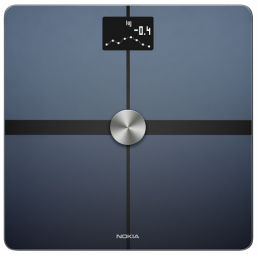


# Week1: COMP4337/9337
# **Challenges in Securing Internet of Things (IoT)**


Prof. Sanjay Jha

Director, Cyber Security and Privacy Laboratory

http://www.cse.unsw.edu.au/~cyspri

The University of New South Wales (UNSW)

# Acknowledgement

My security research is a result of collaboration with a number of my PhD students, postdocs and and colleagues

- PhD Students/Postdocs: Chitra Javali, Girish Revadigar, Jun Young Kim, Arash, Shaghahi, Mossarat Jahan, Zainab Abaid, Dr Taha Ali, Dr Mohsen Rezvani, Dr  Hailun Tan, Dr Weitao Xu,  Other colleagues from CSIRO/Data61, Undergrad Andrew Bennett (Philip Hue)
- Colleagues: A/Prof Salil Kanhere, Dr Wen Hu, A/Prof Aleks Ignatovic, Prof Aruna Seneviratne, (UNSW) A/Prof Kasper Rasmussen (Oxford), Gene Tsudik (UCI), Diet Ostry,  Dali Kafaar, and Dr Hassan Asgar (Data61)

# History of Wireless Sensor Net

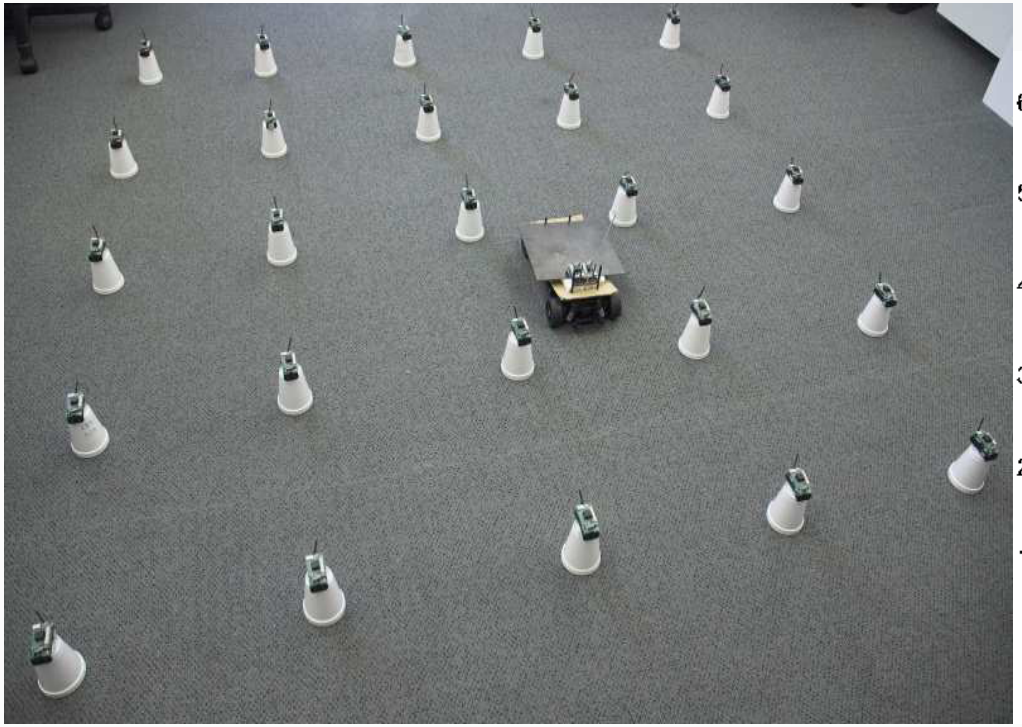
- 1999: Kahn, Katz,Pister: Vision for **Smart Dust**
- 2002 Sensys CFP: Wireless Sensor Network research as being composed of "*distributed systems of numerous smart sensors and actuators connecting computational capabilities to the physical world have the potential to revolutionise a wide array of application areas by providing an unprecedented density and fidelity of instrumentation*".

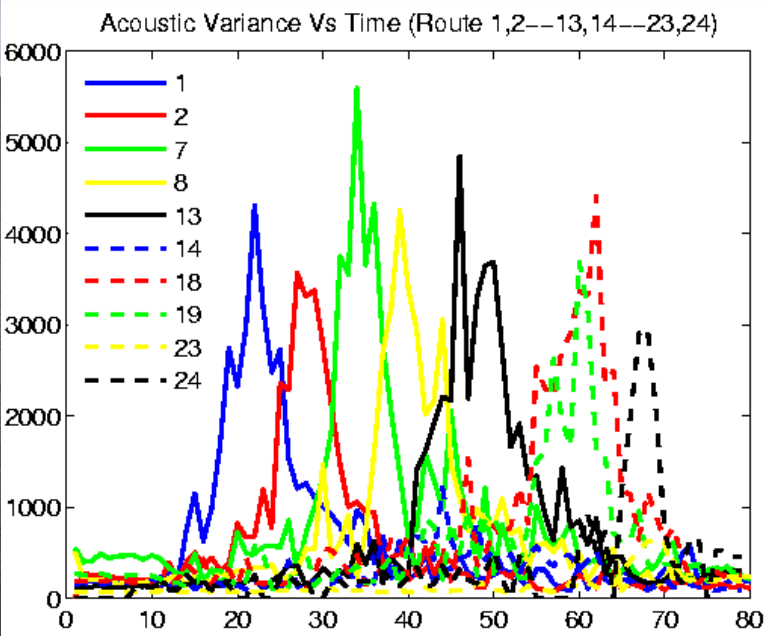
# Environmental Monitoring



"*The Design and Evaluation of a Hybrid Sensor Network for Cane-toad Monitoring*". Wen Hu, Van Nghia Tran, Nirupama Bulusu, Chun-tung Chou, Sanjay Jha, Andrew Taylor. In Proceedings of Information Processing in Sensor Networks (IPSN 2005/SPOTS 2005), Los Angeles, CA, April 2005

# Detection and Tracking

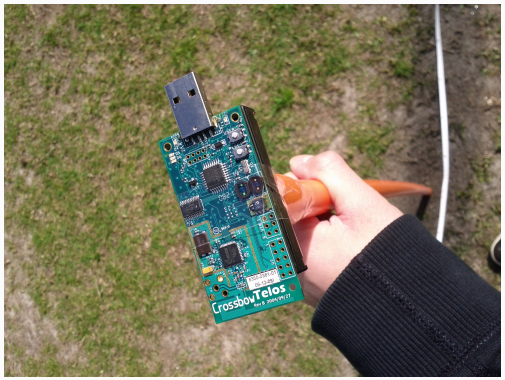





N. Ahmed, M. Rutten, T. Bessell, S. Kanhere, N. Gordon, and S. Jha,
"Detection and Tracking using Particle Filter Based Wireless Sensor Networks"
IEEE Transactions on Mobile Computing (TMC), vol. 9 (9), pp. 1332 – 1345, Sept 2010,

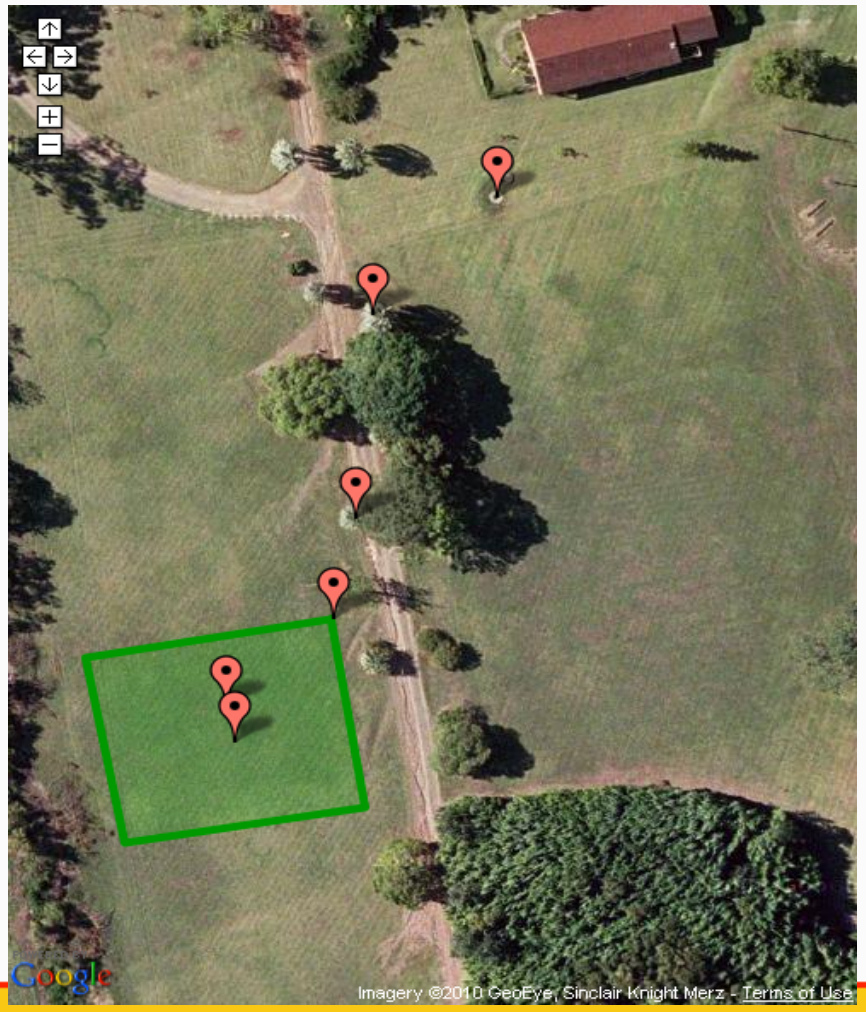
# Quadracopter Prototype

- Various payload capacity (up to 500gm), flying time, motor, wings  (hexacopter).
- Wireless Link Characterisation




N.Ahmed,S.S.Kanhere,S.Jha, "Utilizing Link Characterization for Improving the Performance of Aerial Wireless Sensor Networks", *Journal of Selected Areas in Communications (JSAC)* Special Issue on Communication Challenges and Dynamics for Un-manned Autonomous Vehicles, Vol. 31, No. 8, pp. 1639-1649, Aug, 2013.

# Precision Agriculture: King's School Deployment

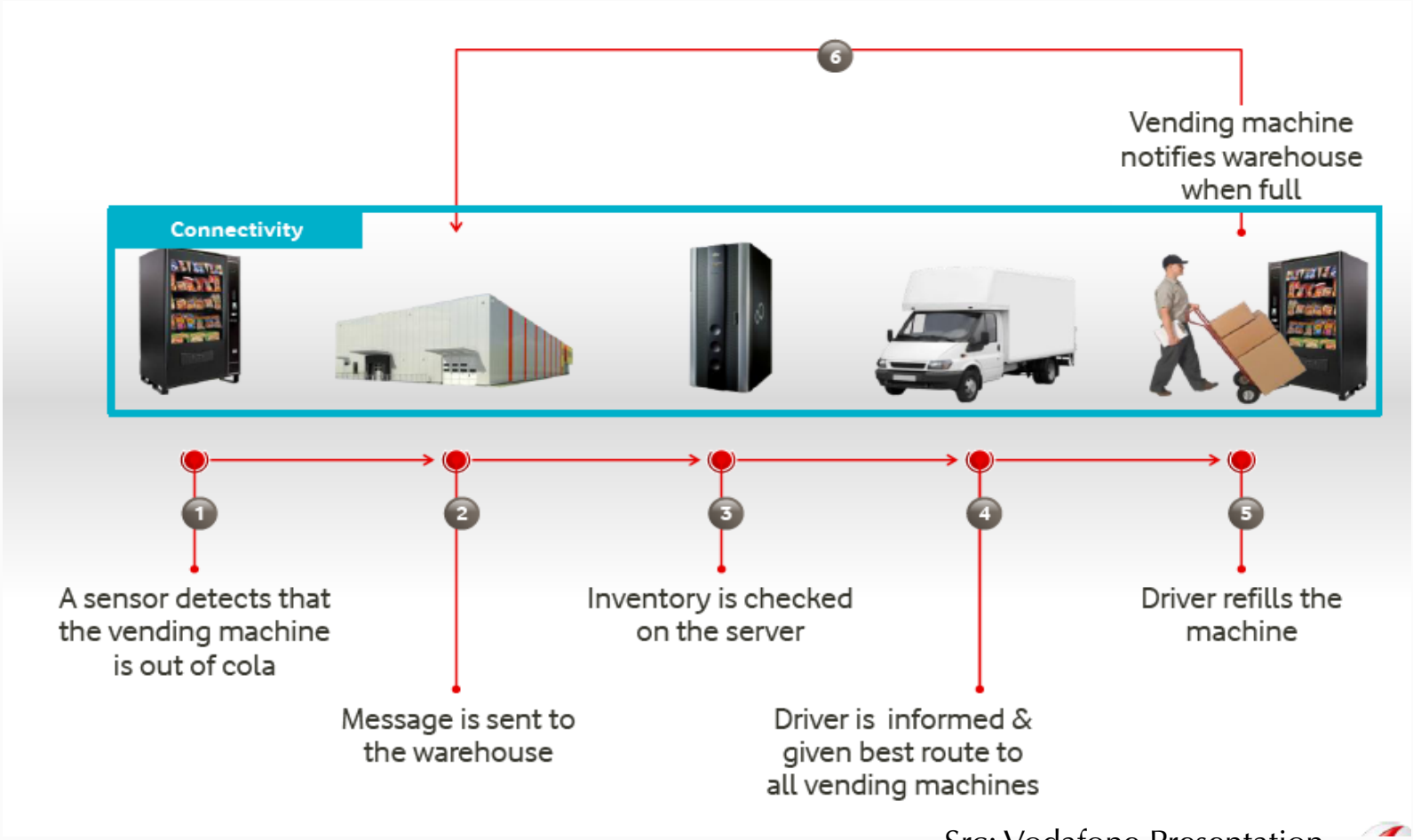



Prasant deploying Hop-2 Node

# History (IoT)

- Early 90s or prior: SCADA systems, Telemetry applications
- Late 90s- Products/services from mobile operators (Siemens) to connect devices via cellular network – Primarily automotive telematics
- Mid- 2000s – Many tailored products for logistics, fleet management, car safety, healthcare, and smart metering of electricity consumption
- Since 2010 – A large number of consortiums mushrooming up to bid for a large market share
  - ABI Projects US$198M by 2018 (?)
  - Berg Insight US$187M by 2014……

# Why Business interest in IoT?




Src: Vodafone Presentation

# Internet of Things

- Connected devices
- Smoke alarms, light bulbs, power switches, motion sensors, door locks etc.

# IoT Enablers

- All IP Network
- Location Positioning Systems (GPS)
- Plethora of devices from sophisticated Wireless Sensor Actuators, tracking and tracing devices, RFID & CLOUD storage
- Ease of programming – Embedded Java
- Software and Service Architectures
- Data Analytics – Big Data (Sensor feed)

# Research Challenges

- Heterogeneity
- Interoperability
- Scalability
- Affordable Coverage
- Software Architecture/Middleware
- Security and Trustworthiness
- Privacy
- Big Data - Data Analytics

# 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
- .....

# Interoperability

- Devices and Software Services Function speak different language
- Trivial Example
  - Milk in the fridge going off – Sensor on carton
  - Sends TXT "drink milk" – Mobile Phone
  - Smart Phone adds milk to shopping list.
- milk carton, fridge, phone, app – all must communicate with each other seamless

# Why IoT Security is Challenging?

- Diversity of devices, capabilities, standards, programming environment
- Lots of these devices store personal data – e.g. fitness/health, home security..
- Application driven field – innovation comes  from non-tech people
  - First to market may mean no/little security
- Potential threats/attacks a guess work.

# A Security Disaster

The Economist | World politics | Business & finance | Economics | Science & technology | Culture

Cyber-security

The internet of things (to be hacked)

Hooking up gadgets to the web promises huge benefits. But security must not be an afterthought

Jul 12th 2014 | From the print edition

Like 217 Tweet 594

**How the Internet of Things Could Kill You**

By Fahmida Y. Rashid JULY 18, 2014 7:30 AM - Source: Tom's Guide US | 5 COMMENTS

**Hacking the Fridge: Internet of Things Has Security Vulnerabilities**

JESS SCANLON | MORE ARTICLES
JUNE 28, 2014

**Philips Hue LED smart lights hacked, home blacked out by security researcher**

By Sal Cangeloso on August 15, 2013 at 11:45 am | 7 Comments

- HP conducted a security analysis of IoT devices[1]
  - 80% had privacy concerns
  - 80% had poor passwords
  - 70% lacked encryption
  - 60% had vulnerabilities in UI
  - 60% had insecure updates

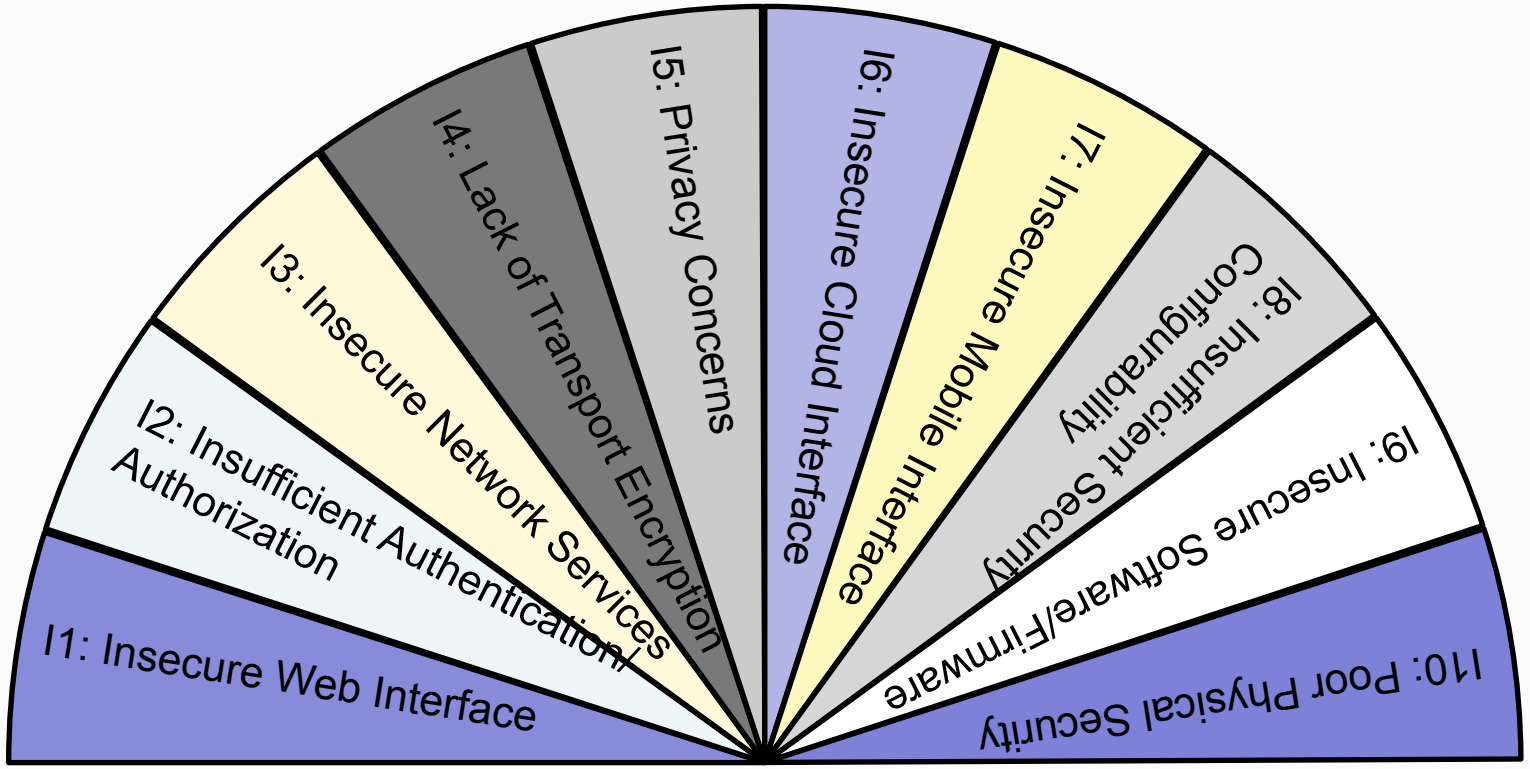
[1] http://fortifyprotect.com/HP_IoT_Research_Study.pdf





Src: Phil Levis's workshop talk at Stanford

# OWASP: IoT Vulnerability Classes



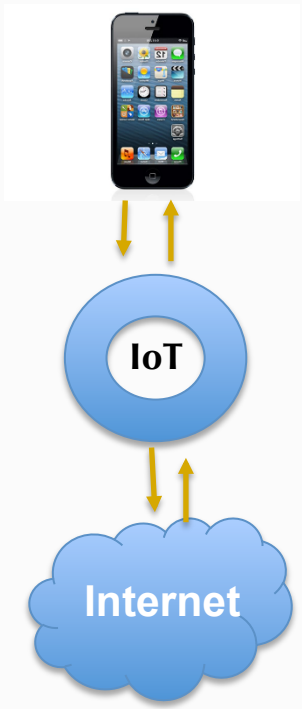

Src: Junia Valente et al, “Security & Privacy in Smart Toys”, IoT S&P@CCS 2017: 19-24

# 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)

# E-Health Applications

Control Unit

Wrist band


Programmer

Deep brain stimulator


Glucose sensor + Insulin pump

Embedded pressure sensor

# Attacks

- Wireless medium vulnerable to threats
  - An intruder can gain access to WBAN
  - Tamper the physiological data
  - Inject false commands

- According to recently published FDA report :

  "An RFID-deep brain stimulator had caused a 'severe rebound tremor' in a patient due to accidental reprogramming via interference from coexisting RFIDs"

# Authentication/Data Origin

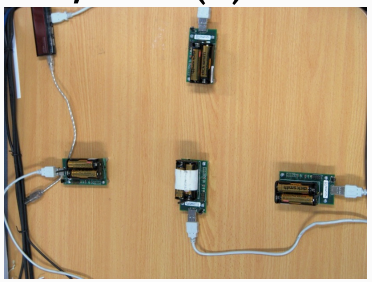
- Link Fingerprint – RSSI or phase unique between sensor device and a base-station
  - Hard to forge, provable session record
- Use standard security primitives (PKI) to secure this signature and data – as needed by applications.
- Optimize the fingerprinting process to reduce memory and transmission overheads

# RSSI Demo: Girish Revadigar (former PhD student)

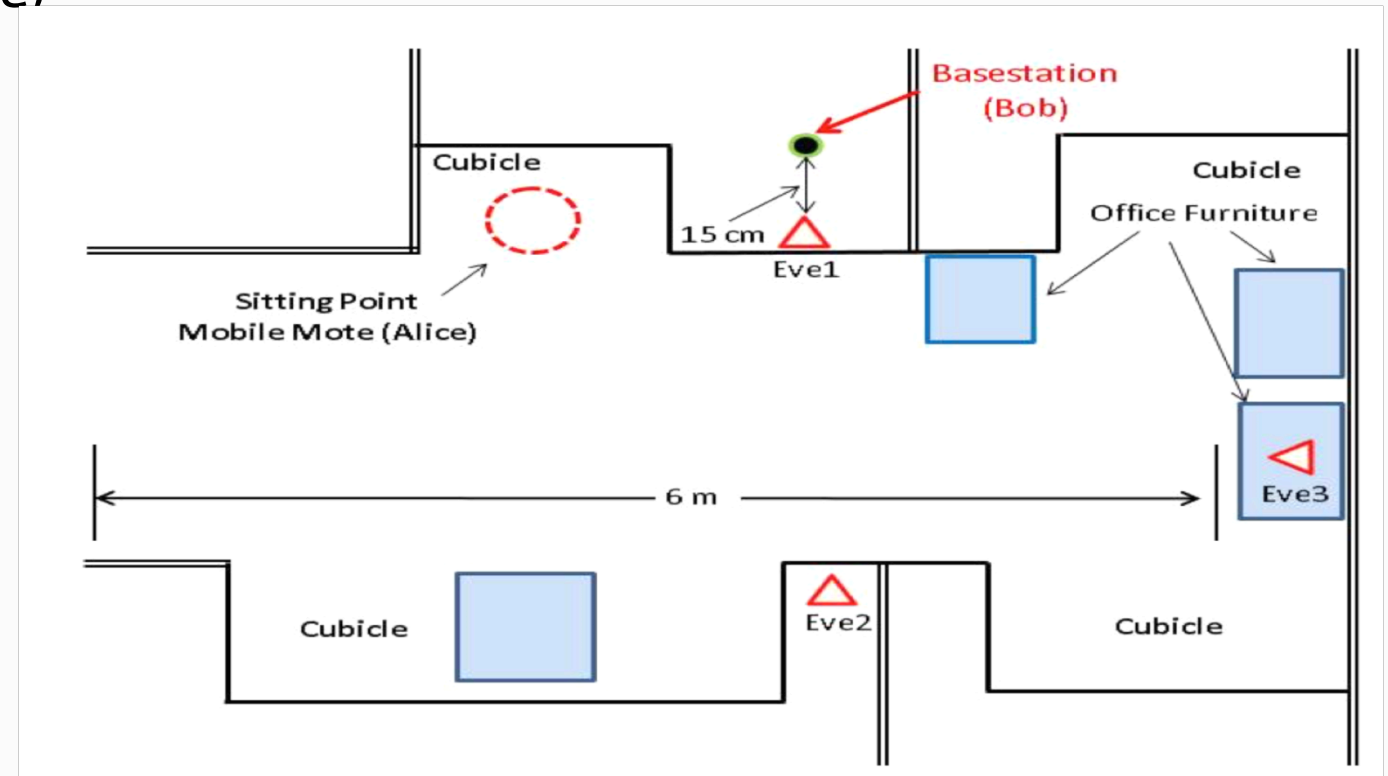
# Experimental Setup

- Bodyworn Device
  - Alice (MicaZ mote)

- Basestation – Bob, Eve(s)



- Indoor Office Environment



# RSSI Correlation

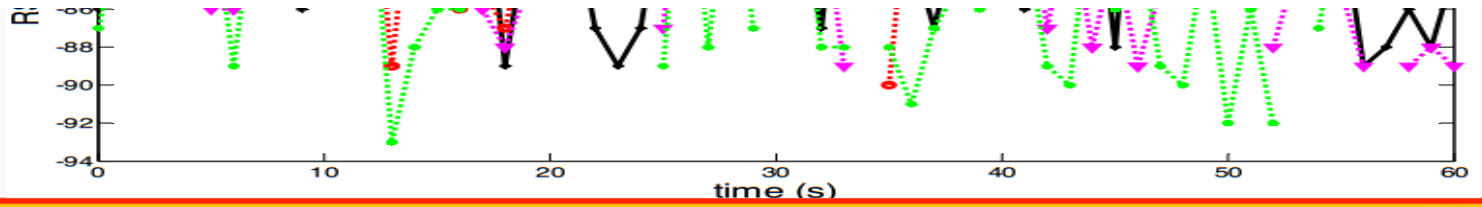
- Variation in RSSI vs. time

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

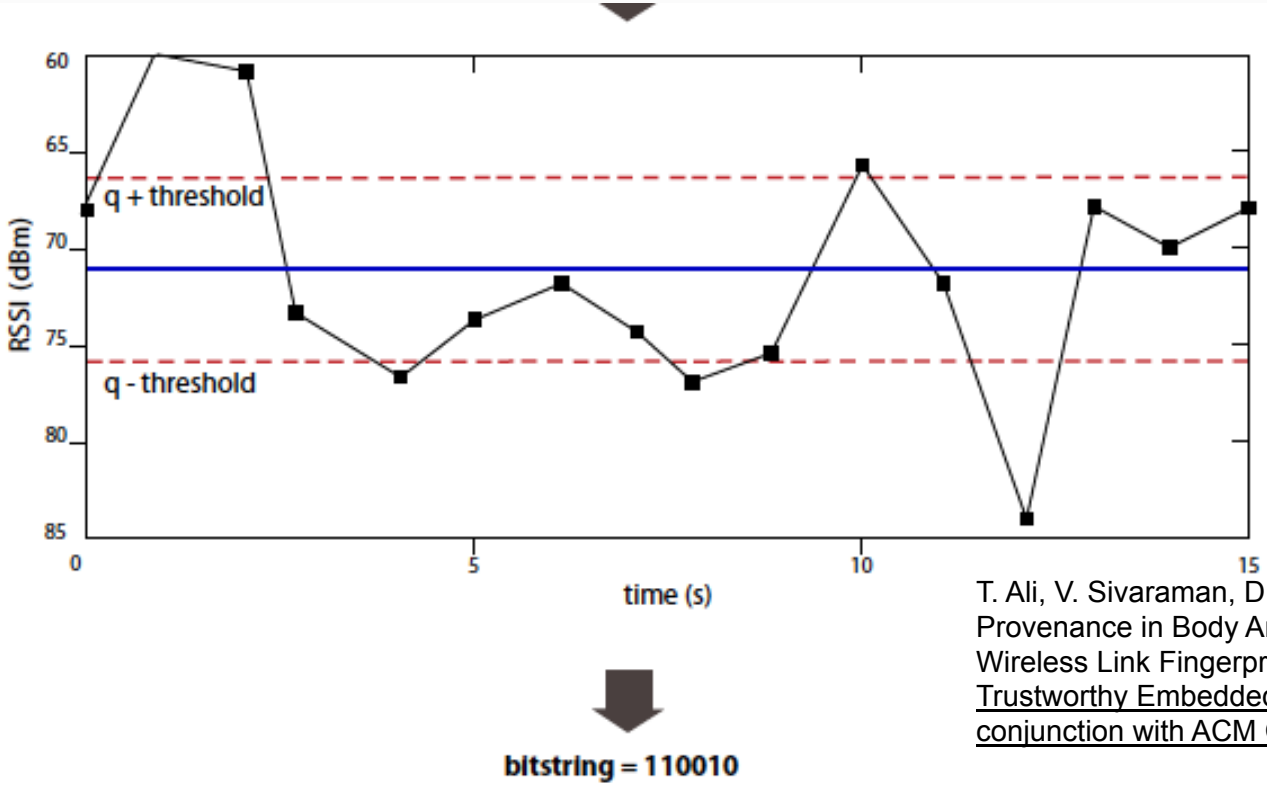
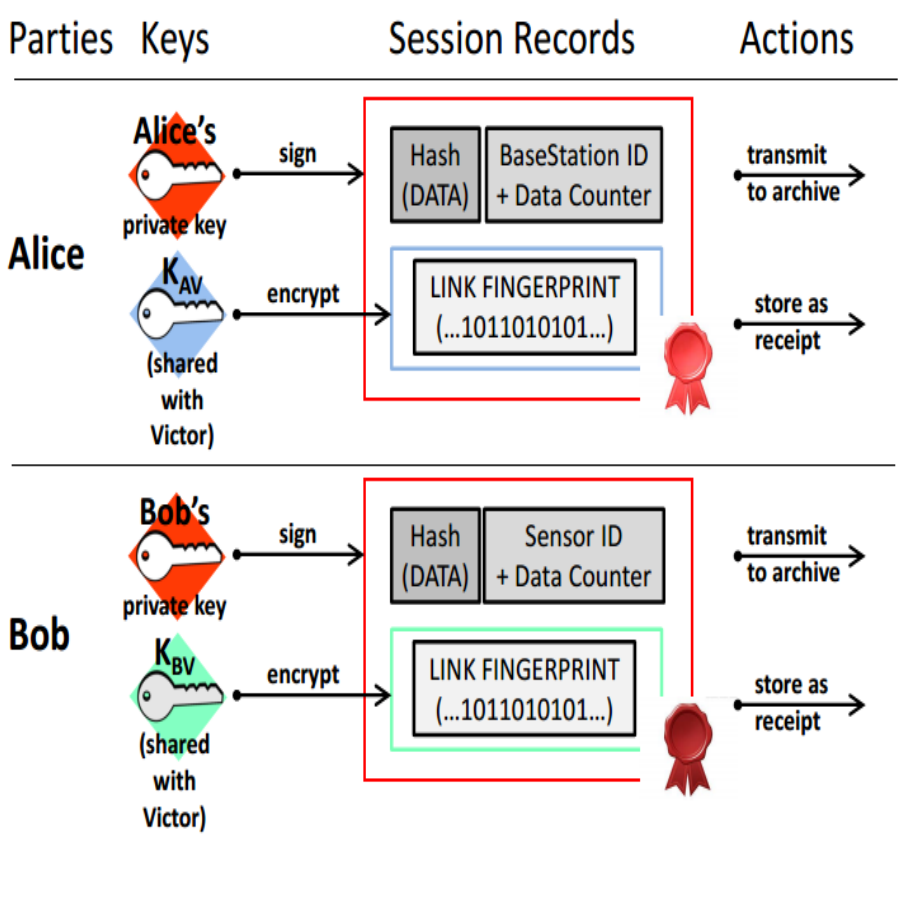


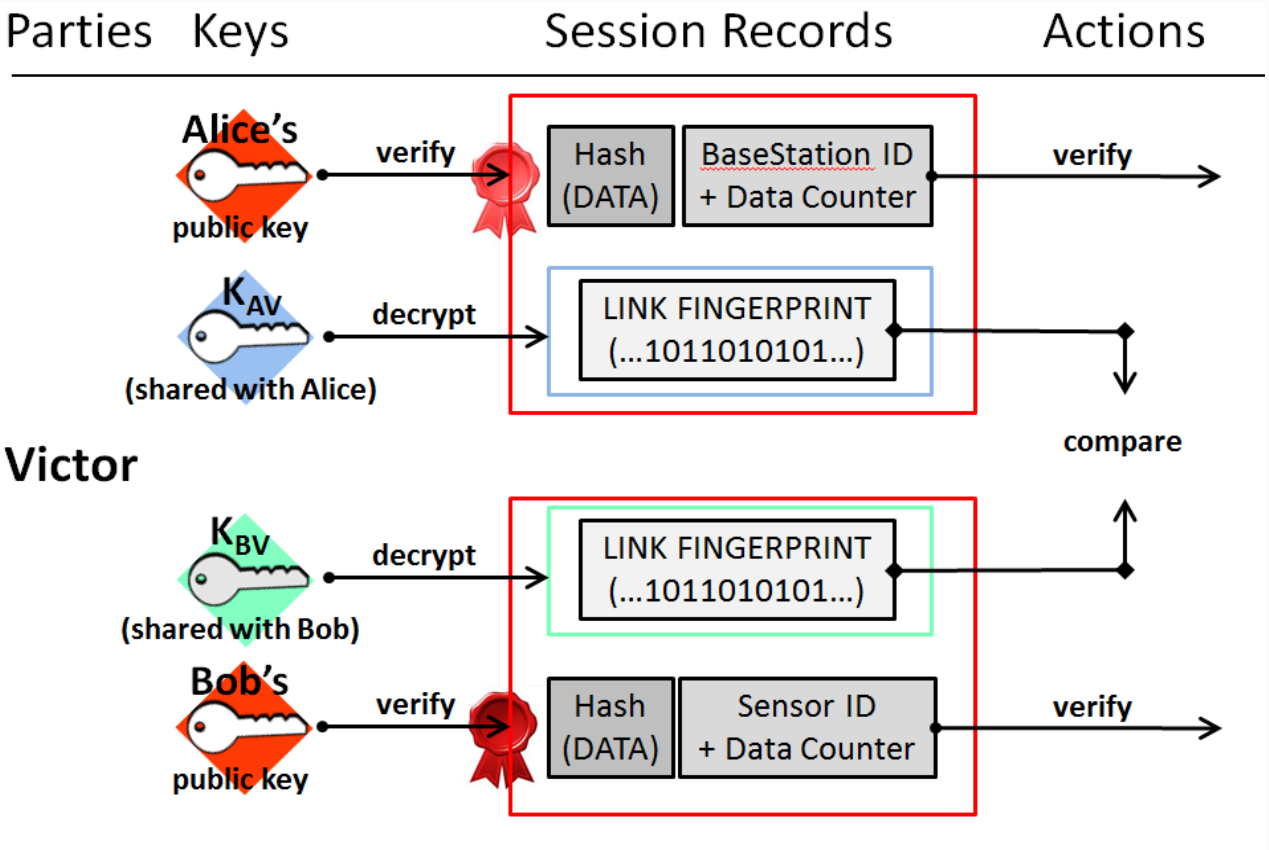

Figure 5: Level crossing quantization technique

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

# Authentication Protocol



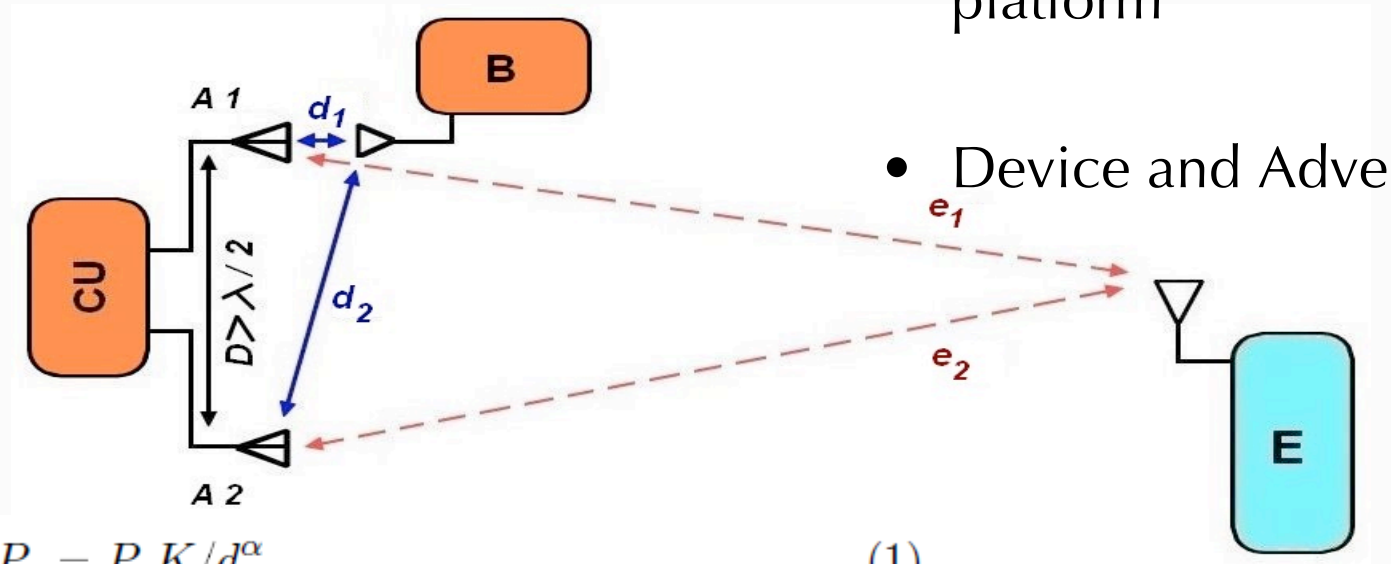
# Verification Protocol



# SeAK: Secure Pairing

**Platforms**

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

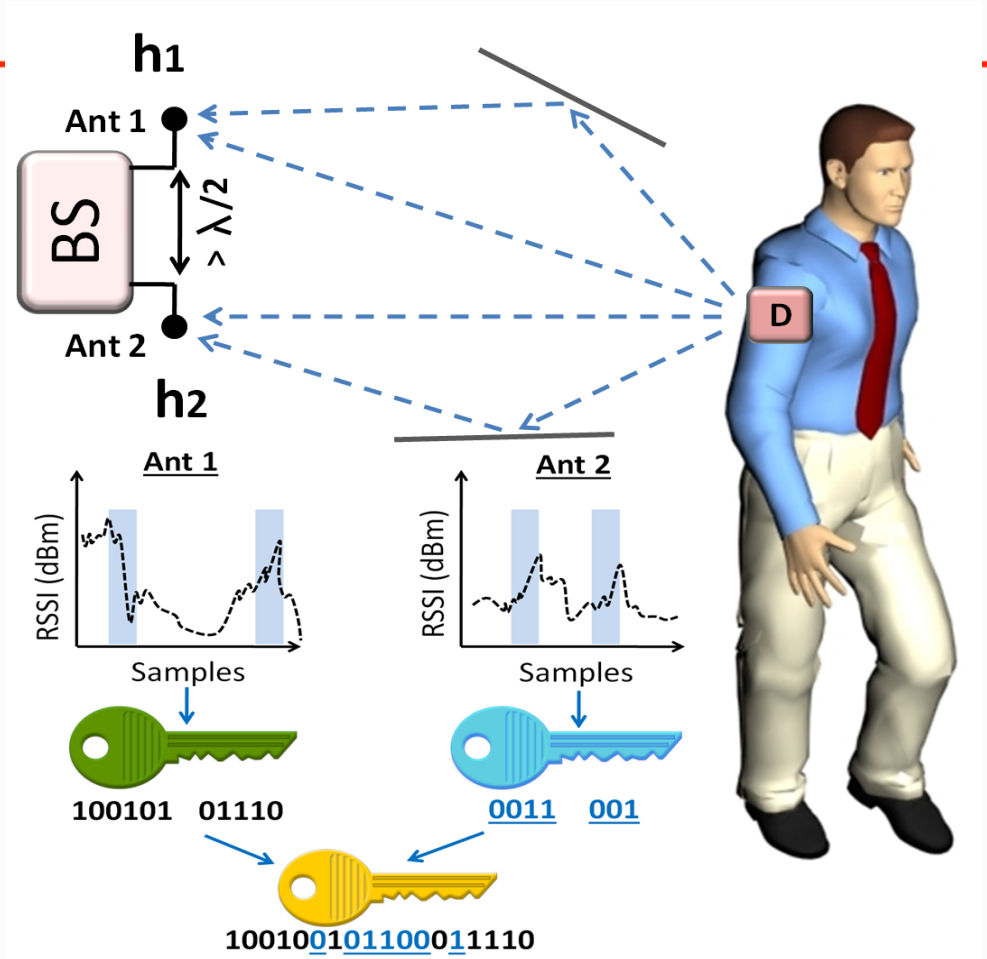



$$P_r = P_s K / d_r^{\alpha} \quad (1)$$

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

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.

# Thread Group (ARM, Consortium of Qualcomm, and Samsung …)

- Adopts PKC for authentication
- AES Symmetric key for confidentiality
- IPv6 Low-power Wireless Personal Area Networks (6LoWPAN) to minimize the energy consumption from wireless communications
- How to build secure-over-air reprogramming for IoT Devices (heterogeneous)?

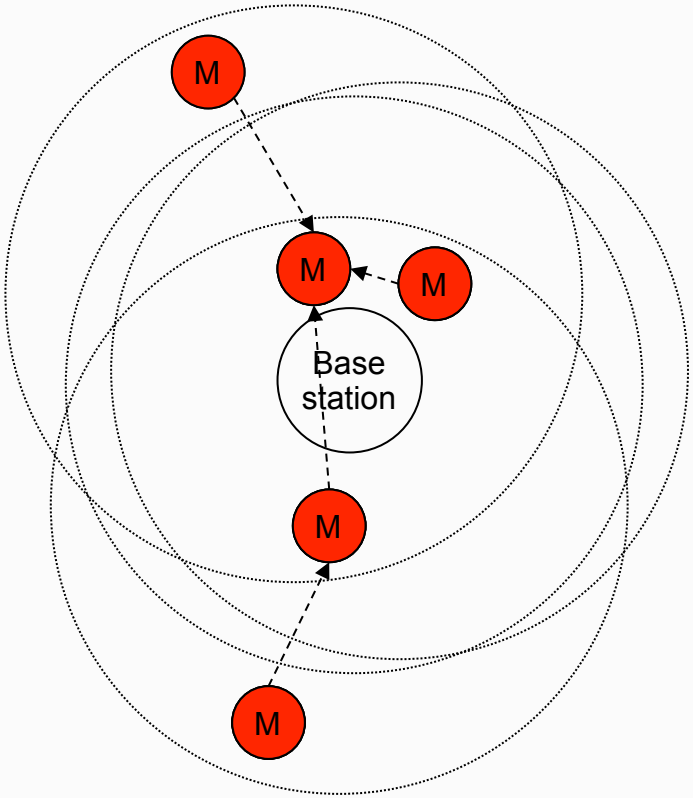
# Broadcast Security – for IoT

- Broadcast applications need security
  - Packet injection or eavesdropping is easy
- Security solutions for point-to-point communication not scalable for large deployments
- Broadcast challenges
  - Scale to large audiences
  - Dynamic membership
  - Low overhead (computation & communication)
  - Packet loss
    - How to achieve reliability in broadcasts?

# WSN Code Dissemination

- Assumes Homogenous Sensor Network
- Epidemic Communication Model
- Exploits spatial multiplexing
  - Parallel transmission in various parts of the network
- Node with the newer version program image becomes a sender and a node with an older version becomes the receiver
- Employ techniques: digital signature, Merkle hash tree, one-way hash functions , pairwise encryption.

# WSN Secure Network Programming



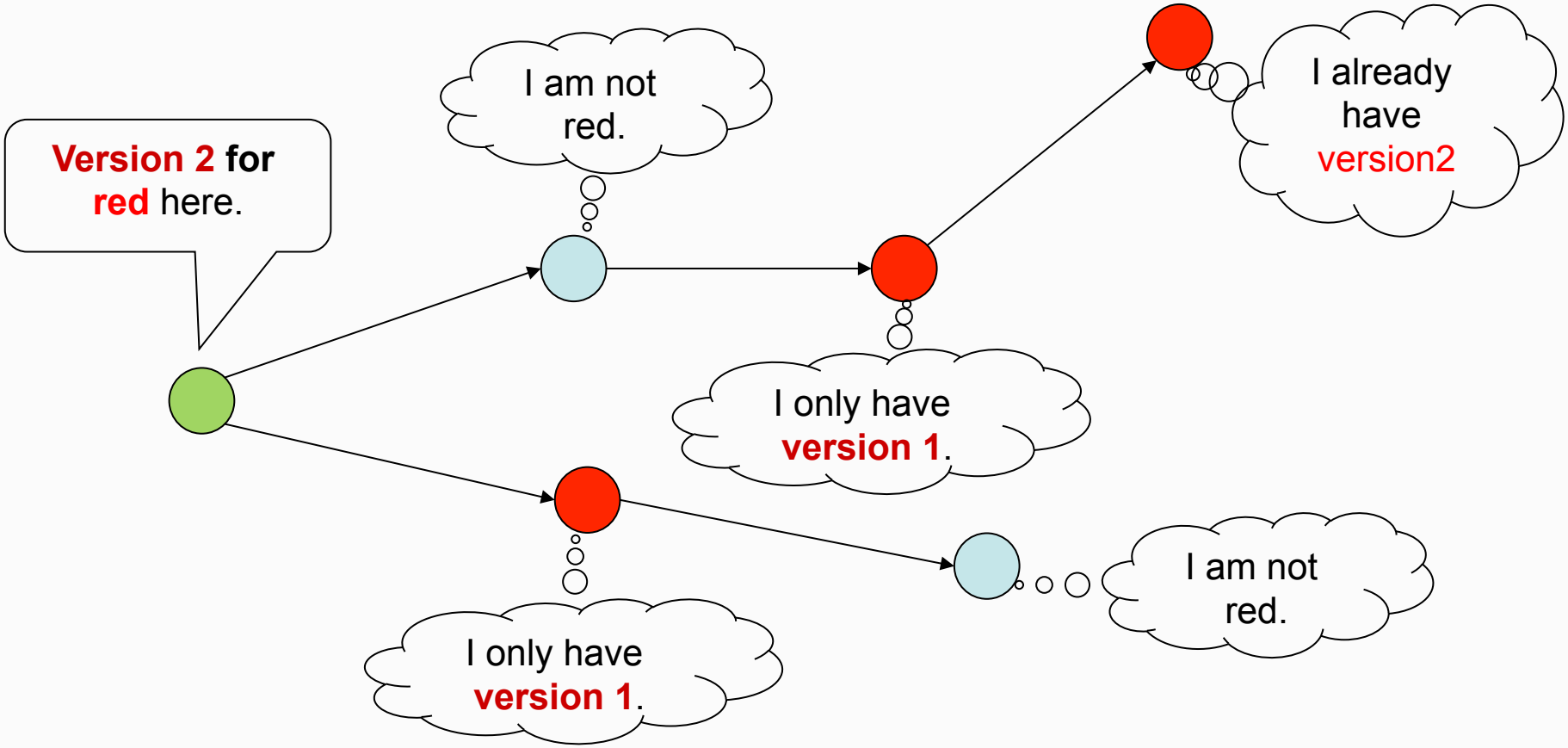

H. Tan, D. Ostry, J. Zic and S. Jha, "Secure Multi-hop Network Programming With Multiple One-way Key Chains", IEEE Transactions on Mobile Computing (TMC), Vol 10(1), pp 16-31, Jan 2011

# SEDA: SEcure Over the air code Dissemination Arhitecture

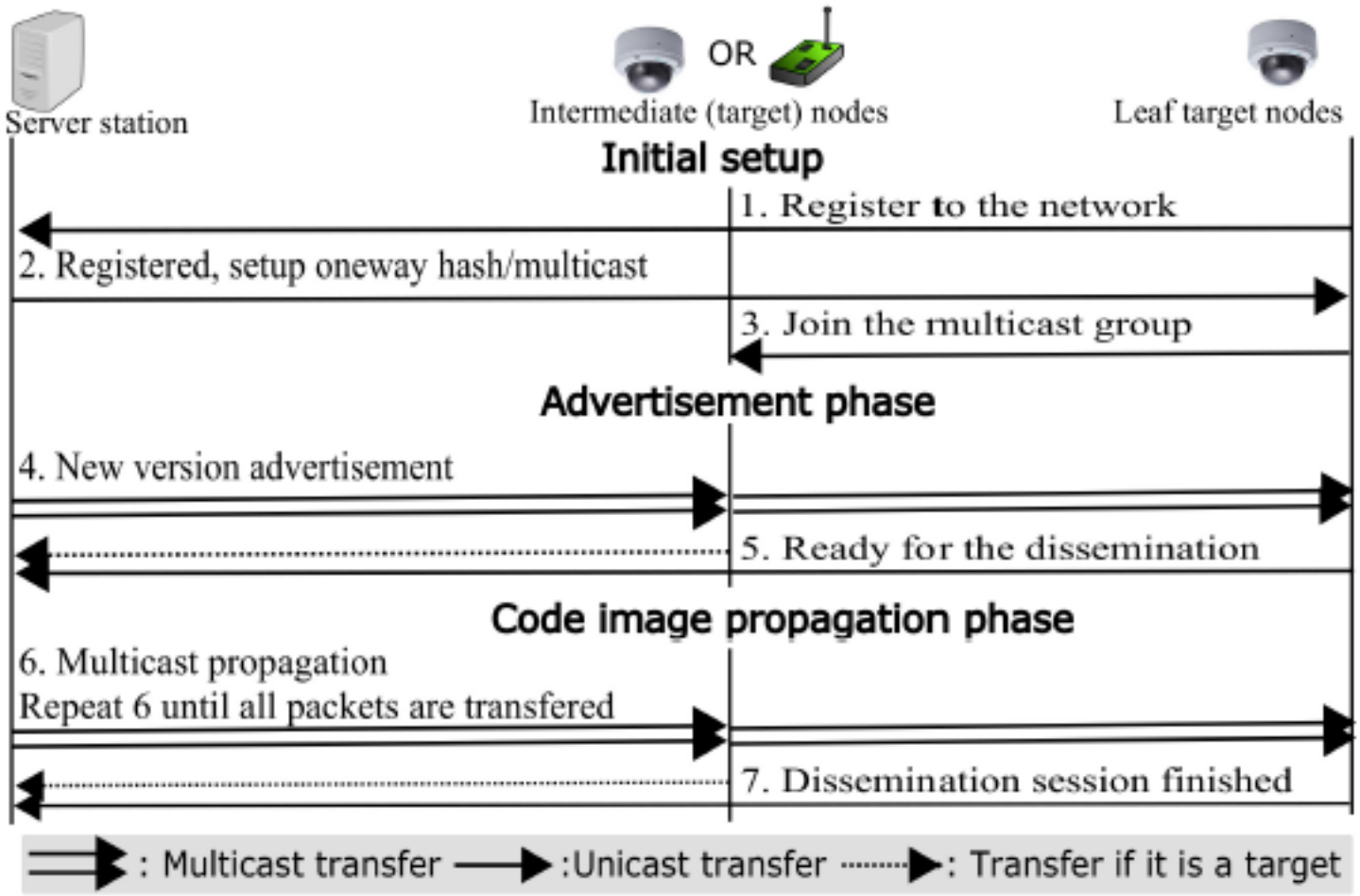
- Motivation: To produce experimental system which serves as a guideline for future deployment
- Use overlay multicast communication model for efficient dissemination and key distribution
- Public key cryptographic broadcast encryption scheme (BGWt) - for efficient group key distribution/management, and low decryption overhead.
- Identify potential security threats and defensive measures
- Experimentally validate the architecture and provide performance benchmark

# Broadcast propagation

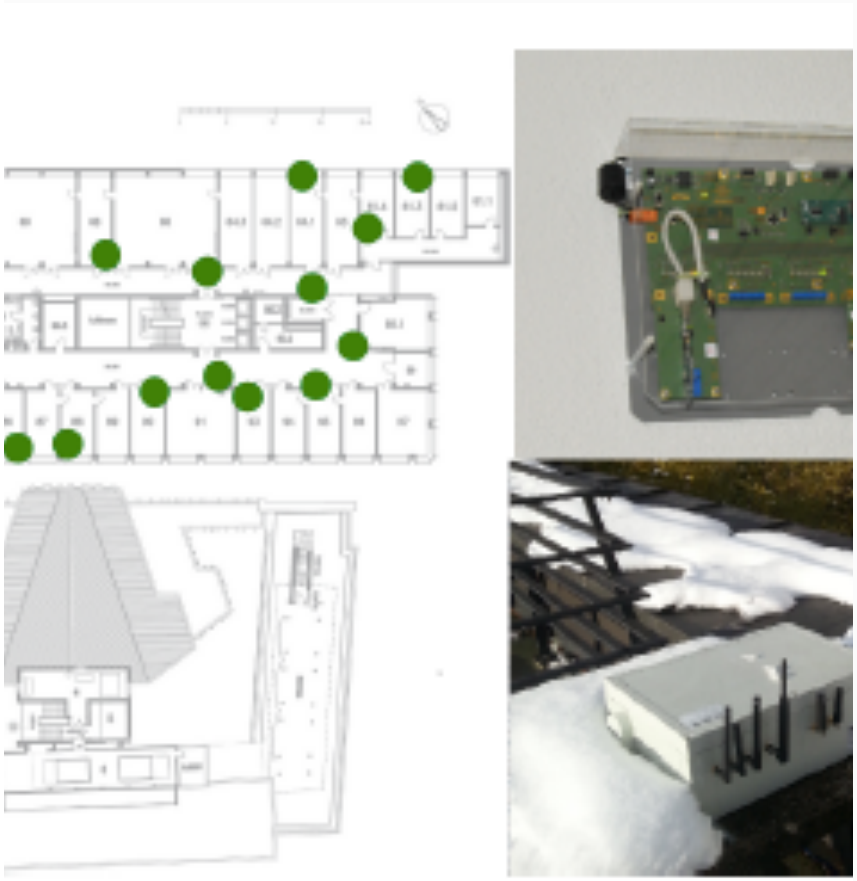
Server periodically broadcasts new version

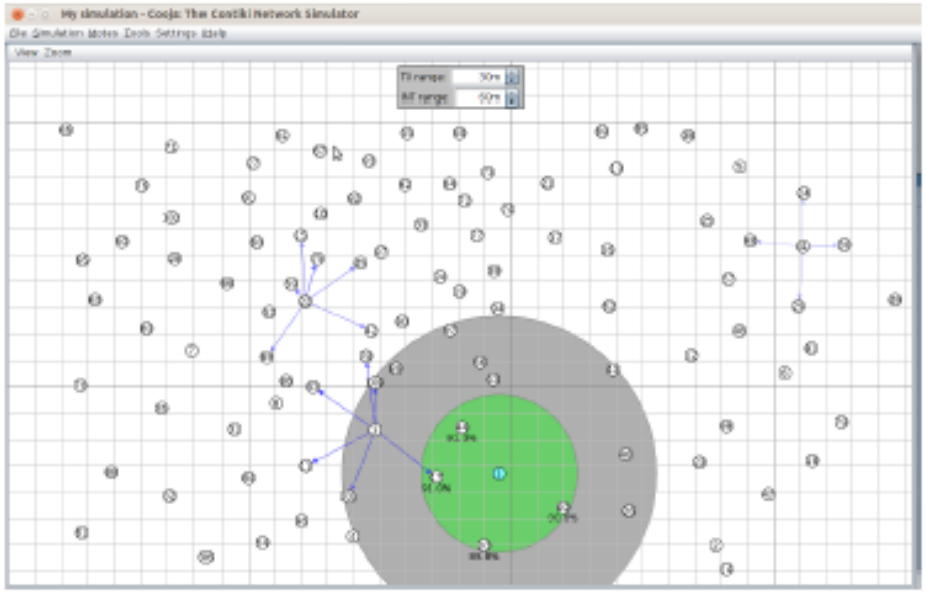


# SEDA Protocol Overview



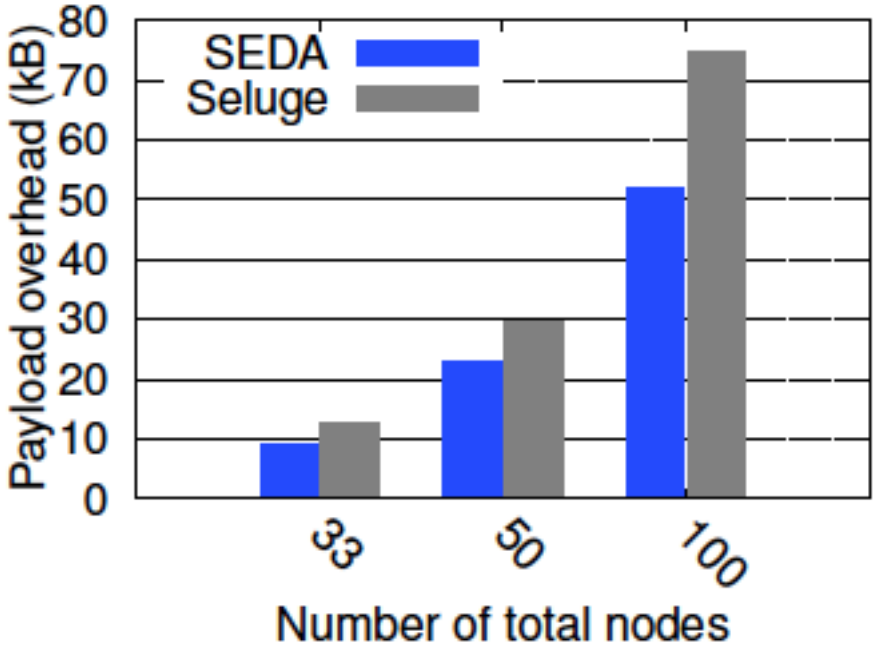
# Flock Testbed and Cooja simulator



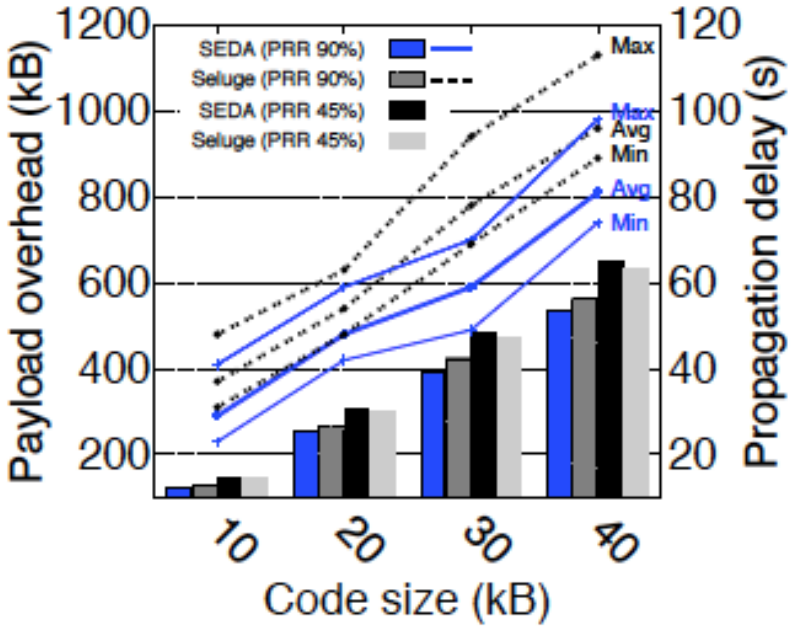


(c) Cooja simulator setting for a 100 node network.

# Results




(a) Key establishment overhead comparis




(b) Propagation overhead (bar, left axis) and delay (line, right axis) comparison.

# Research Contributions

- The selection and implementation of a public key cryptographic broadcast encryption scheme e.g. variation of BGW
- Experimentally validate through a prototype IoT platform and demonstrate the efficiency in practical settings
- Publicly release implementation as an open-source code

# Thank You

# Selected Publications


- Jun Young Kim, Ralph Holz, Wen Hu, and Sanjay **Jha**. Automated Analysis of Secure Internet of Things Protocols. *In Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC 2017)*. ACM, New York, NY, USA, 238-249.
- Quantifying the impact of adversarial evasion attacks on machine learning based android malware classifiers
  Z Abaid, MA Kaafar, S **Jha**, *IEEE 16th International Symposium on Network Computing and Applications* (NCA), 2017
- J. Y. Kim; W. Hu; H. Shafagh; S**. Jha**, "SEDA: Secure Over-The-Air Code Dissemination Protocol for the Internet of Things," *IEEE Transactions on Dependable and Secure Computing* , vol.PP, no.99, pp.1-1, 15 Dec 2016
- Z Abaid, MA Kaafar, S ,**Jha**, Early Detection of In-the-Wild Botnet Attacks by Exploiting Network Communication Uniformity: An Empirical Study - Proc. IFIP Networking, 2017
- Chitra Javali, Girish Revadigar, Kasper Bonne Rasmussen, Wen Hu, and Sanjay **Jha**, "I Am Alice, I Was in Wonderland: Secure Location Proof Generation and Verification Protocol", The *41st IEEE Conference on Local Computer Networks (LCN) Dubai*, UAE, November 7-10, 2016.
- 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.
- Chitra Javali, Girish Revadigar, Lavy Libman and Sanjay **Jha**, "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.

# Selected Publications


- M. Rezvani, V. Sekulic, A. Ignjatovic, E. Bertino and S. **Jha**, "Interdependent Security Risk Analysis of Hosts and Flows", Accepted in IEEE Transactions on Information Forensics and Security, 2015.
- M. Rezvani, A. Ignjatovic, E. Bertino and S. Jha, "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks", IEEE Transactions on Dependable and Secure Computing, 12(1): 98-110, January 2015.
- M. Rezvani, A. Ignjatovic, M. Pagnucco and S. Jha, Anomaly-Free Policy Composition in Software-Defined Networks. The IFIP Networking 2016 Conference (NETWORKING 2016).
- Z. Abaid, M. Rezvani, S. Jha, MalwareMonitor: An SDN-based Framework for Securing Large Networks., ACM CoNEXT'14, Student Workshop, December 2014.
- T. Ali, V. Sivaraman, A. Radford, and S. Jha, "Securing Networks Using Software Defined Networking: A Survey", IEEE Trans. on Reliability Special Section on Trustworthy Computing.
- T. Ali, V. Sivaraman, D. Ostry, G. Tsudik and S. Jha, Securing First-Hop Data Provenance for Bodyworn Devices using Wireless Link Fingerprints, IEEE Transactions on Information Forensics & Security
- Abaid, Z., Sarkar, D., Kaafar, M.A., & Jha, S. "The Early Bird Gets the Botnet: A Markov Chain Based Early Warning System for Botnet Attacks", The 41st IEEE Conference on Local Computer Networks (LCN) Dubai, UAE, November 7-10, 2016.
- M. *Rezvani,* A. Ignjatovic, E. Bertino and S. **Jha**, "A Robust Iterative Filtering Technique for Wireless Sensor Networks in the Presence of Malicious Attacks (Poster Paper)" in proceedings of 13th ACM Conference on Embedded Networked Sensor Systems (SenSys 2013), November 11-13 2013. (accepted 22nd August 2013)