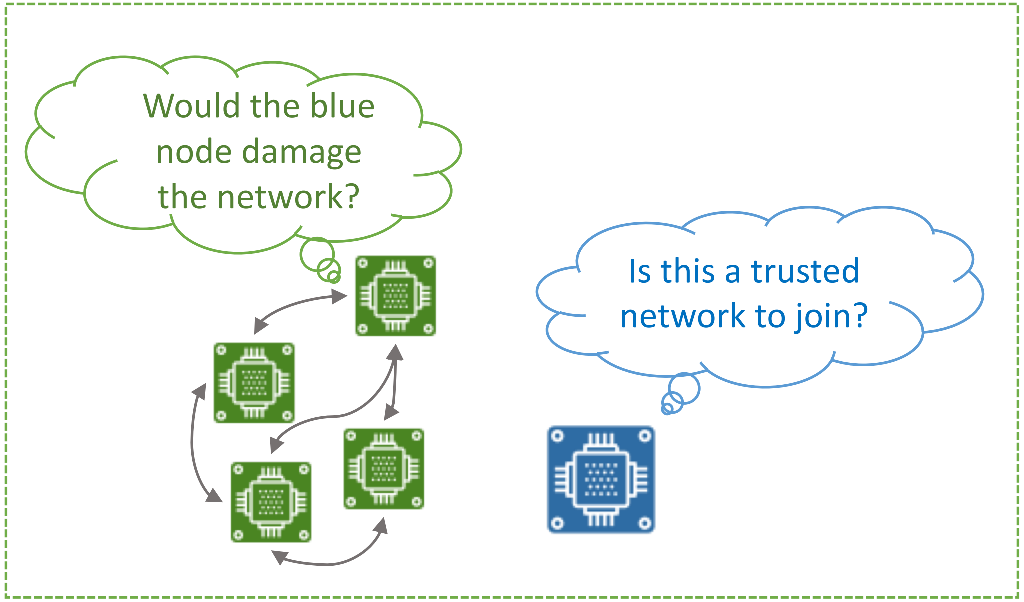
Principles of Secure Bootstrapping for IoTs

Ninghui Li, Syed Hussain, Sze Yiu Chau, Wencheng Wang

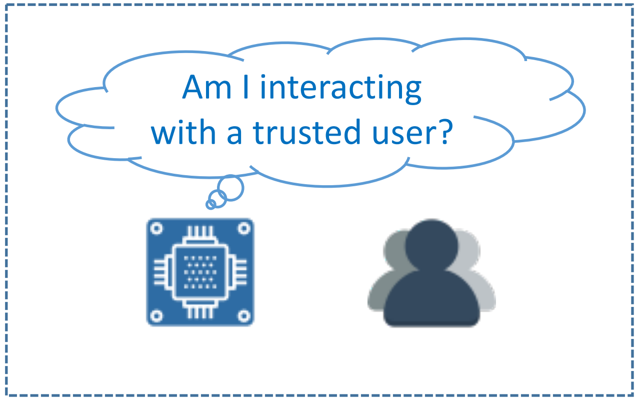
Purdue University

Part of NCSU SoS Lablets

Motivation – IoT devices need trust and secure communication

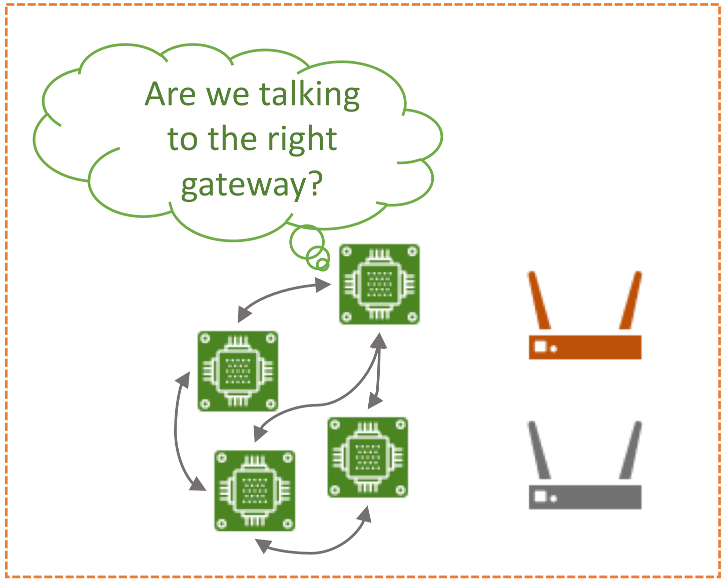


Trust between devices



Trust between device and users

Trust between devices and environment



Constraints

- Deployment scenarios determine resource availability
  - Power supply
  - Resources
    - Memory
    - Processing Power
    - Storage
    - Display
  - Serviceability
    - Physical access
    - Offline ports for update

Constraints limit options

- Deployment scenarios determine resource availability
  - Power supply
  - Resources
    - Memory
    - Processing Power
    - Storage
    - Display
  - Serviceability
    - Physical access
    - Offline ports for update

Limited budget on crypto.; only willing to use infrequently

Difficult to rely on human intervention without these

Must rely on remote updates

Outline

- Privacy attacks to 4G/5G cellular paging protocols
- Zigbee security analysis
- Analyzing semantic correctness of PKCS#1 v1.5 public key signature verification

Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information

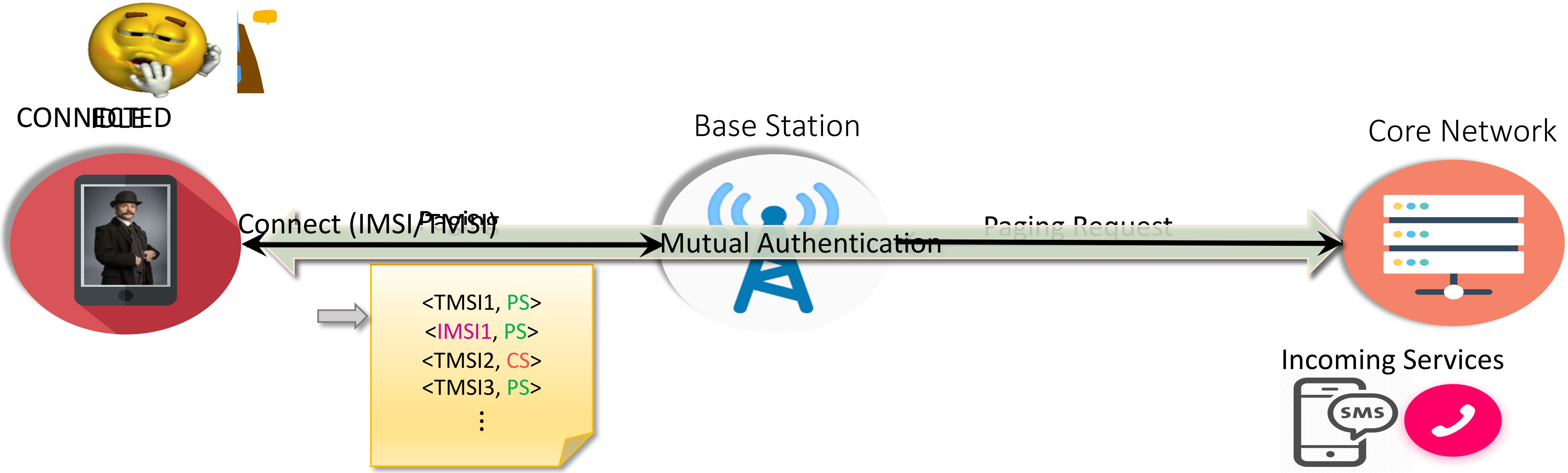
Syed Rafiul Hussain, Mitziu Echeverria[†], Omar Chowdhury[†], Ninghui Li[*], Elisa Bertino[*]

Purdue University, University of Iowa

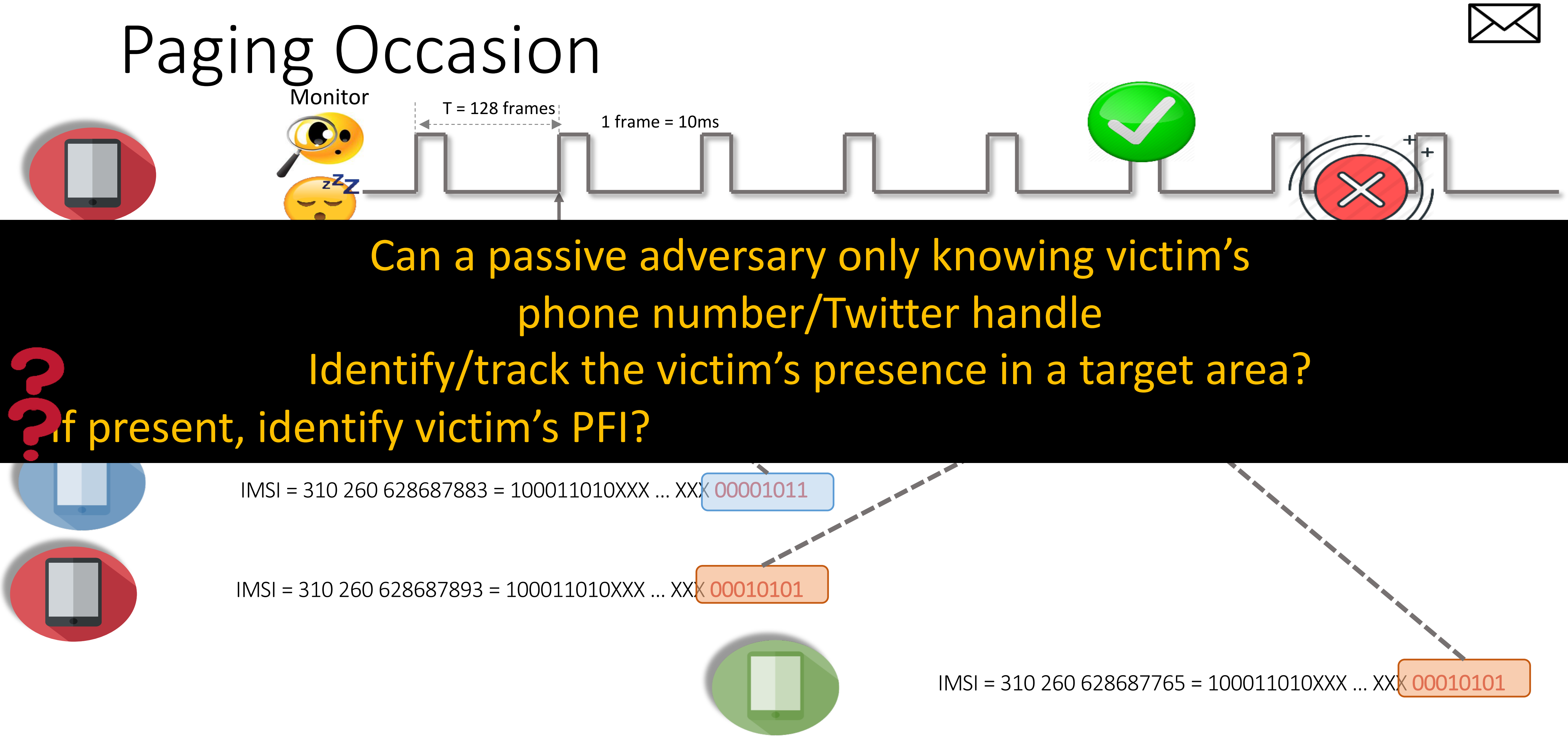
Paging Procedure

IMSI: International Mobile Subscriber Identity

TMSI: Temporary Mobile Subscriber Identity



Paging Occasion

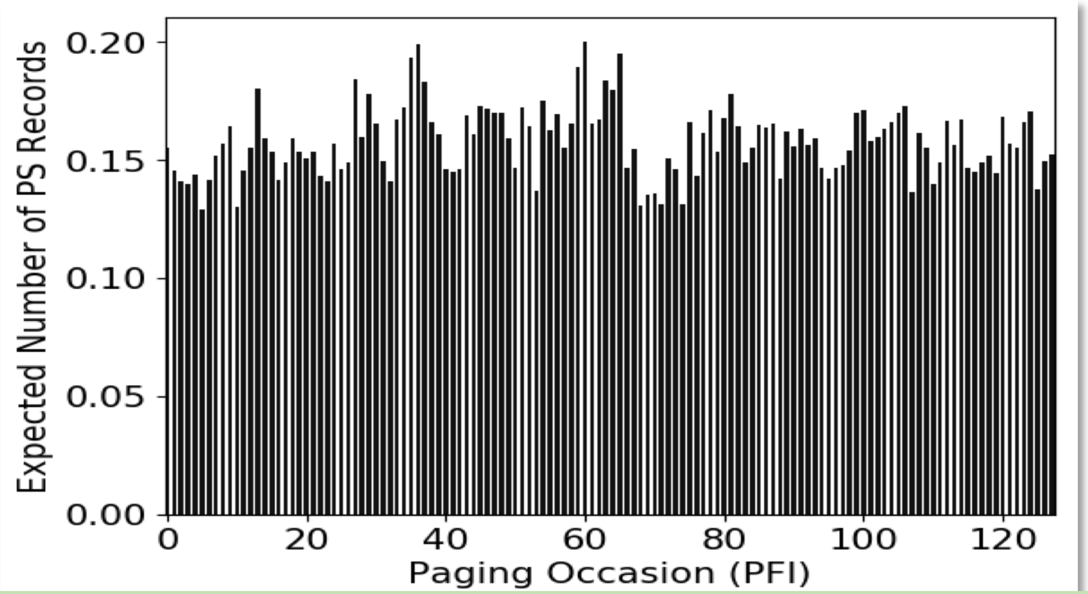


Can a passive adversary only knowing victim’s phone number/Twitter handle

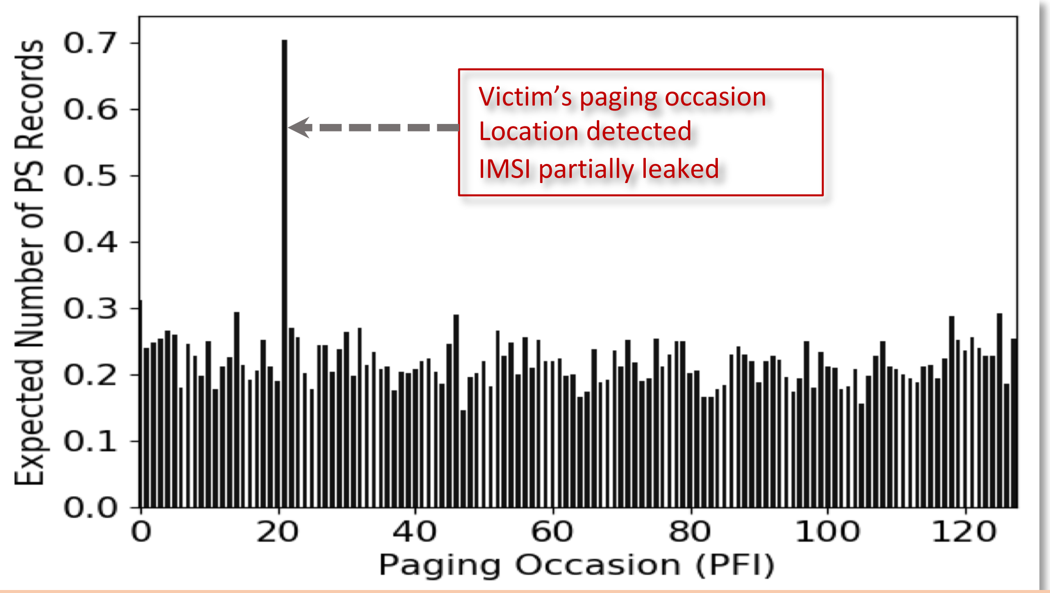
Identify/track the victim’s presence in a target area?

If present, identify victim’s PFI?

ToRPEDO
TRacking via Paging mEssage DistributiOn



Distribution of paging messages (PS records) when attacker makes no phone call



Distribution of paging messages (PS records) when attacker makes silent phone calls

Filtering - ToRPEDO Attack (1/3)

Assumption: Perfect delivery of paging.

Remove from the set of all PFI values that do not have a paging message

Paging Delivery/Capturing Is Not Reliable

Received PFI = {12, 21, 27, 50, 65, 97} Candidate PFI = {12, 21, 27, 50, 65, 97}

+1: Received PFI = {2, 21, 45, 88, 97, 125} Candidate PFI = {21, 97}

+2: Received PFI = {7, 21, 39, 65, 91, 117} Candidate PFI = {21}

Counting - ToRPEDO Attack (2/3)

Continue calling until a unique PFI is found satisfying:

k paging out of *n* calls

Does not filter out the victim's PFI if paging is missed for a call

High number of calls to filter out non-victim's PFI

Likelihood – ToRPEDO Attack (3/3)

16 paging records with PS and CS indication

Timing information

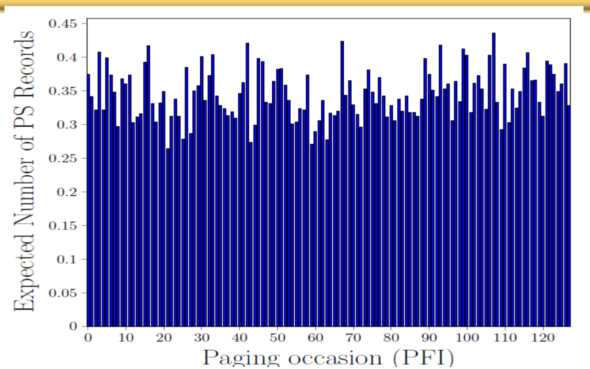
Compute the likelihood L_i of *i* to be the victim's PFI

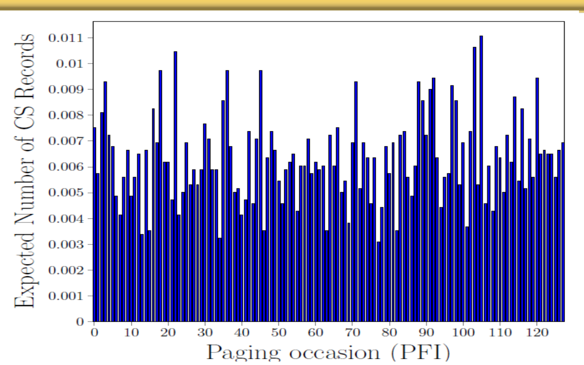
Compute the likelihood L_{-1}

The adversary identifies *i* as the victim's PFI when

$$\frac{L_i}{L_j} > 10^{\mathcal{T}}$$

Base rate of PS, and CS records





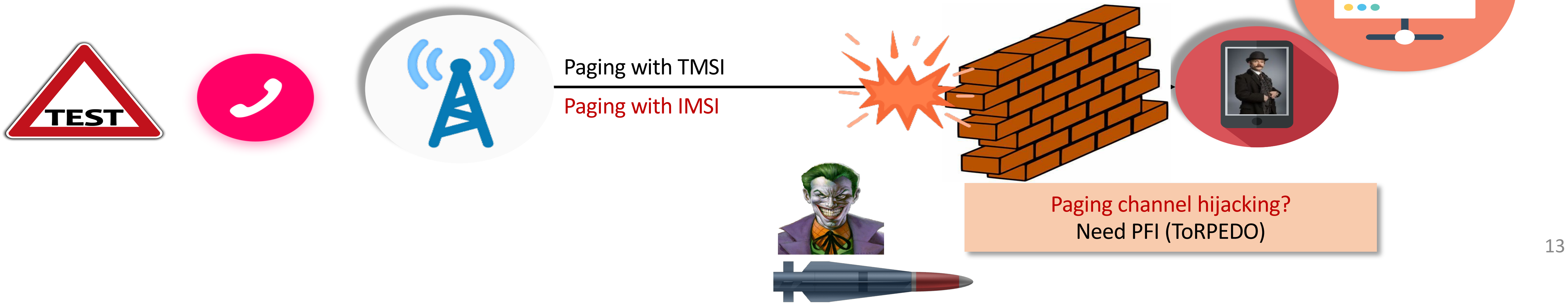
PIERCER (**P**ersistent **I**nformation **E**xposu**R**e by the **C**or**E** netwo**R**k)

MobileInsight

Many network operators use Paging containing IMSI

Link failure during interleaved TMSI reallocation and paging

Network failure



Paging channel hijacking?
Need PFI (ToRPEDO)

IMSI-Cracking Attack in 4G

49 bits

IMSI = 310 260 628687893 = 100011010XXX ... XXXXXXX00010101

MCC USA | MNC T-Mobile | MSIN

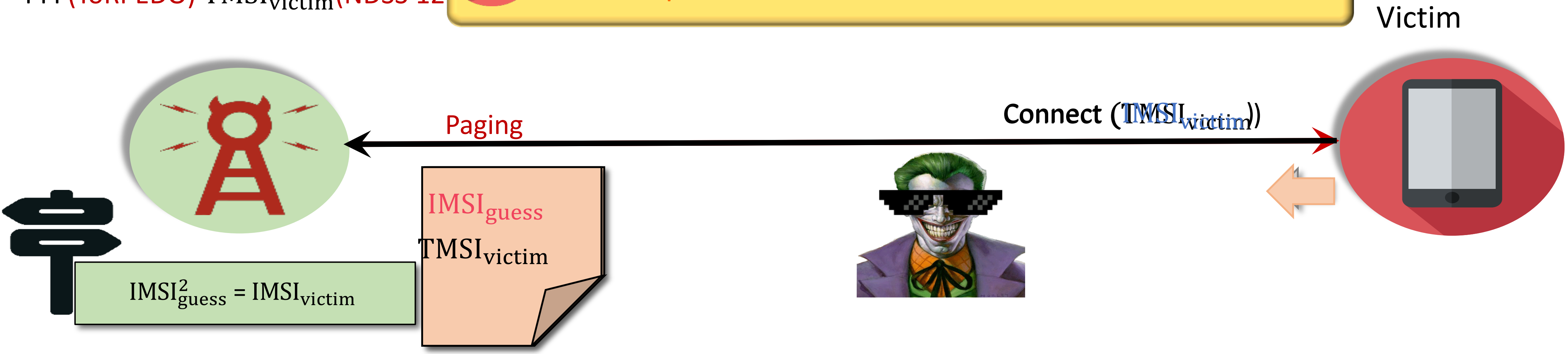
HLR 18 bits | 24 bits unknown | 7 bits

<TMSI1, PS>
<IMSI1, PS>
<TMSI2, CS>
<TMSI3, PS>
⋮

Response to TMSI ≠ Response to IMSI

Respond to TMSI/IMSI whichever comes first

PFI (ToRPEDO) $TMSI_{victim}$ (NDSS'12



IMSI-Cracking Attack in 5G

49 bits

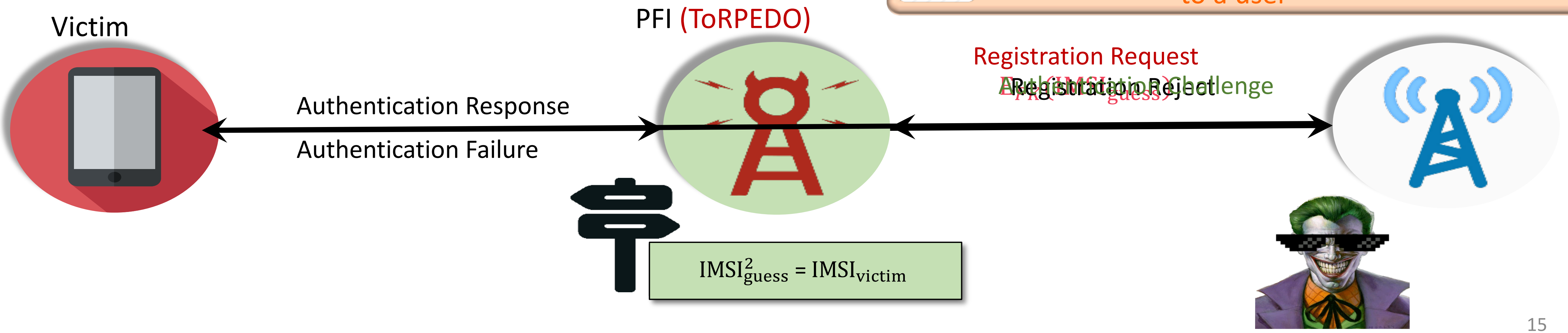
IMSI = 310 260 628687893 = 100011010XXX … XXXXXXX00010101

MCC USA	MNC T-Mobile	MSIN	18 bits	24 bits unknown	7 bits

No paging with IMSI in 5G

Exploit Registration Procedure

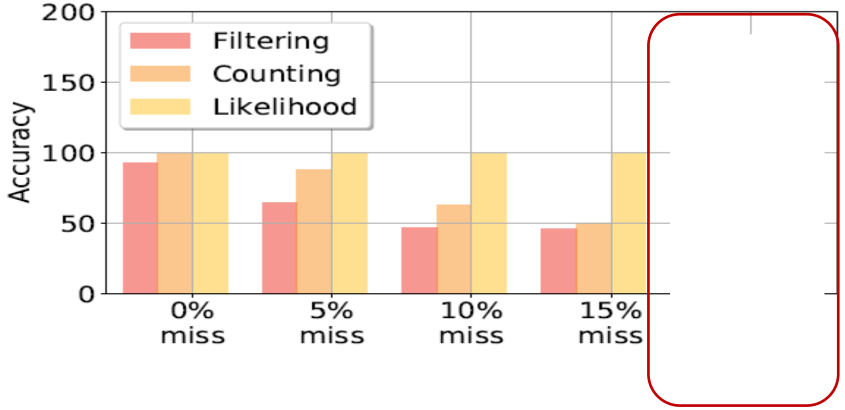
- Check if an IMSI is valid
- Check if an valid IMSI belongs to a user

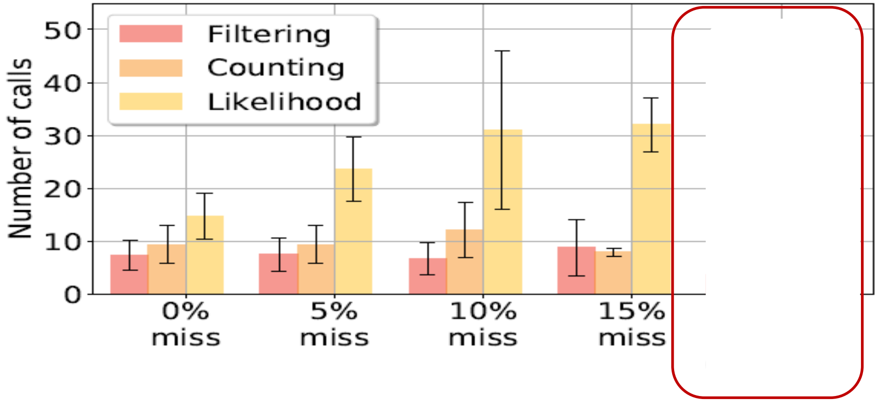


Evaluation

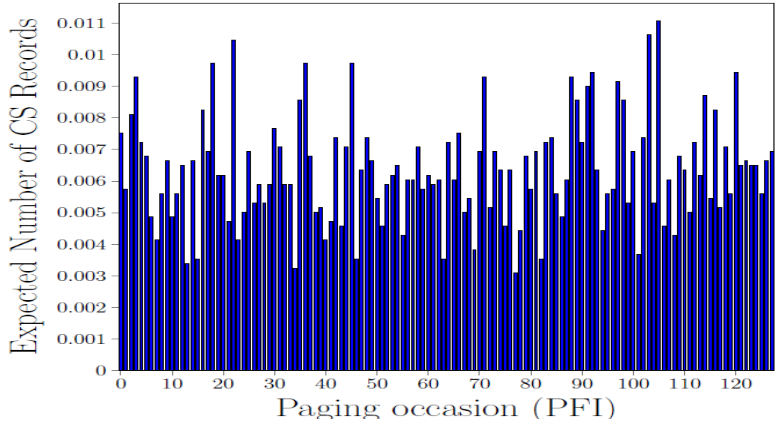
ToRPEDO

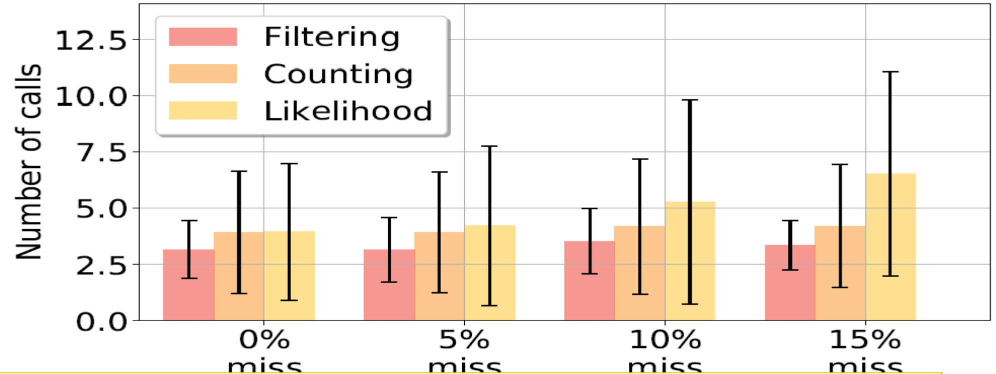
VoLTE calls (peak-time)





CSFB calls (peak-time)





PIERCER

1-2 phone call required

1 US
3 Germany
3 Austria
1 Iceland
3 Bangladesh

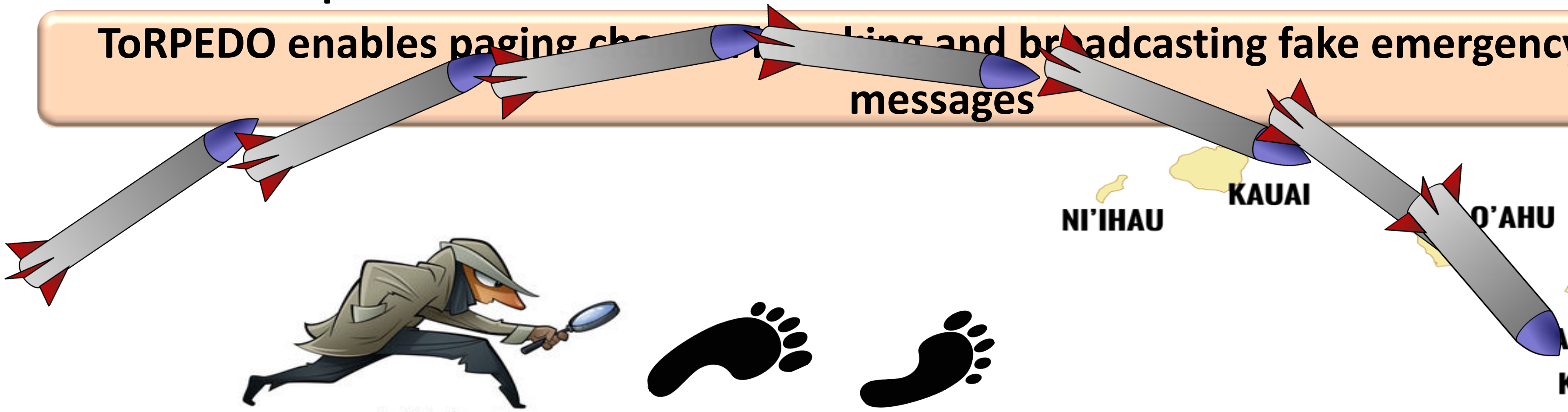
IMSI-Cracking:

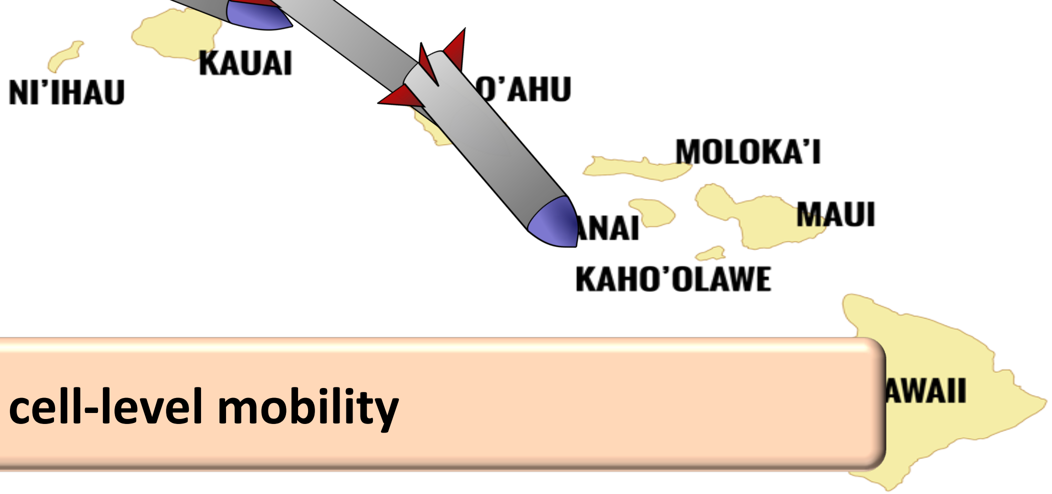
207220 paging messages (74 hours)

1 test device does not accept
16 paging records

Attack Impact

ToRPEDO enables paging ch[illegible]king and broadcasting fake emergency broadcast messages





ToRPEDO also enables profiling cell-level mobility

IMSI-Cracking is an alternative to Stingrays for both 4G and 5G networks enabling known attacks.

Conclusion

Analyzed and identified inherent design flaws and deployment oversights in 4G and 5G paging protocols

ToRPEDO (Location tracking), PIERCER (IMSI exposure), and IMSI-Cracking

Countermeasures for ToRPEDO

Zigbee Security Analysis

Zigbee Introduction

1. Zigbee is an **IEEE 802.15.4-based specification** for a suite of high-level communication protocols used to create personal area networks with small, low-power digital radios, such as for home automation, medical device data collection, and other low-power low-bandwidth needs, designed for small scale projects which need wireless connection. Hence, Zigbee is a low-power, low data rate, and close proximity (i.e., personal area) wireless ad hoc network. --(Wikipedia)

Zigbee Introduction -- History

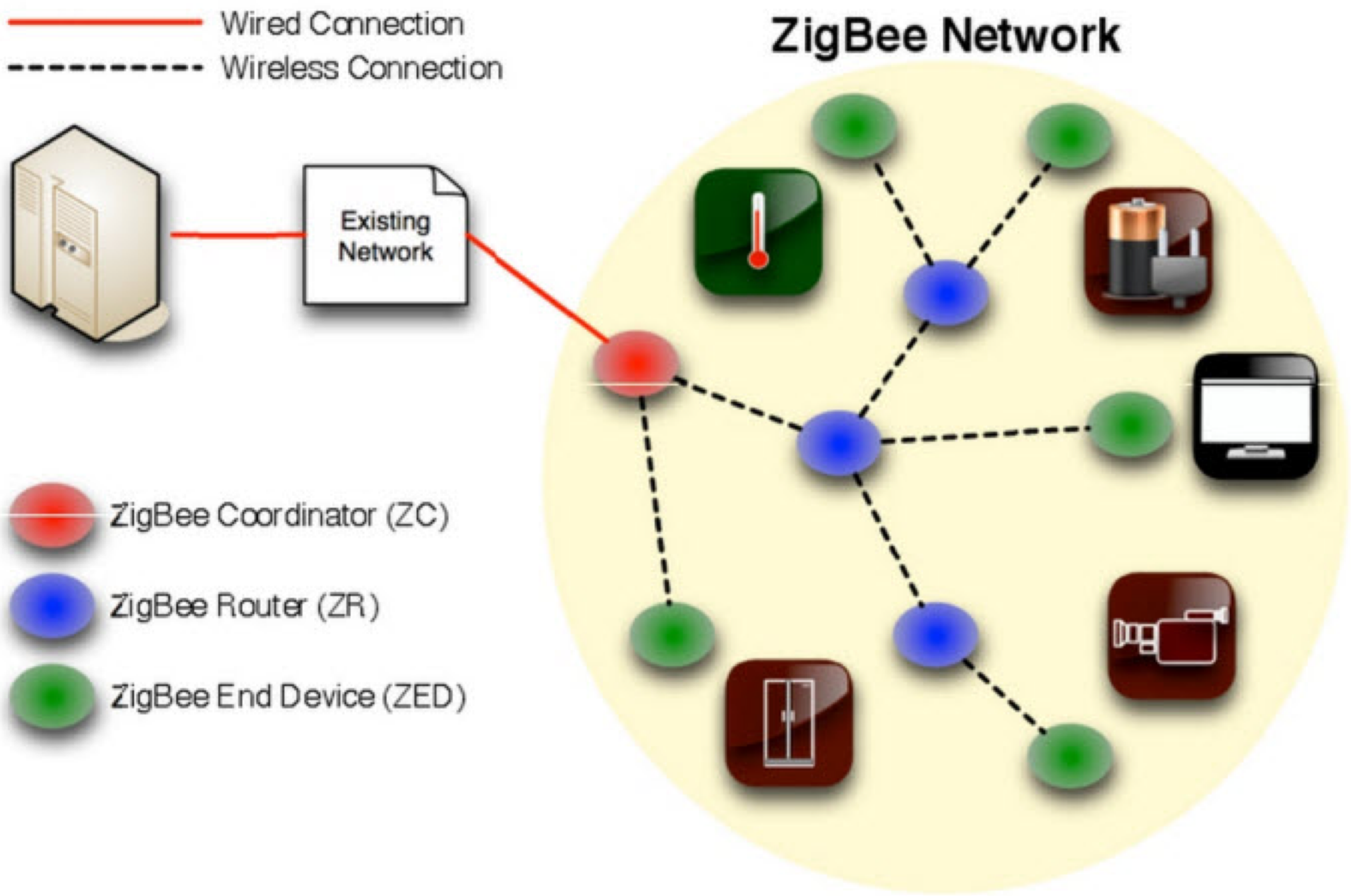
1. Zigbee V.1.0 2005.6
2. Zigbee V.1.1 2007.1
3. Zigbee V.1.2 2008.1

…

1. Zigbee PRO 2015
2. Zigbee 3.0 2017 (Latest version)

Zigbee devices

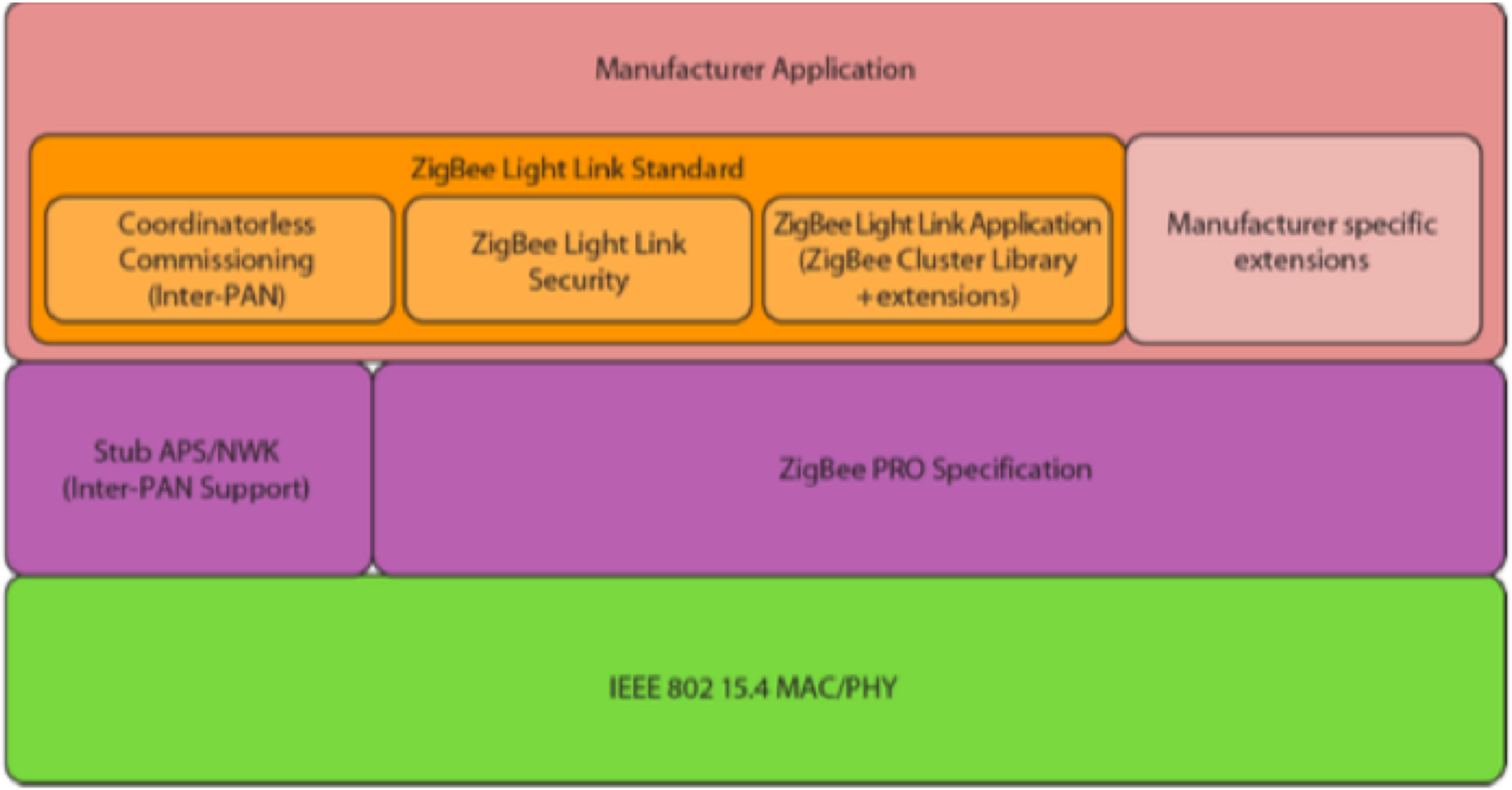
- ❑ Zigbee Coordinator (ZC): The Coordinator forms the root of the network tree and might bridge to other networks.
- ❑ Zigbee Router (ZR): Along with running an application function, a Router can act as an intermediate router, passing on data from other devices.
- ❑ Zigbee End Device (ZED): It contains just enough functionality to talk to the parent node (either the Coordinator or a Router).


Wired Connection
Wireless Connection
ZigBee Network
Existing Network
ZigBee Coordinator (ZC)
ZigBee Router (ZR)
ZigBee End Device (ZED)

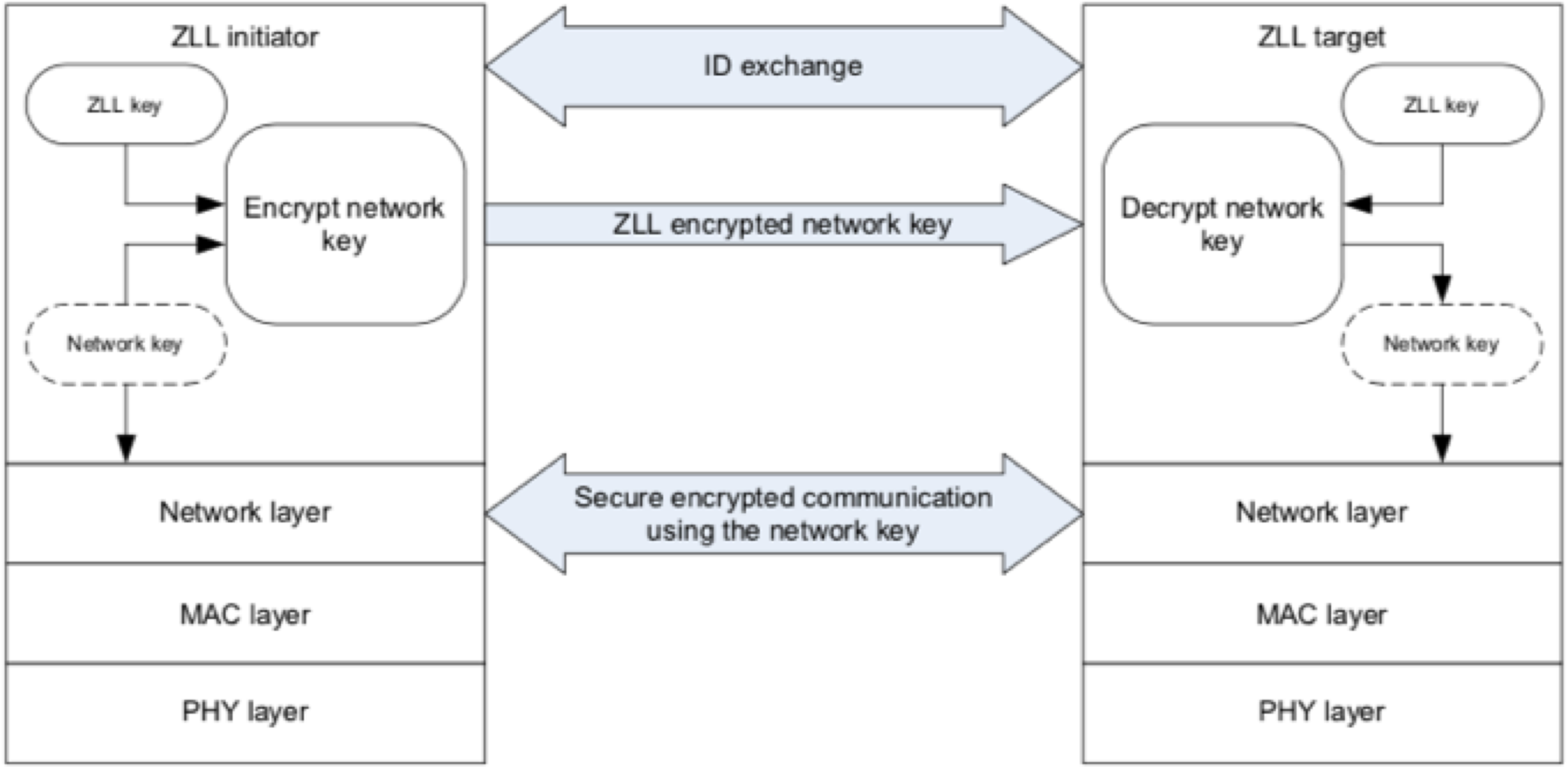
Zigbee protocols

1. Zigbee Smart Energy 2.0
2. Smart Energy 1.3 (not released)
3. Smart Energy 1.4
4. **Light Link 1.1**
5. **Home Automation 1.3**
6. Smart Energy 1.1b
7. Telecommunication Services 1.0
8. Health Care 1.0
9. RF4CE – Remote Control 1.0
10. RF4CE – Input Device 1.0
11. Remote Control 2.0

Zigbee Protocol ZLL



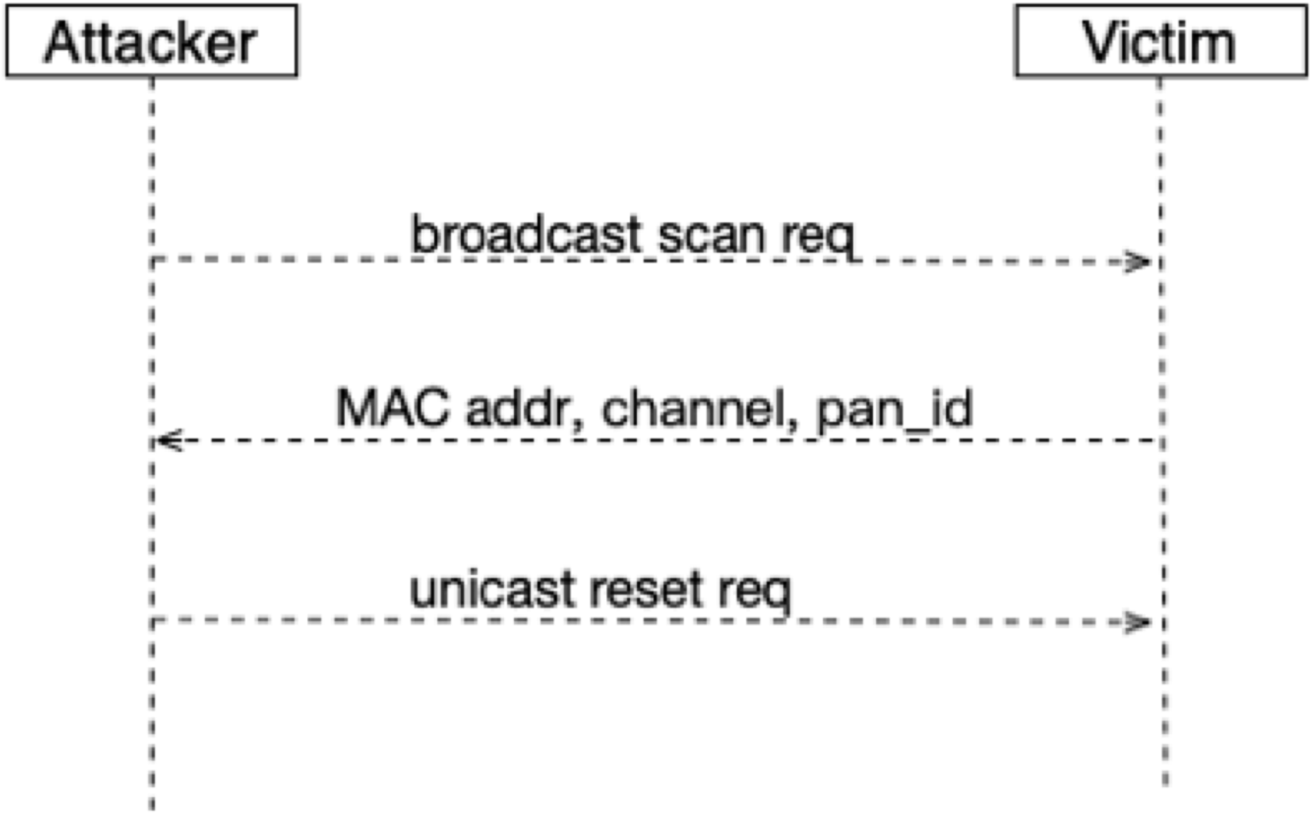
ZLL Security Overview



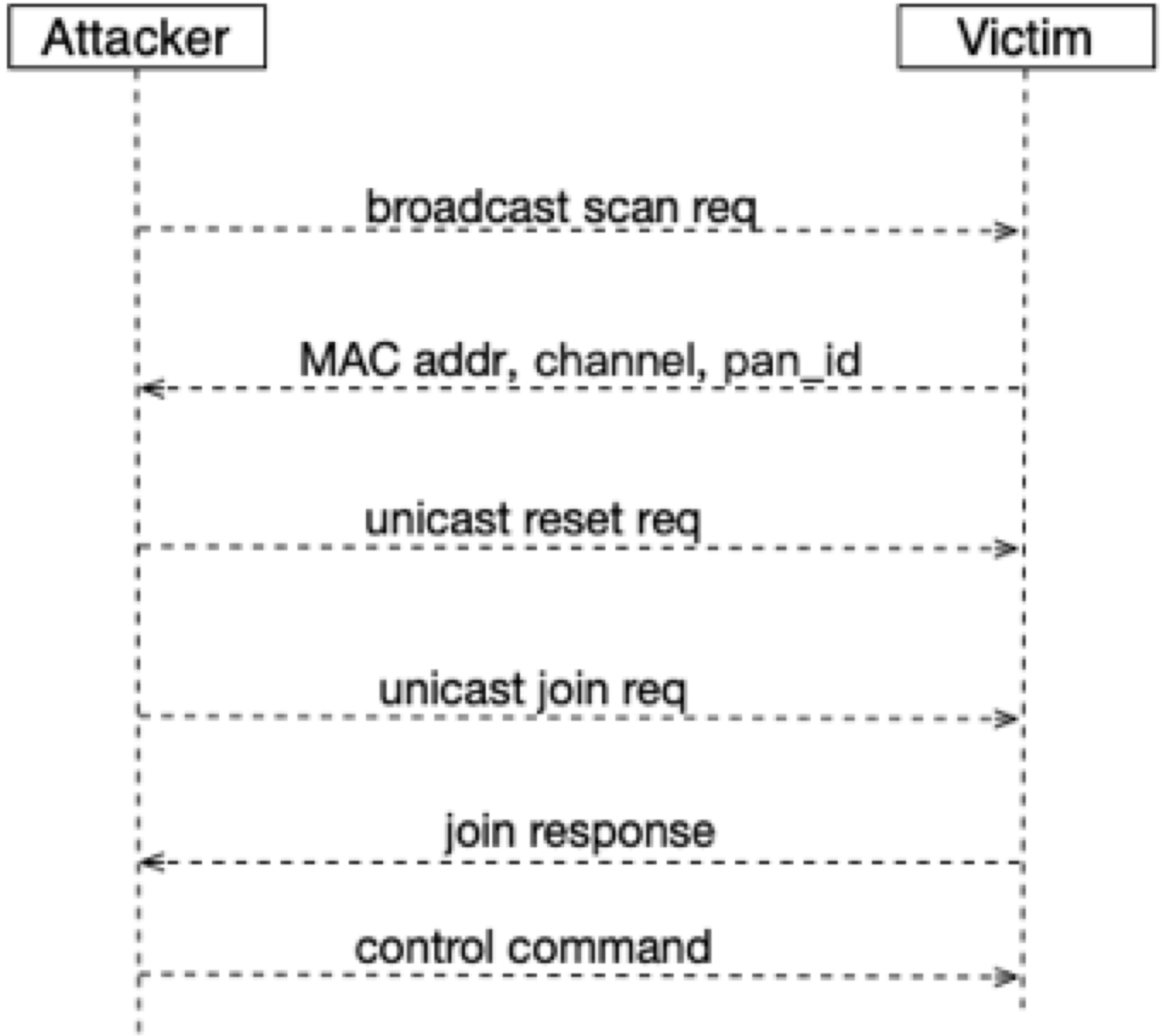
ZLL Testbed Setup with Z3Sec

- Z3Sec: https://github.com/IoTsec/Z3sec
- Z3Sec uses python to set a connection with USRP via GNURadio to send and receive packets out.
- Z3sec supports ZLL protocol and has power to do some attacks

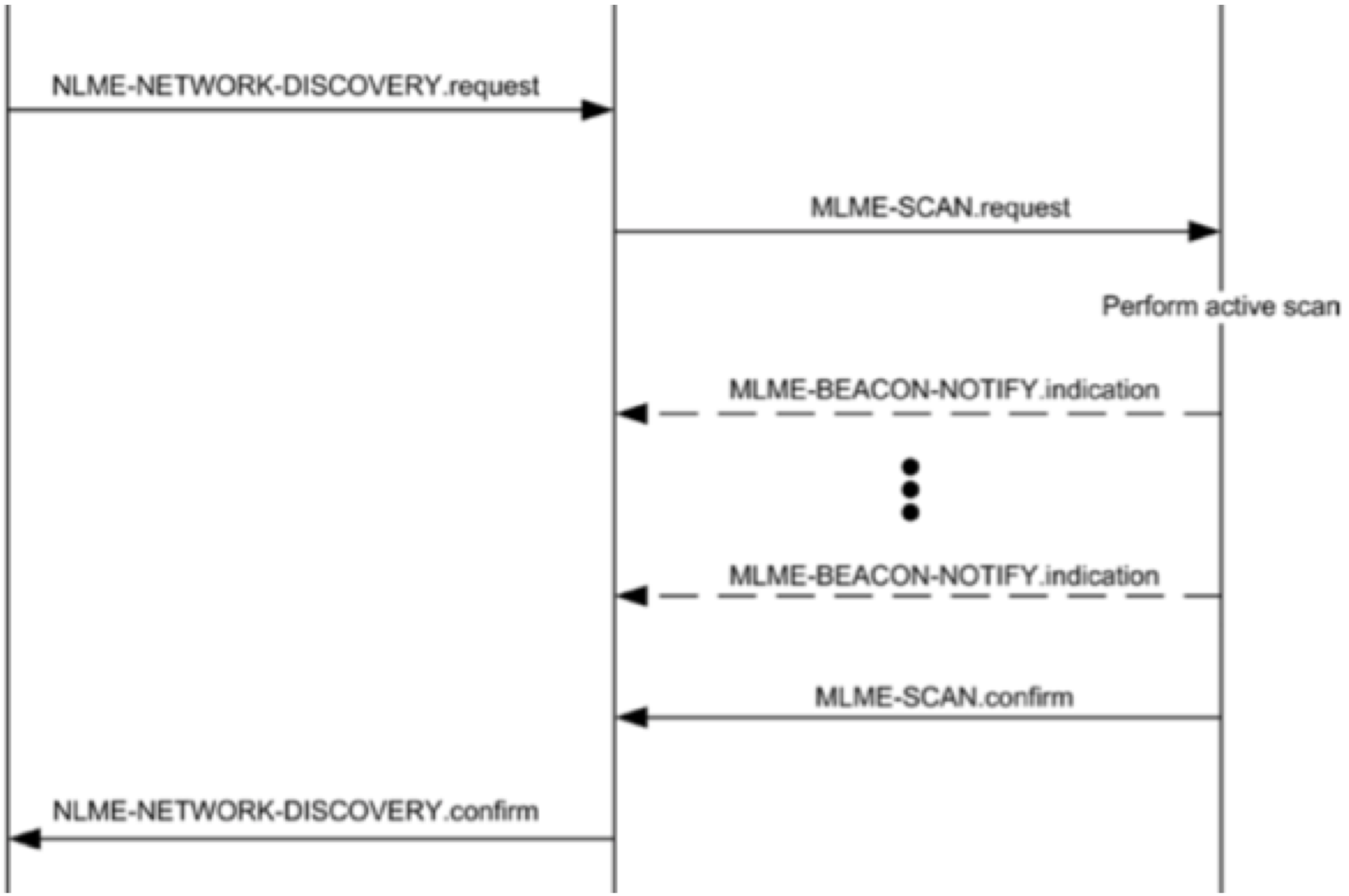
ZLL Attack: Reset the Victim from an Connected Network



ZLL Attack: Overtake attack



Overview of Zigbee Home Automation



Overview of Zigbee Home Automation (Cont.)

Zigbee Home Automation: Network Key Extraction

Key Transport message (Encrypted with Master key)

w

Expression...

No.	Source	Destination	Protocol	Length	Time	Info
199	0x7ee6	0x0000	ZigBee	51	60.351496	Update Device
200			IEEE 802.15.4	5	60.352015	Ack
201	0x0000	0x7ee6	ZigBee	102	60.363576	Transport Key
202			IEEE 802.15.4	5	60.363926	Ack
203	0x7ee6	0x0cf2	ZigBee	73	60.382226	Transport Key
204			IEEE 802.15.4	5	60.382564	Ack

```
▶ Frame 201: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
▶ IEEE 802.15.4 Data, Dst: 0x7ee6, Src: 0x0000
▶ ZigBee Network Layer Data, Dst: 0x7ee6, Src: 0x0000
▼ ZigBee Application Support Layer Command
    ▶ Frame Control Field: Command (0x01)
      Counter: 138
    ▶ Command Frame: Tunnel
▼ ZigBee Application Support Layer Command
    ▶ Frame Control Field: Command (0x21)
      Counter: 139
    ▶ ZigBee Security Header
    ▼ Command Frame: Transport Key
        Command Identifier: Transport Key (0x05)
        Key Type: Standard Network Key (0x01)
        Key: f54be187c20fed0fda1fb43f016f09ce
        Sequence Number: 0
        Extended Destination: Smartthi_00:01:09:56:da (24:fd:5b:00:01:09:56:da)
        Extended Source: Smartthi_00:00:04:96:ab (24:fd:5b:00:00:04:96:ab)
```

Our Current Research Directions

1. Extract finite state machine of Home Automation protocol and perform systematic analysis on the protocol

2. Identify critical flaws in crypto design/implementations.

State Machine Extraction and Formal Verification

Zigbee protocol design may have some flaws that may leads to unexpected states.

Our work:

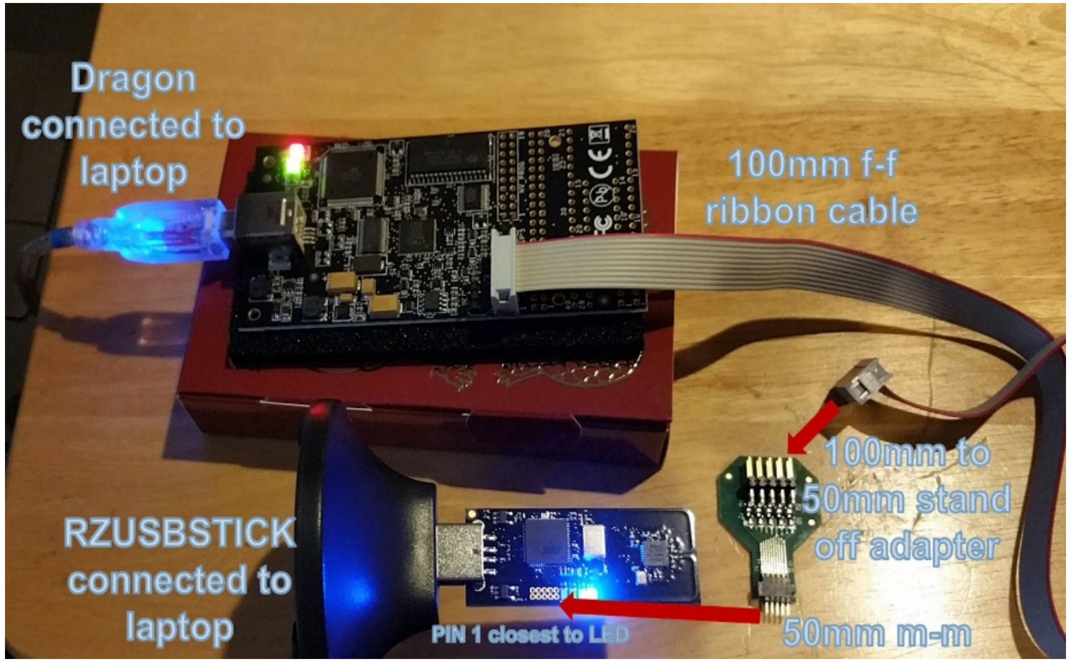
1. Extract state machine from the specification.
2. Extract the security and privacy properties from the security requirements.
3. Apply model checking and find the counter-examples/violations of the tested properties
4. Use a testbed setup with real devices to confirm the counter-examples.

Identify critical flaws in crypto implementations.

- Zigbee implementations may have deeply rooted vulnerabilities in the key exchange, message encryption/decryption and message authentication/verification implementations. Our focus is to identify them with principled approaches.

Involvement of High School Student

- Isaac Lammers (rising senior at Jefferson High School)
- Enrolled in high school's 2-semester Science Research course during the 2018-2019 year
- Worked on Zigbee security
  - Demonstrate the ability for attacker to gain control of light bulbs



Isaac Lammers's Project

- 1st place in the Purdue science fair
- The Intel Excellence in CS Award
- Yale Mathematics and CS Award
- Air Force Intelligence Award,
- Indiana state fair, winner of the CS category