End-to-End Key Establishment using Physical Layer Key Generation with Specific Attacker Models

Stefan Pfennig, Elke Franz, Sabrina Engelmann, and Anne Wolf
Technische Universität Dresden, Germany
{stefan.pfennig, elke.franz, sabrina.engelmann, anne.wolf}@tu-dresden.de

I. Introduction and Problem Statement

Cryptography is a fundamental technique for securing electronic communications, particularly, for ensuring confidentiality, integrity, and accountability of transmitted messages. Of course, cryptographic systems cannot perform their function without establishing the required keys. We have to consider that the security of key establishment crucially influences the security of the cryptosystem. Within this paper, we focus on the use of symmetric cryptography since it provides better performance and requires less computational effort than asymmetric cryptography. However, a drawback of symmetric cryptography is the fact that we need a prior secure exchange of the secret key between the communication partners. In general, existing protocols require that the communication partners already possess a secret that can be used to derive a new cryptographic key, or that a trusted party is involved in the key exchange [2].

In [5] it was shown, that symmetric point-to-point keys can be generated on the physical layer. The key is generated from random characteristics of the wireless channel, which are only available to the sender and the receiver.

The goal of this paper is to evaluate whether we can use such physical layer point-to-point keys for a secure exchange of end-to-end keys. We consider specific attacker models and requirements on keys such as their length. For example, the current standard for symmetric encryption, AES, supports key lengths of 128, 196, and 256 bits [3].

II. System Assumptions and Attacker Model

We assume that sender $\mathcal{S}$ and receiver $\mathcal{R}$ wish to establish a secret key for securing their communication by means of symmetric cryptography. There may be an arbitrary number of $\ell + 1$ hops between sender and receiver, hence, there are forwarders $\mathcal{F}_{1,j}$ with $j \in \{1, 2, ..., \ell\}$ per path that transmit the messages (Fig. 1). We consider k paths and alterable links between subsequent forwarders. We assume wireless communication and apply physical layer key generation.

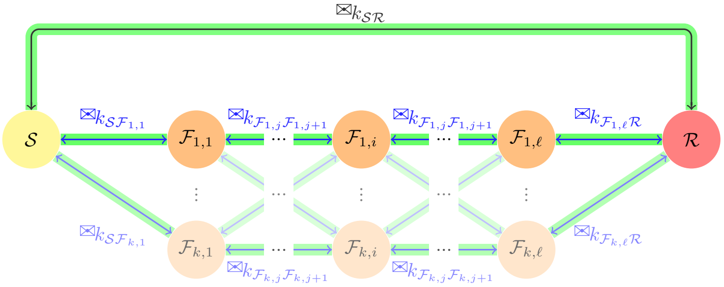
$\boxtimes k_{\mathcal{S}\mathcal{R}}$
$\boxtimes k_{\mathcal{S}\mathcal{F}_{1,1}}$
$\boxtimes k_{\mathcal{F}_{1,j}\mathcal{F}_{1,j+1}}$
$\boxtimes k_{\mathcal{F}_{1,j}\mathcal{F}_{1,j+1}}$
$\boxtimes k_{\mathcal{F}_{1,\ell}\mathcal{R}}$
$\mathcal{S}$
$\mathcal{F}_{1,1}$
$\mathcal{F}_{1,i}$
$\mathcal{F}_{1,\ell}$
$\mathcal{R}$
$\boxtimes k_{\mathcal{S}\mathcal{F}_{k,1}}$
$\mathcal{F}_{k,1}$
$\mathcal{F}_{k,i}$
$\mathcal{F}_{k,\ell}$
$\boxtimes k_{\mathcal{F}_{k,\ell}\mathcal{R}}$
$\boxtimes k_{\mathcal{F}_{k,j}\mathcal{F}_{k,j+1}}$
$\boxtimes k_{\mathcal{F}_{k,j}\mathcal{F}_{k,j+1}}$

Fig. 1. System model.

In order to assess the security of the key exchange, possible attacks need to be considered. As a first step, we have to define the attacker model. In the context of our investigations, we particularly consider the behavior (passive/active) and role (insider/outsider) of the attacker.

- If the attacker is an outsider, he can only access the wireless communication. A passive attacker only eavesdrops the communication, an active attacker is able to jam the communication, i.e., to modify or even delete transmitted messages. In both cases, nodes are assumed to be fully trustworthy.
- If the attacker is an insider, he can control forwarding nodes (sender and receivers are trustworthy). A passive attacker only observes while an active attacker may modify transmitted messages. In this case, it is further relevant how many nodes are controlled by an attacker.

This work is partially supported by the German Research Foundation (DFG) in the CRC 912 "HAEC".

This work was partially funded by the Federal Ministry of Education and Research of the Federal Republic of Germany (Förderkennzeichen 16 KIS 0009, Prophylaxe). The authors alone are responsible for the content of the paper.

III. Physical Layer Key Generation

Key generation on the physical layer is widely discussed in literature nowadays [1]. Mainly, there are two different approaches that need to be distinguished. In the channel-type model, the sender transmits a random sequence over the channel to the receiver, while in the source-type model, sender and receiver observe a common source of randomness, which is, e.g., the fading characteristic of their common reciprocal channel and can be estimated by both partners using pilot signaling. For both models, an appropriate coding scheme and a key agreement protocol over a public authenticated noiseless channel are needed, in order to get a key that is only known by the sender and the receiver. The steps of such a key agreement protocol are presented in the following for the source-type model.

1) *Advantage Distillation:* Sender and receiver try to find observations, where they have an advantage over the eavesdropper and discard all other observations. 2) *Information Reconciliation:* Sender and receiver process their observations in order to correct errors and match their observations. 3) *Privacy Amplification:* Sender and receiver agree on a hash function in order to generate a common key.

The chosen key generation strategy depends on the channel characteristics and the information that is available to the sender and the attacker. In the full paper, optimal key generation strategies will be derived for several cases.

IV. Preview of Results

Passive outsiders: Sender $\mathcal{S}$ generates key $k_{\mathcal{SR}}$ and transmits it hop by hop to receiver $\mathcal{R}$. Thereby, each link is encrypted using the physical layer point-to-point keys. *Active outsiders:* Similar to a passive outsider, but each point-to-point communication is also authenticated by means of the available point-to-point keys. However, we cannot assure availability of the system in case of permanent jamming. *Passive insiders:* It is not possible to prevent the success of such an attack by using a single path and without asymmetric cryptography, since the whole communication between $\mathcal{S}$ to $\mathcal{R}$ is known to each forwarder $\mathcal{F}_{1,i}$. Thus we need at least one additional disjoint path. Then we could use one path for key transmission and the other one for communication. Alternatively, we can use both paths for transmission of two different keys $k_{\mathcal{SR}_1}$, $k_{\mathcal{SR}_2}$ and define $k_{\mathcal{SR}} = k_{\mathcal{SR}_1} \oplus k_{\mathcal{SR}_2}$, where $\oplus$ denotes the binary XOR. Also, it would be possible to exchange keys of half the length and concatenate them later to save transmission overhead [4]. However, parts of the key may reveal some plaintext information or, at least, the search space for a brute-force key attack shrinks. Thus, we recommend the XORing, since the combination of all but one key does not reveal any information.

Cooperating passive insiders: If at most m passive insiders cooperate and share their knowledge, we need at least $m+1$ disjoint paths for key distribution such that $k_{\mathcal{SR}} = \bigoplus_{i=1}^{m+1} k_{\mathcal{SR}_i}$. However, this is not always possible due to limited disjoint paths. A confidential key establishment is still possible, if there exists at least one path from $\mathcal{S}$ to $\mathcal{R}$ which is not controlled by a cooperative passive insider. Therefore, we could use all possible combinations of links between the nodes to exploit this ”trustworthy” path. We need to ensure that each cooperating groups does not have a member in every communication path.

In a $(k \times \ell)$ forwarder matrix, where the sender has a link to each forwarder in column 1, each forwarder in column i has a link to each forwarder in column $i+1$, and each forwarder in column ℓ has a link to the receiver, there exist about $(k!)^{\ell-1}$ link configurations. If we optimize to get all possible paths with least effort, we just need $k^{\ell-1}$ link configurations. However, this still means $k \cdot k^{\ell-1} = k^{\ell}$ partial keys.

In the full paper, we will present results on the probability of secure key exchange, which depends on the number of random paths and the number of forwarders per path.

References

[1] M. Bloch and J. Barros. *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[2] C. Boyd and A. Mathuria. *Protocols for Authentication and Key Establishment*. Springer, 2003.

[3] Federal Information Processing Standard Publication (FIPS PUB 197). Specification for the Advanced Encryption standard (AES), 2001.

[4] H. Ling and T. Znati. End-to-end pairwise key establishment using node disjoint secure paths in wireless sensor networks. *IJSN*, 2(1/2):109–121, 2007.

[5] U. M. Maurer. Secret Key Agreement by Public Discussion From Common Information. *IEEE Transactions on Information Theory*, 39(3):733–742, 1993.