Light-weight Key Generation
based on Physical Properties of Wireless Channels

Matthias Wilhelm, Ivan Martinovic, and Jens B. Schmitt

disco — Distributed Computer Systems Lab
TU Kaiserslautern, Germany
{wilhelm,martinovic,jschmitt}@cs.uni-kl.de

Key management is at the heart of cryptography system designs, enabling and ensuring the overall security of such systems. There are a variety of cryptographic protocols to generate and distribute keying material, and in many applications these well-researched solutions offer good performance and security. However, when considering low-cost and low-performance devices such as wireless sensor motes used for distributed monitoring of the environment, common protocols can introduce too large computational burdens or implementation complexity.

A new approach first considered in the context of information theory offers a promising concept of generating secret keys from *correlated random variables* [MRW07]. Inspired by this idea, wireless communication researchers showed that the wireless channel connecting two devices can be used as a source of such random variables [MTM+08, AKM+07]. Wireless channels show a strong correlation of the channel states between sender and receiver, known as the *reciprocity* of the wireless channel. By exchanging sampling messages and measuring the received signal strength during movement, this property can be used to derive a shared bit string. This string is only known to the involved entities because the channel behavior decorrelated rapidly in space, making this scheme resistant to eavesdropping from other physical positions.

We introduce a new concept that does not rely on movement as the source of randomness, but on the *frequency-selectivity* of the wireless channel. We show by implementation in our wireless sensor network testbed that this approach can be used to successfully generate unpredictable bits, even in static scenarios, which match for Alice and Bob with a very high probability, simply by using only the communication and measurement capabilities of standard sensor mote hardware. We also show how to analyze the secrecy of our proposed key generation protocol by using an information-theoretical approach to quantify the entropy of the resulting bits.

References

[MRW07] Ueli Maurer, Renato Renner, and Stefan Wolf. Unbreakable keys from random noise. Security with Noisy Data, Springer-Verlag, pp. 21-44, 2007.

[MTM+08] Suhas Mathur, Wade Trappe, Narayan Mandayam, Chunxuan Ye, and Alex Reznik. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. MobiCom '08: Proceedings of the 14th ACM international conference on Mobile computing and networking, pp. 128-139, 2008.

[AKM+07] Babak Azimi-Sadjadi, Aggelos Kiayias, Alejandra Mercado, and Bulent Yener. Robust key generation from signal envelopes in wireless networks. CCS '07: Proceedings of the 14th ACM conference on Computer and communications security, pp. 401-410, 2007