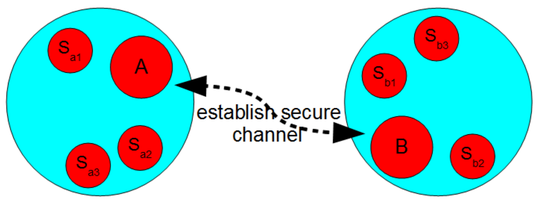
Efficient High Rate Secret Key Extraction in Sensor Networks Using Collaboration

Sriram Nandha Premnath, Neal Patwari, Sneha Kumar Kasera
University of Utah

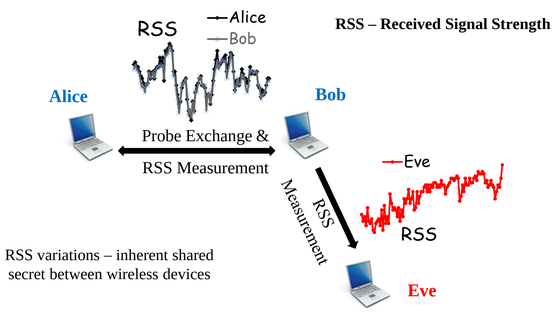
Introduction

- secret key establishment - fundamental requirement for private communication
- **problem:** two groups of sensors need to establish secure channel
- we explore use of inherent randomness in wireless channel for extracting secret key bits



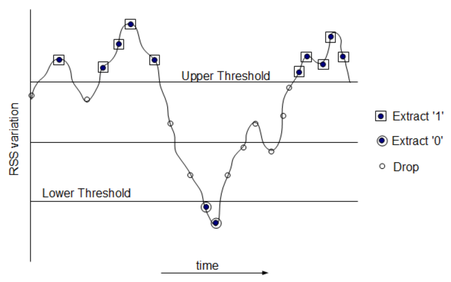
Key Establishment among Two Nodes

Inherent Shared Secret



RSS variations – inherent shared secret between wireless devices

Converting RSS into Bits



- random variations caused by reflection, refraction, scattering, diffraction, mobility etc.
- signals from Alice to Bob & Bob to Alice, traverse same path; so they see similar RSS variations

Secret Key Extraction Process

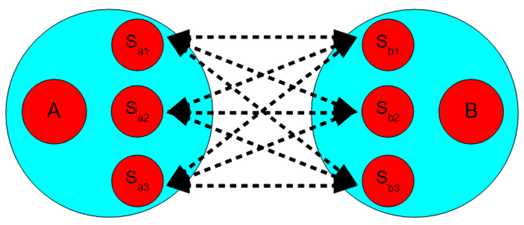
RSS Measurements → Interpolation → Quantization → Information Reconciliation → Privacy Amplification → Secret Key Bits

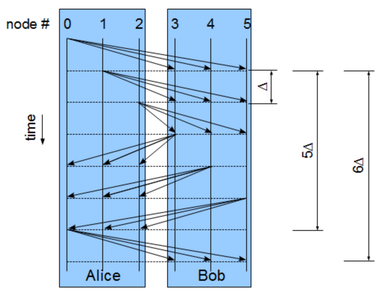
- simultaneous measurements not possible with half-duplex systems
- interpolation – for estimating measurements at common time instant
- quantization – for converting estimates into bits
- information reconciliation – for handling potential bit mismatches
- privacy amplification – for extracting high entropy bits

Key Establishment among Two Groups of Nodes

- nodes collaborate in exchanging probes and collecting measurements
- leverage wireless channel variations between different node pairs

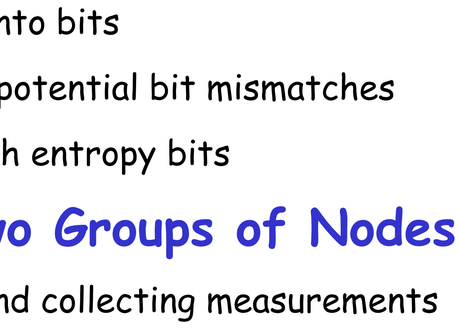
Question: Will collaboration help in establishing *stronger* secret keys at *higher efficiency*?



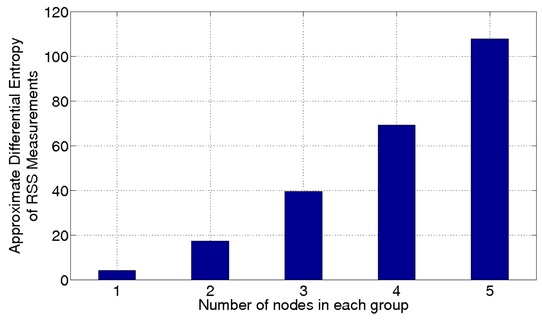


Experimental Setup

- 2 groups of 5 TelosB sensors each arranged in circular pattern
- {A1, B1} ϵ slow-walk experiments
- {A2, B2} ϵ iRobot rotation experiments
- BS – base station
- A1, A2 – stationary; B1 is mobile; B2 rotates in place
- Distance(A1, B1) ~ 4-15 ft; Distance(A2, B2) ~ 10 ft



Approx. Differential Entropy of RSS measurements



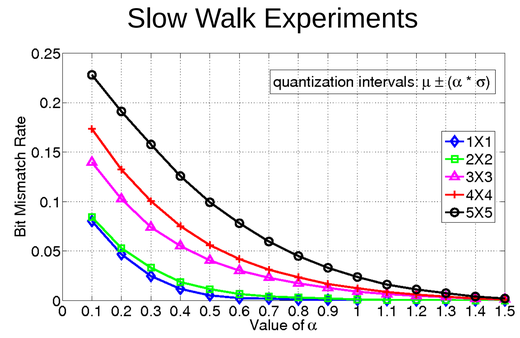
- Approx. differential entropy, $H(X) = \log\sqrt{(2\pi e)^{N^2}|\Sigma|}$
  - X - random vector of length N^2
  - $|\Sigma|$ - determinant of covariance matrix
- $H(X)$ quadratic in no. of nodes, N
  - more randomness with higher N
  - **stronger secret keys extracted!**

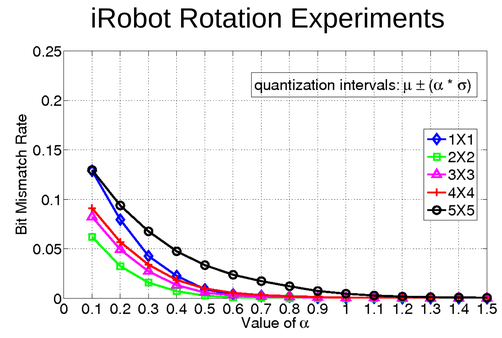
Entropy of output secret bits

- entropy per bit calculation using NIST test suite's approximate entropy test
- entropy ≈ 1, the ideal value

Configuration	Entropy	
	slow-walk experiments	rotation experiments
1 X 1	0.9842	0.9891
2 X 2	0.9874	0.9815
3 X 3	0.9809	0.9862
4 X 4	0.9858	0.9785
5 X 5	0.9873	0.9806

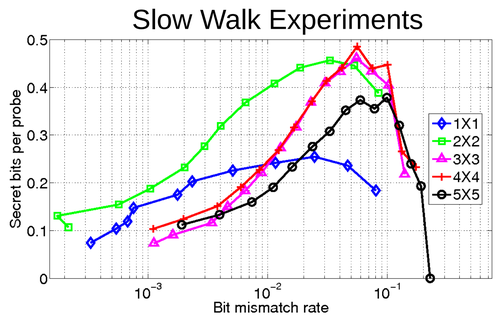
Bit mismatch rate

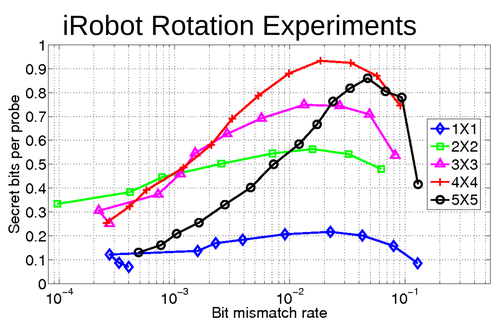




- mismatch increases with N; decreases with quantization parameter α
- mismatch is higher with walk experiments – large & variable distance introduces more noise in the measurements

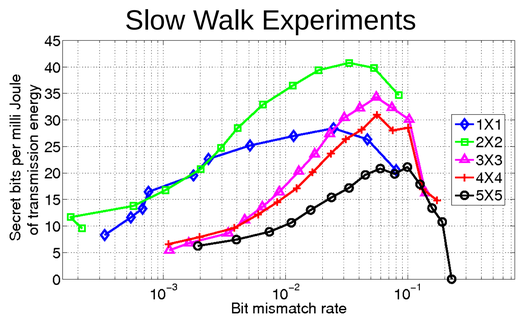
Secret bits per probe packet

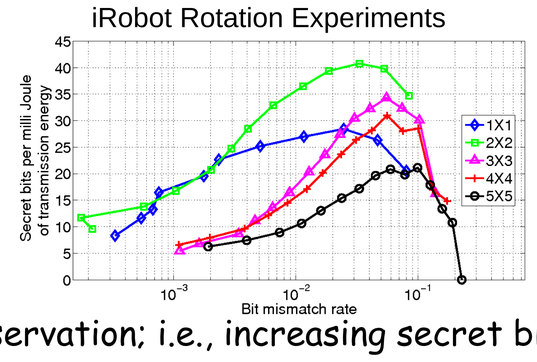




- collaborative probe exchange & simultaneous recording of measurements increases secret bits extracted per probe packet
- slow-walk experiments – **up to 80% increase** over 1X1 case
  rotation experiments – **up to 343% increase** over 1X1 case

Secret bits per Joule of transmit energy

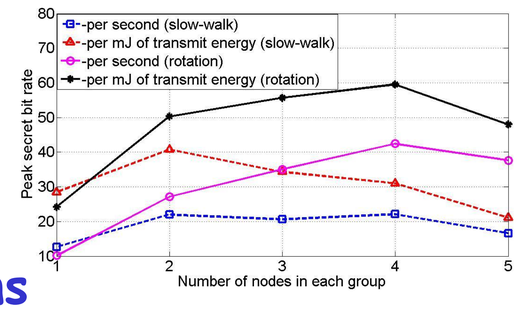




- collaboration helps in energy conservation; i.e., increasing secret bits per Joule of transmit energy
- slow-walk experiments – **up to 46% increase** over 1X1 case
  rotation experiments – **up to 146% increase** over 1X1 case

Performance Tradeoff with Collaboration

- extract stronger keys by increasing N
- but secret bit rates peak at relatively small values of N
- increase in mismatch with N offsets gain in secret bit rates



Conclusions

- significant increase in secret bit per probe, per Joule due to collaboration
- performance trade-off due to increase in measurements vs. increase in bit mismatch rate
- **future work:** investigate transmission scheduling and grouping strategies to further increase differential entropy

References

1. S. N. Premnath, N. Patwari, and S. K. Kasera. Efficient High Rate Secret Key Extraction in Wireless Sensor Networks using Collaboration. IEEE SECON Conference, 2010 (submitted).
2. S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy. On the effectiveness of secret key extraction from wireless signal strength in real environments. In ACM MOBICOM Conference, Sept. 2009.