ECE 5510: Secret Key Generation Application Assignments

Neal Patwari, Fall 2009

1 Introduction

During the course of the semester, we will study in depth one emerging technology in wireless network security, called "Secret Key Generation from Multipath Channel Measurements". This technology has the potential to provide future data privacy and security in wireless networks by presenting a way to make wireless data transmissions truly secret, only able to be decoded by the two wireless devices communicating. It allows privacy by having both wireless devices measure an identical secret key from the multipath radio channel that no other wireless device can measure.

The technology is very young and there is a strong potential for discovery. This is an active area of research here at the U. for team of ECE and SoC researchers, since January, 2008. There has been enough research and prototype development to show the feasibility, but there will still be many more improvements before the technology appears in commercial products. These technology improvements may come from better analysis of the multipath radio channel as a random process, and this is a key motivator to use this technology as a motivating application example, throughout the semester.

The secret key generation technology is highly relevant to this class because a huge portion of its analysis and development requires an in-depth understanding of probability and random processes:

1. Time-varying random processes
2. Models for 'noise' as a random process
3. Distributions (marginal, joint, and conditional)
4. Correlation of random variables
5. Filtering of random processes
6. Transformation of random variables

All of these topics are covered in this class. Any material you will need to understand random fading channels will be given to you as well, only for the purpose of understanding the application better.

2 Technology

Shared secret keys are necessary for private communication over a open channel. Public key cryptography has been the most common method for the establishment of such keys. Cryptography is a detailed subject in itself and we don't attempt to cover it in this document or in this class.

Concerns about the limitations of public key cryptography has spawned interest in new methods for key sharing. Public key cryptography can be computationally expensive, because keys must be long enough to prevent even supercomputers from breaking the code; but even

inexpensive wireless devices (such as wireless sensors) must be able to perform encryption and decryption, which increase in computational complexity with the length of the key. Public key cryptography relies on the difficulty of factoring large numbers, which might be simplified in the future using quantum computers. Such quantum computers may provide one alternative to public key cryptography, that is, quantum cryptography. Quantum cryptography does not use public keys, but may only possible for the most cost-insensitive applications.

Shared secret key sharing from radio channel measurements, on the contrary, is very inexpensive and can be done with standard radio devices. In this technology, two nodes communicate on a radio link. During this communication, they measure channel properties. In the simplest case, this measurement is of the path loss of the link over time. The radio channel is reciprocal – this is a property of electromagnetics you would learn in an antennas class. Reciprocity means that at any given time, the loss in the channel from the antenna of node a to the antenna of node b is the same as the loss from b to a. Because of reciprocity, at any given time, the two nodes share a common measurement over time. Figure 1 shows the RSS measured on a link from 'Alice' to 'Bob', and the RSS measured on the link from 'Bob' to 'Alice'. It is clear that they largely agree.

The received power varies in a wireless link because of multipath fading; slight movements in the positions of the two antennas or of the objects in the environment cause the received power to change. You may have had the experience of a cell phone conversation that is audible when you stand still in one position, but fades in and out when you are somewhere else. Or, if you listening to FM radio in your car at a stoplight and the signal is bad, sometimes moving the car forward a foot or two will improve the signal.

Moreover, the measurement of path loss over time is a secret. Measured path loss would be different at a third node e (an eavesdropper). Node e would be unable to make the same measurement that the first or second node did unless it was in exactly the same position as node a or b. Thus, not only is the path loss measurement over time shared by nodes a and b, it can be considered a shared secret. Figure 1 also shows the measurement at node e which can seen to be dramatically different in shape over time.

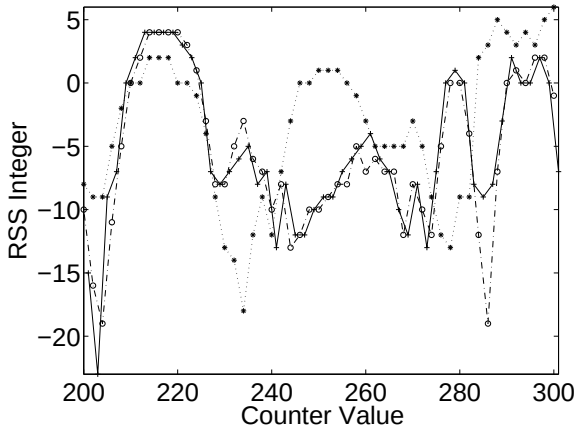

Figure 1: Raw measured RSS Values from a to b (+), b to a (o) and from b to e (*)

Once the first two nodes have measured a shared secret, the problem becomes that encryption of binary data requires us to convert our shared secret measurement (a sequence of measured real-valued path loss values) into a shared secret binary key (a sequence of ones and zeros). This is difficult, first, because we want a shared secret key should have a few key properties:

1. Bits should be equally likely to be a one or a zero.

2. Bits should be independent. Knowing one bit, you should not be able to predict any other bits.

The other big problem with coming up with a binary secret key is that the measurements at the two nodes may be very similar, but they are not in exact agreement, as seen in Figure 1. When we convert them to bits, there will be bit disagreements. If there is even a single bit disagreement in the binary key, the nodes' encrypted messages will not be able to be decrypted by the other node. These disagreements are caused by measurement 'noise'. Although the radio channel is reciprocal, *measurements* of the radio channel are not reciprocal:

1. Additive thermal noise contributes to each measurement as it does in any receiver.

2. The transceiver hardware used by the two nodes are not identical and affect the signal in each direction in a different way.

3. Standard commercial receivers are not capable of transmitting and receiving simultaneously, so measurement from a to b must be half-duplex, *i.e.*, done at a slightly different time than the measurement from b to a.

These random, non-reciprocal elements are referred to as 'noise' and are the ultimate cause of bit disagreements between the secret keys generated at nodes a and b.

The task of converting noisy, real-valued path loss measurements into a binary shared secret key is the task we cover in these application assignments. In each task, you will see how we can use the analytical techniques of probability and random processes in order to achieve a shared secret key which has these features:

1. Bits at the two nodes are agree with high probability,

2. Bits are equally likely to be zeros and ones, and

3. Bits are uncorrelated with other bits in the secret key.

3 Application Assignments in ECE 5510

Probability and Random Processes, in this class, is a set of analytical tools to deal with randomness of the real world. Instruction tends to be abstract, because there are a wide variety of applications of the tools can be applied. I will mention many such examples during lectures in communications, controls, manufacturing, economics, imaging, biology, the Internet, and systems engineering. But this in-depth study of one application is intended to solidify your ability to apply the analytical tools you are learning. More than just knowing that there is an application to security in wireless networks, you will both see first-hand how the concepts apply, and understand the concepts better for having applied them. Further, you will finish with an in-depth understanding of a up-and-coming wireless network security technology.

We will complete six assignments through the course of the semester. Each assignment asks you to apply one or more concepts of probability and random processes to real-world data collected for the secret key generation application.

The units are:

1. Marginal Distribution and Moments

2. Conditional Distribution and Probabilities
3. Joint Distribution and Correlation
4. Transformation of Random Vectors for De-correlation
5. Autocorrelation and Autocovariance
6. Power Spectrum and Filtering

These projects are described in detail on the class web site.