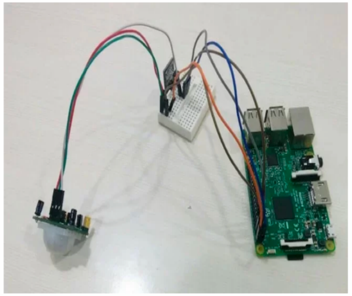
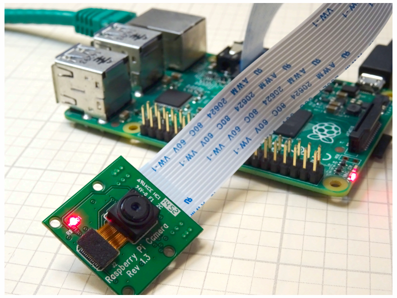
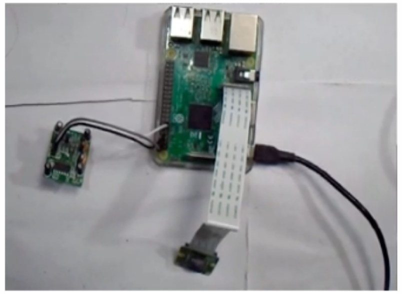
How difficult is it to build an IoT device?



Smart temperature sensor



IP Camera



Baby monitor

Heterogeneity: Standards

- Bluetooth Low Energy (BLE)
- 6LoWPAN
- LoRA
- MQTT
- LTE Cat0
- IEEE 802.15.4
- Internet 0
- RFID
- Sigfox
- Smartdust
- Tera-play
- Xbee
- Z-Wave

Heterogeneity: Hardware

Table I
CROSS-SECTION OF CURRENT MOTE PLATFORM SPECIFICATIONS

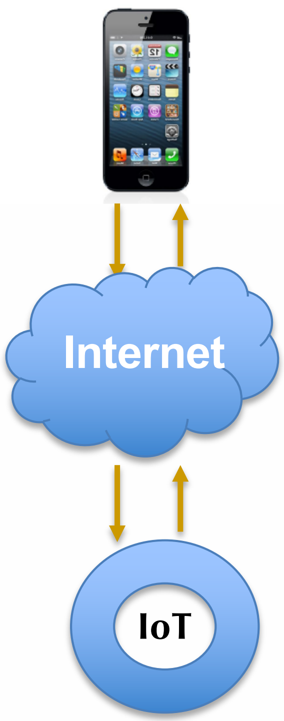
Device	MCU	Word Size	Clock
Imote 2 [12]	Intel PXA271	32 bit	104 MHz
INGA [13]	ATmega 1284p	8 bit	8 MHz
Mulle v5.2 [14]	Renesas M16C/62P	16 bit	10 MHz
SunSPOT v6 [15]	AT91SAM9G20	32 bit	400 MHz
TelosB [16]	TI MSP430F1611	16 bit	4 MHz
XM1000 [17]	TI MSP430F2618	16 bit	8 MHz

Heterogeneity: Platforms

- Arduino
- Contiki
- Electric Imp
- Gadgeteer
- ioBridge
- Raspberry Pi
- SensorTag
- TinyOS
- Wiring
- Xively
- ....

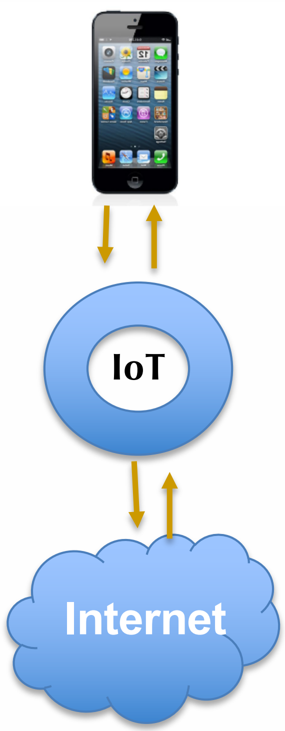
Typical Operational Models

External Server



Eg: Nest Protect Alarm

Direct Access



Eg: Philips Hue Lamps

Transit

Eg: Fitbit Flex

Philips Hue Lamps

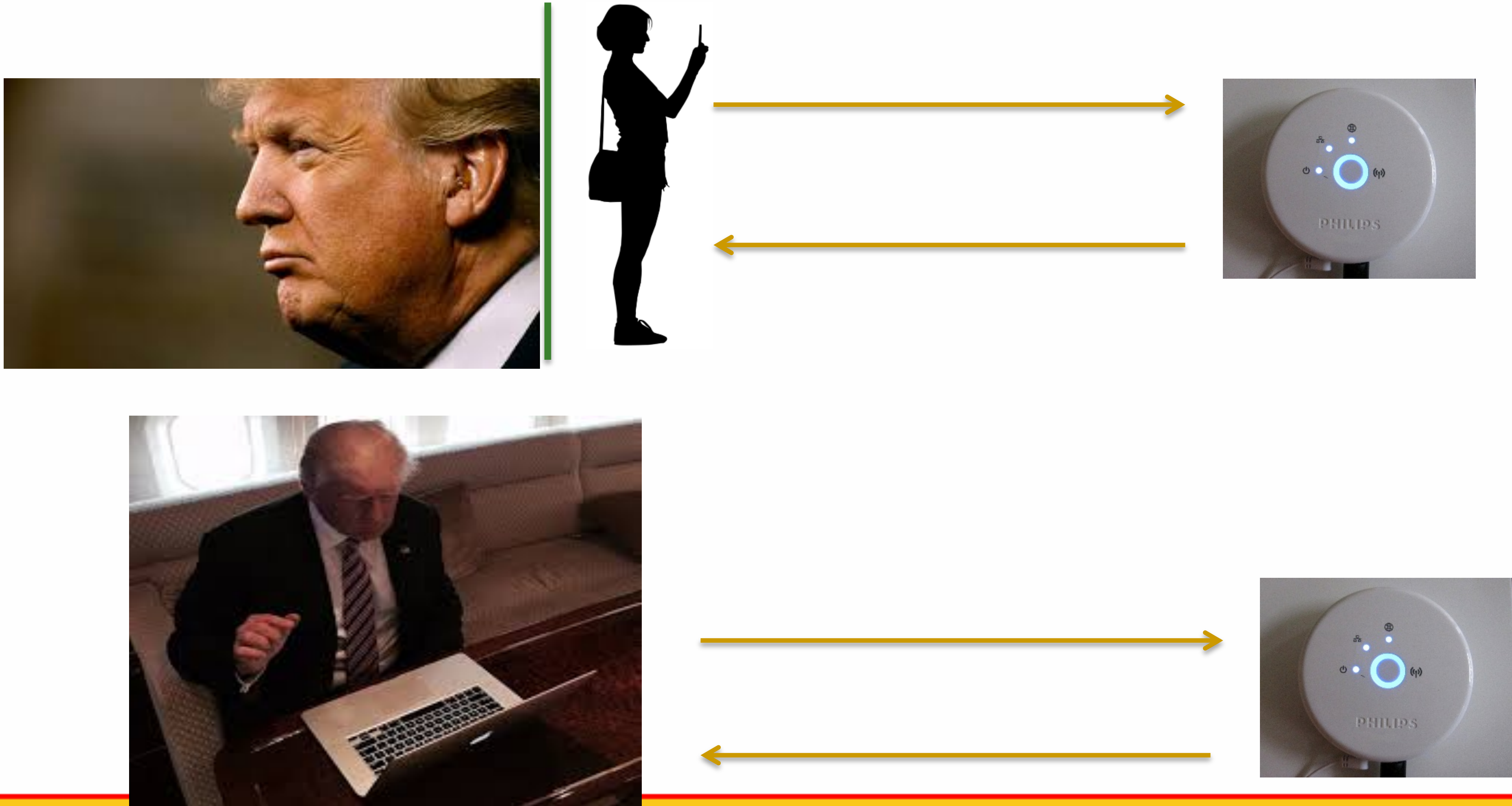
- One of the oldest IoT devices on the market (since 2011).
- Ability to control lights via a smartphone app.
- Highly Customizable and work with a lot of 3rd party services like IFTTT (eg: blink the light if someone sends me a message on facebook)

Communication Process

- Phone talks directly to the hue bridge and bridge then relays appropriate commands to the lights using zigbee.

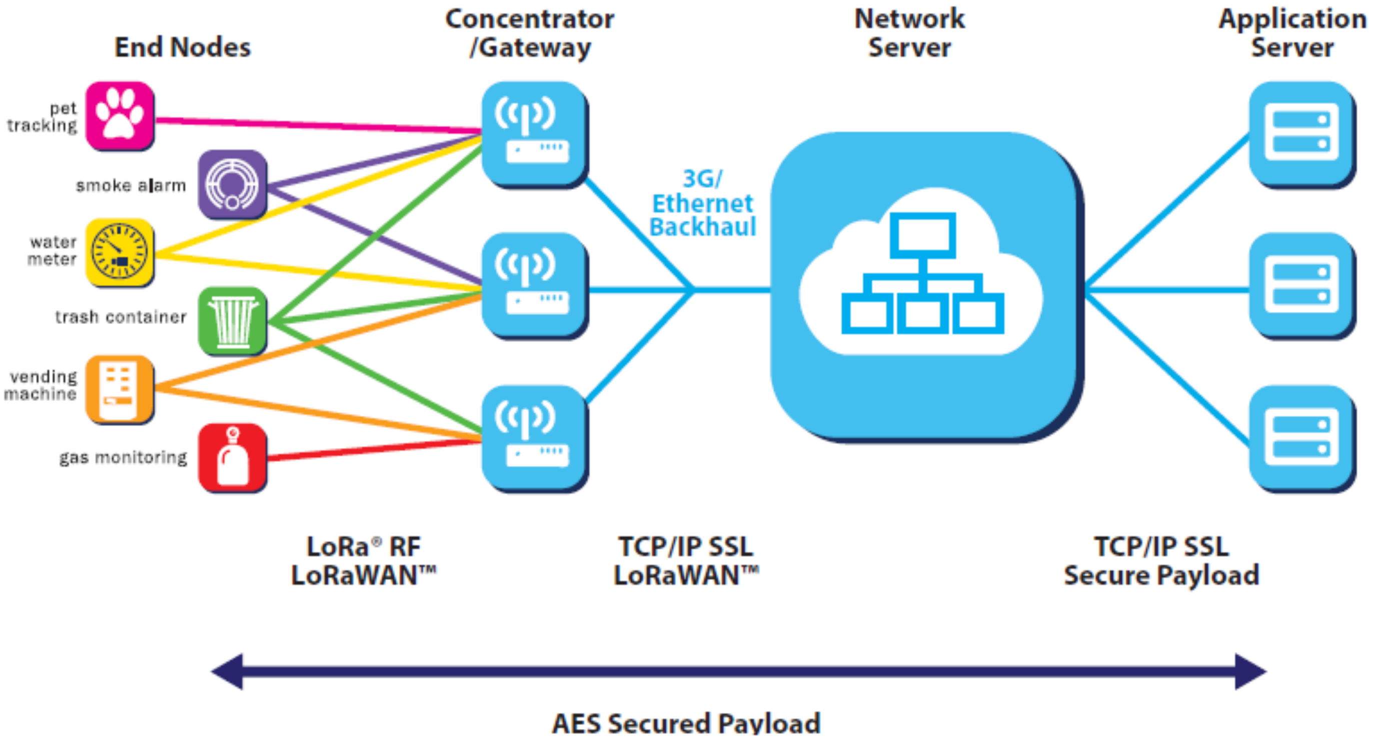
- All Communications between the phone and the bridge are in plain text.

Philips Hue Attack



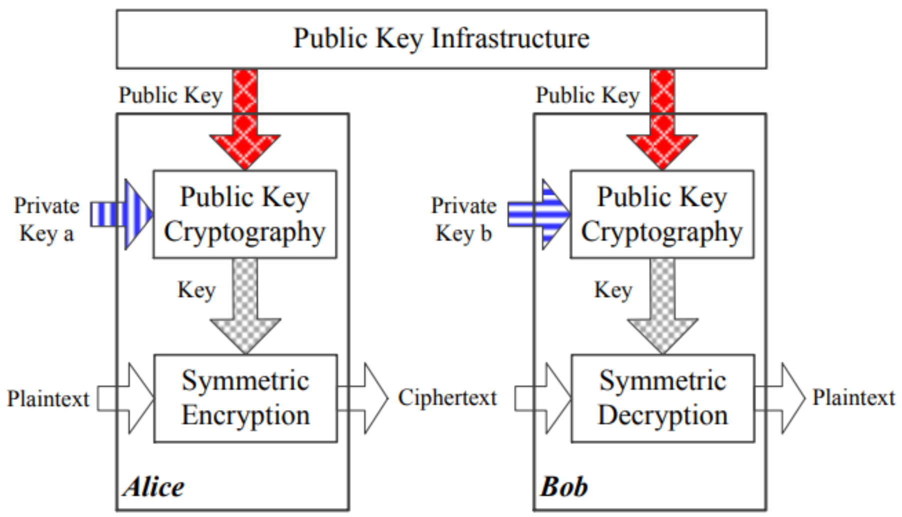
Philips Hue Attack (Demo Andrew Bennet former project student)

LoRaWAN Network Architecture

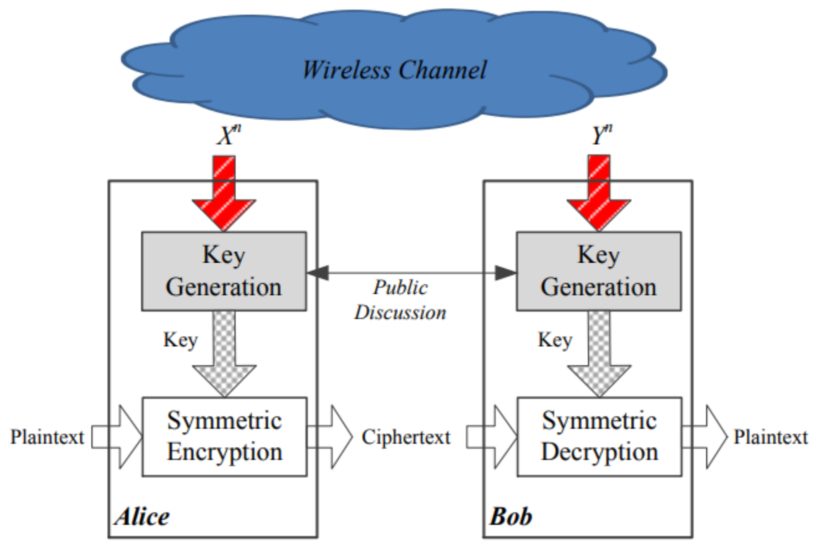


Physical layer key generation

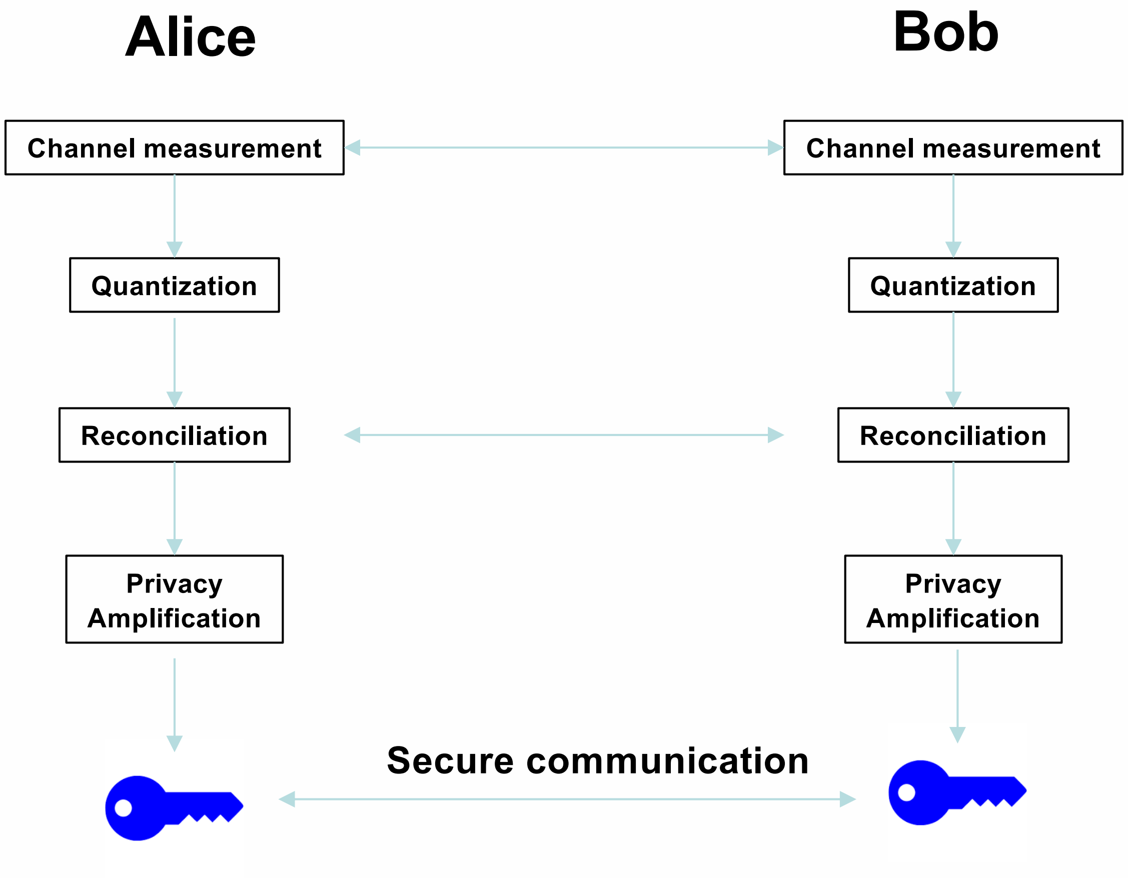
Classical encryption system



Key generation system based on wireless channel



System Design



Evaluation

Experimental device: mdot LoRa module

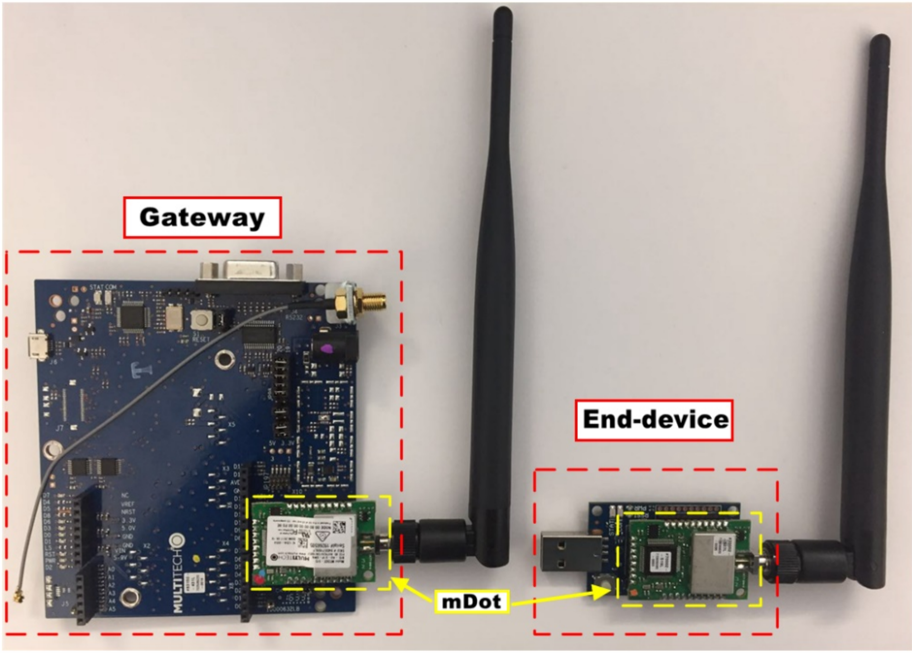


Table I: Parameters setting.

Frequency	Bandwidth	Spread Factor	Code Rate	Transmission Power
AU915MHz	500KHz	7	4/5	20dBm

Evaluation

Experimental setup:

- Indoor static scenario
- Indoor mobile scenario
- Outdoor static scenario
- Outdoor mobile scenario

Metrics:

- Key generation rate (bits/sec)
- Key match rate (%)

RSSI Correlation

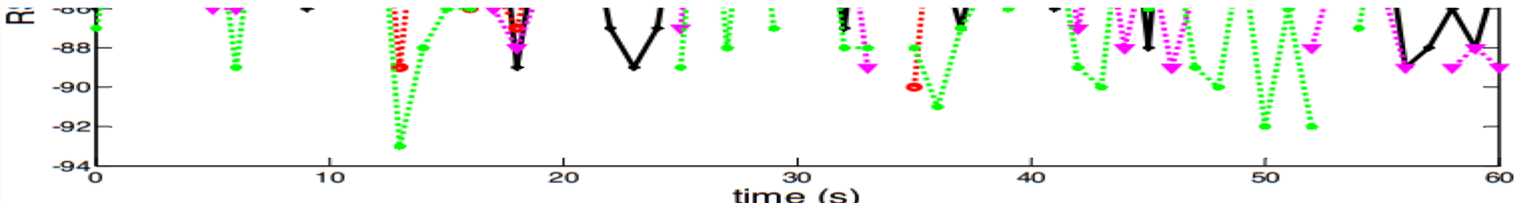
- Variation in RSSI vs. time

Alice and Bob

Bob and Eves

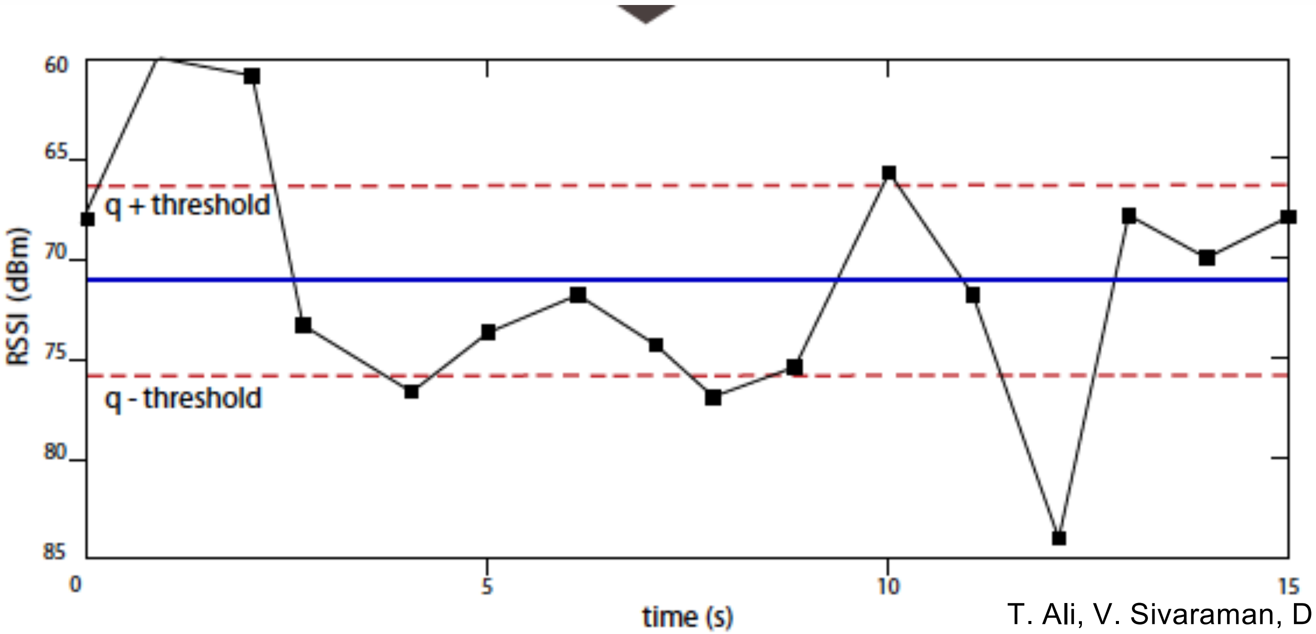
Table 1: Correlation coefficient (r) of RSSI measurements observed by various parties

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



Memory Overhead

Store RSSI for every transactions – Memory overhead?
Solution: Quantization



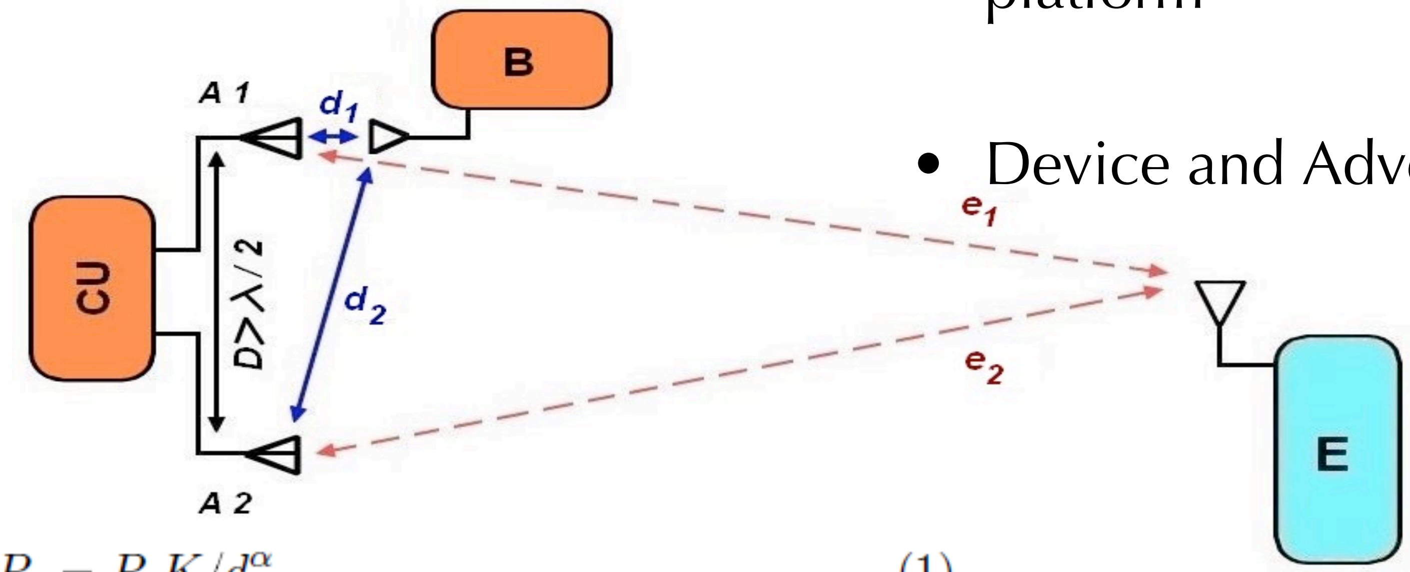
T. Ali, V. Sivaraman, D. Ostry and S. **Jha**, “Securing Data Provenance in Body Area Networks using Lightweight Wireless Link Fingerprints”, International Workshop on Trustworthy Embedded Devices (TrustED 2013) held in conjunction with ACM CCS’13, November 4, Berlin, 2013

Figure 5: Level crossing quantization technique

SeAK: Secure Pairing

Platforms

- Control Unit (CU) - Opal sensor platform
- Device and Adversary – Iris motes

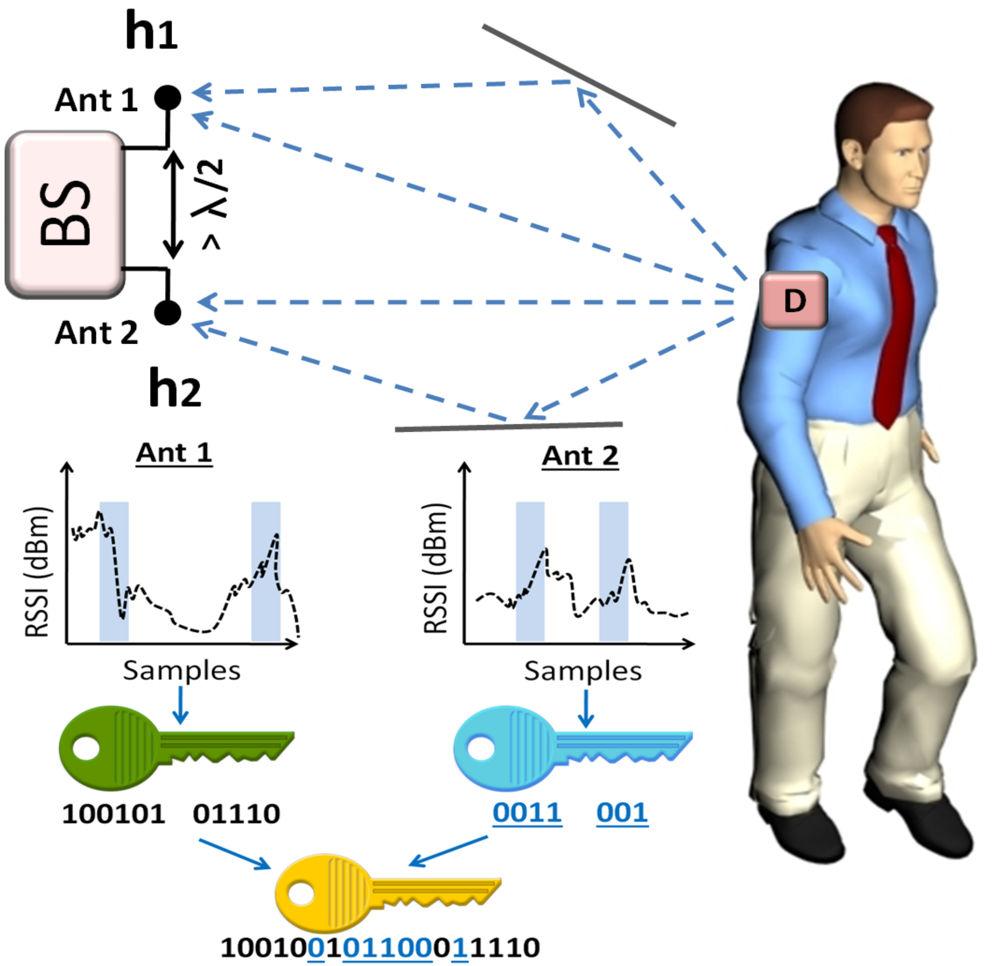


$$P_r = P_s K / d_r^{\alpha} \quad (1)$$

$$\frac{P_{r1}}{P_{r2}} = \frac{P_s K / d_1^{\alpha}}{P_s K / d_2^{\alpha}} \quad (2)$$

Chitra Javali et al, "SeAK: Secure Authentication and Key generation Protocol based on Dual Antennas for Wireless Body Area Networks" by, RFIDSec 2014, Co-hosted with WiSec 2014, Oxford, UK.

DLINK: Dual Link based Radio



Girish Revadigar, Chitra Javali, Wen Hu and Sanjay Jha, "DLINK: Dual Link Based Radio Frequency Fingerprinting for Wearable Devices". 40th IEEE Conference on Local Computer Networks (LCN), Florida, USA, October 2015.