Channel Model and Sounding Method Effects on Wireless Secret Key Rates

Brett T. Walkenhorst, Andrew D. Harper, Robert J. Baxley
Georgia Tech Research Institute
Georgia Institute of Technology
Atlanta, GA 30332
brett@gatech.edu; andrewharper@gatech.edu; baxley@gatech.edu

Abstract—**Ensuring data privacy of wireless communication systems has been a challenging problem for various reasons. The simplicity of eavesdropping on wireless transmissions makes the barrier to entry lower for wireless than for wired systems. Due to size and power constraints, wireless systems are sometimes unable to implement the complex cryptographic algorithms that can ensure the privacy of their data, leaving them with weaker schemes that are more easily exploited. However, the wireless security problem has one distinct advantage over the wired problem in that the channel seen by the eavesdropper is not usually correlated with the channel seen by the intended receiver. Recent research in the community has suggested that the randomness inherent in the wireless channel may be exploited to create secret keys dynamically, making simple wireless cryptographic schemes extremely strong and in some applications providing perfect secrecy. In this paper, we present some information theory bounds on key lengths for various wireless channel models and discuss the impact such physical channel-derived dynamic re-keying would have on various applications. We also present some thoughts on proving out the concepts in actual systems.**

Keywords: secrecy capacity, cryptography, wireless secrecy

I. INTRODUCTION

Recent studies have demonstrated the ability of a transmitter/receiver pair (Alice/Bob) to generate secret keys derived from the physical layer channel [1]-[9]. By creating keys in real-time, perfect secrecy (information-theoretically secure) and/or near-perfect secrecy (computationally secure) can be established with a pair of low-cost transceivers. Initial studies demonstrated the potential for secret communication leveraging differences in the Alice-Bob channel and the Alice-Eve channel using Information Theory [1]-[2]. For simplicity in proving the concepts, many of these early studies assumed a binary symmetric channel with fixed probabilities.

More recent papers have investigated key lengths and key rates available in a Jakes' model, which is applicable to a fixed-to-mobile wireless channel model [3] and Rayleigh/Rician fading channels [4]. The work of [3] concluded that the optimal strategy for a given number of channel samples is one that minimizes the channel sounding time. In this paper, we generalize their approach in three significant ways and thereby generate slightly different conclusions. First, we examine the effects of system delays on the number of key bits generated as well as the channel sounding strategies employed. Second, we incorporate correlation effects for arbitrarily long time periods rather than assuming zero correlation outside the coherence interval. Third, we explore the effects of differing correlation functions on the key generation rates available.

Specifically, we consider three distinct channel models (Jakes, Gaussian, and Sinc) using two basic methods of sounding the channel (simultaneous sounding and time division duplex (TDD) with/without delay). Channel sounding is the process of transmitting a known sequence from one node so the other node can estimate the channel response. The results of our analysis demonstrate secret key generation rates available for some of these combinations and draw conclusions about the available secret rates relative to non-secret rates in typical wireless channels. We will conclude with some discussion of implementation of this key generation in hardware systems.

This paper is outlined as follows. In Section II, we briefly introduce the information theory construct for computing key lengths; section III discusses sounding strategies; and section IV describes the channel models we employ. Simulation results are given in Section V with discussion of results in Section VI and conclusions in VII.

II. SECRET KEY LENGTHS

In the wireless eavesdropping channel, we assume that Alice, the intended transmitter, is attempting to communicate with Bob, while a third party, Eve, is attempting to eavesdrop. The signal that Bob sees when Alice transmits x_a is given by

$$y_b = h_{ba}x_a + n_b \tag{1}$$

the signal Alice sees when Bob transmits is given by

$$y_a = h_{ab}x_b + n_a \tag{2}$$

and the signal Eve sees when Alice transmits is given by

$$y_e = h_{ea}x_a + n_e \tag{3}$$

Although Eve may be interested in Bob's transmissions, the problem is symmetric and it is sufficient to analyze Eve's ability to correctly decode Alice's transmissions. In our system model, we introduce the possibility that Bob transmits to enable both Alice and Bob to estimate their channel so they can agree upon a key. The system model described above is depicted graphically in Figure 1.

We assume that $h_{ab} = h_{ba}$ at any given time. While this assumption may be skewed somewhat by variations in the

978-1-4673-2709-1/12/$31.00 ©2012 IEEE

responses of the transceiver hardware of Alice and Bob, we will assume for our analysis that these variations can be accommodated by proper calibration. We also assume that h_{ea} and h_{ba} are statistically independent. This is reasonable if Eve is far enough away from both Alice and Bob. For channels with sufficiently rich multipath, or a significant number of reflections of the wireless signal, this distance is on the order of a wavelength (e.g. 10cm at a carrier frequency of 3GHz). For channels with less multipath, the distance grows. If this distance assumption breaks down in certain scenarios, the available key lengths will be smaller than what is reported here. The values could be computed assuming correlation values between h_{ea} and h_{ba}. To preserve space, we also restrict our analysis to the single input single output (SISO) case or single antenna transmit/receive nodes, though expanding to multiple input multiple output (MIMO) is relatively straightforward. MIMO is a wireless architecture that assumes multiple antennas at both transmitter and receiver. Some examples of similar MIMO extensions are found in [9]-[10].

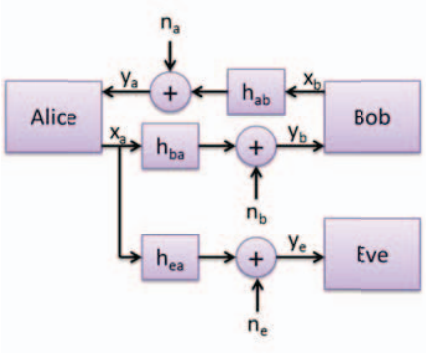

Figure 1. Wireless System Model

Based on this system model, we assume that Alice and Bob both estimate their channels from soundings conducted at discrete intervals. These estimates populate a vector of complex values $\hat{h}_{ab}$ and $\hat{h}_{ba}$ and the number of secret key bits available is given by the mutual information between their estimates (see, for example, [5], [9])

$$K_{abe} = I\left(\hat{h}_{ab}; \hat{h}_{ba} \middle| \hat{h}_{ea}\right). \tag{4}$$

Under the assumption of statistical independence of channels, and assuming that the noise processes are also independent, the estimate $\hat{h}_{ea}$ will yield no information about $\hat{h}_{ab}$ or $\hat{h}_{ba}$, so the number of key bits may be written

$$K_{ab} = I\left(\hat{h}_{ab}; \hat{h}_{ba}\right). \tag{5}$$

If we further assume that the channels and/or noise processes may be approximated by complex Gaussian distributions, and for simplicity in writing the equation, we also assume that $\sigma_a^2 = \sigma_b^2$, we can write

$$\begin{aligned} K_{ab,G} = \log_2\left(\frac{|C_{aa}||C_{bb}|}{|C_{aa\cup ab}|}\right) \\ = 2\log_2|\sigma_h^2\bar{C}_{aa} + \sigma_a^2 I| \\ - \log_2|\sigma_h^2\bar{C}_{aa\cup ab} + \sigma_a^2 I| \end{aligned} \tag{6}$$

where the above covariance matrices are defined as

$$C_{aa} = E\left[\hat{h}_{ab}\hat{h}_{ab}^H\right], \tag{7}$$

$$C_{bb} = E\left[\hat{h}_{ba}\hat{h}_{ba}^H\right], \tag{8}$$

$$C_{ab} = E\left[\hat{h}_{ab}\hat{h}_{ba}^H\right], \tag{9}$$

$$C_{aa\cup ab} = E\begin{bmatrix} C_{aa} & C_{ab} \\ C_{ab}^H & C_{aa} \end{bmatrix}. \tag{10}$$

and $\bar{C}_{ij}$ is the normalized version of C_{ij} such that the maximum correlation coefficient of $\bar{C}_{ij}$ is 1.

To the extent that the channel and noise processes are not well approximated by Gaussian distributions, (6) will yield an upper bound on the number of key bits [11].

The covariance matrices of (7)-(9) are populated using temporal autocorrelation functions of the wireless channel. The specific functions used in our analysis are defined in the next section. The covariance matrix is built from a generic autocorrelation function $R(\tau)$ by

$$C_{ab,ij} = R\left(t_{a,i} - t_{b,j}\right) \tag{11}$$

where $C_{ab,ij}$ is the (i,j)th element of C_{ab}, $t_{a,i}$ represents the ith time at which Alice receives sounding data from Bob, and $t_{b,j}$ represents the jth time at which Bob receives sounding data from Alice. This generic construct can be applied to C_{aa} and C_{bb} by replacing the appropriate letters in (11).

Given (6), we can compute key lengths for an arbitrary set of covariance matrices as a function of signal to noise ratio (SNR). Thus, by selecting a set of channel models with defined autocorrelation functions, we can directly compute key lengths by plugging in correlation coefficients based on the time at which the channel is sounded.

III. Channel Models

The correlation functions in our analysis are derived from three distinct channel models: Jakes (Bessel), Square (Sinc), and Gaussian. These models are among several that are used in various simulation tools and channel emulators and have physical relevance [12]. We assume all channel models to be stationary.

Jakes Model

The Jakes function [13] is a model that is often used to describe the average spectrum resulting from a fixed-to-mobile or mobile-to-fixed channel in a multipath environment with uniform angular scattering. The velocity of the moving node is given by v such that the maximum Doppler shift is $f_m = \frac{vf_0}{c}$ where f_0 is the carrier frequency and c is the speed of light. The temporal autocorrelation function of the channel is then given by

$$R_J(\tau) = J_0(2\pi f_m \tau) \tag{12}$$

where J_0 is the zero-order Bessel function of the first kind.

Rectangular Spectrum Model

The sinc function is used as the temporal autocorrelation function corresponding to a rectangular Doppler spectrum. We define the correlation with parameter β as

$$R_S(\tau) = \frac{sin(\pi\beta\tau)}{\pi\beta\tau} \quad (13)$$

and set $\beta = 2f_m$ to keep the Doppler spread consistent between models. This allows us to define results in terms of velocity for all of our channel models.

Gaussian Spectrum Model

We define our Gaussian spectrum with a Gaussian autocorrelation function with parameter α given by

$$R_G(\tau) = e^{-\alpha\tau^2} \quad (14)$$

where we set $\alpha = \left(\frac{10}{3}\right)\frac{\pi^2 f_m^2}{\log_e 10}$ so that f_m from the Jakes model is at the -3dB point of the Gaussian spectrum, once again giving us a consistent measure of Doppler spread by which to compare the different models.

Model Comparison

For illustration purposes, we plot the autocorrelation functions and Doppler spectra of all three models in Figure 2.

IV. Sounding Strategies

The covariance matrices of (6) are built based on the values of the autocorrelation functions defined above, but those functions are sampled at specific times. Thus, the strategy by which we sound the channel has an impact on the secret key bit rate and we will analyze the following strategies.

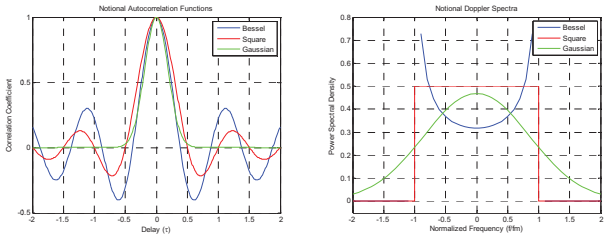

Figure 2. Notional Autocorrelation Functions and Doppler Spectra for Three Channel Models

The first strategy is to simultaneously sound the channel by having both Alice and Bob transmit and receive at the same time. This strategy is unlikely to be implemented in a real system because such simultaneous duplex operation on the same frequency is extremely difficult to achieve. We present these results for completeness and to compare with our other strategy.

We also present results for the case when Alice and Bob take turns sounding the channel by employing time division duplexing (TDD). This scheme allows Alice and Bob to share the channel by alternating their transmissions in time. In the best case, Alice and Bob will swap Tx/Rx modes instantaneously, but realistic effects including electronic switching delays and propagation delay will require an actual implementation to accommodate some finite delay between time slots. We therefore present results in which soundings take place with different delays between slots over a finite period of time.

These two schemes are illustrated in Figure 3 below. The notation Alice->Bob indicates Alice sending a sounding packet to Bob. Free variables in our sounding schemes including the length of the sounding packets and the inter-packet delays.

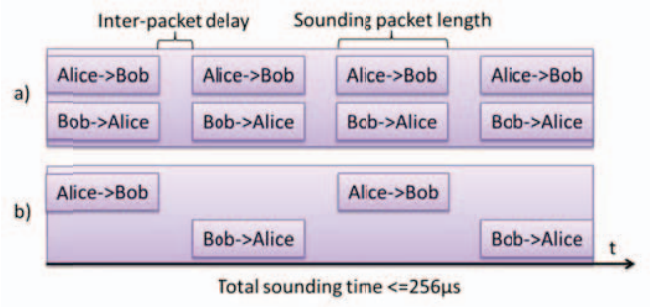

Figure 3. Sounding Strategy Illustrations. a) Simultaneous sounding with variable inter-packet delay; b) TDD with variable delay

Our notional sounding period is 256μs, but in cases where this period results in a non-integer number of sounding packets, the period will be less than 256μs. The resulting key lengths from (6) are then divided by the actual sounding period to yield a secret key rate. This is our metric of interest for the next section, which looks at key rates vs. lengths of sounding packets, channel models, sounding strategies, delays, node velocity, etc.

V. Results

For all scenarios, we assume an SNR of 10dB, a carrier frequency of 2.4GHz, and a sample rate of 1MHz. We compute secret key generation rates in bits/second/Hz using the following parameters: 1) velocities of 0.1m/s to represent stationary nodes, 1m/s for walking speed, 10m/s for residential auto speed, 30m/s for freeway speed, and 90m/s for high speed train; 2) inter-packet delays ranging from 0 to 50μs; 3) packet lengths ranging from 1 to 32μs; 4) channel models as described in Section III and 5) sounding strategies as described in Section IV. The complexity of the parameter space makes it difficult to report on all of the nuances of the results from our model; however, we present several figures to give the reader a sense of the key rates available in some slices of the parameter space we have outlined.

In Figure 4, we consider the impact of the length of our sounding packets on the key rate for the three channel models assuming a velocity of 10m/s, zero delay between packets, and a TDD strategy. For this scenario, the rates are very similar for the different models and longer packets are slightly less efficient than shorter ones.

Although there is value in modeling different Doppler spectra to understand how keys are affected in complex environments, for purposes of this study, we will restrict the rest of our analysis to the Jakes model.

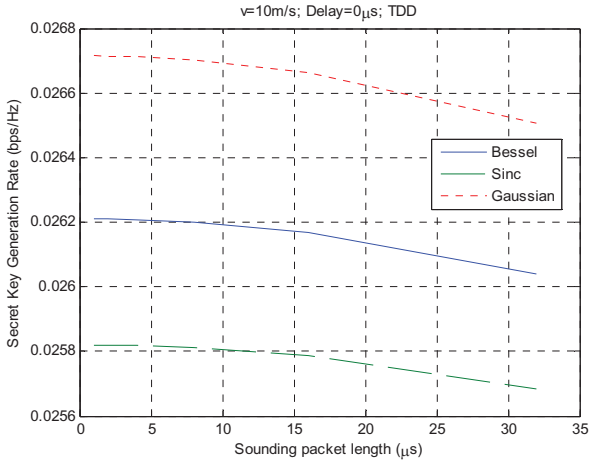

Figure 4. Key rates vs. packet length and channel model

Figure 5 shows key rates versus packet length for different sounding strategies at different velocities. Notice that higher velocities yield higher key rates, which is a trend that will be preserved across all parameter dimensions. Also, simultaneous sounding always outperforms TDD, though we find the assumption of simultaneous sounding to be unrealistic in practice. It is, however, instructive to see how they compare.

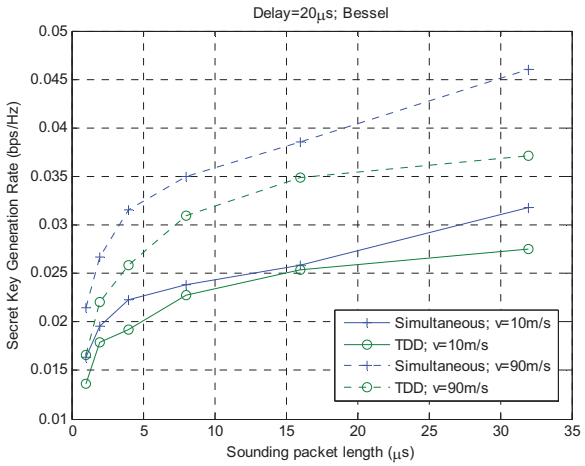

Figure 5. Key rates vs. packet length, sounding scheme, and velocity

Figure 6 shows key rates versus packet length for different velocities assuming a Bessel function, and TDD with 20μs delays between packets. In this case, we see a clustering of performance for low velocities up to 10m/s and then significant increases for higher velocities. We also see a marked increase in key rates with longer sounding sequences for this set of parameters.

Figure 7 shows a similar slice of key rate vs packet length using delay as a second independent variable. We still see increasing efficiency with larger packet sizes except in the case of the zero delay scheme.

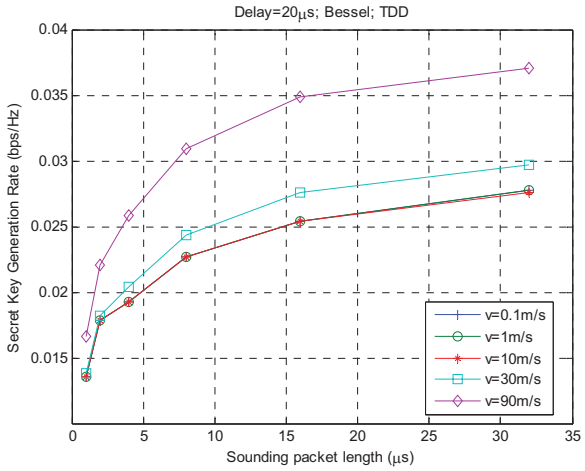

Figure 6. Key rates vs. packet length and velocity

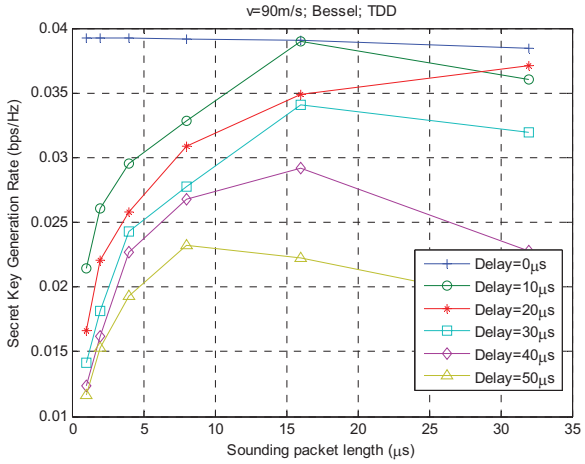

Figure 7. Key rates vs. packet length and delay

Figure 8 shows key rate vs. inter-packet delay. Packet size is a second independent variable. Independent of packet size, it seems wise to keep inter-packet delays as short as possible; however, the impact of such delays is mitigated by longer packet lengths.

Figure 9 shows key rate vs inter-packet delay for various velocities. Interestingly, for the largest packet size, it is helpful to minimize delay at high velocities, but at low velocities, increasing delays can be helpful in improving key rate efficiency.

Figure 10 shows key rate vs. velocity for various delays. Again, we note the value of minimizing delay for high velocities and the benefit of increasing delays for low velocity node pairs.

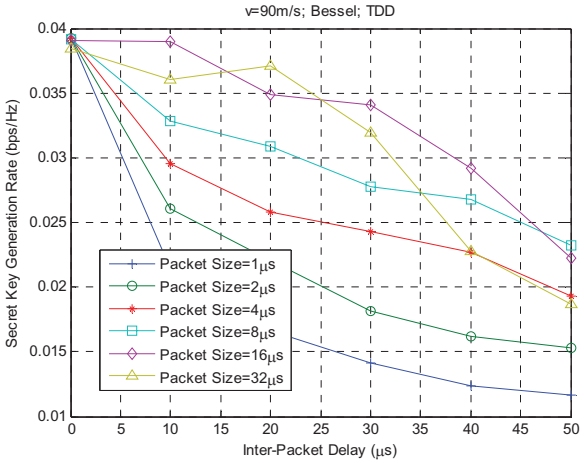

Figure 8. Key rates vs. delay and packet length

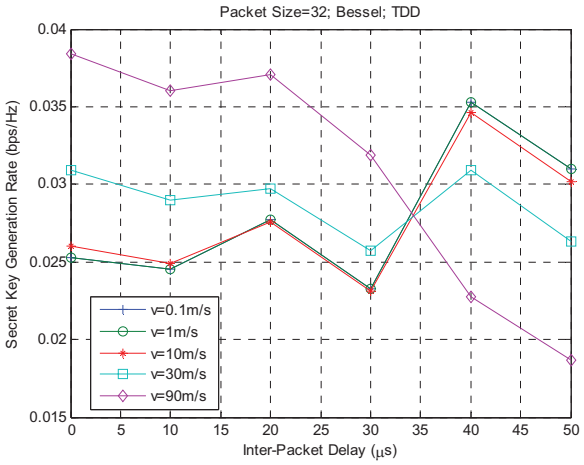

Figure 9. Key rates vs. delay and velocity

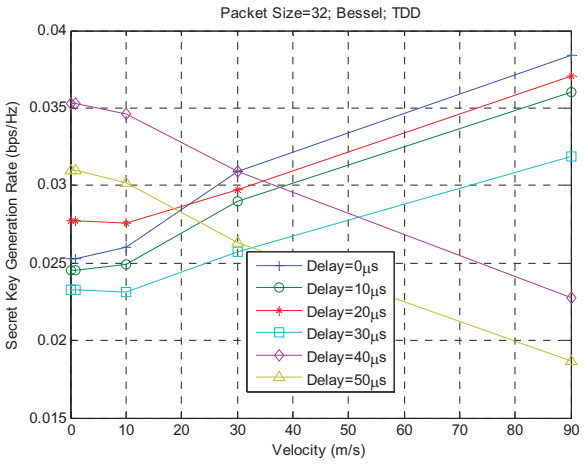

Figure 10. Key rates vs. velocity and delay

Figure 11 shows key rate vs. velocity for various packet sizes, illustrating once again the benefit of longer sounding packets and the value of high velocity in improving key rate generation.

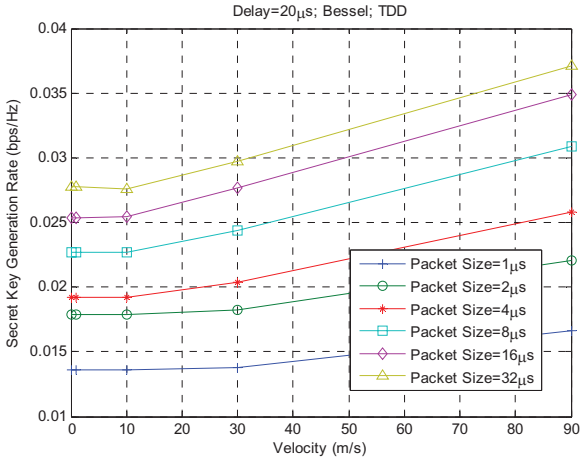

Figure 11. Key rates vs. velocity and packet length

VI. Discussion

Channel Sounding Considerations

According to the model presented here, it seems universally beneficial to have *high velocity nodes* with *minimal inter-packet delay times* and relatively *long packet lengths*; however, there may be some scenarios where this is not the case and channel-targeted modeling should be employed before implementing such a rule in an actual system. Though we did not show different SNRs, key rates grow with SNR similar to the rate at which channel capacity grows.

Notice from Figures 5-7 that longer sounding packets often yield higher key rates than shorter packets; however, Figure 7 clearly shows a knee in the curves where longer packets reduce the available key rate. This can be explained by noting that as the sounding packet length increases, the correlation between packets decreases. However, for very short packets, the noise level becomes the limiting factor in the mutual information between the channel estimates. Accordingly, the key rate has an *optimal packet length* where the noise-reducing benefit of longer packets is balanced with the packet-to-packet decorrelation effects.

Figures 8-10 consider the effect of inter-packet delay on key rates and indicate that *smaller delays* are nearly always correlated with higher key rates. This can be explained by observing that as the Alice-Bob and Bob-Alice soundings are separated in time (packet delay increase), they become more decorrelated. The amount of decorrelation depends on the Doppler spectrum, which depends on the velocity. As the decorrelation increases, the mutual information between channel estimates decreases thereby decreasing the key rate.

Notice from Figures 9-10, that delay has a different effect for different velocities. This is due to the fact that higher speeds induce more decorrelation between nodes for a given delay. As either delay is increased or speed is increased, the decorrelation also increases leading to a reduced key rate.

Implementation Considerations

While high velocities yield higher key rates because of the increased randomness due to evolution of the wireless channel

over time, that same rapid channel evolution also introduces greater ambiguities between the channel Alice estimates and the channel Bob estimates. This is reflected in the model that computes the key rate bound, but this ambiguity presents an implementation challenge independent of the theory presented above. Some practical methods for generating keys and resolving ambiguities have been presented in [4]-[7], but there may be other methods that would work as well or better than what has been offered already. This area of research probably deserves additional attention.

Notice from all of the figures in Section V that with a non-secret channel capacity of 3.46bps/Hz at 10dB SNR, given by $C = \log_2(1 + SNR)$, typical secret key rates are approximately two orders of magnitude lower than non-secret rates.

This leads to the implementation consideration of how much time these soundings should take to generate keys sufficiently long for encryption purposes. Encryption words may utilize a cyclic redundancy check (CRC) to allow Alice and Bob to verify the integrity of their key and data. If this paradigm is employed, key words should be long enough to make it computationally infeasible for Eve to employ a brute force attack. Word lengths on the order of 128, 256, 512, or 1024 bits could be considered. These word lengths are also compatible with many commercial encryption schemes. Based on the 1MHz sample rate of our analysis, approximately 5ms would be required to obtain 128 secret key bits.

This 5ms of sounding would allow the link to transmit secure data for approximately 0.128ms after which another sounding could be conducted. Such a scheme could be *information-theoretically secure* without a CRC by employing the secret word as a one-time pad.

Alternatively, the word could be employed as a key in an existing cryptographic algorithm for a specified period of time after which the sounding would be conducted again to dynamically re-key the crypto algorithm. By this means, we could sound the channel for 5ms to obtain our 128 bit word and use that word for a much longer period of time, perhaps 1s, which leads to minimal overhead while maintaining strong security. In the case of a 1s rekeying rate, the overhead would be 0.5%. This paradigm of physical-layer based dynamic re-keying would not be information-theoretically secure, but could be *computationally secure* while improving the secure data rate over that of the one-time pad significantly. It could also make very weak cryptographic schemes extremely strong by preventing an attacker from accumulating enough data from a single key to reliably break that key. Another advantage to this method is that even if an attacker breaks a single key, subsequent keys are not derived from previous keys and, if created correctly, will be statistically independent from them, making a single key break of limited utility and preserving the privacy of the rest of the data.

VII. Conclusion

In this paper, we have analyzed key generation rates for different channel models using different channel sounding schemes. The effects of parameters were considered including sounding packet length, inter-packet delay, and node velocity leading to observations on optimal strategies for sounding various channels.

Considerations for implementing this key generation scheme in a hardware system were also discussed. Although many studies have been conducted on the theory of physically-derived secret keys, very little has been done to implement these schemes in actual systems. We present this analysis and discussion in part to help motivate additional efforts to do so.

In addition to developing, implementing, and testing practical key generation schemes, studies should also be conducted to identify vulnerabilities in the concept.

References

[1] R. Ahlswede, I. Csiszar, "Common randomness in information theory and cryptography, part I: secret sharing," *IEEE Trans. on Information Theory*, vol. 39, no. 4, pp. 1121-1132, Jul 1993.

[2] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. on Information Theory*, vol. 39, no. 3, pp. 733-742, May 1993.

[3] C. Chen, M. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. on Mobile Computing*, vol. 10, no. 2, pp. 205-215, Feb 2011.

[4] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, N.B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. on Information Forensics and Security*, vol. 5, no. 2, pp. 240-254, Jun 2010.

[5] J.W. Wallace, C. Chen, M.A. Jensen, "Key generation exploiting MIMO channel evolution: algorithms and theoretical limits," *European Conference on Antennas and Propagation*, pp. 1499-1503, Mar 2009.

[6] N. Patwari, J. Croft, S. Jana, S.K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. on Mobile Computing*, vol. 9, no. 1, pp. 17-30, Jan 2010.

[7] Q. Wang, H. Su, K. Ren, K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," Proceedings of IEEE INFOCOM, pp. 1422-1430, Apr 2011.

[8] L. Lai, Y. Liang, H.V. Poor, "A unified framework for key agreement over wireless fading channels," IEEE Trans. on Information Forensics and Security, vol. 7, no. 2, pp. 480-490, Apr 2012.

[9] J.W. Wallace, R.K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: measurement and analysis," *IEEE Trans. on Information Forensics and Security*, vol. 5, no. 3, pp. 381-392, Sep 2010.

[10] C. Chen, M. Jensen, "Encryption key establishment using space-time correlated MIMO channels," *IEEE Antennas and Propagation Society International Symposium*, pp. 1-4, Jul 2010.

[11] T.M. Cover, J.A. Thomas, *Elements of Information Theory*, 2nd ed., John Wiley & Sons, Inc., 1991.

[12] M.K. Simon, *Digital communication over fading channels*, John Wiley & Sons, 2005.

[13] J.G. Proakis, *Digital communications*, 4th ed., McGraw Hill, 2001.