Extracting a Secret Key from a Wireless Channel

Suhas Mathur, Wade Trappe, Narayan Mandayam (WINLAB, Rutgers University), Chunxuan Ye, Alex Reznik (InterDigital)

**Introduction**

**Why extract bits from the channel?**
- Unconditionally secure – even if adversary has unbounded computational power
- Channel decorrelates rapidly in:
  - **Space**: Eve’s channel is uncorrelated if she is > λ/2 away
  - **Time**: Natural source of randomness

**Collecting correlated information**

Alice $X^n = \{X_1, \ldots, X_n\}$
Bob $Y^n = \{Y_1, \ldots, Y_n\}$

**Algorithm**

**Alice**
- Find locations of excursions in $X^n$ of size $\geq m$, e.g., \{6, 27, 42, 52, \ldots\}
- Send a random subset to Bob $L = \{6, 42, 52, \ldots\}$

**Bob**
- Find the set of indices $L \subseteq L$ where $Y^n$ has excursions of size $\geq m - 1$
- If $\frac{1}{m} < \epsilon < \frac{1}{2}$, for some $0 \leq \epsilon \leq \frac{1}{2}$, declare message not sent by Alice

**ELSE**
- Compute $Q(X^n(L)) = q$. The first $N_0$ bits are the key $K_m$. Remaining $N = N_0$ bits are secret key $K$.
  - Send $\{L, MAC(K_m, L)\}$ to Alice

**Experimental evaluation**

**Using CIR from 802.11**
- CIRs of Alice and Eve
- Modified 802.11 board

**Using RSSI on plain 802.11**
- 20 PING pkts per sec

**Performance**

**Prob. of bit error**
- Rate of s-bits/sec

**Rate of s-bits/sec**
- Doppler = 10 Hz
- Rate $\approx$ Rate of change of channel
- Probes / sec $\times 10^3$

**Dependence on channel**
- Running faster won’t always help unless accompanied by increase in probing rate

**Experimental results**
- ~ 1.2 s-bits/sec indoors
- ~ 1.1 s-bits/sec indoors

**Attacks**

**Fake messages:**
- Reply message is protected by a msg authentication code
- Spurious indices in the List message can either
  - reduce the rate (if Bob has no excursion at the index)
  - reveal Eve’s presence (if Bob has an excursion)

**Fake Probes:**
- Test each probe for similarity against recently recd. probes
- Hypothesis testing approach
- Use one-way hash chains at Alice and Bob
- Pre-construct a chain at each user
- Reveal elements of hash-chain in reverse order