RUHR-UNIVERSITÄT BOCHUM

Horst Görtz Institute for IT-Security

Horst Görtz Institute for IT-Security

RUB

Implementation and Evaluation of Channel-based Key Establishment Systems

Christian T. Zenger, Jürgen Förster, Christof Paar

Chair for Embedded Security

Introduction / Motivation

Yes! There is another approach to secure wireless channels beside pre-shared keys or asymmetric cryptography. Numerous experiments have recently demonstrated that **channel-based key establishment (CBKE)** is a promising alternative to well-known symmetric/ asymmetric approaches. Their performance results for establishing a symmetric key suggest possible benefits for many real-world applications. Until now, research has been limited to simulation models. Our research bridges the gap between simulation results and real-world applications, such as on µ-controllers.

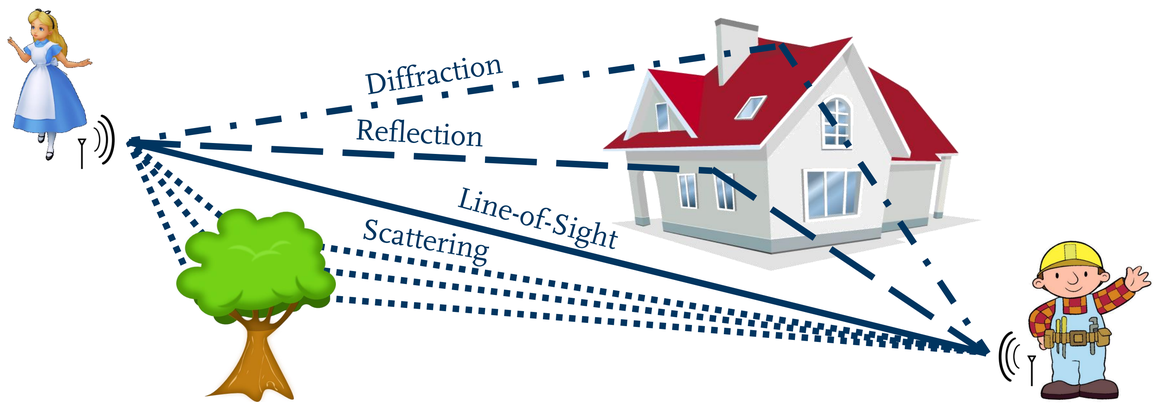

Fig. 1. **Propagation phenomena of the environment.** Path lost, large-scale propagation effects, and small-scale propagation effects.

Methods

After measuring the wireless channel, the constructed channel profile is then quantized into bit strings to obtain a preliminary key. Due to errors in channel measurement, variations in the preliminary keys exist. These variations are corrected in the information reconciliation stage by applying error correcting codes.

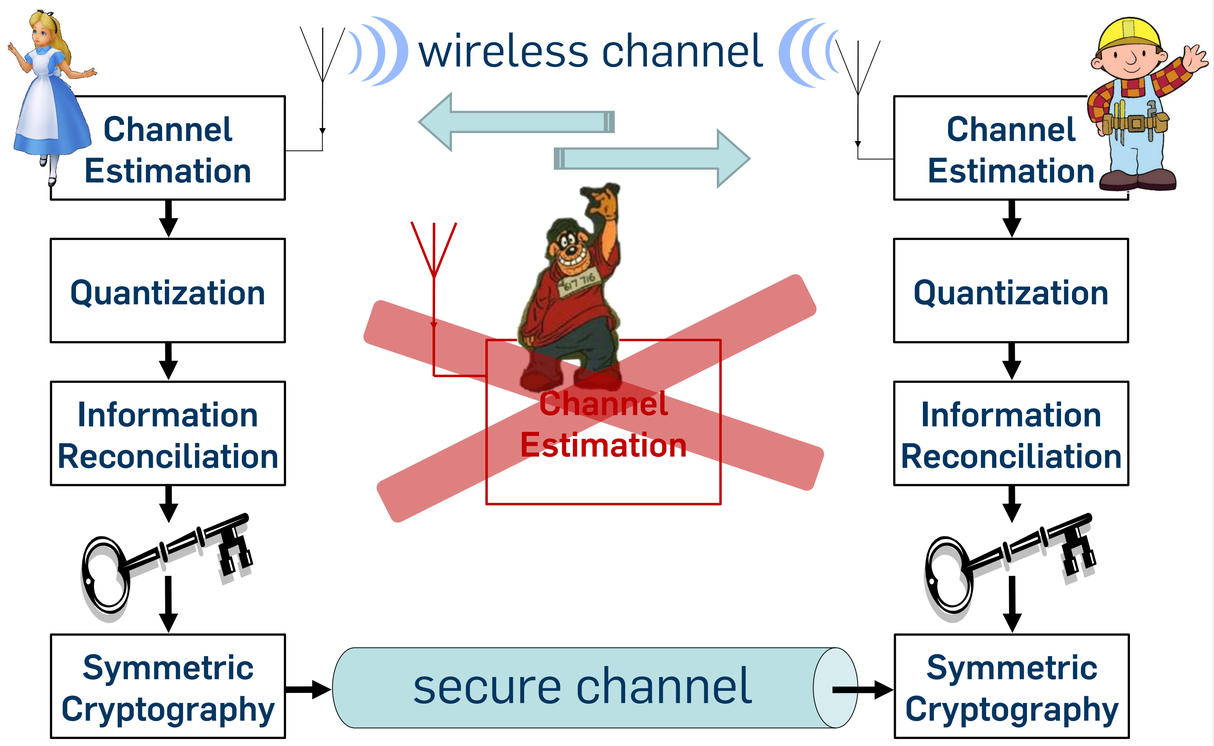

Fig. 2. **System model.** Legitimate nodes Alice and Bob measure properties of the wireless channel. Based on this, common information symmetric private keys can be established.

Results

Despite the large number of different CBKE protocols, there is no research on the evaluation and fair comparison of energy efficiency. We evaluate the efficiency of several CBKE system implementations.

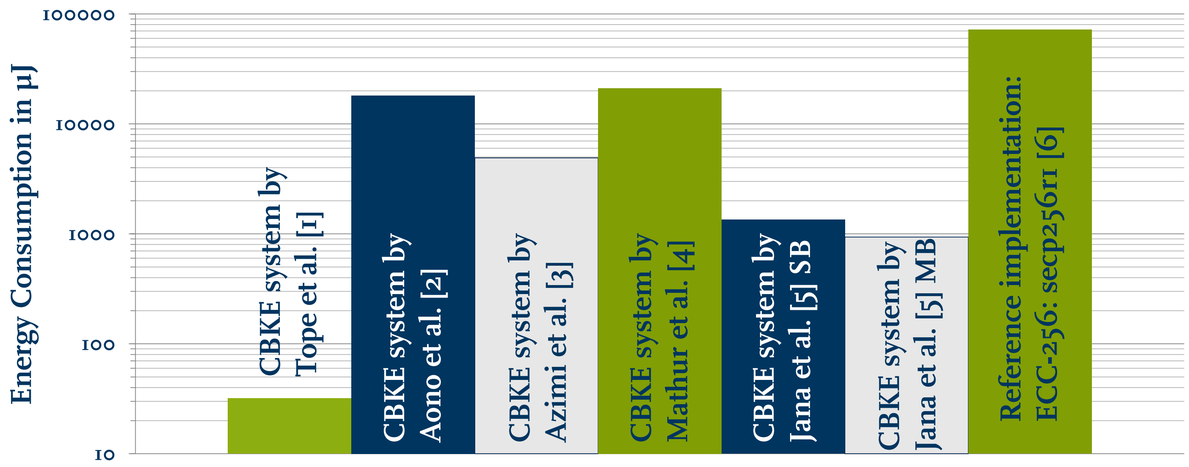

Fig. 3. **Energy Consumption** of the establishment of a 128 bit security level for different CBKE schemes as well as for a very efficient state-of-the-art elliptic curve cryptosystem (ECC) reference implementation.

We chose an **ARM Cortex M3** as the platform for our software implementations. We present the approximate resource overhead of several CBKE schemes [1,2,3,4,5] and compare our results with a current key establishment implementation [6].

Quantizer	Energy [µ Joule]	Code Size [byte]	# of cycles	Communication Overhead [byte]
Tope et al. [1]	32	684	74.613	256
Aono et al. [2]	18.130	1.664	15.692.950	192
Azimi et al. [3]	4.917	1.340	5.370.539	171
Mathur et al. [4]	21.102	1.692	21.060	502
Jana et al. [5] SB	1.350	1.860	1.721.803	103
Jana et al. [5] MB	934	1.240	1.191.695	64
ECC-256 [6]	71.730	8.276	65.799.382	33

Tab. 1. **Approximate resource overhead of our implementations of several CBKE schemes.** Here, "# of cycles", "communication overhead" and "energy" denote resource costs for the generation of a 128 bit key.

References

[1] Michael A. Tope and John C. McEachen. Unconditionally secure communicationsover fading channels. In Military Communications Conference, 2001. MILCOM2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE, volume 1, pages 54–58. IEEE, 2001.

[2] Tomoyuki Aono, Keisuke Higuchi, Takashi Ohira, Bokuji Komiyama, and Hideichi Sasaoka. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels. IEEE Transactions on Antennas and Propagation, 53(11):3776–3784, 2005.

[3] Babak Azimi-Sadjadi, Aggelos Kiayias, Alejandra Mercado, and Bulent Yener. Robust key generation from signal envelopes in wireless networks. In Proceedings of the 14th ACM conference on Computer and communications security, pages 401–410. ACM, 2007.

[4] Suha Mathur, Wade Trappe, Narayan Mandayam, Chunxuan Ye, and Alex Reznik. Radio-telepathy: Extracting a secret key from unauthenticated wireless channel. In Proceedings of the 14th ACM international conference on Mobile computing and networking, pages 128–139. ACM, 2008.

[5] Suman Jana, Sriram Nandha Premnath, Mike Clark, Sneha K. Kasera, Neal Patwari, and Srikanth V. Krishnamurthy. On the effectiveness of secret key extraction from wireless signal strength in real environments. In Proceedings of the 15th annual international conference on Mobile computing and networking (MobiCom), pages 321–332. ACM, 2009.

[6] ECDH and ECDSA for 8-bit, 32-bit, and 64-bit processors. https://github.com/kmackay/micro-ecc, 2014

Acknowledgments / Special thanks

Providing Physical Layer Security for the Internet of Things (PROPHYLAXE) is a strategic research project supported by the German Ministry of Education and Research. The project includes a diverse team of IT-security scientists, electrical and computer engineers and communication engineers from HGI, Fraunhofer HHI, TU-Dresden, TU-Kaiserslautern, ESCRYPT, and the BOSCH Group.

Federal Ministry of Education and Research · Horst Görtz Institute for IT-Security · RUB DKS · Fraunhofer Heinrich Hertz Institute · escrypt Embedded Security · BOSCH · Technische Universität Kaiserslautern · Technische Universität Dresden