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

Qixin Wang*, *Student Member, IEEE*, Xue Liu†, *Member, IEEE*, Weiqun Chen‡, *Student Member, IEEE*, Lui Sha*, *Fellow, IEEE*, and Marco Caccamo*, *Member, IEEE*

***Abstract*— *Wireless LAN for Industrial Control* (IC-WLAN) provides 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,fading, and many electro-magnetic interference sources in industrial environments. The conventional IEEE 802.11 WLANs, originally designed for high bandwidth instead of high robustness, are therefore inappropriate for IC-WLAN. A solution lies in the *Direct Sequence Spread Spectrum* (DSSS) technology: by deploying the largest possible processing gain (slowest bit rate) that fully exploits the low data rate feature of industrial control, much higher robustness can be achieved. We hereby propose using DSSS-CDMA to build IC-WLAN. We carry out fine-grained physical layer simulations and Monte Carlo comparisons. The results show that DSSS-CDMA IC-WLAN provides much higher robustness than IEEE 802.11/802.15.4 WLAN, so that reliable wireless industrial control loops become feasible. We also show that deploying larger processing gain is more preferable than deploying more intensive convolutional coding. The DSSS-CDMA IC-WLAN scheme also opens up a new problem space for interdisciplinary study, involving real-time scheduling, resource management, communication, networking and control.**

***Index Terms*— Real-time and embedded systems, Reliability and robustness, Wireless communication, Industrial control**

I. Introduction

Recently, there are increasing efforts in deploying *Wireless LANs* (WLAN) for industrial control [1][2][3][4][5]. *Industrial Control WLAN* (IC-WLAN) has many desirable features, such as extended mechanical freedom and mobility, low deployment cost and ease of reconfiguration.

Nonetheless, a major concern of IC-WLAN is its robustness: wireless communication must be maintained under adverse channel conditions. Wireless channel conditions are inherently more vulnerable than those of wireline communications for the existence of such problems as multiple-access contention, *Radio Frequency* (RF) interference, large-scale path loss, and fading (a.k.a. multipath) [6]. Industrial environments make these problems deteriorate because of heavy obstructions [6] and possible *Electro-Magnetic Interferences* (EMIs) [7][8]. An example is that EMI from electric welding or electric motor can last for hours, or even days. Nevertheless, IC-WLANs require much higher robustness than conventional WLANs for office or home use. Most office or home wireless communications allow a few seconds or even minutes of adverse channel conditions. They just need to backoff till the channel condition recovers, and then retransmit. Industrial control, however, often forbids such backoff behavior. Because most industrial control loops are real-time, the backoff behavior will cause deadline misses, which further trigger performance losses, halts/resets of manufacturing pipelines, or defects in products. For example, 200msec of backoff may incite an inverted pendulum [9] fall. Therefore, for most industrial controls, communications must be maintained even under adverse channel conditions instead of backing off.

RF interference, large-scale path loss and fading cause adverse channel conditions by reducing *Signal-to-Noise Ratio* (SNR) of the wireless communications. When the SNR is lower than a certain threshold, the *Bit Error Rate* (BER) of the wireless communication rises over the acceptable limit, thus disrupting the wireless connection. Therefore, the key to maintaining wireless communication under adverse channel conditions is to provide as high SNR as possible. To achieve this, a promising solution lies in the state-of-the-art *Direct Sequence Spread Spectrum* (DSSS) technology, which allows tradeoffs between data throughput versus SNR. Specifically, a lower data throughput corresponds to a higher SNR and vice versa. Fortunately, industrial control loop traffics in IC-WLANs are often low-data-throughput stable traffics [10]. For example, most industrial mechanical systems carry out fine-grained high-rate controls locally using step motors [11][12][13], so that only low-data-throughput coarse-grained control traffics are transmitted between distributed nodes. Typically, the sampling/actuating rates between distributed nodes are around $1 \sim 10$Hz, and the packet sizes are around $100 \sim 200$ bits.

Based on above observations, we propose using DSSS technology to fully exploit the low-data-throughput feature of control loop traffics, to build robust IC-WLANs. Through fine-grained physical layer simulations and Monte Carlo comparisons, we show that when the low-data-throughput feature is fully exploited, DSSS IC-WLANs achieve much higher robustness than IEEE 802.11/802.15.4 WLANs (for consistency, we refer to IEEE 802.15.4 as a WLAN scheme in this paper) [14][15][16] do, so that wireless industrial control becomes practical (see Section IV). Specifically, a DSSS IC-

∗ Authors are with Department of Computer Science, University of Illinois at Urbana-Champaign. E-mail: {qwang4, lrs, mcaccamo}@uiuc.edu

† Xue Liu is with School of Computer Science, McGill University. E-mail: xueliu@cs.mcgill.ca

‡ Weiqun Chen is with ECECS Department, University of Cincinnati. E-mail: chenwq@ececs.uc.edu

WLAN achieves $10 \sim 20$dB and $20 \sim 30$dB improvements on robustness compared to an IEEE 802.11b and an IEEE 802.11a WLAN respectively; similar improvements are also achieved against IEEE 802.15.4 WLANs. These are significant improvements according to communication engineering criteria.

DSSS is a physical layer scheme, which only concerns point-to-point communications. At the *Multiple Access Control* (MAC) layer, we need a proper IC-WLAN paradigm, which can either be the fully distributed ad hoc paradigm of IEEE 802.11/802.15.4 WLANs, or the centralized *Code Division Multiple Access* (CDMA) paradigm of cellphone networks. We prefer the CDMA cellphone network paradigm. Under such paradigm, every IC-WLAN is a cell, with one *base station* and several *remote stations*; wireless communications only take place between a base station and a remote station of the same cell; inter-cell communications only exist between base stations via wireline backbones. The reasons why CDMA cellphone network paradigm is preferred run as follows: i) Industrial control loop traffics are usually real-time. The base-station-centered CDMA cellphone network paradigm makes it easy to implement centralized real-time scheduling. In practice, centralized real-time scheduling is often more desirable due to its robustness and simplicity. ii) Most industrial control loops incur low computation, therefore it is a common and economic practice to have one powerful centralized base station controlling all machines in a local area [10]. Many legacy systems are already built upon such base-station-centered communication paradigm. iii) Industrial control applications are typically deployed in well-built permanent facilities, where powerful wireline backbones for inter-base-station communications are available. Therefore, the benefits of wireless communications (mechanical freedom, mobility, flexibility) are only significant at the last hop. A CDMA cellphone network paradigm matches such need. iv) CDMA is also a more preferable technology due to its ease of scheduling, overrun isolation and low overhead.

To sum up, this paper mainly demonstrates that by fully exploiting the low-data-throughput feature of industrial control loops, the DSSS-CDMA cellphone network paradigm presents a better approach to build robust IC-WLANs than the nowadays predominant IEEE 802.11/802.15.4 paradigms. This paper also studies some resource management issues on the proposed DSSS-CDMA IC-WLAN. As an example, we derive optimal resource configuration for maximal robustness. The resource management issues open a new problem space for interdisciplinary study, which involves real-time scheduling, communication, networking and control.

The rest of the paper is organized as follows: Section II gives background on DSSS technology. Section III proposes the DSSS-CDMA IC-WLAN scheme, together with some analytical results on its resource optimization. Section IV carries out fine-grained physical layer simulations to demonstrate DSSS-CDMA IC-WLAN robustness, and more extensive Monte Carlo simulations to compare the robustness with IEEE 802.11/802.15.4 WLANs'. Section IV also includes a discussion on the feasibility of error correction coding besides DSSS. Section V discusses related works. Section VI concludes the paper.

II. Background

DSSS is a physical layer modulation/demodulation scheme for digital communication [17][18][19]. It modulates/demodulates the original data signal to/from a baseband signal which occupies a wider spectrum[1]. At the transmitter, a user data bit stream of bit rate r_b (every bit takes $T_b \stackrel{def}{=} 1/r_b$(sec)) is *scrambled* with a *Pseudo Noise* (PN) sequence of *chip rate* r_c (every chip takes $T_c \stackrel{def}{=} 1/r_c$(sec)), 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 recovers. If a different PN sequence is applied or the scramble/descramble PN sequences are not synchronized, the original data bit stream does not recover and a noise-like random chip stream is generated instead. To summarize, each PN sequence creates a DSSS data channel. Note although DSSS requires synchronization between each transmitter and its receiver, different transmitter-receiver pairs need not be synchronized. Appendix I of [21] gives a more detailed tutorial on DSSS.

DSSS is a physical layer scheme. At the MAC layer, there are two alternatives: *Code Division Multiple Access* (CDMA), or *Time Division Multiple Access* (TDMA). For simplicity, we also categorize the widely used *Carrier Sensing Multiple Access* (CSMA) as a kind of 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 each receiver, by applying different PN sequences, the intended data bit stream is filtered out. If DSSS-TDMA is deployed, different data bit streams are scrambled and transmitted in non-overlapping time slots. Though both alternatives work, DSSS-CDMA fits IC-WLANs better because: i) ease of real-time scheduling; ii) inherent isolation between connections; iii) less communication overhead, especially under adverse channel conditions. i) and ii) are straightforward and interrelated: Under DSSS-CDMA, a real-time connection exclusively occupies a CDMA channel by using a unique DSSS PN sequence. Different CDMA channels can coexist in parallel. Therefore it is not necessary to schedule different real-time connections, and the overrun of one real-time connection does not affect any other real-time connections. In contrast, under DSSS-TDMA, the DSSS PN sequence is shared among all real-time connections, and different time slots must be scheduled to serve different connections. If a real-time connection overruns its time slot, subsequent real-time connections are affected. In terms of iii), a simplified explanation is as follows: DSSS requires time synchronization between the transmitter and the receiver. Under CDMA, packets of a same connection are sent continuously as one bit

[1] We refer to DSSS as a *baseband* modulation/demodulation scheme. In contrast, 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 the same robustness (in sense of BER) with the same SNR per bit [17][20].

stream (i.e., *session*). Synchronization time cost only happens during session setup. During the session, synchronization is maintained in parallel of data transmission. Under TDMA, however, every packet incurs synchronization time cost. Under adverse channel conditions, this cost may be big, causing much more overhead in TDMA than CDMA. Appendix II of [21] further elaborates this.

Quantitatively, many important features of DSSS are captured by its *Bit Error Rate* (BER) upper bound shown in inequality (1)[2] [17][22]:

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

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 turned on accidentally or maliciously; P_i ($i = 1 \ldots \Xi$) is the received power of CDMA channel i; Ξ is the total number of CDMA channels coexisting in parallel; u is the intended channel, with a received power of P_u. Each transmitting node may send out several CDMA channels in parallel, each carries a data stream. To facilitate the reception, the node may transmit an additional chip stream called *pilot tone* [17], which is synchronized with the node's outgoing data streams. In inequality (1) the pilot tone of transmitting node h ($h = 1, \ldots, H$) is of power A_h. $\sum_{i=1,i\neq u}^{\Xi} P_i + \sum_{h=1}^{H} A_h$ is the upper bound of total *Multiple Access Interference* (MAI), that is, 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 usually results from multipath fading. To simplify, we can merge $\sum_{i=1,i\neq u}^{\Xi} P_i$ and P_u to be denoted as $\sum_i P_i$. The component $gP_u/(J + \sum_i P_i + \sum_h A_h)$ shows the effective SNR for the intended channel, $J + \sum_i P_i + \sum_h A_h$ representing the upper bound of noise power and gP_u representing effective signal power. *Inequality (1) implies the bigger the effective SNR, the smaller the probability of bit error $\mathcal{P}_{ber}$.*

A similar notion to BER is *Packet Error Rate* (PER). Without error correction coding, 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, equation (2) and (3) will have a more complicated form, but still, $\mathcal{P}_{per}$ and $\mathcal{P}_{ber}$ maintain one-to-one mapping and $\mathcal{P}_{per}$ decreases as $\mathcal{P}_{ber}$ decreases. When $\mathcal{P}_{per}$ is below a maximal acceptable threshold Θ_{per}, or equivalently, when $\mathcal{P}_{ber}$ is below a maximal acceptable threshold Θ_{ber}, the wireless communication is acceptable for industrial control. Remember inequality (1) implies the bigger the effective SNR, the smaller the BER. Therefore, maintaining an IC-WLAN wireless communication channel (i.e. to maintain $\mathcal{P}_{per} \leq \Theta_{per}$, or say, $\mathcal{P}_{ber} \leq \Theta_{ber}$) means maintaining the effective SNR of the intended channel beyond a threshold Θ_{snr}:

$$\frac{gP_u}{J+\sum_i^{\Xi} P_i + \sum_h^{H} A_h} \quad (4)$$

$$\geq \Theta_{snr} \quad (5)$$

$$= -\ln \Theta_{ber} \quad \text{(because of (1))} \quad (6)$$

$$= -\ln\left(1 - (1 - \Theta_{per})^{1/L^{pkt}}\right) \quad \text{(because of (3))}. \quad (7)$$

Expression (4) is the effective SNR of the intended channel, which can be raised by increasing the processing gain g. Since $g \stackrel{def}{=} r_c/r_b$ and chip rate r_c is usually fixed due to multipath effect and hardware cost constraints [23][17], raising processing gain g means slowing down user data bit rate r_b. *DSSS hereby provides a mechanism to leverage between SNR and data bit rate.*

III. DSSS-CDMA IC-WLAN Architecture

A. The Overall Architecture

Based on Section I and II, we propose building IC-WLAN with DSSS-CDMA cellphone network paradigm: Every IC-WLAN is a cell. Each cell has one *base station* and several *remote stations*. Base stations of different cells are connected via a wireline backbone. All inter-cell communications only go through this wireline backbone. Within a single cell, the base station communicates with its remote stations through wireless. There are no direct wireless communications between remote stations. In this paper, we focus on the single cell, in other words, the single IC-WLAN scenario. Fig. 1 illustrates the architecture of a single IC-WLAN.

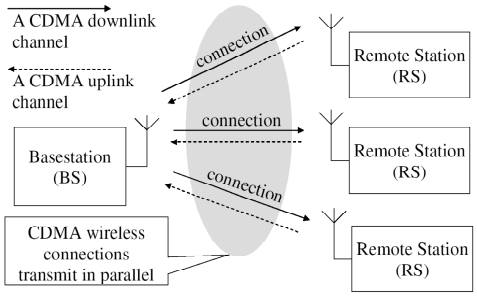


Fig. 1. DSSS-CDMA IC-WLAN architecture

In an IC-WLAN, the RF band available is evenly partitioned into two halves: one for downlink (from base station to remote stations) and the other for uplink (from remote stations to base station). A wireless connection consists of one CDMA channel in each direction (downlink and uplink). Unless explicitly noted, "connection n", a.k.a. "control loop n", refers to both the downlink and uplink of the connection; "a CDMA channel of connection n" refers to both downlink and uplink CDMA channels of the connection. Without loss of generality, we assume sampling packets are sent in uplink, and actuating packets are sent in downlink. In each control loop, sampling/actuating packets are sent continuously so that their bits form a continuous uplink/downlink bit stream respectively.

[2]Inequality (1) assumes QPSK RF modulation and per connection pilot tone. Different implementation alternatives may affect details of the inequality, though there will be no fundamental differences.

This also implies that the sampling/actuating period is the same as the packet transmission period.

B. Resource Planning for Maximized Robustness

In this paper, we attempt to analyze the optimal resource planning for maximized robustness: *given signal attenuation of every wireless connection, how to tolerate maximal external RF interference; and given external RF interference, how to tolerate maximal signal attenuation*. Here, "tolerate" means the packet error rate is maintained below the maximal acceptable threshold.

Although the derivation is complicated, the conclusion is simple and intuitive: maximal robustness is achieved when each connection deploys maximal possible processing gain (i.e., minimal possible data rate). This conclusion is formally described by the following proposition:

Proposition 1 (Maximal Robustness Configuration): To achieve maximal robustness, control loop n ($n = 1, 2, \ldots, N$) of a DSSS-CDMA IC-WLAN should pick maximal possible processing gain:

$$g_n^* = \min\left\{\left\lfloor r_c/(L_n^{pkt} f_n^{min})\right\rfloor, g^{max}\right\}, \tag{8}$$

where r_c is the fixed chip rate, L_n^{pkt} is the packet bit length of control loop n, f_n^{min} is the minimal allowed sampling/actuating rate of control loop n, and g^{max} is the maximal processing gain allowed by hardware.

To derive the above proposition, we first assume the IC-WLAN consists of control loop (a.k.a connection) 1, 2, ..., and N. Control loop n ($n = 1, 2, \ldots, N$) corresponds to a minimal sampling/actuating rate f_n^{min}, a maximal acceptable packet error rate Θ_n^{per}, and a sampling/actuating packet bit length L_n^{pkt} (assume sampling/actuating packets are of the same length; if not, paddings are used to make them the same). The two end nodes of control loop n are the base station, denoted as node 0, and a distinct remote station, denoted as node n. Every node of the IC-WLAN deploys a DSSS chip rate of r_c (i.e. a chip duration of $T_c = 1/r_c$), and carries out conventional *Quadrature Phase Shift Keying* (QPSK) RF modulation/demodulation. The per node maximal transmission power is P^{max}. In the uplink, power balancing is carried out to deal with near-far problem[6]. To assist reception, each node also transmits a pilot tone[17], whose allocated transmission power is the same as any of the node's outgoing CDMA data channels'. The transmitted signal attenuates in the wireless medium due to large-scale path-loss and fading. Let α_n^{down} and α_n^{up} denote the downlink/uplink attenuation of connection n respectively. At the receiver, transmitted signals are received together with external RF interferences (i.e. thermal noise, EMI, and malicious/accidental same-band RF device broadcasts). Denote J_n as the external RF interference power received at Node n ($n = 0, 1, 2, \ldots, N$, Node 0 refers to the base station, Node $1 \ldots N$ refer to remote station $1 \ldots N$ respectively).

The above parameters conform to following relationships:

The configurable parameters are the control loops' processing gain g_n ($n = 1, 2, \ldots, N$), with the following value range:

$$1 \le g_n \le g^{max}, \text{ and } g_n \text{ is an integer.} \tag{9}$$

Here g^{max} is the maximal processing gain allowed by wireless communication hardware (e.g. if g_n is specified by an unsigned byte in the hardware, then g_n can not exceed 256).

Meanwhile, given chip rate r_c, packet bit length L_n^{pkt}, and the chosen processing gain g_n, the packet rate f_n (packets per second) is:

$$f_n = \frac{r_c}{g_n L_n^{pkt}}. \tag{10}$$

Remember the packet rate is the same as the sampling/actuating rate, which must satisfy the minimal sampling/actuating rate requirement, therefore:

$$f_n \ge f_n^{min} \Leftrightarrow g_n \le \frac{r_c}{L_n^{pkt} f_n^{min}}, \qquad n = 1 \sim N. \tag{11}$$

In addition to constraints (9) and (11), there are two more constraints representing the robustness requirements: one for downlink; the other for uplink. *The robustness requirement for connection n is that the packet error rate should not exceed a maximal acceptable threshold Θ_n^{per}, both in downlink and uplink*. According to formulae (5) $\sim$ (7), maximal acceptable packet error rate Θ_n^{per} maps to a minimal acceptable SNR Θ_n^{snr}. To put it in another way, for each connection n, the effective SNR must be maintained above the minimal acceptable threshold Θ_n^{snr}. Inequality (5) quantitatively expresses this notion. According to inequality (5), the robustness requirement for downlink of connection n is:

$$\frac{g_n P_{nn}^{r\_dnlk}}{J_n + \sum_{i=1}^{N} P_{ni}^{r\_dnlk} + A_n^{r\_dnlk}} \ge \Theta_n^{snr}, \quad n = 1 \sim N, \tag{12}$$

where $P_{ni}^{r\_dnlk}$ ($i = 1, 2, \ldots, N$) 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, base station is the only node that transmits pilot tone). Since the base station equally allocates its transmission power to all N downlink channels and the pilot tone, and the total transmission power of the base station is P^{max} to achieve maximal robustness, therefore:

$$\begin{aligned} & P_{n1}^{r\_dnlk} = P_{n2}^{r\_dnlk} = \ldots = P_{nN}^{r\_dnlk} \\ = \quad & A_n^{r\_dnlk} = \alpha_n^{down} \frac{P^{max}}{N+1}. \end{aligned} \tag{13}$$

Substituting formula (13) for (12), the downlink robustness requirement is converted to:

$$\frac{\alpha_n^{down} g_n P^{max}}{(N+1)(J_n + \alpha_n^{down} P^{max})} \ge \Theta_n^{snr}, \quad n = 1 \sim N. \tag{14}$$

For uplink of connection n, again according to inequality (5), the robustness requirement is:

$$\frac{g_n P_n^{r\_uplk}}{J_0 + \sum_{i=1}^{N} P_i^{r\_uplk} + \sum_{i=1}^{N} A_i^{r\_uplk}} \ge \Theta_n^{snr}, \quad n = 1 \sim N, \tag{15}$$

where $P_i^{r\_uplk}$ ($i = 1 \sim N$) is the power of CDMA uplink channel i received at the base station; $A_i^{r\_uplk}$ ($i = 1 \sim N$) is

the power of remote station i's pilot tone received at the base station. Because of power balancing, there is:

$$P_1^{r\_uplk} = P_2^{r\_uplk} = \ldots = P_N^{r\_uplk}. \quad (16)$$

Meanwhile, assume each remote station i ($i = 1, 2, \ldots, N$) equally divides its transmission power $P_i^{t\_uplk}$ between its uplink channel i and pilot tone, then:

$$P_i^{r\_uplk} = A_i^{r\_uplk} = \alpha_i^{up} \frac{P_i^{t\_uplk}}{2}, \qquad i = 1, 2, \ldots, N. \quad (17)$$

Also, each remote station cannot exceed its maximal transmission power:

$$P_i^{t\_uplk} \le P^{max}, \qquad i = 1, 2, \ldots, N. \quad (18)$$

The transmission power of each remote station $P_i^{t\_uplk}$ should be maximized to increase SNR (and therefore robustness), meanwhile maintaining the constraints depicted in formulae (16) and (18). Therefore, the remote station that suffers the most severe uplink power attenuation should transmit with power P^{max}, and all the other remote stations should adjust their transmission power according to power balancing rule (16). The above is formalized as follows:

$$\begin{aligned} & P_k^{t\_uplk} = P^{max}, \\ & \text{therefore } \; P_k^{r\_uplk} = A_k^{r\_uplk} = \alpha_k^{up} \frac{P^{max}}{2}, \quad (19) \\ & \text{where } \; k = \text{argmin}_{i \in \{1,2,\ldots,N\}} \{\alpha_i^{up}\}. \end{aligned}$$

$$\begin{aligned} & (16), (17) \\ \Rightarrow \quad & P_i^{r\_uplk} = A_i^{r\_uplk} = \alpha_i^{up} \frac{P_i^{t\_uplk}}{2} = P_k^{r\_uplk} \\ \Rightarrow \quad & P_i^{t\_uplk} = \frac{\alpha_k^{up} P^{max}}{\alpha_i^{up}} \qquad \text{(because of (19))} \\ \Rightarrow \quad & P_i^{r\_uplk} = A_i^{r\_uplk} = \alpha_i^{up} \frac{P_i^{t\_uplk}}{2} = \alpha_k^{up} \frac{P^{max}}{2} \quad (20) \end{aligned}$$

Denote

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

and substitute (19) $\sim$ (21) for (15), the uplink robustness requirement is converted to:

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

The downlink/uplink robustness requirements (formulae (14) and (22)) can be converted as follows:

$$\begin{aligned} (14) \Leftrightarrow J_n \quad \le \quad & \left(\frac{\alpha_n^{down} g_n P^{max}}{(N+1)\Theta_n^{snr}} - \alpha_n^{down} P^{max} \right) \\ & \stackrel{def}{=} \bar{J}_n^{down}, \quad n = 1, 2, \ldots, N; \quad (23) \\ (22) \Leftrightarrow J_0 \quad \le \quad & \left(\frac{\alpha^{up} g_n P^{max}}{2\Theta_n^{snr}} - \alpha^{up} N P^{max} \right) \\ & \stackrel{def}{=} \bar{J}_n^{up}, \quad n = 1, 2, \ldots, N, \quad (24) \end{aligned}$$

where $\bar{J}_n^{down}$ and $\bar{J}_n^{up}$ represent the maximal 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

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

then J^{min} *represents the minimal external RF interference power needed to disrupt at least one of the connections.*

When the power attenuations α_1^{down}, α_2^{down}, …, α_N^{down}, α_1^{up}, α_2^{up}, …, α_N^{up} are given, robustness maximization means the IC-WLAN tolerates (i.e., the robustness requirements are satisfied, or quantitatively, both inequality (23) and (24) sustain) maximal external RF interference power (i.e., J^{min} is maximized). Since the only configurable parameters are g_n ($n = 1 \sim N$), which comply with constraints (9) and (11), formulae (23) $\sim$ (25) imply that the IC-WLAN tolerates maximal external RF interference power when $g_n = \min\left\{\left\lfloor r_c/(L_n^{pkt} f_n^{min})\right\rfloor, g^{max}\right\}$. When $J_0, J_1, J_2, \ldots, J_N$ are given, robustness maximization means the IC-WLAN tolerates maximal power attenuations (i.e., α_1^{down}, α_2^{down}, …, α_N^{down}, α_1^{up}, α_2^{up}, …, α_N^{up} are minimized). Similarly, this is also achieved when $g_n = \min\left\{\left\lfloor r_c/(L_n^{pkt} f_n^{min})\right\rfloor, g^{max}\right\}$.

Therefore, Proposition 1 holds.

IV. Simulation and Comparisons

In this section, we first demonstrate the robustness of the proposed DSSS-CDMA IC-WLAN based on fine-grained physical layer simulations. Then we carry out more comprehensive comparisons between the DSSS-CDMA scheme and conventional IEEE 802.11/802.15.4 schemes. In the end, the alternative of using error correction coding is discussed.

A. Demo using Fine-Grained Physical Layer Simulation

We carry out fine-grained physical layer simulation to demonstrate the effectiveness of the proposed DSSS-CDMA IC-WLAN scheme. The simulation environment is built on top of J-Sim kernel [24]. Fig. 2(a) depicts the simulated scenario. According to it, the IC-WLAN includes two connections: connection 1 and 2. Each connection controls an *Inverted Pendulum* (IP) [9]: IP 1 and IP 2. As a remote station, each IP periodically sends back its state (x, θ, and time stamp) to the base station. Based on the most up-to-date IP state, the base station calculates the next control (u) and sends it back to the IP. The sampling/actuating packet length are both 152 bits, and the minimal sampling/actuating rates are $f_1^{min} = f_2^{min} = 10$Hz.

Without loss of generality, the two IPs are the same. As shown in Fig. 2(b), x is the position of IP cart, θ is the angular deviation of IP from vertical position, and u is the control voltage applied to IP cart. The state transition equation and control equation are also depicted in the figure (in addition, when θ and u are of opposite signs, u is obviously out-of-date due to delay and is therefore ignored). The IP cart moves along the x axis to keep the IP standing vertically. Each IP fall-down (defined as $|\theta|$ exceeds $\frac{\pi}{6}$) incurs a high cost resetting procedure.

We carry out simulation under both DSSS-CDMA and IEEE 802.11b schemes. A wireless medium instance generated from

TABLE I
WIRELESS MEDIUM MODEL

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

$*$ β is the path loss exponent, σ is the log-normal standard deviation.
† To deal with multipath fading, both DSSS-CDMA and IEEE 802.11b use two-finger RAKE receivers [23][17].
‡ Typically refers to thermal noise.

a typical indoor-industrial-environment model [6][25] depicted in Table I is applied to the simulation of both schemes. To be fair, for both schemes, the maximal transmission power of all nodes (the base station and all remote stations) are 1watt, the maximal transmission power allowed by FCC for IEEE 802.11b. The only exception is for DSSS-CDMA uplinks, where transmission power must also comply with the power balancing requirement to produce the same power level at the base station. The power balancing requirement makes the comparison more pessimistic on the DSSS-CDMA side, because some nodes are not transmitting with maximal power. Again, to make fair comparisons, both DSSS-CDMA and IEEE 802.11b schemes occupy the same RF band of $2.426 \sim 2.448$GHz, a typical RF band of IEEE 802.11b. For DSSS-CDMA, the RF band is divided into two halves: $2.426 \sim 2.437$GHz for downlink and $2.437 \sim 2.448$GHz for uplink. For IEEE 802.11b, the signal occupies the whole RF band, but packets are time multiplexed into downlink packets and uplink packets. These RF bandwidth configurations imply a chip rate of $r_c^{cdma} = 5.5$Mcps for DSSS-CDMA and a chip rate of $r_c^{ieee80211b} = 11$Mcps for IEEE 802.11b.

The above explains parameters relevant to both schemes. Further, the scheme-dependent details run as follows: For DSSS-CDMA scheme, the hardware-dependent processing gain upper bound g^{max} is 1024 (complies with cdmaOne [26]). According to Proposition 1, the processing gain that maximize robustness is therefore $g^{cdma} = \min\{\lfloor \frac{5.5\times10^6}{152\times10} \rfloor, 1024\} = 1024$. Without loss of generality, our DSSS-CDMA scheme deploys QPSK RF modulation/demodulation and per-node pilot tone. For each node, the pilot tone is allocated with the same transmission power as any outgoing CDMA data channel of the node. For IEEE 802.11b scheme, the most robust 1Mbps mode is deployed, corresponding to a processing gain of $g^{ieee80211b} = 11$ and *Differential BPSK* (DBPSK) RF modulation/demodulation. To be fair, the IEEE 802.11b WLAN works in pure PCF, the mode for real-time systems. Under PCF, the base station polls IP 1 and IP 2 in round robin without idling and backoff (backoff causes deadline miss). The control packet is sent to the IP as the poll packet, and the sample packet is sent back from IP as the acknowledgment packet.

To demonstrate the robustness of DSSS-CDMA scheme, an external RF interference source is placed near IP 1 (see Fig. 2(a)). This external RF interference occupies the same RF band that DSSS-CDMA and IEEE 802.11b are using. And the interference source transmits with a power of 1 watt, just the same as the maximal transmission power of a normal IC-WLAN node.

The simulated scenario 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.

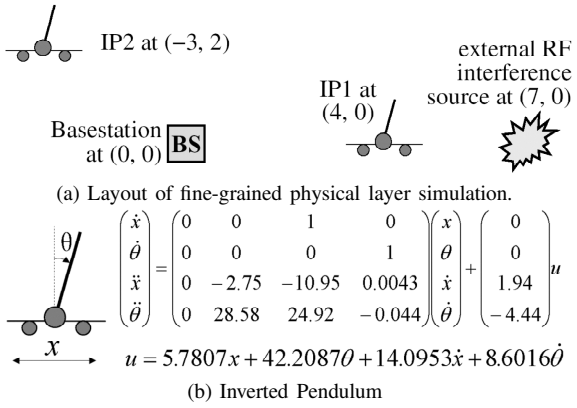
Fig. 3 shows the traces of θ. The traces show that throughout the time, both IP 1 and IP 2 remain fairly stable under DSSS-CDMA, even when there is external RF interference ($5 \sim 15$sec). This means the wireless control loops survive adverse channel conditions. Under IEEE 802.11b, however, IP 1 keeps falling due to external RF interference (every time it falls, the IP resets to 0.5rad and stays there for 0.2sec to restart). Note under IEEE 802.11b, IP 2 can also survive external RF interference because it is much closer to the base station than to the external RF interference source.

B. Comparisons to IEEE 802.11 a/b

IEEE 802.11 is the nowadays predominant WLAN scheme. It can be further categorized into IEEE 802.11b[27], a[28] and g[29]. IEEE 802.11b/a/g differ in their physical layers, but share the same MAC layer specification (with minor variations). IEEE 802.11b operates at the 2.4GHz RF range and deploys DSSS for its most robust mode. IEEE 802.11a operates at the 5GHz RF range and deploys *Orthogonal Frequency Division Multiplexing* (OFDM) [30][31][32] in physical layer. IEEE 802.11g is basically the union of 802.11b and 802.11a. At MAC layer, IEEE 802.11 operates under *Distributed Coordination Function* (DCF) paradigm, which carries out CSMA/CA and MACAW [33] MAC protocols. DCF is therefore contention/random-backoff based and is not for real-time communications. In contrast, IEEE 802.11 also specifies the *Point Coordination Function* (PCF) paradigm, where the base station polls each remote station. PCF is contention-free and is hence for real-time communications.

IEEE 802.11 was mainly designed for high data rate bursty communications in office/home applications, such as FTP, emails and Web browsing. This mismatches the needs of most IC-WLAN control loops, where the demand for data throughput is low (typical packet lengths are $100 \sim 200$ bits, and minimal acceptable sampling/actuating rates are $1 \sim 10$Hz, or lower), while the demand for robustness is high: sampling/actuating packets must be delivered in real-time even under adverse channel conditions. In the following, we see IEEE 802.11's tolerance of adverse channel conditions is much inferior to that of the proposed DSSS-CDMA scheme, which fully exploits the low data throughput feature of IC-WLAN.

The comparisons between DSSS-CDMA and IEEE 802.11 are based on Monte Carlo simulations. In the simulator, the industrial indoor environment is a square room of $20\text{m} \times 20\text{m}$. The base station sits in the center while N remote stations scatter across the room according to uniform random distribution. Each remote station corresponds to a wireless control loop. The value of N varies from 1 to 100. Without loss of generality, the size of all sampling/actuating packets is 152 bits (the same as the inverted pendulum case, a typical control



(a) Layout of fine-grained physical layer simulation.

(b) Inverted Pendulum

Fig. 2. Simulated Scenario

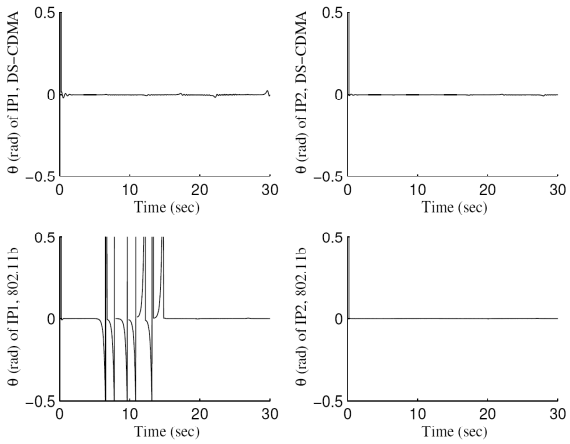


Fig. 3. Simulation Results (θ traces)

TABLE II
PHY. SETTINGS FOR DSSS-CDMA/IEEE802.11 COMPARISONS

	Max per node trans power*	RF mainlobe bandwidth†‡
DSSS-CDMA vs. IEEE 802.11b	1watt	22MHz
DSSS-CDMA vs. IEEE 802.11a	800mw	18MHz for IEEE 802.11a, and 14.6MHz for DSSS-CDMA‡

∗ According to FCC regulation.

† Mainlobe is the main part of a signal's RF spectrum that carries information. For DBPSK, BPSK and QPSK RF modulation that are used in IEEE 802.11b, IEEE 802.15.4a/b and our proposed DSSS-CDMA scheme, the RF mainlobe bandwidth is equivalent to two times of chip rate. IEEE 802.15.4c uses O-QPSK, where the RF mainlobe bandwidth is equivalent to the chip rate. The mainlobe bandwidth of IEEE 802.11a 6Mbps mode (the most robust mode of IEEE 802.11a) can be regarded as 18MHz, although IEEE 802.11a has a special RF spectrum shape due to OFDM.

Note: in this paper, when referring to DSSS-CDMA cellphone scheme, the mainlobe counts both the downlink and uplink RF spectra.

‡ According to IEEE 802.11 specifications, one single IEEE 802.11b RF channel has an RF mainlobe bandwidth of 22MHz, one single IEEE 802.11a RF channel has an RF mainlobe bandwidth of 18MHz. Due to difference between OFDM and DSSS modulations, letting DSSS-CDMA have an RF mainlobe bandwidth of 14.6MHz in the DSSS-CDMA versus IEEE 802.11a comparison safely makes the comparison pessimistic on the DSSS-CDMA side.

packet size), and all control loops have the same minimal acceptable sampling/actuating rate f^{min}. Two values of f^{min} are tested: 1Hz and 10Hz, which are typical for distributed industrial control loops. Every sampling/actuating packet must be delivered with success probability of no less than 0.999, that is, the maximal acceptable packet error rate Θ^{per} is 0.001. For a given N, f^{min} and IC-WLAN scheme (DSSS-CDMA, IEEE 802.11b, or IEEE 802.11a), 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 I). Each trial calculates its J^{min}: the minimal external RF interference power needed to disrupt at least one wireless control loop (see (25)). J^{min} is the quantitative robustness indicator compared between the DSSS-CDMA and IEEE 802.11b/a IC-WLAN schemes.

To make fair comparisons, parameters relevant to both schemes are set according to Table II. Scheme-specific details are as follows:

For IEEE 802.11b, the most robust 1Mbps mode is deployed. For IEEE 802.11a, the most robust 6Mbps mode is deployed, *Note 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*.

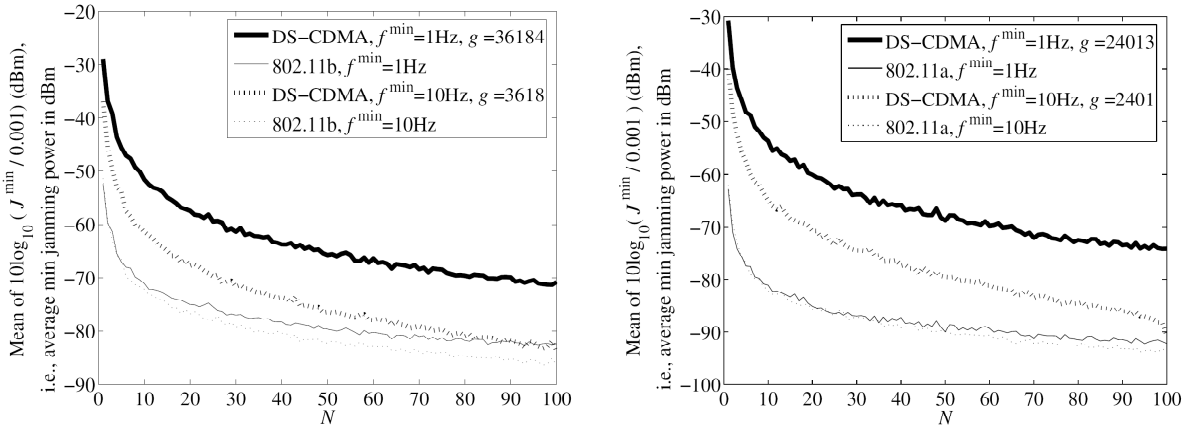
For DSSS-CDMA, QPSK RF modulation/demodulation is deployed, with the RF band evenly divided into two halves: one for downlink and the other for uplink. The DSSS-CDMA scheme also deploys per-node pilot tone. The pilot tone is allocated with the same transmission power as any outgoing data channel of the node. To achieve maximal robustness, we shall set processing gain g_n according to Proposition 1. Assuming the hardware-dependent upper bound on processing gain g^{max} is sufficiently large[3], Proposition 1 implies that the processing gain g_n for control loop n shall be $\lfloor r_c/(f_n^{min} L_n^{pkt}) \rfloor$. Specifically, given packet bit length ($L_n^{pkt} = 152$bit) and the RF mainlobe bandwidth (which decides chip rate r_c, see Table II footnote † for further explanation) listed in Table II, when $f^{min} = 1$Hz and 10Hz, the corresponding processing gains are 36184 and 3618 for DSSS-CDMA/IEEE 802.11b comparison, and 24013, 2401 for DSSS-CDMA/IEEE 802.11a comparison[4].

The calculation of J^{min} for DSSS-CDMA and IEEE 802.11b/a schemes are based on their respective PER(BER)-SNR relationships. For DSSS-CDMA, the upper bound of BER under specified SNR is given in inequality (1). For IEEE 802.11b 1Mbps mode, inequality (26) gives the lower bound of BER under given SNR [20]:

$$\mathcal{P}_{ber}^{80211b} \geq \frac{1}{2}\,\mathrm{erfc}\sqrt{\frac{gP_u}{J}}, \tag{26}$$

[3]The upper bound on processing gain can increase exponentially when hardware increases. For example, with 61 registers, it is enough to produce PN sequence of $2,305,843,009,213,693,951$ chips, which is enough to allow any processing gain in practice [19].

[4]Note RF mainlobe bandwidth determines chip rate r_c. For a given chip rate r_c, any processing gain g can be picked, but a bigger g corresponds to a slower bit rate $r_b = r_c/g$.



(a) Comparison with IEEE 802.11b (b) Comparison with IEEE 802.11a

Fig. 4. Robustness comparison between DSSS-CDMA and IEEE 802.11b/a IC-WLANs. J^{min}(watt) is the minimal external RF interference power needed to disrupt at least one wireless control loop (note P(watt) equals $10\log_{10}(P/0.001)$(dBm)). 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.

where g is the processing gain, P_u is the received signal power, J is the received total external RF interference 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 error correction. The corresponding PER-SNR relationship can be empirically derived through Monte Carlo simulations. Based on these BER(PER)-SNR relationships, J^{min}s of DSSS-CDMA and IEEE 802.11b/a schemes can be calculated. Fig. 4(a) and (b) compare these J^{min}s derived in all Monte Carlo trials. This comparison is pessimistic on the DSSS-CDMA side and optimistic on the IEEE 802.11b/a side because of many reasons: i) 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. ii) in inequality (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, in Fig. 4(a) and (b), the curves for DSSS-CDMA are J^{min} lower bounds while the curves for IEEE 802.11b/a are J^{min} upper bounds.

According to Fig. 4, the proposed DSSS-CDMA scheme can tolerate much bigger external RF interference power than the corresponding IEEE 802.11 schemes. When $f^{min} = 10$Hz and 1Hz, DSSS-CDMA achieves approximately 10dB and 20dB improvements on robustness than IEEE 802.11b, and approximately 20dB and 30dB improvements than IEEE 802.11a respectively. This is because the DSSS-CDMA scheme fully exploits the low data rate feature of industrial control loops by setting processing gain according to Proposition 1. When the data rate demand of control loop decreases (i.e. with smaller f^{min}), larger processing gain can be deployed and the corresponding tolerable external RF interference power increases.

C. Comparisons to IEEE 802.15.4

IEEE 802.15.4 [16] is a PHY/MAC standard for low data rate *Wireless Personal Area Networks* (WPAN). Recently, however, there is growing interest in applying IEEE 802.15.4 to *ad hoc* wireless sensor networks in efforts such as ZigBee [14]. Similar to IEEE 802.11 DCF and PCF, IEEE 802.15.4 also has two paradigms: *Contention Based* (CB) and *Contention Free* (CF). IEEE 802.15.4 CB mode uses CSMA/CA MAC, which is not for real-time communications. IEEE 802.15.4 CF mode is a centralized polling scheme (almost the same as IEEE 802.11 PCF), which supports real-time communications. Therefore, we compare DSSS-CDMA scheme with IEEE 802.15.4 CF.

Similar to IEEE 802.11, IEEE 802.15.4 can be further categorized into IEEE 802.15.4a/b/c according to their assigned RF ranges (see Table III).

TABLE III
IEEE 802.15.4 SUBTYPES

Subtype	RF range* (MHz)	Per RF chnl bandwidth* (MHz)	Number of RF chnls*	Max per node trans power (Watt)
a†	868 ∼ 868.6	0.6	1	0.025†
b	902 ∼ 928	2	10	1‡
c	2400 ∼ 2483.5	5	16	1‡

Subtype	Chip rate (kcps)	RF main-lobe band-width (MHz)	Modu-lation	Bit rate (kbps)	Symbol rate (ksps)	Symbols
a†	300	0.6	BPSK	20	20	Binary
b	600	1.2	BPSK	40	40	Binary
c	2000	2	O-QPSK	250	62.5	16-ary Or-thogonal

∗ See Fig. 5 for definitions of "RF range", "RF chnl", "Per RF chnl bandwidth", and "Number of RF chnls".
† Only allowed in Europe.
‡ According to FCC.

We carry out the same Monte Carlo simulation as Section IV-B to compare DSSS-CDMA and IEEE 802.15.4a/b/c,

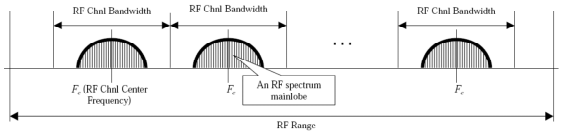


Fig. 5. Definitions of RF range, RF channel, and RF channel bandwidth

TABLE IV
PHY. SETTINGS FOR DSSS-CDMA/IEEE802.15.4 COMPARISONS

			Max per node trans power*	RF mainlobe bandwidth†
DSSS-CDMA 802.15.4a	vs.	IEEE	25mw	0.6MHz
DSSS-CDMA 802.15.4b	vs.	IEEE	1watt	1.2MHz
DSSS-CDMA 802.15.4c	vs.	IEEE	1watt	2MHz

$*$ According to European regulation for IEEE 802.15.4a (FCC forbids free usage of $868 \sim 868.6$MHz for IEEE 802.15.4a) and FCC regulation for IEEE 802.15.4b/c.
† According to IEEE 802.15.4 specification. Also see Table II footnote † for definitions and discussions on mainlobe.

using the wireless medium model given in Table I and the common physical layer settings given in Table IV.

The scheme-dependent details of DSSS-CDMA are slightly different from that of Section IV-B: when $f^{min} = 1$Hz and 10Hz, the corresponding processing gains are 987 and 99 for DSSS-CDMA/IEEE 802.15.4a comparison; 1974 and 197 for DSSS-CDMA/IEEE 802.15.4b comparison; and 3289, 329 for DSSS-CDMA/IEEE 802.15.4c comparison. These differences are due to change of RF mainlobe bandwidths in our comparisons.

Note for IEEE 802.15.4a/b/c schemes, the packet is retransmitted as many times as possible throughout the sampling/actuating period, so as to increase the chance of successful delivery.

We still use J^{min}, the minimal external RF interference power needed to disrupt at least one control loop, as the indicator of IC-WLAN robustness. The calculation of J^{min} for DSSS-CDMA and IEEE 802.15.4a/b/c schemes are still based on BER-SNR relationships ("BER" for *Bit Error Rate*). The DSSS-CDMA BER-SNR relationship is still given in inequality (1). For IEEE 802.15.4a/b, since they both use BPSK (see Table III), their BER-SNR relationship still follows inequality (26). IEEE 802.15.4c, however, uses O-QPSK RF modulation/demodulation with 32-chip pseudo-orthogonal coding (see Table III and [16]). Such scheme makes it hard to derive a closed-form tight lower bound on BER for given SNR. Fortunately, Monte Carlo simulation can still give an empirical BER lower bound that is tight enough. Based on the above BER-SNR relationships, J^{min} of DSSS-CDMA and IEEE 802.11a/b/c schemes can be calculated. Fig. 6(a), (b) and (c) compare these J^{min}s derived in Monte Carlo simulations. As stated in Section IV-B, the comparisons are still pessimistic on the DSSS-CDMA side and optimistic on the IEEE 802.15.4a/b/c side. That is, in Fig. 6(a), (b) and (c), the curves for DSSS-CDMA are J^{min} lower bounds, and the curves for IEEE 802.15.4 are J^{min} upper bounds.

According to Fig. 6, when the sampling/actuating rate is low (see the $f^{min} = 1$Hz curves), DSSS-CDMA significantly out-performs IEEE 802.15.4a/b/c on robustness. When the sampling/actuating rate is high, however, DSSS-CDMA only performs better when N (total number of control loops) is small, and becomes inferior to IEEE 802.15.4b/c when N is large enough (see the $f^{min} = 10$Hz curves). This is because an IEEE 802.15.4a/b/c RF channel is of very narrow RF bandwidth. To squeeze into the same RF bandwidth, the chip rate of DSSS-CDMA scheme must be low. When the data throughput is high (since packet bit size is fixed to 152, a higher sampling/actuating rate f^{min} or a bigger N corresponds to a larger data throughput), DSSS-CDMA cannot deploy a basic-need processing gain g to overcome MAI.

Fortunately, the continuous RF bandwidth available is usually much wider than what is used by an IEEE 802.15.4 RF channel. For example, wherever an IEEE 802.11b WLAN can be deployed, the continuous RF bandwidth available is at least 22MHz, equivalent to 36.7, 11 and 4.4 times the RF bandwidth of an IEEE 802.15.4a, b and c RF channel respectively. Such 22MHz RF bandwidth allows the DSSS-CDMA IC-WLAN mainlobe bandwidth to be 36.7, 18.3 and 11 times the IEEE 802.15.4a, b and c mainlobe bandwidths respectively.

Another way of thinking is as follows: In a 3-D space, one can use 27 non-overlapping RF channels to color cells so that any two cells using the same RF channel are at least three hops (cells) away (see Fig. 7). The FCC *Industrial-Scientific-Medical* (ISM) RF ranges allow 27 non-overlapping RF channels, each with a continuous RF bandwidth of at least 14MHz, which is 23.3, 7 and 2.8 times the RF bandwidth of an IEEE 802.15.4a, b and c RF channel respectively. In terms of RF mainlobes, such 14MHz RF bandwidth allows the DSSS-CDMA IC-WLAN mainlobe bandwidth to be 23.3, 11.7 and 7 times the IEEE 802.15.4 a, b and c mainlobe bandwidths respectively.

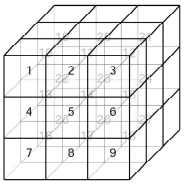
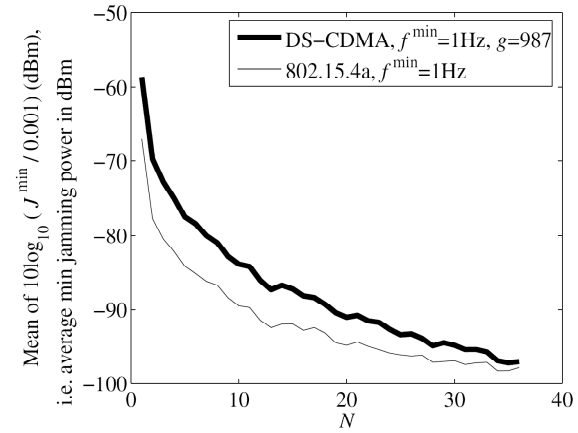


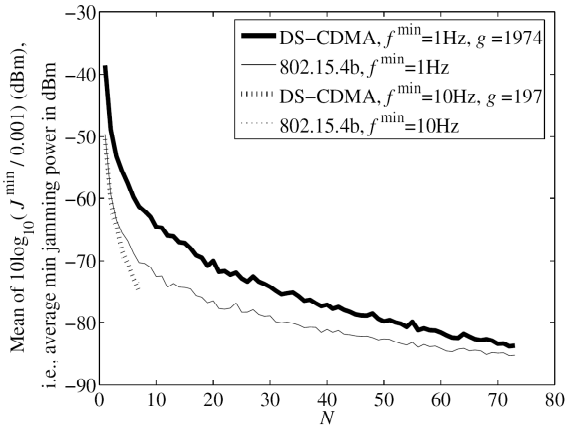
Fig. 7. Twenty-seven colors are enough to color the cells in a 3-D space so that any two same-color cells are at least 3 hops (cells) away.

Therefore, the comparisons in Fig. 6 are too pessimistic on the DSSS-CDMA side. Given a layout of IEEE 802.15.4a/b/c base stations, for each corresponding IC-WLAN, the continuous RF bandwidth available is usually much bigger than that of an IEEE 802.15.4a/b/c RF channel. If DSSS-CDMA fully utilizes the RF bandwidth available, the DSSS-CDMA performance can improve significantly.

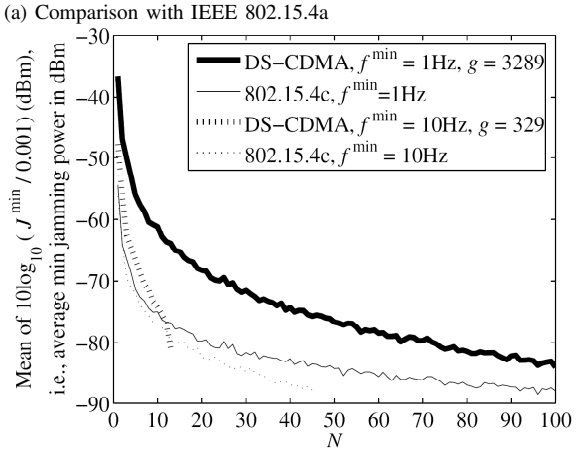
In the following, we redo the Monte Carlo comparisons between DSSS-CDMA and IEEE 802.15.4a/b/c with modified physical layer settings as shown in Table V. According to Table V, the RF mainlobe bandwidth of DSSS-CDMA is w



(a) Comparison with IEEE 802.15.4a



(b) Comparison with IEEE 802.15.4b



(c) Comparison with IEEE 802.15.4c

Fig. 6. Robustness comparison between DSSS-CDMA and IEEE 802.15.4a/b/c IC-WLANs. The meaning of J^{min} and "dBm" is the same as in Fig. 4. N is the number of wireless control loops. The curves for DSSS-CDMA are lower bounds for J^{min}, while the curves for IEEE 802.15.4a/b/c are upper bounds. Note for DSSS-CDMA/IEEE 802.15.4a comparison, when $f^{min} = 10$Hz, with a packet size of 152 bits, an IEEE 802.15.4a IC-WLAN can only afford 3 control loops. Such IC-WLAN is practically useless. Similarly, when $f^{min} = 10$Hz, an IEEE 802.15.4b/c IC-WLAN can only afford 7 and 45 control loops respectively; when $f^{min} = 1$Hz, an IEEE 802.15.4b IC-WLAN can only afford 73 control loops.

TABLE V
PHY. SETTINGS FOR DSSS-CDMA/IEEE802.15.4 COMPARISONS

	Max per node trans power*	RF mainlobe bandwidth†
DSSS-CDMA vs. IEEE 802.15.4a	25mw	600kHz for IEEE 802.15.4a, $w\times$ 600kHz for DSSS-CDMA
DSSS-CDMA vs. IEEE 802.15.4b	1watt	1.2MHz for IEEE 802.15.4b, $w\times$ 1.2MHz for DSSS-CDMA
DSSS-CDMA vs. IEEE 802.15.4c	1watt	2MHz for IEEE 802.15.4c, $w\times$ 2MHz for DSSS-CDMA

$*$ According to European regulation for IEEE 802.15.4a and FCC regulation for IEEE 802.15.4b/c.
† According to IEEE 802.15.4 specification. Also see Table II footnote † for definitions and discussions on mainlobe.

times the mainlobe bandwidth of an IEEE 802.15.4a/b/c RF channel. Different w's are evaluated, with the results plotted in Fig. 8.

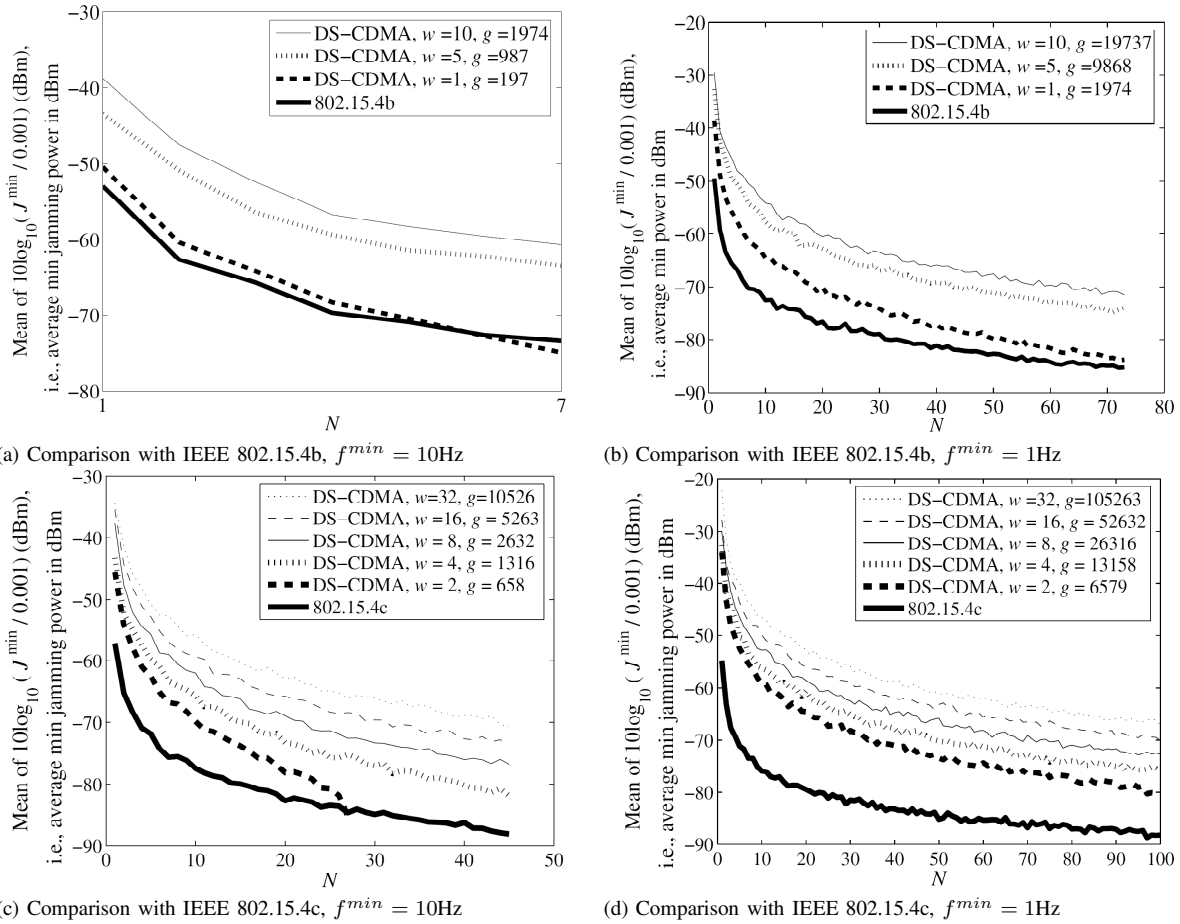
Note in Fig. 8, we do not compare DSSS-CDMA with IEEE 802.15.4a. This is because: i) IEEE 802.15.4a uses the same modulation/demodulation scheme as IEEE 802.15.4b; ii) IEEE 802.15.4a allows much lower maximal transmission power (0.025Watt) than IEEE 802.15.4b (1Watt); iii) IEEE 802.15.4a provides half the bit rate (and chip rate) of IEEE 802.15.4b; iv) IEEE 802.15.4a is not allowed by FCC (only allowed in Europe). Therefore, in terms of either robustness or data throughput, IEEE 802.15.4a is inferior to IEEE 802.15.4b. Given the DSSS-CDMA versus IEEE 802.15.4b comparisons, comparisons to IEEE 802.15.4a are redundant.

D. Discussion on Error Correction Coding

Another way to exploit low data rate for higher robustness is dedicating the redundant bandwidth to error correction code. The most popular error correction coding is the convolutional coding. At the sender end, a convolutional encoder (k, n, m) encodes every k input bits into n output bits using m shift memory registers, where

$$m \geq \lceil \log_2 n \rceil \tag{27}$$

to produce practical convolutional codes. Such encoder corresponds to a coding rate $R \stackrel{def}{=} \frac{k}{n}$. The upper bound of coding gain is decided by k, n and m. Assuming binary antipodal symbol signal and AWGN channel, convolutional coding achieves a gain of Rd_f – which is often called the *Asymptotic Coding Gain* (ACG) – on SNR, where R is the



(a) Comparison with IEEE 802.15.4b, $f^{min} = 10$Hz

(b) Comparison with IEEE 802.15.4b, $f^{min} = 1$Hz

(c) Comparison with IEEE 802.15.4c, $f^{min} = 10$Hz

(d) Comparison with IEEE 802.15.4c, $f^{min} = 1$Hz

Fig. 8. Robustness comparison between DSSS-CDMA and IEEE 802.15.4b/c IC-WLANs, when the DSSS-CDMA RF mainlobe bandwidth is w times the mainlobe bandwidth of an IEEE 802.15.4b/c RF channel (see Table V). J^{min}(watt) is the minimal external RF interference power needed to disrupt at least one wireless control loop. 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 802.15.4b/c are upper bounds. Also note when $f^{min} = 10$Hz, an IEEE 802.15.4b/c IC-WLAN can only afford 7 and 45 control loops respectively; when $f^{min} = 1$Hz, an IEEE 802.15.4b IC-WLAN can only afford 73 control loops.

coding rate and d_f is the free distance of convolutional codes. Denote ACG as g_{acg}. A loose upper bound of d_f is $n(m+1)$, so ACG g_{acg} is upper bounded by:

$$g_{acg} = Rd_f \leq Rn(m+1) = k(m+1). \tag{28}$$

Suppose the available wireless medium bandwidth is B_{medium}(bps), and the information bandwidth is B_{info}(bps). Using DSSS, the maximal gain on SNR is a processing gain

$$g = B_{medium}/B_{info} \qquad \text{(according to Proposition 1).} \tag{29}$$

Using convolutional coding, the maximal gain on SNR is an ACG of $g_{acg} = k(m+1)$. To achieve the maximal ACG, all redundant bandwidth shall be dedicated to convolutional coding, that is, coding rate $R = B_{info}/B_{medium}$, in other words, $n = kB_{medium}/B_{info}$. Because of inequality (27), we shall pick $m = \lceil \log_2 n \rceil = \lceil \log_2(kB_{medium}/B_{info}) \rceil$ (why not to pick a bigger m is explained later). Therefore, the maximal gain on SNR using convolutional coding is:

$$g_{acg} = k(m+1) = k\left(\left\lceil \log_2 \frac{kB_{medium}}{B_{info}} \right\rceil + 1 \right). \tag{30}$$

For the typical IC-WLAN scenario where B_{medium} equals 10Mbps and B_{info} varies from 1bps to 100Kbps, Fig. 9 compares the SNR gain between using DSSS and using convolutional coding with $k = 1$ and $m = \lceil \log_2 n \rceil = \lceil \log_2(kB_{medium}/B_{info}) \rceil$. According to Fig. 9, DSSS significantly outperforms convolutional coding on improving SNR.

Because $g_{acg} \leq k(m+1)$, some may argue if a bigger k or m is picked, the performance of ACG may be better. Nevertheless, even with the small value of $k = 1$ and $m = \lceil \log_2 n \rceil = \lceil \log_2(kB_{medium}/B_{info}) \rceil$, the convolutional coding used in Fig. 9 is already impractical: Empirically, no good convolutional coding scheme with $n > 99$ is known. To achieve maximal ACG, however, the entire bandwidth is dedicated for convolutional code, that is, $n = kB_{medium}/B_{info}$. When $k = 1$, $B_{medium} = 10$Mbps, and B_{info} varies from 1bps to 100Kbps, n varies from 10^7 to 100, all exceeding 99. Picking bigger k or m does not help solve this problem.

Even if convolutional coding schemes with $n > 99$ are found, decoder complexity may still prevent us from picking a bigger k or m: For a convolutional decoder, the number of algorithmic operations per second (denoted as Op) is [34]:

$$Op = c2^{km+1}B_{info}/k, \tag{31}$$

where c is an implementation dependent positive constant,

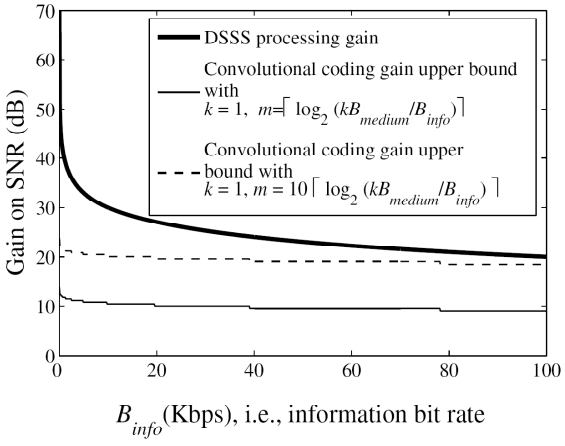


Fig. 9. Comparison on gain over SNR. The available wireless medium bandwidth $B_{medium} = 10$Mbps; information data bit rate B_{info} varies from 1bps to 100Kbps. All redundant bandwidth are dedicated to achieving higher gain on SNR: in the DSSS scheme, $g = B_{medium}/B_{info}$; in the convolutional coding scheme, $n = kB_{medium}/B_{info}$ (note convolutional coding gain (ACG g_{acg}) is upper bounded by $k(m+1)$, where m must be no less than $\lceil \log_2 n \rceil$).

empirically no less than 1. Fig. 10 plots Op when $k = 2$, $m = \lceil \log_2 n \rceil = \lceil \log_2(kB_{medium}/B_{info}) \rceil$, $c = 1$, and $B_{medium} = 10$Mbps. The decoding complexity is daunting ($Op \approx 10^{10}$). Since picking a bigger k is infeasible, the alternative is to pick a bigger m. According to Fig. 9, if $k = 1$, m must be at least $10\lceil \log_2 n \rceil = 10\lceil \log_2(kB_{medium}/B_{info}) \rceil$ to let convolutional coding ACG outperform DSSS processing gain. Fig. 10 also plots Op for this case, that is, $k = 1$, $m = 10\lceil \log_2 n \rceil = 10\lceil \log_2(kB_{medium}/B_{info}) \rceil$, $c = 1$, and $B_{medium} = 10$Mbps. The decoding complexity is even more daunting ($Op > 10^{20}$). Therefore, picking a bigger k or m is not the way out for convolutional coding to outperform DSSS.

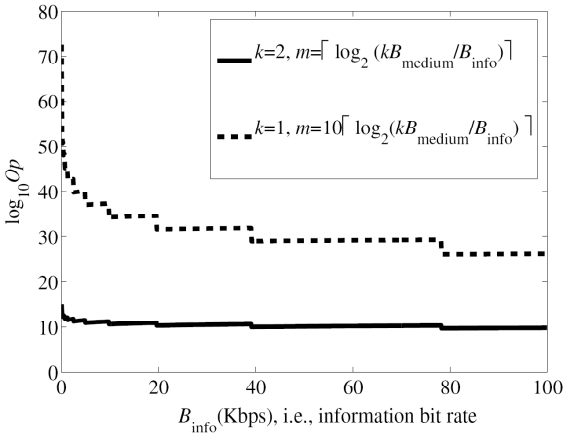


Fig. 10. Convolutional Decoding Complexity

V. Related Work

One purpose of this paper is to demonstrate DSSS-CDMA cellphone network paradigm is more appropriate for IC-WLAN than the dominant IEEE 802.11/802.15.4 WLAN paradigms. Intuitively, industrial control loop and cellphone voice session bear many similarities: they are both low-data-rate regular traffic, and last for long duration in a session-like pattern. The main difference lies in the high robustness concern for industrial control loops. Such concern calls for better exploitation of the low data rate feature to provide more robustness. Current CDMA cellphone network architectures have not yet focused on such demand. However, the current CDMA cellphone network architectures [26][35][36][37] provide good foundations to start building our proposed DSSS-CDMA IC-WLAN with. 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 [38][39] 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 [15][28][27][29] and IEEE 802.15.4 WLANs [16], both of which have fixed robustness levels. Nonetheless, if application-dependent processing gain configuration is provided for IEEE 802.11b or IEEE 802.15.4, its robustness can also be greatly improved. This is exactly the DSSS-*TDMA* IC-WLAN approach, which is shown to be less preferable than DSSS-CDMA for three weaknesses (see Section II). However, it still merits further study on how to overcome these three weaknesses so as to make DSSS-TDMA IC-WLAN a feasible and competitive scheme.

In addition to IEEE 802.15.4, we have another WPAN MAC/physical layer standard IEEE 802.15.1 [40], a.k.a. Bluetooth, which is mainly designed for high-data-rate, low-power and short-range communications between PC and its peripherals. Bluetooth is known to have robustness inferior to IEEE 802.11b [41].

Also, at the physical layer, *Frequency Hopping Spread Spectrum* (FHSS) [6] and DSSS bear great resemblance. That is why under many circumstances, FHSS and DSSS are interchangeable. However, FHSS is less desirable than DSSS in hardware cost and system complexity. And digital wireless FHSS systems that carries out FHSS within every bit duration (so as to achieve processing gain) are not as widely available as DSSS systems.

This paper extends the work in the previous conference version [42] mainly by comparing DSSS-CDMA with IEEE 802.15.4 and discussing the error correction coding scheme.

Finally, our goal is noticeably to maintain wireless control loop communications under channel conditions as harsh as possible, rather than to make wireless control loop communications immune to adverse channel conditions.

VI. Conclusion

The top priority for building *Industrial Control Wireless LAN* (IC-WLAN) is robustness: wireless control loops must be maintained under all adverse channel conditions. Specifically,

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/fading due to heavy obstructions. The robustness requirement makes the IEEE 802.11 WLANs (mainly designed for irregular office/home data traffics) inappropriate for IC-WLAN. In contrast, industrial control loop traffics are mostly regular sustained traffics with extremely low data rates. This feature allows DSSS's deployment of high processing gain for high robustness.

According to fine-grained physical layer simulations and Monte Carlo comparisons, we show that by deploying slowest data bit rate (largest possible processing gain) allowed by minimal sampling/actuating rate, a DSSS IC-WLAN can provide significantly higher robustness than IEEE 802.11/802.15.4 WLAN. At the MAC layer, although either CDMA or TDMA can be deployed, CDMA is more preferable than TDMA 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 better meets the needs of IC-WLAN. That is, we open a new application domain where the CDMA cellphone network paradigm would prevail again due to its unique characteristics. Though some modifications are needed, it is promising to build our proposed DSSS-CDMA IC-WLAN scheme on top of the many contemporary CDMA cellphone network architectures.

DSSS-CDMA IC-WLAN scheme opens a new problem space: many variables can be configured, such as processing gain, data rate, transmission power, number of channels per control loops and acceptable packet error rate threshold; and many objectives can be pursued, such as efficient planning algorithms, capacity, utility, and coexistence of regular-low-throughput versus irregular-high-throughput traffics. Also, the situation will be more complicated for multiple cells. We are interested in carrying out further studies in all these directions.

ACKNOWLEDGMENT

The research of this paper is supported by MURI N00014-01-0576, NSF ANI 02-21357, NSF CCR-0237884, NSF CCR-0325716, NSF CCR 02-09202 and ONR N00014-02-1-0102; and by Vodafone Fellowship (for the first author). The authors highly appreciate the advice by Prof. Venugopal Veeravalli, Prof. Bruce Hajek, Prof. Christoforos Hadjicostis, Prof. Rong Zheng, Ms. Tanya Crenshaw and anonymous reviewers. The completion of this paper is also owed a good deal to Mr. Qingbo Zhu for his assistance on using high-performance computer clusters, and Mr. Zhaoyu Zhou for improving the technical writing.

REFERENCES

[1] N. J. Ploplys, P. A. Kawka, and A. G. Alleyne, "Closed-loop control over wireless networks," *IEEE Control Systems Magazine*, vol. 24, June 2004.
[2] H. Ye and G. Walsh, "Real-time mixed-traffic wireless networks," *IEEE Trans. Ind. Electron.*, vol. 48, no. 5, 2001.
[3] H. Ye *et al.*, "Wireless local area networks in the manufacturing industry," in *Proc. American Control Conf.*, 2000, pp. 2363–2367.
[4] S. Cavalieri and D. Panno, "A novel solution to interconnect fieldbus systems using IEEE wireless LAN technology," *Comput. Standards Interfaces*, vol. 20, no. 1, pp. 9–23, 1998.
[5] S. Jiang, "Wireless communications and a priority access protocol for multiple mobile terminals in factory automation," *IEEE Trans. Robot. Automat.*, vol. 14, pp. 137–143, 1998.
[6] T. S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Prentice Hall, 2002.
[7] F. Zhang, "Investigation of electromagnetic interference of pwm motor drives in automotive electrical systems," MIT Laboratory for Electromagnetic and Electronic Systems, Tech. Rep. TR-99-004, 1999.
[8] G. Antonini, S. Cristina, *et al.*, "A prediction model for electromagnetic interferences radiated by an industrial power drive system," *IEEE Transactions on Industry Applications*, vol. 35, no. 4, 1999.
[9] D. Seto and L. Sha, "A case study on analytical analysis of the inverted pendulum real-time control system," CMU SEI, Tech. Rep. CMU/SEI-99-TR-023, 1999.
[10] E. A. Parr, *Industrial Control Handbook*, 3rd ed. Industrial Press, 1999.
[11] R. B. Kieburtz, "The step motor - the next advance in control systems," *IEEE Transactions on Automatic Control*, vol. 9, no. 1, 1964.
[12] B. Kuo, *Theory and Applications of Step Motors*. West Publishing Company, 1974.
[13] (2005) Stepper motor system basics. [Online]. Available: http://www.ams2000.com/stepping101.html
[14] (2006) Zigbee alliance. [Online]. Available: http://www.zigbee.org
[15] IEEE Std. 802.11, 1997.
[16] IEEE Std. 802.15.4, 2003.
[17] A. J. Viterbi, *CDMA: Principles of Spread Spectrum Communication*. Prentice Hall, Apr. 1995.
[18] M. K. Simon, J. K. Omura, *et al.*, *Spread Spectrum Communications Handbook, Electronic Edition*. McGraw-Hill, 2002.
[19] R. C. Dixon, *Spread Spectrum Systems with Commercial Applications*. Wiley-Interscience, Apr. 1994.
[20] S. Haykin, *Communications Systems*, 3rd ed. Wiley, 1994.
[21] Q. Wang *et al.* (2006) Technical report on building robust wireless lan for industrial control with dsss-cdma cellphone network paradigm. [Online]. Available: http://www-rtsl.cs.uiuc.edu/papers/dsss_cdma_tr_jnl.pdf
[22] A. Muqattash and M. Krunz, "Cdma-based mac protocol for wireless ad hoc networks," in *Proc. of the 4th ACM MobiHoc*, 2003, pp. 153–164.
[23] R. Price and P. E. G. Jr., "A communication technique for multipath channels," *Proceedings of the IRE*, vol. 46, pp. 555–570, 1958.
[24] (2005) Drcl j-sim. [Online]. Available: http://www.j-sim.org
[25] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*, draft ed. (to be published by) Cambridge University Press, 2004.
[26] *Cellular System Recommended Minimum Performance Standards for Full-Rate Speed Codes*, TIA/EIA/IS Std. 95, 1992.
[27] IEEE Std. 802.11b, 1999.
[28] IEEE Std. 802.11a, 1999.
[29] IEEE Std. 802.11g, 2003.
[30] A. R. S. Bahai *et al.*, *Multi-Carrier Digital Communications: Theory and Applications of OFDM*. Kluwer Academic/Plenum Publishers, 1999.
[31] L. Hanzo, W. Webb, and T. Keller, *Single- and multi-carrier quadrature amplitude modulation: principes and applications for personal communications, WLANs and broadcasting*. John Wiley & Sons, Ltd., 2000.
[32] J. Heiskala and J. Terry, *OFDM Wireless LANs: A Theoretical and Practical Guide*. Sams Publishing, 2002.
[33] V. Bharghavan *et al.*, "MACAW: A media access protocol for wireless LAN's," in *Proc. of ACM SIGCOMM*, London, UK, 1994, pp. 212–225.
[34] S. G. Wilson, *Digital Modulation and Coding*. Prentice Hall, 1996.
[35] *CDMA 2000 Series*, TIA/EIA/IS Std. 2000 Series, Release A, 2000.
[36] (2005) Umts forum. [Online]. Available: http://www.umts-forum.org
[37] (2005) Td-scdma. [Online]. Available: http://www.tdscdma-forum.org
[38] (2005) Qualcomm cdma. [Online]. Available: http://www.cdmatech.com
[39] L. Korowajczuk *et al.*, *Designing cdma2000 Systems*. Wiley, 2004.
[40] IEEE Std. 802.15.1, 2005.
[41] J. C. Haartsen and S. Zurbes, "Bluetooth voice and data performance in 802.11 ds wlan environment," Ericsson SIG pub., Tech. Rep., 1999.
[42] Qixin Wang *et al.*, "Building robust wireless lan for industrial control with dsss-cdma cellphone network paradigm," in *Proc. of the 26th IEEE RTSS*, Dec. 2005, pp. 3–14.

Qixin Wang Born in 1977, Qixin Wang received the B.E. and M.E. degrees from Dept. of Computer Sci. and Tech., Tsinghua Univ. (Beijing, China) in 1999 and 2001 respectively. He is currently pursuing the PhD degree in the Dept. of Computer Science, Univ. of Illinois at Urbana-Champaign. His research interests include real-time/embedded systems and networking, wireless technology, and their applications in industrial control, medicine and assisted living. He is a student member of IEEE and ACM.

Xue Liu Xue Liu received the BS degree in Applied Mathematics and MEng degree in Control Theory and Applications from Tsinghua Univ. in 1996 and 1999 respectively. He received his PhD degree in Computer Science from Univ. of Illinois at Urbana-Champaign in 2006. He is currently an assistant professor in the School of Computer Science at McGill Univ. His research interests include real-time and embedded computing, performance and power management of server systems, sensor networks, fault tolerance, and control. He has authored/coauthored more than 20 refereed publications in leading conferences and journals in these fields. He is a member of the IEEE.

Weiqun Chen Born in China in 1976, Weiqun Chen received the B.S. and M.S. degrees in Electrical Engineering from Huazhong Univ. of Sci. and Tech. (Wuhan, China) in 1997 and 2000 respectively. He worked in Motorola and Ali, focusing on baseband ASIC design and application for 3 years. He is currently a graduate student with Electrical and Computer Engr. and Computer Sci. Dept., Univ. of Cincinnati. His research interests include high speed and broadband signal processing for wireless communication, MIMO systems and antenna design. He is a student member of IEEE.

Lui Sha Lui Sha graduated with Ph.D. from Carnegie Mellon University in 1985. He is currently Donald B. Gillies Chair professor of Computer Science at the University of Illinois at Urbana-Champaign. He was elected Fellow of ACM in 2005 and Fellow of IEEE in 1998. His research area is dependable real-time and embedded systems.

Marco Caccamo Marco Caccamo is Assistant Professor at Dept. of Computer Science, University of Illinois, Urbana-Champaign. He received a PhD in Computer Engineering from Scuola Superiore Sant'Anna in 2002. He is recipient of NSF CAREER Award (2003); his research interests include real-time operating systems, real-time scheduling and resource management, wireless sensor networks, and quality of service control in next generation digital infrastructures.