Channel Identification: Secret Sharing using Reciprocity in Ultrawideband Channels

Robert Wilson*, *Member, IEEE*, David Tse, *Member, IEEE*, and
Robert A. Scholtz, *Life Fellow, IEEE*

Abstract

To establish a secure communications link between any two transceivers, the communicating parties require some shared secret, or key, with which to encrypt the message so that it cannot be understood by an enemy observer. Using the theory of reciprocity for antennas and electromagnetic propagation, a key distribution method is proposed that uses the ultrawideband channel pulse response between two transceivers as a source of common randomness that is not available to enemy observers in other locations. The maximum size of a key that can be shared in this way is characterized by the mutual information between the observations of two radios, and an approximation and upper bound on mutual information is found for a general multipath channel and examples given for UWB channel models. The exchange of some information between the parties is necessary to achieve these bounds, and various information sharing strategies are considered and their performance simulated. The vulnerability of such a secret sharing system to attack from a radio in a nearby location is briefly considered in an example.

This work was supported in part by the Integrated Media Systems Center, an NSF Research Engineering Research Center, and by the MURI Project under Contract DAAD19-01-1-0477.

Robert Wilson was with the Ultra-Wideband Radio Laboratory, University of Southern California, Los Angeles, CA 90089-2560 USA, he is now with Sequoia Communications, San Diego, CA 92127 (e-mail: robertwilson@ieee.org.)

David Tse is with the Department of Electrical Engineering and Computer Sciences, University of California at Berkeley, CA 94720-1770 USA (email: dtse@eecs.berkeley.edu.)

R. A. Scholtz is with the Communications Sciences Institute, Department of Electrical EngineeringSystems, University of Southern California, Los Angeles, CA 90089-2565 USA (email: scholtz@usc.edu.)

I. INTRODUCTION

When two antennas A and B with no non-linear components radiate identical signals, the outputs of the antennas due to their excitation by the signal originating at the other antenna will also be identical. This behavior, known as the reciprocity theorem, arises from the reciprocity of the radiating and receiving patterns of antennas and applies when the medium between the antennas is linear and isotropic [1][2]. When wide bandwidth waveforms are transmitted in cluttered environments, such as homes and offices, the signal observed by a receiving antenna at a remote location is the composite of multiple signals that have traveled over different paths from the transmitting antenna, each signal experiencing different shaping and attenuation, resulting in an output signal that differs significantly from the radiated signal and that changes as the locations of the transceivers is changed. In other words, the output signal contains information about the channel through which the transmitted waveform has propagated, and because of reciprocity this information is a source of common randomness that is available at both ends of the link.

The availability of common randomness to a transmitter-receiver pair can be used for cryptography: two transceivers that want to communicate secretly require some common knowledge from which to generate a key, and to achieve perfect secrecy the knowledge of an eavesdropping receiver about the key must be negligible. The large bandwidth and corresponding fine time resolution of transmitted UWB signals results in a large amount of information being available in the observed channel pulse response function. Moreover, because it is a function of the topography of the transceiver-pair and their environment, an eavesdropping receiver in a third location will not observe the same pulse response. These two facts suggest that UWB radios have a large potential for generating secret-keys from their reciprocal observations. The process of key extraction from the channel pulse response is here referred to as channel identification.

The task of generating a secret key from common information has been studied by several authors; in particular Maurer [3][4] and Ahlswede *et al* [5] discovered some fundamental bounds on the so-called secret-key rate of system models where the terminals have access to correlated random variables due to some external source (in this case the 'external source' is the channel impulse response.) When terminals A and B who wish to agree on some secret key K observe a sequence of N random variables $X^N = [X_1, \ldots, X_N]$ and $Y^N = [Y_1, \ldots, Y_N]$ respectively, terminal E from whom the key is to be kept secret observes the sequence Z^N, and A and B exchange a collection of messages denoted by C over a public channel observable by E, the secret-key rate $K(X;Y||Z)$ is the maximum rate R, such that for

every $\epsilon > 0$ and sufficiently large N, satisfying

$$P(K_{\mathrm{A}} = K_{\mathrm{B}}) > 1 - \epsilon$$
$$\frac{1}{N} I(K; C, Z^N) \leq \epsilon,$$
$$\frac{1}{N} H(K) \geq R - \epsilon,$$

and

$$H(K) \geq \log |K| - \epsilon,$$

where K_{A} and K_{B} are the specific samples of K calculated by terminals A and B respectively. If the random variables observed by terminals A, B and E are i.i.d. with marginal distributions X,Y and Z respectively, then the secret-key rate is upper bounded by[1] $K(X;Y||Z) \leq \min[I(X;Y), I(X;Y|Z)]$.

The general scheme for secret sharing described above assumes the availability of a public channel over which terminals A and B can communicate. It has been proven that if A and B do not communicate then the secret-key rate is zero [6][7], and that the bound $I(X;Y)$ (in the absence of any enemy terminal with a correlated observation) can be achieved by transmitting from A to B only, at a rate greater than or equal to the conditional entropy $H(Y|X)$ of the observation of B given A, through application of the Slepian-Wolf theorem for decoding with side-information [5]. Using the reciprocity of the propagation channel as a source of common randomness has been studied by other authors for narrowband radios. In [8] and [9] the authors propose a system where each radio transmits 2 or more unmodulated carriers at orthogonal frequencies and the phase differences between the observed carriers are used as the source of common information. In [10], a secret-key is shared between mobile, narrowband radios in fading channels, using the polarity of some samples of the envelope of the reciprocal received signals, however that analysis does not consider the presence of thermal noise.

This paper presents a more infomation theoretic and extensive study into secret-key agreement using the reciprocity of radio propagation channels than any prior work, and also presents a number of numerical results bounding and simulating the secret-key lengths possible for indoor ultrawideband channels. The paper is organized as follows. In Section II some expressions that approximate the mutual information between the observations, and therefore upper bound the secret-key rate, of radios A and B under some

[1]A tighter bound on secret-key rate is given in [4], however it does not influence the remainder of this work and is not described here for the sake of brevity.

common UWB channel models are found, and compared to empirical results. In Section III the impact of quantization of the observations is examined in terms of mutual information. In Section IV some of the possible techniques for communicating messages over the public channel to aid in secret-key agreement are described, and Section V describes the results of some simulated channel identification experiments using the various public communication methods. Section VI concludes.

II. Mutual Information over UWB multipath channels

In the introduction it was mentioned that given some public communication capability between the two transceivers the secret-key rate is upper bounded by the mutual information between the observations of each receiver. Thus a measure of obvious interest is the maximum mutual information between the observations of two ultrawideband radios in given environments, which will indicate what the maximum long-term average identifier length is for a sequence of independent channels in that environment.

In this section the mutual information between the received waveforms due to identical transmissions at each end of the link is investigated. Two approximations to mutual information are given, depending on the mean power delay profile of the channel or the total energy only, and the specific mutual information for a common ultrawideband channel model is found by Monte Carlo methods and compared to the approximations.

Let the observed waveform of radio k be represented by

$$y_k(t) = h(t) * s(t) + n_k(t) \tag{1}$$

where $h(t)$ is the channel impulse response, $s(t)$ is the pulse transmitted by the other radio, $n_k(t)$ is a Gaussian noise process with power spectral density $N_{ok}/2$ and "*" indicates convolution.

The nature of the ultrawideband channel is different to that encountered in narrowband systems and deserves some discussion. In narrowband systems, the familiar multipath propagation model assumes the existence of a large number of propagation paths with the same time of arrival but uniformly distributed phase, which results in a Rayleigh distributed amplitude gain by appeal to the central limit theorem. Due to the short duration, typically sub-nanosecond, of an ultrawideband pulse, at most a few paths contribute to the channel impulse response at a given delay (it is often assumed that every path is distinct) and the

amplitude is more dependent on the loss that occurs during propagation than on interference between arrivals [11]. The resulting probability distributions for the gains of multipath channel paths are often modeled as log-normal or Nakagami. The other effect of the short pulse width is that the number of resolvable paths in a multipath observation is much larger for ultrawideband signals than for narrower bandwidths.

The analysis of the mutual information between the observations of two radios observing the channel pulse response at opposite ends of a multipath channel will begin by considering the mutual information between the observations due to a single propagation path, and then be extended to multiple paths.

A. Single path case

In the single path case the channel is a delta function $h(t) = \alpha\delta(t)$ and after matched filtering and sampling each radio has generated an output $Y_k = \alpha\sqrt{E_s} + Z_k$. Without loss of generality let $E_s = \int_{-\infty}^{\infty} s^2(t)dt$, $\mathbb{E}[\alpha^2] = 1$ and $\mathbb{E}[Z_k^2] = N_{ok}/2$.

To make the problem tractable α or $|\alpha|$ is assumed to have a Gaussian distribution. Although the empirical distributions of measured ultrawideband channels are not closely approximated by the Gaussian distribution by common measures, it will be seen later to be reasonable for estimating mutual information. Applying the common assumption that any non-line-of-sight propagation path has equiprobable amplitude polarity results in α always being zero-mean.

At low SNR (SNR $= 2E_s/N_{ok}$) approximate α as a zero-mean Gaussian random variable, then the variables (Y_A, Y_B) have a joint Gaussian distribution given by

$$p(Y_A, Y_B) = \frac{1}{2\pi\sigma_A\sigma_B\sqrt{1-r^2}} \exp\left[-\frac{\left(\frac{Y_A^2}{\sigma_A^2} - \frac{2rY_AY_B}{\sigma_A\sigma_B} + \frac{Y_B^2}{\sigma_B^2}\right)}{2(1-r^2)}\right] \quad (2)$$

where $\sigma_k^2 = E_s + N_{ok}/2$ and $r = E_s/\sigma_A\sigma_B$. The mutual information is

$$I(Y_A; Y_B) = \frac{1}{2}\log_2\left(1 + \frac{E_s^2}{E_s(N_{oA}+N_{oB})/2 + N_{oA}N_{oB}/4}\right). \quad (3)$$

If the SNR is sufficiently large that the probability of $|\alpha|E_s + Z_k$ being less than zero is negligible then instead make the simplifying assumption that $|\alpha|$ is a Gaussian random variable with mean $\mu_{|\alpha|} < 1$ and variance $\text{Var}[|\alpha|] = \text{Var}[\alpha] - \mu_{|\alpha|}^2 = 1 - \mu_{|\alpha|}^2$. Then $(|Y_A|, |Y_B|)$ are approximately jointly Gaussian with variances $\sigma_k^2 = E_s^2(1 - \mu_{|\alpha|}^2) + N_{ok}/2$ and correlation coefficient $r = E_s^2(1 - \mu_{|\alpha|}^2)/\sigma_A\sigma_B$. The polarity of the observations contributes 1 bit to the mutual information and is assumed to be detectable without error because of the high SNR, thus the total mutual information between Y_A and Y_B is

$$
\begin{aligned}
&I(Y_A; Y_B) = \\
&1 + \frac{1}{2}\log_2\left(1 + \frac{E_s^2(1-\mu_{|\alpha|}^2)^2}{E_s(1-\mu_{|\alpha|}^2)(N_{oA}+N_{oB})/2 + N_{oA}N_{oB}/4}\right) \\
&\simeq 1 + \frac{1}{2}\log_2\left(1 + \frac{E_s(1-\mu_{|\alpha|}^2)}{(N_{oA}+N_{oB})/2}\right).
\end{aligned}
$$

The approximations are shown with the numerically calculated mutual information between observations when the path magnitude $|\alpha|E_s$ has a Nakagami-m distribution in Figure 1. The Nakagami-m distribution is commonly used to model the path gains of multipath channels and has mean and variance $\mathbb{E}(|\alpha|)^2 = \frac{\Gamma^2(m+1/2)}{m\Gamma^2(m)}$ and $\text{Var}[|\alpha|] = \left(1 - \frac{\Gamma^2(m+1/2)}{m\Gamma^2(m)}\right)$, further details can be found in [12]. If a log-normal distribution with the same mean and variance in path magnitude is substituted for the Nakagami-m distribution the mutual information shows negligible change.

B. Multipath case

To evaluate the multipath case, assume that the frequency spectrums of $s(t)$, $y_A(t)$ and $y_B(t)$ are non-zero only over a band of width W centered at frequency f_c. Then we can write

$$
s(t) = \Re\left\{\tilde{s}(t)\mathrm{e}^{j2\pi f_c t}\right\} \tag{4}
$$

$$
\begin{aligned}
y_k(t) &= s(t) * h(t) + n_k(t) \\
&= \Re\left\{\left[\int_{-\infty}^{\infty} h(\tau)\tilde{s}(t-\tau)\mathrm{e}^{-j2\pi f_c \tau}d\tau + \tilde{n}_k(t)\right]\mathrm{e}^{j2\pi f_c t}\right\} \\
&= \Re\left\{\left[\tilde{x}(t) + \tilde{n}_k(t)\right]\mathrm{e}^{j2\pi f_c t}\right\}
\end{aligned} \tag{5}
$$

where $\tilde{s}(t)$ and $\tilde{x}(t)$ are in general complex valued random processes with bandwidth extent $-W/2$ to $W/2$, $n_k(t) = \Re\left\{\tilde{n}_k(t)\mathrm{e}^{j2\pi f_c t}\right\}$ and $\Re$ indicates taking the real part. Because $\tilde{s}(t)$, $\tilde{x}(t)$ and $\tilde{n}_k(t)$ are baseband processes of limited spectral range they can be precisely reconstructed from a sequence of

samples taken at the Nyquist rate W, and

$$\tilde{x}(t) = \sum_{l=0}^{L-1} h(l/W)\tilde{s}(t - l/W)\mathrm{e}^{-j2\pi f_c l/W},$$

$$\tilde{x}(i/W) = \sum_{l=0}^{L-1} h(l/W)\tilde{s}([i-l]/W)\mathrm{e}^{-j2\pi f_c l/W}, \tag{6}$$

$$\tilde{y}_k(i/W) = \sum_{l=0}^{L-1} h(l/W)\tilde{s}([i-l]/W)\mathrm{e}^{-j2\pi f_c l/W} + \tilde{n}_k(i/W) \tag{7}$$

where $y_k(t) = \Re\left\{\tilde{y}_k(t)\mathrm{e}^{j2\pi f_c t}\right\}$. Let $\mathbf{Y}_{\mathrm{A}}^L = [\tilde{y}_{\mathrm{A}}(0), \ldots, \tilde{y}_{\mathrm{A}}((L-1)/W)]$ and $\mathbf{Y}_{\mathrm{B}}^L = [\tilde{y}_{\mathrm{B}}(0), \ldots, \tilde{y}_{\mathrm{B}}((L-1)/W)]$ represent the samples of radio A and B respectively. Because $y_k(t)$ is fully defined by the sequence $\mathbf{Y}_k^L$ and vice versa the mutual information between $y_{\mathrm{A}}(t)$ and $y_{\mathrm{B}}(t)$ is the same as that between $\mathbf{Y}_{\mathrm{A}}^L$ and $\mathbf{Y}_{\mathrm{B}}^L$.

Assume that the equivalent baseband transmitted pulse satisfies the Nyquist pulse-shaping criterion, i.e.,

$$\tilde{s}((i-l)/W) = \begin{cases} \tilde{s}(0), & \text{if } i = l \\ 0, & \text{if } i \neq l, \end{cases} \tag{8}$$

then

$$\tilde{y}_k(i/W) = h(i/W)\tilde{s}(0)\mathrm{e}^{-j2\pi f_c i/W} + \tilde{n}_k(i/W). \tag{9}$$

Note that $\tilde{n}_k(i/W)$ is a circular Gaussian random variable with power spectral density $N_o/2$, so the angle of $\tilde{s}(0)$ is arbitrary and we can assume $\tilde{s}(0)\mathrm{e}^{-j2\pi f_c i/W}$ is real. Also assume that $h(i/W)$ is a mean zero Gaussian random variable, following the low SNR approximation of the single path case, and using (3) the *power delay profile* (PDP) approximation to mutual information is

$$I(\mathbf{Y}_A^\infty, \mathbf{Y}_B^\infty) = \sum_{i=0}^{L-1} \frac{1}{2}\log_2\left(1 + \frac{E_s^2 E^2[h(i/W)^2]}{E_s E[h(i/W)^2](N_{oA}+N_{oB})/2 + N_{oA}N_{oB}/4}\right). \tag{10}$$

If the power delay profile of the channel is unknown then let

$$E[h(l/W)h(i/W)] = \begin{cases} \frac{1}{L}, & \text{if } i = l \\ 0, & \text{if } i \neq l \end{cases} \tag{11}$$

and neglect the $N_{oA}N_{oB}$ term in the argument of the log, then the concavity of the log results in the *total energy* upper bound (assuming Gaussian gains) on mutual information

$$I(\mathbf{Y}_A^L, \mathbf{Y}_B^L) \leq \frac{L}{2}\log_2\left(1 + \frac{E_s}{L(N_{oA}+N_{oB})/2}\right) \tag{12}$$

where any non-unit channel energy is implicitly incorporated into E_s. Note that neglecting the term $N_{oA}N_{oB}$ is only reasonable if $L << E_s/N_o$ and the bound is not tight for low SNR cases. Note also that the expressions for mutual information given in (10) and (12) are only valid only under the assumption of (8); the optimal transmit pulse to maximize mutual information is an open problem.

As discussed at the beginning of the section, for two radios in an environment where the channel impulse response has some fixed statistical distribution and each observation of the channel pulse response is an i.i.d. random vector, the mutual information between the observations of the radios upper bounds the long-term average identifier length for that environment. By the same argument, under the assumption of a channel impulse response consisting of a sequence of i.i.d. random variables occurring at the Nyquist rate and with a known distribution, i.e. the assumption of (11), the average identifier length due to the observation of any sample point of the channel pulse response at can be upper-bounded, and thus substituting (11) into (10) upper bounds the secret-key length possible for any such channel as L becomes large. Making the substitution and taking the limit of (10)

$$\begin{aligned} I(\mathbf{Y}_A^L, \mathbf{Y}_B^L) &= \lim_{L\to\infty} \frac{L}{2} \log_2 \left(1 + \frac{E_s^2}{LE_s(N_{oA}+N_{oB})/2 + L^2 N_{oA}N_{oB}/4} \right) \\ &= \lim_{L\to\infty} \frac{E_s^2}{LN_{oA}N_{oB}/4} \\ &= 0. \end{aligned} \tag{13}$$

Thus for a fixed amount of energy in the observed waveform the mutual information does not increase monotonically with the number of samples, instead, because the energy of each sample also decreases as the number of samples rises, there is some optimal number of samples, corresponding to an optimal signal bandwidth, for a given channel excess delay and observed signal energy. This optimal bandwidth will be explored in more detail, along with a parallel characteristic of the channel coherence time, later in the paper.

A Monte Carlo computer experiment was performed to calculate the mutual information between the observations of two virtual radios and compare it to the approximation of (10) and bound of (12). Recall that these two expressions characterize the largest achievable long-term average secret-key rate. The channel models in this case are the CM 1 and CM 3 models of [13], simulating a LOS 0-4m channel and NLOS 4-10m channel respectively, and each channel instance is normalized to unit energy. The empirical joint and marginal probability distributions were determined for each sample and samples were taken at 0.2ns intervals, simulating the observation due to a 5GHz bandwidth transmitted pulse satisfying (8). The

duration, and equivalently number of samples, of each channel was set such that the mutual information as calculated by (12) no longer significantly increased, resulting in excess delays of 15ns and 42ns.

Note that for the calculations in (10) and (12) and for the purposes of calculating the empirical mutual information in the Monte Carlo simulation the samples of a given channel impulse response are assumed to be independent, that is, the mutual information between the respective time-samples of the observations of each radio is empirically calculated and the total mutual information calculated as the sum of these. This assumption which is not true for the present channel models and is unlikely to hold in practice, and thus the real mutual information will be lower. This assumption also contributes to the close fit between the simulation results and values predicted by (10).

Results are shown in Figure 2 for the case when the radios do not have a common time reference. If it is assumed that the radios know the theoretical propagation time of a direct path between them then for the NLOS channel model CM 3 some additional bits of mutual information exist due to the actual time of arrival being a random variable, and the gains at signal-to-noise ratios of 25 and 30 dB are approximately 6 and 19 bits respectively.

C. UWB link budget, mobility and bandwidth

To put the upper bounds on key length for given signal-to-noise ratios in context, and describe some of the trade-offs in channel identification with respect to bandwidth and mobility, a nominal ultrawideband link budget will be examined. The transmitted power of a UWB radio is regulated in the United States by part 15 of the Federal Communications Commission's (FCC) rules [14]. Given these limits, the highest average power that can be radiated over the 3.1 - 10.6 GHz band is -2.55 dBm. The power observed by the receiving radio is equal to the EIRP, minus propagation loss, plus the receiving antenna gain. The propagation loss between two radios in a cluttered (e.g. indoor) environment is usually modeled by

$$PL(d)(\text{dB}) = PL(d_{ref}) + 10n \log_{10}\left(\frac{d}{d_{ref}}\right) + X \tag{14}$$

where $PL(d_{ref})$ is the propagation loss at some reference distance, n is the loss exponent, and X is the shadowing factor. For ultrawideband propagation various experiments reported in the literature have found that suitable exponents are near 1.8 and 3.75 for line of sight and non line of sight propagation respectively [15][16], where the loss at the reference distance can be well approximated by the free-space loss at the center frequency[16]. The result after subtracting propagation loss from transmitted power is the total available power over the entire channel response.

For the sake of the nominal link budget calculated here shadowing is neglected; published estimates of the standard deviation of shadowing are in the range of 1 to 4 dB [17][16]. A receiver antenna gain of 3dB is assumed. The receiver noise power spectral density $N_o/2$ is assumed to be -177 dBm and the receiver noise figure to be 10 dB.

The observed energy is the integration of the signal power over the observation interval, thus performance is not just a function of power but also time. The following table shows the integration time required to achieve SNR of 30 dB for transmitter to receiver distances of 3, 10, 30 and 50 meters, for both LOS and NLOS propagation, assuming a transmitted pulse of average power -7 dBm, and the loss exponents and noise parameters described above. A 10 dB change in SNR corresponds to a factor of 10 change in integration time.

The receiver can only improve its SNR by integrating over a number of observed pulses for as long as the channel remains constant, a period of time approximately given by the coherence time of the channel and dependent on the physical environment and the relative rate of movement of the radios. If the rate of change of the channel impulse response is high and the radios can only achieve relatively low levels of averaging and signal-to-noise ratio, this does not necessarily lead to the failure of channel identification as a method for generating secret information. Although the radios may only be able to generate a few bits of common information for a given channel, they can do so for each channel they encounter and thus accumulate independent bits as they communicate via successive independent channels.

To investigate the trade-off between increased SNR and the rate of change of the channel impulse response consider the expression for the mutual information between observations over a multipath channel in (10). There will be some value of E_s (equivalent to an SNR $2E_s/N_o$) at which the increase in mutual information due to increasing the SNR will be less than the increase from observing more independent channels at the same SNR. Each SNR in turn corresponds to some optimal channel coherence time that is a function of the observed power and the propagation time. The numerically solved mutual information for channel models CM 1 (LOS) and CM 3 (NLOS) over propagation distances 10, 30 and 50 meters are is plotted against coherence time in Figure 3, where the total amount of time allocated to key agreement is 1 second and the signal bandwidth is 5GHz. The impact of bandwidth on mutual information is discussed in the sequel.

The optimal coherence time increases with both distance and channel blockages due to lower observed power, and also increases with distance due to the longer propagation time.

The propagation channel in a residential environment, over the band 2-8 GHz, was found to have spatial correlation lengths ranging from 2 to 6 inches for both LOS and NLOS measurements in one published experiment [18]. Consider a block fading model, where the channel is assumed to be constant over each consecutive 6 inch distance and independent between successive 6 inch intervals. Terminals traveling at a fast pedestrian speed of 7 m/s would experience a coherence time of 21.8 ms; comparing this value to the curves of Figure 3 shows that this coherence time is longer than the optimal time for all demonstrated cases, thus, for these cases and for terminals moving in the pedestrian range, faster movement will generally lead to higher mutual information and corresponding potential secret-key rate.

In the previous section it was noted that (11) and (10) suggest an optimal bandwidth exists for a given signal energy and channel excess delay. Assume that the channel impulse response has a finite duration equal to τ and that the number of resolvable paths is equal to $L = \tau \cdot W$ where W is the signal bandwidth. Then substituting (11) into (10) and assuming typical excess delays of 5, 15 and 30 ns [13], the value of W that maximizes mutual information is plotted against SNR in Figure 4. The FCC has defined the minimum bandwidth for ultrawideband signals as 500MHZ [14], so the optimal bandwidth for secret-key agreement meets this definition of UWB signals for SNR's greater than approximately 4, 7, and 12 dB for channels with delay spreads of 5, 15 and 30 ns respectively.

III. Secret sharing with a communication rate constraint

It was noted in the introduction that the upper bound on shared secret information is equal to the mutual information $I(X;Y)$ bits in the case where terminal A can transmit information to terminal B over a public channel at a rate greater than or equal to $H(Y|X)$ bits, the conditional entropy of the observation of B given the observation of A. In practice, the observations of terminals A and B are continuous and the conditional entropy is infinite, thus with a rate constraint on the public discussion channel, $I(X;Y)$ bits of common randomness may not be achievable. The optimal scheme for secret sharing with a rate constraint on the public discussion channel has been studied in [19]. In this section a suboptimal scheme where the rate of communication is constrained by quantizing the observations of both terminals is considered and the effect of quantization technique examined.

By the data processing inequality quantization always reduces the available secret common information, and moreover, coarser quantization typically results in lower mutual information. But while the overall capacity of the system in terms of channel identifier length is dictated by the mutual information between

the observations, the minimum required public communication rate to achieve that capacity is determined by the conditional entropy [5], and there is a trade-off of diminishing returns between maximizing mutual information and minimizing conditional entropy. To see this consider the limits of mutual information and conditional entropy as the quantization bin size tends to zero [20]

$$\lim_{\Delta \to 0} I(Y_1^{\Delta}, Y_2^{\Delta}) = I(y_1, y_2) \tag{15}$$

$$\lim_{\Delta \to 0} H(Y_1^{\Delta} | Y_2^{\Delta}) = h(y_1|y_2) - log_2(\Delta) \tag{16}$$

where $Y^{\Delta} = \Psi_i$ if $i\Delta \leq y < (i+1)\Delta$ and $h(y_1|h_2)$ is the differential conditional entropy[20]. Thus, as the quantizer becomes more precise the mutual information approaches a constant while the conditional entropy increases linearly with the number of bits. Beyond a certain quantizer resolution each new bit of information only results in another bit of public communication transmitted between terminals, resulting in an insignificant possible gain in secret information.

Optimizing the quantizer requires choosing the quantization regions in such a way that mutual information is maximized subject to some conditional entropy constraint. The problem can be solved generally for known probability distributions by numerical integration, however the distributions involved are often not known, and an empirical quantizer design that can self-organize given some training data will often be preferable. In the literature an algorithm for empirically designing a quantizer to maximize mutual information has been proposed in [21]. Another algorithm based on a gradient descent technique was also considered, which had slightly better performance. Both algorithms demonstrate only a small improvement over the best uniform quantizer (the optimization in the uniform case being over bin size,) as demonstrated in Table II for a Gaussian source distribution. The results for a log-normal source distribution were similar. Neither algorithm constrains conditional entropy, but conditional entropy could be incorporated into either algorithm through the use of a Lagrangian term. Note that both algorithms demonstrate increasing improvement over uniform quantization with increasing SNR.

The discussion thus far has been limited to scalar quantization, but the more general problem is to find a vector quantizer that preserves the mutual information of some input sequence, either the entire sequence of observations or some subset thereof, and this problem is not addressed here. For the purposes of the simulations described below the observed data was passed through an LMS prediction filter and the quasi-Gaussian prediction error was decorrelated using a whitening filter based on training data, then the approximately i.i.d sequence was quantized using a uniform scalar quantizer. Under this system the mutual information between individual samples is inversely proportional to the sampling rate, thus sampling rate

and quantizer resolution can be traded off.

IV. Public Feedback Methods

In the introduction it was mentioned that if terminals A and B cannot exchange messages about their observations then the achievable secret key rate is zero [6][7]. The problem can be considered as an equivalent to the problem of decoding with side-information, where terminal B wants to determine the value of terminal A's observation when it has some correlated observation available to it. In [5] it is proven through application of the Slepian-Wolf theorem [20] that $I(X;Y)$ bits of shared secret information can be formed when terminal A sends information to terminal B at rate greater than or equal to the conditional entropy of the observation of A given the observation of B, $H(X|Y)$.

Practical methods for encoding (at terminal A) decoding (at terminal B) in the presence of side-information have been proposed in [22], and the details of the techniques can be found therein. The techniques draw on the theory of forward error correction (FEC), where the possible observations of terminal A are grouped into cosets so that the minimum distance between elements of a coset is maximized. Terminal A finds the coset to which its observation belongs and communicates the index of the coset to terminal B. Because the observation of terminal B should in some sense be close to that of terminal A, then as long as the number of cosets, and thus the minimum distance between elements of the coset, is large enough, terminal B can accurately determine what terminal A observed as that element of the coset closest to its own observation. Any enemy terminal monitoring the public communication channel can learn the coset of the observation, but nothing about which element of the coset was observed, thus the maximum shared secret information is equal to the entropy within the cosets.

The specific methods of coset assignment considered here are: per sample, block-coded and trellis-coded. In the per sample case each quantization bin is labeled in ascending order of magnitude with a N bit identifier q_n, i.e., call the bin with smallest expected value $0\ldots00$, the next bin $0\ldots01$ and so on. The set of all bin identifiers are partitioned into cosets according to their $N-K$ least significant bits (LSBs), and terminal A transmits to terminal B the $N-K$ bits identifying the coset (LSBs) of its quantized observation. Terminal B then uses its observation to choose among the quantization values in the given coset, thus K bits of common information are created.

For block-coded communication the cosets correspond exactly to the cosets of the block-code. Terminal A 'decodes' its observation, finds the nearest codeword of the code, and sends a message to terminal B

indicating the coset of its observation. If terminal B then chooses the element of that coset closest to its own observation, and the index of the coset element is the channel identifier. Both radios will calculate the same identifier, as long as the number of differences between the observations is fewer than the number of errors correctable by the code. An (n, k) block code provides k secret bits per n observation bits and requires the communication of $n - k$ bits from one transceiver to the other.

Typically, block-code decoding algorithms are based on Hamming distance, while the distance between two observations in this case is better measured by Euclidian distance. Thus block-code based algorithms are going to suffer some loss due to the approximation of Euclidian distance by Hamming distance.

Trellis-coded communication methods are analogous to convolutional-codes when Hamming distance is used as the metric, or trellis-coded modulation when Euclidian distance is used. In either case soft-decoding can be used at terminal B. Consider a rate K/N trellis, where at each trellis transition N bits of the observation will be used, $N - K$ bits will be sent over the public channel, and K bits of secret information will be created. In general $N = B \cdot M$ where B is the resolution of the quantizer and M is some number of samples, and trellis-coded communication is analogous to detecting trellis-coded modulated (TCM) signals on a B^M-ary constellation in M dimensions. For example, $M = 1$ is analogous to B-PAM and $M = 2$ is analogous to B^2-QAM. If a Hamming distance metric is used then trellis-coded communication is analogous to the decoding of a convolutional code with codewords of length N; in this work Hamming distance is only used when $B = 1$. The best labeling schemes for TCM, or convolutional coding as appropriate, are also the best for the present application. Given some scheme, there are 2^{N-K} alternative ways to label the trellis which have the same distance properties, one of which will always feature the current observation as the label of a transition out of the current state. Thus the alternative labels form the cosets of the transitions, and terminal A transmits the index of the labeling scheme that matches its own observation for each transition to terminal B, which then uses those labels to decode its own observation.

V. Simulation Results

Using some of the techniques for coset calculation described in the previous sections, a number of computer simulations have been performed to determine the feasible lengths and success rates (of agreement between radios) of a channel identifier, for different UWB indoor channels. In all simulations it was assumed that no errors were made in communicating over the public channel. Before presenting

the results the simulation environment is described, in particular those aspects of the processing that are common to all simulations, such as pre-digitization processing, sampling, and quantization. A schematic of the channel ID system is shown in Figure 5

The transmitted pulse is a raised cosine pulse with 4GHZ bandwidth and 7GHz center frequency. The channel model is the proposed 802.15.3a UWB channel model [13] and simulations results are presented for parameter sets 1 and 3, corresponding to 0-4m line-of-sight and 4-10m non-line-of-sight channels respectively.

The performance of each method of communication over the public channel is presented in terms of the identifier length and the probability of error, that is, the probability that the radios fail to agree on a channel identifier, due to differences in one or more bits. Those statistics were calculated by Monte Carlo simulation over 10000 sample channels, thus the accuracy of the probability of error is limited to approximately three decimal places (10^{-3}); absent data on the probability of error curves indicates no error occurred.

A. Pre-digitization processing

Rather than correlating the observed channel pulse response directly with the source pulse, the envelope of the observation first taken (by I-Q detection) and then correlated with the source envelope, sampled and quantized for the calculation of the channel identifier. Using the envelope of the observation dramatically reduces the sensitivity of the system to timing error, and, although perfect synchronization between the radios was assumed here, use of the signal envelope was considered more realistic as a model of a real channel identification system. The trade-off in using the signal envelope is the loss of sensitivity to timing translates into a loss of variability in the channel identifier, i.e., a lowering of the entropy, compared to what could be achieved with the original observation.

Although the virtual radios for this simulation are identical, in practice the gains and filters applied by any two radios will be different due to random variability in real components. To some extent such variability can be controlled by the design, calibration and testing of the units, but the channel identification process should also be robust to some variation. To this end the envelope samples are normalized relative to the magnitude of the largest sample before quantization.

B. Digitization and Whitening

Nearby samples of the envelope tend to be correlated, thus some method of decorrelating the samples is desirable to reduce the size of the quantizer required and to reduce the number of bits that must be sent over the public channel. It is also critical to ensuring that the entropy in the resulting identifier can be accurately measured. One method for decorrelating is to predict the value of the sample based on prior samples and to quantize the difference between the observation and its prediction.

The predictive quantizer used a three tap LMS algorithm to predict the next observation value. Under the assumption that the prediction errors are jointly Gaussian, data whitening is performed on the resulting sequence of errors to produce a set of independent data, which are then quantized. The whitening matrix was calculated using a set of training data.

The sampling and whitening process is performed at 3, 5 or 7 times the Nyquist rate.

C. Per sample coset assignment

The easiest pubic communication method to implement quantizes each sample using N bits and sends $N - K$ bits per sample to indicate the coset, as described in Section IV. In this example each data point was quantized using 3 bits and 2 bits were communicated from one transceiver to the other, identifying one of 4 cosets and resulting in 1 secret bit per sample.

Figure 6 plots the probability of disagreement (probability of error) between the identifiers formed at each radio for a range of SNRs using the CM1 LOS 0-4m channel model [13], sampled at 3 times the Nyquist rate. To determine the effective identifier length the empirical entropy of the secret bit due to each sample is calculated and the entropies are summed over the sequence of observation samples, assuming that the secret bit determined by different samples are independent. The effective number of bits per sample agrees well with the theoretical number of bits (K), which is important for later examples where the identifier is not calculated on a sample-by-sample basis and the empirical entropy will not be accurately calculable. Moreover, the sums of the entropies of pairs of adjacent secret bits agrees well with the sum of the individual entropies, which supports the assumption of independence.

D. Public communication using Reed-Muller codes

The block code mechanism uses a a 1-bit differential quantizer in combination with a $(2^m, m+1, 2^{m-1})$ Reed-Muller code, denoted by R$(1, m)$. In this example m equals 3, thus 4 bits are sent from radio A to radio B per 8 bit word, leaving 4 bits of secret information.

Performance using 1-bit quantization and a Reed-Muller code for public communication is compared to 3-bit quantization and per sample in Figure 7 for rate 3 sampling. The graph is on a linear scale to clarify the differences at low SNR. The curves for per sample coset assignment where information about the observation is sent over the public channel at rate 1/3, while for the Reed-Muller case information is sent at rate 1/2. Note that even at a lower rate of communication, better performance is achieved at high SNR using 3-bit quantization due to the additional available information per sample. However, at low SNR 1-bit quantization with block-coded rate 1/2 communication performs better because not enough additional information is available in 3-bit quantized data to compensate for the lower rate.

E. Trellis coded pubic communication

The final public communication technique implemented used trellis coding techniques and Viterbi decoding on a trellis to calculate the channel identifier. As mentioned in Section IV trellis coded communication can be used with either a Hamming or Euclidian distance metric.

Figure 8 demonstrates how a longer code can be used to trade of the number of secret bits for probability of error in SNR limited scenarios. Probability of error versus theoretical identifier length is shown at 25dB SNR for rate 1/2, 1/3, 1/4, 1/7 and 1/16 codes, using channel model CM 1. The rate 1/2, 1/3 and 1/4 codes are the constraint length 3 maximal free distance codes [23], and the rate 1/7 and rate 1/16 codes used are respectively constraint length 7 and 11 maximal free distance codes given in [24]. Note that increasing the rate of communication loses its effectiveness as the identifier length increases, as more low SNR bits from the tail of the observation are used.

Figure 9 shows the results when public communication is sent using a trellis for which each transition corresponds to one of the 64 possible values of successive pairs of 3-bit quantized samples, and the code rate is 1/6, i.e., 5 bits of are sent for every bit of shared secret information. The channel model is CM 1. The process of calculating the bits sent over the public channel in this case is analogous to demodulating 64-QAM rate 1/6 trellis code modulated signal using the Viterbi algorithm. The trellis was chosen based

on the Ungerboeck criteria [25].

In Figure 10 the channel identifier lengths achieved with 90% reliability over CM 1 are compared to the upper bounds of Section II-B for some public communication techniques described above. For the best performing methods there is about 10 - 12 dB shortfall from the mutual information bound. The curves that are only plotted to 40dB never reached 10% error probability for the simulations that were performed.

In Figure 11 the channel identifier lengths achieved with 90% reliability over CM 3 are compared to the upper bound. The required SNR for a given identifier length is approximately 10 dB from the bound.

F. Experiments with measured data

In a final experiment 5 pairs of pulse responses were measured in each direction over some line-of-sight and non-line-of-sight channels and some channel identifer bits extracted, the location of the antennas for channels A through E are shown on the floorplan of Figure 12.

The transmitted pulse is a Gaussian monocycle with 10dB bandwidth of about 2GHz. The data were received and stored using a digital sampling oscilloscope and the measurements at each end were taken consecutively by switching the transmit and receive cables. The way in which the measurements were taken means that the observations are not due to reciprocal pulse propagation in precisely the same environment, as people and cables had been moved between observations. Nonetheless the observations showed good agreement in different propagation directions.

Identifiers were calculated for all 5 channels using trellis-coded communication with 3-bit quantization and 1 or 2 bits transmitted. Without access to training data the whitening step of the method used above cannot be implemented, thus to minimize correlation between samples a low sample rate of 500MHz was used. To approximately remove the mean value the envelope samples of all channels were used to find minimum mean square error exponential curve that approximates the power delay profile, and for each channel the difference between the envelope samples and approximate profile were taken. Finally, the difference between adjacent arrivals was taken.

For each channel the number of identifier bits successfully agreed upon are listed in Table III for various degrees of timing error; note that the maximum identifier lengths for this example are 56 and 28 bits for 1 and 2 bits of public communication respectively and any random sequence of bits would be expected

to agree with the identifer 50% of the time. For a practical system to achieve the identifier lengths given in Table III each radio would have to know which of its bits were the same as those calculated by the other radio.

As would be expected, timing synchronization error reduces the possible identifier length. However, for almost all channels a few bits of shared secret information can be created even with timing error on the order of a pulse width.

Because channels A and B have one node in common the outer node of each channel can be treated as an eavesdropper on the radios of the other channel, and its ability to guess the identifier of the other channel tested. Assuming that the eavesdropping radio can observe the publicly transmitted information perfectly, the eavesdropper on channel A trying to determine the channel identifier of radios on channel B correctly determined 29 and 19 bits (52% and 68%) of the identifier for 1 and 2 transmitted bits respectively, and for the reverse situation the eavesdropper on channel B determined 25 and 14 bits (60% and 50%.) In the ideal situation the eavesdropping radio should calculate 50% of the identifier on average, but without knowing which bits are correct and which are not.

VI. Conclusions

A method called channel identification has been proposed for generating secret keys for the encryption and decryption of data, using the reciprocity and rich multipath of the ultrawideband wireless propagation channel.

Approximations for the mutual information between observations over typical indoor, ultrawideband, propagation channels have been derived, which upper bound the average secret key length in bits. The bounds show that at 30dB SNR keys of up to 95 and 150 bits are theoretically achievable over a 0 - 4 m LOS and 4 - 10 m NLOS channel respectively, and moreover that even for a NLOS channel with transmitter-receiver separation of 50m SNR of 30dB can be achieved by integration for time on the order of 10ms.

It has been shown that mobile terminals can sometimes form longer secret keys than stationary ones, and the optimal coherence times for some UWB channels have been calculated based on the bounds, finding that for a simplified model the achievable secret key length typically increases with speed up to at least 7 m/s when the transmitted signal bandwidths are 5GHz. The ability of mobile radios to synchronize

their observations is an important factor that merits further investigation, although a limited study here has shown some resistance to synchronization error. It has also been shown that the maximum secret-key rate does not increase monotonically with bandwidth, and the optimal signalling bandwidths to maximize potential secret key rate has been given as a function of SNR for some typical ultrawideband channel excess delays.

The effect of quantization of the observations was examined, and it was found that optimizing the quantizater resulted in only a small improvement over uniform quantization. Expansion of the general theory of maximizing mutual information under some conditional entropy constraint is a topic of planned future research.

A number of channel identification simulations have been performed using 1- and 3-bit quantization and different public communication methods. The best performing systems achieved secret key lengths at SNRs approximately 10dB from the bound. Finally, measurement of some ultrawideband pulses in a multipath environment demonstrated the validity of the theory of reciprocity, and showed that two radios using the proposed channel identification technique can form a secret key that a third radio in a different location cannot estimate well.

In addition to the needed investigation on synchronization and rate-constrained communication already mentioned, further study is required into the correlation between channel impulse responses as a function of distance, for different environments, and for different signal bandwidths and frequencies, as this information is critical in understanding how secure the system is against enemy terminals trying to determine the identifier. The potential ability of enemy terminals to break the system is an important area in need of investigation, as well as techniques to counter-act such attacks.

REFERENCES

[1] C. A. Balanis, *Antenna Theory: Analysis and Design*, 2nd ed. New York: John Wiley & Sons, 1997.

[2] G. S. Smith, "A direct derivation of a single-antenna reciprocity relation for the time-domain," *Trans. on Antennas and Propagation*, vol. 52, pp. 1568–1577, Jun. 2004.

[3] U. M. Maurer, "Secret key agreement by public discussion from common information," *Trans. on Information Theory*, pp. 733–742, 1993.

[4] ——, "Unconditionally secure key agreement and the intrinsic conditional information," *Trans. on Information Theory*, pp. 499–514, 1999.

[5] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography - part i: secret sharing," *Trans. on Information Theory*, pp. 1121–1132, July 1993.

[6] P. Gács and J. Korner, "Common information is far less than mutual information," *Problems of Control and Information Theory*, pp. 149 – 162, 1973.

[7] N. Vereshchagin, "A new proof Ahlswede - Gács - Korner theorem on common information," Tech. Rep., September 2002, `http://lpcs.math.msu.su/~ver/papers/gka.ps`.

[8] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, "Cryptographic key agreement for mobile radio," *Digital Signal Processing*, vol. 6, pp. 207–212, Oct. 1996.

[9] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *Trans. on Communications*, vol. 43, pp. 3–6, Jan. 1995.

[10] M. A. Tope and J. C. McEachen, "Unconditionally secure communications over fading channels," in *Proc. MILCOM*. IEEE, 2001, pp. 54–58.

[11] A. F. Molisch, J. R. Foerster, and M. Pendergrass, "Channel models for ultrawideband personal area networks," *Wireless Communications*, pp. 14–21, Dec. 2003.

[12] J. G. Proakis, *Digital Communications*, 4th ed. New York, NY: McGraw-Hill, 2001.

[13] J. R. Foerster, "Channel modeling sub-committee report (final)," IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs), Tech. Rep. P802.15-02/368r5-SG3a, December 2002, http://grouper.ieee.org/groups/802/15/pub/2002/Nov02/02490r0P802-15_SG3a-Channel-Modeling-Subcommittee-Report-Final.zip.

[14] Federal Communications Commission, "Revision of part 15 of the commission's rules regarding ultra-wideband transmission systems: First report and order," April 2002, eT-Docket 98-153.

[15] R. J.-M. Cramer, "An evaluation of ultra-wideband propagation channels," Ph.D. dissertation, University of Southern California, Los Angeles, California, 2000.

[16] W. Ciccognani, A. Durantini, and D. Cassioli, "Time domain propagation measurements of the uwb indoor channel using pn-sequence in the fcc-compliant band 3.6-6ghz," *Trans. on Antennas and Propagation*, vol. 53, pp. 1542–1539, Apr. 2005.

[17] D. Cassioli, M. Z. Win, and A. F. Molisch, "The ultra-wide bandwidth indoor channel: from statistical model to simulations," *J. Selected Areas of Communications*, vol. 20, pp. 1247–1257, Aug. 2002.

[18] C. Prettie, D. Cheung, L. Rusch, and M. Ho, "Spatial correlation of UWB signals in a home environment," in *Proc. Ultra-Wideband Systems and Technology*. IEEE, 2002, pp. 65–69.

[19] I. Csiszar and P. Narayan, "Common randomness and secret key generation with a helper," *Trans. on Information Theory*, pp. 344–366, 2000.

[20] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: John Wiley & Sons, 1991.

[21] L. Vasudevan, A. Ortega, and U. Mitra, "Jointly optimized quantization and time delay estimation for sensor networks," in *International Symposium on Control, Communications and Signal Processing*. IEEE, 2004, pp. 203–208.

[22] S. S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): Design and construction," *Trans. on Information Theory*, pp. 626–643, March 2003.

[23] S. Benedetto, E. Biglieri, and V. Castellani, *Digital Transmission Theory*. New Jersey: Prentice-Hall, 1987.

[24] P. Frenger, P. Orten, and T. Ottosson, "Code-spread CDMA using maximum free distance low-rate convolutional codes," *Trans. on Information Theory*, pp. 135–144, 2000.

[25] G. Ungerboeck, "Channel coding with multilevel/phase signals," *Trans. on Information Theory*, pp. 55–67, January 1982.

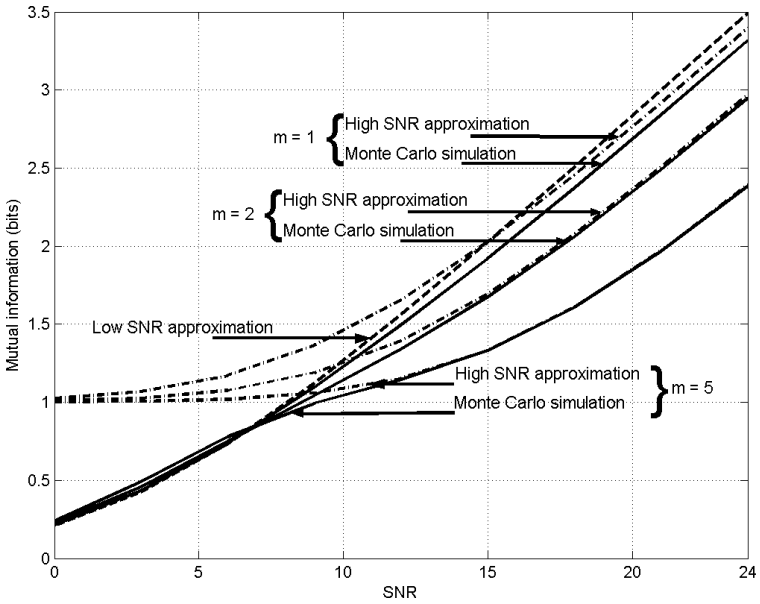

Fig. 1. True mutual information between a path with Nakagami-m (m = 1,2,5) magnitude distribution and its observation in additive Gaussian noise, and approximations that assume Gaussian path magnitudes.

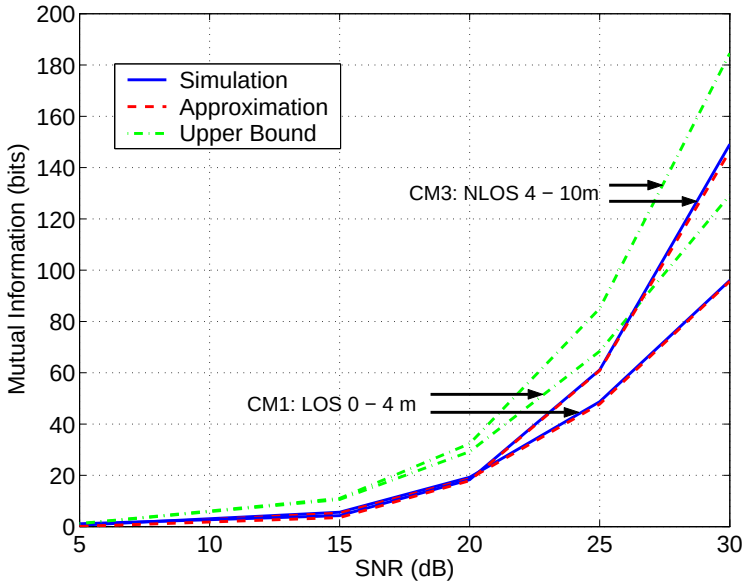

Fig. 2. Numerically evaluated mutual information compared to the PDP approximation and total energy bound for channels CM1 and CM3 when the radios have no common time reference and pulse bandwidth is 5GHz.

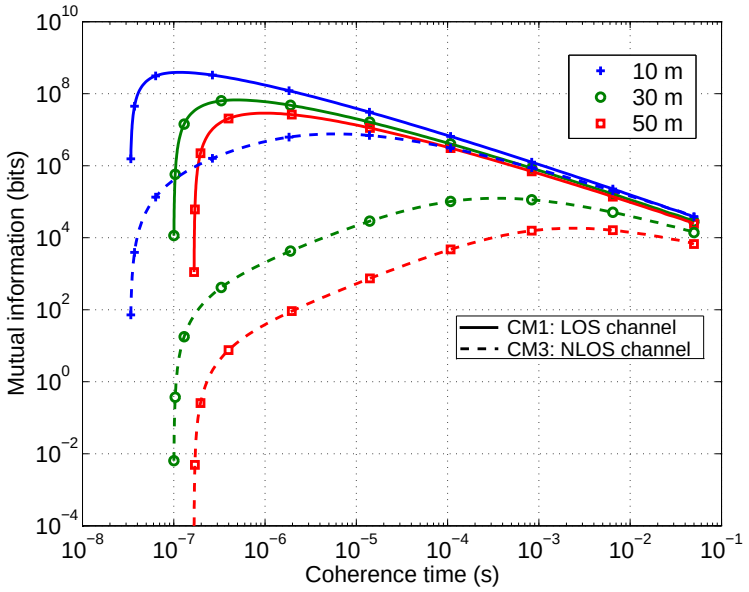

Fig. 3. Mutual information for different channel coherence times.

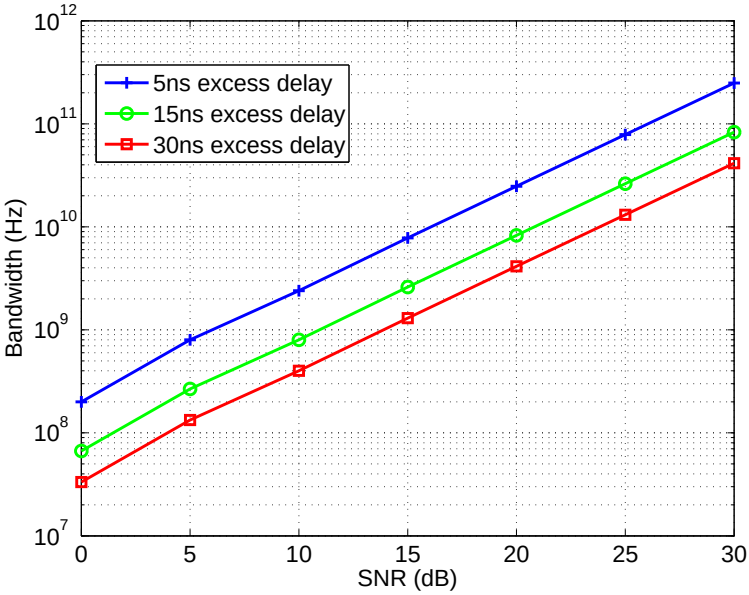

Fig. 4. Signal bandwidth that maximizes mutual information as a function of signal to noise ratio.

TABLE I

EXAMPLE OF REQUIRED INTEGRATION TIMES TO ACHIEVE 30DB SNR

Distance (m)	LOS time (s)	NLOS time (s)
3	32×10^{-9}	271×10^{-9}
10	278×10^{-9}	24.80×10^{-6}
30	2.01×10^{-6}	1.53×10^{-3}
50	5.04×10^{-6}	10.46×10^{-3}

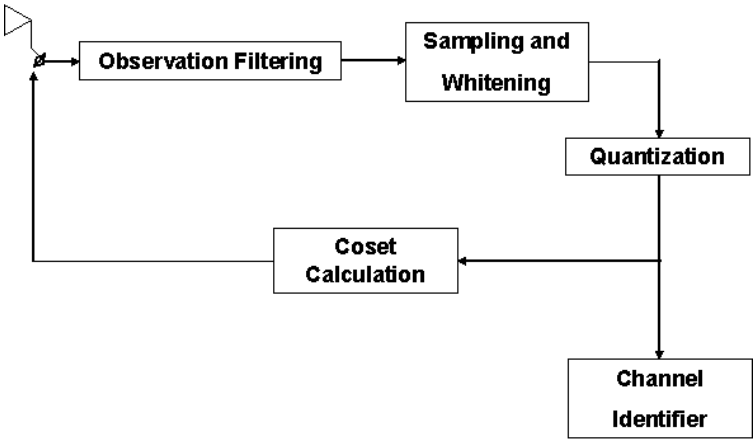

Fig. 5. Schematic diagram of a channel ID sub-system

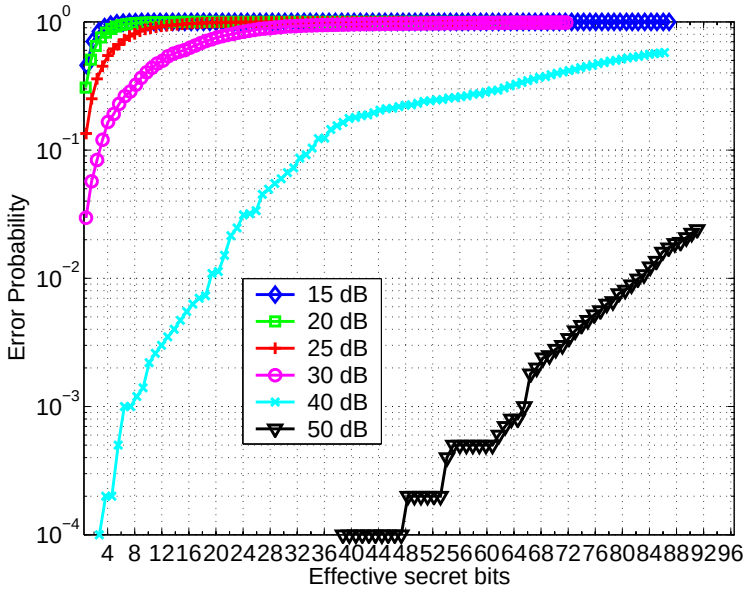

Fig. 6. Cumulative probability of error versus conditional entropy of identifiers when each radio quantizes the samples independently using a 3-bit quantizer, radio A sends 2 bits to radio B over the public channel, and the channel model is CM 1.

TABLE II

MUTUAL INFORMATION ACHIEVED BY QUANTIZER OPTIMIZATION ALGORITHMS WHEN THE SOURCE DISTRIBUTION IS GAUSSIAN.

SNR	Bits	Uniform	Gradient Alg.	Vasudevan Alg.
10	1	0.423	0.423	0.424
10	4	1.200	1.200	1.200
20	3	2.004	2.001	2.004
20	4	2.444	2.453	2.449
20	5	2.675	2.685	2.676
50	4	3.823	3.838	3.838
50	5	4.678	4.689	4.701

TABLE III

LENGTH IN BITS OF AGREEING IDENTIFIER BITS FOR VARIOUS TIMING SYNCHRONIZATION ERRORS.

Timing error	0		50 ps		500 ps		1 ns	
Feedback bits	1	2	1	2	1	2	1	2
Channel A	56	28	56	28	37	28	25	18
Channel B	42	28	44	28	36	21	22	12
Channel C	41	20	38	20	37	16	21	12
Channel D	30	21	30	21	26	25	24	20
Channel E	33	27	43	27	36	13	31	18

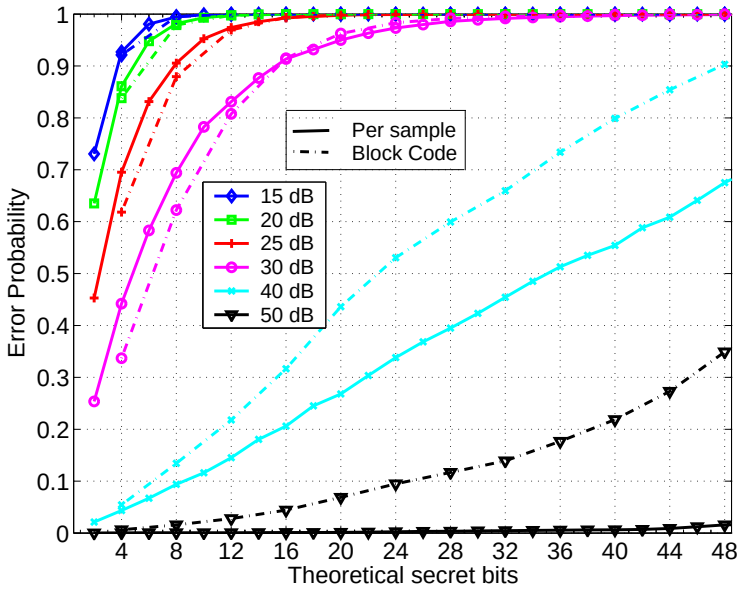

Fig. 7. Probability of error per shared secret bit over CM1 when information is sent per sample at rate 1/3 after 3-bit quantization or via Reed-Muller code at rate 1/2 after 1-bit quantization.

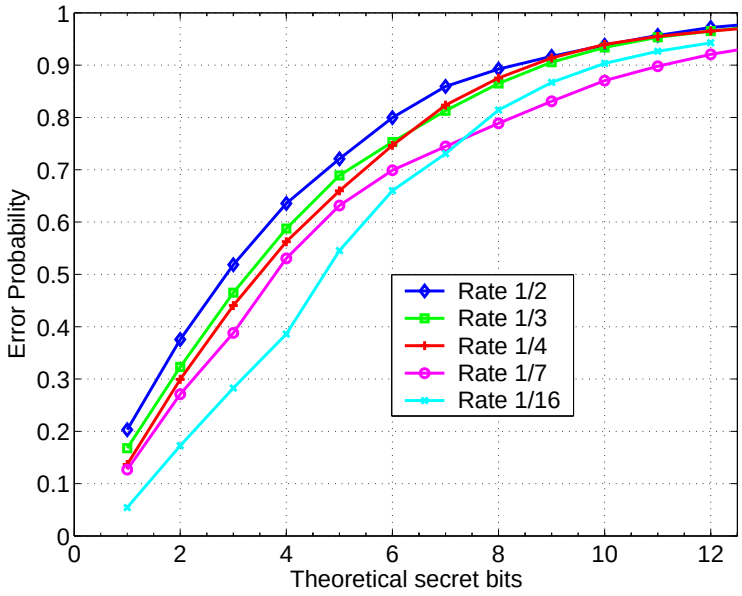

Fig. 8. Cumulative probability of error for identifiers at 25 dB SNR where convolutional codes of different rates are used to communicate over the public channel. The channel model is CM 1.

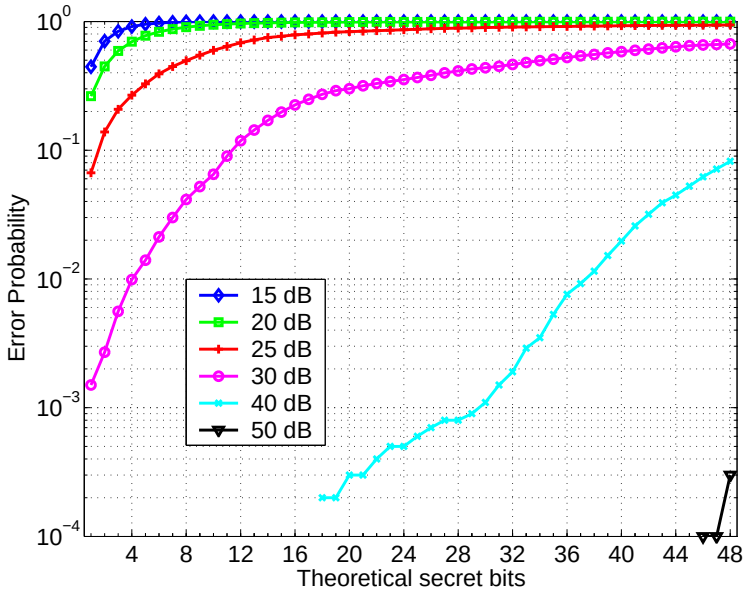

Fig. 9. Cumulative probability of error between identifiers formed over CM 1 from 96 consecutive 3-bit quantized samples calculated with public information sent using a rate 1/6 constraint length 4 trellis with a 2-dimensional mapping.

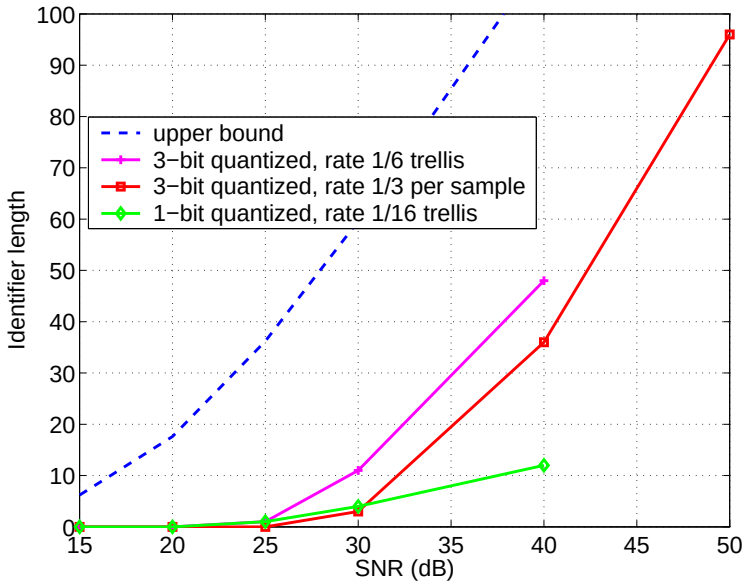

Fig. 10. Achieved identifier lengths over CM 1 for 1- and 3-bit quantization and per sample and convolutional code based public communication methods, compared to the upper bound.

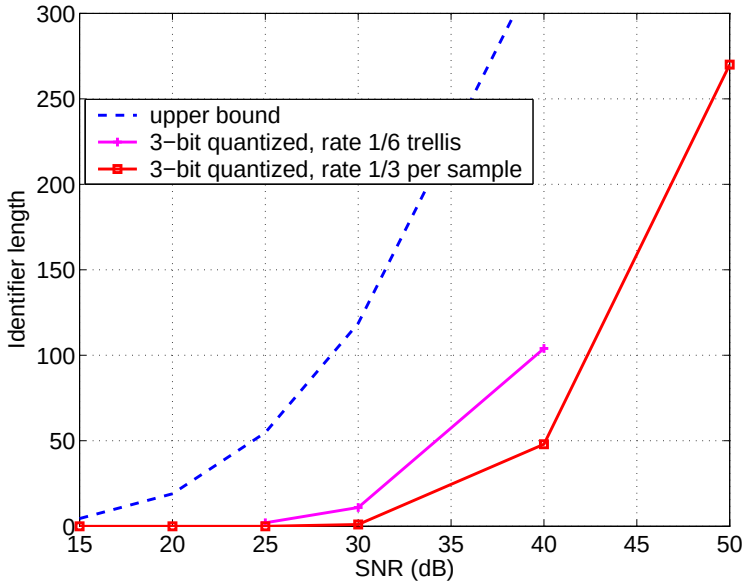

Fig. 11. Achieved identifier lengths over CM 3 for 3-bit quantization and per sample and convolutional code based public communication methods, compared to the upper bound.

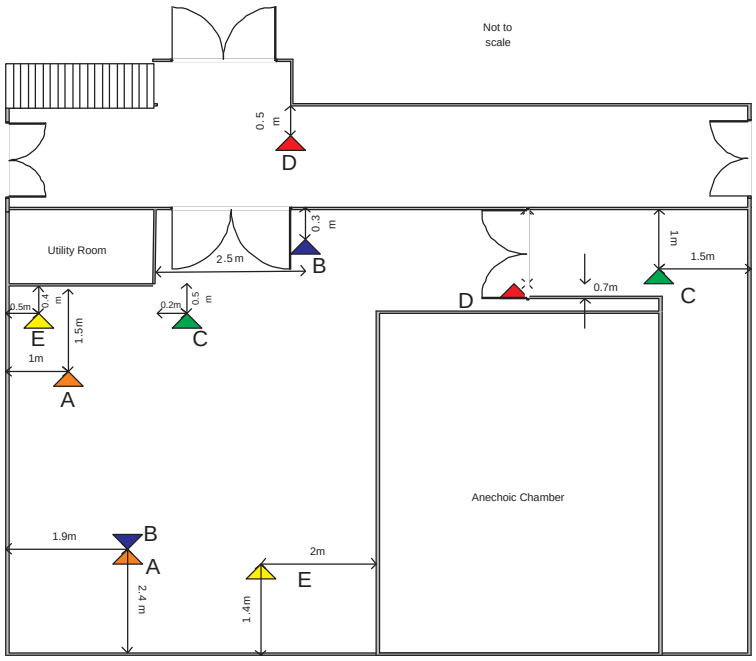

Fig. 12. Layout of transmitter-receiver pairs for channel ID experiments.