Mobility Assisted Secret Key Generation Using Wireless Link Signatures*

SCHOOL OF COMPUTING

Junxing Zhang†, Sneha Kasera†, Neal Patwari‡

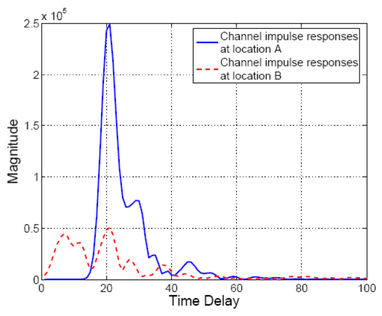
THE UNIVERSITY OF UTAH

†School of Computing, ‡Dept. of Electrical & Computer Engineering, University of Utah

Introduction

Signature Based Key Generation

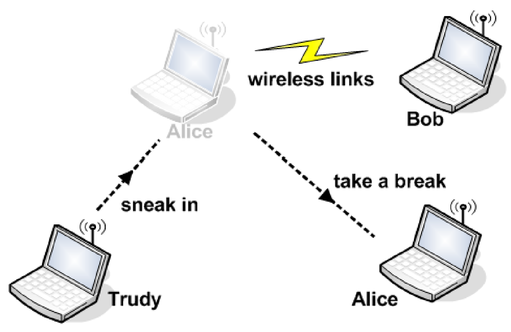
- wireless link signature
  - multiple paths caused by radio waves
  - their measurements are good "signature" of links
- link signatures measured almost symmetrically at two ends of wireless link, but cannot be measured from another location
- use for secret key establishment



Multipath properties at two locations

Why Device Mobility?

- problem: location locking attack

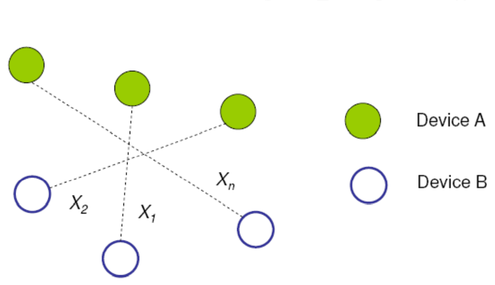


- rely on movement in environment
  - Jana et al. [1] show adversary can cause predictable movement in environment, fool endpoints to extract deterministic keys
- devices move to cause wireless variations
  - but must move continuously during key generation

Our Approach

- wireless devices sample link signature space in physical area
- collect measurements at different unpredictable locations
- combine them to produce strong keys

$$\text{Secret Key} = f(X_1, X_2, X_3, \ldots X_n)$$



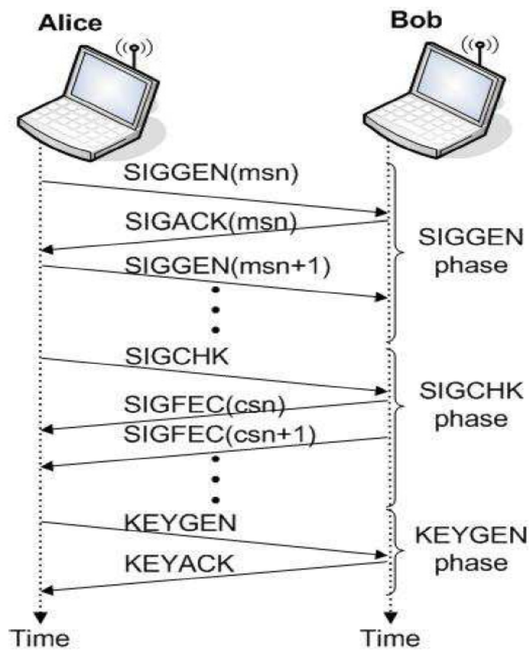
Methodologies

Adversary Model

- overhear all communication between two devices Alice, Bob
- can be at some of locations of Alice, Bob but not all
- does not address man-in-the-middle (authentication) or denial-of-service

Mobility Assisted Protocol

- move between channel probes
- remove correlated measurements, quantize, and encode
- parity symbols fix reciprocity error



Building Blocks

- uniform quantization
  - reciprocal error
  - when increasing quantization bit number, reciprocal error grows dramatically
- jigsaw encoding
  - further encode each uniformly quantized value with multiple values

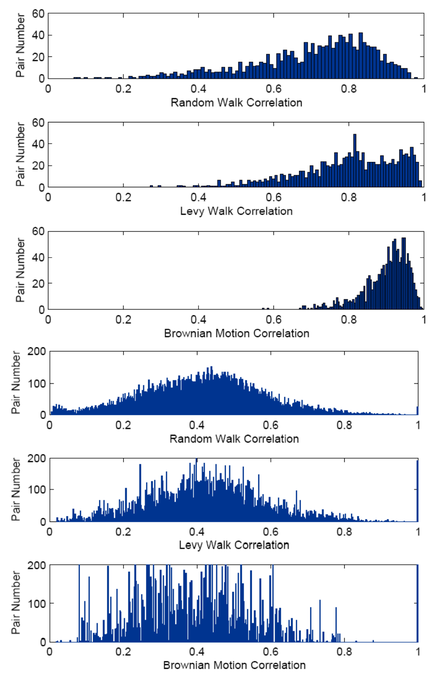
Quantization Bit Number	1	2	3	4	5	6	7	8
Uniform Quantization	0.006	0.09	0.20	0.37	0.48	0.65	0.76	0.84
Jigsaw Encoding	0.003	0.02	0.03	0.04	0.04	0.04	0.04	0.04

- Reed-Solomon forward error correction
  - send parity symbols only
  - constrain correction capability according to reciprocal error
  - make discovery of signature using brute force and public parity symbols computationally infeasible

Evaluation

Mobility Models

- models to study impact of device mobility
- three mobility models chosen, they are decreasingly less diffusive
- observations

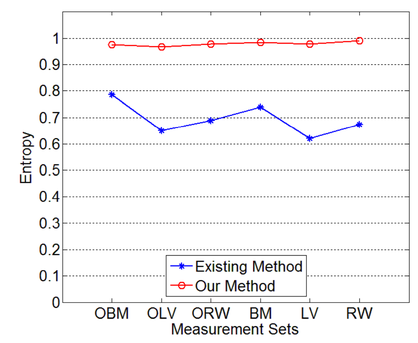


more diffusiveness result in less correlation

larger than one foot step-size results in uncorrelated measurements

Quality of Keys

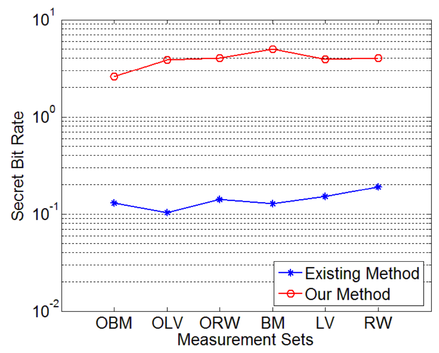
- pass eight randomness tests in NIST suite
- consistently higher entropy values in all measurement sets compared to existing method



OBM, OLV, ORW are outdoor Brownian motion, levy walk, random walk sets; BM, LV, RW are indoor sets from the respective models

Efficiency of Key Extraction

- secret bit rate
  - average number of secret bits extracted from each channel response
  - order of magnitude higher than existing method



References

[1] Suman Jana, Sriram Premnath Nandha, Michael Clark, Sneha Kumar Kasera, Neal Patwari, and Srikanth Krishnamurty, "On the Effectiveness of Secret Key Extraction Using Wireless Signal Strength in Real Environments." Mobicom 2009, Beijing, China.

[2] Junxing Zhang, Sneha Kumar Kasera, and Neal Patwari, "Mobility Assisted Secret Key Generation Using Wireless Link Signatures." To appear in INFOCOM Mini-Conference 2010, San Diego, CA.

* This research is funded in part by the National Science Foundation and the Army Research Lab.