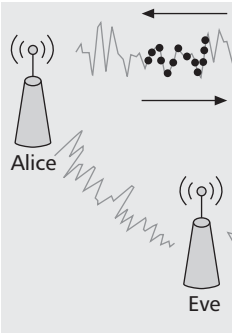
EXPLOITING THE PHYSICAL LAYER FOR ENHANCED SECURITY

SUHAS MATHUR, RUTGERS UNIVERSITY
ALEX REZNIK AND CHUNXUAN YE, INTERDIGITAL INC
RAJAT MUKHERJEE, INDEPENDENT CONSULTANT
AKBAR RAHMAN AND YOGENDRA SHAH, INTERDIGITAL INC
WADE TRAPPE AND NARAYAN MANDAYAM, RUTGERS UNIVERSITY



The authors argue that new security paradigms that exploit physical layer properties of the wireless medium, such as the rapid spatial, spectral and temporal decorrelation properties of the radio channel, can enhance confidentiality and authentication services.

ABSTRACT

While conventional cryptographic security mechanisms are essential to the overall problem of securing wireless networks, they do not directly leverage the unique properties of the wireless domain to address security threats. The wireless medium is a powerful source of domain-specific information that can complement and enhance traditional security mechanisms. In this article we argue that new security paradigms which exploit physical layer properties of the wireless medium, such as the rapid spatial, spectral, and temporal decorrelation properties of the radio channel, can enhance confidentiality and authentication services. We outline some basic constructions for these services, and then provide a case study for how such strategies can be integrated into a broader security framework for a wireless network.

INTRODUCTION

Most of the focus of cross-layer optimization in wireless networks has been on enhancing basic network operations, such as routing and medium access control, and little attention has been devoted to using cross-layer information to enhance security. This is somewhat surprising, given that wireless networks have properties that make them markedly less secure than their wired counterparts. Perhaps foremost of these is the fact that the wireless medium is intrinsically a broadcast medium. In order for an adversary to overhear communications in the *wired* world, a physical connection to the wire is required. In contrast, for wireless networks, adversaries can easily witness anything that is transmitted as long as they are within listening range of the transmitter. Further complicating matters are the ubiquity and portability of the platform itself, implying that adversaries can attempt to access the network from anywhere. This fact is evidenced by extensive underground wardriving efforts, and the end result is that network intrusion and subversion is now easier.

In spite of the unique challenges the wireless domain presents, the approach commonly taken to secure wireless networks has been to translate traditional cryptographic security protocols to the wireless domain. Although the application of conventional security protocols to wireless networks is essential, such an approach ignores the opportunities provided by the wireless aspect of the problem. For example, the wireless channel can be employed to explicitly provide *forward* and *backward* security, which present systems largely lack.

In this article we present the case for new wireless security modalities that turn the wireless medium from being a disadvantage into an advantage. In essence, rather than relying solely upon generic, higher-layer cryptographic mechanisms, as has been the norm, we argue that it is possible to achieve a cross-layer approach that uses physical layer information to enhance encryption and authentication functionality. At the heart of the approach are the following key characteristics of wireless channels:

- Multipath-rich environments exhibit channel responses that rapidly decorrelate in space and time.
- Wireless channels are reciprocal in space, implying that the channel behaves in the same manner irrespective of in which direction it is used/observed.
- Wireless channels change in time, thus providing a natural refresh mechanism for a channel-based security mechanism.
- The time variation is slow enough that any reasonable wireless system can accurately estimate and process channel impulse responses well within the coherence time of the channel.

These properties result from the manner in which RF waves propagate in a multipath rich environment (i.e., an environment with a large

This research was supported in part by NSF grant CNS-0626439.

1536-1284/10/$25.00 © 2010 IEEE

Although 802.11i addresses a wide range of security threats facing wireless LANs, the protocol suite is not complete and there are many threats that can undermine 802.11i.

number of reflectors and scatterers), which is typical for most terrestrial wireless systems, and represent a benefit to security services that does not exist for conventional wired or optical channels. The fact that the radio channel between two entities is unique and decorrelates quickly with distance can serve as the basis for establishing shared secrets that may be used as encryption keys for higher-layer services needing confidentiality. Similarly, the wireless channel can allow entities to authenticate each other's transmitters by having each user track the other's ability to produce an appropriate received signal at the recipient.

We begin by identifying opportunities for the physical layer to enhance security services, using 802.11 systems as an example case study. We then review some basic properties of wireless propagation that are relevant to these methods for enhancing security. Physical layer authentication methods that can be used to enhance security in 802.11 systems are described in the following section. We then focus on PHY-layer encryption services that can enhance 802.11i by using the channel to establish secret bits for encryption. We end with concluding remarks and research challenges.

Wireless Security: Threats and Opportunities for Enhancements

Securing network systems focuses on addressing confidentiality, data integrity, authentication, and non-repudiation through protocol suites that are typically applied at the link, network, transport, and application layers, as is evidenced by 802.11i, IPSec, and SSL/TLS. Although each of these suites might support multiple security objectives (e.g., confidentiality and authentication in 802.11i), with few exceptions these protocol suites tend to be focused on a single layer and not involve cross-layer design. Wireless systems inherently have unique properties at the physical layer that can be exploited to enhance security. Such enhancements require the sharing of information between the physical layer and higher layers.

In considering a cross-layer security architecture, which includes the physical layer, we concentrate on two central themes:

- It is often desirable to enhance the security of a wireless LAN without requiring new cryptographic material. This goal can be accomplished by properly utilizing physical layer resources. For instance, *spoofing* in a wireless LAN is a problem that can be addressed using information from the physical layer without explicitly introducing new cryptographic primitives.
- When new cryptographic matter is required, the physical layer can provide a good resource for obtaining such new matter.

802.11i Overview

In order to set the stage for how physical layer information can enhance security, we provide a review of current wireless LAN security. Given the widespread use of the 802.11 standard, we use this system as our representative example, although our ideas are applicable to wireless systems in general.

Among the innovations of 802.11i is the introduction of two authentication modes. The first mode is based on the availability of an authentication server (hereafter referred to as 802.1X-based authentication). The second mode is based on configuring a secret password or pass-phrase on the participating devices: the pre-shared key (PSK) mode. In the PSK mode a user authenticates by demonstrating knowledge of the secret key. 802.1X-based authentication is typically used in WLAN office or enterprise deployments. It is based on the availability of digital certificates at both the client as well as the authentication, authorization, and accounting (AAA) server.

Figure 1 summarizes the sequence of steps in the 802.1X authentication and key distribution process. In the PSK mode association between the STA and AP replaces the communication prior to the establishment of the pairwise master key (PMK) in Fig. 1. The PSK then becomes the PMK, and the rest of the procedure is unchanged. Note that the master key (MK, shared by STA and AAA server) and PMK (shared by STA, AP, and AAA server) are not the same because the roles of the AP and AAA server are separated. Furthermore, the PMK and pairwise transient key are not the same; since updating the entire key mechanism is resource intensive, the PTK is the key that is updated.

Opportunities to Enhance 802.11i

Although 802.11i addresses a wide range of security threats facing wireless LANs, the protocol suite is not complete, and there are many threats that can undermine 802.11i. The research and standards community literature is filled with examples of exploits against 802.11i, ranging from denial of service (DoS) attacks to attacks that undermine 802.11i because it attempts to maintain backward compatibility. Although it may be possible to address such threats through further refinement of the security protocol suite, many threats may easily be addressed in a cross-layer security framework using information provided by the physical layer. In this article we briefly touch on two such opportunities. The first opportunity addresses the fact that management and control frames are unprotected, and hence various DoS attacks are possible by conducting a spoofing attack on the identity of an access point (AP) (e.g., the well-known de-authentication or disassociation attack), or by a single client conducting a Sybil attack by claiming multiple network identities. As seen later, such a threat can be dealt with by tracking the channel between transmitter and receiver (e.g., between a client and an AP), and declaring unusual channel responses as an anomaly, indicating spoofing. The physical layer also provides an opportunity to address risks associated with the compromise of the PMK in 802.11i. In particular, by integrating secret bits extracted from the physical layer channel into the key establishment process, it is possible to achieve forward and backward secrecy.

The Wireless Channel

We now provide a brief review of wireless propagation in multipath environments. A more detailed and precise exposition on propagation can be found in [1].

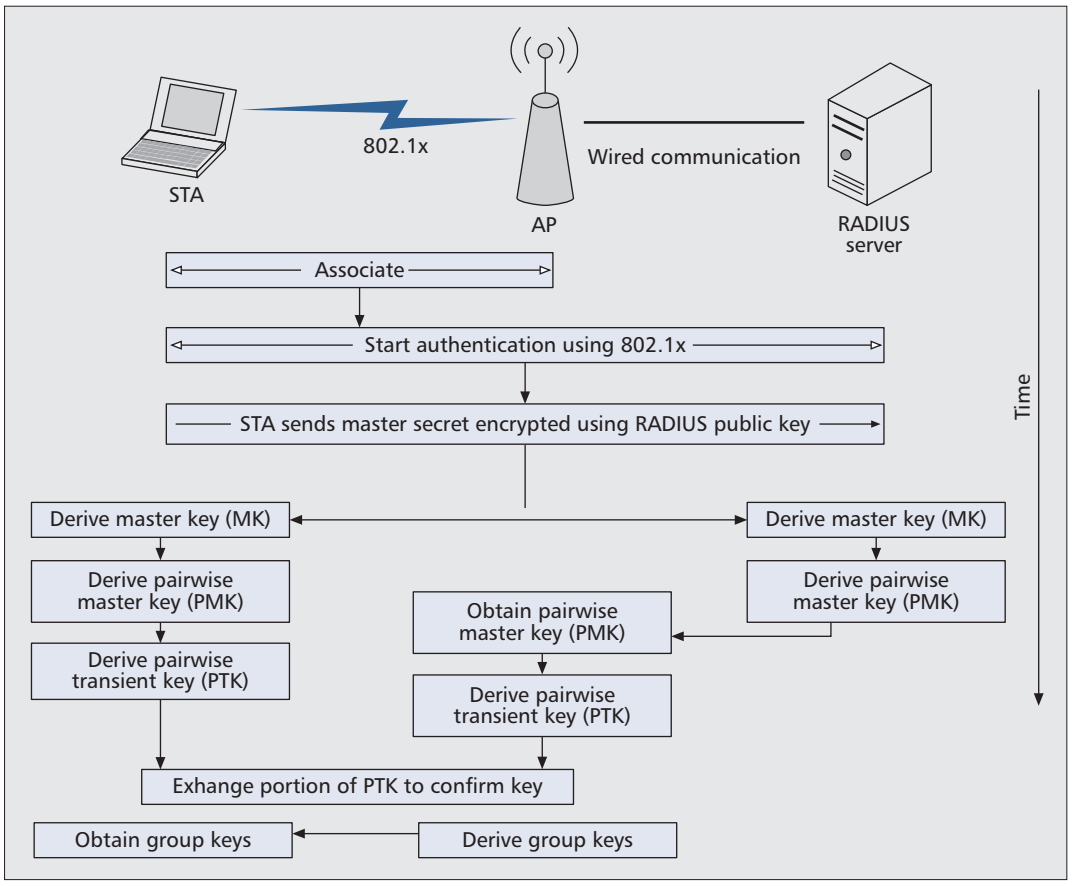


Figure 1. *Overview of 802.1X-based authentication and key distribution.*

In multipath environments, the unique characteristics of the channel between Alice and Bob can enable the creation of a unique secret key between them — a key that cannot be created from any other location.

Throughout our discussion, we shall assume that all of our parties are in listening range of one another. We shall employ the popular security convention of introducing three parties, Alice, Bob, and Eve, who are potentially located at spatially diverse positions, as in Fig. 2. The two legitimate users are Alice and Bob; Alice serves as the transmitter that initiates communication, while Bob serves as the intended receiver. Their nefarious adversary, Eve, may be either a passive eavesdropper or an active adversary that injects communications.

Across the wireless channel, the radio frequency (RF) signal from Alice to Bob is affected by a variety of factors, ranging from attenuation to large- and small-scale fading. Fading arises when a transmitted signal traverses multiple paths that combine constructively or destructively. As a result, fading is largely absent when there is no multipath, such as in deep space. The effect of multipath for a specific transmitter-receiver pair can be represented as a system with a time varying transfer function. In the time domain this transfer function is referred to as the time-varying *channel impulse response* $h(t,\tau)$. While a direct formulation of $h(t,\tau)$ from underlying physics is generally unwieldy, this function is unique between any pair of transceivers, *reciprocal*, and decorrelates very rapidly in space. The decorrelation property implies that if the location of one of the transceivers is changed by an order of half a wavelength, the resulting new channel impulse response will be statistically uncorrelated with the previous one. These properties form the basis for the channel-based authentication and confidentiality services being proposed by the community [2]. We now examine these objectives.

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 to detect anomalous communications. The wireless channel thus provides an additional layer of guarantee against a breach in authentication.

Secret Key Establishment via Multipath Channels — Confidentiality is traditionally achieved through encryption using a shared key. In multipath environments the unique characteristics of the channel between Alice and Bob can enable the creation of a unique secret key between them — a key that cannot be created from any other location. Furthermore, this key can be refreshed often and is independent of the authentication credentials of the users.

These topics are based on the ability of the multipath environment to provide a waveform whose structure an adversary cannot measure or model accurately. Our assumption throughout this article 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. Lastly, we note that the proposed techniques are only suitable

In commodity 802.11 networks, it is easy for a device to alter its MAC address by simply issuing an ifconfig command. This is a dangerous problem because many of the management and control frames in 802.11 networks are not authenticated.

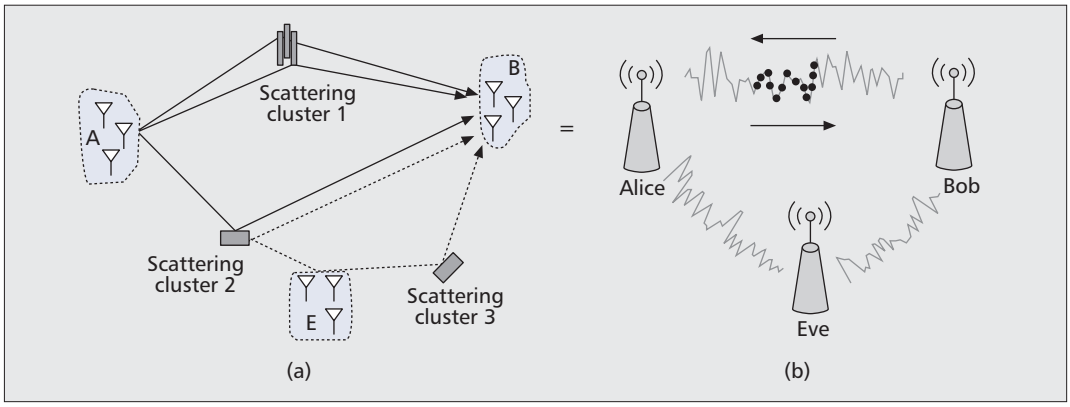


Figure 2. *a) The adversarial multipath environment involving multiple scattering surfaces. The transmission from Alice (A) to Bob (B) experiences different multipath effects than the transmission/reception by the adversary, Eve (E); b) the resultant wireless channel between Alice and Bob is reciprocal — that is, the channel has the same random state if measured in either direction at the same time instant. The channel decorrelates in space, so the Alice-Eve and Bob-Eve channels are statistically uncorrelated with the Alice-Bob channel if Eve is more than an order of a wavelength away from Alice and Bob.*

for channel responses and not gross received power levels, which may easily be affected by anisotropic conditions and adversarial attacks.

Enhancing 802.11 Security Using Channel-Based Authentication

We now show how the security of 802.11 can be improved by providing a form of authentication via the physical layer. It must be noted that such an identification service must be interpreted within the restrictions of the physical layer — it is not possible to verify the identity of a person involved in communication (which must be accomplished at a higher layer). However, wireless authentication can recognize a particular device based on its unique channel characteristics (i.e., authentication of the actual *transmitter*).

Spoofing for DoS in 802.11

Spoofing attacks are very easy to launch in many wireless networks. For example, in commodity 802.11 networks, it is easy for a device to alter its medium access control (MAC) address by simply issuing an `ifconfig` command. This is a dangerous problem because many of the management and control frames in 802.11 networks are not authenticated. This implies that a rogue device can spoof another device by simply changing its MAC address and then cause a variety of DoS attacks. For instance, an attacker can transmit de-association or de-authentication frames, since these are not protected by 802.11i, and thereby cause repeated disruptions in valid 802.11 links. In another variant, an attacker can forge the unprotected EAPOL-Start or EAPOL-Logoff messages in the 802.1X authentication protocol, which would prevent 802.1X authentication from succeeding and disconnecting the supplicant, respectively. Similar DoS attacks are possible on unprotected control frames such as the request to send (RTS) virtual carrier sense mechanism. Each of these attacks is possible because there is no simple means to detect that the transmitter initiating the attack is not in fact the legitimate transmitter.

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 one. To illustrate how the property of rapid spatial decorrelation can be used to authenticate a transmitter, consider a simple transmitter identification protocol in which Bob seeks to verify that Alice is the transmitter. Suppose that Alice sends messages to Bob sufficiently frequently to ensure temporal coherence between successive messages and that, prior to Eve's arrival, Bob has estimated the Alice-Bob channel. Now, Eve wishes to convince Bob that she is Alice.

Bob can use the received 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, Bob will conclude that the source of the message is the same as the source of the previously sent message. Otherwise, Bob should conclude that the source is likely not Alice. Mutual authentication can be achieved by having Alice similarly estimate the Bob-Alice channel using successive transmissions. In one formulation of this problem, the authenticator signal consists of multiple simultaneous carrier tones [3], such as in an orthogonal frequency-division multiplexing (OFDM) system. To ensure independent fading across carriers, the carrier frequencies should be separated by at least the channel coherence bandwidth [1]. Let us suppose that Alice has initially sent Bob N carrier waves. The received tones at Bob allow him to measure $H_i = \tilde{H}_i + z_i$ for $i = 1 \ldots N$, where $\tilde{H}_i$ is the gain of the Alice-Bob channel at frequency f_i, and z_i is the corresponding noise and interference, modeled as a complex Gaussian $\mathcal{N}(0,\sigma^2)$. At a later time, the claimant sends Bob N carrier waves with the same carrier frequencies, and Bob measures the corresponding set of complex gains $\{G_i\}$. The verification process involves testing $\{G_i\}$ against $\{H_i\}$ using a hypothesis testing framework [3]. 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 $\widetilde{G}_i$ has average power γ_E. We may choose 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 [1] and that Eve is several wavelengths away from Alice, we can assume independence between $\widetilde{H}_i$ and $\widetilde{G}_i$. In Fig. 3 we present the probability of detecting Eve vs. the (adversarial) power ratio γ_A/γ_E for a 1 percent false alarm rate with the number of carriers N as a parameter. If we make assumptions on Eve's largest likely channel power γ_E, these results serve as guidelines for choosing the number of carriers needed for reliable physical layer discrimination and authentication. Alternately, if we have limits on N, such as might arise from regulatory or hardware constraints, 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. When Eve has a much larger power γ_E compared to γ_A, the correlator alone performs poorly. However, Eve can then be detected through energy detection techniques because the larger received power of her signal makes it easily distinguishable from the legitimate user's signal.

Physical-layer authentication compares each new measurement with prior channel estimates, thereby verifying whether the new measurement likely came from the source of prior measurements. Even in the absence of an initial cryptographically verifiable association between Alice's identity and her channel response, the physical layer can still detect whether there has been a change in the transmitter. In essence, physical layer authentication is a form of anomaly detection, and thus can be used to detect anomalous spoofed frames in 802.11.

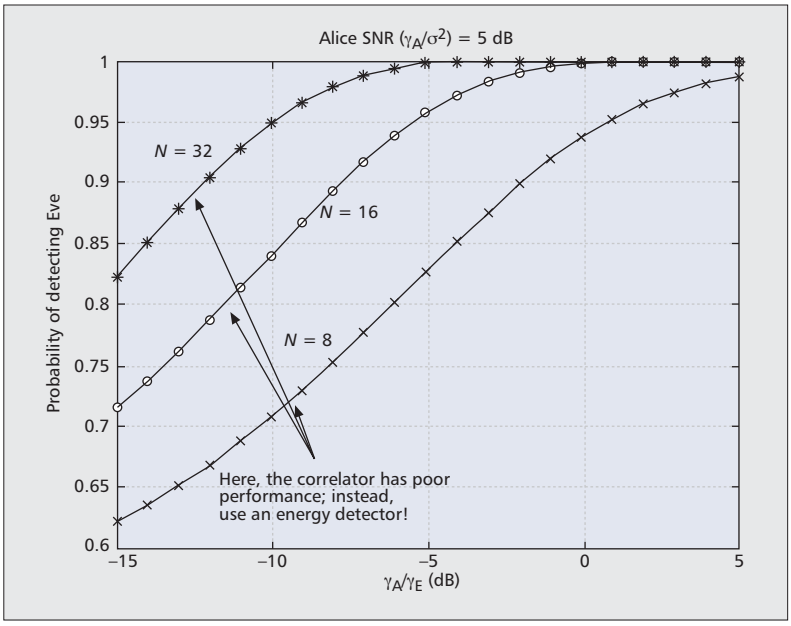


Figure 3. *Probability of detecting Eve as a function of different power ratios.*

Enhancing 802.11i Security using the Physical Layer

Rather than try to design new encryption algorithms, the wireless channel may be used to generate secret bits that can be used as keys for conventional encryption algorithms like the Advanced Encryption Standard (AES). Although such utilization may appear limited at first, it in fact delivers a significant improvement in the security of the baseline crypto-systems and does so precisely in the aspects that traditional (computational) cryptography cannot address.

Overview of Information-Theoretic Secrecy

Our focus is on secrecy extraction schemes. We note, however, that there is a complimentary approach, secrecy dissemination, which has also received attention recently [2, 4, 5]. Referring back to Fig. 2, when Alice transmits a signal to Bob, he receives a signal that is a result of the Alice-Bob channel, while Eve receives a signal that follows from the Alice-Eve channel. In a secrecy extraction scheme, Alice's signal may be a probing signal that Bob uses to estimate channel state information h_{AB}, from which secret bits (keys) are extracted.

In this article we only outline the basic process. The interested reader can find details of the analysis and algorithm design in the references provided. In our discussion we assume that Alice and Bob each have estimates of their shared channel (e.g., by probing the channel repeatedly in a time-division duplex [TDD] fashion). We denote by h_{AB} Bob's estimate of the Alice-Bob channel, and by h_{BA} Alice's estimate of the Bob-Alice channel. Similarly, we denote by h_{AE} Eve's estimate of the Alice-Eve channel. The channel estimates may correspond to scalar or vector quantities.

Secrecy Extraction from Channel Estimates

Once channel state information has been estimated, the process of key extraction is rather straightforward. One simple approach to extracting shared keys employs cryptographic one-way functions [6]. 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 $h_{BA} = h_{AB}$, they have arrived at the same result.

In the ideal situation we would have $K_A = K_B$, and hence Alice and Bob would have a shared key. However, in practice Alice and Bob have slightly different channel estimates. To resolve this difference, Alice and Bob must communicate over a public channel to ensure that they generate identical bit strings. The challenge for them, therefore, is how to communicate publicly in a manner that gives away little of their shared secret and yet results in a common identical key string.

The solution involves simple use of an error correction code. One of the parties, say Alice, simply pretends that Bob's quantized channel observation h_{AB} is obtained by Bob as a result of transmission of h_{BA} by Alice through a noisy channel. (We stress that this is just a thought experiment; in reality, no such transmission has occurred!) The discrepancies between h_{BA} and h_{AB} are due to errors introduced by this (imaginary) channel. Alice's challenge is therefore to correct these errors. This is accomplished by

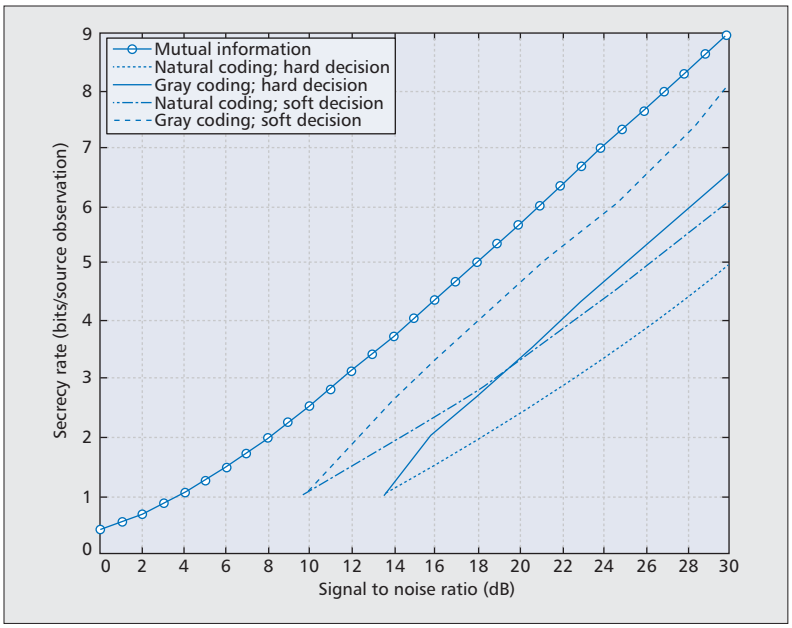


Figure 4. *Secret key rate against SNR.*

transmitting a set of error correction bits generated using an appropriate error correction code. Unfortunately, in transmitting these bits, part of the secret information contained in the h_{AB}, h_{BA} pair is leaked. This problem is eliminated through the use of an appropriate hash function that replaces the one-way function and produces somewhat shorter keys, K'_A and K'_B. Through proper selection of the error correcting code and the hash, we can make sure that K'_A and K'_B are:

- Arbitrarily close to complete secrecy in a strong sense
- Equal with probability arbitrarily close to 1

For a detailed analysis of this procedure, we refer the reader to the seminal work of Maurer [7] and Ahlswede and Csiszar [8]. This work demonstrated that under certain conditions and by using appropriate code and hash functions, the resulting extracted key, $K'_A = K'_B$, is the largest theoretically possible. Over the last decade the ideas developed in [7, 8] have been successfully implemented in quantum cryptography systems. The application to the wireless channel is more recent; however, significant progress has been made. An earlier work [9] demonstrates how many bits may be generated from a flat (e.g., Rayleigh) fading channel. Figure 4, taken from [9], shows both the theoretical limit (mutual information) and the performance attained using simple scalar quantization techniques described therein.

Finally, recent work [10] demonstrated key generation from actual 802.11 channels as measured in a real propagation environment.

Enhancing 802.11i with Channel-Based Secrecy

To demonstrate how the introduction of channel-generated information-theoretic-secret (ITS) bits can improve the 802.11i protocol, we begin with minimal modification. In Fig. 5 we show how a WLAN transmission using PSK authentication mode can be modified using channel-based secrets.

First, as shown on the left of Fig. 5, we vary the 802.11i protocol only slightly. We simply use information-theoretically secure strings obtained as described earlier to derive the PT from the PMK. That is, $PTK = Hash\{PMK, PTK\text{-}old, Info\text{-}in\text{-}the\text{-}clear, ITS\ bits\}$, where the hash is a secure, one-way, many-to-one function. It not only provides computational security for its input as a whole, but makes sure that the presence of ITS bits makes it impossible to deduce PMK with a certainty that exceeds the entropy of the ITS bits. The measurements required to generate the ITS bits can be carried out at any time prior to deriving the PTK (not just after deriving the PMK as shown in Fig. 5).

We now depart from the key hierarchy of 802.11i to show how we might maximize the potential benefits of the ITS bits. The resulting approach is shown on the right of Fig. 5. If 802.1x authentication is used, the AAA server and STA verify each other's credentials, and the STA provides the server with a secret. The AAA server forwards the secret to the AP, and an encryption key (EK) is derived by the STA and AP using the secret and the ITS bit-string. If authentication is PSK-based, the PSK acts as the secret. Part of the EK is used for verification, a second part is used to protect group keys derived later and the remaining part is the portion actually used as the session key. We note that in place of the key hierarchy of 802.11i we simply have the following two sets of keys:

- The pre-shared secret used for authentication
- An intermittently updated EK, which is used for actual data transmission

Let us examine how the proposed scheme addresses the security threats we pointed out in our discussion of 802.11i. Suppose an attacker has been able to gain access to a user's PSK and is eavesdropping on the transmission. With the scheme on the left in Fig. 5, the eavesdropper is able to obtain the PMK, but can go no further since it cannot obtain the ITS bits used to derive the PTK. Similarly, the scheme on the right of Fig. 5 permits the eavesdropper to realize that authentication has transpired, but does not allow it to eavesdrop on actual data being transmitted.

The proposed scheme specifically provides forward and backward security. Since ITS bit strings are constantly generated in time, we are regularly provided with a fresh set of ITS bits that can then be immediately used to derive a new PTK or EK for communication. Thus, even when the key is completely exposed, data is vulnerable only during the period of time it takes to accumulate enough ITS bits for a new key. Finally, we note that attacks where Eve impersonates Alice in the key extraction protocol can be dealt with using physical layer authenticatio, in a manner similar to that in [3, 10].

Concluding Remarks

The selectivity and uniqueness of a wireless channel, along with the fact that the channel decorrelates away in space over distances that are on the order of a wavelength, can allow the channel to be used as a means to prevent spoof-

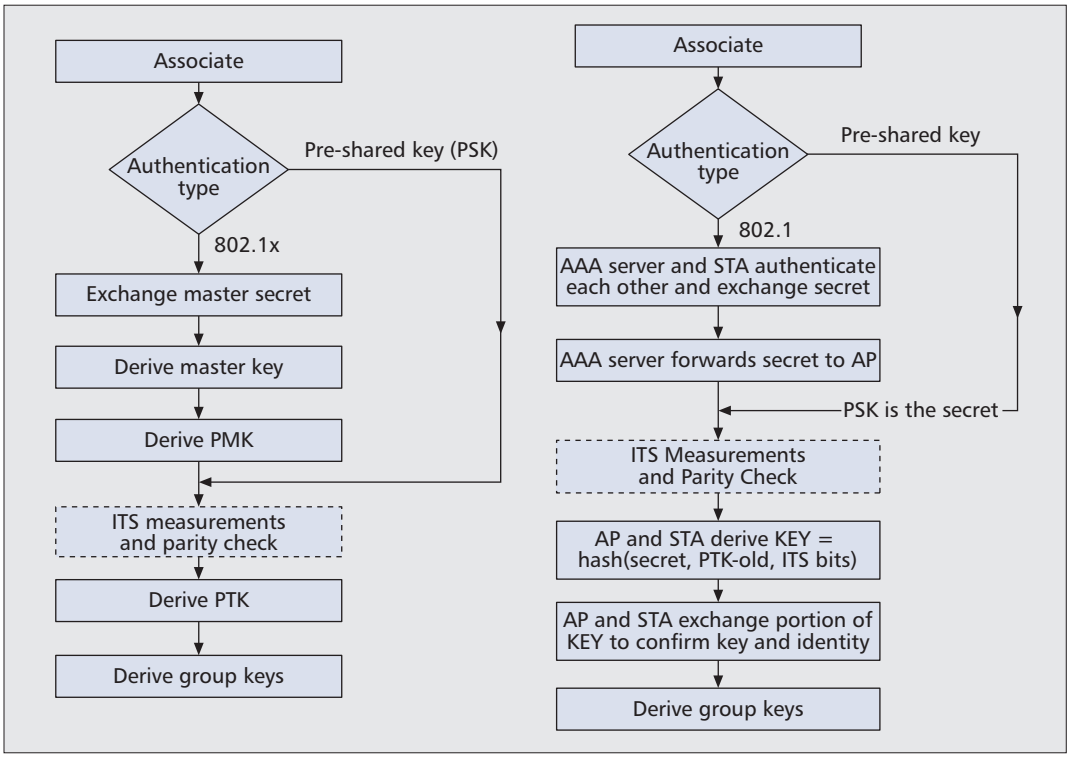


Figure 5. *Enhanced 802.11i protocol.*

The selectivity and uniqueness of a wireless channel, along with the fact that the channel decorrelates away in space over distances that are of the order of a wavelength, can allow the channel to be used as a means to prevent spoofing attacks and thus maintain an authenticator for the legitimate transmitter.

ing attacks and thus maintain an authenticator for the legitimate transmitter. Furthermore, the fact that the channel follows reciprocity allows the collection of highly correlated information, which can be used to extract a string of secret bits for use as cryptographic keying material. Thereby the channel also provides a simple means for enhancing confidentiality services in wireless networks.

Research Challenges

One of the main challenges is the careful integration of physical layer information into existing security infrastructure such that the resultant systems are quantifiably resistant to attacks. Since physical-layer security techniques rely on the randomness inherent in the wireless channel, another challenge that remains is to ensure that, as time evolves, terminals properly adapt to the amount of randomness the channel provides. This may be possible, for example, by estimating the *K*-factor of the channel to distinguish between channels with sufficient multipath from those without. Otherwise, the methods are susceptible to overestimating the level of security.

Finally, a major challenge faced by these methods is to *prove* that the randomness provided by a wireless channel is in fact hidden from a suitably defined adversary. One important direction to explore is the capability of an active adversary to manipulate the phase characteristics of the channel and its estimates in a controlled manner. Critics further argue that modeling the wireless channel can reveal information to a passive adversary. However, randomness in the channel in fact arises from the hardness of acquiring accurate information about the positions and velocities of all scatterers and reflectors, and the extremely sensitive dependence of the channel conditions on these parameters. A relevant direction for security researchers to explore is to relate the underlying security provided by the physical layer with the complexity needed to specify a model that accurately describes the actual realizations of the physical channel. For example, there is no physical layer security in free space, where the actual channel realization is trivial to predict.

References

[1] A. Goldsmith, *Wireless Communications*, Cambridge Univ. Press, 2005.
[2] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*, Springer, 2009.
[3] L. Xiao *et al.*, "Using the Physical Layer for Wireless Authentication in Time-Variant Channels," *IEEE Trans. Wireless Commun.*, vol. 7, 2008, pp. 2571–79.
[4] J. Hershey, A. Hassan, and R. Yarlagadda, "Unconventional Cryptographic Keying Variable Management," *IEEE Trans. Commun.*, vol. 43, 1995, pp. 3–6.
[5] M. Bloch *et al.*, "Wireless Information-Theoretic Security," *IEEE Trans. Info. Theory*, vol. 54, no. 6, June 2008, pp. 2515–34.
[6] A. Menezes, P. vanOorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.
[7] U. M. Maurer, "Secret Key Agreement by Public Discussion from Common Information," *IEEE Trans. Info. Theory*, vol. 39, 1993, pp. 733–42.
[8] R. Ahlswede and I. Csiszar, "Common Randomness in Information Theory and Cryptography, Part 1: Secret Sharing," *IEEE Trans. Info. Theory*, vol. 39, 1993, pp. 1121–32.
[9] C. Ye, A. Reznik, and Y. Shah, "Extracting Secrecy from Jointly Gaussian Random Variables," *Proc. Int'l. Symp. Info. Theory*, 2006, pp. 2593–97.
[10] S. Mathur *et al.*, "Radio-Telepathy: Extracting a Cryptographic Key from an Unauthenticated Wireless Channel," *14th ACM MobiCom*, 2008.

Biographies

SUHAS MATHUR (suhas@winlab.rutgers.edu) received his B.Tech. degree in electrical engineering from the Indian Institute of Technology (IIT) Madras in 2004, and his M.S. degree

in electrical engineering from Rutgers University, New Jersey, in 2006. He is currently working toward a Ph.D. degree at the Wireless Information Networking Laboratory (WINLAB), Rutgers University. His research work spans mobile sensing, wireless networking, and information security. His doctoral research is focused on building practical mechanisms for improving security and privacy in wireless systems. For his Master's thesis he worked on studying cooperation in wireless networks using game theoretic tools. He spent the summer of 2006 working at the Corporate R&D division of Qualcomm Inc. and the summer of 2008 at the Chief Technology Office of InterDigital Inc. He received the best paper award at ACM MobiSys 2010 and the Best Research Presentation Award at Cyber Security Awareness Week at NYU in 2008. His research interests include wireless networks, mobile systems, and the security and privacy challenges arising out of emerging mobile wireless systems.

ALEX REZNIK (Alex.Reznik@interdigital.com) earned his B.S.E.E. from The Cooper Union, his S.M. in electrical engineering and computer science from Massachusetts Institute of Technology, and his Ph.D. in electrical engineering from Princeton University in 1996, 1998, and 2005, respectively. During 2000–2002 he held a MURI fellowship at Princeton University. He has been with InterDigital since 1999 where he is currently a principal engineer in the Advanced Communication Networks Group, leading a number of activities in the area of cognitive radio. His past contributions at InterDigital included technical leadership positions on projects in physical layer security, cellular modem architecture, and advanced receiver design. He holds a visiting faculty appointment at WINLAB, Rutgers University. His research interests are in information and communication theory, and architecture and design of modern communication systems and devices. He is an inventor or co-inventor on over 40 granted U.S. patents, and has been awarded several Presidents and CTO innovation awards at InterDigital.

CHUNXUAN YE (Chunxuan.Ye@interdigital.com) obtained a B.Eng. (Hons) degree in electrical engineering from Shanghai Jiao Tong University (P.R. China), an M.Phil. degree in information engineering from the Chinese University of Hong Kong, and a Ph.D. degree in electrical and computer engineering from the University of Maryland, College Park in 1997, 2000, and 2005, respectively. He has been working at InterDigital Communications since 2005. His research interests are in the areas of information theory, communication theory, and wireless communication systems. These include physical layer security, cooperative and relayed networks, network coding and source coding, wireless system prototyping platforms, and wireless communications networks. He has published more than 20 papers and book chapters. He has more than 12 pending U.S. patents. He is a member of the technical program committee of the 2010 IEEE Sarnoff Symposium. He received the 2006 President's award at InterDigital.

RAJAT MUKHERJEE (rpmukherjee@gmail.com) is a strategy and innovation consultant at a leading global ICT management consultancy. He was awarded a Bachelor's degree in electrical engineering (Honors) by McGill University, Montreal, Canada, and a Master's degree in management science and engineering by Stanford University, Palo Alto, California. His prior work in the telecommunications industry has focused on next-generation access and convergence technologies. His consulting expertise centers around best practices in product and service launch strategies, and innovation research and management.

AKBAR RAHMAN (Akbar.Rahman@interdigital.com) has a Bachelor of Applied Science (mechanical engineering) from the University of Waterloo, Ontario, Canada. He has 27 issued (granted) U.S. patents. He has 17 years of experience in development and standardization in the field of cellular telecommunications.

YOGENDRA SHAH (Yogendra.Shah@interdigital.com) earned his B.Sc. and Ph.D. in electrical engineering from The City University, London, in 1982 and 1985, respectively. He has worked in the wireless industry developing consumer products incorporating wireless technologies from the early CT2 digital cordless telephony standard through to current 3G systems. He has worked as a systems engineer and product developer at various organizations before joining InterDigital. He is currently a manager in the R&D Department at InterDigital with research interests in developing advanced communications modem technologies and wireless security technologies. He is an inventor or co-inventor on several U.S. patents, and has been awarded the President's and CTO innovation awards at InterDigital.

WADE TRAPPE [M] (trappe@winlab.rutgers.edu) received his B.A. degree in mathematics from the University of Texas at Austin in 1994, and a Ph.D. in applied mathematics and scientific computing from the University of Maryland in 2002. He is currently associate director of WINLAB, and an associate professor in the Electrical and Computer Engineering Department at Rutgers University. His research interests include wireless security, wireless networking, multimedia security, and network security. He has led projects involving security and privacy for sensor networks, physical layer security for wireless systems, a security framework for cognitive radios, the development of wireless testbed resources, and new RFID technologies. Recently, his research group has developed several cross-layer security mechanisms for wireless networks, and jamming detection and jamming defense mechanisms for wireless networks, and has investigated privacy-enhancing routing methods for wireless networks. He has published over 100 papers, including two best papers in media security, a best paper on the localization of cognitive radios, and several wireless security papers at premier conferences. His experience in network security and wireless systems spans 12 years, and he has co-authored a popular textbook in the field, *Introduction to Cryptography with Coding Theory*, as well as four other books on wireless systems and multimedia security. He is a member of the ACM.

NARAYAN B. MANDAYAM [F] (narayan@winlab.rutgers.edu) received his B.Tech (Hons.) degree in 1989 from IIT Kharagpur, and his M.S. and Ph.D. degrees in 1991 and 1994 from Rice University, all in electrical engineering. From 1994 to 1996 he was a research associate at WINLAB, Rutgers University, before joining the faculty of the Electrical and Computer Engineering Department at Rutgers where he became an associate professor in 2001 and a professor in 2003. Currently, he also serves as associate director at WINLAB. He was a visiting faculty fellow in the Department of Electrical Engineering, Princeton University in 2002 and visiting faculty at the Indian Institute of Science in 2003. His research interests are in various aspects of wireless data transmission including system modeling and performance, signal processing, and radio resource management with emphasis on techniques for cognitive radio networks. He is a recipient of the Fred W. Ellersick Prize from the IEEE Communications Society in 2009 along with O. Ileri for their work on dynamic spectrum access models and spectrum policy. He is also a recipient of the Institute Silver Medal from the IIT in 1989 and the National Science Foundation CAREER Award in 1998. He is a coauthor with C. Comaniciu and H. V. Poor of the book *Wireless Networks: Multiuser Detection in Cross-Layer Design* (Springer). He has served as an Editor for *IEEE Communications Letters* and *IEEE Transactions on Wireless Communications*. He has also served as a guest editor of *IEEE Journal on Selected Areas in Communications* (Special Issues on Adaptive, Spectrum Agile, and Cognitive Radio Networks, 2007, and Game Theory in Communication Systems, 2008).