SPATIAL CHANNEL PREDICTION FOR EAVESDROPPING ON WIRELESS FADING BASED KEY GENERATION

Eric Brown, Clara Gamboa, and K. C. Kerby-Patel
University of Massachusetts Boston, Boston, MA
kc.kerby-patel@umb.edu

Physical layer key generation techniques based on wireless channel fading are generally considered to be secure as long as any eavesdroppers are separated from the terminals by a distance greater than the channel correlation length. In fact, this is true only if the channel observations are jointly Gaussian random variables, which is often not the case in real channels. A channel's transfer function is determined by the physical scatterers in that particular channel realization, and information about the legitimate nodes' channel may persist over significantly longer distances than the correlation length if the physical parameters of the channel are slowly varying. Linear prediction has previously been employed to predict samples of the channel transfer function ahead in time. In this work, we demonstrate that it is also possible to predict the channel transfer function ahead in space, over distances larger than the correlation length. This leads to the conclusion that a more pessimistic minimum safe eavesdropper distance for link signature keying is needed.

1 Introduction

It has been demonstrated [1–4] that two parties' reciprocal observations of a fading wireless channel can be used as a common source of randomness to generate symmetric encryption keys in cases where two parties cannot pre-arrange or securely exchange keys. Each party transmits a predetermined waveform, which the other party receives and uses to determine the channel transfer function. These measurements are assumed to be the same in both directions if completed within a short period of time, because of the channel's reciprocity. This technique has been referred to by a number of names, including fading-based key generation and link signature keying. Since the channel transfer function is also position dependent, eavesdroppers at other locations observe a different channel transfer function and the legitimate nodes' channel measurements are usually assumed to be secret. In order for this technique to be useful as a practical encryption method, the secrecy of the channel measurements must be quantified. This work examines how, and under what circumstances, an eavesdropper could predict the channel observations of the communicating parties.

The security claim of link signature keying is based on the assumption that if an eavesdropper is located farther than a correlation length from the communicating parties, it will have essentially no information about the symmetric key generated from their reciprocal

channel measurements [1–5]. Since the channel correlation function in many channels falls off quickly with distance [6], the minimum secure distance is often stated to be a half wavelength. However, mutual information between two channel observation locations may be high even if the channel correlation function is low or has a minimum, since the channel transfer function is a deterministic function of physical environmental parameters such as the amplitudes and phase delays of the scattering paths in the channel. Although the values of these environmental parameters may be unknown to all parties, they often vary quite slowly with distance compared to the correlation function of the channel [6, 7]. The mutual information between the channel parameters at two locations represents an upper bound on the mutual information between channel observations at those locations [8]. Such information may persist over distances longer than the correlation length, so security claims based on the correlation length are inappropriate. In this work, we apply channel prediction techniques [7] to investigate the distance over which it is possible to predict the channel transfer function.

A similar but narrower problem was identified by He *et al*. in [5]. That work pointed out that the correlation functions of some channels have broad peaks in the spatial domain, and link signature keying using such channels is vulnerable to correlation-based attacks based on linear minimum mean-square error estimation. By contrast, the minimum secure distance discussion we present is not based on the width of the correlation function but on the mutual information between separated channel observations, which can persist even when the correlation function is highly oscillatory and has a narrow peak. As a result, it applies to a more general set of channels and is not limited to those with low angular spread. In order to predict a channel with wide angular spread, the eavesdropper in this work is assumed to use a parameter estimation technique.

Section 2 briefly summarizes the argument for a mutual information based minimum secure distance that was presented in [8]. Next, Section 3 outlines a method by which an eavesdropper may apply long-range prediction techniques to a series of spatial samples in order to predict the channel transfer function over distances greater than the correlation length. In Section 4, this technique is applied to a simple simulated channel to examine the dependence of prediction length on the properties of the channel and the eavesdropper array.

2 Mutual Information vs. Correlation

The ability of an eavesdropper to estimate the legitimate nodes' encryption key depends on the mutual information between the eavesdropper's channel observations and the legitimate nodes' observations. In the literature, the channel correlation function is usually used as a proxy for the mutual information. In [8] it was argued that this leads to an inappropriately optimistic minimum secure eavesdropper distance, and an eavesdropper may be able to predict the legitimate nodes' channel observations despite being more than a correlation length away. This section briefly summarizes that argument, which is the motivation for the channel prediction simulation that follows.

If two random variables are jointly Gaussian, their mutual information is a monotonic function of their correlation function. Thus, jointly Gaussian observations of a wireless channel at two locations, $h(\mathbf{r})$ and $h(\mathbf{r}+\mathbf{\Delta r})$, have mutual information given by

$$I(h(\mathbf{r}), h(\mathbf{r}+\mathbf{\Delta r})) = -\frac{1}{2}\ln\left(1 - \frac{R_h(\mathbf{r}, \mathbf{r}+\mathbf{\Delta r})}{\sigma_h^2}\right) \tag{1}$$

where R_h is the correlation function, defined as usual, and σ_h^2 is the average power.

$$R_h(\mathbf{r}, \mathbf{r}+\mathbf{\Delta r}) = E[h(\mathbf{r})h^*(\mathbf{r}+\mathbf{\Delta r})] \tag{2}$$

If the two observations are not jointly Gaussian, the expression given in (1) is merely a lower bound on the mutual information. In general, the channel transfer function at a particular location is a deterministic function of a set of environmental parameters $\boldsymbol{\theta}$ at that location. The environmental parameters may be considered to be a random variable. The data processing inequality can be applied to find that the mutual information of channel transfer function values at two locations with environmental parameters $\boldsymbol{\theta_1}$ and $\boldsymbol{\theta_2}$ is bounded by the mutual information of the environmental parameters.

$$I(h(\boldsymbol{\theta_1}, \mathbf{r_1}); h(\boldsymbol{\theta_2}, \mathbf{r_2})) \leq I(\boldsymbol{\theta_1}; \boldsymbol{\theta_2}) \tag{3}$$

Observations of the channel are given by $\tilde{h}(\boldsymbol{\theta}) = h(\boldsymbol{\theta}) + n$, where n is additive white Gaussian noise. The mutual information between two observations is limited by the mutual information between the channel transfer function itself at those two locations, again by the data processing inequality. Equation (**??**) is further bounded by (**??**).

$$I(\tilde{h}(\boldsymbol{\theta_1}, \mathbf{r_1}); \tilde{h}(\boldsymbol{\theta_2}, \mathbf{r_2})) \leq I(h(\boldsymbol{\theta_1}, \mathbf{r_1}); h(\boldsymbol{\theta_2}, \mathbf{r_2})) \tag{4}$$

If the observations are close enough to each other spatially that the environmental parameter vector $\boldsymbol{\theta}$ does not change appreciably, the upper bound on the mutual information between two observations is the entropy of $\boldsymbol{\theta}$. This means that the two observations may both contain all of the information about the channel parameters.

$$I(\tilde{h}(\boldsymbol{\theta}, \mathbf{r_1}); \tilde{h}(\boldsymbol{\theta}, \mathbf{r_2})) \leq H(\boldsymbol{\theta}) \tag{5}$$

This discussion has provided a lower bound and an upper bound on the mutual information between two observations of a wireless channel. Clearly, significant room remains for variation between the two bounds. However, it has been observed that environmental parameters are slowly varying spatially compared to the channel transfer function and its correlation function [6, 7]. This indicates that information about the legitimate nodes' channel may be available to the eavesdropper even at a distance of more than a correlation length. The correlation length merely indicates that the value of the correlation function is zero at a particular location and does not necessarily predict the availability of information to an eavesdropper.

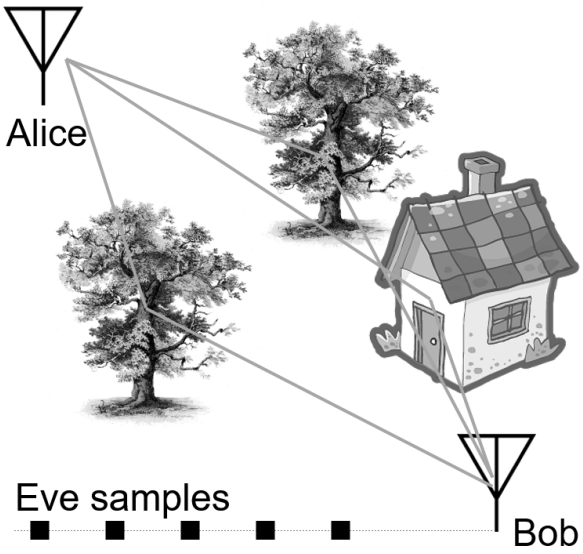

Figure 1: Depiction of an outdoor environment with two transmitters (Alice and Bob) and an eavesdropper (Eve).

3 Spatial Long-Range Channel Prediction Method

As discussed in Section 2, channel information may persist over distances greater than the correlation length. Therefore, long-range prediction techniques as in [7] may be applied to predict the channel from spatial samples. Rather than using long-range prediction to predict the channel transfer function ahead temporally, as is the typical usage, this simulation will use spatial sampling and spectral estimation to discover the channel's parameters and reconstruct its transfer function at a distance.

It is assumed that the eavesdropper has knowledge of the location of one of the legitimate nodes, and has the ability to take a number of spatial samples along a line in the direction of that node. Previous literature has shown that spectral estimation can be applied to a temporal prediction scenario by estimating channel parameters in an assumed channel model, then predicting the channel using the estimated parameters [7]. In experimental implementation with real-world channels, the channel parameters varied slowly enough that this prediction method was accurate within a Doppler wavelength. In this work a prediction length of a few carrier wavelengths—significantly less than a Doppler wavelength—would be sufficient to demonstrate the inadequacy of the half-wavelength minimum safe distance. Therefore, it is reasonable for the eavesdropper to reconstruct the channel with parameter estimation using spatial sampling and spectral estimation.

An example scenario is shown in Figure 1. Alice and Bob are both transceivers. Eve is a passive eavesdropper sampling array in line with Bob. Scatterers are represented by the objects surrounding Alice and Bob. It has been observed that most real world channels

contain less than 10 significant scattering paths [9].

In the simulation of Section 4, it is assumed that the sender Alice and all the scatterers reside in the far field of the eavesdropper array as well as the desired estimation location. The eavesdropper uses direction of arrival techniques to estimate the amplitudes and spatial frequencies of the scattering paths. Once the eavesdropper estimates the channel parameters, it uses them to reconstruct the channel transfer function. The eavesdropper uses a sampling array of length Md, where d is the spacing between measurements and M is the number of spatial samples. The eavesdropper attempts to reconstruct the channel out to a length of $(M + q)d$, where q is number of additional samples between the end of the sampling array and Bob.

Equation 6 describes the channel transfer function along the line of eavesdropper samples.

$$h_m = \sum_{n=1}^{N} \alpha_n e^{-j(k_n)md} \tag{6}$$

Above, h_m is the channel transfer function at the m^{th} location, N is the number of scatterers, α_n is the n^{th} complex amplitude, and k_n is the spatial frequency of that scatterer along the sampling array.

The solution to the parameter estimation problem can be broken into two parts: estimating the wave numbers k_n, then estimating the complex amplitudes α_n. The simulated eavesdropper uses the rootMUSIC algorithm supplied in MATLAB to determine the spatial frequencies of the scattering paths [10]. RootMUSIC uses eigenvalue analysis of the channel's correlation matrix to estimate the signal's frequency content. The specific command used in this simulation takes the sampling results, a threshold value, and a maximum dimension value. The threshold value serves to separate the noise subspace from the signal subspace, while the maximum dimension value sets a number of sinusoids that make up the signal supplied. It then estimates the discrete frequency spectrum, as well as providing the signal power of each frequency component.

In order to determine the complex amplitudes of the scattering paths, the method described in [11] was used. The spectral estimation algorithm determines the spatial frequency of each scattering path. Constant spatial sampling is used, so (6) is simplified by substituting the signal poles z_n for the complex exponentials.

$$h_m = \sum_{n=1}^{N} \alpha_n e^{-j(k_n)md} = \sum_{n=1}^{N} \alpha_n z_n^m \tag{7}$$

Based on the estimated values of the signal poles, the complex amplitudes can be derived by solving the following linear equations. $\boldsymbol{A}$ is a Vandermonde matrix of signal poles, where the M^{th} row contains all the poles raised to the $(M-1)^{\text{th}}$ power.

$$\mathbf{h} = \mathbf{A}\boldsymbol{\alpha} \tag{8}$$

Equation 8 is a system of linear equations of complex amplitude $\boldsymbol{\alpha^T} = [\alpha_1, \alpha_2, ..., \alpha_M]$. The estimated complex amplitudes $\hat{\boldsymbol{\alpha}}$ are then found by solving (8) for $\boldsymbol{\alpha}$ [11].

$$\hat{\boldsymbol{\alpha}} = (\boldsymbol{A^H A})^{-1} \boldsymbol{A^H h} \tag{9}$$

The weakness of using spectral estimation, and rootMUSIC in particular, is the sensitivity to noise in the signal. Direction of arrival applications typically take many snapshots over a span of time and average them to mitigate noise. The simulated eavesdropper is assumed to use this same procedure. The result is an effective signal-to-noise ratio (SNR) increase by a factor of the number of averaged snapshots.

4 Spatial Long-Range Channel Prediction Simulated Results

Section 3 described a plausible channel estimation process for a hypothetical eavesdropper. In this section, a Monte Carlo simulation is used to determine the average maximum estimation distance for the scenario with varying channel parameters. Each value of each variable which shows impact on the estimation outcome is simulated in 1000 randomly generated channel scenarios. An average is assembled for each swept variable in the Monte Carlo. During each of the 1000 runs, the first sample number at which the difference between the estimate and the true channel exceeds 5% of the root-mean-square amplitude of h is recorded. This sample number is the maximum estimation distance. Plots in this section show the average result after completion of the Monte Carlo simulation for each value of each swept variable.

The Monte Carlo simulation tests 7 different variables: M, the number of samples taken; d, the sample spacing in terms of wavelength; N, the number of scatterers; O, the number of observation snapshots; P, the maximum number of sinusoids allowed in the rootMUSIC estimate; T, the threshold value used in the rootMUSIC algorithm to separate the signal and noise subspaces; and SNR, the signal-to-noise ratio.

Each parameter is swept over a reasonable span to determine the estimation's sensitivity to that parameter, with all other parameters held constant in a default scenario. The resultant average sample values are plotted against each swept parameter. The Cramér-Rao lower bound presented in [8] was used to identify suitable parameters for a default simulation scenario. These parameters are: $M = 133$; $d = .3$; $N = 7$; $O = 100$; $P = 33$; $T = 100$; SNR $= 13$dB. The array length in carrier wavelengths with these parameters is 40λ and the averaging raises the effective default SNR to 33dB. For reference, a 1000 iteration Monte Carlo simulation was conducted using the default scenario.The average maximum prediction length past the sampling array was 21λ.

Figure 2 shows the number of samples in the eavesdropper's sampling array. It is evident that the quality of the estimation increases significantly up to 160 samples, then levels off. With the default spacing of $d = 0.3\lambda$, a measurement length of 160 samples corresponds to 48λ. The average maximum prediction length with 160 samples is 130 samples past the sampling array, or 39λ.

Figure 2: Plot showing the increase of samples and array length improving the estimation quality, then deteriorating slightly past 300 samples. $d = 0.3\lambda$ is the default spacing interval

Figure 3: Average maximum prediction length vs. the spacing between samples. The default number of samples in the eavesdropper array in this test is $M = 133$.

Figure 3 shows the average maximum prediction length vs. the spacing between spatial samples. There is a steady increase in the estimation quality of the array as the spacing increases. The number of samples remains constant as the spacing is increased, so the length of the array grows throughout the test. At its optimal spacing of 0.45λ the length of the eavesdropper array is approximately 60λ, with the resulting maximum prediction length being 43λ.

Figure 4 shows how the average maximum prediction length varies depending on the number of scatterers in the scenario. Predictably, additional scattering paths increase the complexity of the estimation problem. With this eavesdropper configuration, there is a smooth drop-off in the quality of the estimation, finally failing to predict past the sampling array at 10 scatterers. This is consistent with the behavior predicted in [8]. Changing aspects of the eavesdropper configuration, such as averaging more snapshots to further limit the noise of the sampled signal, can improve the prediction capabilities past 10 scatterers.

Figure 5 shows how increasing the signal-to-noise ratio of the eavesdropper observations greatly increases the estimation performance and extends the average maximum prediction length. The default value for the simulations in all other tests was 13dB. In all tests, including the swept SNR tests used to generate this plot, the eavesdropper averages 100 snapshots. The averaging produces an additional processing gain of 20dB. Estimation performance drastically improves at SNR values above 24dB (44dB including the gain due to averaging). Signal-to-noise ratio is the most important factor in the effectiveness of the estimation method.

Figure 6 shows the effect of averaging multiple observation snapshots of the same channel realization. This technique has a great impact on estimation quality. Given the ability to take multiple observations the resultant estimation is very accurate. This figure shows that for the default scenario 100 snapshots, which is typical for direction of arrival applications, is sufficient to significantly improve estimation performance, raising the effective SNR to 33db.

The rootMUSIC algorithm uses the threshold value to separate the signal subspace of

Figure 4: Average maximum prediction length vs. the number of scatterers.

Figure 5: Average maximum prediction length vs. SNR.

Figure 6: Average maximum prediction length vs. number of snapshots averaged. At 75 snapshots the estimation reaches the end of the sampling array, and by 100 snapshots the estimation is good enough to predict several wavelengths.

the correlation matrix from the noise subspace. Eigenvalues below the smallest estimated eigenvalue of the signal's correlation matrix, $\lambda_{min} * T$ are assigned to the noise subspace [10]. Figure 7 shows the average maximum prediction length plotted vs. the rootMUSIC modifier threshold. There is a general trend towards better quality of the estimate using higher noise threshold, however the improvement is unpredictable value to value.

Figure 8 shows the effect of the second modifier value for the rootMUSIC algorithm. This value specifies the maximum dimension of the signal subspace. For the default scenario, a value of 20 is optimal for prediction length. The threshold modifier, and to a lesser extent the maximum dimension modifier are both very sensitive to changes in the scenario construction. If the sampled correlation matrix is too small or too large vs. these modifier values the performance of the estimation is severely degraded. Additionally, the performance of the threshold value for a given scenario is extremely uneven, as evidenced by the roughness of the plot in Figure 7.

Figure 7: Average maximum prediction length vs. noise subspace threshold.

Figure 8: Average maximum prediction length vs. maximum dimension of the signal subspace.

5 Conclusion

The simulated results provided here indicate that an eavesdropper could reconstruct the channel transfer function at a particular location from more than a correlation length away by applying long-range prediction to estimate the channel transfer function. This indicates that the minimum safe distance for secure key generation based on wireless fading must be reexamined.

In order to successfully predict the wireless channel at a distance in the scenario constructed here, the eavesdropper must know details about the environment, specifically the location of Bob. Besides this knowledge, the eavesdropper would have to possess a large sampling array on the order of tens of wavelengths in length, and the processing power to conduct the estimation. The situation for the eavesdropper improves with higher SNR, however using the method of averaging used in the simulation that would only be achieved by higher and higher dwell times. So while possible, estimating a channel in this manner is far from trivial.

This work invites investigation of a number of additional questions. The immediate next step is to demonstrate the feasibility of spatial channel prediction experimentally. Future investigations will attempt to identify alternative eavesdropper array geometries and estimation techniques that are more efficient or robust. Situations in which the scatterers are not in the far field of the eavesdropper may require time difference of arrival analysis techniques rather than spectral estimation. Thorough understanding of the potential capabilities of an eavesdropper will lead to strategies that the legitimate nodes may implement for improved security.

References

[1] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, 2007, pp. 401–410.

[2] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless Information-Theoretic Security," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[3] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, 2008.

[4] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-Theoretically Secret Key Generation for Fading Wireless Channels," *Information Forensics and Security, IEEE Transactions on*, vol. 5, no. 2, pp. 240–254, Jun. 2010.

[5] X. He, H. Dai, W. Shen, and P. Ning, "Is link signature dependable for wireless security?" in *INFOCOM, 2013 Proceedings IEEE*, April 2013, pp. 200–204.

[6] W. C. Jakes, *Microwave Mobile Communications*. New York: Wiley and Sons, 1974.

[7] A. Duel-Hallen, "Fading Channel Prediction for Mobile Radio Adaptive Transmission Systems," *Proceedings of the IEEE*, vol. 95, no. 12, pp. 2299–2313, Dec. 2007.

[8] K. C. Kerby-Patel, "Short paper: Effect of non-ergodic channels on wireless fading-based key generation," in *Vehicular Technology Conference (VTC Fall), 2015 IEEE*, Sept. 2015.

[9] A. Duel-Hallen, S. Hu, and H. Hallen, "Long range prediction of fading signals: enabling adaptive transmission for mobile radio channels," *IEEE Signal Processing Magzine*, no. 17, pp. 62–75, 2000.

[10] "Matlab and signal processing toolbox release 2015a."

[11] J. Andersen, J. Jensen, S. Jensen, and F. Frederiksen, "Prediction of future fading based on past measurements," in *Vehicular Technology Conference, 1999. VTC 1999 - Fall. IEEE VTS 50th*, vol. 1, 1999, pp. 151–155 vol.1.