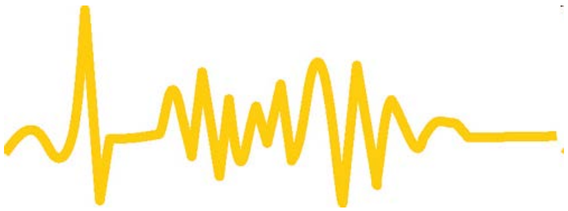
# Securing Data Provenance using Link Fingerprints in Body Area Networks

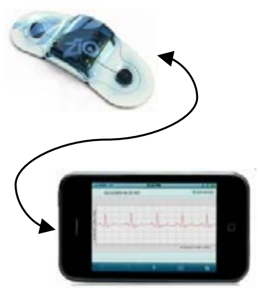

- Syed Taha Ali (UNSW)
- Vijay Sivaraman (UNSW)
- Diethelm Ostry (CSIRO)
- Sanjay Jha (UNSW)

# Introduction

- The market for wearable wireless sensors is projected to grow to more than 420 million devices by 2014.

- Fundamental applications in patient monitoring, personalized healthcare, telemedicine, and athlete training.



**1. Apple iPhone SensorStrip**

**2. Nike + iPod Sports Kit**

**3. Nokia Sports Tracker**

**4. Toumaz Life Pebble**

- Security is critical because these devices generate medical data, and challenging given that they have low power and computation capabilities.

# Data Provenance

¤ Provenance may be defined as a record of the origin and evolution of data within the network. It allows for an objective evaluation of the **trustworthiness** of the data.

¤ Application: Alice who is informed by her insurance provider that they will cut her rates if she gives up smoking – to ensure compliance, they provide her with a bodyworn sensor device

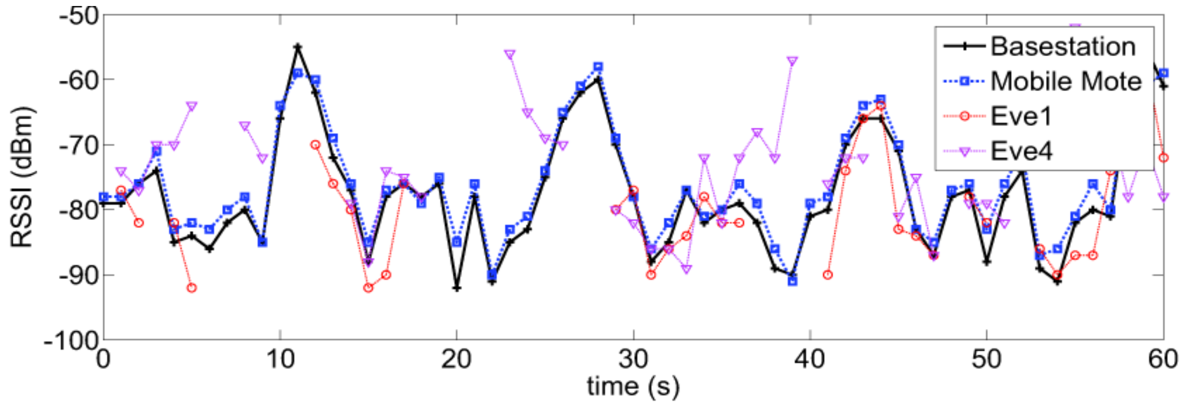
¤ The **identity transference attack** - Alice can affix the sensor on to a non-smoker friend for the duration of the trial

¤ It would help to have information about the sensor data – e.g. what are the most common sensor data offload points, Alice's smartphone, Alice's home WiFi network, Alice's gym, etc.

# Our Contributions

- Our goal is to fingerprint the wireless link between sensor device and data offload point (i.e. basestation) in a **secure**, **lightweight**, and **non-repudiable** way.

  - **We describe a way to fingerprint the wireless link between two parties by exploiting the intrinsic symmetry in wireless channel characteristics**

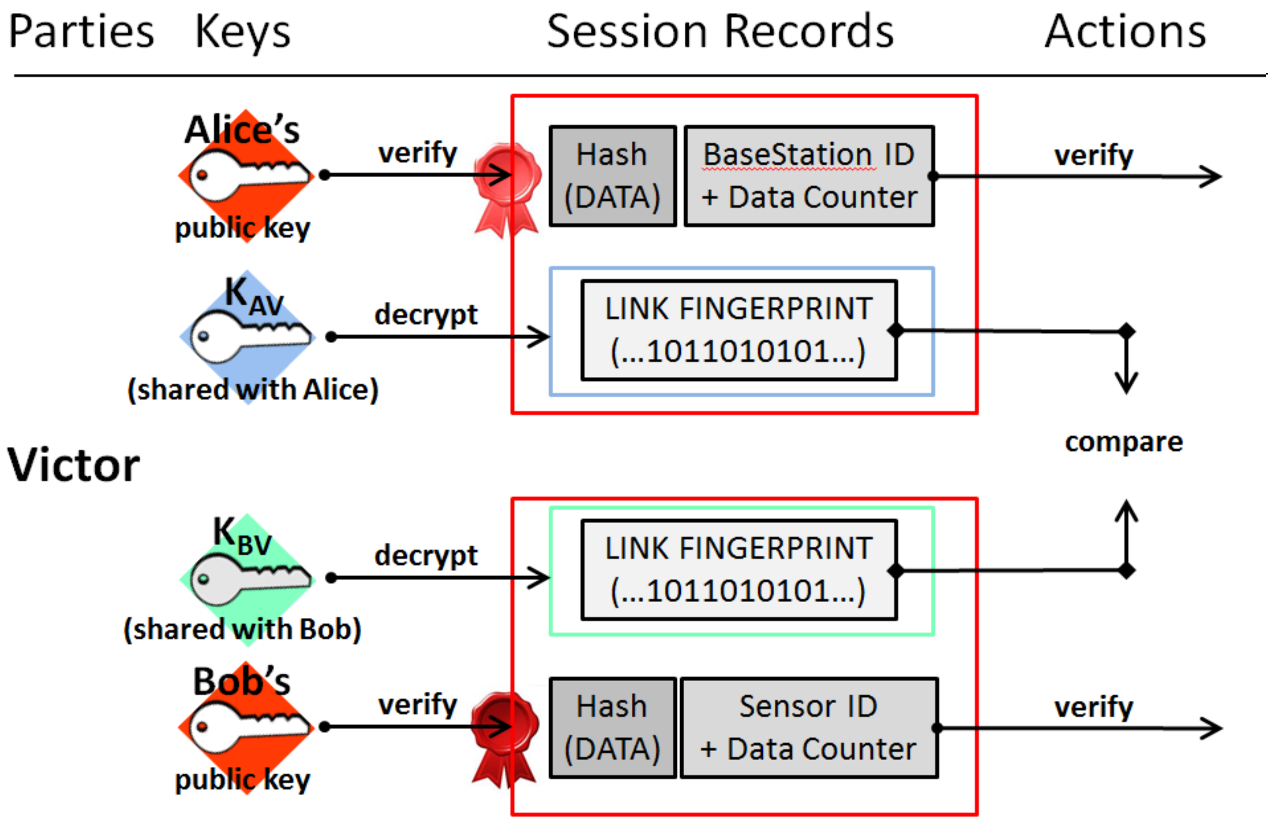



  - **We present experimental results confirming that this solution generates usable link fingerprints for typical bodyworn sensor applications**

  - **We optimize the fingerprinting process to reduce memory and transmission overheads for resource constrained devices**

# Data Provenance Protocol

- Alice = bodyworn sensor
- Bob = basestation (smartphone, WiFi AP, etc.)
- Victor = verifying party (insurance agency, forensics, etc.)




- Encryption keeps fingerprint **secret** (from all except Victor)
- Signature ensures **authenticity** and **non-repudiation**
- Session record also provides **accountability** – i.e. Alice can ensure that Bob or Victor don't tamper with the data

# Protocol

## Alice

- Keys: $K_{AV}$, ($K_A^+$, $K_A^-$)
- Sign ([H(data), DeviceID, counter, Enc(LinkFingerprint-A, $K_{AV}$)], $K_A^-$)

## Bob

- Keys: $K_{BV}$, ($K_B^+$, $K_B^-$)
- Sign ([H(data), DeviceID, counter, Enc(LinkFingerprint-B, $K_{BV}$)], $K_B^-$)

## Victor

- Keys: $K_{AV}$, $K_{BV}$, $K_A^+$, $K_B^+$
- Verify ([H(data), DeviceID, counter, Dec(LinkFingerprint-A, $K_{AV}$)], $K_A^+$)
- Verify ([H(data), DeviceID, counter, Dec(LinkFingerprint-B, $K_{BV}$)], $K_B^+$)
- Compare (LinkFingerprint-A, LinkFingerprint-B)

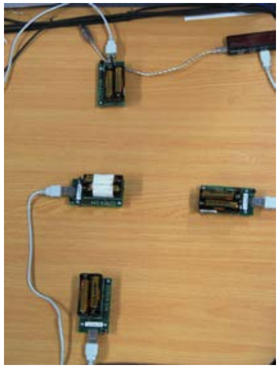
# Link Fingerprinting

- Considerable interest recently in ‘physical layer security’
- The wireless channel between Alice and Bob is
  - **symmetric**
  - **highly sensitive to spatio-temporal changes**
  - **cannot be deciphered in detail by eavesdropper (6~13 cm zone)**
- Alice and Bob can use these shared channel characteristics to generate a shared secret known only to them
- Technique has been applied very successfully in secret key agreement, authentication, and location distinction

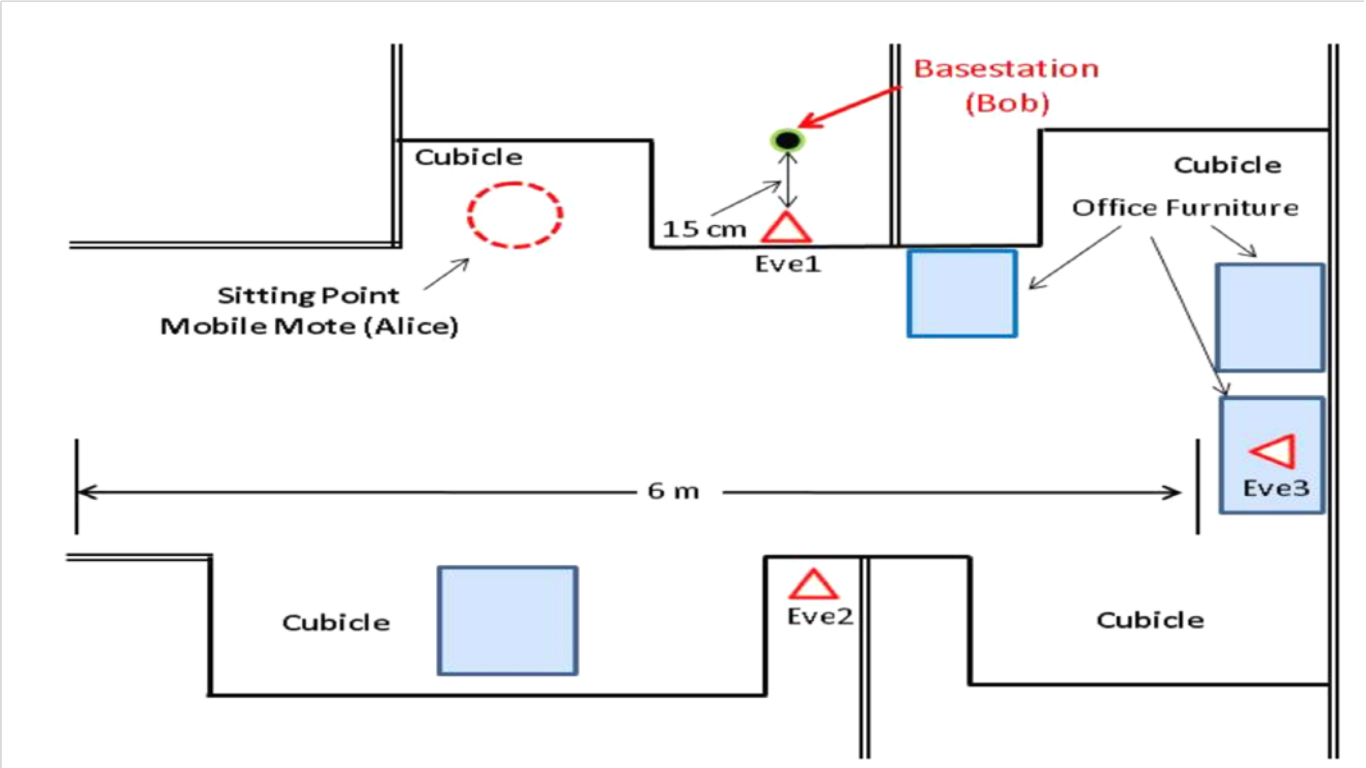
# Experimental Setup

- Bodyworn Device –Alice (MicaZ mote)

- Basestation – Bob, Eve(s)

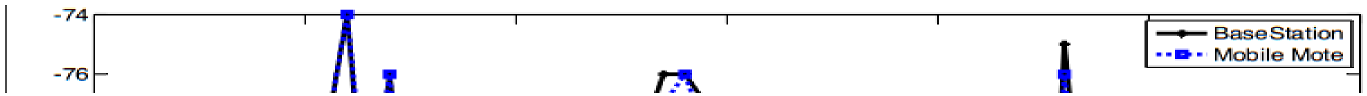


- Indoor Office Environment



# Results

- Variation in RSSI vs. time

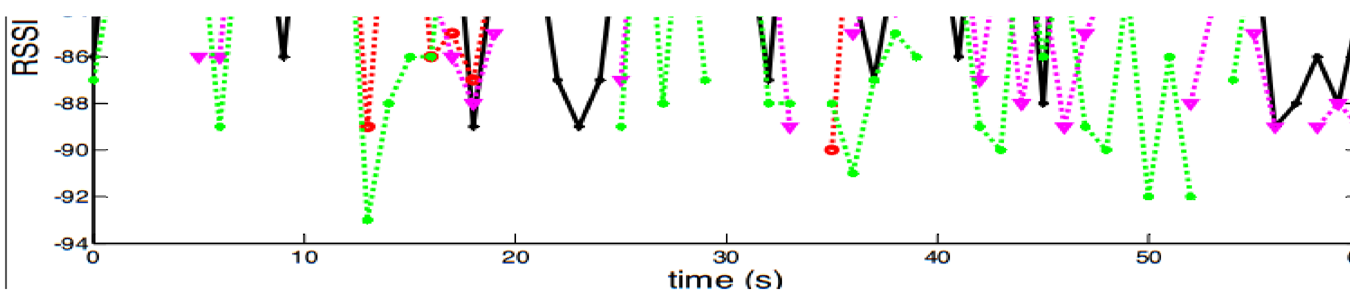



**Alice and Bob**

Table 1: Correlation coefficient ($r$) of RSSI measurements observed by various parties

| Experiment | Alice-Bob ($r$) | Alice-Eve1 | Alice-Eve2 | Alice-Eve3 |
|---|---|---|---|---|
| *High Activity* | 0.974 | 0.197 | 0.088 | 0.038 |
| *Low Activity* | 0.950 | 0.129 | 0.102 | 0.158 |
| *High Activity* (filtered) | 0.986 | 0.281 | 0.118 | 0.065 |
| *Low Activity* (filtered) | 0.976 | 0.205 | 0.152 | 0.224 |

**Bob and Eves**



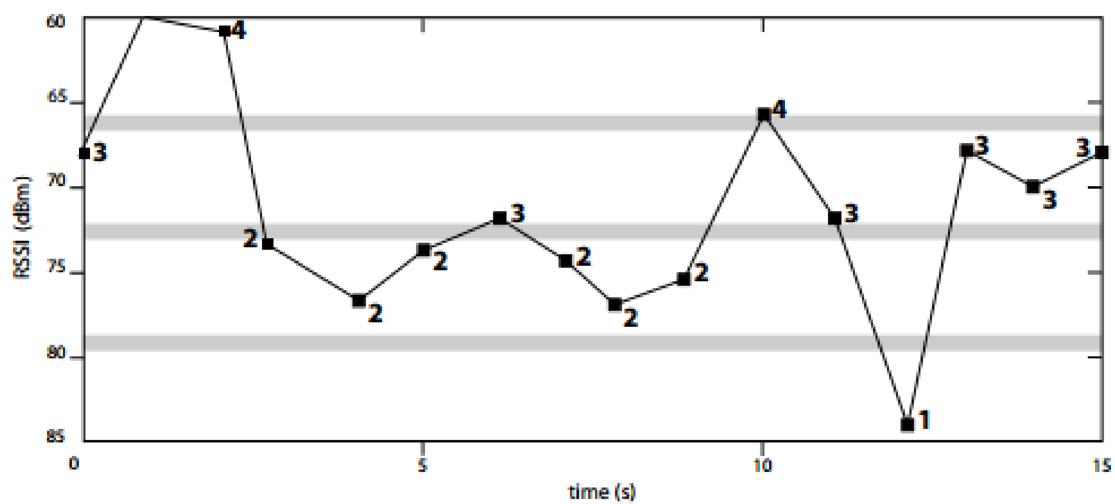
# Optimization



- Storing and signing RSSI information for entire data transaction is not practical

- **Solution**: quantize RSSI information to reduced length bitstring

## Level Crossing Quantization
## Ranking Quantization




$q+ = \mu + \alpha\sigma$
$q- = \mu - \alpha\sigma$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 |

# Performance

| Activity (Quantization) | Fingerprint Agreement | Bit (bit/s) | Min. Session Length (mins) | Eve1 Agreement | Eve2 Agreement | Eve3 Agreement | Entropy |
|---|---|---|---|---|---|---|---|
| *High Activity* (Level Crossing) | 98.40% | 0.205 | 10.41 | 47.11% | 46.48% | 47.34% | 0.997 |
| *Low Activity* (Level Crossing) | 95.53% | 0.139 | 15.35 | 46.26% | 46.80% | 47.60% | 0.997 |
| *High Activity* (Ranking) | 93.60% | 2 | 2.13 | 44.39% | 46.92% | 48.74% | 1 |
| *Low Activity* (Ranking) | 96.08% | 2 | 2.13 | 50.54% | 50.41% | 52.92% | 1 |

**Table 2: Link fingerprint performance for experimental scenarios**

- Results highlight the advantages/disadvantages of quantizers:

- **Ranking can be used for lossless multi-bit quantization with high key generation rate which is good for small session times**

- **Level crossing is better for larger session times and shows higher fingerprint agreement**

- **Customized quantizers can be developed too as per application**

# Conclusion

- Our solution takes 2-10 minutes to fingerprint a wireless link

- Positive first step in using wireless channel characteristics for provenance (lightweight alternative to crypto-based solutions)

# Future Work

- extending this idea to multihop networks to fingerprint the entire wireless path
- fingerprinting links in delay-tolerant networks
- amortizing digital signature costs over multiple session records (using Merkle trees, coding?)

---

THANK YOU for LISTENING