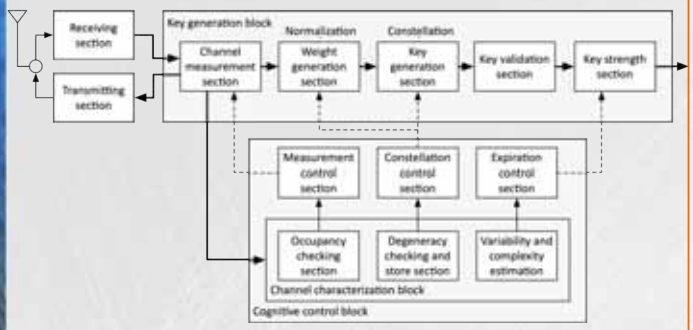
The Generation of Cryptographic Keys through Impulse Response Estimation

Sandia National Laboratories
Michael A. Forman, Derek Young, and Suresh Gollu

Problem

Private-key cryptography employs a class of algorithms that use an identical key for both encryption and decryption. Because this key must be private between, yet distributed among, communicating nodes, a secure key-distribution infrastructure is required. In scenarios where this is infeasible, several alternative methods for managing keying variables have been proposed, one of which utilizes the communications channel itself to generate a keying variable.

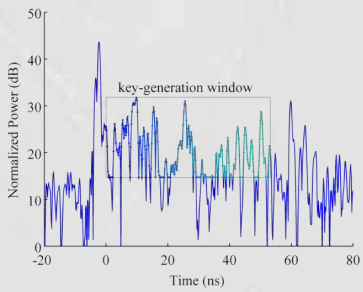


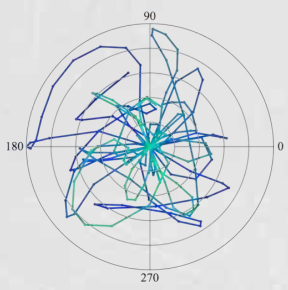
We present a system that generates private data for cryptographic communications using channel impulse-response estimation at 60 GHz. Further, novel cognitive enhancements measure channel characteristics, to dynamically change transmission and reception parameters and estimate private key strength. The demonstrated hardware is a partial implementation of a previously published simulated generalized system. The recent advance is the replacement of the simulated front end with a millimeter-wave front end and channel impulse-response estimation system.

Approach

Wireless signals exchanged over a reciprocal channel experience identical multipath fading. This fading is, in essence, a modulation that conveys information about the state of the channel. This information is extracted through channel measurements, transformed into weights, and demodulated with a constellation to generate binary data. Because fading is reciprocal, the shared data generated by the communicating nodes is suitable for use as a private cryptographic key. Eavesdropping is not possible, as third parties do not share the same channel.

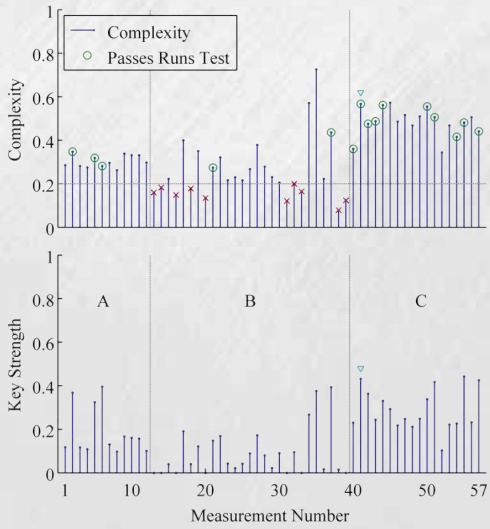
In the shown measurement, 269 vectors extracted from a key-generation window provide 1076 b of data using a 16-symbol constellation in 10 ms at a rate of 107.6 kb/s.





Results

The millimeter-wave testbed consists of two transceivers, laboratory test equipment, and a sin-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.
The system estimates complexity by identifying impulse responses with a large dynamic range and many reflections. As one would expect, the full rooms of environments A and C are more 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. Key strength estimates in the three environments agree with logically expected results.



Significance

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 testbed for the generation of private keys using channel 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. Such systems could enable secure communications in ad hoc deployments (battlefield, scattered sensors) where a key management system is unavailable.

Sandia National Laboratories is a multi-program 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.

SAND 2010-5367P

Sandia National Laboratories