UNSW
SYDNEY

Security Challenges in Internet of Things (IoT)

Prof. Sanjay Jha
Director, Cyber Security and Privacy Laboratory
UNSW Lead, Cybersecurity CRC
UNSW Sydney

sanjay.jha@unsw.edu.au
https://sites.google.com/view/profsanjayjha/home

Acknowledgement

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

- Current and former PhD Students/Postdocs: Chitra Javali, Girish Revadigar, Rizka Purwanto, Uzma Maroof, Jun Young Kim, Arash, Shaghahi, Mossarat Jahan, Zainab Abaid, Prasant Mishra, Dr Nadeem Ahmed, Dr Regio Michelin, Dr Wanli Xue, Dr Weitao Xu, Dr Abdelwahed Khamiss, Dr Taha Ali, Dr Mohsen Rezvani, Dr Hailun Tan, Other colleagues from CSIRO/Data61, UG Andrew Bennett (Philip Hue)*
- Colleagues: Prof Salil Kanhere, Dr Wen Hu, A/Prof Aleks Ignatovic, Dr Alan Blair, Prof Aruna Seneviratne, Prof Vijay Sivaraman, Prof Rob Malaney (UNSW) A/Prof Kasper Rasmussen (Oxford), Gene Tsudik (UCI), Prof Elisa Bertino (Purdue), Dali Kafaar, Dr Hassan Asgar (Macq), Diet Ostry, Dr Siqi Ma, Dr Surya Nepal, Dr Sushmita Ruj, Dr Arindam Pal (Data61)*

*AND many more that I have missed here

* Views expressed in this talk are my personal views not representing UNSW or other funding bodies.

UNSW SYDNEY

Wireless Sensor Net (WSN) to IoT

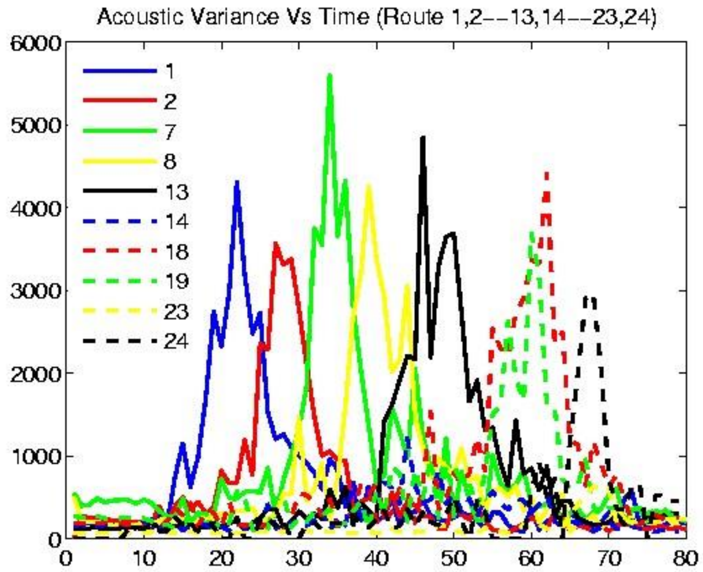
- 1999: Kahn, Katz,Pister: Vision for **Smart Dust**

- 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

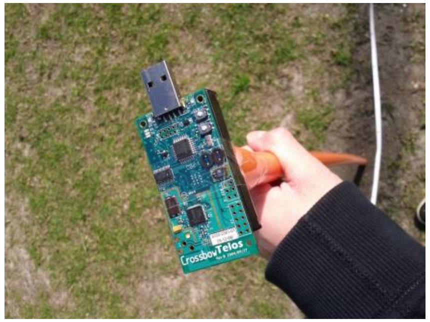


N. Ahmed, M. Rutten, T. Bessell, S. Kanhere, N. Gordon, and S. Jha, "Detection and Tracking using Particle Filter Based Wireless Sensor Networks" IEEE Transactions on Mobile Computing (TMC), vol. 9 (9), pp. 1332 – 1345, Sept 2010,

Quadracopter Prototype

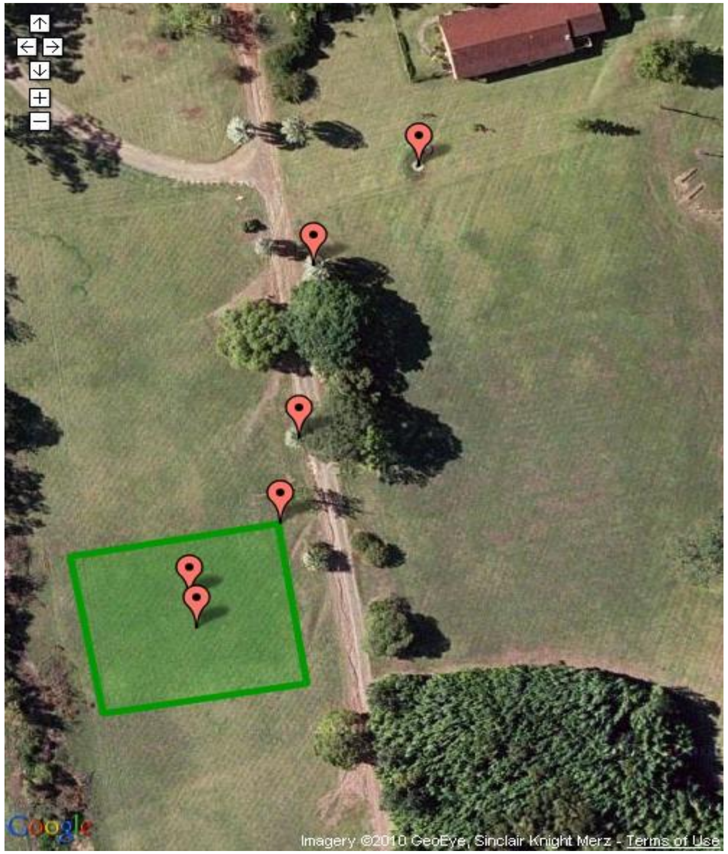
- Various payload capacity (up to 500gm), flying time, motor, wings (hexacopter).

- 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

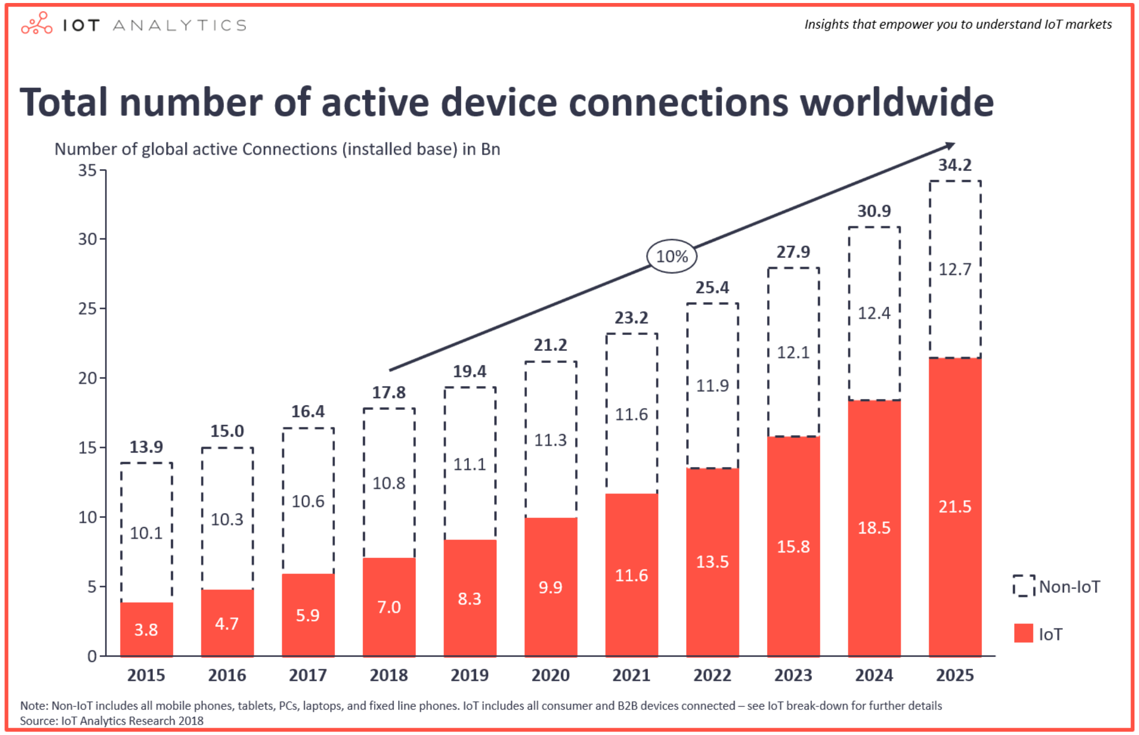
Node

Internet of Things

- Connected devices
- Smoke alarms, light bulbs, Power switches, motion sensors Door locks etc.

Internet of Things (IoT)

- Out of 17 Billion connected devices 7 Billion are IoTs



https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

IoT Research Challenges

- Heterogeneity
- Interoperability
- Scalability

- Affordable Coverage
- Software Architecture/Middleware
- **Security and Trustworthiness**
- Privacy
- Big Data - Data Analytics

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 | Timekeeper | 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 26, 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

Secure Internet of Things

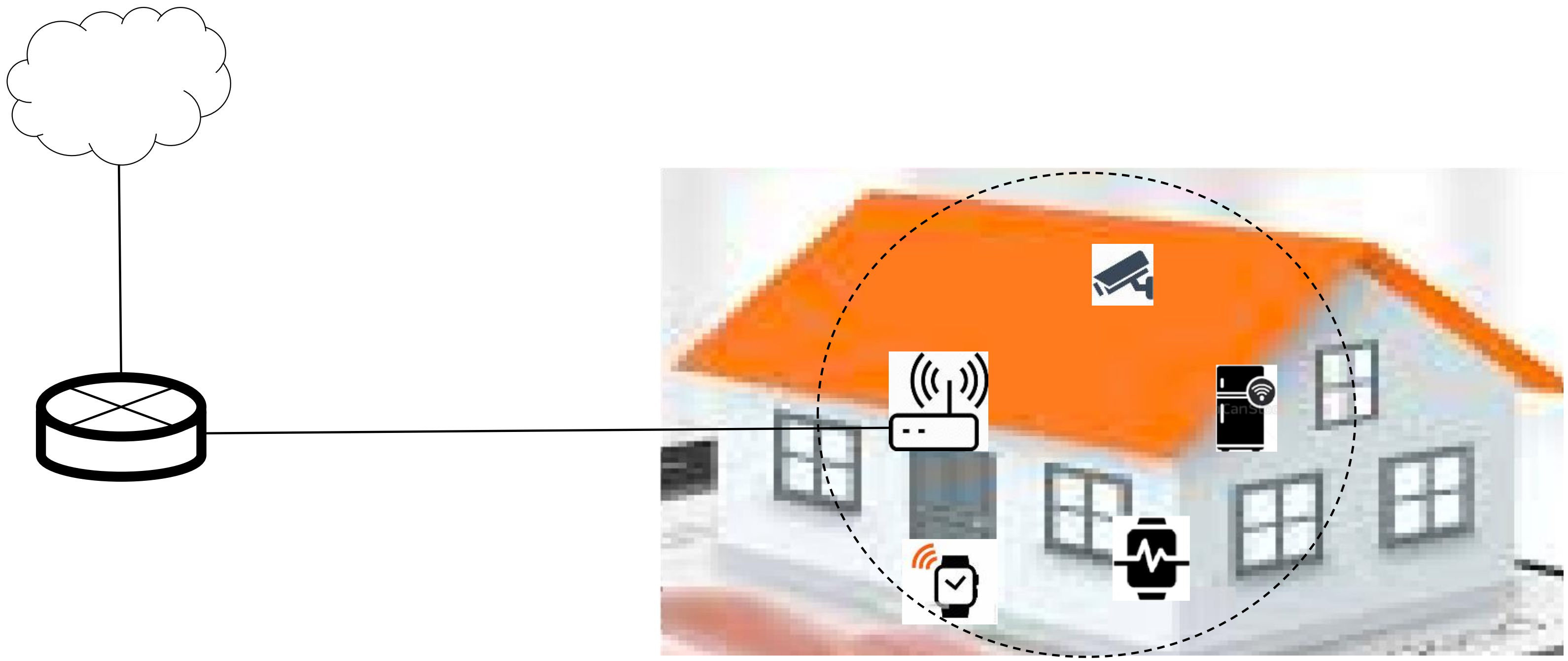
Src: Levis's workshop talk at Stanford

What is different in IoTs?

1. Resource constraint devices	Heavy Cryptographic algorithms
2. Need connectivity, as Client as well as Server	• Open Ports • Global IP Addresses • Vendor or 3rd Party analytics
3. Design is based on easy of use	• Not designed for Periodic & Remote updates • Unsafe open source libraries
4. Heterogenous with proprietary protocols	• “Security by Obscurity”

UNSW SYDNEY

IoT and Smart Home



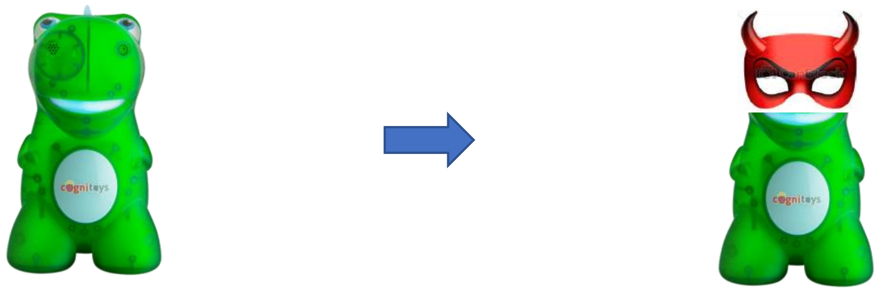
IoT and Smart City

IoT and Military Base

The Guardian reported on 01/28/2018:“Fitness tracking app Strava gives away location of secret US army bases”

IoT Vulnerabilities : Consumer Goods

- **Smart Children toys**: Best Inventions of 2015 by TIME Magazine



Rapid7: Baby monitors hacked to view video and speak to children

CloudPets: Teddy bear hacked to speak to children and access voice records

Hello Barbie: Doll Automatically connected to unsecured Wi-Fi networks

MiSafes: Children's smartwatch: 'easy to hack' , lacks of encryption, enabling location-tracking, spoof calls to the watch

IoT Vulnerabilities : E-Health Applications

Control Unit

Wrist band

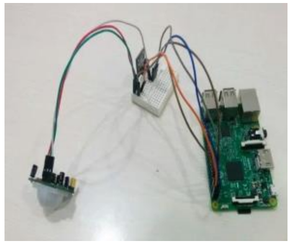
Programmer

Deep brain stimulator

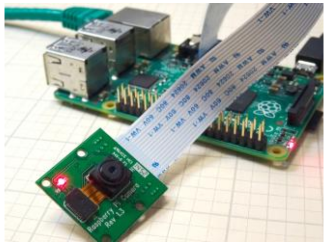
Glucose sensor + Insulin pump

Embedded pressure sensor

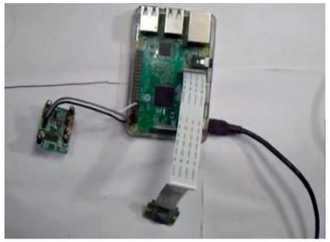
How difficult is it to build an IoT device?



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

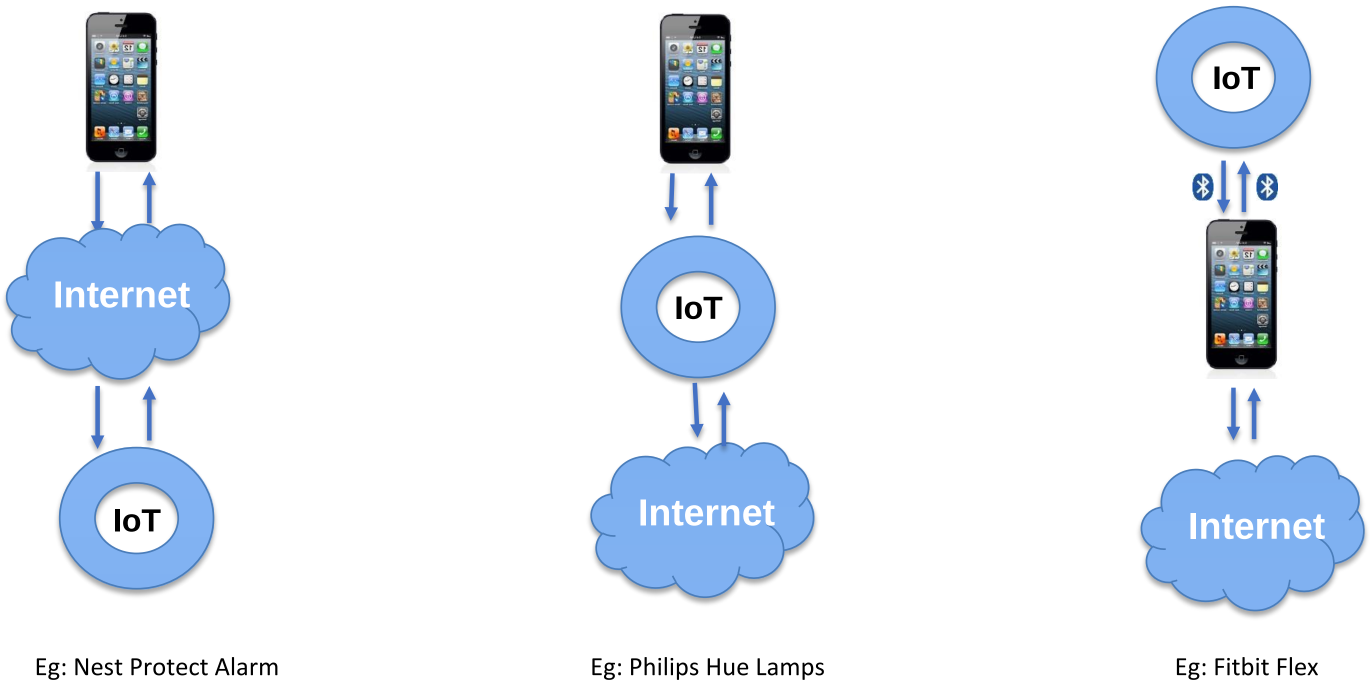
- Arduino
- Contiki
- Electric Imp
- Gadgeteer
- ioBridge
- Raspberry Pi
- SensorTag
- TinyOS
- Wiring
- Xively
- …….

Heterogeneous Comms Interfaces

External Server

Transit

Direct Access



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)

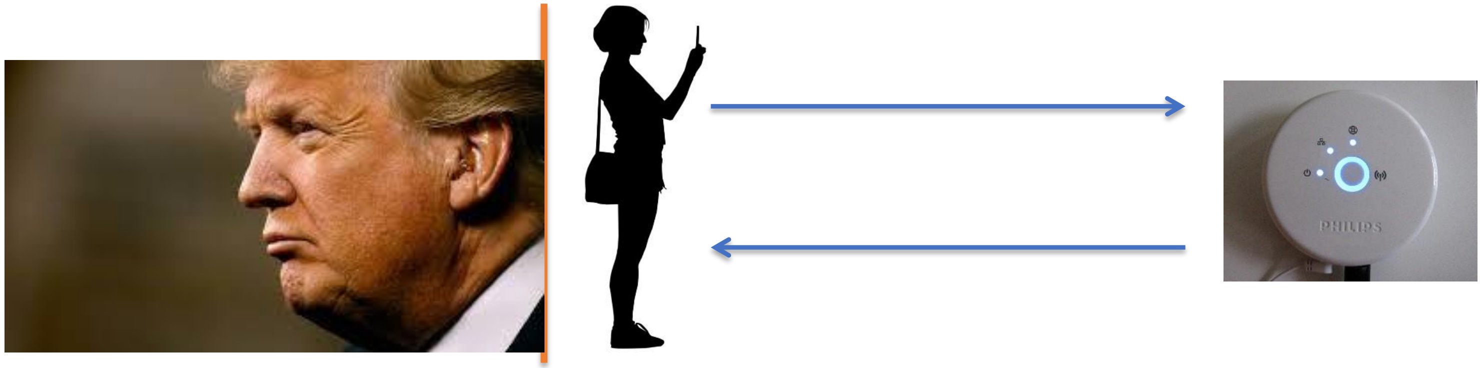
Communication Process

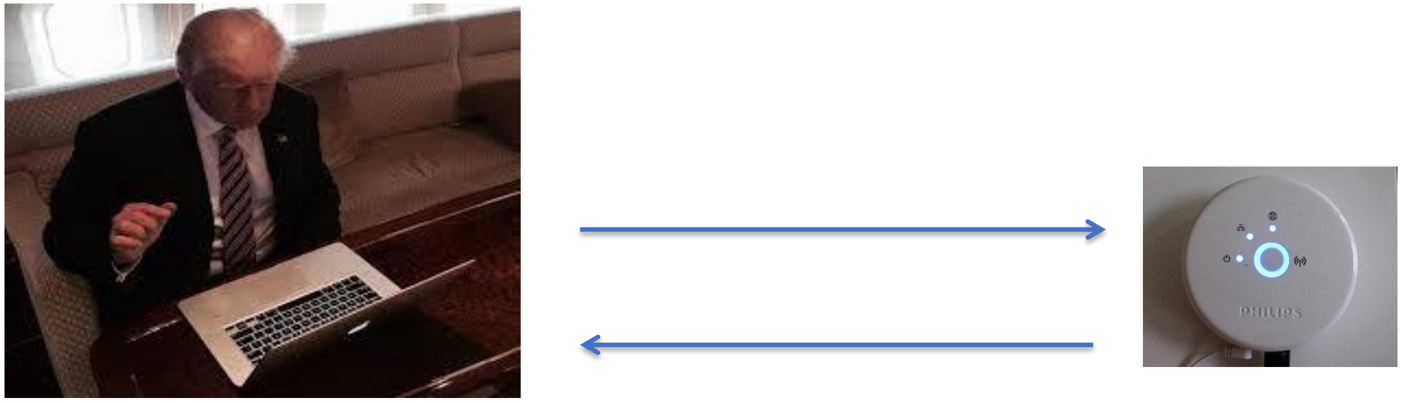
- Phone talks directly to the hue bridge and bridge then relays appropriate commands to the lights using ZigBee.

- All Communications between the phone and the bridge were in plain text in **Older** versions.


Plaintext
IP
Plaintext
ZigBee™
PHILIPS

Philips Hue Attack



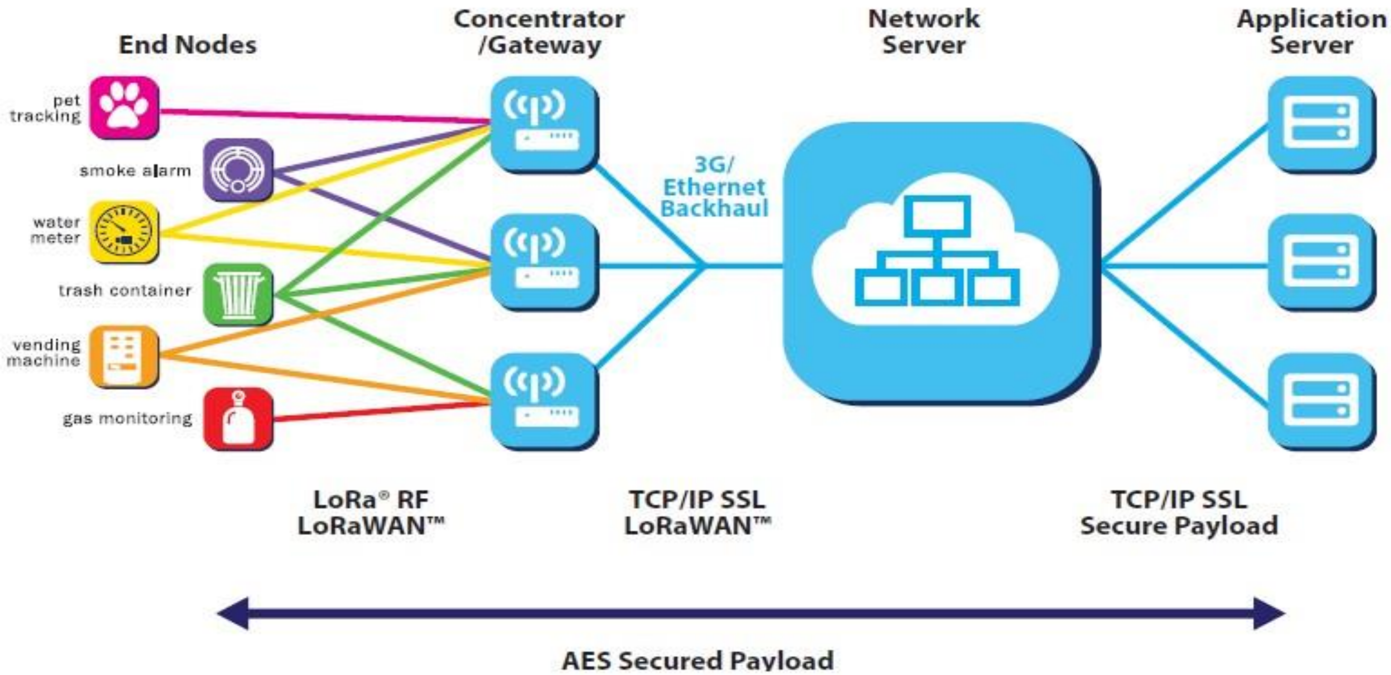


Philips Hue Attack

(Demo former UNSW student Andrew Bennet)

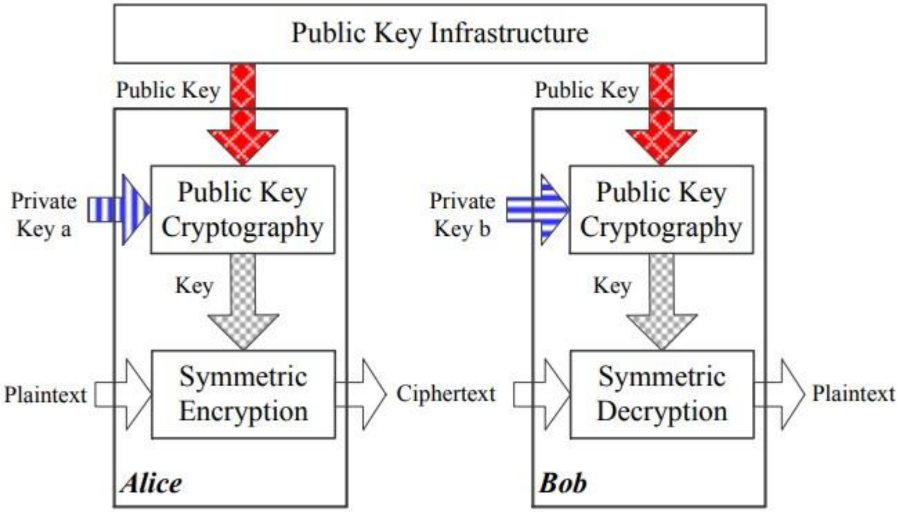
Vieo removed to reduce file size

LoRaWAN Network Architecture

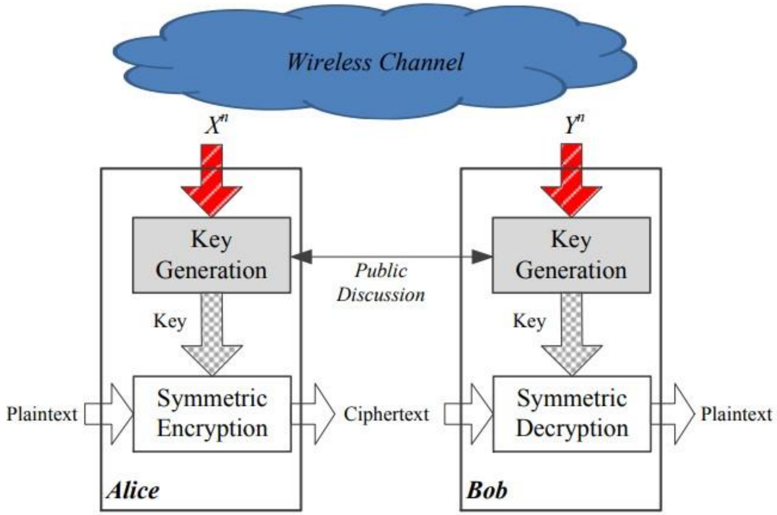


Physical layer key generation

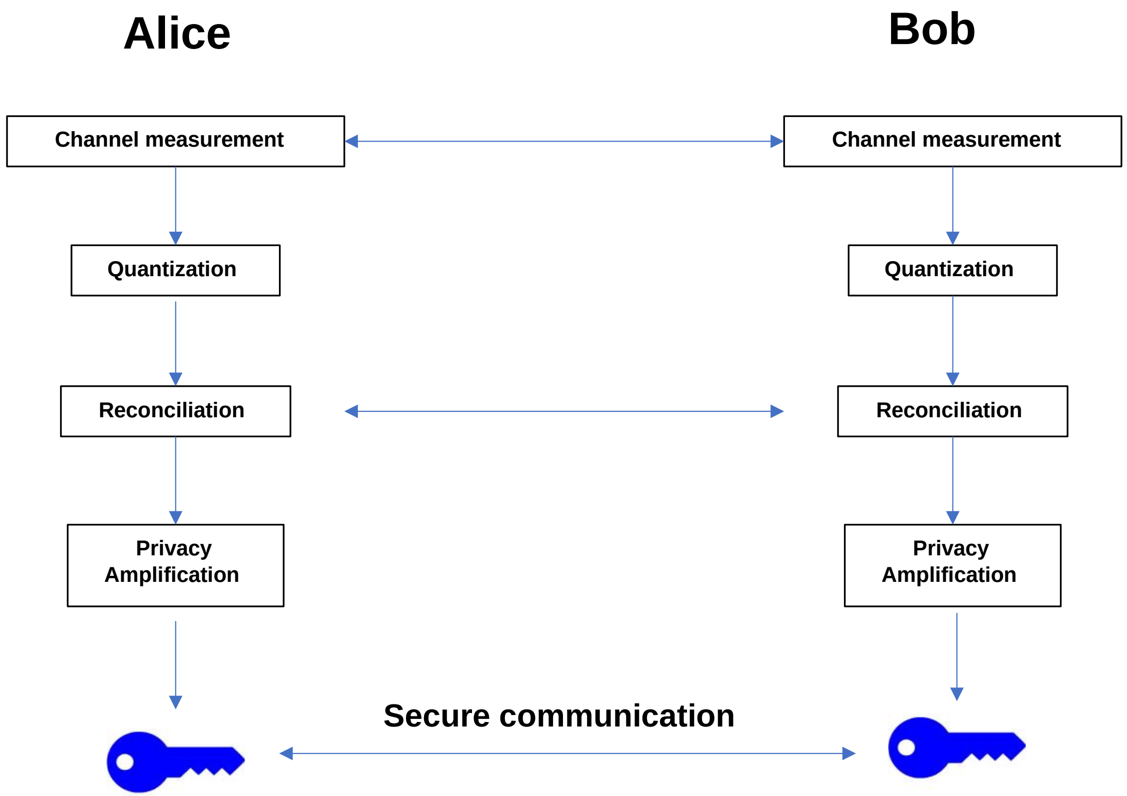
Classical encryption system



Key generation system based on wireless channel



System Design



Evaluation

Experimental device: mdot LoRa module

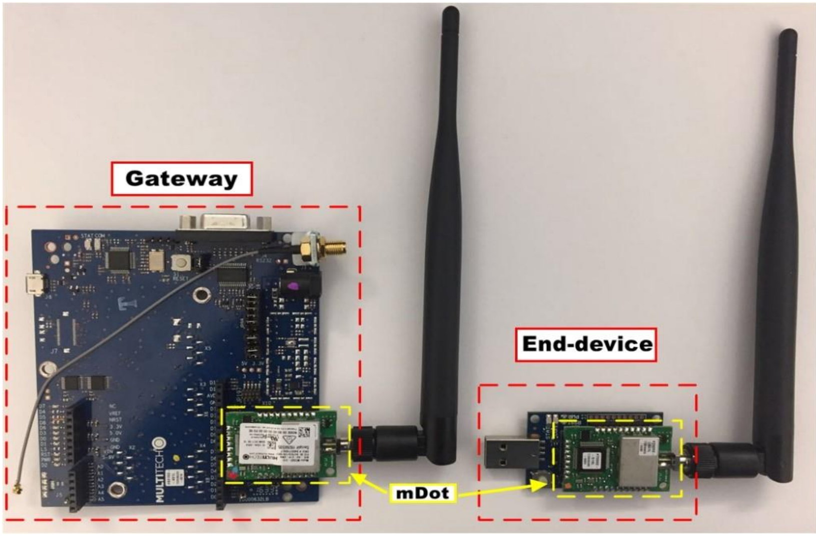


Table I: Parameters setting.

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

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

UNSW SYDNEY

Memory Overhead

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

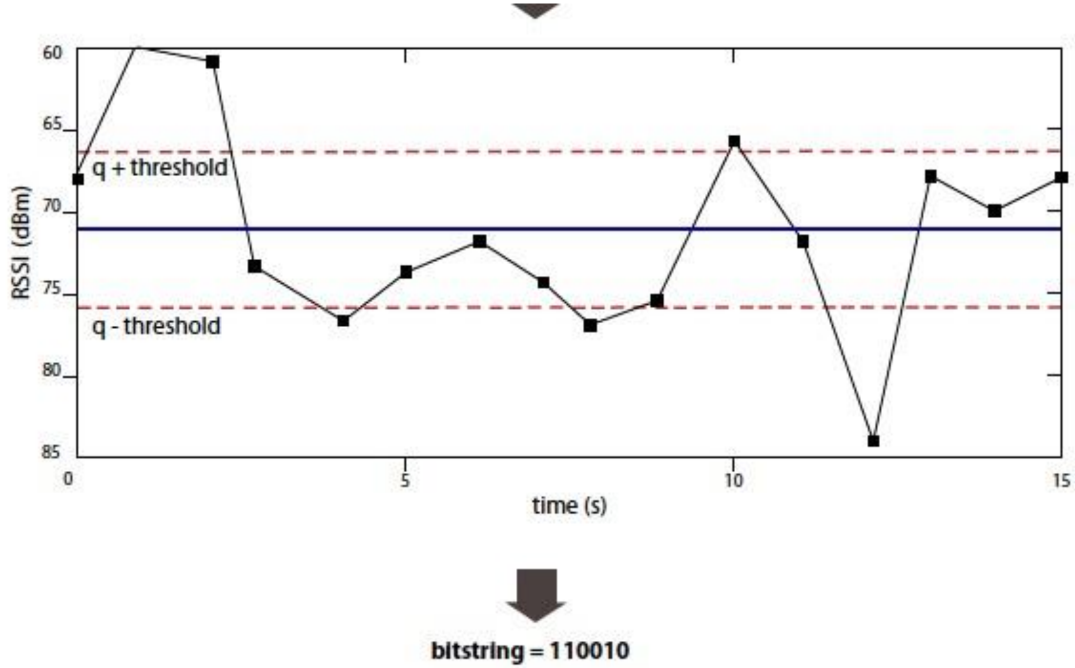


Figure 5: Level crossing quantization technique

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

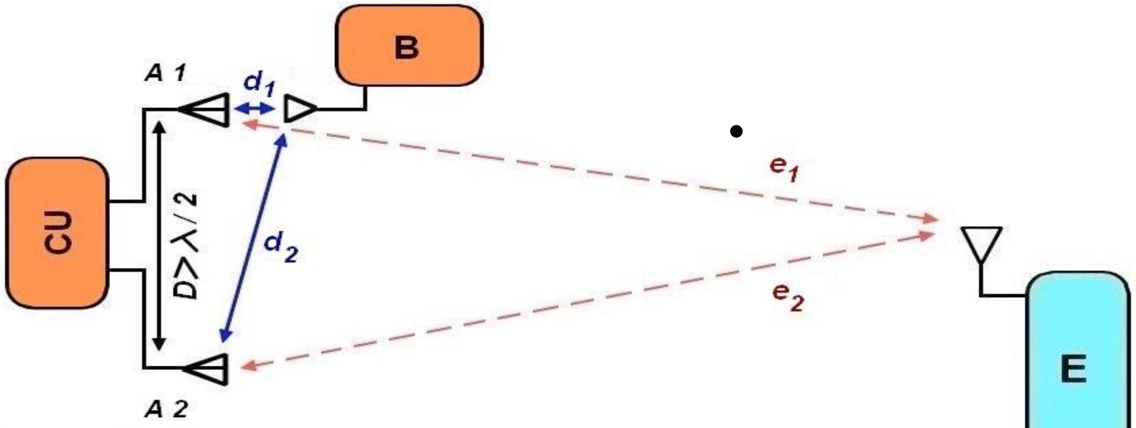
SeAK: Secure Pairing

Platforms

- Control Unit (CU) - Opal sensor platform

Device Iris motes

- and Adversary –



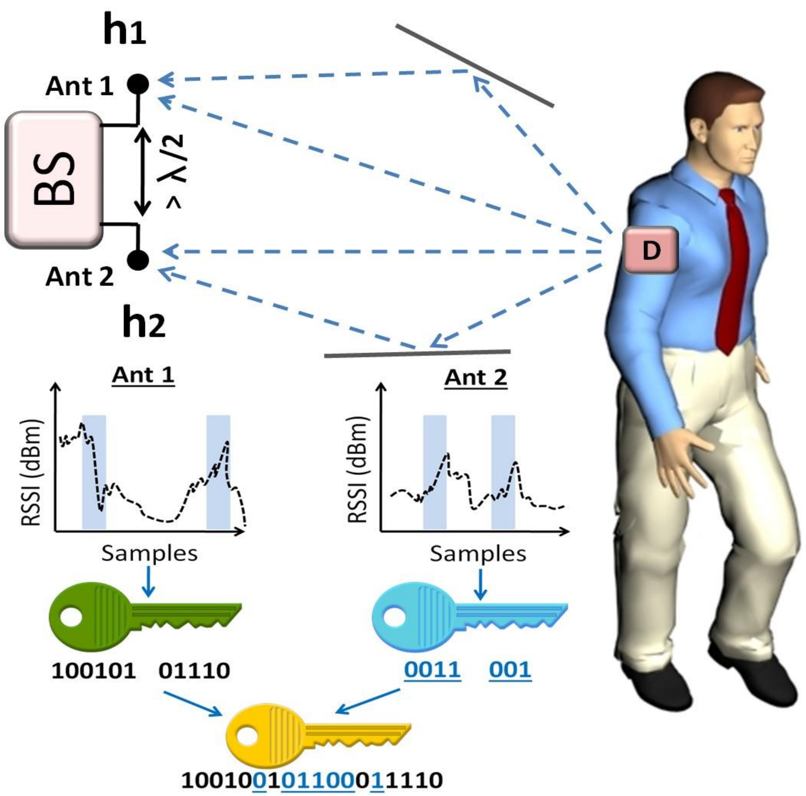
$$P_r = P_s K / d_r^{\alpha} \quad (1)$$

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

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.

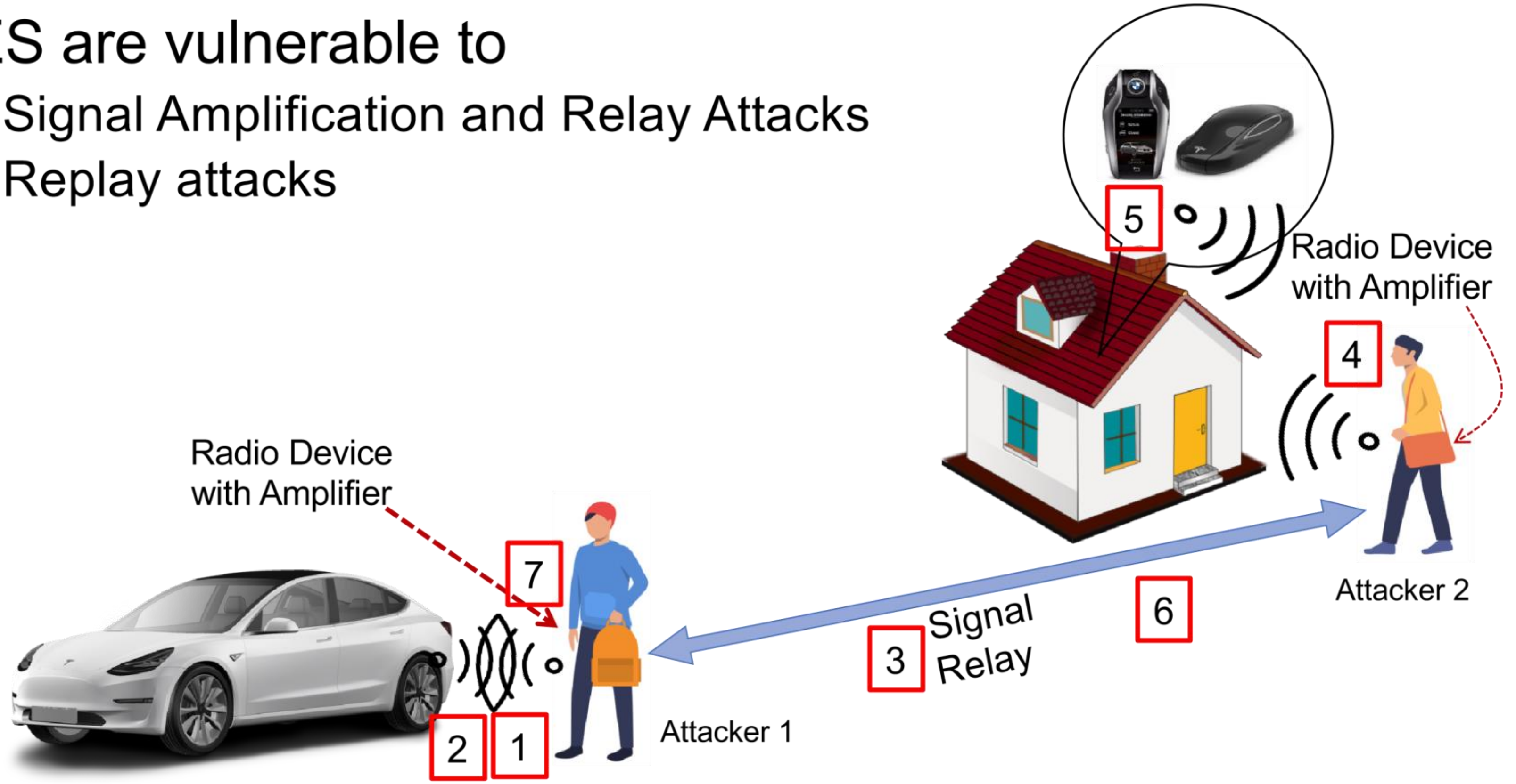
Keyless Entry Systems for Modern Vehicles

- Key-less entry systems (KES) for vehicles are becoming increasingly popular due to their ease of usage and convenience.
- Remote door unlock and engine start by detecting the proximity of key fob/owner's personal device
- The traditional physical key of the car is being replaced by a digital key stored in personal device – phone, wearables etc.

G. Revadigar, C. Javali and S. Jha, "ProxiCar: Proximity-Based Secure Digital Key Solution for Cars," 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), Bengaluru, India, 2020

KES Security Vulnerabilities

- KES are vulnerable to
  - Signal Amplification and Relay Attacks
  - Replay attacks

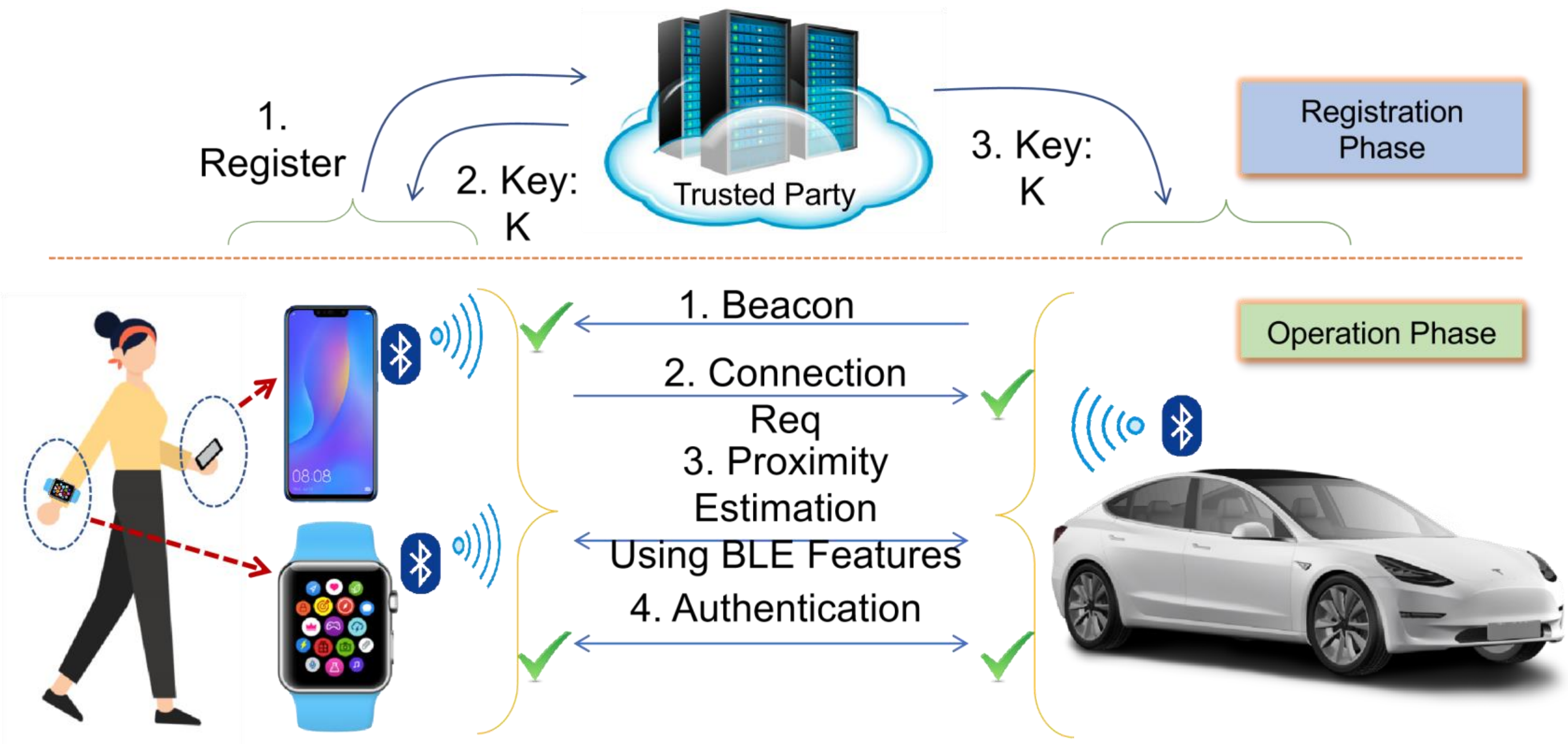


Relay Attack on KES

Video:

Insert the relay attack video here

ProxiCar Architecture

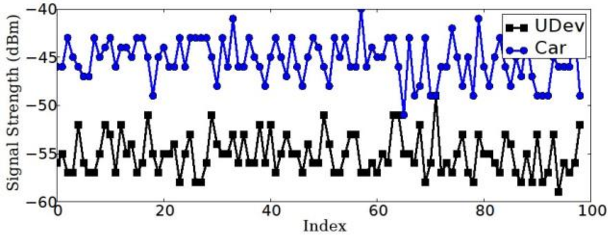


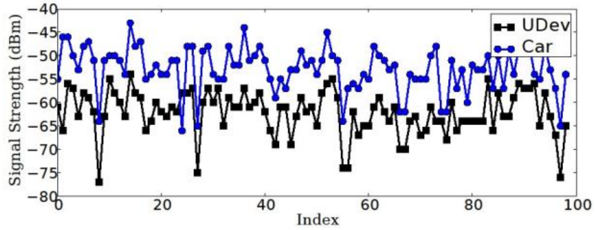
UNSW SYDNEY

Experiments – RSSI Processing

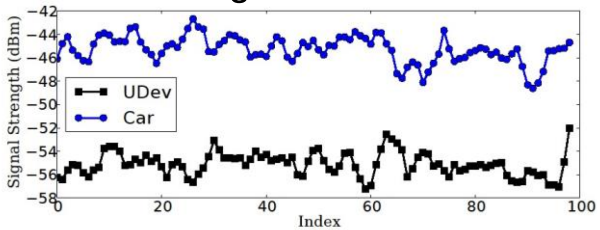
Case1: Near+StaticCase 2: Near+Wave

Filtered RSSIFiltered RSSI

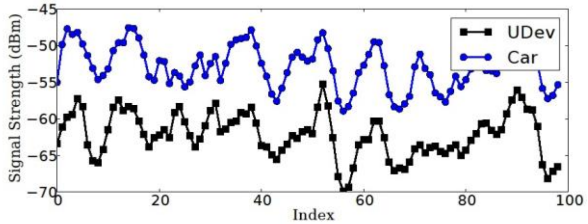




Original RSSI



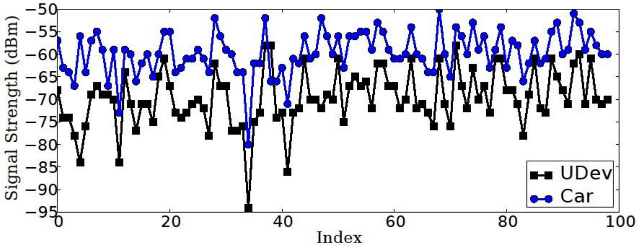
Original RSSI

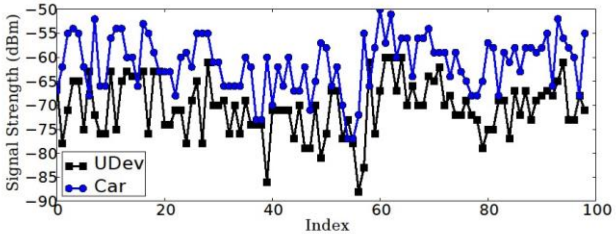


Experiments

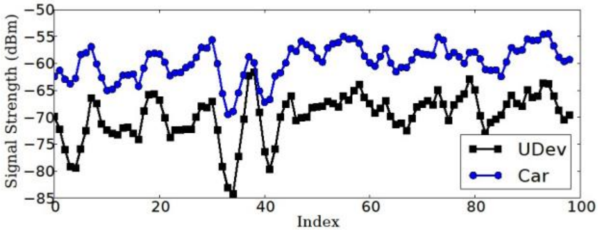
Case 3: Walk+HandCase 4: Walk+Pocket

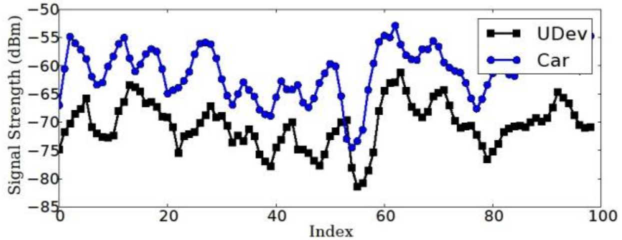
Original RSSIOriginal RSSI





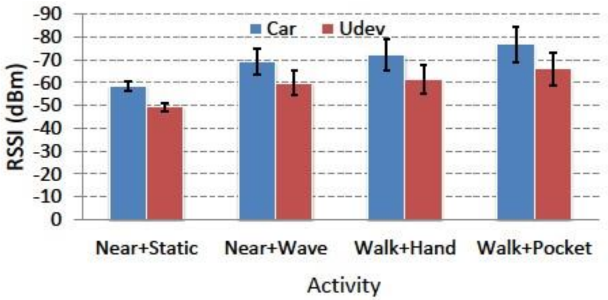
Filtered RSSIFiltered RSSI



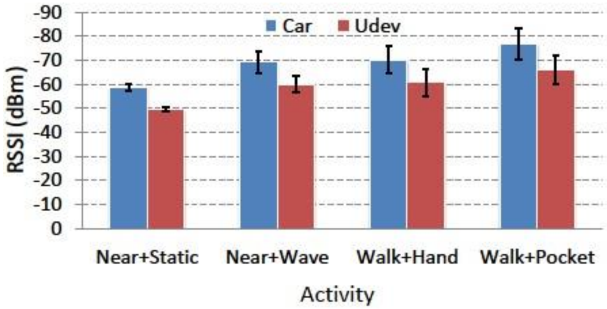


User Activity Detection Using RSSI Information

Activity Detection



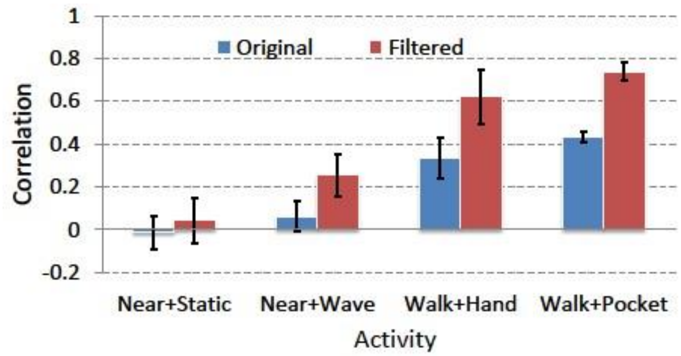
Analysis of correlation



Filtered data

Abort authentication if static case (attack).

Raw data



RSSI information helps to identify different user activities – mainly between static and mobile cases –

Security Features of Proposed Solution

- ***Passive Attacker***: cannot learn about the channel features obtained by two legitimate parties by observing their communication - Like Eve-1,2,3 in LoRAWAN experiments

- ***Active Man-in-the-middle Attack***: UDev and Car use pre-shared secret key K for encrypting all communication content.
- ***Relay Attack***: The channel reciprocity holds true only between a pair of transceivers communicating directly with each other (i.e., without a relay)
- ***Denial-of-service Attack***: by analysing the BLE beacon intervals and on-board sensors of UDev, actual device mobility and/or attack can be recognised to abort connection

Location Proof - Motivation

Hospitals

Bank, Organizations

Location Proof: System Model

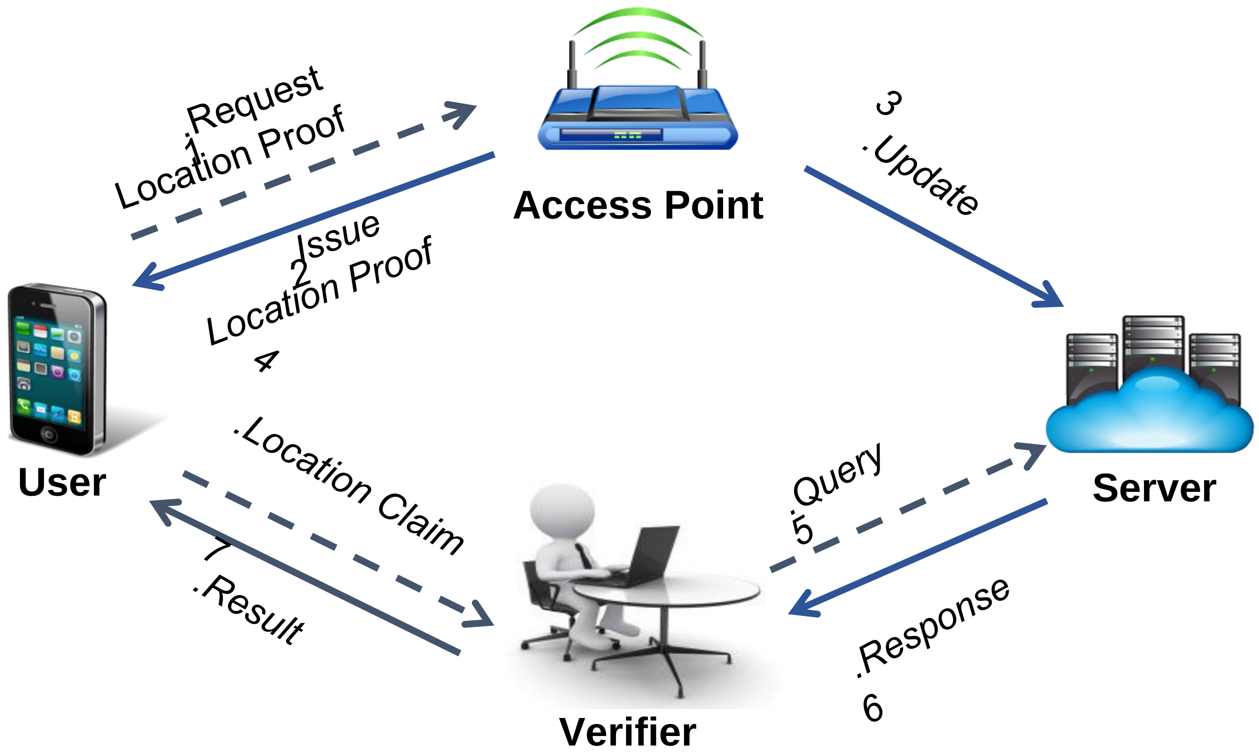


Figure 1: System Model

Location Proof: Basic Ideas

- Generation of the location tag based on wireless PHY layer characteristics
- Information theoretically secure (Fuzzy Extractor/Vault based schemes)
- Non-reproducible by an adversary
- Assumptions:
- AP and Verifier are honest
- Users are registered with LBS
- Public-private key pairs are certified by Certificate Authority (CA)
- Users and APs are recognized by their identities public keys

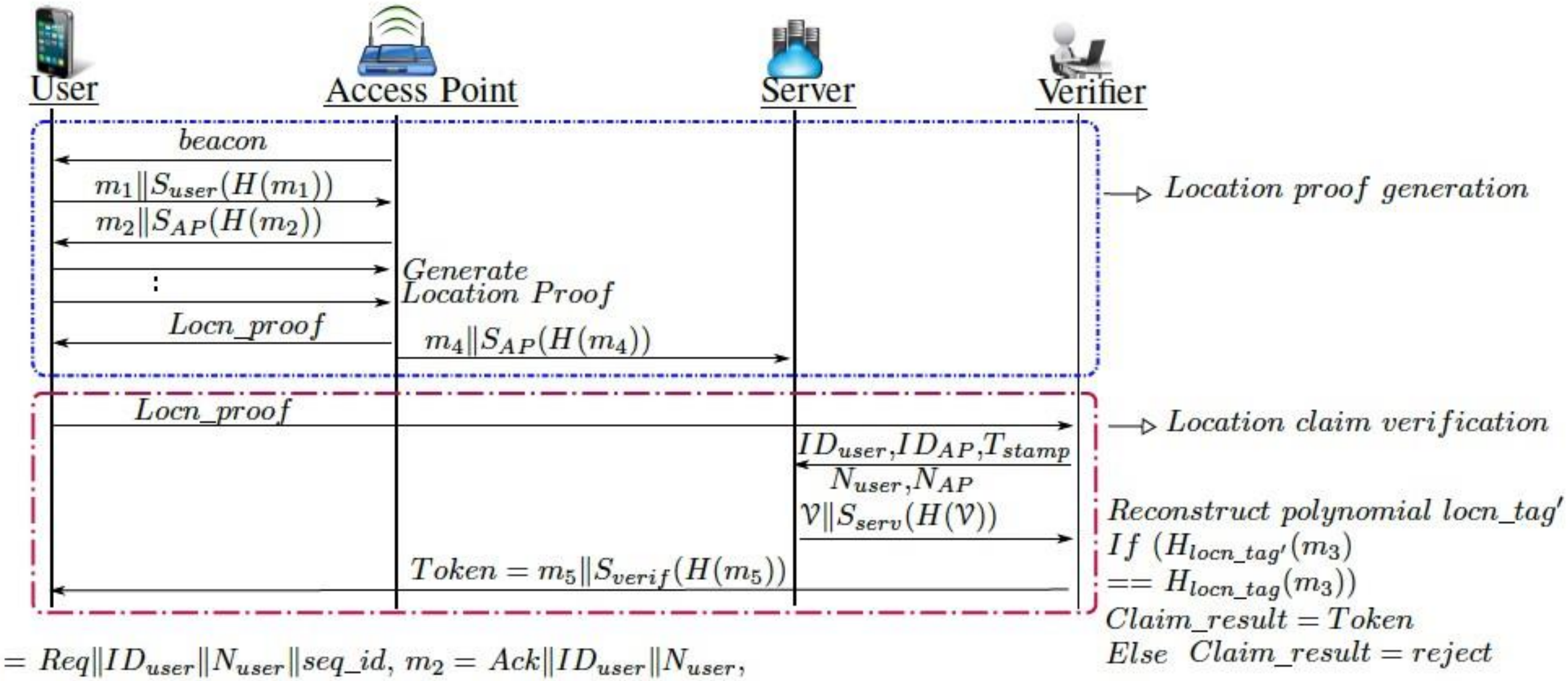
Fuzzy Vault Scheme (Juels and Sudan)

- A nice Crypto scheme to hide secret *S* in a vault using set *A*
- Unlocking of Vault: secret revealed only if set *B* is close to set

A

- *B* shares sufficient number of values to *A*
- We use channel state information (CSI) to construct shared secret
- AP extracts the CSI from all the received packets
- Also gets coarse-grained location of user (a DB of mapped grid of location available at AP)

Protocol for Location Tag



$m_1 = Req \| ID_{user} \| N_{user} \| seq\_id$, $m_2 = Ack \| ID_{user} \| N_{user}$,

$m_3 = E_{verif}(\mathcal{B}) \| ID_{user} \| N_{user} \| ID_{AP} \| N_{AP} \| T_{stamp}$, $Locn\_proof = m_3 \| S_{AP}(H_{locn\_tag}(m_3))$

$m_4 = \mathcal{V} \| ID_{user} \| N_{user} \| ID_{AP} \| N_{AP} \| T_{stamp}$, $m_5 = N_{verif} \| locn\_tag$

Fig. 2: Message flow between the four entities of our proposed solution.

Location Proof: Security Properties

- If a User creates his/her own location claim and submits to the Verifier?
- If a User tampers the location proof to gain benefits for a different location and time?
- If a User transfers his/her location proof to another User?
- Can an adversary obtain information from locn_tag from vault V?
- Can an adversary modify the token?

For details:

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

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

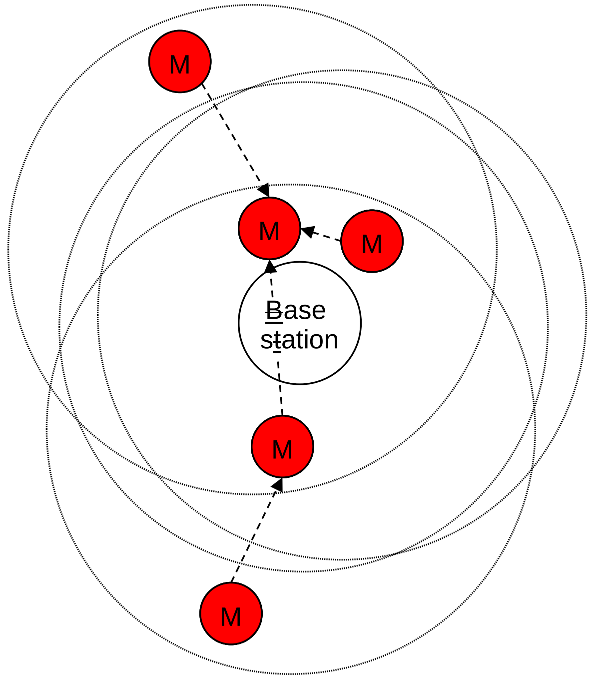
- Packet injection or eavesdropping is easy
- Security solutions for point-to-point communication not scalable for large deployments
- Broadcast challenges
- Scale to large audiences
- Dynamic membership
- Low overhead (computation & communication)
- Packet loss
- How to achieve reliability in broadcasts?

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



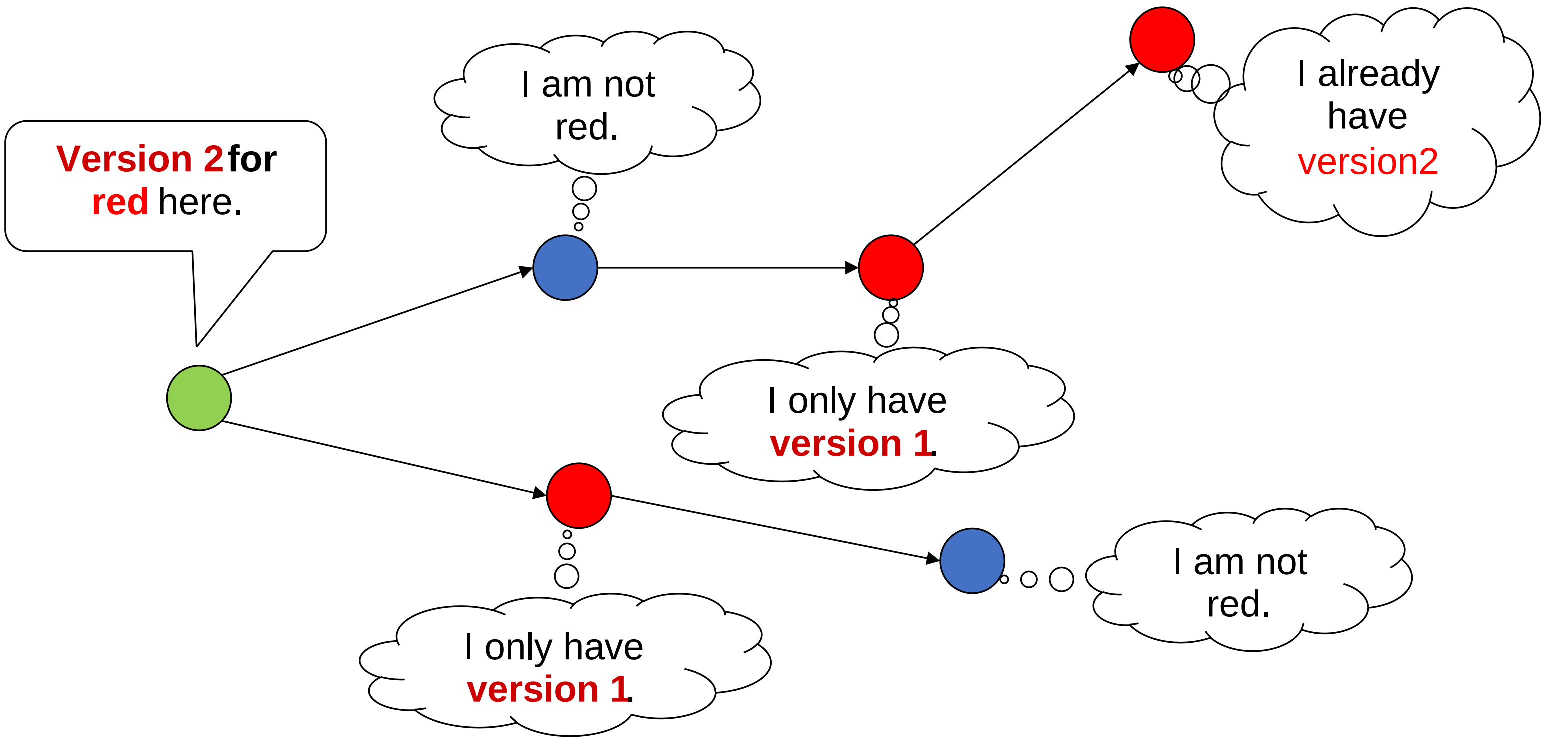
SEDA: SEcure Over the air code Dissemination Architecture

- Motivation: To produce experimental system which serves as a guideline for future deployment

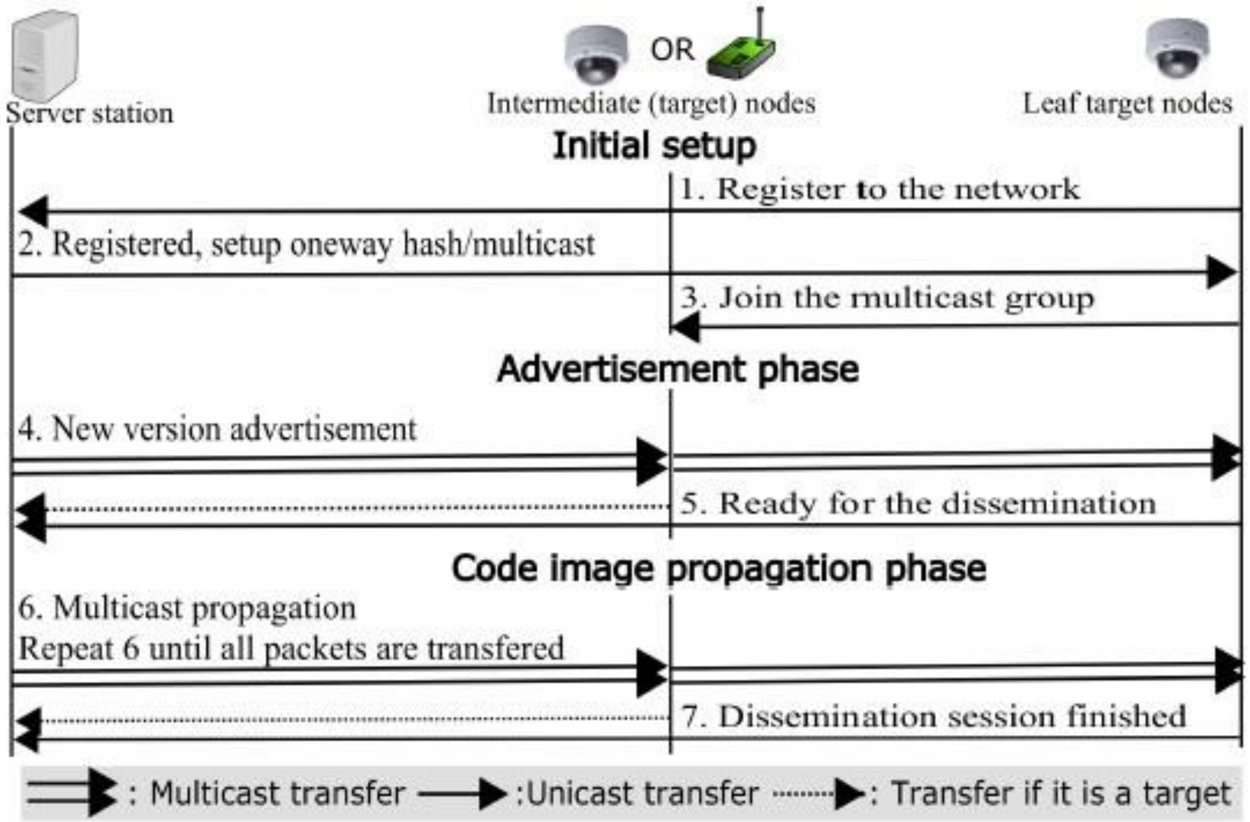
- Use overlay multicast communication model for efficient dissemination and key distribution
- Public key cryptographic broadcast encryption scheme (BGWt) - for efficient group key distribution/management, and low decryption overhead.
- Identify potential security threats and defensive measures
- Experimentally validate the architecture and provide performance benchmark

Broadcast propagation

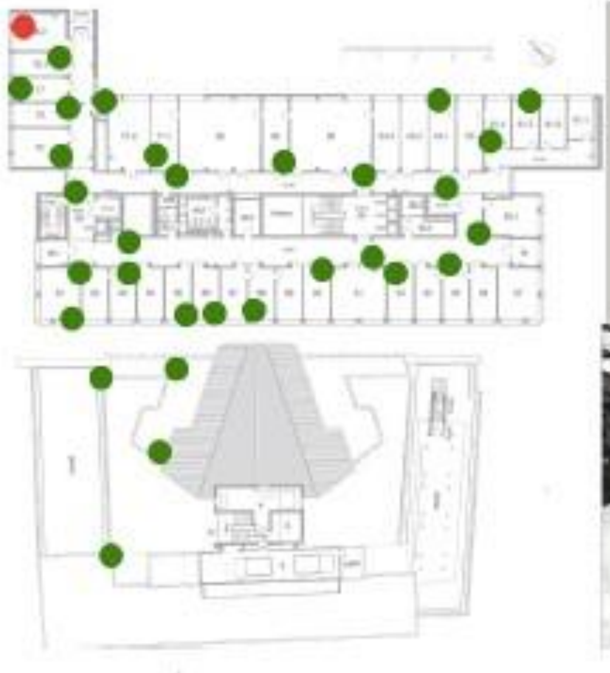
Server periodically broadcasts new version

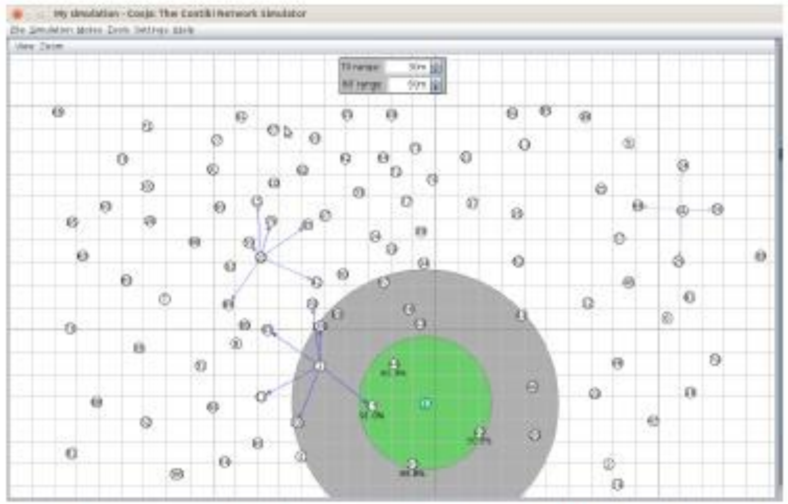

Version 2 for red here.
I am not red.
I already have version2
I only have version 1.
I only have version 1.
I am not red.

SEDA Protocol Overview



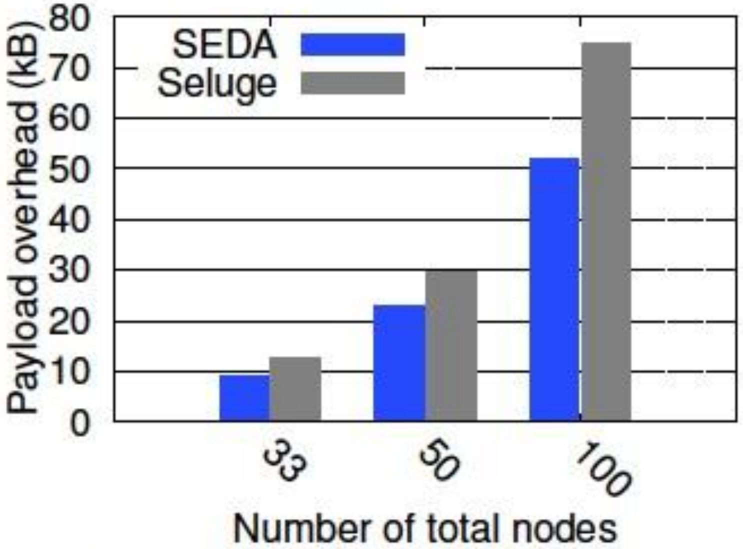
Flock Testbed and Cooja simulator



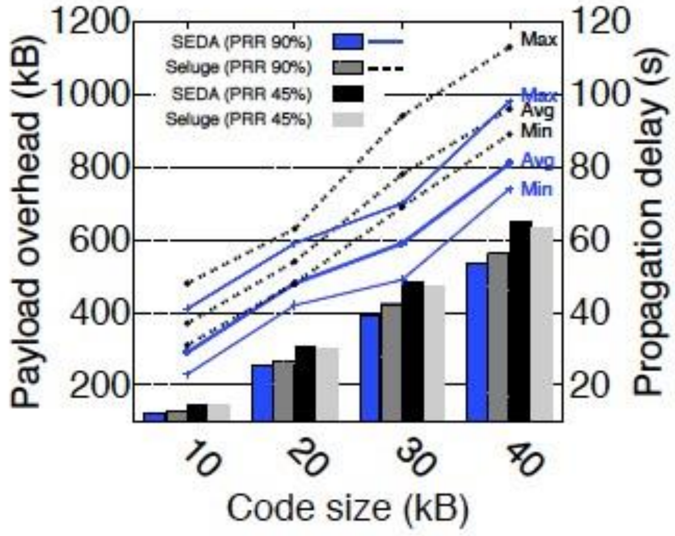


(c) Cooja simulator setting for a 100 node network.

Results



(a) Key establishment overhead comparison.



(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 !!

UNSW SYDNEY

Q&A

Selected Publications

- Ahmed, Nadeem & Michelin, Regio & Xue, Wanli & Ruj, Sushmita & Malaney, Robert & Kanhere, Salil & Seneviratne, Aruna & Hu, Wen & Janicke, Helge & **Jha**, Sanjay. (2020). A Survey of COVID-19 Contact Tracing Apps. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.3010226.

- Sanjay **Jha**, Covid Tracing App: Privacy and Security Concerns, https://www.youtube.com/watch?v=jyzh_kQEMo8&t=88s (Youtube Talk)

- Weitao Xu, Sanjay **Jha**, Wen Hu, Exploring the Feasibility of Physical Layer Key Generation for LoRaWAN, In proceedings of The 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (Turstcom), New York, USA,

- Weitao Xu, Sanjay **Jha**, Wen Hu, LoRa-Key: Secure Key Generation System for LoRa-based Network . IEEE IoT Journal (SCI IF: 5.863). In-press, accepted in Dec 2018.

- G. Revadigar, C. Javali and S. Jha, "ProxiCar: Proximity-Based Secure Digital Key Solution for Cars," 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), Bengaluru, India, 2020, pp. 282-289, doi: 10.1109/COMSNETS48256.2020.9027327.

Selected Publications

- 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.
- 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.
- 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

- 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, 238249.
- Z Abaid, MA Kaafar, S **Jha**, Quantifying the impact of adversarial evasion attacks on machine learning based android malware classifiers *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
- 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)

UNSW SYDNEY