RADIO FREQUENCY WATERMARKING FOR OFDM WIRELESS NETWORKS

John E. Kleider, Steve Gifford, Scott Chuprun, and Bruce Fette

General Dynamics, Decision Systems, Scottsdale, Arizona, USA 85257

john.kleider, steve.gifford, scott.chuprun, bruce.fette @gdds.com

ABSTRACT*

Digital watermarking typically allows embedded signals to be separated from audio and video signals for purposes such as copyright protection, distribution tracing, authentication, and authorized access control. In this work we apply watermarking to the physical layer of the wireless baseband modulation waveform, with the motivation to improve flexibility and efficiency of authentication processes in a secure wireless network. We present two baseband watermarking methods called constellation dithering (CD) and baud dithering (BD) applied to Orthogonal Frequency Division Multiplexing (OFDM). We provide the watermark detection and capacity performance attributes in an additive white Gaussian noise (AWGN) channel. Both watermarking techniques allow interoperability with uninformed systems (such as receivers in the 802.11 WLAN commercial standard). Results indicate that, while the BD method provides higher detection robustness and capacity, the CD method exhibits more performance flexibility and is easily modified to the desired user characteristics.

1. INTRODUCTION

Digital watermarking has experienced an intense interest in the research and scientific communities over the past few years. Traditionally, watermarking can be described as the creation of a separate communications side channel that is an imperceptible and intrinsically embedded part of the watermarked source information [1]. The information provided in this channel can be utilized to protect the source information (such as copyright protection), prevent misuse of the information, or enhance the user's capabilities by conveying control information.

Predominantly, watermarking methods have dealt with embedding the watermark signal at or above the medium access layer of the system protocol stack [1] [2]. In these schemes, the information is embedded directly into the media to be protected, is independent of the broadcast or transmission format, and remains present even after decryption [1]. However, in ad hoc networks, the communication transmissions occur in a highly dynamic and open environment, which necessitates insertion of physical layer control or protection. In many cases it is highly desirable to minimize the dependency among the different layers of the protocol stack layers. For example, IS-95 and CDMA-2000 systems insert CRC checking at the physical layer to facilitate power control. User identification is also a desirable feature to insert at the physical layer as proposed in [2], which embeds periodic binary watermark sequences into the convolutionally coded data stream in the transmitter. This scheme provides limited design flexibility because the watermarked signal is not transparent to the regular (uninformed) receiver operating without watermark extraction.

Major concerns exist about wireless security and its effect on the future of evolving wireless LAN standards such as 802.11i [3]. In fact, the concerns are so grave, that the Secretary of Defense has prohibited most uses of wireless information exchange in government facilities because of exploitation vulnerabilities [4]. Similar concerns most certainly could be raised regarding protection of government contractor and commercial enterprise proprietary business and technical data. Even more so, numerous applications of secure wireless LANs exist for military use of ad hoc communication and sensor networks. There is thus a need to investigate potential methods that provide a means of control, identification, and/or authentication of communication nodes at the physical layer. In fact, authentication and key management in a secure ad hoc network becomes burdensome, incurring high delays and inefficient use of handheld power resources, when considering techniques that depend on end-to-end encryption only [4] [5].

This work proposes physical layer watermarking for OFDM as a means of providing an efficient and flexible side information control, identification, and/or authentication channel for use with any ad hoc secure wireless network. While there are potentially many useful watermarking methods for OFDM, that are applicable in practice, we propose two methods that show initial promise due to their ease of implementation, performance attributes, and transparency to the uninformed receiver.

Both methods assume that QPSK (or QAM) is the constellation used for modulating the OFDM sub-channel data, however either method can be used with any QAM constellation. The first method, constellation dither (CD), embeds the watermark information by first mapping the watermark bits to a QPSK watermark constellation, spreading this information using a Gaussian distributed spreading code and then embedding (superimposing) the watermark information onto the OFDM payload data at an imperceptible level. The CD technique has the same effect as a very low-level additive white Gaussian noise signal in the OFDM payload symbols. The level of which the CD is embedded has a very minor effect on the BER performance of the payload data. These performance attributes will be discussed later in the paper. The second method, baud dither (BD), exploits the cyclic properties of the OFDM time-domain signal (after cyclic prefix is attached), by conveying information through positive and negative cyclic time shifts over the transmitted time-domain symbols. The watermark bits are

* Work supported by the U.S. Air Force Research Laboratory under Cooperative Agreement No. F30602-C-02-0182. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Air Force Research Laboratory or the U.S. Government.

first mapped using Manchester encoding to ensure a zero-mean time-shift, with the information conveyed using the 1 or 0 Manchester encoding property. In the BD technique, the primary consideration for receiver performance is ensuring that the receiver tracking loop remains stable, and exhibits the capability to remove timing shifts on each unique OFDM symbol. We will show that both methods provide unique advantages in terms of the capacity of the watermark side channel information, ease of implementation, impact on interoperability, and watermark detection performance.

This paper is organized as follows. Section 2 provides a description of the CD and BD techniques. Section 3 gives the parameters of the OFDM waveform used for this work, while Section 4 provides performance results of both the CD and BD methods. A conclusion is then provided in Section 5.

2. WATERMARKING APPROACH

In an OFDM transmitter, before guard interval (cyclic prefix) insertion, the baseband time-domain signal can be written as $s(t) = \frac{1}{N}\sum_{n=0}^{N-1} d_n^p \exp(j2\pi f_n t)$, and if $f_n = n/(NT_s)$ and $t = mT_s$, where m and n represent the discrete time sample and subcarrier frequency indexes, respectively, and T_s is the sample period, then the discrete sampled signal can be written as

$$s_m = \frac{1}{N}\sum_{n=0}^{N-1} d_n^p \exp(j2\pi \frac{mn}{N}); \qquad m = 0, 1,\ldots,N\text{-}1 \qquad (1)$$

(1) is noticeably the IDFT of d_n^p, where d_n^p is complex-valued, resulting form the payload bit-to-constellation symbol mapping operation using any BPSK, QPSK, or M-ary QAM constellation. After synchronization and guard interval removal, the received sampled signal, in an AWGN channel, can be written as $y_m = s_m + w_m$, where w_m is a zero-mean complex AWGN signal. A noisy version of the OFDM payload symbols can be recovered by passing y_m through a DFT operation in the receiver, written as

$$\hat{d}_n^p = \sum_{m=0}^{N-1} y_m \exp(-j2\pi \frac{mn}{M}); \qquad n = 0, 1,\ldots,N\text{-}1 \qquad (2)$$

where $\hat{d}_n^p$ is then passed through a slicer (QAM demodulator) to determine an estimate of the transmitted symbols d_n^p.

For a multipath fading channel, the guard interval is assumed greater than the maximum channel delay for all reflections with narrowband subcarrier spacing. The transmitted symbols at time-slot m and subcarrier n are disturbed by a factor $H_{m,n}$ (the Fourier transform of the channel impulse response) which is the channel transfer function. In this case, the received signal for time-slot m, denoted as $\hat{d}_{m,n}^p$, can be written as

$$\hat{d}_{m,n}^p = d_{m,n}^p H_{m,n} + w'_{m,n}, \qquad (3)$$

where $w'_{m,n}$ is the Fourier transform of w_m at frequency index n, and the fading channel effects are removed by dividing by $H_{m,n}$.

2.1. Constellation Dither Watermark

The CD signal is generated by first mapping the watermarking information bits to QPSK symbols, represented by d_k^{wm}, and then spreading d_k^{wm} using a Gaussian distributed code, C_G, resulting in a signal $d_{CD} = C_G d_k^{wm}$. A single spread CD watermark symbol is comprised of N_f X N_t discrete samples, resulting in a processing gain, $PG_{CD} = N_f N_t$. The N_f frequency-domain samples of d_{CD} are added to the frequency-domain payload symbols, d_n^p, over N_t OFDM symbols. Scaling is utilized to provide the same power as an OFDM signal without a CD watermark. The frequency-domain composite signal prior to the IDFT operation for a single OFDM symbol can be written as

$$d_n^{pwm} = \sqrt{\alpha} d_{CD} + \sqrt{1-\alpha} d_n^p. \qquad (4)$$

Using (3) and (4), and assuming synchronization is achieved, the watermark information is detected by first match filtering the composite signal $\hat{d}_n^{pwm}$ with tap coefficients C_G^*. This provides a near replica of the QPSK modulated watermark data, which can be written as $\hat{d}_k^{wm}$. $\hat{d}_k^{wm}$ is then passed through a QPSK slicer to recover the transmitted watermark bits.

The OFDM payload signal can be approximated by a Gaussian distribution [6], and thus disturbs the watermark signal in a manner similar to additive white Gaussian noise (AWGN). In the AWGN channel, the received signal and noise powers are given by $\sigma_y^2 = E\left[|y_m|^2\right]$ and $\sigma_w^2 = E\left[|w_m|^2\right]$, respectively, where E is the expected value operator. Given α, the received payload SNR is $SNR_p = (1-\alpha)\sigma_y^2 / (\alpha\sigma_y^2 + \sigma_n^2)$, and the watermark signal SNR prior to dispreading is, $SNR_{CD} = \alpha\sigma_y^2 / \left[(1-\alpha)\sigma_y^2 + \sigma_w^2\right]$. The watermark detection SNR after despreading is $SNR_{CDds} = PG_{CD} \cdot SNR_{CD}$. The bit rate for the CD scheme can be written as $R_{CD} = 2/(T_{sym}N_t)$ bits/sec, where T_{sym} is the total OFDM symbol length including the guard interval and the "2" arises from mapping of 2 watermark bits per QPSK constellation symbol.

Clearly, the watermark detection performance will depend on both the processing gain, PG_{CD}, and α. For example, using a typical value of $\alpha = 0.01$, with $N_f = 180$ subcarriers, $N_s = 10$ OFDM symbols, and ignoring receiver noise, results in an $SNR_{CDds} \cong 12.6$ dB. Assuming we use QPSK demodulation, this results in a fairly low demodulated BER of approximately 10^{-5}. The communications capacity for the CD method will thus be a function of SNR_{CDds}, and provides very flexible tradeoffs in terms of BER performance and transmitted watermark bit rate. Since the payload information will typically be sent un-spread, α must be small enough to minimize any degradation to the payload demodulated BER. Results on this degradation will be presented in Section 4.

2.2. Baud Dither Watermark

The BD watermark can generally be described as a controlled timing jitter process induced onto the OFDM symbols after cyclic prefix insertion. The signal is generated by first encoding the watermark information according to a Manchester (or biphase) encoding rule [7]. The purpose of the Manchester encoding is to ensure that the average jitter is zero over any watermark bit. For example, given the watermark bit sequence b_{wm} = [1, 0, 1, 1, 0, 0, 1], the resulting Manchester encoded bits are Mb_{wm} = [+1-1, -1+1, +1-1, +1-1, -1+1, -1+1, +1-1], which results in the following controlled offset pattern, δt = [+1,-1,-1,+1,+1,-1,+1,-1,-1,+1,-1,+1,+1,-1]. δt_m can be applied using fractional- or integer-valued discrete time shifts, but each

discrete shift must be applied one-to-one to the OFDM symbols. This ensures minimal degradation to the receiver tracking circuit performance. Using our example δt_m above, which has a length 14, δt_m must then be applied over 14 consecutive OFDM symbols of baud dither. Given the OFDM baseband transmit signal is defined by $s_m = [s_0, s_1, s_2, s_3, s_4, s_5, s_6]$, then after guard interval insertion we can write the signal as $s_{mg} = [s_{m4}, s_{m5}, s_{m6}, s_{m0}, s_{m1}, s_{m2}, s_{m3}, s_{m4}, s_{m5}, s_{m6}]$, assuming the discrete sample length of the guard interval, $L_{GI} = 3$ samples.

The guard interval is used as a means of preserving orthogonality between OFDM symbols that are subjected to ISI from the channel and/or filtering. We note that as long as the largest multipath delay, L_m, is less than the guard interval length minus the induced shift or $L_{GI} - \delta t_m$, then there will be no ISI performance degradation caused by the BD watermark. Due to the cyclic nature of signal s_{mg}, a very simple method can be used to induce the controlled timing dither. For instance, let $\delta t_m = [+1,-1]$, where $m = 1, 2$. The two resulting baud dithered OFDM symbols would be $s_{1g} = [s_{16}, s_{14}, s_{15}, s_{16}, s_{10}, s_{11}, s_{12}, s_{13}, s_{14}, s_{15}]$ and $s_{2g} = [s_{25}, s_{26}, s_{20}, s_{21}, s_{22}, s_{23}, s_{24}, s_{25}, s_{26}, s_{24}]$, respectively. In the BD scheme, a single watermark bit is spread across 2 OFDM symbols (reference Manchester encoding above), thus in this case we have $N_t = 2$ and $N_f \approx N_p$ as the processing gain realized from the receiver tracking circuit which utilizes N_p pilots to resolve fine synchronization estimates. The bit rate for the BD scheme can be written as $R_{CD} = 1/(T_{sym}N_t)$ bits/sec. Specifically, if we set N_t to 2 and 10 for the BD and CD schemes, respectively, $R_{BD} = (5/2)R_{CD}$. However, due to the large difference in the design between the BD and CD methods, it is impossible to set the detection SNR equal for both cases over all received SNR values.

The BD detection performance is primarily dependent on the received payload SNR, SNR_p, and the processing gain provided by the number of pilots used in the receiver tracking circuit (note that SNR_p in the BD method is not equivalent to the SNR_p for the CD approach). The processing gain of the receiver tracking algorithm is approximately $PG_{\text{track}} \approx N_f^{'} / N_{dd}$, where $N_f^{'}$ is the number of frequency subcarriers at the pilot subcarrier indexes that are utilized in the tracking algorithm. N_{dd} is the performance penalty due to the differential process used to estimate timing offset. If the average time offset over multiple OFDM symbols is $\bar{t}_{offset} = E[t_{offset}]$, where $E[]$ is the expected value operator, and t_{offset} is the tracking algorithm estimate of the time offset of each individual OFDM symbol, then the watermark instantaneous offset over each OFDM symbol can be written as $t_m^{wm} = \bar{t}_{offset} - t_{offset}$. Note that $\bar{t}_{offset}$ represents the actual untracked receiver timing error, which exists regardless of the BD process timing perturbations induced at the transmitter. $\hat{\delta}t_m$ is found by computing the Signum function of t_m^{wm}. Subsequently, the Manchester words are formed and the watermark bits are recovered with the reverse process performed at the transmitter.

From the above BD detection scheme, it is evident that the performance will depend on both the received signal SNR and the associated performance of the receiver tracking algorithm. In noisy channels, phase calculations may result in 2π ambiguities, which cannot be resolved, thus producing undesirable timing error estimates. However, this will happen even without a BD watermark. We will see in Section 4 that for reasonable values of SNR, the BD watermark is very robust in terms of its detection performance. In the BD scheme, the detection SNR can be written as $SNR_{BD} = PG_{track} \cdot SNR_p$. In this case if $PG_{track} = 6$ dB and $SNR_p = 10$ dB, then $SNR_{BD} = 16$ dB. We know that the probability of improperly decoding the Manchester shift sequence is proportional to the bit error probability for BPSK signaling. However, since N_{dd} changes as a function of the received SNR, SNR_{BD} is not always a constant multiple of SNR_p. As we will show in Section 4, this variable SNR gap between SNR_{BD} and SNR_p was confirmed via simulation of the BD and OFDM payload BER performance.

3. OFDM WAVEFORM

The same OFDM waveform was used to host both watermarking methods, described by the following parameters: RF bandwidth $\approx$ 1 MHz, $T_{sym} = 251.4$ μsec, N=256 total subcarriers, 76 null carriers, 160 of data-bearing carriers, and 20 pilot carriers. The baseband sample rate is 1.2727 Msps. We note that this OFDM waveform was successfully implemented using the CD watermark and transmitted over the air using a wireless testbed and source data comprised of digitally compressed imagery.

4. WATERMARK PERFORMANCE RESULTS

The bit error rate (BER) for BPSK and QPSK signaling can readily be found in the literature to be

$$P_B = Q\left(\sqrt{2E_b/N_0}\right), \tag{5}$$

where E_b is the energy per information bit and $N_0 = 2\sigma_w^2$ is the single-sided receiver noise spectral density. If we let $SNR = 2E_b/N_0$, and since both the payload and watermark utilize QPSK modulation, the CD watermark BER, P_B^{CD}, and OFDM payload BER, P_B^p, can be computed by inserting SNR_{CDds} and SNR_p (ref. Section 2.1), respectively, into (5). For the BD method, $SNR_p = \sigma_y^2 / \sigma_w^2$, and thus the performance of the OFDM payload is unaffected by the watermark insertion and can be computed directly from (5). The BD BER, P_B^{BD}, however, requires insertion of SNR_{BD} (ref. Section 2.2) before an analytical solution can be computed.

From Section 2.1, we see a relationship between R_{CD} and P_B^{CD}. For example, varying N_t will affect both R_{CD} and SNR_{CDds} and consequently P_B^{CD}. Figure 1 illustrates this relationship by plotting P_B^{CD} and R_{CD} as a function of SNR_{CDds} for the case when $N_f = 160$ and $1 < N_t < 1000$. The simulated BER confirms the analytic predictions of the watermark BER. Figure 2 shows the associated degradation in P_B^p as a function of α for the CD method. As can be seen from Figure 2, very little degradation occurs to P_B^p, provided α is low (< 0.01).

Simulated performance of P_B^{BD} and P_B^p versus received SNR was used to evaluate performance of the BD technique. In this case both DQPSK and QPSK were used as the payload modulation choices. For the BD method we chose to plot the performance using a fixed watermark bit rate of 1.99 kbit/sec. We note that variable bit rates are also possible and will be a

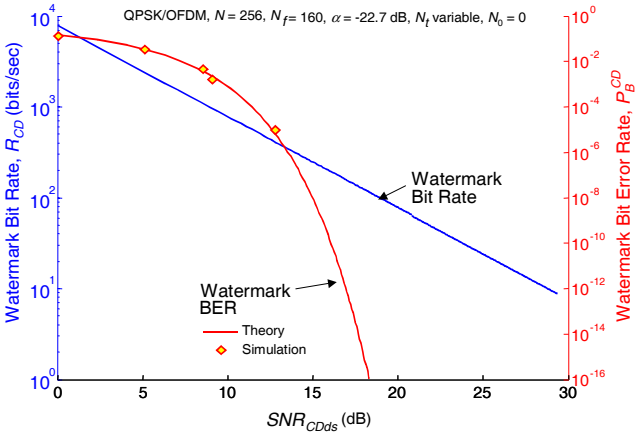

Figure 1: R_{CD} and P_B^{CD} versus SNR_{CDds} for CD watermark.

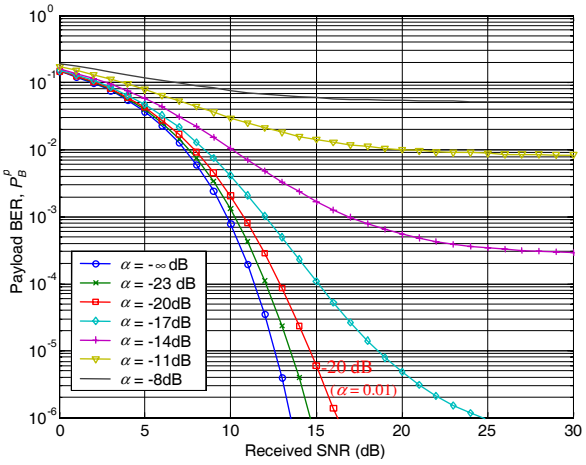

Figure 2: CD watermark P_B^p versus received SNR for varying α.

function of detection SNR, however, higher capacity methods will require receiver tracking loop algorithm modifications and thus, we did not consider this viable due to interoperability issues when applied to existing OFDM waveform standards. Figure 3 shows the respective BER for the payload and watermark signals. We highlight two points from Figure 3. First, it is clear that the watermark BER performance is significantly better than the payload, and in addition does not affect the performance of the payload BER for either DQPSK or coherent QPSK (the BER performance curves for the payload is the same with and without the BD watermark).

We were also interested in finding R_{CD} and R_{BD} for 802.11 OFDM applications, since both watermarking schemes could provide enhanced and more flexible authentication choices in ad hoc scenarios for secure wireless LAN applications. Using approximately equivalent detection SNRs for each scheme, results in R_{CD} = 12.5 kbits/sec and R_{BD} = 15.6 kbits/sec when applied to the OFDM 802.11a physical layer. This watermarking capability can provide some unique control, identification, or authentication capabilities and enhance efforts toward secure wireless LAN applications, especially in roaming ad hoc configurations. In our testbed measurements, we found there to be no visual perturbations to the OFDM transmitted spectrum using the CD technique, while the received statistics retained their original Gaussian noise-like distribution.

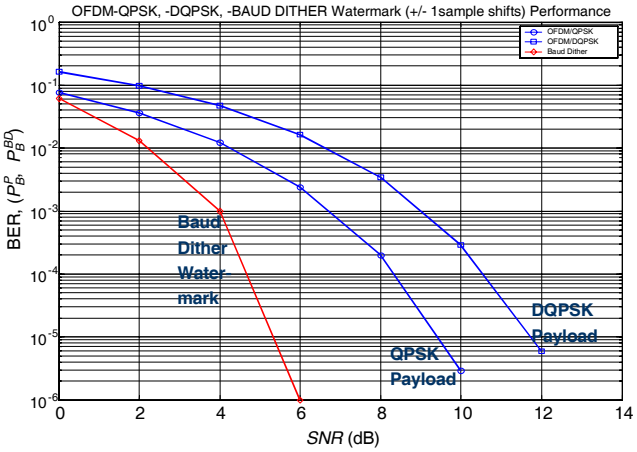

Figure 3: OFDM payload and BD watermark BER performance.

5. CONCLUSIONS[#]

CD and BD watermarking methods were presented as potential methods for source information protection and network node identification and/or authentication in secure wireless OFDM networks. The CD technique has been implemented on a prototype wideband OFDM waveform transmitting compressed digital imagery. Over the air testing confirms the simulated results presented in this paper, with no perceptual degradation in the reconstructed image quality and no visual or statistical differences to the transmitted spectrum or time-domain OFDM waveform. The BD technique was presented as a more robust and higher capacity watermarking approach, but requires specific attention to operational performance in the receiver tracking circuit to maintain interoperability with non-informed receivers (such as an 802.11a OFDM PCMCIA card operating without BD detection).

6. REFERENCES

[1] I.J. Cox, M.L. Miller, and A.L. McKellips, "Watermarking as communications with side information," *Proc. of IEEE*, vol. 87, no. 7, pp. 1127-1141, July 1999.

[2] Y. Jiang and F.-W. Sun, ""Watermarking" for convolutionally/turbo coded systems and its applications," *Proc. of Globecomm*, vol. 87, no. 7, pp. 1127-1141, 2001.

[3] B. Potter, "Wireless security's future," *Security & Privacy Mag.*, vol. 1, no. 4, pp. 68-72, July-Aug. 2003.

[4] H. Feil, "802.11 wireless network policy recommendation for usage within unclassified government networks," *Proc. of MILCOM*, Oct. 2003.

[5] D. Carman and G. Cirincione, "Energy and latency costs of communicating certificates during secure network initialization of sensor networks," in *Proc. of Collaborative Technologies Alliance Conference*, pp. 113-118, April-May 2003.

[6] H. Ochiai and H. Imai, "On the distribution of the peak-to-average power ratio in OFDM signals," *IEEE Trans. On Comm.*, vol. 49, no. 2, pp. 282-289, Febr. 2001.

[7] J.D. Spragins, J.L. Hammond, and K. Pawlikowski, *Telecommunications Protocols and Design*, Addison-Wesley Publ. Co., Inc., 1991.

[#] The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Air Force Research Laboratory or the U.S. Government.