The Creation of Shared Cryptographic Keys through Channel Impulse Response Estimation at 60 GHz

Michael A. Forman
Sandia National Laboratories
P.O. Box 969, MS 9102
Livermore, CA 94551-0969 USA
Michael.Forman@Sandia.GOV

Derek Young
Sandia National Laboratories
P.O. Box 969, MS 9102
Livermore, CA 94551-0969 USA
Derek.Young@Sandia.GOV

ABSTRACT

We propose the demonstration of a research test bed capable of generating private cryptographic keys based on measured wireless channel characteristics at 60 GHz. The test bed is composed of commercial millimeter-wave *VubIQ* transceivers, laboratory equipment, and software implemented in *MATLAB*. Novel cognitive enhancements will be demonstrated, which use channel estimation by correlation to dynamically change system parameters and estimate cryptographic key strength.

Keywords

cognitive radio, symmetric cryptography, channel estimation

1. DEMONSTRATION

The proposed research test-bed demonstration will provide attendees a diverse set of interrelated technologies, including cryptography, channel estimation, cognitive radio, and state-of-the-art 60 GHz physical-layer technology. Because such a system requires a time-varying and complex channel to generate strong cryptographic keys, an interactive session is an ideal demonstration environment. It is hoped that the presentation of a system with such a diverse set of technologies will lead to discussion and possible collaboration with experts in the respective fields.

The required equipment to be supplied by the authors are two tripods with 60 GHz V60DSK02 *VubIQ* transcievers, an HP 8110A Pattern Generator, a Tektronix TDS5104 Sampling Scope, and two laptop computers. Only a single table will be required to hold the equipment and small tripod. The second transceiver will be placed elsewhere in the exhibition hall at a distance of approximately 10 m. The radiated power at the transmitter is a safe 10 mW.

The cognitive key-generation system has been implemented with simulated channels and recently published [1]. The 60 GHz channel-estimation system has been implemented and tested in the field successfully. The authors have recently completed the integration of these systems, replacing the channel simulations with 60 GHz channel measurements. The final work to be done is the implementation of the cognitive functionality and key-strength estimation code. An overview of the key-generation system with simulated channels is provided in the following text.

CCS 2009 Chicago, Illinois USA

2. INTRODUCTION

For a wireless communications link to be secure, it must provide data confidentiality and integrity during transmission. The principal method through which this is achieved is the use of cryptography, of which there are generally two types, public key [2] and private key.

Despite differing characteristics, both methods of cryptography require some form of key-distribution infrastructure responsible for either authenticating public keys or securely distributing private keys. Because in some deployment scenarios such an infrastructure can be cost prohibitive or logistically impossible, several alternative methods of managing cryptographic keying variables have been proposed, one of which utilizes the communications channel as a keying variable [3]. This solution eliminates the need for a key-distribution infrastructure, in that private keys are generated during communications, using shared physical information between two nodes.

In the research test bed, we will demonstrate a system with novel cognitive enhancements which generates private keys using the measured response of channel at 60 GHz.

3. CHANNEL CHARACTERISTICS

Stated simply, a communications channel is the medium between a transmitter and receiver. Information is conveyed over this channel by varying a metric, such as voltage or phase, over a domain, such as space, time, frequency, or polarization. For example, AM radio is broadcast in free space (medium), and carries its information on a carrier that varies in amplitude (metric) over time (domain).

If a channel is passive and isotropic (linear), it possesses the property of being reciprocal.Specifically applied to wireless systems, if two antennas transmit an identical signal, then the received signals will also be identical [4], [5]. It is this quality of reciprocity which is exploited to generate the shared information used to create a private key.

It is also required that the communication channel be uncorrelated with the channel of an eavesdropper and sufficiently complex that the time required to deduce the channel characteristics are on the order of the time necessary to do a brute-force search for the cryptovariable. For a static channel, the lifetime and strength of the cryptovariable is thus related to the complexity of the channel. Channels which vary in a metric over a domain (such as power over time), provide a source of entropy from which keys can be derived continuously. Provided the generation rate is in excess of the time necessary to do a brute-force search of the cryptovariable, the

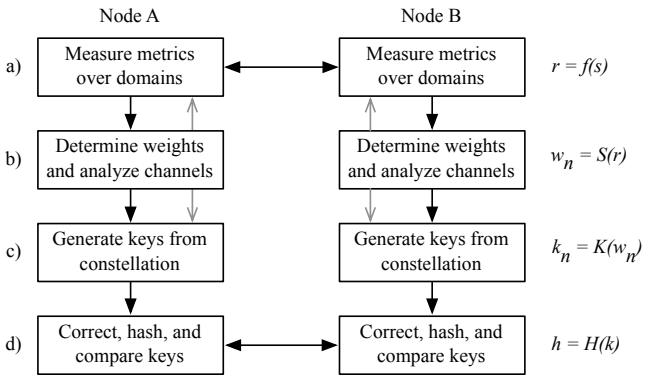

Figure 1: A generalized scheme for the creation of shared private keys through uncorrelated reciprocal channels in multiple domains. In (a) a signal, s, is transmitted across one or more channels in one or more domains and is received as a modulated signal, r. One or more domain-varying metrics, w_n, are measured (b) and converted to key symbols, k_n, using a key-generation function (c). The resulting key is error corrected and checked for agreement between nodes (d).

only requirement on the system is that an eavesdropper not share a correlated channel. This suggests that wireless transmissions have great potential for the generation of private keys from reciprocal transmissions.

4. SIMULATED SYSTEM

An activity diagram of the implemented system is shown in Figure 1. System activity can be broken down into four principal steps. In step (a), a signal, s, is pseudorandom sequence is transmitted across one or more uncorrelated channels. Channel complexity and variation modulate this signal and upon reception and correlation the impulse response of the channel is estimated, r. In step (b), these measures are scaled and converted to one or more multidimensional weights, w_n. It is at this step that the channels are characterized, the result of which are cognitively fed to the preceding and following steps to change the transmission and reception parameters. In step (c), weights are converted to key symbols, k_n, using a key-generation constellation. In step (d), the final key is corrected, hashed, h, and verified.

4.1 Channel Variability

Wireless signals exchanged by a pair of nodes simultaneously over a reciprocal channel will experience identical multipath fading. This fading is in essence a modulation of the carrier that conveys information about the physical state of the channel. Upon reception, this information can be extracted by measuring channel metrics over domains absolutely or differentially.

There is a well understood relationship between the size of a cryptovariable and the resources required to perform a brute-force search for it. Despite this, a system which uses the environment as a keying variable must set a key expiration time that is at most the time required to do a brute-force key search or at least the time required to solve for the channel. In short, a simple environment generates weak keys and a well implemented system must take this into consideration. Indeed, even a generalized system with access to all domains without limit, suffers from degenerate environments, such as free space, where channels provide no information (complexity or variation) for key generation.

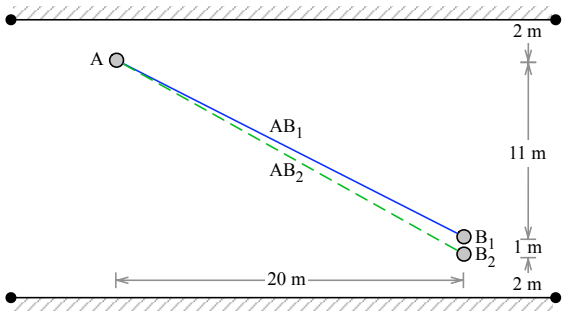

Figure 2: This simulated system represents communication across and down a street between two buildings. Only the principal ray is shown, however rays that reflect between the structures, up to the convergence point of ten reflections, are included in the simulation.

4.2 Measurement and Cognition

After transmission through and modulation by the channel, a signal is measured as metrics over domains. These metrics are then conditioned through optional linearization or normalization and stored a weights. These weights serve as inputs into a key-generation function or constellation to produce key symbols.

Because the strength of the private key is a direct function of the complexity and variability of the communication channels, the radio which uses the channel as a keying variable must be aware of the state of the channel at all times. Principally, this state information provides a method to estimate the strength of the generated keys and their expected expiration times. Secondarily, the state of the channel can be fed backwards into the preceding components to dynamically change sampling and forward into the following components to modify constellations. Such adaptive features, however, require communication and agreement between both nodes and is considered a method to improve data extraction as opposed to increasing key strength.

4.3 Constellations

A key-generation function or constellation is a mechanism that converts measured weights into key symbols using constellation points or regions. Key symbols represent one or more bits which are combined to form a complete key. In the generalized scheme, a constellation space has one or more dimensions and is addressed with a vector comprised of one or more weights.

With either a function or constellation, it is important to normalize and linearize a metric such that the probability of a weight appearing in each region is equal. A metric refers to the value as measured, whereas a weight is a normalized and linearized value for use in a keying function or constellation such that it provides equal probability of returning any symbol.

4.4 Key Correction and Expiration

After generation, one or more keys are corrected and compared between nodes while maintaining key secrecy. Previously published systems utilize both well-understood algebraic decoding methods [6] and more novel methods such as fuzzy information reconciliators [7]. For the algebraic decoding method, keys are padded with known data and a syndrome is generated and exchanged between nodes. Depending on the algorithm and the syndrome size, such a scheme allows for the correction of several erroneous bits in a key. After correction, final agreement of the keys is checked by

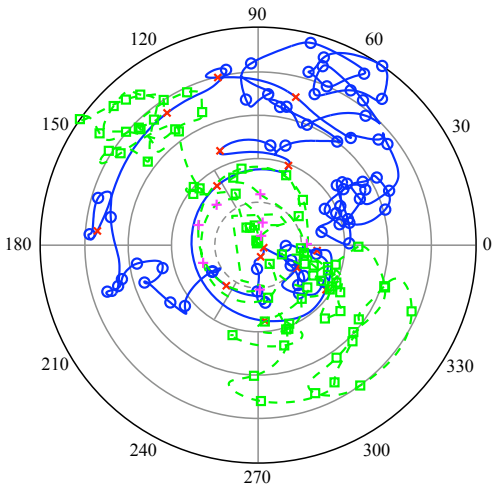

Figure 3: The simulated system uses a constellation with sixteen regions. For low carrier amplitudes that correspond to regions of rapid phase change, regions with reduced or no phase divisions are used. The path followed by the weights over frequency demonstrates qualitatively that the channels are uncorrelated.

comparing a one-way hash of the private keys [8].

One of the more important contributions a cognitive system can provide to a key-generation system is an estimate of key strength and thus expiration time. Although an adversary's knowledge of the environment, including locations of eavesdroppers, cannot be known, it is possible to measure metric variations over each domain. This metric variation can be quantified as a domain coherence, such as coherence time or coherence bandwidth for amplitude fading. This measure is used to estimate the key strength and set expiration times. The exact relationship between these metrics and key expiration time is dependent on the implementation of each system.

5. PROOF OF CONCEPT

A physical system is modeled in *MATLAB* using a two-dimensional ray-tracing code with the topology shown Figure 2. This simulated system represents communication across and down a street between two buildings. Although only the principal ray is shown, the model includes reflections between the reflectors, up to the convergence point with a maximum of ten reflections. Two nodes, A and B, are separated in the simulation space, with node B having two antennas, B_1 and B_2, which are placed in close proximity.

The channel is simulated between 2.4 and 2.6 GHz with a 200 MHz or 8 % working bandwidth, a realistic figure for a communications system. The separation between the antennas of node B is 1 m, which at the center frequency of 2.5 GHz is approximately 8.3λ. By means of the channel impulse response, the coherence bandwidth of both channels is calculated to be 320 kHz. The frequency step size is dynamically set to approximately eight times this value or 2.5 MHz, yielding a total of 80 frequency points over the bandwidth at which metrics are measured.

The magnitude and phase of the received carrier are measured at the sample points.To be suitable as weights which are combined to form vectors to access symbols in the constellation, the metrics are conditioned. The magnitude of the received signal is normalized and scaled. The phase is unrolled, removing the phase change due to the frequency sweep and is similarly scaled.

Figure 3 shows the path of the vectors over the constellation in frequency, with the location of the sample points marked. There are 80 sample points for each of the two paths through the constellation, generating a total 640 b in a single time step. It can be seen qualitatively that the the vectors vary over the constellation space randomly and appear uncorrelated. A runs test in MATLAB confirms this, returning a p-value of 0.09. This demonstrates that a random shared key can be generated in a single time step by measuring multiple metrics over the frequency domain.

6. CONCLUSIONS

Methods to generate private keys based on wireless channel characteristics have been proposed as an alternative to standard key-management schemes. In this paper, we present a generalized scheme for the creation of private keys using uncorrelated channels in multiple domains. Proposed cognitive enhancements measure channel characteristics, to dynamically change transmission and reception parameters as well as estimate private key randomness and expiration time. We evaluate a proof-of-concept implementation of this system with and without interferers in software using a channel model that provides variation in multiple domains.

7. ACKNOWLEDGMENTS

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2009-1716C approved for unlimited public release.

8. REFERENCES

[1] M. A. Forman and D. Young. A generalized scheme for the creation of shared secret keys through uncorrelated reciprocal channels in multiple domains. *International Conference on Computer Communications and Networks*, August 2009.

[2] R Rivest, A Shamir, and L Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, Jan 1978.

[3] J Hershey, A Hassan, and R Yarlagadda. Unconventional cryptographic keying variable management. *Communications*, Jan 1995.

[4] Constantine A. Balanis. *Antenna Theory: Analysis and Design*, chapter 1. Harper & Row, New York, 1982.

[5] G Smith. A direct derivation of a single-antenna reciprocity relation for the time domain. *IEEE Transactions on Antennas and Propagation*, Jan 2004.

[6] S. Lin and D. Costello. *Error Control Coding: Fundamentals and Applications*. Prentice-Hall, Englewood Cliffs, NJ, 2004.

[7] B Azimi-Sadjadi, A Kiayias, A Mercado, and B Yener. Robust key generation from signal envelopes in wireless networks. *Proceedings of the 14th ACM conference on Computer and communications security*, Jan 2007.

[8] T Hashimoto, T Itoh, M Ueba, H Iwai, H Sasaoka, K Kobara, and H Imai. Comparative studies in key disagreement correction process on wireless key agreement system. *Lecture Notes in Computer Science*, 4867:173, 2007.