shows the timing metric output of the sliding correlation described above where the first vertical line indicates the starting point of the first symbol and the last vertical line is the starting point of the second symbol. Our simulation results show that this timing synchronization method works well in AWGN channel and an exponential channel that will be described in the next section. Statistical results of the timing metric obtained from our simulations (which are omitted here due to lack of space) also closely match the theoretical results presented in [6].

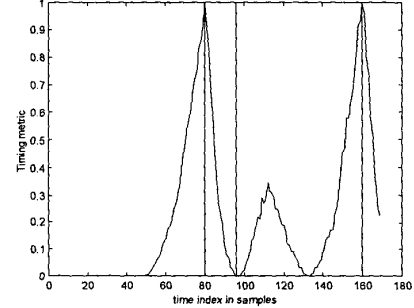


Figure 7: Timing metric without noise.

V. SIMULATION RESULTS

To study the performance of geolocation systems, ranging accuracy must be obtained first. Then the ranging accuracy can be mapped into positioning accuracy by simulations or by statistical methods. We obtained statistical results of timing errors from computer simulations using the timing synchronization method presented in the preceding section. Parameters for computer simulations are summarized in Table 1. A raised-cosine lowpass filter is used to take account of band-limitation condition that has impacts on the accuracy of timing synchronization. At the receiver an up-sampling rate of 10 is used, which is needed to make adequately high resolution in delay/distance estimation.

Two channel models are used in our simulations, AWGN channel and frequency selective channel with an exponential power delay profiles as described in [6]. AWGN channel is used to show the performance in a benign channel while the exponential channel represents a more realistic environment. For the frequency selective channel, 5 paths are chosen with path delays of 0, 2, 4, 6, and 8 samples, where sampling rate is 20MHz, so that the channel impulse response is shorter than the guard interval. The amplitude of each path is calculated from the exponential distribution:

$$A_i = \exp(-\tau_i / 8) \quad (5)$$

where A_i is the amplitude of the i th path and τ_i is the delay of the i th path in samples. The phase of each path is chosen from a uniform distribution from 0 to 2π .

Table 1: Parameter values for HIPERLAN/2 OFDM transceiver simulations.

PARAMETER	VALUE
Number of OFDM sub-carriers	52
Sub-carrier frequency spacing	0.3125 MHz
Sampling rate	20MHz
Samples per symbol	80
Samples in cyclic prefix	16
Raised-cosine lowpass filter	$T = 1/(20\text{MHz}), \alpha = 0.25$
Up-sampling rate at receiver	10

Figure 8 shows simulation results of timing errors for the two aforementioned channel models. We can observe that compared to the AWGN channel, the mean and standard deviation of timing errors became worse for exponential channel. Since the sampling period at the receiver is $T_s = 5\text{ns}$ (with up-sampling rate 10), one sample timing error maps to 1.5m ranging error. As a result, the mean of ranging errors remains around 3m for AWGN channel and 7.5m for exponential channel when signal-to-noise ratio is greater than 9dB. The timing synchronization method used in our simulations is pretty simple since only one OFDM training symbol is used. Some other timing methods are needed to further improve the accuracy in real multi-path indoor environment.

VI. CONCLUSIONS

In this paper we presented indoor geolocation methods and system architectures for HIPERLAN/2 wireless LANs. A novel method is proposed to measure TOA and TDOA from OFDM signal by exploiting MAC frame structure in HIPERLAN/2 wireless LANs. A symbol timing synchronization method is used to obtain the statistical results of timing errors that were mapped into ranging accuracies. The simple timing method used in this paper can result in a mean ranging errors around 7.5m in the exponential channel. Other timing methods have to be combined to further improve the performance.

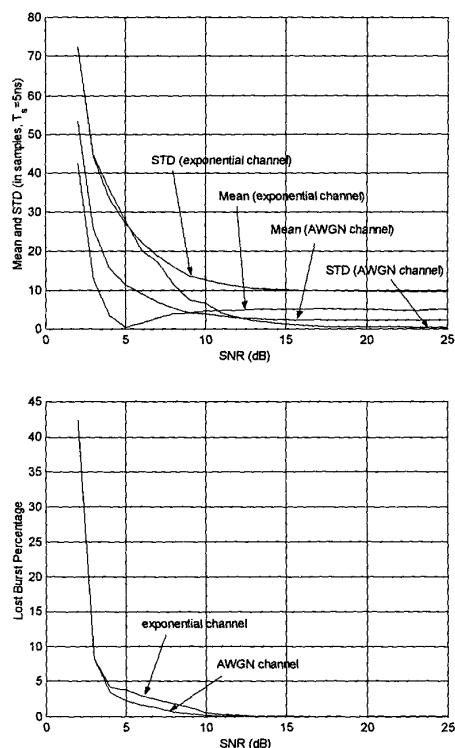


Figure 8: Mean and STD (standard deviation) of timing errors for AWGN and exponential channels.

ACKNOWLEDGEMENT

The authors would like to express their appreciation to TEKES, Nokia, and Finnish Defense Forces for supporting most parts of this project. We also thank Dr. Jacques Beneat, our colleague at CWINS, for fruitful discussions and a variety of help.

REFERENCES

- [1] K. Pahlavan, P. Krishnamurthy and J. Beneat, "Wideband radio propagation modeling for indoor geolocation applications" *IEEE Comm. Magazine*, pp. 60-65, April 1998.
- [2] K. Pahlavan, X. Li, et al., "An overview of wireless indoor geolocation techniques and systems", *Proceeding of MWCN'2000*, Paris, France, May 2000.
- [3] C. Sinner and R. Sigle, "Toward wireless multimedia communications. Current stands and future directions", *Int'l J. of Wireless Information Networks*, vol. 5, No.1, pp. 61-73, January 1998.
- [4] ETSI, *Technical Report: TR 101 031 v2.2.1 - Requirements and architectures for wireless broadband access* January 1999.
- [5] Martin Johnsson, "HiperLAN/2 - The broadband radio transmission technology operating in the 5GHz frequency band", *HiperLAN/2 Global Forum* (<http://www.hiperlan2.com>), 1999.
- [6] T.M. Schmid and D.C. Cox, "Robust frequency and timing synchronization for OFDM", *IEEE Trans. Comm.*, vol. 45, No. 12, pp. 1613-1621, December 1997.