

Comparison of Indoor Geolocation Methods in DSSS and OFDM Wireless LAN Systems

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, over}@ees2.oulu.fi

Abstract

Geolocation methods for HIPERLAN/2 OFDM systems were reported recently. This paper continues to study the possibility of overlaying geolocation functions in 802.11 DSSS wireless LANs. In this paper, a delay measurement-based TDOA measuring method is proposed for 802.11 wireless LANs, which eliminate the requirement of initial synchronization in the conventional methods. The performance of the potential overlaid geolocation systems for DSSS and OFDM wireless LANs are analyzed and compared in terms of symbol synchronization performance.

1. Introduction

Recently, as a result of FCC ruling concerning the enhanced wireless E911 services, considerable research interests have been attracted to geolocation techniques in cellular systems [1][2][3]. Providing geolocation based services and integrating context awareness in the mobile systems are becoming more and more desirable from both service provider and subscriber point of view [4]. These new features are coming into the picture of the 4th (and even the 3rd) generation wireless communication systems. Similar to the applications in outdoor cellular systems, a number of new indoor geolocation applications have been evolved for both military and commercial scenarios [5][6][7]. In the commercial applications, there is an increasing need for indoor geolocation systems in the hospitals to locate the patients or expensive equipment and in homes to locate the children and equipment. In the military and public safety applications, there is a need for in-building communication and geolocation networks enabling soldiers, policeman, and fire fighters to complete their missions in these areas. These incentives have led to research in designing accurate geolocation systems in indoor environment where the severe multipath radio propagation condition makes it very difficult for

traditional GPS systems and cellular geolocation systems to provide adequate accuracy.

With the finalization of new series of IEEE 802.11 and ETSI BRAN HIPERLAN standards, new features are being integrated into the next generation of wireless LAN systems so that it becomes important and interesting to study the methods to integrate geolocation services into wireless LANs. Geolocation methods for HIPERLAN/2 OFDM systems were reported in [8] recently. In this paper, we continue to investigate the possibility of overlaying geolocation functions in 802.11 DSSS system, which is another major wireless LAN standard. Considerable research works have been done on ranging and geolocation methods using DSSS signals, but existing literatures on DSSS ranging methods all assume that separately located transmitter and receiver are initially synchronized [1][2][3]. As we will discuss in the following sections, the initial synchronization is hardly achieved for overlaid geolocation systems, especially in indoor environment. We propose a TDOA measuring method for overlaid geolocation systems, which depends on delay measurement using a high-precision timer instead of initial synchronization. The basic principle of the proposed TDOA measuring method can be applied to DSSS and OFDM systems without any difference. Then the comparison of the performance is of interest. The performances of the potential overlaid systems are compared in terms of symbol synchronization performance, which determines ranging accuracy in geolocation systems. The performance of ranging and positioning is beyond the scope of this paper.

The paper is organized as follows. In section 2, geolocation methods for 802.11 wireless LAN systems are presented. Then in section 3, we compare the geolocation method with statistical results of symbol synchronization errors obtained from both DSSS and OFDM system simulations. Finally, the paper is closed with a summary and conclusions.

2. Geolocation methods for 802.11 wireless LANs

A geolocation system generally requires three or more Geolocation Base Stations (GBS) for measuring geolocation metrics and a Geolocation Control Station (GCS) for collecting geolocation metrics and performing positioning as well as for central control of location information. To overlay geolocation services in existing wireless LANs, the functionality of GBS can be either implemented in the Access Point (AP) or in a separate Geolocation Reference Point (GRP). The selection of AP-based or GRP-based implementation methods depends on the specific application scenarios and the relating implementation considerations. For example, in some application scenarios, only one AP is available and thus we need a number of separate GRPs operating around the AP to provide geolocation services.

In this section, general mechanism of TOA/TDOA measuring methods is presented first. Then we continue to illustrate how to apply the mechanism to form TDOA measurement within 802.11 wireless LANs by exploiting the existing signaling format. At last we discuss how to measure TDOA from DSSS signals.

2.1 General TOA/TDOA measuring mechanisms

There are two basic approaches to measure TOA/TDOA metric from radio signals, i.e. synchronized transceiver method and round-trip TOA method. To measure TOA using synchronized transceiver method, the MT transceiver and the GBS transceivers are all synchronized to some common time reference. If the transmitting time of the signal is sent to the receiver as a timestamp while the receiving time of the signal is measured at the receiver, the TOA can be easily calculated by differentiating the receiving and transmitting time of the signal. The TOA measurements from at least three GBS's can be relayed to a GCS to form TDOA measurements from differences between the pairs. However, to measure TDOA using synchronized transceiver method, only GBS receivers need to be synchronized to a common time reference without concerning about the MT transmitter. Each GBS receiver measures receiving time of the signal from the MT transmitter and a GCS collects timestamps of the receiving time from at least three GBS receivers to form TDOA measurements. A generalized cross-correlation method can also be used to form TDOA measurements if the received signals at three or more GBS receivers can be sampled, digitized and relayed to the GCS [3].

The synchronization of MT and GBS transceivers are usually very difficult to achieve in real application scenarios where they are physically separated and randomly located. To avoid the synchronization

requirement, round-trip TOA method can be utilized [6]. In round-trip TOA based geolocation systems the GBS transmitter sends a signal to MT at time t_0 first and the MT simply echoes the signal back to the GBS using a different carrier frequency for proper simultaneous operation of GBS transceivers or using the same carrier frequency but after waiting for a known time period. Then the GBS measures the receiving time of the signal t_1 . The delay between transmitting and receiving time of the signal at the GBS includes round-trip time-of-flight 2τ , i.e. round-trip TOA, and processing delay τ_p encountered in MT transceiver. The additional processing delay τ_p can be easily compensated or accurately measured during the system initialization or calibration period. Consequently, the TOA measurement is obtained as

$$TOA = \tau = \frac{1}{2}[t_1 - t_0 - \tau_p] \quad (1)$$

For dedicated geolocation systems, the preceding simple measuring approaches, synchronized transceiver method and round-trip TOA method, can be easily applied. But for overlaid geolocation systems, direct application of these simple methods is almost impossible because the geolocation function is overlaid without significant modifications to the existing infrastructure and signaling systems. However, as we will see in the following sections, 802.11 wireless LAN standards have some specific features that can be utilized in measuring TOA/TDOA.

2.2 TOA/TDOA measuring methods for 802.11

Three basic access mechanisms have been defined for IEEE 802.11 MAC (Medium Access Control) layer: the mandatory basic method based on CSMA/CA, an optional RTS/CTS method to avoid the hidden terminal problem, and a contention-free polling method for time-bounded service. For all access methods, there are three important parameters for controlling the waiting time before accessing the medium, i.e. SIFS (Short inter-frame spacing), PIFS (PCF inter-frame spacing) and DIFS (DCF inter-frame spacing). These three parameters define the priorities of medium access as shown in Figure 1. The medium can be busy due to the transmission of data frames or other control frames. During a contention phase, several nodes try to access the medium. The parameter DIFS denotes the longest waiting time and thus the lowest priority for medium access. This waiting time is used for asynchronous data service within a contention period. The waiting time PIFS is used for a time-bounded service. That is an access point polling other nodes only has to wait PIFS for medium access. The SIFS for medium is defined for short control messages such as

acknowledgements for data packets or polling responses. As we will describe in details shortly, this feature of MAC layer access mechanism can be exploited in measuring TDOA for geolocation purposes.

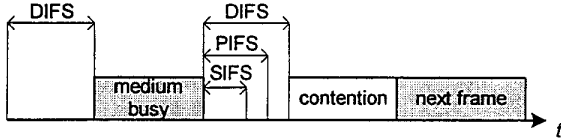


Figure 1. Inter-frame spacing and medium access priorities.

The unicast data transfer mode as defined in the standard is illustrated in Figure 2. A sender accesses the medium and sends its data. The receiver replies directly with a short acknowledgement message ACK after waiting for a short SIFS duration. Since the waiting time SIFS is the shortest waiting time and other stations can only access the medium after a longer waiting period DIFS, no other stations can access the medium in the meantime to cause a collision. The other stations must wait for DIFS plus their backoff time in the contention period. In other words, the ACK message has the highest priority. This mechanism ensures the proper transmission and reception of the ACK message.

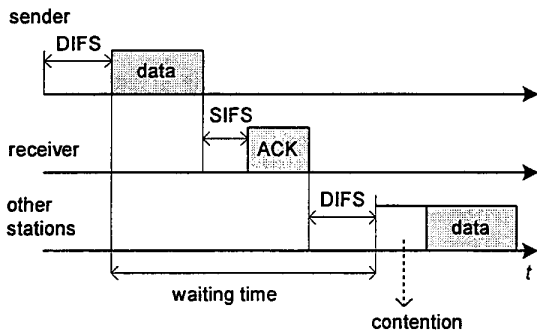


Figure 2. Unicast data transfer mode for IEEE 802.11.

If the lengths of SIFS and data frame are known, the round-trip TOA can be determined at the AP by differentiating the transmitting time of the data frame and the receiving time of the ACK. But according to the standard, in a real implementation, the accuracy of spacing between frames that are defined to be separated by a SIFS time is only within $2\mu s$, which corresponds to 600m maximum ranging error. Apparently, this method is not appropriate for indoor geolocation applications because the coverage of indoor communication systems is far below 100m for most of application scenarios. Instead of measuring TOA, a TDOA method can be used in 802.11 wireless LANs as shown in Figure 3. In this

method after the geolocation service is initiated by the MT or the GCS, the AP sends a data frame to the MT at time t_0 and MT replies with an ACK message after it receives the data. Meanwhile each GRP monitors the communication between AP and MT and measures the time delays between the arriving time of the data frame and the ACK message, i.e. τ_{11} and τ_{21} as shown in Figure 3. The GRP1 and GRP2 receive the data frame at t_{10} and t_{20} , and ACK message at t_{11} and t_{21} respectively. The delays τ_{10} and τ_{20} are TOA from AP to GRP1 and GRP2 while the delays τ_1 and τ_2 are TOA from MT to GRP1 and GRP2 respectively. Since the distance from AP to each GRP is known, the TOAs from AP to GRPs τ_{10} and τ_{20} can be accurately estimated. Therefore, the TDOA from MT to GRP1 and GRP2 can be obtained as follows:

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

Using this method, the GCS acts as a master that collects measurements of time delays τ_{11} and τ_{21} , i.e. the delay between arriving times of data frame and ACK message at each GRP, as well as estimating the position of the MT. As a result each GRP needs to report the measurement data to GCS through AP. Since the measurement at each GRP is time delay not timestamp relative to a common time reference, the clocks in GRPs are not necessarily to be synchronized. However, it should be noted that to measure the time delay accurately, a high-precision timer is needed at each GRP.

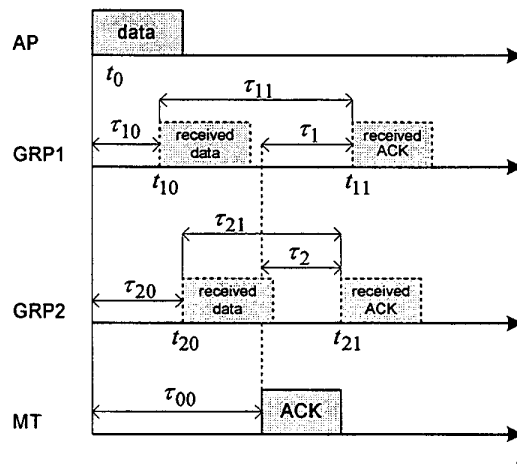


Figure 3. GRP-based TDOA method for IEEE 802.11 wireless LAN.

The same principle of TDOA measuring method can be used for systems using the optional RTS/CTS

mechanism. Utilizing RTS/CTS for geolocation purpose might be a more appropriate choice than using the unicast mode of the mandatory CSMA/CA mechanism since the RTS message can also act as a request for geolocation services to reserve a time period for geolocation only. Furthermore, the fragmentation mode defined by the standard, as shown in Figure 4, can be used to improve the performance in measuring TDOA by averaging multiple consecutive measurements to eliminate measurement errors caused by random noise.

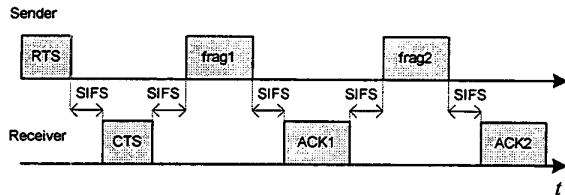


Figure 4. Fragmentation mode of IEEE 802.11.

2.3 TOA/TDOA measuring techniques using DSSS signals

The conventional spread spectrum ranging techniques assume that the transmitter and the receiver are synchronized in time. The system estimates the arrival times of the transmitted signals relative to a master PN signal, which is initially aligned with the transmitter PN signal, and uses these to form TDOA measurements. The accurate TOA/TDOA measurement is obtained in two steps using PN code acquisition and tracking techniques respectively [3]. First a sliding correlator receiver or a matched filter receiver is used to obtain a coarse TOA measurement by performing a full or partial correlation between the incoming code and the local code at the receiver. Then a PN tracking circuit, such as delay lock loop (DLL) or tau-dither loop (TDL), takes over the synchronization process to obtain a fine TOA/TDOA measurement. As we will discuss soon, direct application of these techniques to overlaid geolocation systems is very difficult. For geolocation in cellular systems, it is normally suggested to use GPS time at each GBS as a common time reference for synchronization. This is not practical for geolocation in wireless LANs since GPS receiver may not operate properly in indoor environment. For geolocation in wireless LANs, the other alternative, round-trip TOA method, is not practical too. To use round-trip TOA method together with the conventional correlation technique, the turn-around time, i.e. delay between receiving and transmitting a signal, is required to be less than the length of the PN code, which is $1\mu s$ for 802.11 wireless LANs. No existing signals satisfy this requirement.

In our approach the TDOA measuring method is not based on the assumption of synchronization between the transmitter and the receiver, but on the delay measurement of receiving times of two signals using a high-precision timer. The 802.11 wireless LANs employ burst transmission mode in the physical layer. The format of a 802.11 DSSS PHY frame is shown in Figure 5. The first 128-bit SYNC of the burst preamble are for synchronization and the following 16-bit SFD (Start Frame Delimiter), which has a specific bit pattern, denotes the starting point of the header. When the receiver receives a signal, i.e. a PHY burst, symbol synchronization is established using the first 128-bit synchronization part while the beginning of the data part is determined by searching for the special bit pattern SFD. Once the SFD is detected, the timer will be started or stopped by a timing signal. The PN acquisition and tracking techniques are used to obtain high-precision timing signal to determine the arriving time of the signals.

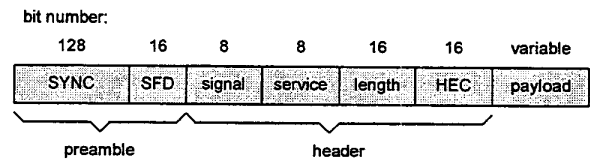


Figure 5. The format of IEEE 802.11 PHY frame using DSSS.

3. Comparison of geolocation methods for 802.11 and HIPERLAN/2

The basic mechanism of the TDOA measuring method is based on time delay measurement of two signals using high-precision timer. Since no specific properties of spread spectrum signals are required for the proposed TDOA measuring method, it can be used for systems using any modulation techniques as long as the receiving time of the signal can be measured within an acceptable accuracy for geolocation. HIPERLAN/2 is another major wireless LAN standard that is expected to receive considerably wide support in the near future. Detailed discussion of TDOA measuring methods for HIPERLAN/2 and TOA/TDOA measuring techniques using OFDM signal were reported in [8]. There is no difference in the basic mechanism of the TDOA measuring methods for DSSS and OFDM systems.

To compare the performance of the potential geolocation systems for 802.11 and HIPERLAN/2 wireless LANs, we concern with the accuracy of ranging and positioning. If we assume the receiver processing delay remains constant, the ranging accuracy is only determined by the accuracy of symbol synchronization since the constant processing delay can be measured and

completely compensated during system initialization. In this paper we only investigate the performance of symbol synchronization to study the possibility of overlaying geolocation functions onto DSSS and OFDM systems. The ranging and positioning performances are beyond the scope of this paper. For both DSSS and OFDM systems, symbol synchronization is achieved by peak detection of a triangular-shape correlation function. As the peak detection operation is usually performed using a threshold device, the accuracy of the symbol synchronization is roughly determined by the size of the base-width of the triangular-shape correlation peak, the smaller the width the more accurate the detection. As illustrated in Figure 6, where δ is the detection error, if the threshold increases, detection error decreases but with a higher probability of misdetection in a noisy environment. For 802.11 DSSS signals, the base-width of the correlation peak is $2 \times \frac{1}{R_c} = 0.18 \mu s$, where R_c is the chip rate, and

for HIPERLAN/2 OFDM signals, it is about $2.4 \mu s$, more than 10 times larger. On the other hand, for 802.11 DSSS systems, 128 bits in PHY burst preamble are designed for symbol synchronization, which results in 128 correlation peaks at the receiver, so that PN code tracking techniques can be easily employed to achieve sub-chip accuracy in correlation peak detection. In contrast, only two OFDM symbols are used in PHY burst preamble to acquire symbol synchronization, i.e. only two correlation peaks are available. Due to the wide correlation peak and small number of synchronization symbols, the simple threshold test method cannot provide adequate accuracy for OFDM symbol synchronization. More complicated methods are usually used together with the threshold device, which requires significantly higher system capacity in data buffering and processing. Basing on our preceding discussions, we can conclude that 802.11 DSSS systems has greater potential than HIPERLAN/2 OFDM systems for overlaying geolocation functions.

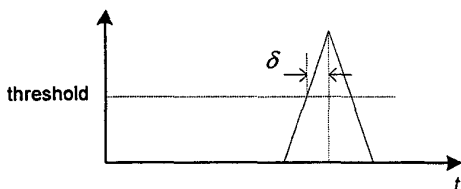


Figure 6. Correlation peak detection for symbol synchronization.

Preliminary results are obtained from computer simulations to compare the accuracy of symbol synchronization of DSSS and OFDM systems. The simulation parameters of DSSS systems are summarized in Table 1 and those of OFDM systems are the same as in

[8] except that the up-sampling rate is changed to 5 to make the final sampling rate of both receivers similar, i.e. 99MHz for DSSS system and 100MHz for OFDM system. A raised-cosine low-pass filter is used for both systems to simulate band-limited situation in practical communication systems. In our simulations of DSSS systems, we employed a matched filter for PN code acquisition and an early-late gate for PN code tracking [9]. For OFDM systems, the correlation peak is detected by finding the maximum point within a sliding window of some predefined length. As shown in Figure 7 and 8, statistics of symbol synchronization errors are obtained from 10000 runs of both DSSS and OFDM system simulations for different SNR (signal-to-noise power ratio) values in AWGN channel. From the results we can observe that DSSS has better performance than OFDM systems, especially for low SNR cases. Using code tracking techniques, DSSS systems can achieve very high symbol synchronization accuracy, but for OFDM systems the probability of synchronization errors that are larger than 2 samples are still pretty high. It should be noted that the synchronization errors are measured in the unit of samples and 10ns time error corresponds to 3m distance error.

Table 1. Parameters for 802.11 DSSS transceiver simulations.

PARAMETER	VALUE
SYNC bits	128 bits of scrambled 1
Bit rate of SYNC	1Mbps
Spreading code	11-chip Barker code
Modulation	DBPSK
Up-sampling rate at receiver	9
Raised-cosine low-pass filter	$T = 1/(1\text{MHz}), \alpha = 0.25$

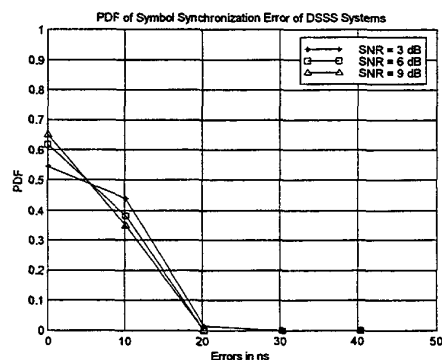


Figure 7. PDF of DSSS symbol synchronization errors (absolute value) for different SNR values.

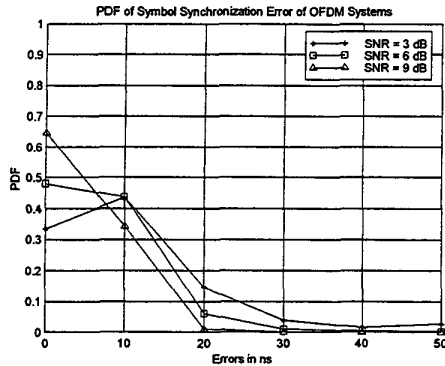


Figure 8. PDF of OFDM symbol synchronization errors (absolute value) for different SNR values.

4. Summary and conclusions

Geolocation methods using 802.11 DSSS systems are presented in this paper. A delay measurement-based TDOA method is proposed for 802.11 wireless LANs, which eliminates the initial synchronization requirement in the conventional methods. The performance of the possible overlaid geolocation systems in DSSS and OFDM wireless LANs are compared in terms of symbol synchronization performance. Basing on our preliminary results and discussions, we can conclude that DSSS systems show higher potential than OFDM systems to accommodate geolocation functions using existing systems and signals. The effects of multipath channels to the performance of the overlaid geolocation systems are to be studied.

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] P. Goud, A. Sesay, and M. Fattouche, "A spread spectrum radiolocation techniques and its applications to cellular radio", *Proc. IEEE Pacific Rim Conf. on Comm., Comp., and Signal Processing*, 1991.
- [2] J.J. Caffery and G.L. Stuber, "Vehicle location and tracking for IVHS in CDMA microcells", *Proc. IEEE PIMRC'94*, 1994.
- [3] J.J. Caffery, *Wireless Location in CDMA Cellular Radio Systems*, Kluwer Academic Publishers, 2000.
- [4] K. Pahlavan, X. Li, M. Ylianttila, and M. Latva-aho, "Wireless data communication systems", Chap. 9 of *Wireless Communication Technologies: New multimedia systems*, edited by R. Kohno, S. Sampei, and N. Morinaga, Kluwer Academic Publishers, 2000.
- [5] K. Pahlavan, P. Krishnamurthy and J. Beneat, "Wideband radio propagation modeling for indoor geolocation applications", *IEEE Comm. Magazine*, pp. 60-65, April 1998.
- [6] J. Werb and C. Lanzl, "Designing a positioning system for finding things and people indoors", *IEEE Spectrum*, vol. 35, no. 9, Sep 1998.
- [7] K. Pahlavan, X. Li, *et al.*, "An overview of wireless indoor geolocation techniques and systems", *Proc. MWCN'2000*, May 2000.
- [8] X. Li, K. Pahlavan, M. Latva-aho, and M. Ylianttila, "Indoor geolocation using OFDM signals in HIPERLAN/2 wireless LANs", *Proc. IEEE PIMRC'2000*, Sep. 2000.
- [9] J.G. Proakis, *Digital Communications*, 3rd Ed., McGraw-Hill, 1995.