Wireless Key Exchange with Long-Term Security

KIRILL MOROZOV (Research Team for Physical Analysis, RCIS, AIST)

General objective: Key exchange with information-theoretic security, which is *independent* of current computing technology.

Background idea (comes from [1,2]):

- Security relies on hardness of solving a problem of detecting and recovering a signal.
- No computer can help the attacker Eve to recover the signal completely, due to channel noise.
- Therefore, security of noise-based key exchange is *independent of current computer technology*, i.e. it is *long-term.*

Technical idea: How to ensure noise for attacker

- Fact: Multipath interference is a source of noise (see the figure on the right).
- Reciprocity principle (first used in [3]): For two stationary parties, the channel behaves in the same way for signals sent in either direction.

Reciprocity-based key exchange protocol (main idea)

1. Alice sends a predefined signal s.
2. Bob receives h * s,
   where h is impulse response, "*" is convolution.
3. Bob sends s.
4. Alice receives h * s.

Correctness: Alice and Bob agree on the same message h * s which can be used to compute a common key.

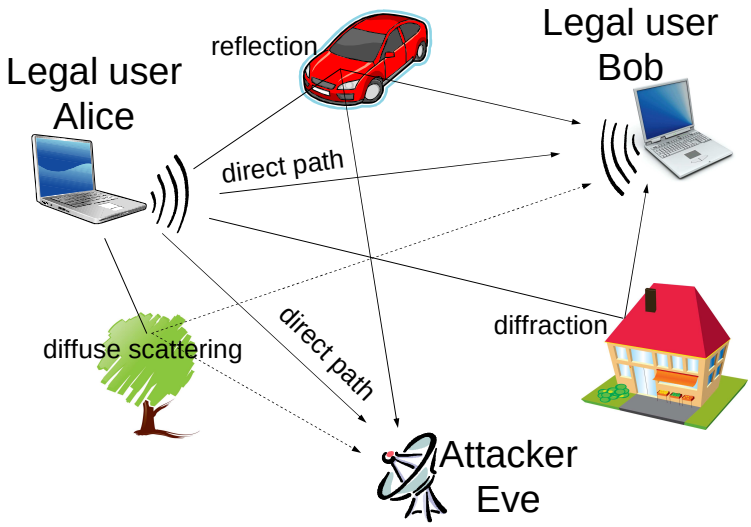

Figure: Multipath interference in wireless communications.

Security: Eve receives h_{AE}*s ≠ h*s and h_{BE}*s ≠ h*s, the difference between her measurements and h*s is due to spatial decoherence which is growing very fast with distance between Eve and either legal player, hence she *loses information* on h*s.

Privacy amplification [2] (that is some proper hash function, denoted by PA) is used by Alice and Bob to compute a common key K=PA(h*s), such that for Eve, PA(h_{AE}*s) and PA(h_{BE}*s) are independent of K.

Current research objective: Given a particular application, construct the corresponding security model and prove the prototype system of [4] (preliminary security evaluation in [5,6]) to be a long-term secure implementation of wireless key exchange.

Selected references:

1. A. Wyner, The wiretap channel, Bell Syst Tech. J., vol. 54: 1355-1387, 1975.
2. U.M. Maurer, Secret key agreement by public discussion from common information. IEEE-IT 39(3): 733-742, 1993
3. C.H. Bennett, G. Brassard, C. Crépeau, U.M. Maurer, Generalized privacy amplification. IEEE Trans. IT 41(6): 1915-1923, 1995.
4. J.E. Hershey, A.A. Hassan, R. Yarlagadda, Unconventional cryptographic key agreement for mobile radio. IEEE Trans. Comm 43: 3-6, 1995.
4. T. Aono, K. Higuchi, T. Ohira, B. Komiyama, H. Sasaoka, Wireless Secret Key Generation Exploiting Reactance-Domain Scalar Response of Multipath Fading Channels. IEEE Trans. Antennas and Propagation 53(11): 3776-3784, 2005.
5. H. Imai, K. Kobara, K. Morozov, On the possibility of key agreement using variable directional antenna. JWIS'06: 153-167, 2006.
6. T. Hashimoto, T. Itoh, M. Ueba, H. Iwai, H. Sasaoka, K. Kobara, and H. Imai, Comparative studies in key disagreement correction process on wireless key agreement system. WISA'08: 173-187, 2008.

Impact to Society: Long-term secure systems for protecting sensitive information

無線通信を用いた長期的セキュリティを有する鍵共有

情報セキュリティ研究センター　モロゾフ　キリッル

- 二つの無線ネットワークデバイスが安全に通信を行うためには、まず秘密鍵について合意を行うことが必要です。
- この鍵共有プロトコルにおいて、無線伝送路の雑音パターンがそれらデバイスの位置に特有のものであることを用いると、非常に強力な計算能力を持つ攻撃者に対しても永続的な安全性を持つような方式が可能となります。