Key Exchange in Wireless Networks with Physical Layer Security

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

General objective: Secure key exchange using wireless channel noise

Basic facts:

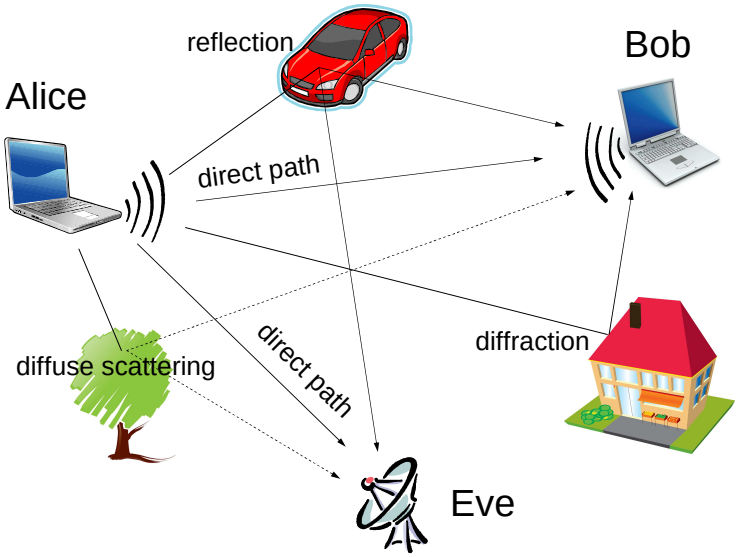
- Multipath interference is one source of noise
- Reflections and diffractions occur at large metallic objects, scattering/attenuation by dielectric media
- Wireless channel is characterized by the impulse response h

Reciprocity principle (simplified):

- For two stationary parties, the channel behaves in the same way for signals sent in either direction, i.e. $h_{AB} = h_{BA} = h$

Reciprocity-based key exchange protocol (basic idea)

1. Alice sends a predefined message f
2. Bob receives h * f, "*" is convolution
3. Bob sends f
4. Alice receives h * f



Correctness: Note that Alice and Bob agree on the same message

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

Privacy amplification* [2] (its function is denoted by PA) can be used by Alice and Bob to compute a shared key K = PA(h*f), such that for Eve, PA(h_{AE}*f, h_{BE}*f) is almost completely independent of K

* Think of PA as some properly chosen hash function

Advanced security details: In reality, Alice and Bob receive slightly different signals due to noise, but it can be fixed using error-correcting codes; PA can be adjusted accordingly

- Eve may also try to intervene into the information exchange, but proper authentication can prevent such an attack

Current research objective: Construct an adequate security model, prove the above protocol secure (under some reasonable assumptions), and argue that the prototype [5] is a secure implementation of reciprocity-based key exchange in this model

Selected references:

1. U.M. Maurer, Secret key agreement by public discussion from common information. IEEE Trans. IT 39(3): 733-742 (1993)
2. C.H. Bennett, G. Brassard, C. Crépeau, U.M. Maurer, Generalized privacy amplification. IEEE Trans. IT 41(6): 1915-1923 (1995)
3. J.E. Hershey, A.A. Hassan, R. Yarlagadda, Unconventional cryptographic key agreement for mobile radio. IEEE Trans. Comm 43: 3-6 (Jan,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: Bringing ultimate protection to wireless key exchange

National Institute of Advanced Industrial Science and Technology
AIST

Research Center for Information Security

Key Exchange in Wireless Networks with Physical Layer Security

Kirill Morozov (RCIS, AIST)

RCIS Workshop 2009

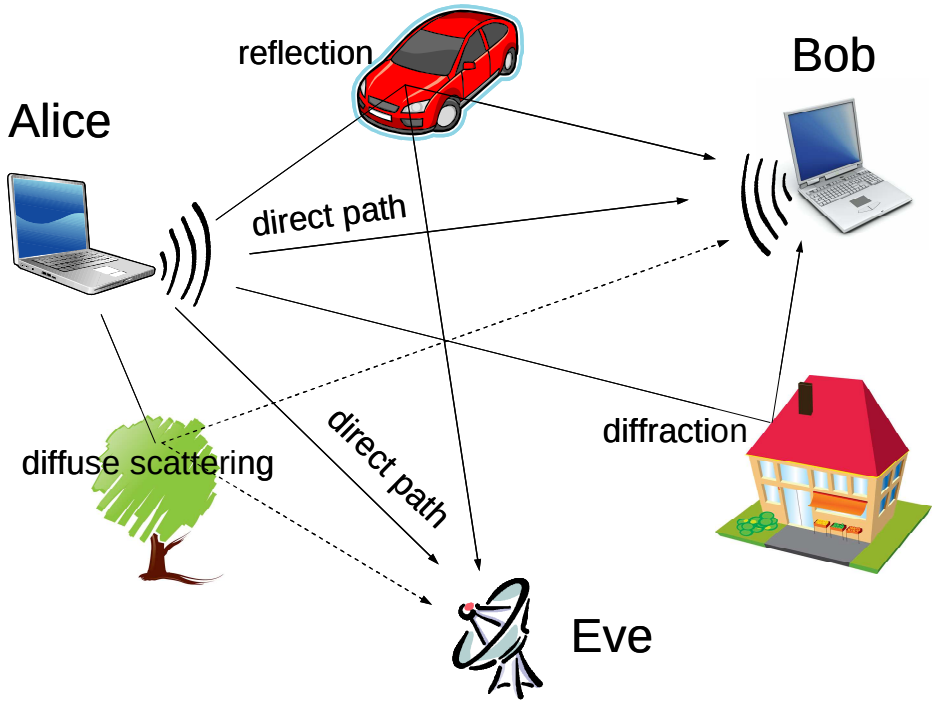
UDX Theater, Tokyo

May 15, 2009

Wireless Key Exchange

- Current approach in wireless key exchange: To use computationally secure cryptographic algorithms (such as RC4, AES, RSA etc)
- Alternative approach: To use wireless channel noise
  - Originates from the work of Wyner in 1975, later developed by Maurer, Ahlswede, Csizar in early 90-ies
  - Achieves information-theoretic security, i.e. protection against *computationally unbounded*(!) adversary
- Reciprocity-based key exchange scheme
  - Originates from a series of papers by Hershey et al in 90-ies
  - Recently attracted attention due to the (first) experimental prototype by Aono et al, IEEE Transactions on Antenna and Propagation (2005)

Wireless Channels as Source of Noise

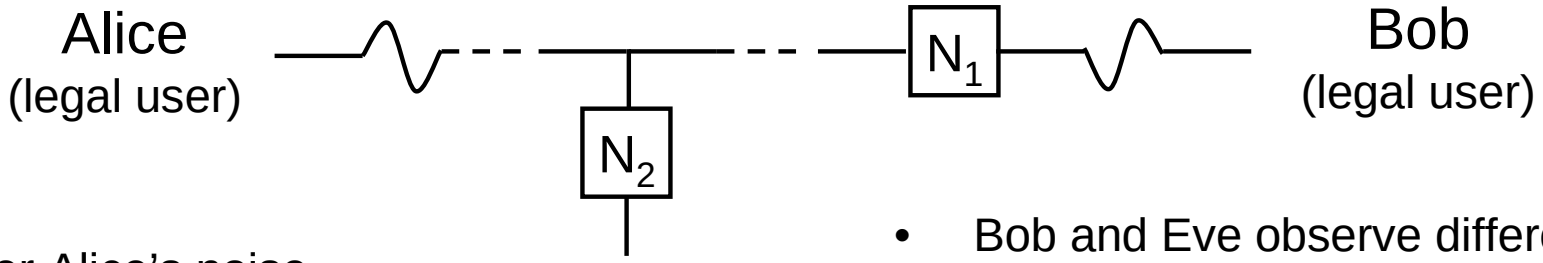


- Multipath-interference is one source of noise
- Reflections and diffractions occur at large metallic objects; scattering/attenuation by dielectric media
- Assume that Eve is not very close to either Alice or Bob
- Then, the noise pattern for Eve is *very different* from the noise pattern of Bob due to spatial decoherence

- Reciprocity principle (from communication theory): the wireless channel impulse response is quite similarly between two stationary points, no matter the direction of signal propagation
- Corollary: The noise pattern for Alice is *very similar* to that of Bob
- Basic idea [Hershey et al '95]: Alice and Bob send each other a publicly known fixed message, obtain the noise patterns and use them as data for computing shared key

Wiretap Scenario

- In fact, we are in the famous wiretap scenario:



- Consider Alice's noise pattern as an input to some imaginary channel
- Bob and Eve observe different (uncorrelated) noise vectors
- N_2 is "noisier" that N_1, due to decoherence

- It is well known that Alice and Bob can compute information-theoretically secure key in this scenario
  - *Ideally*, no matter how much computing power Eve has, she cannot restore information which is lost due to noise
- Here, only a basic idea is presented, the actual system is somewhat more complicated
  - In particular, it uses variable directional antenna for randomization

Concluding Remarks

- We propose to use this scheme for *increasing security* of the current cryptographic techniques
  - A physically secure key can be combined with a (standard) computationally secure key, so that Eve *must break computational key exchange many times* in order to succeed
- Ongoing and future research:
  - Evaluating security against different attacks: active attacks, environment reconstruction, side channel etc
  - Develop an adequate security model for rigorous proof of security (under some reasonable assumptions)