

Building Robust Wireless LAN for Industrial Control with DSSS-CDMA Cellphone Network Paradigm

Qixin Wang*, Xue Liu*, Weiqun Chen[†], Wenbo He*, and Marco Caccamo*

* Department of Computer Science, University of Illinois at Urbana-Champaign

Email: {qwang4, xueliu, wenbohe, mcaccamo}@uiuc.edu

[†] ECECS Department, University of Cincinnati

Email: chenwq@ececs.uc.edu

Abstract

Deploying Wireless LAN for Industrial Control (IC-WLAN) has many benefits, such as mobility, low deployment cost and ease of reconfiguration. However, the top concern is robustness of wireless communications. Wireless control loops must be maintained under persistent adverse channel conditions, such as noise, large-scale path loss and fading. Many electro-magnetic interference sources in industrial environments, e.g. electric motor and welding, make wireless communication more challenging. The conventional IEEE 802.11 WLANs, which are designed for providing high bandwidth instead of high robustness, are therefore inappropriate for IC-WLAN. On the other hand, if the low data rate feature of industrial control is fully exploited by the state-of-the-art Direct Sequence Spread Spectrum (DSSS) technology, much higher robustness can be achieved. We hereby propose using DSSS-CDMA to build IC-WLAN, and exploiting the low data rate feature of industrial control loops for enhanced robustness. We carried out fine-grained physical layer simulations and Monte Carlo comparisons. The results show that DSSS-CDMA IC-WLAN provides much higher robustness than IEEE 802.11 WLAN, so that reliable wireless industrial control loops are made feasible. The DSSS-CDMA IC-WLAN scheme also opens up a new problem space for interdisciplinary study, involving real-time scheduling and resource management, communication, networking and control. In this paper, we study the resource management problems on maximizing robustness and minimizing control utility loss. Analytical resource optimization solutions are given.

1. Introduction

Recently, there are increasing efforts in deploying *Wireless LANs* (WLAN) for industrial control

[28][37][38][16][22]. *Industrial Control WLAN* (IC-WLAN) has many desirable features, such as extended mechanical freedom and mobility, low deployment cost and ease of reconfiguration, and is therefore important for the deployment of robots, automatic vehicles and distributed manufacturing systems. At a larger scale, deploying IC-WLAN is also part of the efforts toward ubiquitous computing.

However, IC-WLAN also raises new challenges, among which, probably the most outstanding one is its robustness. WLAN communications are inherently more vulnerable than wired LAN communications due to many reasons, e.g. multiple-access contention, *Radio Frequency* (RF) interference, large-scale path loss and fading [31]. IC-WLANs pose much higher robustness requirements than conventional WLANs for office or home use. For most office or home WLAN applications, it is acceptable to have a few seconds or even minutes of RF interference, such as accidentally turning on an uncooperative device which broadcasts at the same RF band as the existing WLAN. The interfered wireless connections just need to backoff till the interference is over and then retransmit. In fact, this is the standard behavior adopted by IEEE 802.11 WLAN [2][3][4][7], which is the nowadays dominant WLAN scheme. However, for industrial control, such behavior is often not acceptable. Most distributed industrial control loops are real-time, the backoff behavior will cause deadline misses, result in performance losses, halts/resets of manufacturing pipelines or defects in products. For example, a couple of hundred milliseconds of backoff is enough to make an inverted pendulum fall. Therefore, for most industrial controls, communications must be maintained even under adverse channel conditions. To achieve such robustness, cables of industrial control wired LANs are shielded to protect against interference. For wireless LAN, providing similar “shielding” is more necessary and challenging. The interfering RF sources can be other radio devices that use the same RF

band, turned on inside or even outside of the factory; or the many *Electro-Magnetic Interference* (EMI) sources, such as electric motors or electric welding [39][13]. The EMI is especially challenging, not only because it is common to industrial environments, but also because it is persistent, e.g. an electric motor can run for hours or days. Also, due to heavy obstructions, the wireless mediums of industrial environments are known to suffer much more serious large-scale path loss and fading than other indoor environments [31].

Generically speaking, RF interference, large-scale path loss and fading reduce the *Signal-to-Noise Ratio* (SNR) of the wireless channel. When the SNR is lower than a certain threshold, the *Bit Error Rate* (BER) rises over the acceptable limit, and the wireless connection may break down. Therefore, for IC-WLAN, it is necessary to provide highest SNR possible to maintain wireless control loops under adverse conditions. A promising solution lies in the state-of-the-art *Direct Sequence Spread Spectrum* (DSSS) technology. DSSS has the desirable feature that allows tradeoffs between data throughput versus SNR. Specifically, a smaller data throughput (for control loops, it means slower sampling/actuating rates and smaller packet sizes) corresponds to a higher SNR and vice versa. On the other hand, industrial control loops usually consist of low-data-throughput stable traffics [27]. For example, due to decades of development and wide deployment of step motors [23][25], for most contemporary industrial mechanical controls, fine-grained high-rate controls are carried out locally, whereas control traffics between distributed nodes are mostly coarse-grained, consisting of low sampling/actuating rates and small packet sizes. Typically, the sampling/actuating rates between distributed nodes are around or below 10Hz, sometimes even around 1Hz; the packet size are usually around a couple of hundred bits.

In this paper, we are interested in exploiting the features of control loop traffic and DSSS technology to build robust IC-WLANs. By carrying out fine-grained physical layer simulations and Monte Carlo comparisons, we show that when the low data rate feature of control loops is fully exploited, DSSS can achieve much higher robustness than what is provided by IEEE 802.11, so that wireless industrial control is made practical (see Section 4). Specifically, around 10 ~ 20dB and 25 ~ 35dB robustness improvements are achieved compared to IEEE 802.11b and IEEE 802.11a respectively, which are significant according to communication engineering criteria.

Meanwhile, compared to the predominant ad hoc paradigm of IEEE 802.11 WLAN, the conventional DSSS-CDMA cellphone network paradigm is also more desirable for IC-WLAN. That is, every WLAN is a cell, with one *Basestation* (BS) and several *Remote Stations* (RS). Wireless communications only take place between a basestation

and a remote station of the same cell. Inter-cell communications are carried out through wireline backbones between basestations. The reasons are as following: i) Control loop traffics are often periodic traffics with low data rates, and most control logics incur low computation. Therefore it is a common and economic practice in factories to have one powerful centralized basestation controlling all machines in a local area [27]. A lots of legacy systems are built upon such basestation-centered communication paradigm. ii) The basestation-centered paradigm also makes centralized real-time scheduling easy to implement. In practice, centralized real-time scheduling is often more preferable than distributed real-time scheduling due to its robustness and simplicity. iii) Industrial control applications are typically deployed in well-built permanent facilities, where powerful wireline backbones for inter-basestation communications are available. Therefore, in most cases, the benefits of wireless communications (mechanical freedom, mobility, flexibility) are only significant at the last hop. A cellphone network paradigm matches such demand. iv) At the MAC layer, CDMA is more preferable because of its ease of scheduling, overrun isolation and low overhead.

The main contribution of this paper is to point out that by fully exploiting the low data rate feature of industrial control loops, the conventional DSSS-CDMA cellphone network paradigm is a better approach for building robust IC-WLAN, although IEEE 802.11 is the nowadays predominant WLAN scheme. However, contemporary DSSS-CDMA cellphone networks are still more focused on providing higher data throughput instead of higher robustness, and no much effort has been made to customize resource allocations to the needs of industrial control. In this paper, we study the resource management issues on DSSS-CDMA IC-WLAN. Analytical resource optimization solutions are given for maximizing robustness and minimizing control utility loss respectively. Our study also show that the resource management problems on DSSS-CDMA IC-WLAN are non-trivial. In fact, DSSS-CDMA IC-WLAN scheme opens up a new problem space for interdisciplinary study, involving real-time scheduling and resource management, communication, networking and control.

The rest of the paper is organized as follows: Section 2 gives background on DSSS technology. The DSSS-CDMA IC-WLAN is proposed in Section 3, together with some analytical results on its resource optimization. Fine-grained physical layer simulations are carried out in Section 4 to illustrate the robustness of the DSSS-CDMA IC-WLAN, followed by more extensive Monte Carlo simulations that compare the robustness with IEEE 802.11 WLANs. Related works are discussed in Section 5. Section 6 concludes the paper.

2. Background

DSSS is a physical layer modulation/demodulation scheme for digital communication [35][33][18]. It reshapes baseband signal to occupy a wider spectrum¹. At the transmitter, a user data bit stream of bit rate r_b (i.e. bit duration of $T_b \stackrel{def}{=} 1/r_b$) is *scrambled* with a *Pseudo Noise* (PN) sequence of *chip rate* r_c (i.e. chip duration of $T_c \stackrel{def}{=} 1/r_c$), producing a chip stream of rate r_c . r_c is a positive integer multiple of r_b , the ratio $g \stackrel{def}{=} r_c/r_b$ is called *processing gain*. At the receiver, if the chip stream is *descrambled* with the same PN sequence, the original data bit stream is recovered. If a different PN sequence is applied, or the scramble/descramble PN sequences are not synchronized, the original data bit stream cannot be recovered, instead, a noise-like random chip stream is generated. To summarize, each PN sequence creates a DSSS data channel. Note although DSSS requires synchronization between each transmitter-receiver pair, synchronizations between transmitters are not needed if CDMA is deployed at the MAC layer. More details on DSSS and its terminologies are elaborated in [36] Appendix I.

At the MAC layer, most contemporary digital wireless systems pick either of the two alternatives: one is *Code Division Multiple Access* (CDMA), the other is *Time Division Multiple Access* (TDMA). If DSSS-CDMA is deployed, different data bit streams scrambled with different PN sequences are transmitted in parallel through the same RF band. At the receiver, by applying different PN sequences, the intended data bit stream is filtered out. If DSSS-TDMA is deployed, different data bit streams scrambled with different PN sequences occupy non-overlapping time slots, which requires more sophisticated scheduling schemes. Though either alternative is feasible, we find DSSS-CDMA to be more preferable for IC-WLANs for the following reasons: i) ease of real-time scheduling; ii) inherent isolation between connections; iii) less communication overhead, especially under adverse channel conditions. The first two points are straightforward and interrelated: Under CDMA architecture, a connection exclusively occupies one or several CDMA channels (PNs), i.e., at MAC layer and above, CDMA channels are not shared. There is no need to schedule different real-time connections within one CDMA channel, and the overrun of one real-time connection does not affect any other real-time connections. In contrast, in a TDMA scheme, time slots must be scheduled to serve

¹For convenience, we refer to DSSS as a *baseband* modulation/demodulation scheme. Correspondingly, the modulation/demodulation scheme that shifts baseband signal to/from RF band is referred to as RF modulation/demodulation. Typical RF modulation/demodulation schemes for DSSS can be *Quadrature Phase Shift Keying* (QPSK) or *Binary Phase Shift Keying* (BPSK), both can achieve same robustness (in sense of BER) with same SNR per bit [35][20].

different real-time connections, and if a real-time connection overruns its time slot, subsequent real-time connections will be affected. The third point needs more elaboration: Generically speaking, DSSS requires time synchronization between transmitter and receiver. However, under adverse channel conditions, TDMA incurs much more time synchronization overhead than CDMA. Further quantitative analysis is given in [36] Appendix II.

Quantitatively, a number of important features of DSSS communication is captured by its *Bit Error Rate* (BER) upper bound (1), which assumes QPSK RF modulation, and per connection pilot tone [35][26] (different implementation alternatives may affect details of the formula, but will not cause fundamental differences):

$$\mathcal{P}_{ber} \leq \exp \left(- \frac{gP_u}{J + \sum_{i=1, i \neq u}^{\Xi} P_i + \sum_{h=1}^H A_h + P_u} \right) \quad (1)$$

where \mathcal{P}_{ber} is the BER; g is processing gain; J is the received power of *External RF Interference* (EI), which specifically refers to EMI, thermal noise and the RF interference from RF devices that are turned on accidentally or maliciously. P_i ($i = 1 \dots \Xi$) is the received power of CDMA channel i , Ξ is the total number of CDMA channels. u is the intended channel, whose corresponding received power is P_u . Each transmitting node may send out several CDMA channels in parallel. To ease the reception, the node may also transmit an additional pilot tone. In (1) the pilot tone of transmitting node h ($h = 1, \dots, H$) is of power A_h . $\sum_{i=1, i \neq u}^{\Xi} P_i + \sum_{h=1}^H A_h$ is therefore the upper bound of total *Multiple Access Interference* (MAI), i.e. the interference caused by other CDMA channels and pilot tones received in parallel with the intended channel. Note P_u also appears in the denominator, adding up to the total interference power. This is to provide a pessimistic estimation on *Inter Symbol Interference* (ISI), which is usually a result of multipath fading. To simplify, we can merge $\sum_{i=1, i \neq u}^{\Xi} P_i$ and P_u together to be denoted as $\sum_i P_i$. The $gP_u / (J + \sum_i P_i + \sum_h A_h)$ part shows the effective SNR for the intended channel, where $J + \sum_i P_i + \sum_h A_h$ represents the upper bound of noise power and gP_u represents effective signal power. The bigger the SNR, the smaller the probability of bit error \mathcal{P}_{ber} . When \mathcal{P}_{ber} is below a certain threshold Θ_{ber} , the wireless communication is acceptable for industrial control. Therefore, to maintain a IC-WLAN channel in fact means to maintain the SNR of the channel from dropping below an acceptable threshold Θ_{snr} .

Without error correction coding, the *Packet Error Rate* (PER) \mathcal{P}_{per} is:

$$\mathcal{P}_{per} = 1 - (1 - \mathcal{P}_{ber})^{L^{pkt}} \quad (2)$$

Or equivalently:

$$\mathcal{P}_{ber} = 1 - (1 - \mathcal{P}_{per})^{1/L^{pkt}} \quad (3)$$

where L^{pkt} is the bit length of the packet. When error-correction coding is deployed, such as convolutional code [30], (2) will have a more complicated form, but still, \mathcal{P}_{per} decreases as \mathcal{P}_{ber} decreases. Generally speaking, a maximum acceptable packet error rate Θ_{per} corresponds to a maximum acceptable bit error rate Θ_{ber} , which further maps to a minimum acceptable SNR Θ_{snr} . Specifically, we should maintain:

$$\frac{gP_u}{J + \sum_i^E P_i + \sum_h^H A_h} \geq \Theta_{snr} \quad (4)$$

$$= -\ln \Theta_{ber} \quad (5)$$

(because of (1))

$$= -\ln \left(1 - (1 - \Theta_{per})^{1/L^{pkt}} \right) \quad (6)$$

(because of (3))

(1) implies that SNR of the intended channel can be raised by increasing the processing gain g . Meanwhile, g is defined as the ratio of chip rate and bit rate: $g \stackrel{def}{=} r_c/r_b$. Usually, chip rate r_c is fixed by hardware because of multipath effect and hardware cost constraints [29][35], therefore raising processing gain means slowing down user data bit rate r_b . DSSS hereby provides a mechanism to leverage between SNR and data bit rate. Later on, we will carry out resource optimization analysis based on the above equation/inequations (see Section 3.2 and 3.3).

3. DSSS-CDMA IC-WLAN Architecture

3.1. The Overall Architecture

According to the analysis of Section 1 and 2, we choose to design our IC-WLAN following the DSSS-CDMA cellphone network paradigm, which deploys DSSS for physical layer, and CDMA for MAC. In each cell, there is a *Basestation* (BS). Basestations of different cells are connected via wireline. The wireless communications only take place between a basestation and a *Remote Station* (RS) of the same cell. Specifically, the IC-WLAN architecture is illustrated by Fig. 1.

In this paper, we focus on the single cell scenario. The whole RF band is evenly partitioned into two halves, one for downlink (from basestation to remote stations) and the other for uplink (from remote stations to basestation)². Each connection consists of one CDMA channel in each direction (downlink and uplink). Unless explicitly denoted, “connection n ” a.k.a. “control loop n ” refers to both downlink and uplink of the connection; “a CDMA channel of

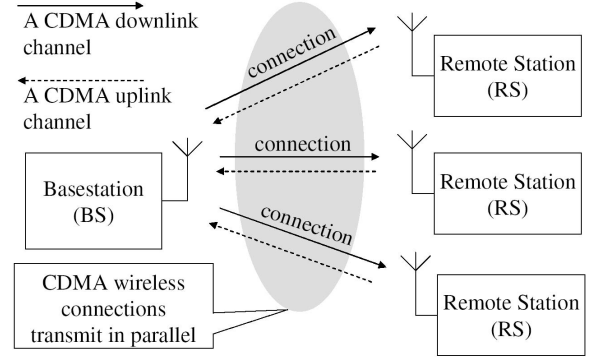


Figure 1. DSSS-CDMA IC-WLAN architecture

connection n ” also refers to both channels in downlink and uplink. Sampling/actuating packets are sent continuously in each CDMA channel, i.e., the bits of consequent sampling/actuating packets of same control loop form a continuous bit stream, similar to the cellphone *session* pattern. Therefore, the sampling/actuating period is the same as the packet transmission period.

3.2. Resource Planning for Maximized Robustness

Based on given conditions and different optimization goals, various resource planning problems can be formulated. Since robustness is often the top concern for IC-WLAN, let us first analyze the optimal configuration for maximized robustness.

Suppose the following parameters are given: The set of control loops to be included in the IC-WLAN are $\mathcal{C} \stackrel{def}{=} \{C_1, C_2, \dots, C_N\}$. Each control loop C_n ($n = 1, 2, \dots, N$) corresponds to a minimum sampling/actuating rate f_n^{min} , a maximum acceptable packet error rate Θ_n^{per} , and a sampling/actuating packet bit length L_n^{pkt} (suppose sampling/actuating packets are of same length, if not, paddings are used to make them the same). Each node can transmit with maximum power of P^{max} . In the uplink, power balancing is carried out to deal with near-far problem [31]. Without loss of generality, suppose the conventional QPSK RF modulation/demodulation and per node pilot tone are deployed. The power level of a node’s pilot tone is the same as that of a CDMA data channel. The hardware fixed chip rate is r_c , which corresponds to a chip duration of $T_c = 1/r_c$.

The configurable parameters are the control loops’ processing gain g_n , with the following value range:

$$1 \leq g_n \leq g^{max}, \text{ and } g_n \text{ is an integer. } n = 1, 2, \dots, N. \quad (7)$$

where g^{max} is a hardware-implementation-dependent constant (e.g. if g_n is specified by an unsigned byte in the hardware, then g_n can not exceed 256).

²This is a common practice for CDMA architecture, so that the receiver is not interfered by the transmitter of the same node.

On the other hand, given chip rate r_c , packet bit length L_n^{pkt} , and the chosen processing gain g_n , the packet rate f_n (i.e. the number of packets that can be transmitted per second) is:

$$f_n = \frac{r_c}{g_n L_n^{pkt}} \quad (8)$$

The packet rate should not violate minimum sampling/actuating rate requirement, that is:

$$\begin{aligned} f_n \geq f_n^{min} &\Leftrightarrow \frac{r_c}{g_n L_n^{pkt}} \geq f_n^{min} \\ \Leftrightarrow g_n &\leq \frac{r_c}{L_n^{pkt} f_n^{min}}, \quad n = 1, 2, \dots, N. \end{aligned} \quad (9)$$

As for the wireless medium, let J_n ($n = 0, 1, 2, \dots, N$) be the external RF interference power received by node n (node 0 refers to the basestation, node $1, 2, \dots, N$ refer to the remote station of connection $1, 2, \dots, N$ respectively). Suppose the downlink/uplink power attenuation for connection n are α_n^{down} and α_n^{up} respectively.

The robustness requirement for connection n is that the packet error rate should not exceed a threshold Θ_n^{per} , both in downlink and uplink. According to (6), the maximum acceptable packet error rate Θ_n^{per} can be mapped to a minimum acceptable SNR Θ_n^{snr} .

According to (4), the robustness requirement for downlink of connection n is formalized as:

$$\frac{g_n P_{nn}^{r-dnlk}}{J_n + \sum_{i=1}^N P_{ni}^{r-dnlk} + A_n^{r-dnlk}} \geq \Theta_n^{snr}, \quad (10)$$

$$n = 1, 2, \dots, N.$$

where P_{ni}^{r-dnlk} ($i = 1, 2, \dots, N$) is the received power of CDMA downlink channel i at remote station n . A_n^{r-dnlk} is the received pilot tone power at remote station n (for downlink, basestation is the only node that transmits pilot tone). Assume the basestation transmission power allocated to all N downlink channels are equal, and the pilot tone is of same power level as a CDMA channel. Also, for maximum robustness, the basestation should transmit with its maximum power P^{max} , therefore:

$$\begin{aligned} P_{n1}^{r-dnlk} &= P_{n2}^{r-dnlk} = \dots = P_{nN}^{r-dnlk} \\ &= A_n^{r-dnlk} = \alpha_n^{down} \frac{P^{max}}{N+1} \end{aligned} \quad (11)$$

Substituting (11) into (10), the downlink robustness requirement is transformed to:

$$\frac{\alpha_n^{down} g_n P^{max}}{(N+1)(J_n + \alpha_n^{down} P^{max})} \geq \Theta_n^{snr}, \quad (12)$$

$$n = 1, 2, \dots, N.$$

According to (4), the robustness requirement for uplink of connection n shall be formalized as:

$$\frac{g_n P_n^{r-uplk}}{J_0 + \sum_{i=1}^N P_i^{r-uplk} + \sum_{i=1}^N A_i^{r-uplk}} \geq \Theta_n^{snr}, \quad (13)$$

$$n = 1, 2, \dots, N.$$

where P_i^{r-uplk} ($i = 1, 2, \dots, N$) is the received power of CDMA uplink channel i at the basestation. A_i^{r-uplk} ($i = 1, 2, \dots, N$) is the (basestation's) received power of pilot tone transmitted from remote station i . Because of power balancing, there should have:

$$P_1^{r-uplk} = P_2^{r-uplk} = \dots = P_N^{r-uplk} \quad (14)$$

On the other hand, assume for each remote station i ($i = 1, 2, \dots, N$), its transmission power P_i^{t-uplk} is equally divided by uplink channel i and the pilot tone, then:

$$P_i^{r-uplk} = A_i^{r-uplk} = \alpha_i^{up} \frac{P_i^{t-uplk}}{2}, \quad i = 1, 2, \dots, N. \quad (15)$$

Lastly, each remote station cannot transmit with power larger than P^{max} , i.e.:

$$P_i^{t-uplk} \leq P^{max}, \quad i = 1, 2, \dots, N. \quad (16)$$

The transmission power of each remote station P_i^{t-uplk} should be maximized to increase SNR (and therefore robustness), meanwhile maintaining the constraints of (14) and (16). Therefore, the remote station that suffers the worst case uplink power attenuation should transmit with power P^{max} , and all other remote stations should adjust their transmission power according to (14). Formally:

$$P_k^{t-uplk} = P^{max},$$

$$\text{therefore } P_k^{r-uplk} = A_k^{r-uplk} = \alpha_k^{up} \frac{P^{max}}{2}, \quad (17)$$

$$\text{where } k = \operatorname{argmin}_{i \in \{1, 2, \dots, N\}} \{\alpha_i^{up}\}. \quad (18)$$

Note operator $\operatorname{argmin}_{x \in \mathcal{A}} \{F(x)\}$ returns $x^* \in \mathcal{A}$, such that $\forall x \in \mathcal{A}, F(x^*) \leq F(x)$.

(14), (15)

$$\Rightarrow P_i^{r-uplk} = A_i^{r-uplk} = \alpha_i^{up} \frac{P_i^{t-uplk}}{2} = P_k^{r-uplk} \quad (19)$$

$$\Rightarrow P_i^{t-uplk} = \frac{\alpha_k^{up} P^{max}}{\alpha_i^{up}} \quad (\text{because of (17)})$$

$$\Rightarrow P_i^{r-uplk} = A_i^{r-uplk} = \alpha_k^{up} \frac{P^{max}}{2}. \quad (20)$$

Denote

$$\alpha_k^{up} \stackrel{def}{=} \alpha_k^{up} = \min\{\alpha_1^{up}, \alpha_2^{up}, \dots, \alpha_N^{up}\}, \quad (21)$$

and substitute (17) and (20) into (13), the uplink robustness requirement is transformed to:

$$\frac{\alpha^{up} g_n P^{max}}{2(J_0 + \alpha^{up} N P^{max})} \geq \Theta_n^{snr}, \quad n = 1, 2, \dots, N. \quad (22)$$

Suppose the power attenuations $\alpha_1^{down}, \alpha_2^{down}, \dots, \alpha_N^{down}, \alpha_1^{up}, \alpha_2^{up}, \dots, \alpha_N^{up}$ are given,

$$(12) \Leftrightarrow J_n \leq \left(\frac{\alpha_n^{down} g_n P^{max}}{(N+1)\Theta_n^{snr}} - \alpha_n^{down} P^{max} \right) \stackrel{def}{=} \bar{J}_n^{down}, \quad n = 1, 2, \dots, N. \quad (23)$$

$$(22) \Leftrightarrow J_0 \leq \left(\frac{\alpha^{up} g_n P^{max}}{2\Theta_n^{snr}} - \alpha^{up} N P^{max} \right) \stackrel{def}{=} \bar{J}_n^{up}, \quad n = 1, 2, \dots, N. \quad (24)$$

\bar{J}_n^{down} and \bar{J}_n^{up} therefore represents the maximum tolerable external RF interference for downlink and uplink of connection n respectively. That is, when J_n exceeds \bar{J}_n^{down} , connection n 's downlink will have a packet error rate over acceptable limit Θ_n^{per} ; when J_0 exceeds \bar{J}_n^{up} , connections n 's uplink will have a packet error rate over acceptable limit Θ_n^{per} . Define

$$J^{min} \stackrel{def}{=} \min\{\bar{J}_1^{down}, \bar{J}_2^{down}, \dots, \bar{J}_N^{down}, \bar{J}_1^{up}, \bar{J}_2^{up}, \dots, \bar{J}_N^{up}\}, \quad (25)$$

i.e. J^{min} represents the minimum external RF interference power needed to break down at least one of the connections. To maximize robustness therefore means to maximize J^{min} under the constraints of (9) and (7). It is easy to derive that J^{min} is maximized when $g_n = \min\{\lfloor r_c / (L_n^{pkt} f_n^{min}) \rfloor, g^{max}\}$.

Similarly, suppose $J_0, J_1, J_2, \dots, J_N$ are given, the tolerable power attenuations are maximized (i.e. $\alpha_1^{down}, \alpha_2^{down}, \dots, \alpha_N^{down}, \alpha_1^{up}, \alpha_2^{up}, \dots, \alpha_N^{up}$ are minimized) when $g_n = \min\{\lfloor r_c / (L_n^{pkt} f_n^{min}) \rfloor, g^{max}\}$.

Therefore, maximum robustness is achieved when each control loop deploys maximum processing gain possible, such that the packet rate is slowed down as much as possible. Formally, this is summarized by the following proposition:

Proposition 1 (Maximum Robustness Configuration)

To achieve maximum robustness, a DSSS-CDMA IC-WLAN should pick $g_n^* = \min\{\lfloor r_c / (L_n^{pkt} f_n^{min}) \rfloor, g^{max}\}$ ($n = 1, 2, \dots, N$).

In Section 4, we shall see that by deploying processing gain according to Proposition 1, a DSSS-CDMA IC-WLAN can achieve approximately 10 ~ 20dB and 25 ~ 35dB robustness improvement compared to IEEE 802.11b

and IEEE 802.11a respectively, which are significant improvements according to communication engineering criteria. The underlying reason is that IC-WLAN does not aim at achieving high data throughput; instead, control traffics are of extremely low data throughput, which can be exploited by DSSS to achieve much higher robustness.

3.3. Resource Planning for Minimized Utility Loss

The resource planning in Section 3.2 does not consider control performance. Simply speaking, given minimum allowed sampling/actuating rate f_n^{min} and maximum acceptable packet error rate Θ_n^{per} , Proposition 1 gives the configuration that will tolerate maximum external RF interference J^{worst} or worst case power attenuation α^{worst} . If the wireless channel condition is better than the worst case (represented by J^{worst} or α^{worst}), sticking to the configuration denoted by Proposition 1 is wasteful. Higher control performance can be achieved with less robust configuration.

Specifically, suppose the following conditions are given: α_n^{down} and α_n^{up} are the downlink/uplink power attenuation for connection n respectively. Denote $\alpha^{up} = \min\{\alpha_1^{up}, \alpha_2^{up}, \dots, \alpha_N^{up}\}$. J_n is the external RF interference received at the RS of connection n ($n = 1, 2, \dots, N$). J_0 is the external RF interference received at the BS. The hardware fixed chip rate is r_c . The maximum transmission power of each node is P^{max} . For a connection n ($n = 1, 2, \dots, N$), the sampling/actuating packet bit length is L_n^{pkt} ; its minimum allowed sampling/actuating rate is f_n^{min} ; and maximum acceptable packet error rate for both downlink/uplink is Θ_n^{per} . It can be reasonably assumed that the utility loss function for each connection n ($n = 1, 2, \dots, N$) is $U_n(f_n, \mathcal{P}_n^{per})$, i.e. a function of the connection's sampling/actuating rate f_n and packet error rate \mathcal{P}_n^{per} . It is also reasonable to assume the global utility loss function U to be $U = \sum_{n=1}^N U_n(f_n, \mathcal{P}_n^{per})$. Same as Section 3.2, we still assume the configurable variables are the process gain of each connection g_n .

Due to page limits, we directly give our results:

For clarity, the optimization problem is restated as follows:

$$\min U = \sum_{n=1}^N U_n(f_n(g_n), \mathcal{P}_n^{per}(g_n)) \quad (26)$$

$$\text{s.t.} \quad g_n \geq -\frac{1}{\zeta_n} \ln\left(1 - (1 - \Theta_n^{per})^{1/L_n^{pkt}}\right) \quad (27)$$

$$g_n \leq \frac{r_c}{f_n^{min} L_n^{pkt}} \quad (28)$$

$$1 \leq g_n \leq g^{max} \quad (29)$$

$$g_n \text{ is an integer, } n = 1, 2, \dots, N. \quad (30)$$

where $f_n(g_n)$ is defined in (8); ζ_n is defined as follows:

$$\zeta_n \stackrel{def}{=} \min \left\{ \frac{\alpha_n^{down} P^{max}}{(N+1)(J_n + \alpha_n^{down} P^{max})}, \frac{\alpha_n^{up} P^{max}}{2(J_0 + \alpha_n^{up} N P^{max})} \right\}, \quad (31)$$

and

$$\mathcal{P}_n^{per} = 1 - (1 - \exp(-\zeta_n g_n))^{L_n^{pkt}}. \quad (32)$$

Constraints (27) ~ (30) either result in an empty set, which means no feasible g_n exists; or are equivalent to the following form:

$$a_n \leq g_n \leq b_n, \quad g_n \text{ is an integer, and } n = 1, 2, \dots, N, \quad (33)$$

where a_n, b_n are positive integers.

Specifically, when U_n are of the following shapes, quasi-closed-form analytical optimal solution exists:

$$U_n(f_n, \mathcal{P}_n^{per}) = w_n (f_n(1 - \mathcal{P}_n^{per}))^{-\beta_n},$$

or $U_n(f_n, \mathcal{P}_n^{per}) = w_n \exp(-\beta_n f_n(1 - \mathcal{P}_n^{per}))$ (34)

where w_n and β_n are positive weight and sensitivity coefficients. $f_n(1 - \mathcal{P}_n^{per})$ is the expected number of sampling/actuating packets that are delivered correctly per second.

Lemma 1 For function $F(x) = \exp(\zeta_n x) - (1 + L_n^{pkt} \zeta_n x)$, where L_n^{pkt} and ζ_n have the same definitions as before and $L_n^{pkt} > 1$, equation $F(x) = 0$ has one and only one positive root $\tilde{x} > 0$.

Theorem 1 (Minimum Utility Loss Configuration)

Suppose feasible g_n for the constraint set (33) exists. And suppose \tilde{x}_n is the singleton positive root to equation $\exp(\zeta_n x) - (1 + L_n^{pkt} \zeta_n x) = 0$, $L_n^{pkt} > 1$ and U_n complies with either form defined in (34). Then the optimal g_n for the utility loss minimization problem is:

$$g_n^* = \begin{cases} a_n & \text{when } \tilde{x}_n < a_n, \\ \operatorname{argmin}_{g \in \{\lfloor \tilde{x}_n \rfloor, \lceil \tilde{x}_n \rceil\}} \left\{ U_n(f_n(g), \mathcal{P}_n^{per}(g)) \right\} & \text{when } a_n \leq \tilde{x}_n \leq b_n, \\ b_n & \text{when } \tilde{x}_n > b_n \end{cases}$$

where a_n and b_n are defined in (33).

4. Simulation and Comparisons

In this section, we are going to demonstrate the effectiveness of our DSSS-CDMA IC-WLAN design, and compare it with IEEE 802.11 WLANs, which are the current pre-dominant WLAN schemes.

IEEE 802.11 WLANs can be further categorized into IEEE 802.11b[4], a[3] and g[7]. IEEE 802.11b/a/g share the same MAC layer specification (with minor variations), while differ in their physical layers. IEEE 802.11b operates at the 2.4GHz RF band and deploys DSSS in physical layer³. IEEE 802.11a operates at the 5GHz RF band and deploys *Orthogonal Frequency Division Multiplexing* (OFDM) [14][19][21] in physical layer. IEEE 802.11g is basically the combination of 802.11b and 802.11a. Usually, IEEE 802.11 operates under *Distributed Coordination Function* (DCF) mode, which carries out CSMA/CA and MACAW [15] MAC protocol. DCF is therefore contention/random-backoff based and is not designed for real-time systems. However, IEEE 802.11 also specifies the *Point Coordination Function* (PCF) mode, where the basestation polls each remote station. PCF is contention-free and is the scheme designed for real-time systems. Therefore, we compare the performance of our proposed DSSS-CDMA IC-WLAN with IEEE 802.11b/a PCF IC-WLAN.

4.1. Fine-grained Physical Layer Simulation

First we carry out fine-grained physical layer simulation to demonstrate the effectiveness of the DSSS-CDMA IC-WLAN scheme. We build our simulation environment on top of J-Sim kernel [9]. The scenario is depicted in Fig. 2(a). The IC-WLAN includes two connections: connection 1 and 2, each controls an *Inverted Pendulum* (IP) [32], denoted as IP 1 and 2 in Fig. 2(a). Each IP is a remote station of the IC-WLAN, which periodically sends back IP state to the basestation. Based on the most up-to-date IP state, the basestation calculates the next control and sends it back to the IP.

Without loss of generality, we assume the two IPs are the same, as shown in Fig. 2(b), where x is the position of IP cart, θ is the angular deviation of IP from vertical position, and u is the velocity control voltage applied to IP cart. The state transition matrix and control matrix are also depicted in the figure⁴. The IP cart moves along the x axis to keep the IP standing vertically. The requirement is that the IP must not fall, otherwise a high cost resetting procedure is incurred. Specifically, we must maintain $|\theta| < \frac{\pi}{6}$. The sampling/actuating packet length are both 152 bits. Empirically, we know the IP's minimum sampling/actuating rate is $f_1^{min} = f_2^{min} = 10\text{Hz}$.

We carry out simulation under both DSSS-CDMA scheme and IEEE 802.11b scheme. To make a fair comparison, both schemes occupy the same RF band of 2.425 ~ 2.449GHz, which is a typical RF band deployed by IEEE

³IEEE 802.11b also deploys CCK for higher data throughput modes, which are less robust.

⁴An additional heuristic is added for the control: when θ and u are of opposite signs, u is obviously an out-of-date control (because of delay) and therefore ignored.

802.11b. For DSSS-CDMA, the RF band is divided into two halves: 2.425 ~ 2.437GHz for downlink and 2.437 ~ 2.449GHz for uplink. For IEEE 802.11b, the signal occupies the whole RF band, but packets are time divided into downlink packets and uplink packets. Therefore, the chip rate for DSSS-CDMA and IEEE 802.11b are $r_c^{cdma} = 5.5\text{Mcps}$ and $r_c^{ieee80211b} = 11\text{Mcps}$ respectively. For DSSS-CDMA scheme, we pick the hardware-implementation-dependent processing gain upper bound to be $g^{max} = 1024$.⁵ According to Proposition 1, the processing gain that maximize robustness is therefore $g^{cdma} = \min\{\lfloor \frac{5.5 \times 10^6}{152 \times 8} \rfloor, 1024\} = 1024$. Furthermore, without loss of generality, QPSK and per-node pilot tone are deployed for RF modulation/demodulation; the received power of all data channels are the same, and the pilot tone is of same power level as a data channel transmitted from the same node. At the uplink, power balance is carried out to deal with the near-far problem. For IEEE 802.11b scheme, the most robust mode of 1Mbps throughput is deployed, which corresponds to a processing gain of $g^{ieee80211b} = 11$ and *Differential BPSK* (DBPSK) RF modulation/demodulation. Again, to be fair, the IEEE 802.11b WLAN works in pure PCF, which is the real-time mode for IEEE 802.11 WLAN. Under such mode, the basestation basically polls IP 1 and IP 2 in a round robin pattern. The control packet is sent to the IP as the poll packet, and the sample packet is sent back from IP as the acknowledgement packet.

To demonstrate the robustness, an external RF interference source is placed near IP 1 (see Fig. 2(a)), whose power spectrum occupies the same RF band that DSSS-CDMA and IEEE 802.11b are using. To be fair, under both DSSS-CDMA and IEEE 802.11b schemes, the maximum transmission power of all nodes (include basestation, remote stations and the external RF interference source) are 30dBm (dBm is the widely used unit for signal power. A signal power of P watt is said to be of $10 \log_{10}(P/0.001)$ dBm), which is the maximum transmission power allowed by FCC for IEEE 802.11b. The only exception is for DSSS-CDMA uplinks, where the transmission power must also comply with the power balancing requirement to produce the same power level at the basestation. The power balancing requirement makes the situation more pessimistic on the DSSS-CDMA side.

The simulation starts at time 0sec and ends at time 30sec. The external RF interference source is turned on at time 5sec and turned off at time 15sec. The wireless medium instance is generated according to the random model described in Table 1. The model is typical for indoor industrial environments [31][34]. To deal with multipath fading, two-finger RAKE receivers [29][35] are deployed for both

⁵This value is picked simply because cdmaOne [1] (the most prevalent DSSS-CDMA cellphone network standard in North America) compliant hardware all supports a processing gain of at least 1024.

Table 1. Wireless Medium Model

Large-scale path loss model	Log-normal shadowing model with $\beta = 4 \sim 6, \sigma = 6.8\text{dB}$ *
Small-scale fading model	Rayleigh
Multipath max excess delay	90.909nsec
Additive White Gaussian Noise [†]	Spectral density = -174dBm/Hz

* β is the path loss exponent, σ is the log-normal standard deviation.
[†] Typically refers to thermal noise.

DSSS-CDMA and IEEE 802.11b nodes.

Fig. 3 shows the trace of θ . It can be seen that throughout the time, under DSSS-CDMA scheme, both IP 1 and IP 2 remain fairly stable, even during external RF interference (5 ~ 15sec) period. This shows the wireless control loops are maintained under adverse channel conditions. However, under IEEE 802.11b, IP 1 always fall due to external RF interference (every time it falls, the IP is set to 0.5rad and stay there for 0.2sec to restart). Note IP 2 under IEEE 802.11b can also survive external RF interference because it is much closer to basestation than to the external RF interference source⁶.

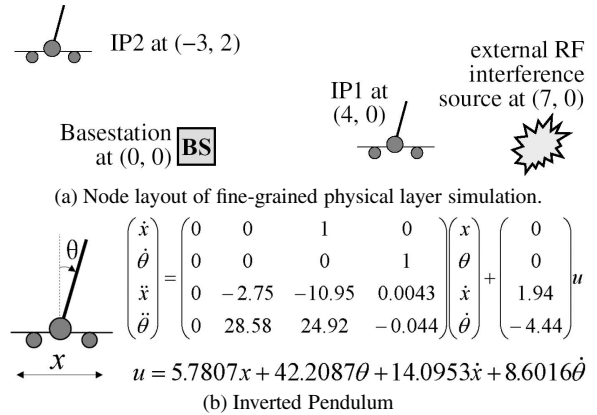


Figure 2. Simulated Scenario

4.2. Robustness Comparisons

Next, we are interested in carrying out more rigid comparisons on robustness, between the proposed DSSS-CDMA scheme and IEEE 802.11 schemes.

Generally speaking, the main objective of IEEE 802.11 WLANs is to provide high data throughput. This is a mismatch for most distributed industrial control loops, for which, the data throughput demand may be extremely low

⁶To make the simulation more optimistic on the IEEE 802.11 side, instead of backing off (which will certainly cause deadline miss on the real-time wireless control loop), the PCF scheme keeps polling the remote station even if it detects noise on the wireless medium.

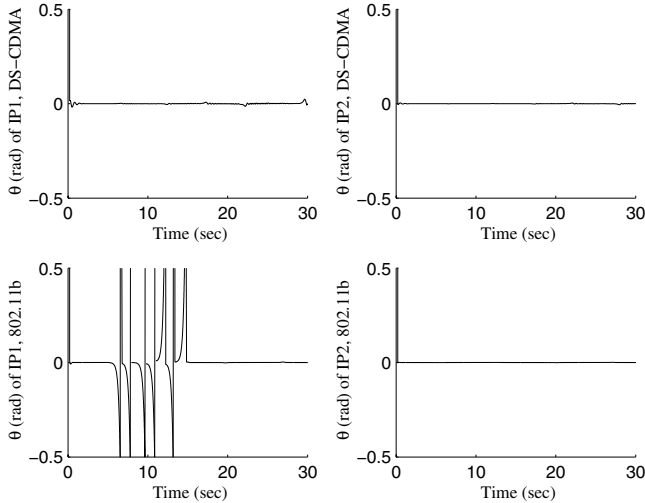


Figure 3. Simulation Results (θ trace)

(typical packet lengths are around 100 ~ 200 bits, and minimum acceptable sampling/actuating rate can be lower than 10Hz, or even around 1Hz), whereas the robustness demand is high. Industrial control requires the periodical sampling/actuating messages be delivered even when there is persistent external RF interference, and making the communication link as robust as possible is often of top concern. We shall show that by fully exploiting the low data throughput feature, the DSSS-CDMA IC-WLAN scheme can achieve much higher level of robustness.

We carry out Monte Carlo simulation to compare the robustness between DSSS-CDMA and IEEE 802.11b/a schemes. Specifically, in each trial, a layout of the basestation and n remote stations is generated, together with the wireless medium instance. The quantitative robustness indicator is J^{min} (i.e. the minimum external RF interference power needed to break down at least one of the wireless control loops, see the definition in (25)), which is calculated and compared between the DSSS-CDMA and IEEE 802.11b/a IC-WLAN schemes.

The industrial indoor environment is supposed to be a square area of 20m \times 20m, with the basestation located at the center. n remote stations are uniformly distributed across the room, each corresponds to a wireless control loop. The value of n varies from 1 to 100. Without loss of generality, all sampling/actuating packets are of 152 bits (same as the inverted pendulum case, a typical control packet size), and all control loops have the same minimum acceptable sampling/actuating rate f^{min} . Specifically, Two values of f^{min} are tested: 1Hz and 10Hz, which are typical for distributed industrial control loops. Every application layer sampling/actuating packet must be delivered with success probability of no less than 0.999. For a given n , f^{min} and

Table 2. Physical Layer Settings for Comparisons

	Max trans power*	RF band [†]
DSSS-CDMA vs. IEEE 802.11b comparison	1watt	2.425 ~ 2.449GHz
DSSS-CDMA vs. IEEE 802.11a comparison	800mw	5.735 ~ 5.795GHz

* According to FCC regulation.

[†] According to IEEE 802.11 specification. Note RF bandwidth also decides baseband bandwidth (i.e. chip rate for DSSS and bit rate for OFDM).

IC-WLAN scheme, 200 trials are simulated. In each trial, an instance of remote station layout and an instance of the wireless medium are generated. The wireless medium instance follows the random model depicted in Table 1.

To make fair comparisons, physical layer settings of wireless devices are summarized in Table 2. Without loss of generality, the DSSS-CDMA scheme deploys QPSK with per-node pilot tone for RF modulation/demodulation, received power of all data channels are the same, the pilot tone is of same power level as a data channel transmitted from the same node. For IEEE 802.11b, the most robust 1Mbps DBPSK mode is assumed; and for IEEE 802.11a, the most robust 6Mbps mode is assumed, which deploys BPSK and 1/2 convolutional coding for forward error correction. For DSSS-CDMA scheme, we assume the hardware-implementation-dependent upper bound on processing gain g^{max} is sufficiently large⁷, so that the processing gain g_n for control loop n is picked to be $g_n = \lceil r_c / (f_n^{min} L_n^{pkt}) \rceil$ according to Proposition 1. According to the given packet bit length (152bit) and RF bandwidth listed in Table 2, when $f^{min} = 10\text{Hz}$ and 1Hz, the corresponding processing gain are 3618 and 36184 for DSSS-CDMA/IEEE 802.11b comparison, and 9868, 98684 for DSSS-CDMA/IEEE 802.11a comparison⁸. For IEEE 802.11b/a schemes, the packet is retransmitted as many times as possible throughout the sampling/actuating period so as to increase the chance of successful delivery.

The upper bound of DSSS-CDMA BER under specified SNR is given in (1). For IEEE 802.11b 1Mbps mode, inequality (35) gives the lower bound of BER under specified SNR [20].

$$\mathcal{P}_{ber}^{80211b} \geq \frac{1}{2} \operatorname{erfc} \sqrt{\frac{gP_u}{J}} \quad (35)$$

where g is the processing gain, P_u is the received signal power, J is the received total external RF interference

⁷This is a practical assumption: with very little hardware cost increase, the PN sequence length can be increased exponentially, so that the upper bound on processing gain is increased exponentially with it [18].

⁸Note RF bandwidth is decided by chip rate r_c , which is fixed. Any processing gain g can be picked, but a bigger g corresponds to a slower bit rate $r_b = r_c/g$.

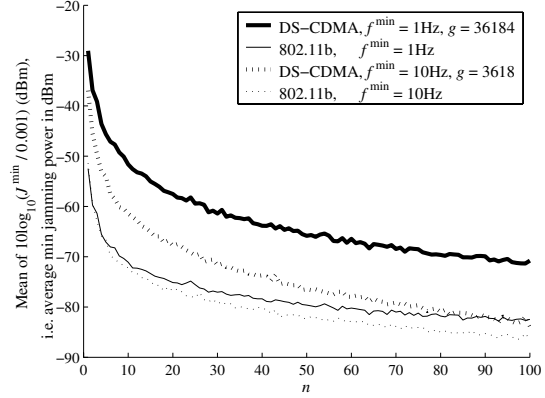
power, and erfc is the well-known *complementary error function* [20]. The IEEE 802.11a 6Mbps mode deploys BPSK and 1/2 convolutional code for forward error correction, which makes it hard to give a closed-form BER-SNR formula⁹. However, its PER-SNR relationship can be empirically derived through Monte Carlo simulation. Based on these BER(PER)-SNR relationships, J^{\min} of DSSS-CDMA and IEEE 802.11b/a schemes for the same wireless medium, node layout and application can be calculated, which are shown in Fig. 4(a) and (b). This comparison is pessimistic on the DSSS-CDMA side because of many reasons: First the *upper bound* of BER is used for DSSS-CDMA scheme, while for IEEE 802.11b/a the *lower bound* of BER and empirical *exact* PER are used respectively. Second, in (1), the intended signal power P_u is included as part of interference to provide a (overly) pessimistic estimation on ISI; while for IEEE 802.11b/a, ISI is assumed to be 0. Therefore, the actual tolerable external RF interference power for DSSS-CDMA should be no less than what is plotted in Fig. 4(a) and (b), and the actual tolerable external RF interference power for IEEE 802.11b/a should be no greater than what is plotted in Fig. 4(a) and (b).

From Fig. 4, it is obvious that DSSS-CDMA can tolerate much higher external RF interference power than corresponding IEEE 802.11 schemes. When $f^{\min} = 10\text{Hz}$ and 1Hz , DSSS-CDMA achieves approximately 10dB and 20dB improvement on robustness than IEEE 802.11b. Compared to IEEE 802.11a, the improvement on robustness is approximately 25dB and 35dB respectively. This is because our DSSS-CDMA scheme fully exploits the low data rate feature of industrial control loops by setting processing gain according to Proposition 1. We see when the data rate demand of control loop is smaller (i.e. with smaller f^{\min}), larger processing gain can be deployed, and the corresponding tolerable external RF interference power is increased. It is worth noting that for each fixed application setting, the tolerable external RF interference power goes down when the number of control loops (n) increases. This is intuitively correct. Because the Shannon bound of information theory [17] basically says when the application layer data throughput increases, and the signal power is fixed (for downlink, there is always only one basestation), the tolerable noise power decreases.

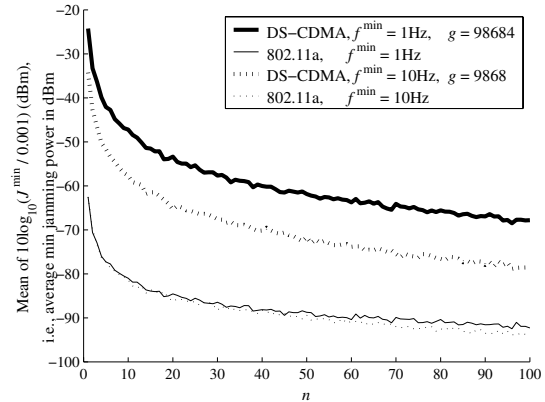
5. Related Work and Discussion

One of the major purposes of this paper is to show DSSS-CDMA cellphone network paradigm is more appropriate for IC-WLAN compared to the dominant IEEE 802.11 schemes for WLAN. Intuitively, the communication patterns of industrial control loop and cellphone voice session share

⁹An upper bound exists [30], but it should not be used for a fair comparison or a comparison that is pessimistic on the DSSS-CDMA side.



(a) Comparison with IEEE 802.11b



(b) Comparison with IEEE 802.11a

Figure 4. Robustness comparison. J^{\min} (watt) is the minimum external RF interference power needed to break-down at least one of the wireless control loops. n is the number of wireless control loops. Note the curves for DSSS-CDMA are lower bounds for J^{\min} , while the curves for IEEE 802.11b/a are upper bounds.

many similarities. They are both of low data rate, stable regular traffic, and last for long duration in a session-like pattern. The main difference is the high robustness concern for industrial control loops, which calls for better exploitation of the low data rate feature to achieve as much robustness as possible. The current CDMA cellphone network architectures have not yet focused on such demand. For example, the recent 3-G standards [5][12] are more focused on providing higher data throughputs (which means smaller processing gain) to compete with IEEE 802.11 on home/office applications domain. Nevertheless, it would be easy to build our proposed DSSS-CDMA IC-WLAN on top of the many existing CDMA cellphone network architectures, e.g. cdmaOne [1], cdma2000 [5], W-CDMA

[12], TD-SCDMA [11] etc. The technologies needed by our scheme are already mature, specifically, the capability of providing multiple reconfigurable CDMA channels, processing gain options and power levels are already standard practices supported by most contemporary CDMA cellphone chip sets, such as Qualcomm CSM6800, CSM6700, CSM5500 [10][24] etc. The major modification pending is to better customize the configurable options and the resource management strategies according to the industrial control needs.

We have shown that DSSS-CDMA IC-WLAN can achieve much higher robustness than IEEE 802.11 WLANs [2][3][4][7], whose robustness levels are fixed, and not designed for adverse channel conditions. However, if application-dependent processing gain configuration is provided for IEEE 802.11b, its robustness can also be greatly improved. This is exactly the DSSS-TDMA IC-WLAN approach, which we have already discussed in Section 2, and come to the conclusion that it is less preferable than DSSS-CDMA. However, DSSS-TDMA IC-WLAN is still a feasible approach, which merits further study.

Recently, *Wireless Personal Area Network* (WPAN) also emerges as a scheme for smaller networks than WLAN. The main MAC/physical layer standards are IEEE 802.15.1 [6] (Bluetooth) and IEEE 802.15.4 [8]. Generically speaking, their MAC schemes are both TDMA based. They are aiming at low power short range communications. The main focus is to achieve higher power saving than IEEE 802.11, instead of significantly higher robustness.

Also, at the physical layer, *Frequency Hopping Spread Spectrum* (FHSS) [31] and DSSS share similar analytical characteristics. Under many circumstances, FHSS and DSSS are interchangeable. However, FHSS is less advantageous than DSSS for its hardware cost and system complexity. And digital wireless FHSS-CDMA (Bluetooth is fundamentally a FHSS-TDMA scheme) systems are not as widely available as DSSS-CDMA systems.

In the end, it is worth noting that we cannot achieve infinite robustness. The goal is to maintain wireless control loop communications under as harsh channel conditions as possible, instead of becoming totally immune to adverse channel conditions.

6. Conclusion

The top concern for building *Industrial Control Wireless LAN* (IC-WLAN) is robustness. Wireless channel conditions can vary significantly. Power attenuation may change drastically because of large-scale path loss and fading. Contending RF devices may be turned on accidentally or maliciously. For industrial environments, the situation is even worse because of various EMI sources such as electric motor and welding, and serious large-scale path loss and fading

because of heavy obstructions. Wireless control loops must be maintained under all these adverse channel conditions, instead of backing off. This makes the IEEE 802.11 WLANs, which is mainly designed for office/home bursty data traffics, inappropriate for IC-WLAN. On the other hand, industrial control loop traffics are mostly regular sustained traffics with extremely low data rates. DSSS technology can therefore achieve high robustness by deploying high processing gain.

According to fine-grained physical layer simulations and Monte Carlo comparisons, we show that by fully exploiting the low data rate feature of industrial control loops, a DSSS IC-WLAN can provide significantly higher robustness than IEEE 802.11 WLAN. At the MAC layer, either CDMA or TDMA can be deployed, however, CDMA is more preferable for its ease of scheduling, overrun isolation, and low overhead for regular sustained traffics. Therefore, we claim that by fully exploiting low data rate feature of industrial control loops, DSSS-CDMA is a more appropriate scheme for IC-WLAN. That is, we basically point out a new application domain where the CDMA cellphone network paradigm would prevail again due to its unique characteristics. Though some modifications are needed, it promising to build our proposed DSSS-CDMA IC-WLAN scheme on top of the many contemporary CDMA cellphone network architectures.

On the other hand, we also foresee a large number of real-time QoS and resource management problems to be addressed for the DSSS-CDMA IC-WLAN scheme. We study the optimal resource configuration to achieve maximum robustness and minimum utility loss, and give analytical closed-form solutions. The resource management problem can be more complicated when more maneuverable variables are introduced, such as power allocation, channels per connection and control loops to be included in the IC-WLAN (see [36] Appendix IV for a discussion on resource optimization when per connection power allocation is uneven). Generally speaking, DSSS technology provides the mechanism to combine the many variables, such as data rate, real-time schedule, utility, power, number of control loops and robustness as a whole. Many problems are to be explored, such as efficient planning/optimization algorithms, capacity bound, utility bound, robustness bound, co-existence of regular low throughput data traffic and bursty high throughput data traffic etc. Also, the situation will be more complicated for multiple cells. We are interested in carrying out further studies in all these directions.

7. Acknowledgement

The first author is supported by Vodafone Fellowship. This research is also supported by (in alphabetical order) MURI N00014-01-0576, NSF ANI 02-21357, NSF CCR-

0237884, NSF CCR-0325716, NSF CCR 02-09202, and ONR N00014-02-1-0102. We especially thank Prof. Lui Sha for his insightful feedback that helped to achieve the results of this work. We also thank Prof. Venugopal Veeravalli, Prof. Bruce Hajek, Prof. Christoforos Hadjicostis, Prof. Rong Zheng, Tanya Crenshaw and anonymous reviewers for their comments. We thank Ning Li for providing assistance on using J-Sim, and Qingbo Zhu for providing assistance on carrying out simulations on high-performance computer clusters.

References

- [1] TIA/EIA/IS Std. 95. 1992.
- [2] IEEE Std. 802.11. 1997.
- [3] IEEE Std. 802.11a. 1999.
- [4] IEEE Std. 802.11b. 1999.
- [5] TIA/EIA/IS CDMA 2000 Series, Release A (2000). 2000.
- [6] IEEE Std. 802.15.1. 2002.
- [7] IEEE Std. 802.11g. 2003.
- [8] IEEE Std. 802.15.4. 2003.
- [9] Drcl j-sim. <http://www.j-sim.org>, 2005.
- [10] Qualcomm cdma technologies. <http://www.cdmatech.com>, 2005.
- [11] Td-scdma forum. <http://www.tdscdma-forum.org>, 2005.
- [12] Umts forum. <http://www.umts-forum.org>, 2005.
- [13] G. Antonini, S. Cristina, et al. A prediction model for electromagnetic interferences radiated by an industrial power drive system. *IEEE Transactions on Industry Applications*, 35(4), 1999.
- [14] A. R. S. Bahai and B. R. Saltzberg. *Multi-Carrier Digital Communications: Theory and Applications of OFDM*. Kluwer Academic/Plenum Publishers, 1999.
- [15] V. Bharghavan, A. Demers, S. Shenker, and L. Zhang. MACAW: A media access protocol for wireless LAN's. *Proceedings of the Conference on Communications Architectures, Protocols and Applications (ACM SIGCOMM 1994)*, pages 212–225, 1994.
- [16] S. Cavalieri and D. Panno. A novel solution to interconnect fieldbus systems using IEEE wireless LAN technology. *Comput. Standards Interfaces*, 20(1):9–23, 1998.
- [17] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley-Interscience, 1991.
- [18] R. C. Dixon. *Spread Spectrum Systems with Commercial Applications*. Wiley-Interscience, April 1994.
- [19] L. Hanzo, W. Webb, and T. Keller. *Single- and multi-carrier quadrature amplitude modulation: principles and applications for personal communications, WLANs and broadcasting*. John Wiley & Sons, Ltd., 2000.
- [20] S. Haykin. *Communications Systems*. Wiley, third edition, 1994.
- [21] J. Heiskala and J. Terry. *OFDM Wireless LANs: A Theoretical and Practical Guide*. Sams Publishing, 2002.
- [22] S. Jiang. Wireless communications and a priority access protocol for multiple mobile terminals in factory automation. *IEEE Trans. Robot. Automat.*, 14:137–143, 1998.
- [23] R. B. Kiebert. The step motor - the next advance in control systems. *IEEE Transactions on Automatic Control*, 9(1), 1964.
- [24] L. Korowajczuk, B. de Souza Abreu Xavier, A. M. F. Filho, et al. *Designing cdma2000 Systems*. Wiley, 2004.
- [25] B. Kuo. *Theory and Applications of Step Motors*. West Publishing Company, 1974.
- [26] A. Muqattash and M. Krunz. Cdma-based mac protocol for wireless ad hoc networks. *Proceedings of the 4th ACM Intl' Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2003)*, pages 153–164, 2003.
- [27] E. A. Parr. *Industrial Control Handbook*. Industrial Press, third edition, 1999.
- [28] N. J. Ploplys, P. A. Kawka, and A. G. Alleyne. Closed-loop control over wireless networks. *IEEE Control Systems Magazine*, 24(3):58–71, June 2004.
- [29] R. Price and P. E. G. Jr. A communication technique for multipath channels. *Proceedings of the IRE*, 46:555–570, 1958.
- [30] J. G. Proakis and M. Salehi. *Communication Systems Engineering*. Prentice Hall, second edition, 2002.
- [31] T. S. Rappaport. *Wireless Communications: Principles and Practice*. Prentice Hall, second edition, 2002.
- [32] L. Sha, X. Liu, M. Caccamo, and G. Buttazzo. Online control optimization using load driven scheduling. *Proc. of 39th IEEE Conference on Decision and Control*, 5:4877–4882, Dec. 2000.
- [33] M. K. Simon, J. K. Omura, et al. *Spread Spectrum Communications Handbook, Electronic Edition*. McGraw-Hill, 2002.
- [34] D. Tse and P. Viswanath. *Fundamentals of Wireless Communication*. (to be published by) Cambridge University Press, draft edition, 2004.
- [35] A. J. Viterbi. *CDMA: Principles of Spread Spectrum Communication*. Prentice Hall, April 1995.
- [36] Q. Wang, X. Liu, W. Chen, W. He, and M. Caccamo. Technical report on building robust wireless lan for industrial control with dsss-cdma cellphone network paradigm. http://www-rtsl.cs.uiuc.edu/papers/dsss-cdma_tr.pdf, 2005.
- [37] H. Ye and G. Walsh. Real-time mixed-traffic wireless networks. *IEEE Trans. Ind. Electron.*, 48(5), 2001.
- [38] H. Ye, G. Walsh, and L. Bushnell. Wireless local area networks in the manufacturing industry. *Proc. American Control Conf.*, pages 2363–2367, 2000.
- [39] F. Zhang. *Investigation of Electromagnetic Interference of PWM Motor Drives in Automotive Electrical Systems*. Number TR-99-004. MIT Laboratory for Electromagnetic and Electronic Systems, 1999.