SAND REPORT

SAND2010-6662
Unlimited Release
Printed September 2010

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

Michael A. Forman, Derek Young, and Donald R. Dowdle

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@adonis.osti.gov
Online ordering:	http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.fedworld.gov
Online ordering:	http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2010-6662
Unlimited Release
Printed September 2010

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

Michael A. Forman, Derek Young, and Donald R. Dowdle
Sandia National Laboratories
P.O. Box 969
Livermore, CA 94551-0969 USA
Michael.Forman@Sandia.GOV

Abstract

Methods to generate private keys based on wireless channel characteristics have been proposed as an alternative to standard key-management schemes. In this work, we discuss past work in the field and offer a generalized scheme for the generation 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 times.

Finally, results are presented on the implementation of a system for the generation of private keys for cryptographic communications using channel impulse-response estimation at 60 GHz. The testbed is composed of commercial millimeter-wave VubIQ transceivers, laboratory equipment, and software implemented in MATLAB. Novel cognitive enhancements are demonstrated, using channel estimation to dynamically change system parameters and estimate cryptographic key strength. We show for a complex channel that secret key generation can be accomplished on the order of 100 kb/s.

Acknowledgment

Sandia National Laboratories is a multiprogram laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Contents

Figures

Tables

This page intentionally left blank

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

Generalized System

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 [1] and private key [2].

Public-key cryptography is a method for secret communication between two parties without the requirement of an initial exchange of secret keys. It employs a pair of keys, one private, which is held secret, and one public, which is distributed. Messages are encrypted with the recipient's public key and decrypted with the recipient's corresponding private key. Public-key cryptography is thus relatively unencumbered with key-exchange difficulties and key-interception vulnerabilities, however it is computationally intensive.

Private-key cryptography is a method for secret communication between two parties that requires an initial exchange of a single shared secret key. Messages are encrypted by the sender and decrypted by the recipient using this same shared key. Private-key cryptography is less computationally intensive than public-key cryptography, however key distribution and management are problematic. Key distribution risks that the secret key will be intercepted during transmission. Key management requires the generation and transport of a different key for each communicating party [3].

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 [4]. 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 this paper, we discuss the properties of wireless channels that enable this technology, prior work on the use of a channel as keying variable, and present a generalized scheme for the generation of private keys using uncorrelated channels in multiple domains. We follow with a proof-of-concept demonstration of the generalized scheme using a ray-tracing channel model that provides variation in multiple domains, basic channel cognition to optimize performance, and estimations of encryption key strength. Finally, we conclude with a demonstration of how cognitive radios can respond to narrow- and broad-band interference from primary users occupying a channel.

Table 1. Characteristics of Cryptographic Methods

Measure	Private Key	Public Key
Computation	light	heavy
Distribution	private	public
Interception	easy	difficult
Management	difficult	easy

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 [5]. Specifically applied to wireless systems, if two antennas transmit an identical signal, then the received signals will also be identical [6], [7]. 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 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.

Related Work

Using a reciprocal channel as a source of shared information to generate private keys has been demonstrated in a variety of systems that measure different metrics over various domains. In [4] and [8] the authors propose a system where each radio transmits two or more unmodulated carriers at orthogonal frequencies and the phase differences between the observed carriers are used as the source of common information. In [9], the polarity of carrier envelope samples of a narrowband signal is used to generate a private key. In [10], threshold magnitude carrier variations in time and frequency are measured. In [11] and [12], threshold magnitude-only signal-strength variation is measured in time with pseudorandom variation added via switched parasitic antenna elements [13], [17]. In [14], an ultra-wideband pulse is used to measure the channel impulse response in time. In [15], the authors present a MIMO system with two antennas per node which generates bits for a keying variable based on which antenna receives the stronger signal. In [16], threshold

Table 2. Metrics and Domains of Variation

Measurement		Variation		
Metric	Domain	Metric	Domain	System
differential phase	time frequency	-	-	[4], [8]
signal polarity	time	-	-	[9]
magnitude	time frequency	function	time	[10]
magnitude	time	gain function	angle time	[11], [12], [13]
impulse response	time	-	-	[14]
differential magnitude	time space	-	-	[15]
magnitude	time	-	-	[16]

detection of deep fades in signal strength is measured in time.

All systems exploit reciprocity to generate a private key. All systems generate keys in time, with two systems also using frequency or space. All systems measure a single metric, with most using carrier magnitude. All systems employ a binary constellation (two-state threshold or differential) to convert measured metrics into key bits. All systems have a constant sample period or bandwidth. Two systems provide pseudorandom variation of static channels. A summary of measurement and variation metrics and their corresponding domains for each system is shown in Table 2.

Generalized Scheme

A generalized scheme for a system that uses the channel as a keying variable assumes that a pair of nodes are capable of accessing all channels in all domains without limit. For example, such a system would have the ability to measure polarization over a complete sphere, vector signal strength over all of frequency, or relative phase between any two points in space. In actuality, a realized system will be limited by the capabilities of its hardware and thus its ability to respond to and extract data from the channel. However, a general analysis is useful as a means to better understand how a cognitive radio can access, measure, and exploit multiple metrics in multiple domains to generate private cryptographic keys.

An activity diagram of a generalized system is shown in Figure 1. System activity can be broken down into four principal steps. In step (a), a signal, s, is transmitted across one or more uncorrelated channels. Channel complexity and variation modulate this signal and upon reception several metrics over several domains are measured as the signal, r. In step (b), these metrics 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 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 function or constellation. In step (d), the final key is corrected,

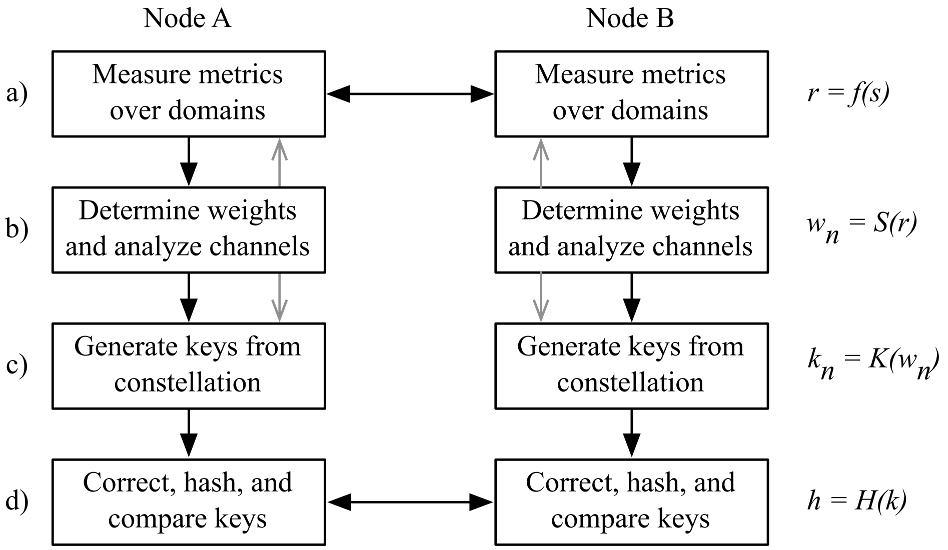

Node A
Node B
a)
Measure metrics over domains
Measure metrics over domains
r = f(s)
b)
Determine weights and analyze channels
Determine weights and analyze channels
w_n = S(r)
c)
Generate keys from constellation
Generate keys from constellation
k_n = K(w_n)
d)
Correct, hash, and compare keys
Correct, hash, and compare keys
h = H(k)

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).

hashed, *h*, and verified. The following sections discuss the measurement of metrics over a domain, the channel characterization for system feedback, the keying functions used to convert weights to key symbols, and the correction, hashing, and comparison of keys.

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. For instance, in a given channel one can measure the variation of carrier magnitude (metric) over time (domain) or relative carrier phase (metric) between many antennas over space (domain). In essence, the received carrier is demodulated by the system and the resulting information is used to create a shared cryptographic key. The amount of information that a system can extract from the environment is a function of the channel's complexity and the number uncorrelated channels that a radio can access.

In previously published work, time is the primary domain over which channel metrics are measured to generate keys. Although two systems pair time with an additional domain, it is entirely possible to exclude time altogether to generate one or more keys in a single time step. Additionally, the system can monitor the state of many channels in multiple domains to select uncorrelated varying channels. For carrier amplitude fading, this variability can be quantified in time, frequency, or space by measuring the coherence time, coherence bandwidth, or coherence length [18].

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.

One solution to this problem is independent reciprocal pseudorandom variation of the channel by individual nodes. That is, each node without knowledge of the state of the other node can introduce pseudorandom reciprocal variations in the carrier of transmitted signal over any domain. Such a capability has been demonstrated in a system that varies antenna gain over time [11], [12]. Note that the variations must be independent as it is a tenet in cryptography that an adversary is presumed to be in possession of the encryption algorithm and that security rests solely on the secret key. Thus it is not sufficient for two nodes to reorder data using a shared function, such as interleaving [11], [12], as this algorithm is considered to be known. A summary of pseudorandom metric variations over domains is shown in Table 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. In all previously demonstrated systems, the domain sample sizes (sampling rate or bandwidth) is constant. Systems instead attempt to correct errors due to slowly or rapidly varying channels by skipping or interleaving redundant data and error-correction algorithms respectively.

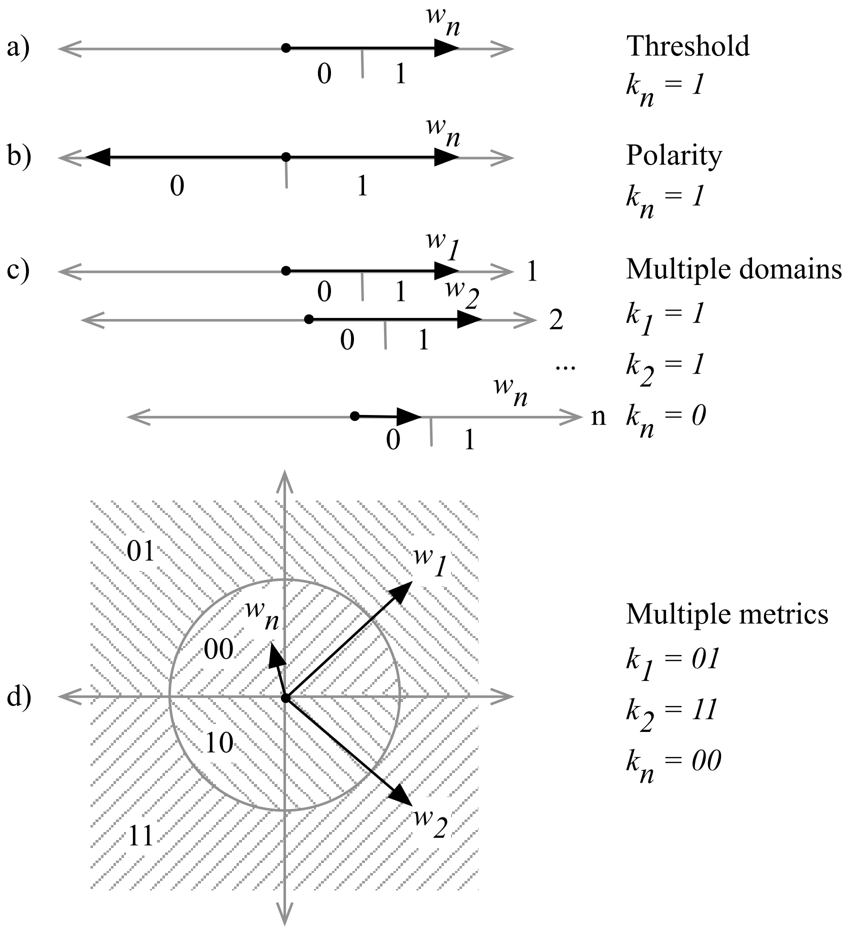


Figure 2. Previously demonstrated systems utilized a single metric converted directly to binary using threshold magnitude (a), signal polarity (b), or thresholds (c) at several frequencies. With with the measure of multiple uncorrelated metrics over multiple domains, a multidimensional constellation (d) can be utilized.

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.

All previously demonstrated systems convert a single metric directly to a single key bit by using a magnitude- or polarity-threshold keying function. While constellations are not discussed, these magnitude-threshold functions are equivalent to a one-dimensional constellation with two binary symbols, as shown in Figure 2a and 2b. The system demonstrated in [10] extends this paradigm

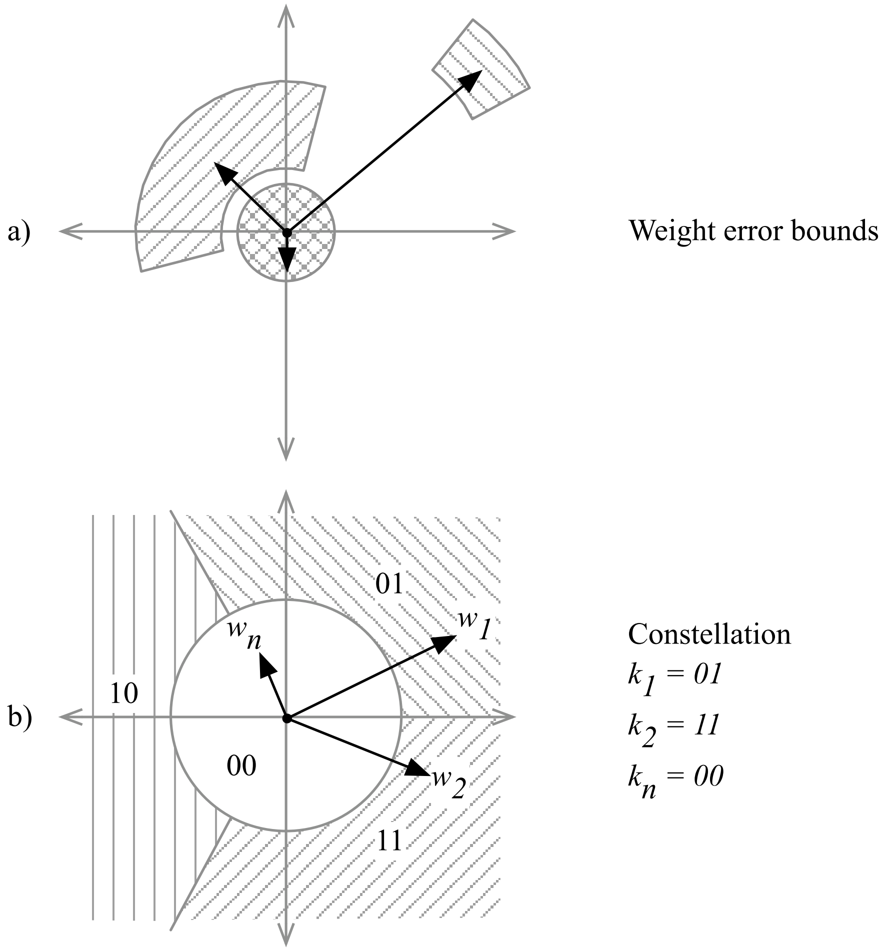


Figure 3. If domain synchronization errors exist, the error bounds is defined around a weight whose size is a function of the rate of the metric variation over the domain (a). A constellation can be defined to minimize the impact of weights with correlated errors (b).

to fourteen parallel one-dimensional binary-threshold functions, equivalent to the constellation shown in Figure 2c. Alternately, with the measure of multiple independent metrics, it is possible to instead utilize a single multidimensional constellation, an example thereof is shown in Figure 2d.

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. In previously published work, metrics with nonlinear distributions and a static threshold yield key bits that are not equally distributed [16]. It is to emphasize the importance of conditioning that metrics and weights are defined separately. 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.

Even with a perfectly reciprocal channel, differences in weight values will exist between nodes due to domain synchronization errors, such as synchronization in time, clock drift in phase, or oscillator drift in frequency. If a domain synchronization error exists, an error bounds can be defined around a weight whose size is a function of the rate of the metric variation over the domain, as seen in Figure 3a. To reduce errors a system can analyze a channel and change the sampling rate or reduce the constellation complexity to compensate for the increased error bounds. Previously demonstrated systems maintained constant sample rates and employed static keying functions, instead relying on error-correction postprocessing.

There can also exist a dependence of error bounds between dimensions of a single weight. Specifically, in a two-dimensional vector-magnitude constellation, because phase changes slowly at amplitude peaks and rapidly at amplitude nulls in a time-varying channel, error bounds in phase are a function of amplitude (Figure 3a). While most implemented systems ignore phase, an alternative is to define a constellation which excludes phase information for low amplitudes and includes phase information for high amplitudes as shown in Figure 3b.

Key Correction and Expiration

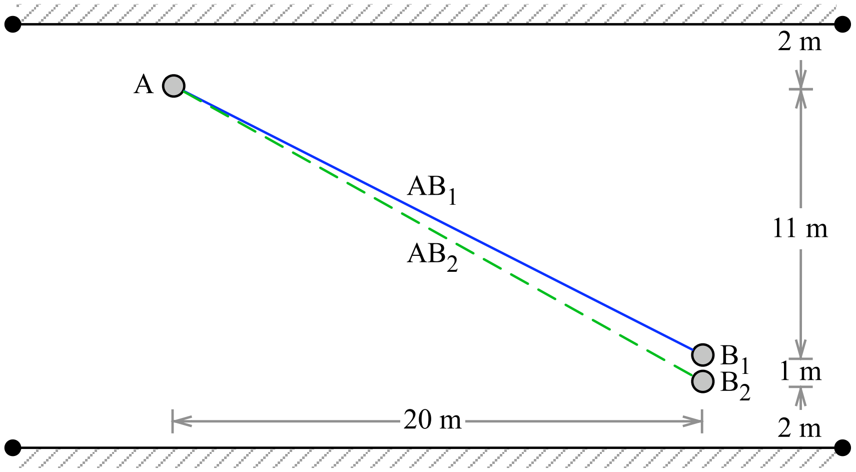
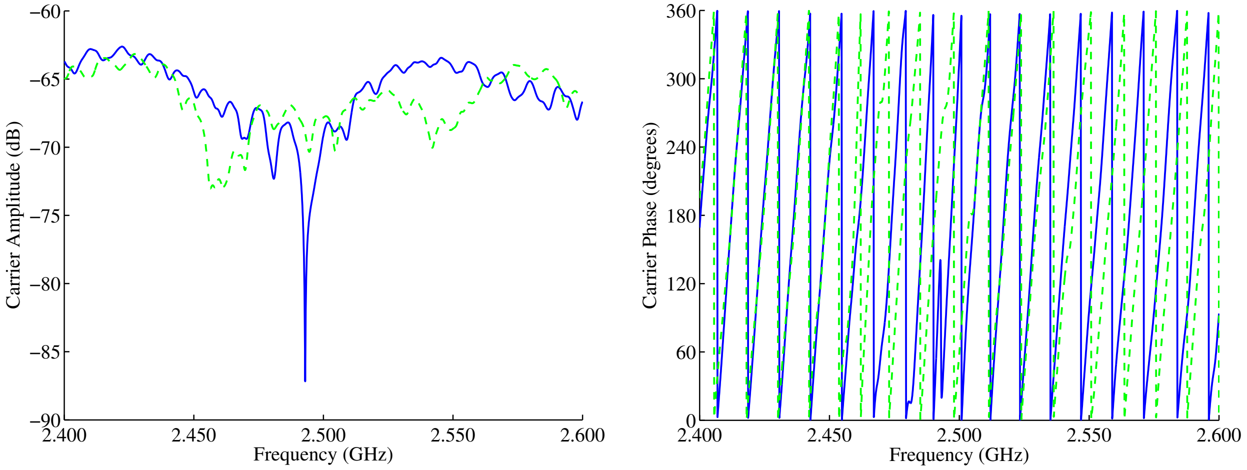


Figure 4. This simulated system represents communication across and down a street between two buildings. Only the principal ray is shown, however rays that reflect between the structures, up to the convergence point of ten reflections, are included in the simulation.

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 [19] and more novel methods such as fuzzy information reconciliators [16]. 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 comparing a one-way hash of the private keys [20].



(a)

(b)

Figure 5. Measured carrier amplitude (a) and phase (b) as a function of frequency, corresponding to the channels shown in Figure 4.

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.

Although it is discussed in a preceding section that a system can generate keys in domains other than time, ultimately it is in the time domain in which keys are solved for by an adversary. Thus even if multiple keys are generated simultaneously in a single time step and used serially, key expiration times are set together. Thus such a system ultimately relies on a time-varying channel to build new keys over the lifetime of its deployment.

It is important to note, that some environments can periodically revert to a degenerate state, such as an office building on a weekend morning. If channel variation between each degenerate state is low, keys generated during these periods are vulnerable, as the time an adversary has to understand the environment is the history of all time that environment has previously been in that state. Thus it can be beneficial to a system to maintain a history of the channel over time to identify periodic degenerative states and avoid the generation of keys during those periods.

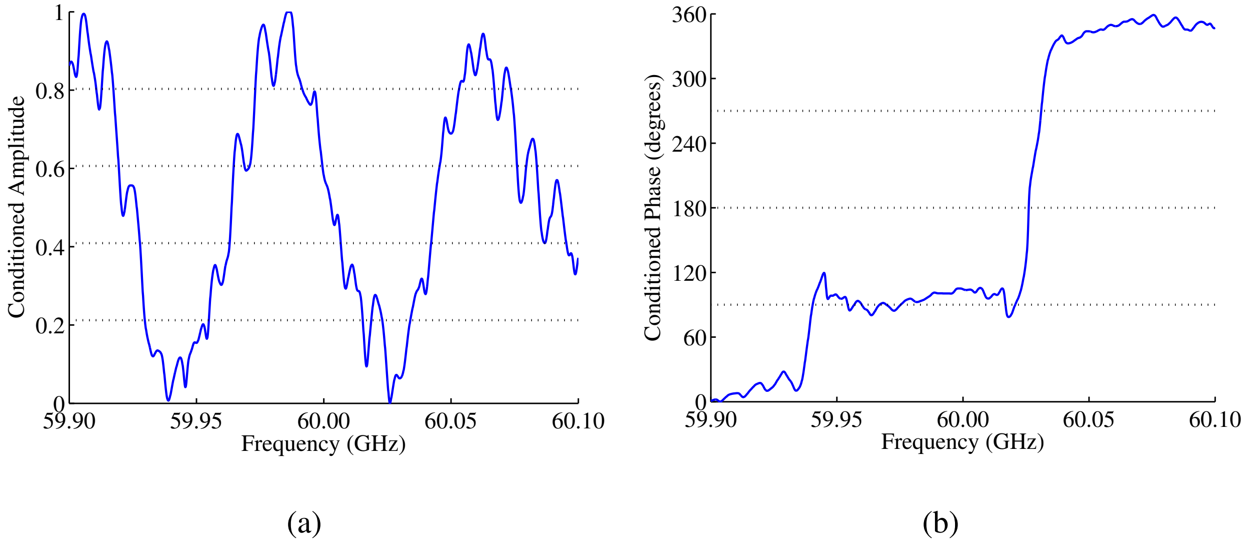


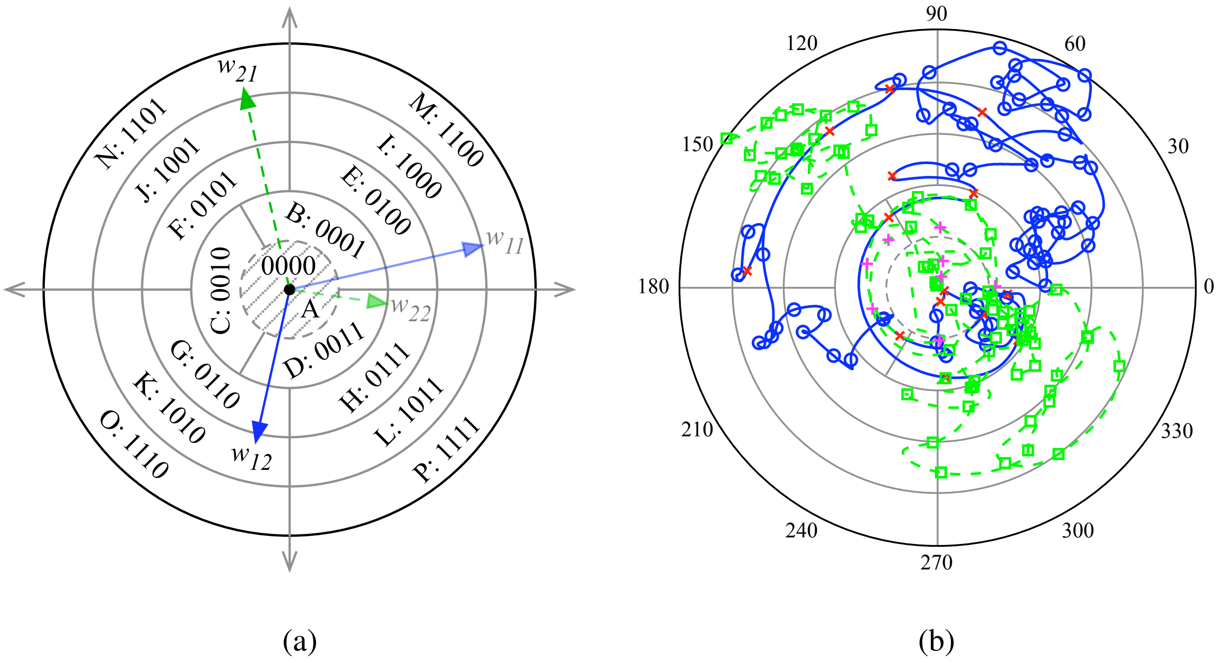
Figure 6. Conditioned carrier amplitude (a) and phase (b) as a function of frequency. The amplitude has been normalized and phase linearized. The first amplitude threshold is related to the median amplitude minus the standard deviation. The following amplitude and all phase thresholds are equal division.

Proof of Concept

This section presents the results of a simulation which demonstrates several of the topics discussed in the previous section. A physical system is modeled in *MATLAB* using a two-dimensional ray-tracing code with the topology shown Figure 4. 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 and shown in Figure 5. 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. The conditioned metrics are shown in Figure 6.



(a)

(b)

Figure 7. The simulated system uses a constellation with sixteen regions (a). 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 (b) demonstrates qualitatively that the channels are uncorrelated.

The constellation is shown in Figure 7a. The lowest magnitude threshold is dynamic and set by the median of the conditioned amplitude minus the standard deviation as an approximate boundary between a signal and a null. The remaining amplitude region is divided equally. All amplitude regions have four phase regions with the exception of the first and second which have one and three regions respectively. There are a total of sixteen regions each corresponding to a four-bit symbol.

As stated in previously, the variation of the magnitude and phase over frequency are often correlated, with a null in magnitude corresponding to rapid change in phase. Likewise, amplitude peaks tend to correspond to slow phase variation. Thus, to improve variability over the constellation, the magnitude from channel AB_1 is combined with the phase from channel AB_2 to create the weight w_{12} and conversely the weight w_{21}. These two weights are utilized simultaneously to generate the private encryption key. However, the weights w_{11} and w_{22}, which are comprised of the magnitude and phase of channel AB_1 and AB_2, are still utilized to detect regions of rapid change. In use, the symbols returned by the weights w_{12} and w_{21} are used, unless the weights w_{11} and w_{22} return symbol A.

Figure 7b 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. The symbols, each representing four bits, returned by the simulated channel are as follows:

```
IJNMMIMM MMMIMMIE IIEEEAAA AAAADDDD
DDDDAADD DACCGGGG GKKKJJJA ANAAIIII
EEIEEEEE EBBEEBBB JJJJNNNJ JNNNJJNJ
JCCCBCCB BBBABBBA ABBAAAAA DDDDDDDD
HHHDDDDD DDDDDDDH LHHLLLLL LLKGDDHG
```

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.

Because of perfect reciprocity in the channel, there is no bit disagreement between nodes. However, as discussed previously, misalignment of the sample metric between nodes can lead to errors. Simulations show that a 2.5 MHz frequency misalignment between node A and B generates approximately three bit errors, which can easily be corrected using previously discussed error-correction methods.

Interference

The ability of an eavesdropper to deduce the shared cryptographic key has been analyzed in several prior works [11], [12], [13], [14], [15], [20], however the effect of an interferer has not yet been considered. In the following section, the effects of a narrow-band FM transmitter and a low-power, broadband jammer on the performance of the key-generation system are discussed.

The physical system with the topology shown in Figure 8 is modeled using previously described methodology and parameters. This simulated system represents communication across and down a street between two buildings in the presence of an interferer. Three nodes, A, B, and J, are separated in the simulation space. For simplicity, only antenna B_1 is considered.

One of the primary capabilities of a cognitive radio is the ability to scan a spectral band for the presence of other transmitting nodes. This process can be performed either locally by a single cognitive system or collectively through a network of many [21]. In the case of a narrow-band transmission, such as the FM transmitter shown in Figure 9a, a cognitive radio avoids utilizing the occupied band. Using the previously described demodulation method, the system generates a key identical to the previous, minus the bits from the occupied band.

However, in the presence of a low-power, broadband jammer, a cognitive radio can not avoid transmitting in the same band (Figure 9b). Because the jammer is closer to node A than node B, the received power from the jammer is different at each node. Depending on the method of measuring the channel, either the signal-to-noise ratio or the total measured power at a given frequency will differ. Regardless, channel symmetry is broken and the generation of a symmetric key becomes difficult.

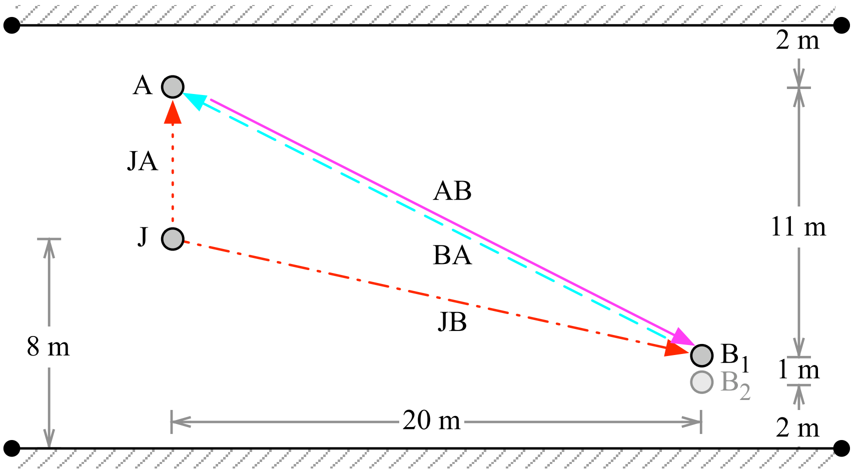


Figure 8. This simulated system represents communication across and down a street between two buildings. Two nodes, A and B, transmit in the presence of an interferer, J. For simplicity, only a single antenna is considered on node B and reciprocity is not assumed, requiring the definition of path AB and BA. Only the principal rays are shown, however rays that reflect between the structures, up to the convergence point of ten reflections, are included in the simulation.

Assuming the system is able to iteratively simplify the constellation in response to failed attempts to create matching keys, the simplest constellation, a binary magnitude-threshold constellation which omits phase, as shown in Figure 10a, will be converged upon. Figure 10b shows the path of the vectors over the constellation in frequency, with the location of the sample points marked. If the channel were symmetric, the two paths would be identical.

There are 80 sample points for the single path, generating 80 b in a single time step. The bits generated by node A are as follows:

```
11111111 11111111 11100000 00000000
00000000 00000010 11111111 11111111
11110001 00010000
```

The bits generated by node B are as follows:

```
11111111 11111111 11000000 00000000
00000000 00000110 01111111 11111111
11100011 00000000
```

There are six disagreements and both keys fail a runs test.

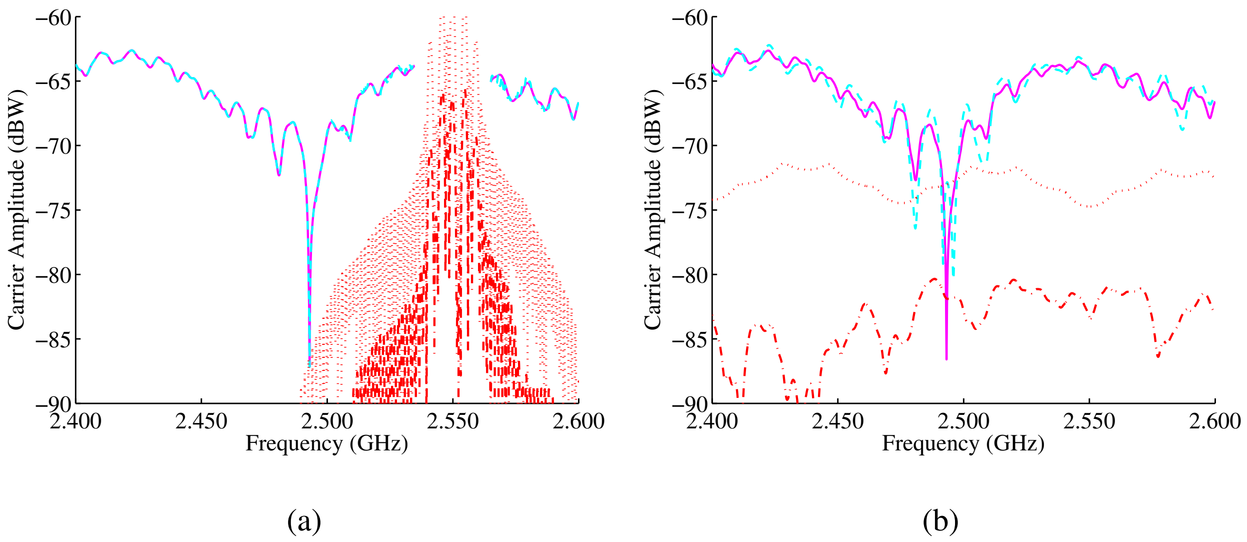


Figure 9. Measured carrier amplitudes in the presence of a narrow-band FM transmitter (a) and a low-power, broadband jammer (b), corresponding to the channels shown in Figure 8. Note the difference in received power from the interferer due to proximity.

It is shown here that a low-power, broadband jammer located in close proximity to a single node is capable of breaking receiver symmetry and preventing the creation of a shared cryptographic key. A possible solution is the measurement and exchange of noise floors between nodes, however, while restoring symmetry, dynamic range would still be limited.

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.

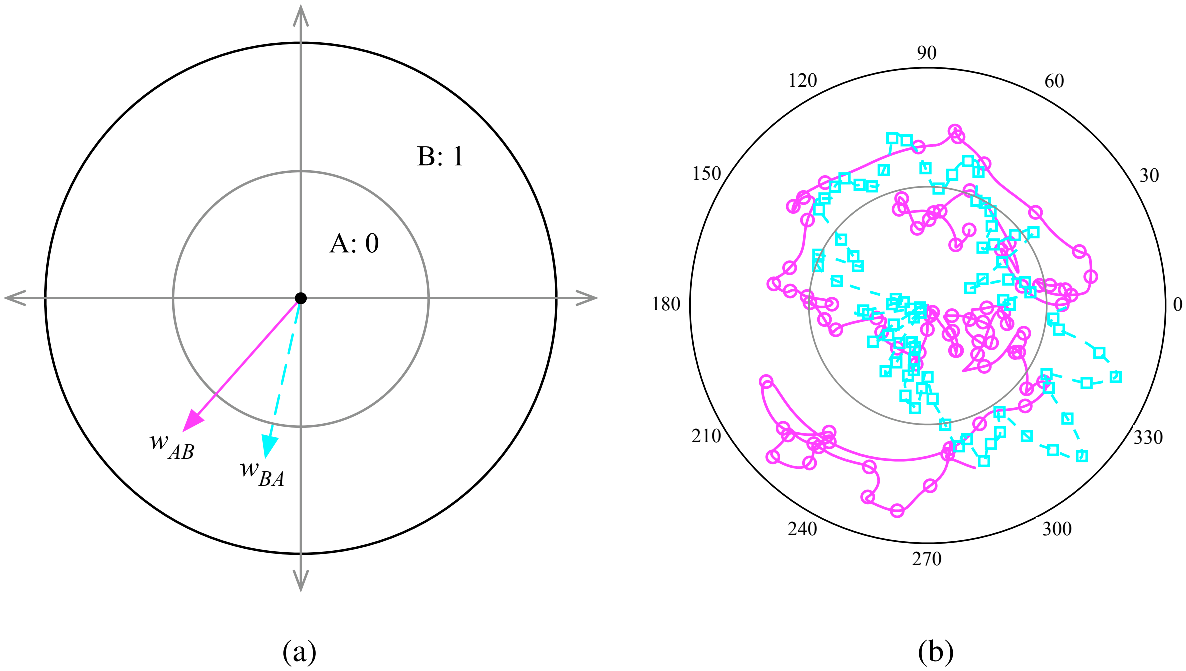


Figure 10. The simulated system uses a constellation with two only regions (a). The path followed by the weights over frequency (b) demonstrate the loss of symmetry due to the presence of a broadband jammer in close proximity to one node.

Half-Duplex Channel Impulse Response Estimation System

Overview

A block diagram of a cognitive node capable of creating shared private keys through channel measurements is shown in Figure 11. The system is composed of a key-generation block and a cognitive-control block which work together to improve and estimate the strength of generated keys.

The key-generation block converts received signals into cryptographic keys and consists of five sections. The channel-measurement section records and forwards data for analysis and key generation. The weight-generation section normalizes the data, converting it to vectors for demodulation. The key-generation section uses a constellation with symbols to convert vectors into binary data. The key-validation section uses a hash to permit the exchange and validation of a generated key between nodes, using previously published methods [16]. Finally, the key-strength section stores a key with its estimated strength for use and comparison against future keys to identify degenerate (recurring) channel states.

For a channel to be suitable for use as a keying variable, it must be reciprocal, sufficiently com-

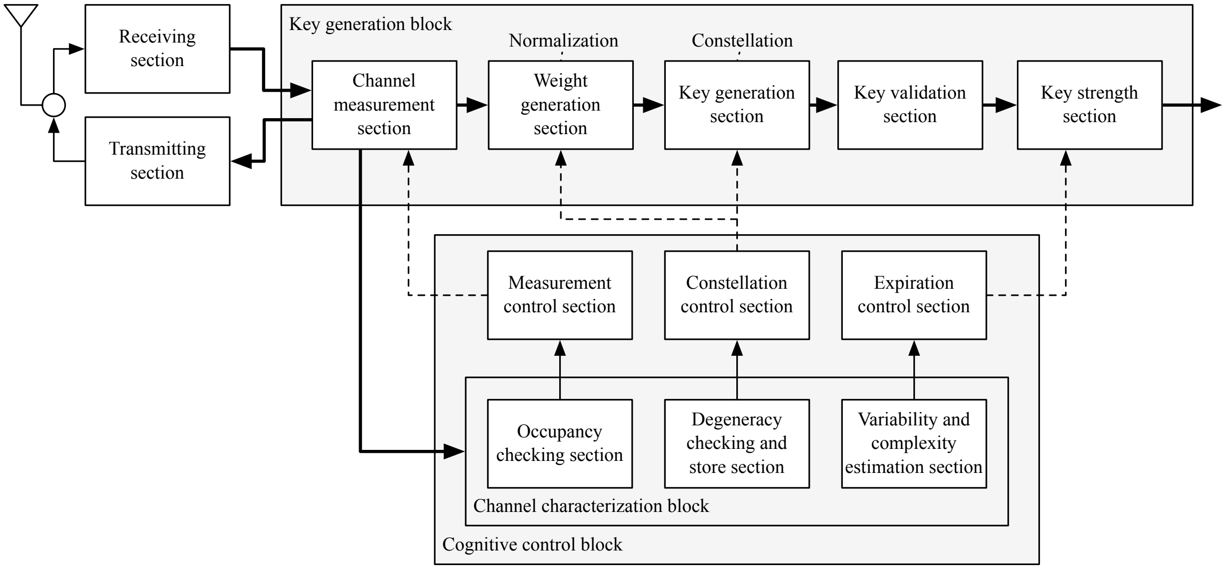

Receiving section
Transmitting section
Key generation block
Normalization
Constellation
Channel measurement section
Weight generation section
Key generation section
Key validation section
Key strength section
Measurement control section
Constellation control section
Expiration control section
Occupancy checking section
Degeneracy checking and store section
Variability and complexity estimation section
Channel characterization block
Cognitive control block

Figure 11. A block diagram of a cognitive node capable of creating shared private keys through channel impulse response estimation. The system is composed of a key-generation block and a cognitive-control block, which work together to improve and estimate the strength of generated keys.

plex, varying within bounds, and not in a degenerate state. While resistance of this key-generation method to eavesdropping is often discussed, the vulnerabilities introduced by the absence of the above channel requirements are often ignored.

In an attempt to address these vulnerabilities and to improve the performance of the system, a cognitive-control block is introduced, composed of three parallel paths. The measurement-control section analyzes the measured channel, to look for reciprocity and occupancy and to identify a subset of usable data for key generation. The constellation-control section selects the method of converting data to vectors and the type of constellation. The expiration-control section estimates the strength of the generated key based on channel characteristics.

Implementation

A half-duplex testbed has been implemented to demonstrate elements of the proposed key-generation system. The testbed consists of two transceivers, laboratory test equipment, and a single computer running MATLAB for control. The transceivers are the 60 GHz VubIQ V60DSK01 with integrated digital control and antennas, selected for their 1.5 GHz bandwidth, allowing the differentiation of path lengths that differ by as little as 60 cm. This enables a detailed measurement of channel complexity, important in the evaluation of generated key strength.

Using previously published techniques [22], the system estimates the impulse response of a channel by repeating series of 1023 b pseudorandom numbers (PN), modulated on to the 60 GHz carrier. The PNs are transmitted at 500 Mb/s, repeating approximately every 2 ms, and providing a 2 ns channel time resolution. The PN sequence length is tradeoff between signal gain and clock drift. Because the key-generation section makes use of phase information to generate data, the sequence is short enough to prevent the accumulation of significant phase errors from clock drift between the receiver and transmitter. Additionally, the system averages five consecutive channel measurements together, with phase normalized to the peak return, to reduce noise. Thus the system has a sampling period of 10 ms, setting the upper bound on the variability that an environment can possess and still be characterized.

Measurements

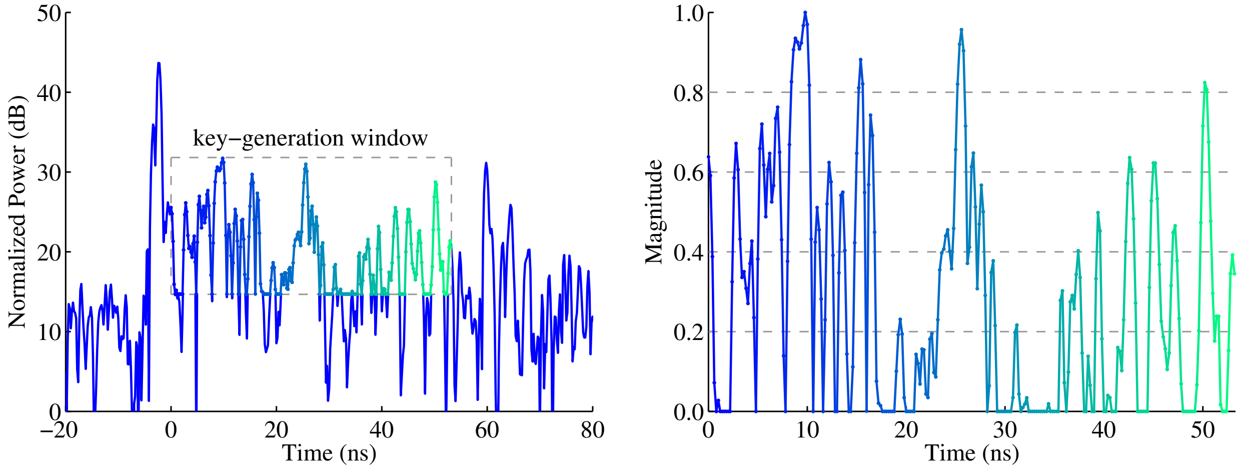
The following measurements were performed with the half-duplex testbed while demonstrating late-breaking results at the 16th ACM *Conference on Computer and Communications Security* on 11 November 2009. A total of 57 measurements were taken in three sessions, each in distinct environments. The transmitter and receiver were separated by a distance of approximately 2 m and oriented in the same direction into a large room. Because of their configuration, each channel impulse-response estimate includes an initial pulse representing the line-of-sight link between the transmitter and receiver – useful returns reflect from objects and return to the receiver. A single measurement from this session is presented initially to demonstrate the key-generation process, followed with an analysis of the entire data set and performance of the system in various environments.

Single Measurement

The power-delay profile of measurement number 41, made in a complex environment, is shown in Figure 12a. Phase information is omitted due to space constraints. This data originates in the channel-measurement section and is passed to the measurement-control section for the definition of a key-generation window.

The key-generation-window start time is 2.5 ns after the unchanging line-of-sight peak. The stop time is 53.3 ns after the start time, corresponding to a path length of 16 m, an approximate limit imposed by transmitter power and receiver sensitivity. The lower power bound is set to be one standard deviation above the mean of the noise floor as measured over a 200 ns period preceding the initial peak. The upper power bound is the maximum power present within the window. The dynamic range of the shown key-generation window is 17.1 dB.

The data in the key-generation window is passed to the weight-generation section which renormalizes the data (Figure 12b) and creates an array of vectors. The path of the vectors over the constellation is shown in Figure 12c. Each vector sample is converted to a 4 b value corresponding to one of the 16 symbols. In this measurement, 269 vectors generate 1076 b of data from the 16-symbol constellation in 10 ms. This is a data generation rate of 107.6 kb/s. The key validation-section is skipped in the half-duplex system.



(a)

(b)

Figure 12. The power-delay profile of measurement number 41 (a), the normalized vector magnitude from the key-generation window (b), and the path over the 16-symbol constellation (c).

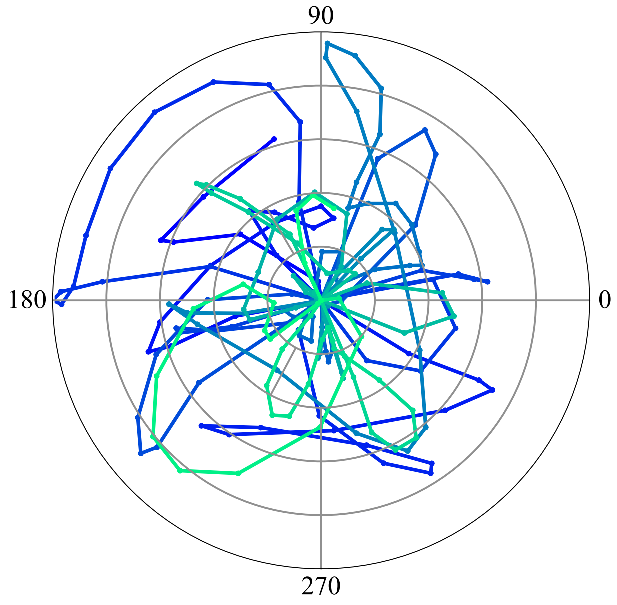


Figure 13. The power-delay profile of measurement number 41 (a), the normalized vector magnitude from the key-generation window (b), and the path over the 16-symbol constellation (c).

The cognitive-control section estimates key strength using a weighted average of the key-generation-window dynamic range, the power-delay-profile complexity, and the key randomness estimated from a runs test. The key strength is stored as metadata with the generated key and used to set an expiration time for the key. Values for measurement number 41 are shown in the following subsection.

Multiple Measurements

The key-generation-window dynamic range, the key-generation-window complexity, and the estimated key randomness for all 57 measurements are shown in Figure 14. The measurements were taken in three environments, labeled A, B, and C. The single, previously presented measurement, number 41, is marked with an inverted triangle.

Measurements in environment A were taken between 15:00 and 15:30 and represent a period of system setup, measuring close, static objects. Measurements in environment B were taken between 15:30 and 17:30 during system debugging in a large, empty room before the demonstration session. Measurements in environment C were taken between 18:00 and 19:00 in the same room filled with many moving conference attendees.

Studying the dynamic range, it can be seen that the close objects in environment A yielded a relatively high dynamic range due to the close proximity of objects, while the large, empty room of environment B did not. Outliers in the dynamic range in environment B are due to reflections from group members moving randomly about during the testbed setup. Environment C with a full room of interested onlookers has a higher dynamic range than the same empty room that is environment B.

The system estimates complexity by calculating the ratio of areas above and below the signal in the key-generation window. This method identifies impulse responses with a large dynamic ranges that are nonetheless relatively simple, differentiating between one return and many returns. As one would expect, the full room of environment A is more complex (has more returns) than the empty room that is environment B.

Key strength is estimated using a weighted average of the the key-generation-window dynamic range, the key-generation-signal complexity, and the calculated p-value from a runs test to measure randomness. Keys which passed the runs test are indicated with circles in the complexity plot in Figure 14b. Key strength estimates in the three environments agree with logically expected results, in that complex and varying environments provide stronger keys than simple and static environments.

Conclusions

Methods to generate private keys based on wireless channel characteristics have been demonstrated as an alternative to standard key-management schemes. We have demonstrated a half-duplex testbed for the generation of private keys for cryptographic communications using channel

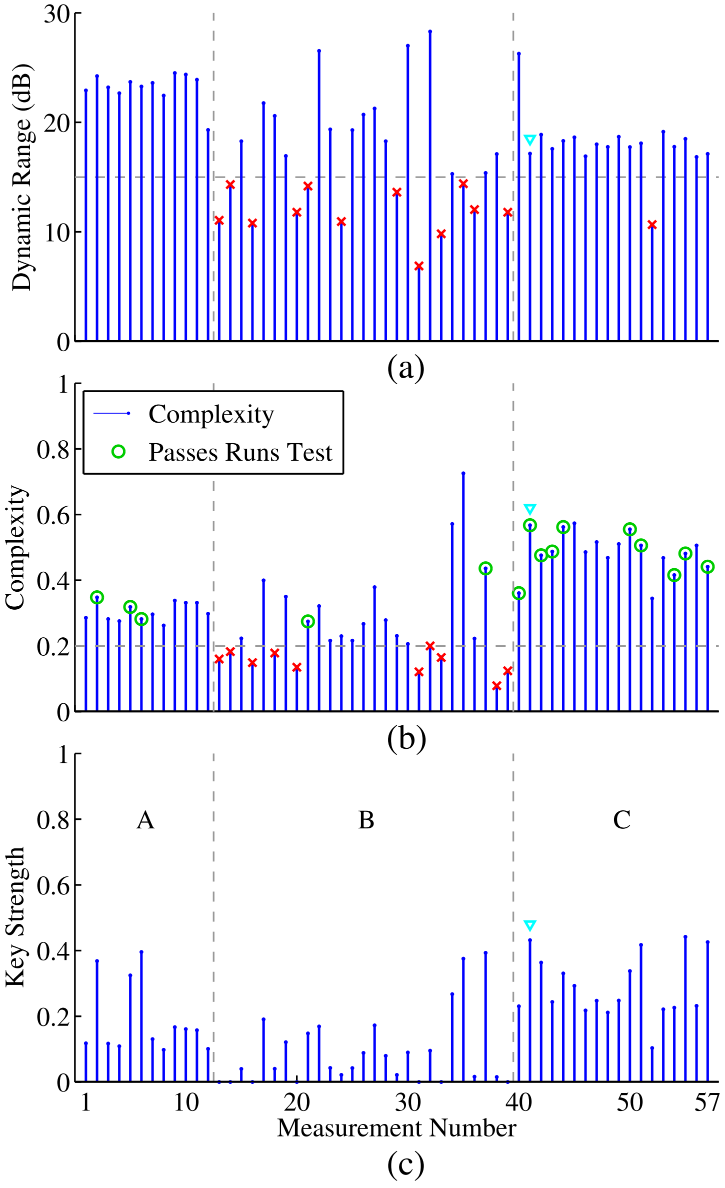


Figure 14. The key-generation-window dynamic range for all measurements (a), the key-generation-signal complexity and runs-test results (b), and the estimated key strength (c).

impulse-response estimation at 60 GHz. Further we have defined and implemented a prototypical cognitive testbed which can respond to variations in the environment by adjusting sampling methods and assigning key strengths. Future work will include the implementation of a full-duplex system and further development of the algorithms used to estimate channel complexity and key strength.

Full-Duplex Channel Impulse Response Estimation System

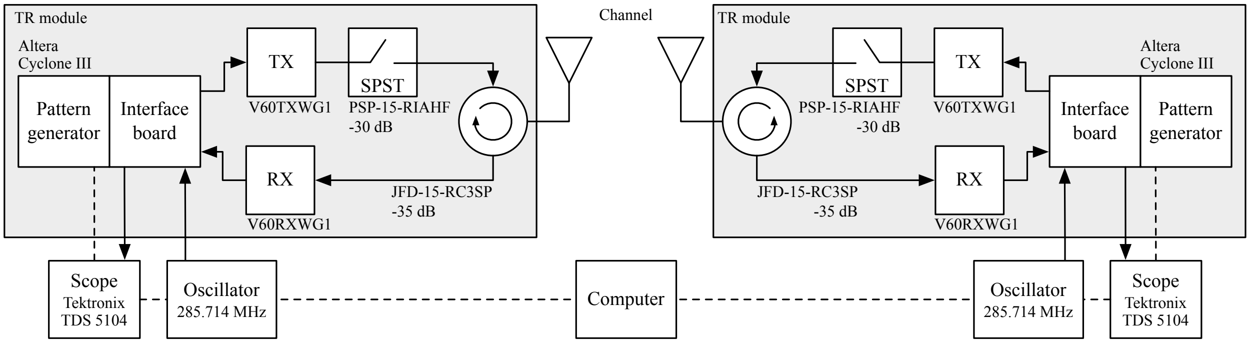


Figure 15. Block diagram of the full-duplex channel impulse-response estimation system showing two millimeter-wave transceivers, test equipment, and a control computer.

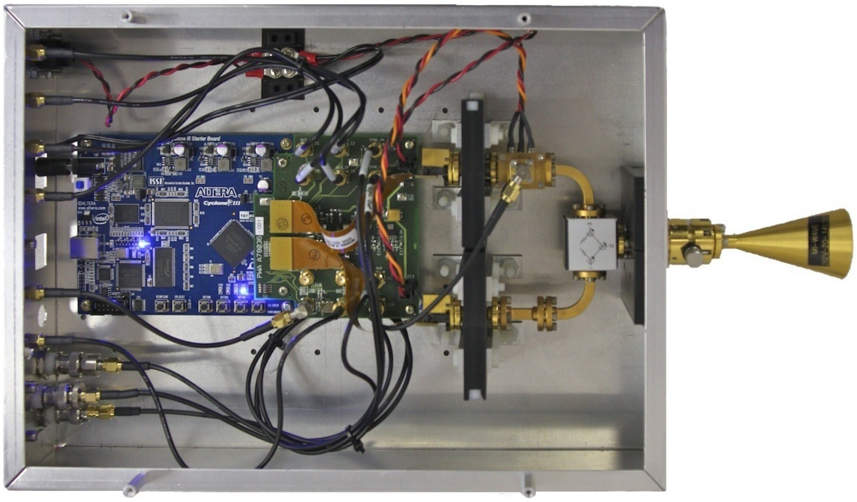


Figure 16. One of the millimeter-wave transceivers used in the full-duplex, key-generation system. The transceiver consists of an FPGA, interface board, parallel transmitter and receiver, and a waveguide front end with horn antenna.

A full-duplex testbed has been implemented to measure the realized reciprocity of key-generation system and is shown in Figure 15. The testbed consists of two custom transceivers, laboratory test equipment, and a single computer running MATLAB for control. The transceivers, one of which is shown in Figure 16, consists of pattern generator, interface board, parallel transmitter and receiver, and a waveguide front end with horn antenna.

The pattern generator, implemented with an Altera Cyclone III FPGA, generates a repeating sequence of four pseudorandom numbers (PN) created using a Galois linear feedback shift register. This PN sequence is equivalent to a BPSK-modulated baseband signal with no pulse-shaping filter. The sequences are stored in ROM and padded with an extra bit to make the pattern an even power of two. Because the PN sequence has a bit rate of 500 Mb/s, corresponding to a time resolution of 2 ns, channel path length differences as small as 60 cm can be differentiated.

From the pattern generator, the custom PCB interface board routes the PN sequence and an external 285.714 MHz external signal to the VubIQ V60TXWG1 transmitter. The PN sequence is mixed onto a 60 GHz carrier, routed through WR-15 waveguide and components, and radiated from a horn antenna.

After modulation by the channel and reception by an identical transceiver, the signal is downconverted to baseband in-phase (I) and quadrature (Q) signals and sampled by a high-speed oscilloscope with deep memory. Using previously published methods [22], the estimated channel impulse response is returned by performing cross correlation on the received signal with the original PN sequence.

Because the key generation algorithm makes use of phase information, the PN sequence has been chosen to repeat every 2 ms at the expense of higher coding gain to prevent the accumulation of phase error due to clock drift. To further compensate for drift, the system averages five consecutive channel measurements together, with phase normalized to the peak return. Thus the system has a maximum sampling period of 10 ms. This period sets a bound on the variability that an environment can possess and still be characterized with a full-duplex system.

Measurements from the full-duplex system will be published in a following document.

References

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

[2] U.S. National Bureau of Standards, "Data encryption standard," *Federal Information Processing Standards Publication 46 (FIPS-46)*, 1977.

[3] S. Camtepe and B. Yener, "Key distribution mechanisms for wireless sensor networks: a survey," *Rensselaer Polytechnic Inst.*, Jan 2005.

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

[5] R. Potton, "Reciprocity in optics," *Reports on Progress in Physics*, Jan 2004.

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

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

[8] A. Hassan, W. Stark, J. Hershey, and S. Chennakeshu, "Cryptographic key agreement for mobile radio," *Digital Signal Processing*, Jan 1996.

[9] M. Tope and J. McEachen, "Unconditionally secure communications over fading channels," *IEEE Military Communications Conference*, Jan 2001.

[10] A. Kitaura and H. Sasaoka, "A scheme of private key agreement based on the channel characteristics in ofdm land mobile radio," *Electronics and Communications in Japan (Part III Fundamental . . .)*, Jan 2005.

[11] T. Aono, K. Higuchi, M. Taromaru, T. Ohira, and H. Sasaoka, "Wireless secret key generation exploiting the reactance-domain scalar response of multipath fading channels: Rssi interleaving scheme," *Wireless Technology*, Jan 2005.

[12] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *Antennas and Propagation*, Jan 2005.

[13] T. Ohira, "Secret key generation exploiting antenna beam steering and wave propagation reciprocity," *2005 European Microwave Conference*, Jan 2005.

[14] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *Information Forensics and Security*, Jan 2007.

[15] A. Kitaura, H. Iwai, and H. Sasaoka, "A scheme of secret key agreement based on received signal strength variation by antenna switching in land mobile radio," *Advanced Communication Technology*, Jan 2007.

[16] 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.

[17] R. Vaughan, "Switched parasitic elements for antenna diversity," *Antennas and Propagation*, Jan 1999.

[18] J. D. Parsons, *The Mobile Radio Propagation Channel*, John Wiley & Sons, Inc., New York, NY, Jan 1992.

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

[20] 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*, vol. 4867, pp. 173, 2007.

[21] Chetan N. Mathur and K. P. Subbalakshmi, "Security issues in cognitive radio networks," in *Cognitive Networks: Towards Self-Aware Networks*, Qusay H. Mahmoud, Ed., chapter 11, pp. 271–291. John Wiley & Sons, Ltd., New York, 2007.

[22] D. Tholl, M. Fattouche, R. J. C Builtitude, P. Melancon, and H. Zaghloul, "A comparison of two radio propagation channel impulse response determination techniques," *IEEE Transactions on Antennas and Propagation*, vol. 41, no. 4, pp. 515–517, 1993.