Securing Wireless Systems via Lower Layer Enforcements

Conference Paper · September 2006

DOI: 10.1145/1161289.1161297 · Source: DBLP

4 authors, including:

Wenyuan Xu
University of South Carolina
68 PUBLICATIONS **2,513** CITATIONS

SEE PROFILE

W. Trappe
Rutgers, The State University of New Jersey
254 PUBLICATIONS **9,181** CITATIONS

SEE PROFILE

Securing Wireless Systems via Lower Layer Enforcements

Zang Li, Wenyuan Xu, Rob Miller, Wade Trappe
Wireless Information Network Laboratory (WINLAB)
Rutgers, The State University of New Jersey
73 Brett Rd.
Piscataway, NJ 08854
zang, wenyuan, trappe@winlab.rutgers.edu

ABSTRACT

Although conventional cryptographic security mechanisms are essential to the overall problem of securing wireless networks, these techniques do not directly leverage the unique properties of the wireless domain to address security threats. The properties of the wireless medium are a powerful source of domain-specific information that can complement and enhance traditional security mechanisms. In this paper, we propose to utilize the fact that the radio channel decorrelates rapidly in space, time and frequency in order to to establish new forms of authentication and confidentiality that operate at the physical layer and can be used to facilitate cross-layer security paradigms. Specifically, for authentication services, we illustrate two channel probing techniques that can be used to verify the authenticity of a transmitter. Similarly, for confidentiality, we examine several strategies for establishing shared secrets/keys between two communicators using the wireless medium. These strategies range from extracting keys from channel state information, to utilizing the channel variability to secretly disseminate keys. We then validate the feasibility of using physical layer techniques for securing wireless systems by presenting results from experiments involving the USRP/GNURadio software defined radio platform.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: [distributed networks, network communications]

General Terms

Security

Keywords

Authentication, Confidentiality, Key Establishment, Propagation, Wireless Channel Estimation, Fading

1. INTRODUCTION

WiSe'06, September 29, 2006, Los Angeles, California, USA.

Wireless communication systems have undergone considerable evolution in the past decade, in large part due to significant advances in the underlying physical layer technologies, leading to substantial performance leaps in data rates and reliability. These advancements have made wireless devices the platform of choice for communicating. However, as wireless devices become increasingly pervasive, they will also become both a target for attack and the very weapon with which such an attack can be carried out.

Traditional higher-layer computer and network security techniques can, and must, play an important role in combating such attacks. Accordingly, there have been numerous attempts to make various wireless platforms secure by migrating traditional network security strategies to the wireless domain. In spite of these efforts, the development of secure wireless protocols has proven to be a very elusive goal- a fact that is supported by numerous papers revealing successful attacks on many wireless security protocols [1–5]. Perhaps one of the most fundamental reasons why wireless systems have been difficult to secure stems from the broadcast nature of the medium itself, which facilitates both eavesdropping and easy network intrusion.

In this paper we present the viewpoint that there are new modalities for securing wireless systems that can turn the nature of the wireless medium from a disadvantage into an advantage. In essence, rather than rely solely upon generic, higher-layer cryptographic mechanisms, as has been the norm, we will show that it is possible to achieve a lower-layer approach that supports important security objectives, such as authentication and confidentiality. The enabling factor in our approach is that, in the rich multipath environment typical of wireless scenarios, the response of the medium along any transmit-receive path is *frequency-selective* (or in the time domain, *dispersive*) in a way that is *location-specific*. In particular, channel characterizations (e.g. a set of complex gains at different frequencies, or the impulse response at different time delays) decorrelate from one transmit-receive path to another if the paths are separated by the order of an RF wavelength or more.

These unique space, time, and frequency characteristics of the wireless physical layer can be used to augment traditional higher-layer authentication and confidentiality methods. Two wireless entities can identify or authenticate each other's transmitter by tracking each other's ability to produce an appropriate received signal at the recipient. Similarly, the fact that pairwise radio propagation laws between two entities are unique and decorrelate quickly with distance

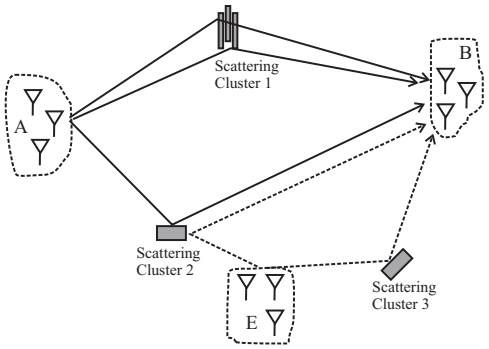

Figure 1: The adversarial multipath environment involving multiple scattering surfaces. The transmission from Alice (A) to Bob (B) experiences different multipath effects than the transmission by the adversary, Eve (E).

can serve as the basis for establishing shared secrets. These shared secrets may be used as encryption keys for higher-layer applications or wireless system services that need confidentiality. In short, these two strategies suggest that merely using cryptographic methods does not capture the full spectrum of possible solutions that are available to the wireless engineer.

We begin the paper in Section 2 by providing an overview of our proposed PHY-layer security services. We then turn to focus on PHY-layer authentication/identification services in Section 3, and then examine PHY-layer protocols that support confidentiality services in Section 4. After describing the protocols and theoretical underpinnings, we proceed to describe our initial validation efforts in Section 5, where we have conducted experiments using the USRP/GNURadio platform. We wrap up the paper by discussing our work in relation to other research efforts in Section 6, and provide concluding remarks in Section 7.

2. ALICE, BOB AND EVE GET PHYSICAL

We now set the stage for the discussion in the remainder of this paper by describing the basic communication scenario we are considering. Further, in order to make the paper more accessible, we provide a brief survey of the relevant principles of radio propagation. A more detailed and precise exposition on propagation can be found in [6].

Both the authentication and confidentiality services we describe make use of the complexity associated with multipath propagation. Throughout our discussion, we shall employ the popular security convention by introducing three different parties: Alice, Bob and Eve. For our purposes, these three entities may be be thought of as wireless transmitters/receivers that are potentially located in spatially diverse positions, as depicted in Figure 1. Our two "legal" protagonists are the usual Alice and Bob, and for the sake of discussion throughout this paper, Alice will serve as the transmitter that initiates communication, while Bob will serve as the intended receiver. Their nefarious adversary, Eve, may either be a passive eavesdropper or an active adversary that injects undesirable communications into the medium. We note that, in this communication scenario, all entities are considered to be within radio range of one another, and hence the techniques presented in this paper are meant to serve as local "one-hop" security mechanisms.

Across the wireless channel, RF signals transmitted from Alice to Bob are affected by a variety of factors, ranging from attenuation due to conservation of energy as the wavefront expands, to large and small-scale fading. Fading arises from a transmitted signal traversing different paths (multipaths) that combine constructively or destructively at the receiver. The effect of multipath for a specific transmitter-to-receiver scenario can be represented as a system where the input $u(t)$ is the transmitted signal and the received signal is

$$r(t) = \int_{-\infty}^{\infty} h(t,\tau)u(t-\tau)d\tau.$$

In this system, the *channel response* is the time-varying function $h(t,\tau)$. A direct formulation of $h(t,\tau)$ from underlying physics is generally unwieldy, and the practice is to apply reasonable stochastic assumptions to simplify the model. The wide-sense stationary with uncorrelated scatterers (WSSUS) assumption implies that the channel response can be modeled (in the time-domain sense) as a tapped-delay line

$$h(t,\tau) = \sum_{i=1}^{N} h_i(t)\delta(t-\tau_i),$$

and with the additional assumption of a Rayleigh fading model, the $h_i(t)$ become a zero-mean complex Gaussian stochastic process. Thus, the channel response can be interpreted as the sum of N delayed, attenuated and phase-shifted versions of the original signal. Since $h(t,\tau)$ is itself stochastic, there is a temporal and spectral variability of the channel response, i.e. the multipath profile will change with time and affect different frequency components of $u(t)$ differently. The fading effects experienced at two different times or at two different frequencies is closely related to the separation between these times/frequencies. The level of temporal and spectral variability is reflected by two notions, the *coherence time* and *coherence bandwidth* of the channel. Coherence time is a measure of the difference in time that is needed in order for the fading correlation to drop below a threshold amount, and coherence bandwidth is similarly defined. Finally, we note that, at a specific instance and frequency, we may examine the fading correlation between a source and two different receiver locations. In this case, the common rule of thumb (c.f. the well-known Jakes uniform scattering model [7]), is that the received signal rapidly decorrelates over a distance of roughly half a wavelength, and that spatial separation of one to two wavelengths is sufficient for assuming independent fading paths.

Turning back to physical layer security, our security objective is to provide authentication and confidentiality to Alice and Bob, in spite of the presence of Eve. Authentication is associated with the assurance that a communication comes from a specific entity, while confidentiality is concerned with the assurance that communication between entities is illegible to eavesdroppers [8]. In our communication scenario, these two objectives may be interpreted as follows. Since the adversary, Eve, is within range of Alice and Bob, and can inject her own signals into the environment (perhaps for the purpose of impersonating Alice), it is desirable for Bob to have the ability to differentiate between legitimate signals from Alice and illegitimate signals from Eve. He therefore needs some form of evidence that the signal he receives did, in fact, come from Alice. On the other hand, for the purpose of confidentiality we wish to ensure that the adversary Eve

cannot decipher the communication between Alice and Bob.

The focus of this paper is to further develop these two security objectives at the PHY-layer. Towards this end, we discuss the following:

- *Channel-based Authentication:* Rather than employ a shared "cryptographic authentication key" between Alice and Bob, we instead exploit the uniqueness of the Alice-Bob channel relative to the Eve-Bob channel. We will outline techniques to distinguish between legitimate transmissions from Alice and anomalous traffic from an adversary Eve.
- *Secret Key Establishment via Multipath Channels:* Confidentiality is traditionally achieved through encryption using a shared key between Alice and Bob that is unknown to Eve. In multipath environments, the unique characteristics of the channel between Alice and Bob can provide parameters that create a unique private key between them– a key that cannot be created from any other location.

These topics are related– each is based based upon the ability of the multipath environment to provide a waveform whose structure an adversary cannot measure or model accurately. Our assumption throughout this paper is that the radio environment is both quasi-static and richly scattered. These conditions are highly favorable to the effectiveness of the techniques we propose, and correspond to a wide range of practical scenarios: The Rayleigh scattering nature of cellular channels, for example, is well-known [6,7,9,10] and the slow temporal variations of channel responses on fixed outdoor links have been reported by many researchers [11–13].

3. PHY-ENHANCED AUTHENTICATION

Authentication and identification services deal with verifying the identity of an entity involved in a transaction. Such a notion of authentication can be addressed through traditional techniques. Wireless authentication, however, can be expanded to include new functionalities, such as recognizing a particular device based upon its unique channel characteristics. It is the authentication of the actual *transmitter* that we now discuss.

3.1 Channel-based Authentication

We seek to exploit the uniqueness of the Alice-Bob channel as an authenticator to distinguish between a legitimate transmitter and an illegitimate transmitter. The ability to distinguish between different transmitters would be particularly valuable for preventing spoofing attacks, in which one wireless device claims to be another wireless device. Currently, spoofing attacks are very easy to launch in many wireless networks. For example, in commodity networks, such as 802.11 networks, it is easy for a device to alter its MAC address by simply issuing an `ifconfig` command. This weakness is a serious threat, and there are numerous attacks, ranging from session hijacking [14] to attacks on access control lists [2], that are facilitated by the fact that an adversarial device may masquerade as another device.

To illustrate how the property of rapid spatial decorrelation can be used to authenticate a transmitter, let us return to Figure 1 and consider a simple transmitter identification protocol in which Bob seeks to verify that Alice is the transmitter. Suppose that Alice probes the channel sufficiently frequently to assure temporal coherence between channel estimates and that, prior to Eve's arrival, Bob has estimated the Alice-Bob channel [15]. Now, Eve wishes to convince Bob that she is Alice. Bob will require that each information-carrying transmission be accompanied by an authenticator signal. The channel and its effect on a transmitted signal between Alice and Bob is a result of the multipath environment. Bob may use the received version of the authenticator signal to estimate the channel response and compare this with a previous record for the Alice-Bob channel. If the two channel estimates are close to each other, then Bob will conclude that the source of the message is the same as the source of the previously sent message. If the channel estimates are not similar, then Bob should conclude that the source is likely not Alice. Here we have achieved unilateral authentication. Mutual authentication can be achieved by having Bob subsequently send Alice an authenticator signal.

Realizing channel-based authentication in a time-varying radio environment involves two aspects. One is the authenticator signaling technique for a fixed instantiation of the channel, and the other is the necessary measures for ensuring the continuity of such an authentication procedure when the channel changes in subsequent epochs. We first discuss approaches for authenticator signaling and then techniques for maintenance of such authentication.

We now describe two strategies for authenticator signaling, but note that other forms of channel sounding, such as used for multiple-input multiple-output (MIMO) channels, are also appropriate.

Temporal (Pulse-type) Probing: Ideally, Bob's received signal $r(t)$ will be the convolution of Alice's signal $u(t)$ with the channel response plus the addition of receiver-side noise. In order for Bob to measure the channel response, Alice will send a probing pulse $u(t)$. The pulse bandwidth is critical to the ability to resolve the multipath environment. If $u(t)$ has sufficiently wide bandwidth W, i.e. $1/W$ is small compared to the temporal width of the impulse response, then the multipath profile can be resolved [6, 9]. Consequently, wideband channel probing strategies, such as direct RF pulsing [9, 16] or spread spectrum methods [17, 18], can be used to construct channel estimates for authentication.

Suppose that the channel impulse response between Alice and Bob is time-invariant over the time period of interest τ, i.e., $h_{AB}(t,\tau) = h_{AB}(\tau)$. Once Bob has an estimate of $h_{AB}(\tau)$, there are two approaches to performing authentication at a later time. The first method involves the claimant (the entity wishing to be authenticated) transmitting another probe, allowing Bob to build a candidate response $\tilde{h}(\tau)$. Bob would compare $\tilde{h}(\tau)$ with $h_{AB}(\tau)$ and decide the claimant is Alice if they are sufficiently similar. The second method involves the claimant sending a known authenticator signal $g(t)$, which would ideally lead to Bob receiving $r_g(t) = (h_{AB} \star g)(t) + n(t)$, where $\star$ denotes convolution. However, if the transmitter is not Alice, then what is observed is $\tilde{r}(t) = (h_E \star g)(t) + n(t)$. To authenticate, Bob compares $\tilde{r}(t)$ with $(h_{AB} \star g)(t)$. The main difference between these two variations is whether the discrimination is performed directly on the received signal, or on parameters derived from the received signal.

Multiple Tone Probing: In this approach, the authenticator signal consists of multiple, simultaneous carrier waves. To ensure independent fading across these different carriers, we require that the carrier frequencies f_i are separated by an

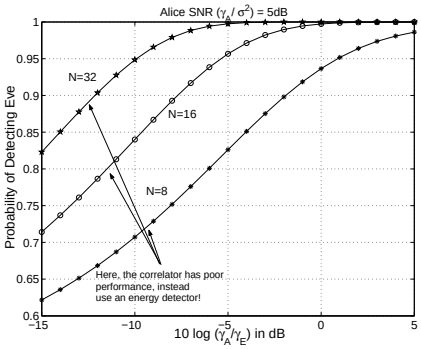

Figure 2: Probability of detecting Eve as a function of different power ratios γ_A/γ_E for varying number of carriers, N, used in a multiple tone authentication scheme. The probability of false alarm is 0.01**.**

amount greater than the channel coherence bandwidth [6,9]. Let us suppose that Alice has initially sent Bob N carrier waves. Disregarding noise, on the ith carrier, Bob has received

$$\Re\left\{e^{j(2\pi f_i t-\phi_0)}\left(\sum_k \alpha_k e^{-j\phi_k}\right)\right\} = \Re\left\{\tilde{H}_i e^{j(2\pi f_i t-\phi_0)}\right\},$$

where ϕ_0 is the phase of Alice's carrier wave at transmission, the summation is over the amount of multipaths for that carrier, and the complex factor $\tilde{H}_i$ is the gain of the Alice-Bob multipath channel at the ith carrier. Bob measures all $H_i = \tilde{H}_i + z_i$, where z_i is noise and interference that is modeled as a complex Gaussian $\mathcal{N}(0,\sigma^2)$. At a later time, the claimant will send Bob N carrier waves with the same carrier frequencies, and Bob will measure the corresponding set of complex gains $\{G_i\}$. The verification process involves testing $\{G_i\}$ against $\{H_i\}$. Under the null hypothesis $\mathcal{H}_0$, the claimant is Alice, and $G_i = \tilde{H}_i + n_i$, for measurement noise $n_i \sim \mathcal{N}(0,\sigma^2)$, while under $\mathcal{H}_1$ the claimant is Eve and $G_i = \tilde{G}_i + n_i$. Here, over i, $\tilde{H}_i$ has average power γ_A, while $\tilde{G}_i$ has average power γ_E. We may choose, for example, a normalized correlation statistic, $T = (\sum_i H_i G_i^*)/(N\gamma_A)$ for discrimination. If we assume that we have a uniform scattering environment [7], and that Eve is several wavelengths away from Alice, then we can assume independence between $\tilde{H}_i$ and $\tilde{G}_i$. In this case $E[T|\mathcal{H}_0] = 1$, $Var(T|\mathcal{H}_0) = (2\gamma_A\sigma^2+\sigma^4)/(N\gamma_A^2)$, while $E[T|\mathcal{H}_1] = 0$ and $Var(T|\mathcal{H}_1) = (\sigma^2+\gamma_A)(\sigma^2+\gamma_E)/(N\gamma_A^2)$. The variance of the test statistic decreases as we increase the number of carriers N. In Figure 2, we present the probability of detecting Eve versus the (adversarial) power ratio γ_A/γ_E for a 1% false alarm rate with the number of carriers N as a parameter. If we make assumptions on Eve's largest likely channel gain power γ_E, then these results serve as guidelines for choosing the number of carriers needed for reliable discrimination and authentication. Similarly, if we have limits on N, such as might arise from regulatory or hardware constraints, then we may use these results to assert Eve's ability to successfully forge a single authentication challenge, thereby quantifying the additional security gain provided by physical layer authentication. It should be noted that, when Eve has a large power γ_E, the correlator alone performs poorly. However, Eve can then be detected through energy detection techniques.

3.2 Maintenance of the channel authenticator

In PHY-layer authentication, we can assume that Bob uses traditional higher-layer authentication procedures to associate the initial link between Alice and Bob with Alice's identity. The PHY-layer authentication described compares a new measurement with a prior channel estimate, thereby verifying whether the new measurement likely came from the source of the prior measurement. The newly verified channel estimate then replaces the prior measurement, allowing for the verification of the next channel estimate. Using $y \rightsquigarrow x$ to denote "y is verified from x", we thus have the verification chain $h(t_M,\tau) \rightsquigarrow h(t_{M-1},\tau) \rightsquigarrow \cdots \rightsquigarrow h(t_0,\tau)$, where $t_M > t_{M-1} > \cdots > t_0$ and t_0 is the time of the initial channel estimate, and thus we only authenticate the transmitter of the initial communication. For this reason, it is necessary to employ traditional higher layer methods to do the initial link association.

However, even in the absence of an initial "cryptographically" verifiable association between $h(t_0,\tau)$ and Alice's identity, we may still use the verification chain to detect whether there has been a change in the transmitter. For example, by maintaining the transmit-receive channel history between a transmitter and receiver, we can detect scenarios where Eve tries to act as Alice. Such an approach could find application in detecting device spoofing.

In either case, the utility of the PHY-layer verification chain is related to the time-varying nature of the channel. In particular, in implementing these techniques, it is necessary to probe the channel at time intervals less than the channel's coherence time in order to support valid comparisons. We note that, for unilateral identification, this process only needs to be one-directional, that is Alice transmits to Bob and Bob maintains the verification chain. On the other hand, for full mutual identification (as opposed to two separate unilateral identifications), the exchanges must be both bidirectional and it is necessary that they have the same channel with which to base their verification chains upon. This implies that channel reciprocity should apply[1], and hence Alice and Bob must use the same carriers in a time-division-duplexing (TDD) manner. In this case, Bob transmits a channel-probing set of tones over some interval $(t_0, t_0+T]$. Alice transmits the same tones over $(t_0+T, t_0+2T]$. Data is transmitted in one or both directions before the process repeats. The temporal width of the exchange, $2T$ plus the data transmission interval, must be small compared to the correlation time of the channel response. This condition can be met using realistic channel probing/data transmission times (e.g., see [11,12]).

Finally, we note that a single verification failure $h(t_M,\tau) \not\rightsquigarrow h(t_{M-1},\tau)$ does not definitively indicate the presence of an adversary, but rather should serve as a warning flag. It may be that $h(t_M,\tau) \not\rightsquigarrow h(t_{M-1},\tau)$ is merely a false alarm, and the warning flag should trigger more careful analysis by the software. For example, as Alice and Eve are both communicating, there will be a repetition of failures, and Bob may record a history of channel estimates in order to enhance the detection of Eve's intrusion. Thus, just as in any intrusion detection system, it is not a single event that should trigger a response, but rather it is the persistence of anomalous

[1]We note the difference between channel reciprocity and the notion of asymmetric links, e.g. [19]. Channel reciprocity is the equivalence of the channel transfer function, and not a statement about noise conditions relative to each entity.

events that should serve to indicate verification failure and set off warning messages.

4. PHY-ENHANCED CONFIDENTIALITY

Confidentiality services, like encryption and key management, are the work horses for many security protocols. A fundamental belief held by the security community is that, when designing confidentiality services, one should not replace traditional ciphers, such as AES, with new ciphers as existing ciphers are very thoroughly cryptanalyzed and designed for bulk-data processing. Hence, our approach to achieving confidentiality focuses on the issue of establishing keys between wireless entities. In one sense, the methods we describe are analogous to Diffie-Hellman key establishment, and can be considered as building blocks rather than complete security solutions.

Referring back to Figure 1, our communication scenario for our confidentiality methods involves Alice transmitting an encoded message to Bob, the intended recipient. Bob receives a signal that is a result of the Alice-Bob channel, while Eve receives a signal that follows from the Alice-Eve channel. Alice's objective is to maximize the rate at which she communicates with Bob (i.e. the key establishment rate), while simultaneously minimizing the information that Eve learns. There are two different extremes to using the wireless channel to establish keys: *extraction* and *dissemination*. In extraction, Alice's signal may be a probing signal that Bob uses to estimate channel state information h_{AB}, from which keys are extracted. In dissemination, however, Alice transmits a signal that is an appropriately coded version of the information Alice wishes to give to Bob. We will present several constructions that represent a variety of methods ranging between these two extremes.

In all of the methods we describe, we assume as a starting point that Alice and Bob each have estimates of their shared channel, e.g. by probing in a TDD fashion. We will denote h_{AB} to be Bob's estimate of the Alice-Bob channel, and h_{BA} to be Alice's estimate of the Bob-Alice channel. Similarly, we will denote h_{AE} to be Eve's estimate of the Alice-Eve channel. The channel estimates may correspond to scalar or vector channel estimates.

4.1 Key Extraction from Channel Estimates

Once channel state information has been estimated, the process of key extraction is rather straight-forward. One simple approach for extracting shared keys would employ cryptographic one-way functions [20]. For example, once Alice and Bob have converted h_{BA} and h_{AB} to a binary representation (requiring quantization of the channel state information), Alice can calculate $K_A = f(h_{BA})$, while Bob can calculate $K_B = f(h_{AB})$, where f is a one-way function. If $h_{BA} = h_{AB}$, then they will have arrived at the same result. To prevent scenarios where a key from a previous time period was captured yet the channel state had not changed enough to make the subsequent key extraction yield a different result, we can employ nonces and achieve added security. In this case, Alice will send a random bit sequence r, and Alice then calculates $K_A = f(h_{BA}\|r)$ and Bob calculates $K_B = f(h_{AB}\|r)$, where $\|$ is concatenation.

Ideally, $K_A = K_B$, and hence they have a shared key. A challenge may arise because Alice and Bob could have slightly different channel estimates. Since we use a pseudo-random one-way function, if $h_{AB} \neq h_{BA}$ then K_A and K_B will be dramatically different, i.e. a single bit difference will produce dramatically different outputs. In order to fix this, one strategy that can be used is a subsequent higher-layer challenge-response verification protocol: Alice sends Bob $E_{K_A}(r_1)$ and Bob responds with $E_{K_B}(r_1 + 1)$. If Alice decrypts and verifies $r_1 + 1$, then she accepts that Bob has obtained the correct key. Similarly, Bob can do likewise.

4.2 Key Dissemination via Channel State Masking

The previous scheme extracted keys from common information shared between Alice and Bob, much like is done in Diffie-Hellman key agreement, and neither Alice nor Bob have control over what the key will be. At the other extreme, are key dissemination techniques where it is possible for one entity to choose the key and distribute it to the other party. We now look at a simple approach to key dissemination that uses the channel state to mask the key being distributed.

In channel state masking, Alice and Bob convert h_{AB} and h_{BA} into binary representations, and then using them as the key sequence in a one-time pad to mask the key being distributed. For example, suppose Alice creates a vector of bits x that she wishes to use as a shared key with Bob. She forms a message $y = x \oplus h_{BA}$, where $\oplus$ is bitwise XOR. Now, if Alice sends this to Bob, say over a public channel, then ignoring errors in the transmission (through the use of an error correcting code on y), Bob calculates $z = y \oplus h_{AB}$, and can recover x if $h_{AB} = h_{BA}$. For the adversary, Eve, her channel estimate h_{AE} will be quite different from h_{AB}, and thus her attempted decoding will be corrupted with errors.

In practice, Alice's and Bob's channel estimates are merely correlated and $h_{AB} \approx h_{BA}$, causing $z \neq x$. To cope with this, an error correcting code must be applied to x, producing a codeword $\tilde{x}$, and now $y = \tilde{x} \oplus h_{BA}$. Bob will calculate $\tilde{z} = \tilde{x} \oplus h_{AB} \oplus h_{BA} = \tilde{x} \oplus e_{AB}$, where e_{AB} captures the mismatch between h_{AB} and h_{BA}. Now, Bob will decode $\tilde{z}$ as x as long as the Hamming weight of e_{AB} is sufficiently small. On the other hand, the sequence $h_{BA} \oplus h_{AE}$ should have a larger Hamming weight than e_{AB}. If the Hamming weight of $h_{BA} \oplus h_{AE}$ is beyond the error correction capability, then Eve will fail to recover the key.

Several interesting issues arise regarding the choice of the error correcting code. In particular, it is desirable to choose an error correcting code that guarantees the formation of the Alice-Bob key while minimizing the likelihood of Eve being able to form the key. On the other hand, error correcting codes work by mapping observed data to a "best guess" codevector. Even should an error correcting code fail to decode, it can still provide some information about the original message (such as parity checks). This also raises an interesting question in the formal context of cryptography about the semantic security of such a scheme. A semantically secure protocol is one in which the communications do not reveal *any* advantageous information to the adversary [21]. In particular, there may be some correlation between h_{AB} and h_{AE}, especially if Eve is physically close to Bob, and thus it might be possible for Eve to estimate certain bits (such as sign bits) of h_{AB} and this, combined with partial decoding, can allow her to infer some bit values of x, or to narrow down the possible decodings of $y \oplus h_{BA} \oplus h_{AE}$ to codewords close to $\tilde{x}$.

4.3 Key Dissemination via Probabilistic Encoding

The next approach that we describe takes a different approach to disseminating keys, and achieves semantic security by using techniques from the theory of probabilistic encryption, and hence inherits the advantages of distinguishability and robustness to the leakage of partial information [22] associated with probabilistic encryption. Further, we note that the scheme we describe is motivated by constructions for Wyner's classical wiretap channel [23], and insight gained from Csiszar and Korner [24] extensions of Wyner's work.

Our approach makes use of trapdoor functions and hard core predicates. Loosely speaking, a trapdoor function $f(x)$ is one for which calculating $c = f(x)$ is easy, but determining x from observing c is difficult without additional, *private* knowledge. A hard core predicate for the trapdoor function $f(x)$ is a Boolean function $G(x)$ such that calculating $G(x)$ is easy, but calculating $G(x)$ from just $f(x)$ is computationally hard. The basic probabilistic encryption of a single plaintext bit $m \in \{0, 1\}$ via hard core predicates is presented in Figure 3 (a). Here, Alice chooses a *random* $x \in \{0, 1\}^N$ such that $G(x) = m$. Now, Alice sends Bob the ciphertext $c = f(x)$. Since Bob possesses the trapdoor, he may calculate $f^{-1}(c) = f^{-1}(f(x)) = x$, and from x he calculates the plaintext via $G(x) = m$.

We seek a similar construction that uses wireless-specific components. Our basic strategy is portrayed in Figure 3 (b). Here, suppose Alice and Bob have estimated their channel conditions, and have produced a channel with error rate p_{AB}, and that the Alice-Eve channel has an error rate p_E, with $p_E > p_{AB}$. Alice will send a plaintext bit m to Bob by mapping it to an appropriate random code word. Let us look at an extreme case where $p_{AB} = 0$. Suppose Alice wishes to send Bob a 0 or a 1. She will encode this with a *random* N bit sequence x of the same parity, i.e. $G(x) = m$ is the parity function. Since Bob's channel is error-free, he calculates the parity of x, and recovers m. The situation is different for Eve. For sufficiently large N, the probability that there is an even amount of bit errors is arbitrarily close to the probability of an odd amount of bit errors (the probability of an even amount of bit errors is $0.5[1+(1-2p_E)^N] \rightarrow 0.5$). Hence, Eve does not learn anything about the actual value of the bit, and since x was random it is very unlikely that she will witness the same ciphertext again (thus providing semantic security). This basic scenario can be modified for the general $p_{AB} > 0$ case.

The heart of our probabilistic construction boils down to the validity of the $p_{AB} < p_E$ assumption. If we can make $p_{AB} < p_E$, then sending multiple codebits through the communication medium naturally makes it harder for Eve to decode than Bob.

Thus, we must utilize the channel in a manner that forces $p_{AB} < p_E$, even if Eve is closer to Alice than Bob. To this end, our strategy uses a multicarrier system (similar methods can be applied in a MIMO system). Here, information is encoded across k out of K carriers with a separation larger than the channel coherence bandwidth in order to guarantee independent fading. The information received by Bob on subchannel i may be modeled via $y_i = \alpha_i x_i + n_i$, where $|\alpha_i|$ is a Rayleigh random variable describing the subchannel gain, and n_i is noise that is assumed to have equal power σ^2 across all subchannels. The quantity $|\alpha_i|^2/\sigma^2$ reflects the quality of subchannel i, and will vary across subchannels,

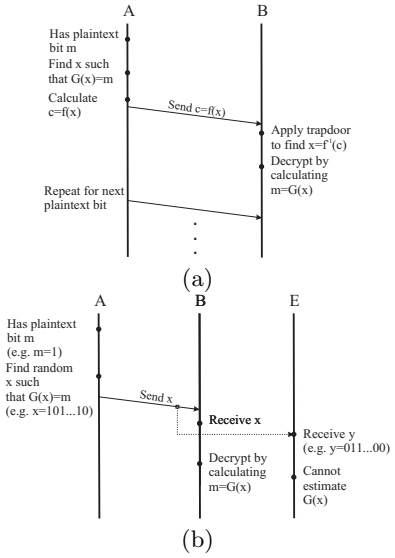

Figure 3: (a) Probabilistic encryption via trapdoor functions, (b) Key dissemination motivated by probabilistic encryption.

as depicted in Figure 4 (a). Since Alice and Bob share an estimate of the same channel, they know which channel is the best, and may send their information on that subcarrier.

Assuming that Eve is far enough from Bob so that the Alice-Eve and Alice-Bob subchannel gains are independent (i.e. on the order of one wavelength, $\lambda \approx 0.1 - 1.0$m for 300MHz - 3GHz.), then there is a good chance that one of the better Alice-Bob subchannels will be bad for Eve and hence, if we code only on this channel, then $p_{AB} < p_E$. More specifically, we may code only on Alice-Bob's best channel, in which case the question of whether $p_{AB} < p_E$ boils down to whether Alice-Bob's best subchannel is better than a random subchannel for Alice-Eve. For Rayleigh fading, Bob's gains $|\alpha_i|$ are Rayleigh (and hence $|\alpha_i|^2$ are exponential) with average power γ_B, while Eve's gains $|\alpha_E|$ are Rayleigh with average power γ_E and Eve's noise has power σ^2, we may calculate the probability of $p_{AB} < p_E$ by finding $Pr\left(\max\{|\alpha_i|^2\} > |\alpha_E|^2\right)$:

$$\beta_1 = Pr\left(\max\{|\alpha_i|^2\} > |\alpha_E|^2\right) \quad (1)$$

$$= 1 - \int_0^\infty (1 - e^{-x/\gamma_B})^K \frac{1}{\gamma_E} e^{-x/\gamma_E} dx \quad (2)$$

$$= 1 - \sum_{n=0}^{K} \binom{K}{n} (-1)^n \frac{\gamma_B}{n\gamma_E + \gamma_B}. \quad (3)$$

We present a plot of β_1 versus $10\log(\gamma_B/\gamma_E)$ in Figure 4 (b), for the case of $K = 32$ subcarriers. From this, we see that in many cases, even when Eve has a better average gain than Bob (i.e. $\gamma_E > \gamma_B$), it is likely that $Pr(p_{AB} < p_E)$. Still, for enhanced secrecy, it is desirable to improve this likelihood and instead of using one subcarrier, we may choose the k best Alice-Bob subcarriers, and code in such a way that Eve must have better gains on *all* of these k subcarriers in order for $p_E < p_{AB}$, for example by employing a hash function. The corresponding probabilities $\beta_k = Pr(p_{AB} < p_E)$ are presented for $k = 2$ and $k = K$ in Figure 4 (b).

There are many possible variations for how we select car-

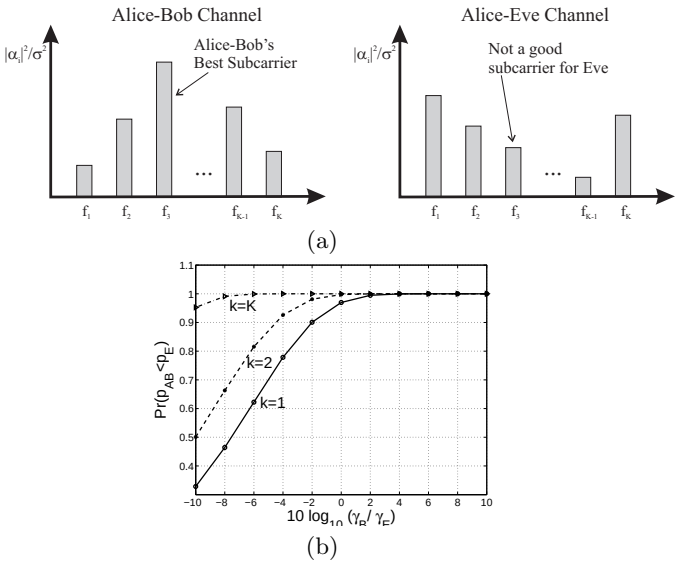

Figure 4: (a) Alice-Bob and Alice-Eve channel gains across different subcarriers. (b) Probability that $p_{AB} < p_E$ versus $10\log(\gamma_B/\gamma_E)$ for $K = 32$ subcarriers, and for different choices of k (the number of subcarriers used).

riers and allocate resources across these channels. For example, rather than choose the best k channels, we may instead apply a waterfilling strategy [25]. Even with such constructions, though, we cannot absolutely guarantee that Eve has a worse decoding capability than Bob. However, by tying in a propagation and shadowing model, we may relate γ_B/γ_E to the relative distances that Bob and Eve are from Alice. This allows us to define a *threat region* about Alice where, with a prescribed likelihood, Eve may be able to successfully decipher the key bits that Alice is sending Bob. To assure complete security, Alice would then need to physically guarantee that Eve is not within this threat region.

5. EXPERIMENTAL VALIDATION

The proposed PHY-layer security methods introduce new functionalities to the radio that are not possible to validate using conventional off the shelf equipment, and it was therefore necessary to conduct our experimental efforts using a software defined radio (SDR) platform that allows for access to waveform-level details. In our experiments, we used the Universal Software Radio Peripheral (USRP) board in conjunction with GNURadio running on a personal computer. GNURadio is an open source, free software toolkit that provides a library of signal processing blocks for developing communications systems and experiments. Our experiments were implemented using GNURadio under Debian GNU/Linux (kernel 2.6).

The USRP supports the simultaneous transmit and receive of four real or two complex channels in real-time. For reception it utilizes four 12-bit analog-to-digital converters (ADCs) operating at 64MHz, and four digital-downconverters with programmable decimation rates. The transmit side of the USRP incorporates four 14-bit DACs that operate at 128MHz, and two digital-upconverters with programmable interpolation rates. Data is transferred between the computer and the USRP via a USB2.0 interface. Given a sustainable data rate of 32 MBps and complex 16-bit samples, the effective total spectral bandwidth is limited to 8MHz. The USRP itself is not directly capable of RF input/output, and it is necessary to interface the USRP with RF daughterboard modules for actual RF transmit/receive. In our experiments, we used the RFX400 transceiver, which operates in the 400-500MHz band, and is capable of outputting 100 mW (+20 dBm) with a Noise Figure of 3-5 dB. The platform used as the transmitter is depicted in Figure 5 (a).

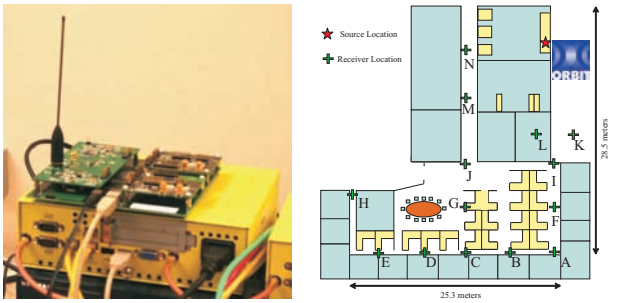

Figure 5: (a) USRP/GNU Radio platform and the RX400 RF Frontend used in experiments. (b) Relative locations of transmitter and receiver during experiments.

5.1 Fundamental Measurements

We first conducted several experiments to evaluate the spatio-temporal coherency properties of the indoor wireless channel. We conducted all experiments in our building, as depicted in Figure 5 (b). For all experiments, we fixed the location of the transmitter in a laboratory (upper right hand corner), and then varied the positions of the receiver platform throughout the building. For each position, we measured data at a net sampling rate of 2MHz (following decimation by 32). The following experiments were performed:
Experiment 1: In this experiment, we were interested in the temporal coherency of the channel for a fixed location. We used three carrier frequencies at 420MHz, 450MHz and 480MHz. The 30MHz separation between these carriers was chosen to ensure fading independence across the carriers. Data was measured at location G. For this experiment, we sampled the carriers for a duration of 1 second every 15 minutes, collecting roughly 16MB for each carrier frequency and each sampling interval. This sampling was carried out over an experimental period of 1 hour. We calculated the magnitude of the channel gain for each frequency versus time across our 1sec interval, using a sliding window with an integration time of 1msec.

We present the magnitude of the channel gains for 0.1 seconds for each of four sampling intervals (a period of 1 hour) in Figure 6 (a), for each of the three carrier frequencies. From this figure, we can see that there is some variability in the channel across time, as illustrated by the 420 and 450MHz gains crossing each other in between the second and third interval. We also note that the 480MHz gains were much lower. Overall, although there is some temporal variability, this variability is still within a constrained dynamic range, implying that the variation occurs around a mean response profile for this location.

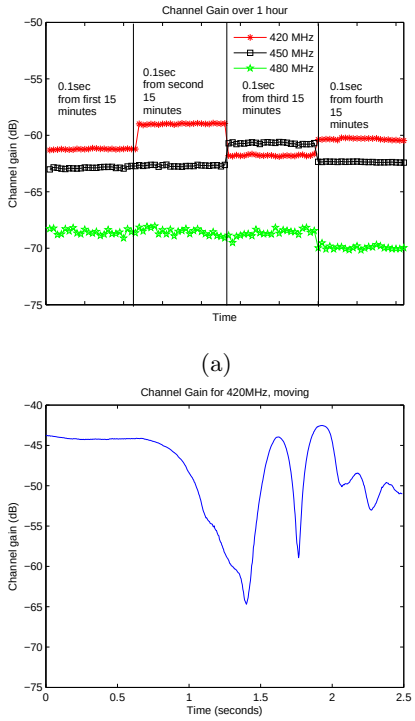

Figure 6: (a)Magnitude of the channel gains for location G over 1hour. (b) Channel gain for 420MHz as receiver moves from N to J.

Experiment 2: In this experiment, we examined the spatial nature of the channel by collecting data from each of the three carriers at different locations in the building. For this experiment, we again collected roughly 16MB for each carrier frequency at each location. One challenge that we encountered was the fact that we could not measure in different locations simultaneously. To minimize the temporal variations, we conducted our experiments during a time of no activity in the building. Even so, we note that we encountered difficulty discriminating between channel phase and oscillator drift, and thus restricted our attention to comparing the magnitudes of the gain across locations. We observed several instances where different pairs of locations would exhibit rather diverse properties across different carrier frequencies. In general, the fact that two locations might exhibit correlation for one carrier but not for another is an important observation that is critical to the success of using the channel to identify the transmitter. It implies that, with the application of more carriers, we should be able to improve our ability to discriminate between the channels associated with different locations.

Experiment 3: In this experiment, we examined the effect of mobility on the channel coherence by gathering data on just the 420MHz carrier as we moved the receiver from location N to location J (as depicted in Figure 5 (b)). For this experiment, a roughly 100MByte trace was collected. We present the channel gain versus time for 2.5 seconds of data in Figure 6(e). In this trace we see that there is variability of the channel as we move. We note that there are two periods of "deep" fades, which we conjecture are due to shadowing as we passed by two metal doors. However,

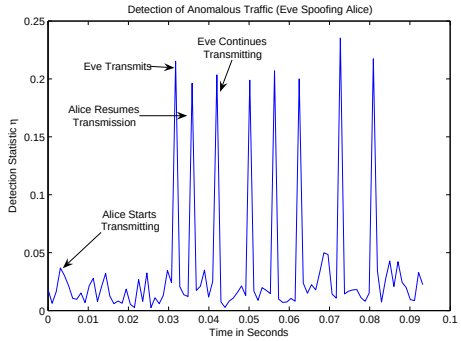

Figure 7: Value of the change point statistic $\eta(t)$. After a short time, Eve commences spoofing Alice, and then Eve and Alice alternately transmit for random durations.

even so, a visual inspection suggests that for the most part the channel is coherent over time intervals of roughly 20-100msec, which would imply that in a mobile environment we should conduct channel probing at intervals of tens of milliseconds.

5.2 Evaluation of PHY Authentication

The spatial and temporal correlation properties across the three carriers we examined are encouraging and suggest that it should be possible to discriminate between two transmitters at two different locations.

Applying the principle of channel reciprocity, we used our traces from Experiment 2 to construct a synthetic trace to explore the utility of PHY-layer authentication techniques to discriminate between transmitters in a spoofing scenario. In our trace, we placed Bob (the receiver) at the location of the transmitter in Experiment 2, and we placed both Alice and Eve (the transmitters) at two receiver locations from Experiment 2. We chose Alice to be located at position A, while we placed Eve at location H. In our synthetic trace, we assume that Alice has started communication for a short period before introducing Eve. Following the Alice-only period, we employed a randomized schedule corresponding to Alice and Eve alternately communicating. This randomized schedule is meant to reflect the fact that Alice would most likely continue transmitting while Eve is conducting a spoofing attack. In the trace, we assume that Eve knows that verification requires transmission on 420MHz, 450MHz, and 480MHz, and hence Eve transmits on all these carriers.

To detect Eve, we estimated the magnitude of the channel gains versus time $|\alpha_j(t)|$ across the three carriers, and constructed a feature vector $\mathbf{v}(t) = [|\alpha_1(t)|, |\alpha_2(t)|, |\alpha_3(t)|]^T$. Since our objective is to detect a change in the channel state versus time, we employed a simple change-point detector

$$\eta(t) = \frac{\|\mathbf{v}(t) - \mathbf{v}(t-1)\|}{\|\mathbf{v}(t-1)\|}.$$

We present $\eta(t)$ for our synthetic trace in Figure 7. We note that during periods where just Alice transmits, the value of $\eta(t)$ is small, but that $\eta(t)$ exhibits large spikes in its value at times where there is a change in the transmitter, thereby facilitating the detection of device spoofing. Similar change point detection was observed for all other Alice-Eve location pairs.

5.3 Evaluation of PHY Confidentiality

We also used the traces from Experiment 2 to explore the feasibility of using the PHY layer to establish cryptographic keys. We calculated the dynamic range for the magnitude of the channel gains over the entire data set from Experiment 2 (across frequency, time and location). Using this, we built an 8-bit uniform quantizer to quantize channel gains for each of the three carriers at each location, producing a total of 24 bits of channel symbol information. In order to remove any correlation from channel symbol information across locations, we used the SHA-1 hash function in conjunction with a random seed r that was transmitted via a public channel (i.e. we assume each location receives r perfectly). Our keys were 24bits, as calculated by

$$K = M_{24}\left[f_{SHA-1}([Q(\mathbf{v}(t))\|r])\right],$$

where $Q()$ is the 8-bit quantizer, M_{24} is extraction of the middle 24 bits, and $\|$ denotes concatenation. As an example of the output, we present results of the 24-bit key sequence generated at each of the locations A through N using the first channel state estimates from Experiment 2. Using a random seed $r = 0$x374573, the resulting keys were

Location	Key Sequence
A	1001 1001 1101 1000 0101 1011
B	0110 0101 0010 1000 1110 1110
C	1101 0111 0000 0011 0011 1010
D	1111 0001 1101 1001 1111 0111
E	0100 0001 1101 1101 1000 0001
F	1111 1000 1101 1101 0001 1011
G	1100 0001 1110 1010 0110 1101
H	0000 1101 0000 1000 0000 0101
I	1111 0010 1011 0010 0111 1111
J	0010 1110 0011 0101 1111 0001
K	1010 1010 0101 0111 0100 0000
L	1011 1000 0110 0001 1001 0101
M	0101 1010 1010 1101 1010 1000
N	1100 1011 0101 1100 0111 1000

In particular, in spite of the correlation that exists between certain pairs of locations on individual carriers, the fact that we are utilizing more than one carrier with different correlation properties causes the quantized feature vector, and hence the resulting bit sequences, to differ.

6. RELATED WORK AND PERSPECTIVES

The objective behind this paper is to highlight the utility of the physical layer and wireless channel for supporting the objectives of authentication and confidentiality. Although applying these methods for security might seem to be a radical paradigm shift, we note that this is not the first time that multipath and advanced physical layer methods have proven advantageous, and we are encouraged in our belief by two notable parallel paradigm shifts in wireless systems: (1) code division multiple access (CDMA) systems, where the use of Rake processing transforms multipath into a diversity-enhancing benefit; and (2) multiple-input multiple-output (MIMO) antenna techniques, which transform scatter-induced Rayleigh fading into a capacity-enhancing benefit.

The techniques that we have presented are, in many ways, motivated by results from information theory. Notably, the problem of secure communication in the presence of an eavesdropper was originally laid out in Wyner's classical wiretap paper [23], where Eve's channel was considered a subsequent degradation of the Alice-Bob channel. Alice's objective is to appropriately encode information so that information can be secretly conveyed between Alice and Bob while ensuring Eve learns no information about Alice-Bob's communication. The notion of secrecy capacity was introduced to quantify the maximum rate for such secret communication, and Csiszar and Korner [24] extended the formulation to the more general wiretap channel, where positive secrecy capacity is achievable as long as Alice-Bob's channel is "better" than Alice-Eve's channel. Maurer showed that secret communication can be achieved even when Eve's channel is better [26–28], as long as the Alice-Bob and Alice-Eve channels differ and public discussion (a method that allows creation of a virtual channel between Alice-Bob that is less noisy than the virtual channel between Alice-Eve) is allowed. Maurer's idea, combined with the results of [23, 24], suggest an intuitive fundamental strategy for secret communications: one should develop methods that ensure that the Alice-Bob channel "effectively" has higher quality than the Alice-Eve channel. We note that these theoretical developments are all reliant on the Alice-Eve channel being known by Alice, which is an unrealistic assumption from the security viewpoint.

The theoretical underpinnings suggest that many forms of security are possible if we can take advantage of some physical property. Notably, one type of physical property that has received considerable attention over the past few decades is the quantum channel [29, 30]. More recently, the wireless channel has been suggested for secret communication [31–33], though to our knowledge the wireless channel has not been proposed for identification purposes. In [31], the authors outline three methods for establishing a key using the channel. Two of their methods seek to create an asymmetrical workload for Eve, but are based upon non-standard complexity assumptions, such as the difficulty of deconvolution, and may not achieve sufficient complexity for reliable security. Similar to the third method of [31], the methods of [32, 33] use the channel's phase characteristics for security, where phase compensation is proposed to securely transmit information. Spacetime coding and transmitter filtering have recently been considered as a means for secure communication [34, 35]. Our work builds upon these methods and represents one of the first implementation efforts to exercise the wireless channel at the physical layer for security purposes.

7. CONCLUDING REMARKS

Wireless networks represent a dramatically different type of communication system than traditional "wired" networks. Typically, these differences have been seen as a challenge making it harder to secure wireless systems. In this paper, however, we have proposed that it is possible to exploit the underlying properties of the wireless medium in order to support security objectives. Channel probing techniques, such as wideband pulsing and multitone probing, may be used to estimate the channel state, which can be compared against a history of transmitter-receiver channel states in order to detect anomalous behavior. Further, the rapid decorrelation properties of the multipath channel allows for either the extraction of key material from channel state information, or the secret dissemination of keying information across the channel through suitable encoding.

We have presented the results of an initial validation effort using the USRP/GNURadio SDR platform. The objective

behind this effort was to support the feasibility of physical layer identification and confidentiality techniques. Our initial results indicate the merit of physical layer security, and in particular illustrate that it is possible to detect change points associated with instances where entity spoofing is performed. Additionally, we presented a simple example of how key information could be shared across a public channel once the transmit-receiver channel has been estimated. However, our experience has also shown the importance of employing probing techniques with sufficient transmit bandwidth (e.g. more carriers separated by the coherence bandwidth in our multicarrier techniques). This, however, necessitates a more powerful SDR platform capable of processing hundreds of MHz of bandwidth, or even a UWB platform. Our current efforts are focused on developing these methods for more powerful SDRs. One further direction that we are exploring is the degree to which temporal variability affects our proposed schemes. We have observed more temporal variability at 5GHz, which would thus require more frequent channel probing at these frequencies. We believe there is a point where too little temporal coherency can make our techniques impractical, and we are currently working on exploring this conjecture.

Finally, we note that the two security objectives that we have focused on are a fraction of what can be accomplished at the physical layer of the protocol stack. For example, a non-repudiation service can exploit the broadcast nature of the wireless medium by introducing witnesses, making it harder for wireless entities to deny carriage of information. An availability service can use spreading and power control to maintain network connectivity in the presence of RF interference attacks. Overall, we envision that it will be possible to develop a suite of lower-layer enforcement strategies that can complement traditional methods, and ultimately lead to more secure wireless systems.

Acknowledgements: The authors would like to express their gratitude to Larry Greenstein, and Ivan Seskar for guidance in conducting channel sounding experiments. Additionally, the authors would like to thank Narayan Mandayam, Roy Yates, Alex Reznik and Yogendra Shah for valuable discussions.

8. REFERENCES

[1] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: the insecurity of 802.11," in *MobiCom '01: Proceedings of the 7th annual international conference on Mobile computing and networking*, 2001, pp. 180–189.

[2] A. Mishra, M. Shin, and W. A. Arbaugh, "Your 802.11 network has no clothes," *IEEE Communications Magazine*, pp. 44 – 51, 2002.

[3] D. Wagner, B. Schneier, and J. Kelsey, "Cryptoanalysis of the cellular encryption algorithm," in *Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology*, 1997, pp. 526–537.

[4] R. Housley and W. Arbaugh, "Security problems in 802.11-based networks," *Commun. of the ACM*, vol. 46, no. 5, pp. 31–34, 2003.

[5] N. Cam-Winget, R. Housley, D. Wagner, and J. Walker, "Security flaws in 802.11 data link protocols," *Commun. of the ACM*, vol. 46, no. 5, pp. 35–39, 2003.

[6] A. Goldsmith, *Wireless Communications*, Cambridge University Press, 2005.

[7] W.C. Jakes Jr., *Microwave Mobile Communications*, Wiley, 1974.

[8] W. Trappe and L.C. Washington, *Introduction to Cryptography with Coding Theory*, Prentice Hall, 2002.

[9] T.S. Rappaport, *Wireless Communications- Principles and Practice*, Prentice Hall, 2001.

[10] A. F. Molisch, Ed., *Wireless Communications*, John Wiley and Sons, 2005.

[11] A. Domazetovic, L. J. Greenstein, I. Seskar, and N.B. Mandayam, "Propagation models for short range wireless channels with predictable path geometries," *IEEE Trans. on COM*, vol. 53, no. 7, pp. 1123–1126, July 2005.

[12] A. Domazetovic, L. J. Greenstein, I. Seskar, and N.B. Mandayam, "Estimating the doppler spectrum of a short range fixed wireless channel," *IEEE COM Letters*, vol. 7, no. 5, pp. 227–229, May 2003.

[13] V. Erceg et. al., "Channel Models for Fized Wireless Applications," IEEE 802.16 Broadband Wireless Access Working Group, July 27, 2003.

[14] A. Mishra and W. A. Arbaugh, "An initial security analysis of the IEEE 802.1x standard," Tech. Rep. CS-TR-4328, University of Maryland, College Park, 2002.

[15] J. Tugnait, L. Tong, and Z. Ding, "Single-user channel estimation and equalization," *IEEE Signal Processing Magazine*, pp. 17–28, 2000.

[16] T. S. Rappaport, "Characterization of UHF multipath radio channels in factory buildings," *IEEE Trans. on Antennas and Propagation*, vol. 37, pp. 1058–1069, 1989.

[17] D. C. Cox, "Delay doppler characteristics of multipath delay spread and average excess delay for 910 MHz urban mobile radio paths," *IEEE Trans. Antennas and Propagation.*, vol. 20, pp. 625–635, 1972.

[18] R. J. C. Bultitude and G.K Bedal, "Propagation characteristics of microcellular mobile radio channels at 910 Mhz," *IEEE J. Sel. Areas Commun.*, vol. 7, pp. 31–39, 1989.

[19] G. Zhou, T. He, S. Krishnamurthy, and J. Stankovic, "Impact of radio irregularity on wireless sensor networks," in *MobiSYS '04: Proceedings of the 2nd international conference on Mobile systems, applications, and services*, 2004, pp. 125–138.

[20] A. Menezes, P. vanOorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[21] "Lecture notes on cryptography," MIT Summer Course, available at http://www.cs.ucsd.edu/users/mihir/papers/gb.html, 2001.

[22] S. Goldwasser and S. Micali, "Probabilistic encryption," *Journal of Computer and System Sciences*, vol. 28, pp. 270–299, 1984.

[23] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. Journal*, vol. 54, pp. 1355–1387, 1975.

[24] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, pp. 339–348, 1978.

[25] T. Cover and J. Thomas, *Elements of Information Theory*, John Wiley and Sons, 1991.

[26] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, pp. 733–742, 1993.

[27] U. M. Maurer, "Perfect cryptographic security from partially independent channels," in *STOC '91: Proceedings of the twenty-third annual ACM symposium on Theory of computing*, 1991, pp. 561–571.

[28] U. M. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels .i. definitions and a completeness result," *IEEE Trans. Inform. Theory*, vol. 49, pp. 822–831, 2003.

[29] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, "Quantum cryptography, or unforgeable subway tokens," *Advances in Cryptology: Crypto '82*, p. 267 275, 1982.

[30] D. Wiedemann, "Quantum cryptography," *Sigact News*, vol. 18, pp. 48–51, 1987.

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

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

[33] H. Koorapaty, A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Commun. Letters*, vol. 4, pp. 52–55, 2000.

[34] S. Goel R. Negi, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference*, September 2005, pp. 1906–1910.

[35] A.O. Hero, "Secure space-time communication," *IEEE Transactions on Information Theory*, pp. 3235–3249, December.