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.

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].

FIGURE 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.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Tappe et al. [4]</td>
<td>18.130</td>
<td>1.664</td>
<td>15.692.950</td>
<td>192</td>
</tr>
<tr>
<td>Jana et al. [5]</td>
<td>9.34</td>
<td>2.420</td>
<td>1.191.695</td>
<td>64</td>
</tr>
</tbody>
</table>

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

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, ECRYPT, and the BOSCH Group.