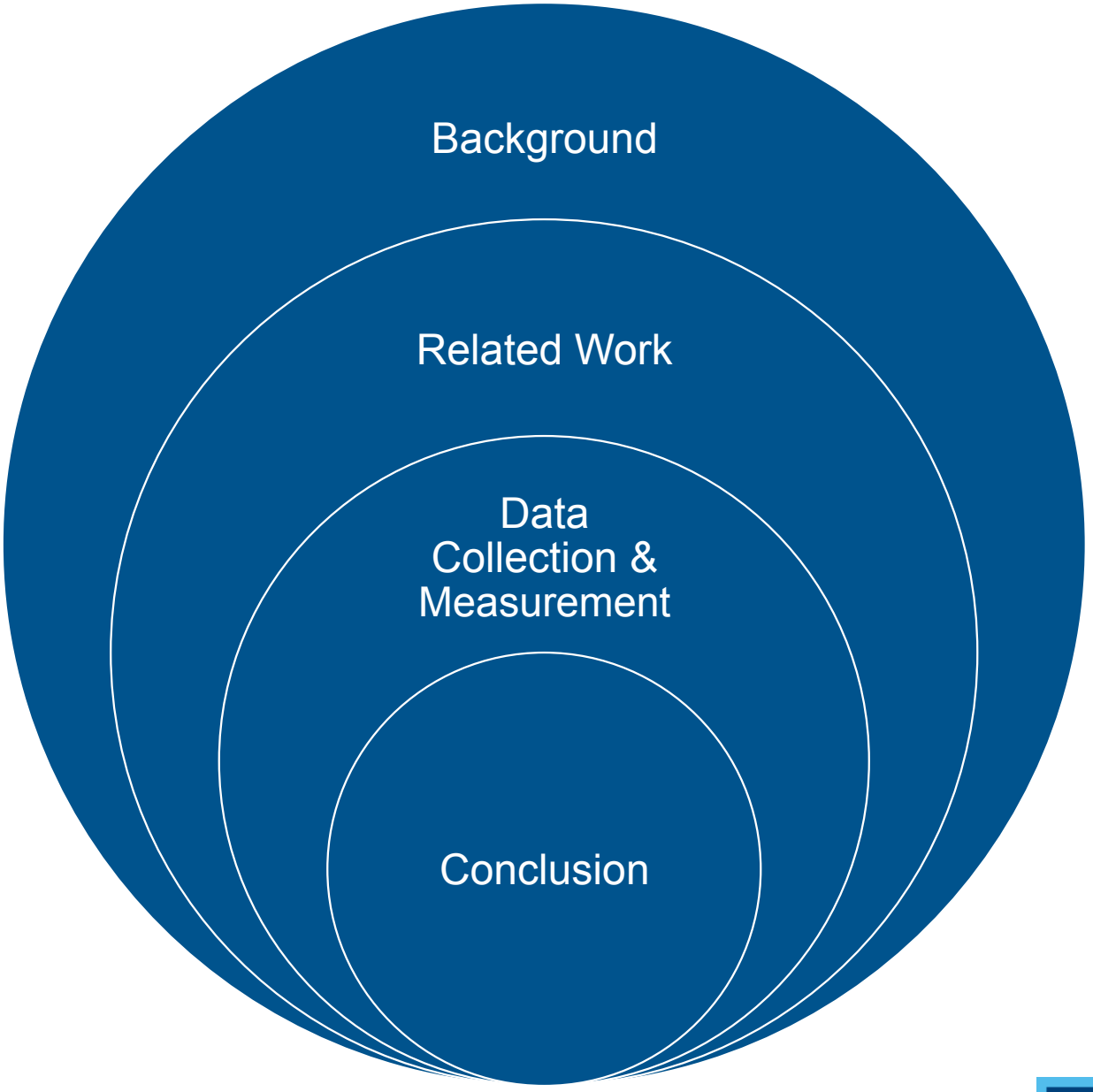
KU LEUVEN

Characterizing Wi-Fi Network Discovery

Student: Yun-Chih Joy Chou
Supervisors: Gunes Acar, Rafael Galvez
Promotor: Claudia Diaz

26/06/17


Background
Related Work
Data
Collection &
Measurement
Conclusion

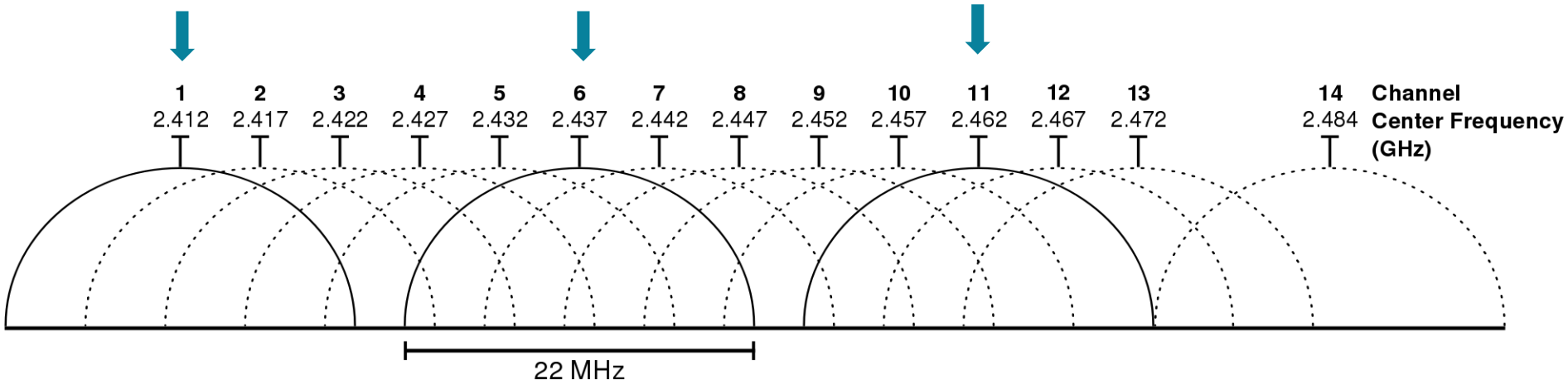
KU LEUVEN

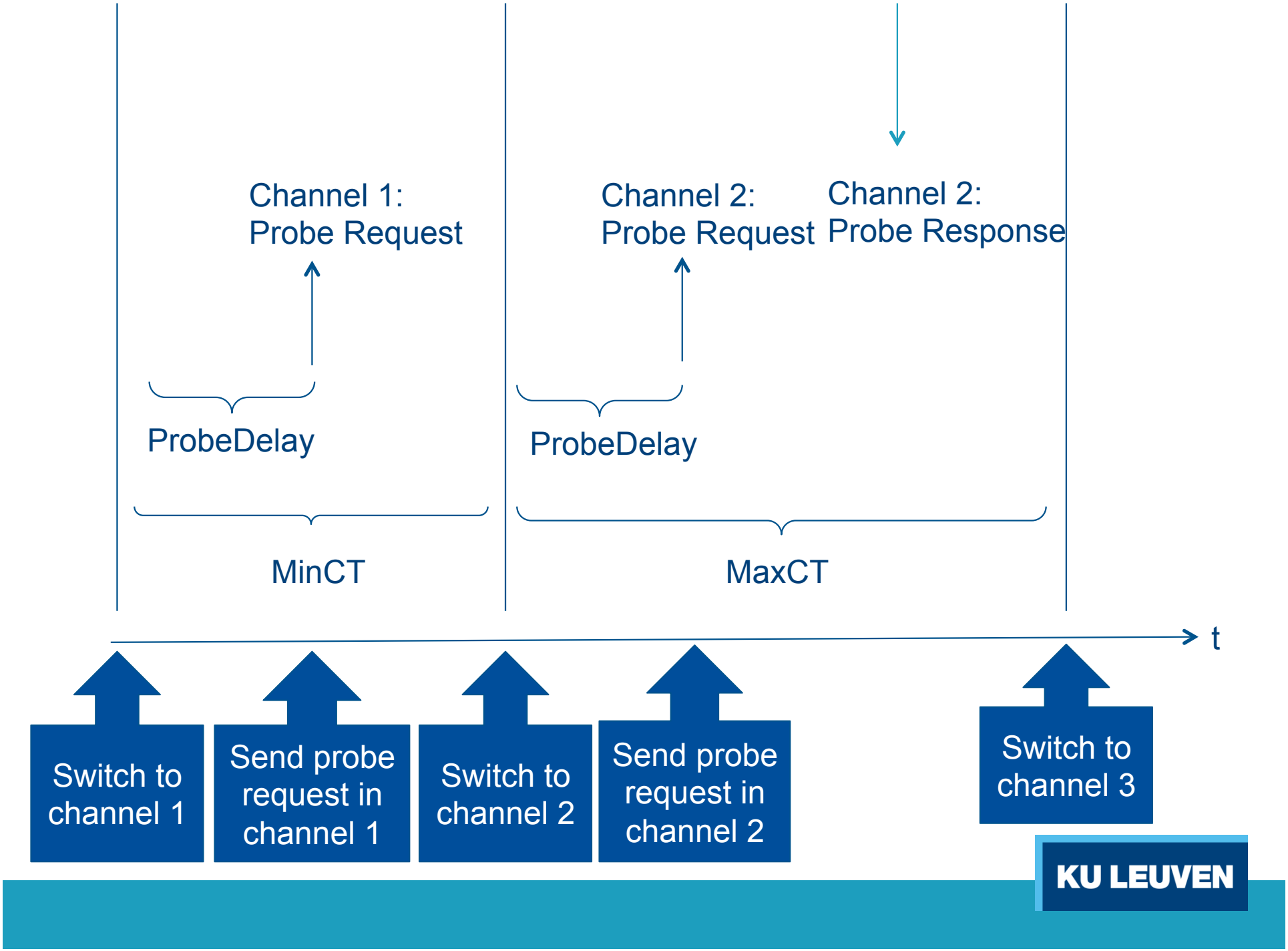
Introduction

- Wi-Fi standard: IEEE 802.11.
- Network discovery – scanning.

Fig. Scanning Scenario

Channels: 2.4 GHz




Channel 1:
Probe Request
Channel 2:
Probe Request
Channel 2:
Probe Response
ProbeDelay
ProbeDelay
MinCT
MaxCT
t
Switch to channel 1
Send probe request in channel 1
Switch to channel 2
Send probe request in channel 2
Switch to channel 3
KU LEUVEN

IEEE 802.11: MLME-SCAN.request

- MAC Layer Management Entity (MLME) primitive parameters for the request to scan: 16 parameters in the 2016 protocol.

- ProbeDelay
- MinChannelTime
- MaxChannelTime
- Service Set Identifier (SSID) : The name of the network. Ex. ‘eduroam’

IEEE 802.11: Probe Request Frame (PRF)

- PRF: Contain the information to join the network.
- Sequence Number (SN).
- Contain MAC address of the device.

Source	Destination	Protocol	Length	Subtyp	Signal strength (dBm)	Current Channel	SSID	Info
Apple_b6:18:00	Broadcast	802.11	166	4	-39	13		Probe Request, SN=454,
Apple_70:78:0a	Broadcast	802.11	123	4	-84	11		Probe Request, SN=3210,
Apple_70:78:0a	Broadcast	802.11	123	4	-85	12		Probe Request, SN=3214,
SamsungE_31:24:e7	Broadcast	802.11	163	4	-87	11	eduroam	Probe Request, SN=3416,
SamsungE_31:24:e7	Broadcast	802.11	163	4	-87	11	eduroam	Probe Request, SN=3417,
LiteonTe_17:f2:fc	Broadcast	802.11	90	4	-86		students	Probe Request, SN=1509,
LiteonTe_17:f2:fc	Broadcast	802.11	90	4	-87		students	Probe Request, SN=1541,
LiteonTe_17:f2:fc	Broadcast	802.11	90	4	-91		students	Probe Request, SN=1542,

Fig. Probe request frames displayed in Wireshark

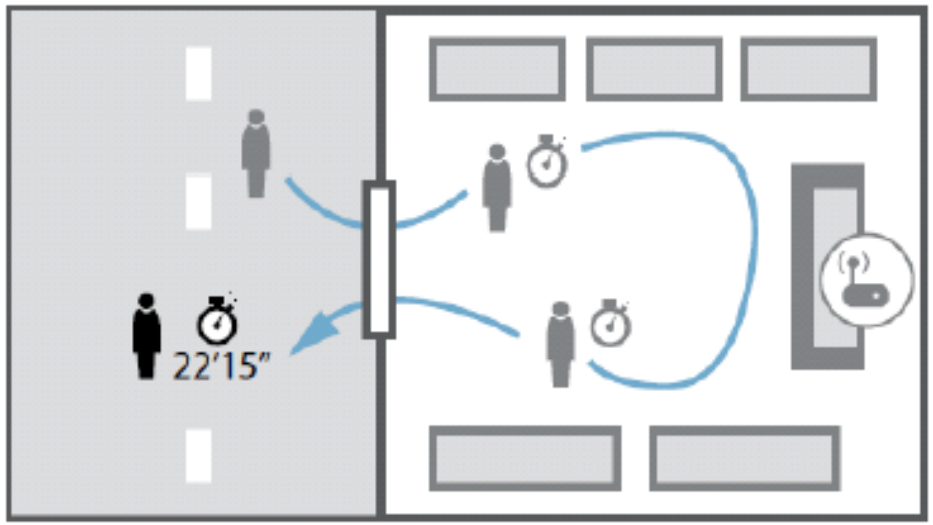
Privacy concerns

PRF is sent in clear text : Contain MAC address and even SSIDs of previously connected networks

Adversary model: Passive network adversary.

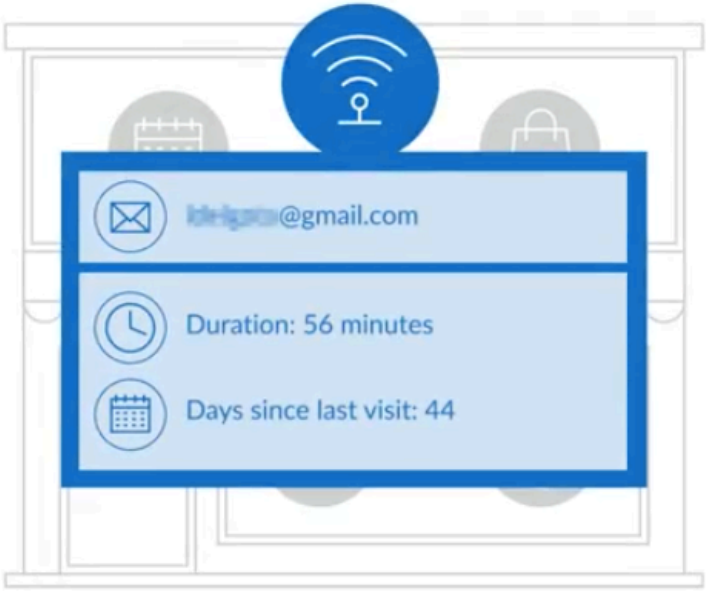
It can be exploited without the users' knowledge.

PRF Application: Positioning (Cheng, 2005), tracking (Musa, 2012), infer social relationship of two persons (Cunche, 2014), customer profiling (Soltani 2014), identify devices (Gentry, 2016) etc.



Euclid analytics

MARY SMITH



KU LEUVEN

Related Work: MAC Randomization Reversal

- Devices can be fingerprinted by combining MAC with the parameters in the PRF and the SN of the frames. Some devices use real MAC when connected to AP (Vanhoef et al., 2016) (Robyns et al., 2017).
- Successful reversal among a dataset of 2.6 million addresses. At least three ways to retrieve the global MAC (Martin et al., 2017).

Related Work

Characterization:

- Early study to characterize the Wi-Fi scanning (Gupta et al., 2007).
  - Channel on which the first PRF is sent.
  - Number of PRFs transmitted per channel.
  - Delays between PRFs on the same channel.
  - Frequency and order of the channels probed.
- Compare the number of probe requests sent by different devices under different conditions (Freudiger et al., 2015).

Related Work

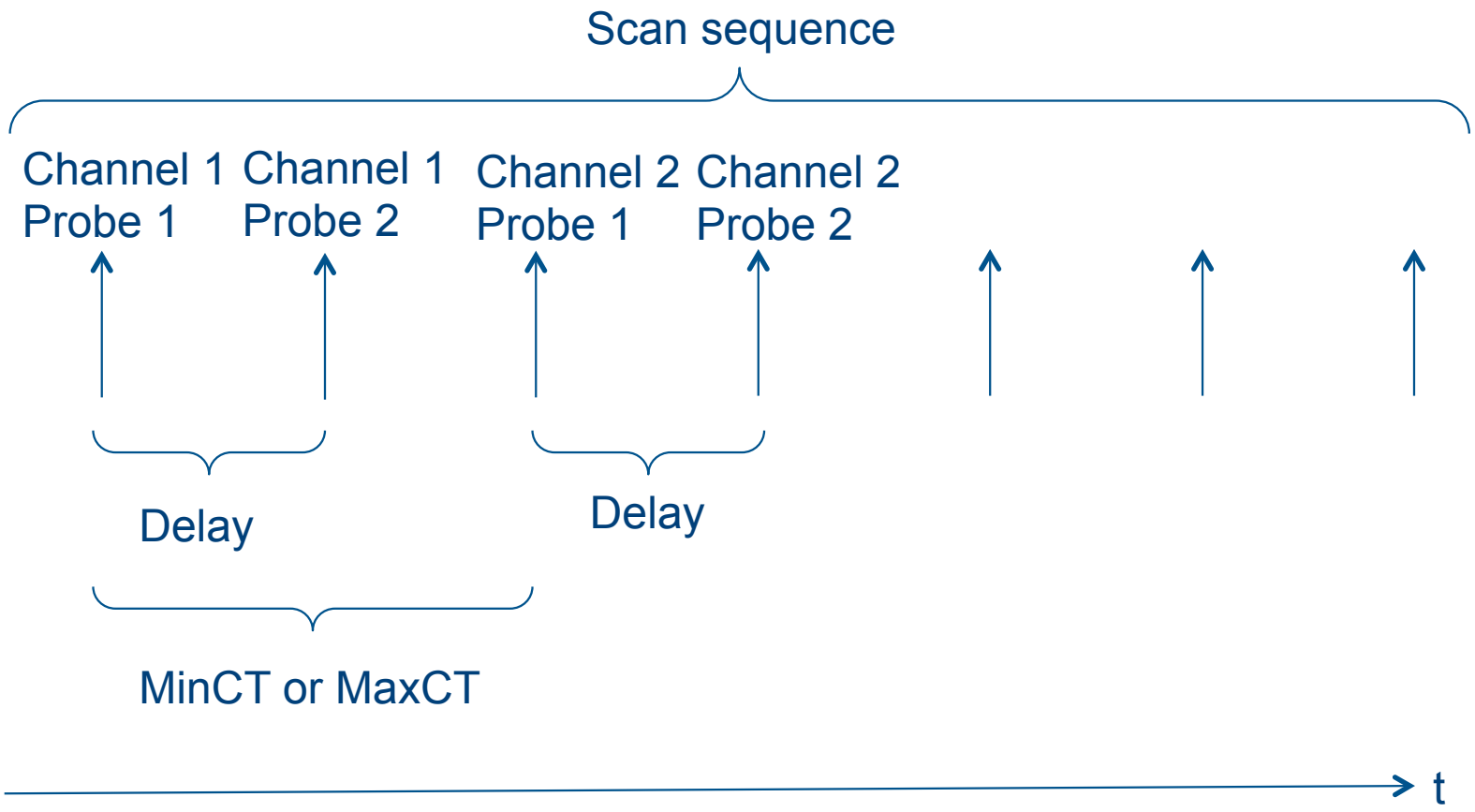
- Optimization:
  - Scan only when moving beyond 10m (Wu et al., 2009) or when known AP is around (Kim et al., 2014).
  - Change MinCT/MaxCT adaptively based on AP availability (Castignani et al., 2011).
  - Modify scanning sequence to do priority scanning (Goovearts et al, 2017).

Objectives

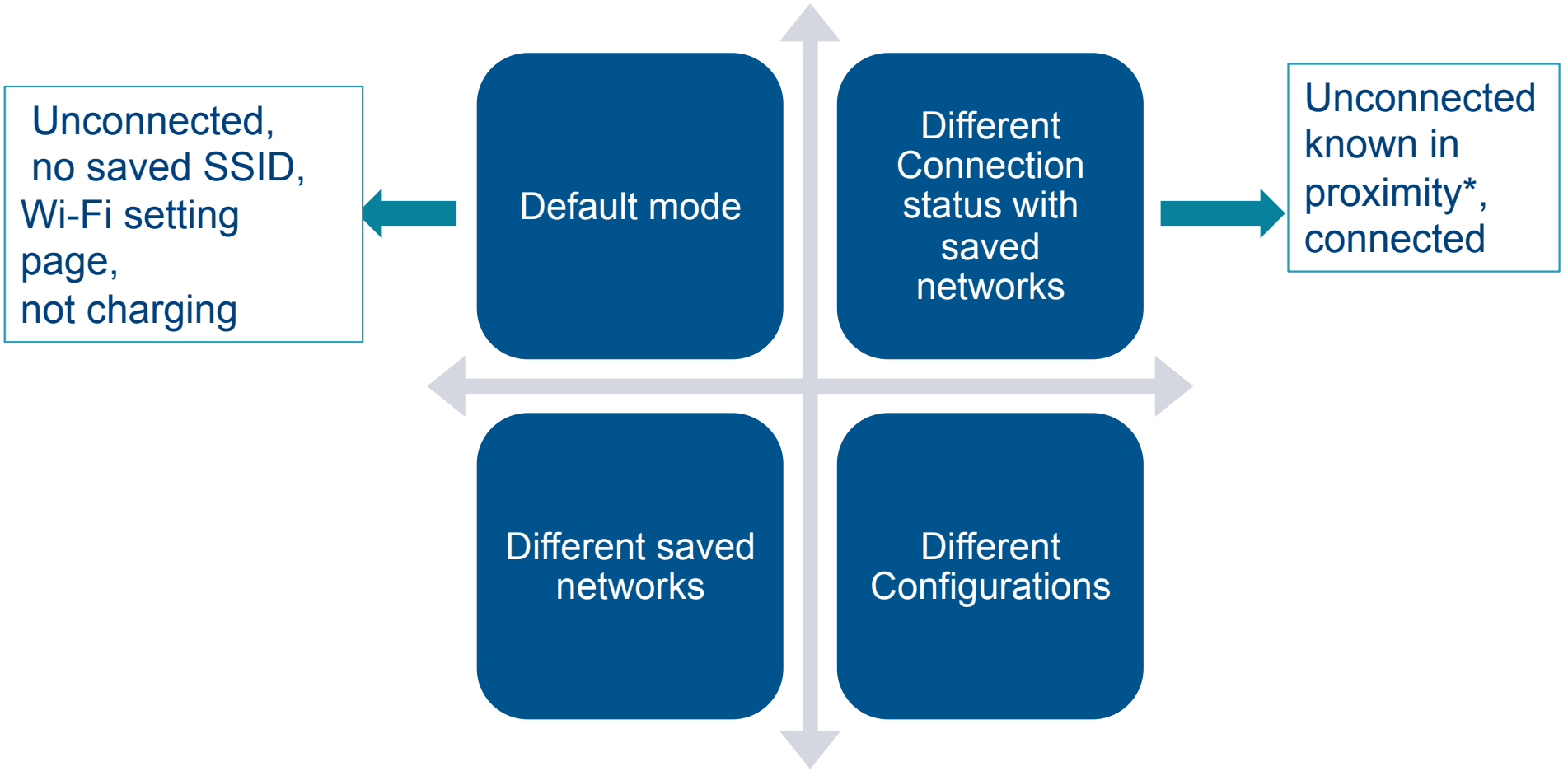
- Characterization: Know how stations scan on top of the standard.

- Improvements/ recommendation to the current scanning method to defend possible attacks.

Characterization Parameters



Test Scenarios



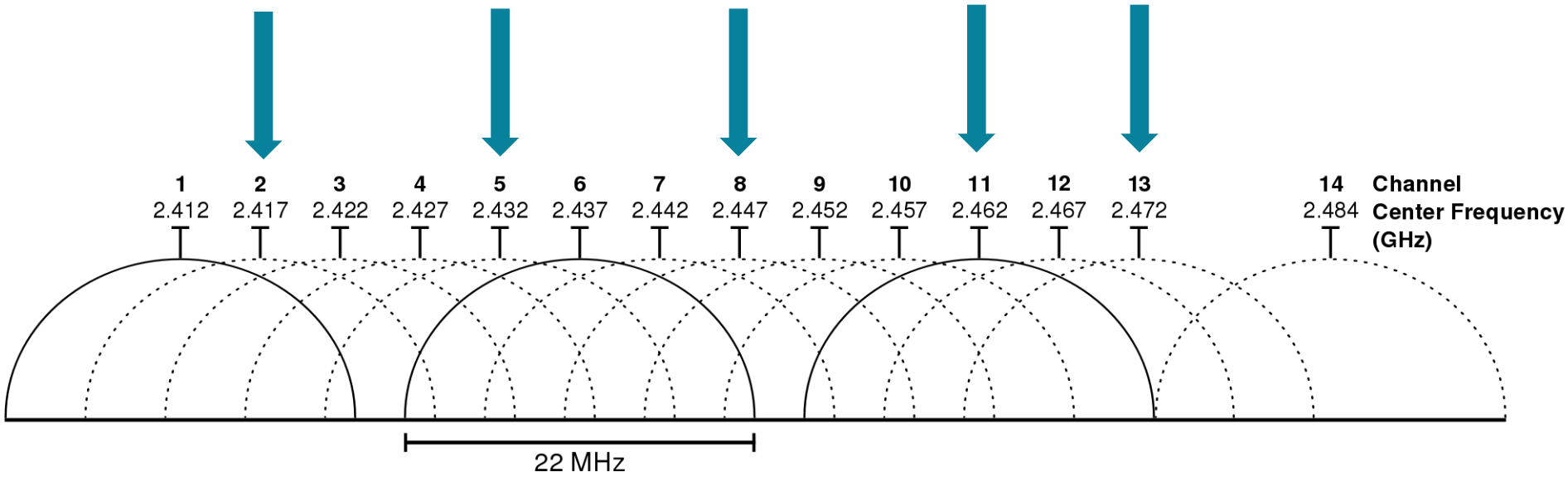
Experimental setup

- 2.4 GHz Setup: A Linux pc + USB hub + 5 antennas

KU LEUVEN

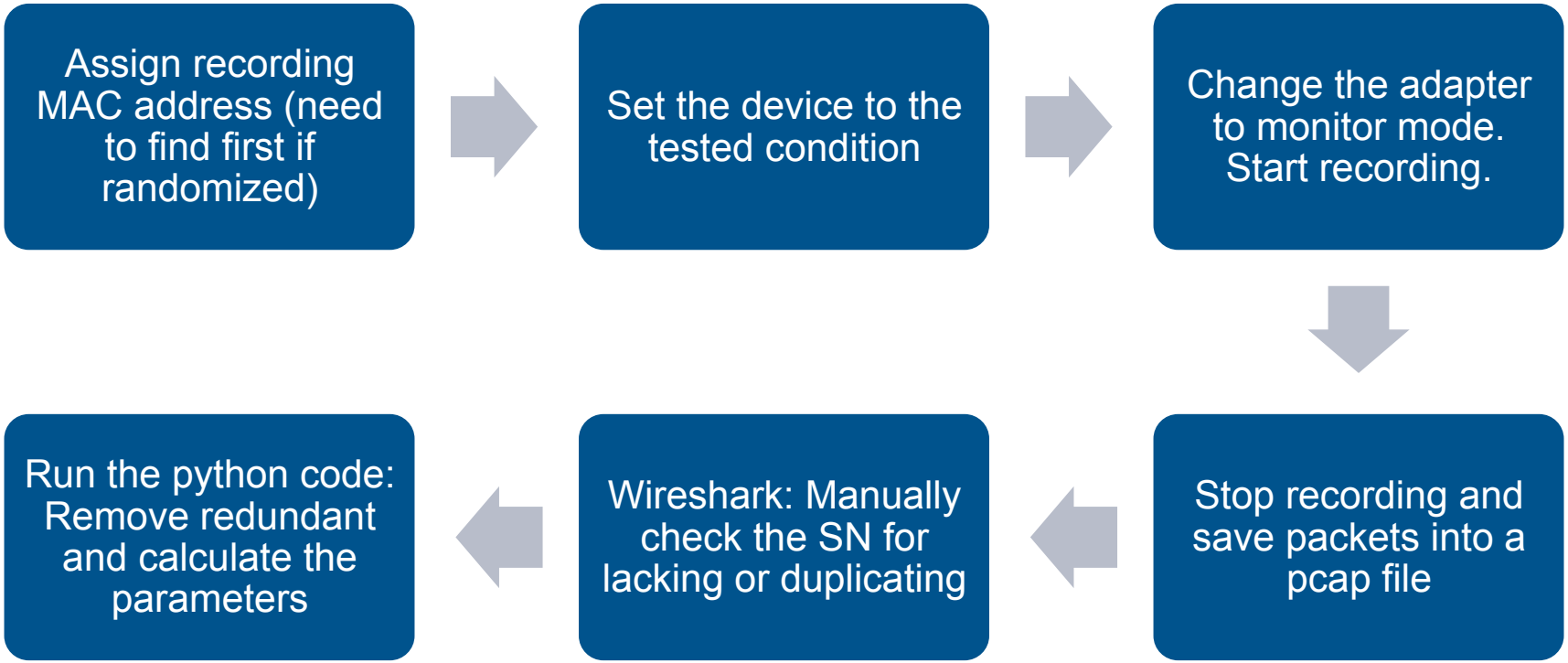
Scanning Frequencies

- 2.4 GHz band: 5 antennas for 13 channels.
- 5 GHz band: One antenna per channel.



KU LEUVEN

Process Flow



KU LEUVEN

The Devices tested

iPhone 6s Plus
5,5-inch display
iOS 10.2.1

MacOS 10.12.4

KU LEUVEN

Test Scenario - The Default Mode

- Result: Diversity, devices scan differently.
- Mostly: MinCT = MaxCT
- Preliminary: 5G channels follow 2.4GHz band.

Devices	Version	Scan Sequence	1st PRF	PRF /channel	Interprobe Delay (ms)	MinCT (ms)	MaxCT (ms)
Linux	14.04	1,2,3...11	1	2	18.6 ± 1.2	40.5 ± 1.5	39.9 ± 1
Linux	16.04	1,2,3...13	1	1	n	24.2 ± 0.6	24.3 ± 0.6
Windows	10	1,2,3...13	1	1	n	24.2 ± 0.4	105.6 ± 0.4
MacBook	10.12.4	1,2,3...13	1	2	21.2 ± 0.4	47.4 ± 2.8	53.1 ± 7.5
iPhone	10.2.1	1,2,3...13	1	1	n	43.6 ± 0.5	43.6 ± 0.5
Samsung	4.1.2	1,2,3...13	1	2	41.6 ± 0.7	84.8 ± 1.0	84.9 ± 1.1

Test Scenario – Different Connection Status

- Result: Devices scan differently.

- Known in proximity: Most devices send a probe request with the SSID of the known AP in its channel.
- MacBook: Does priority scanning when not connected.
- iPhone: Most irregular behavior (even double probes).

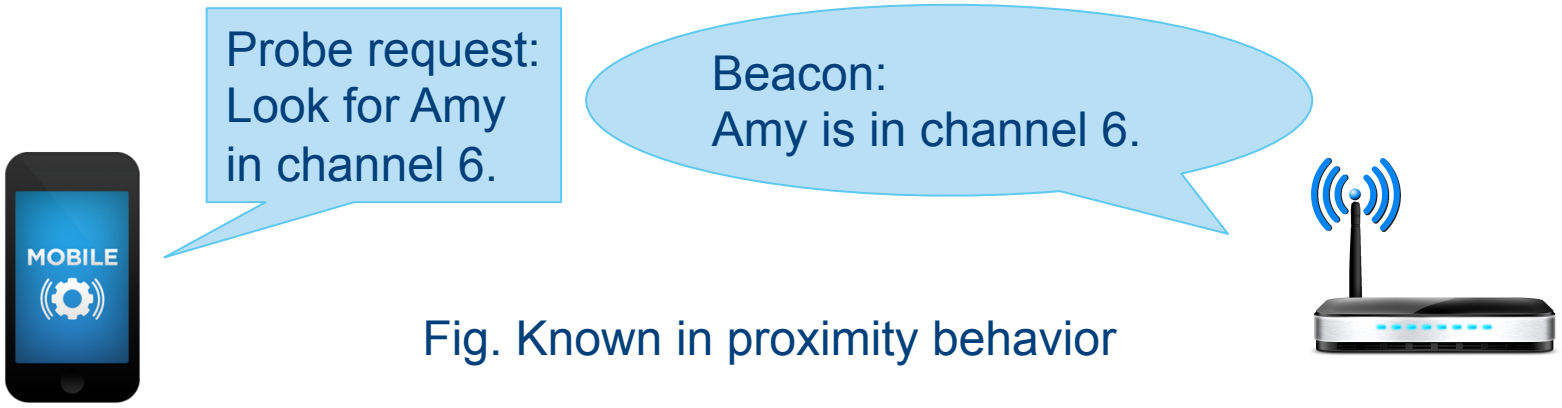


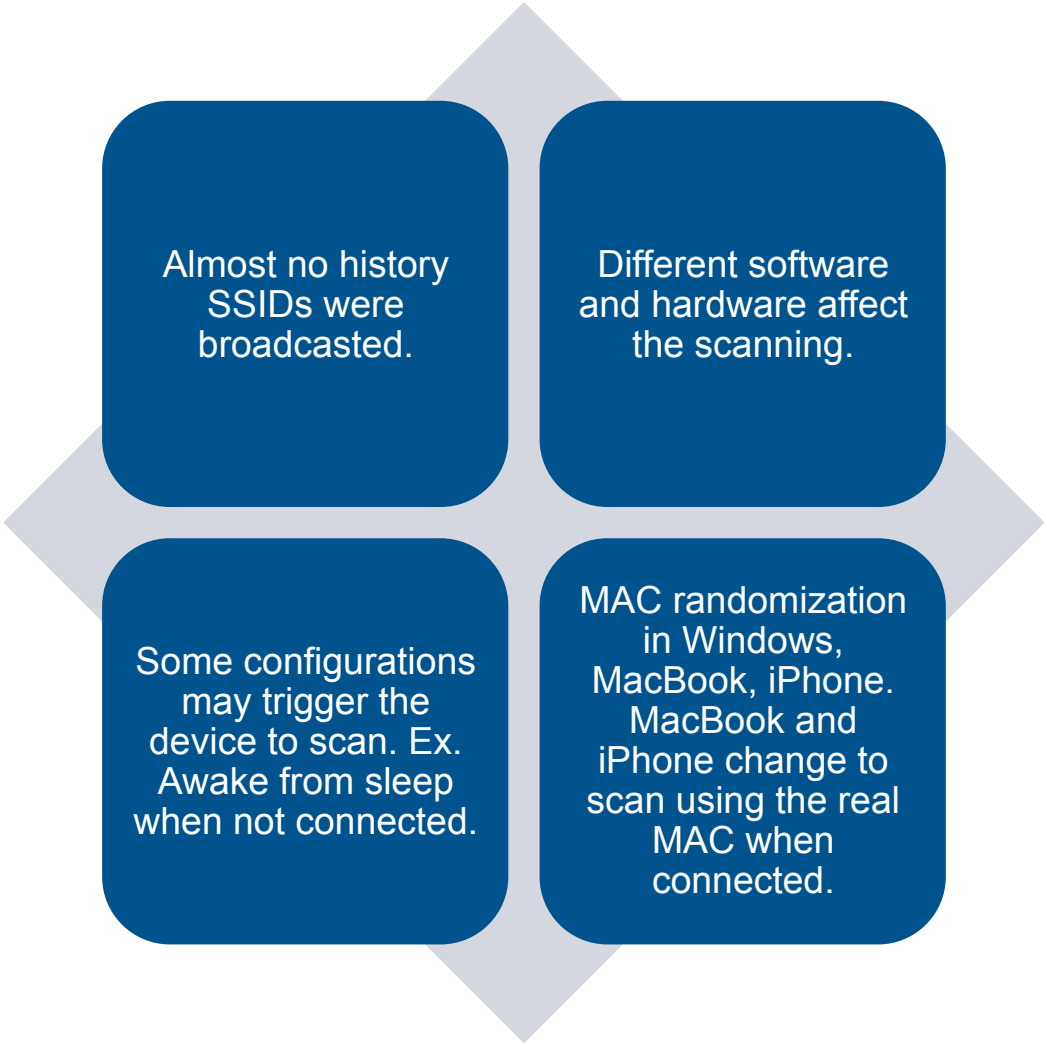
Fig. Known in proximity behavior

Test Scenario – Saved SSIDs

- Result: MacBook Priority scanning

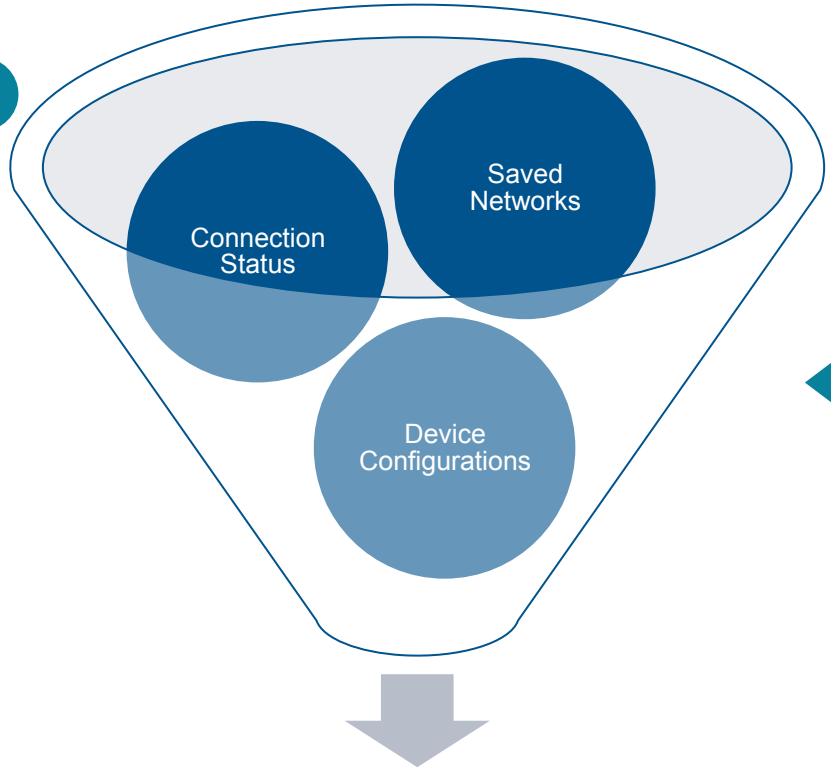
Scan channel 6 first, then 3,10,11,12, then other channels

Other findings



Conclusion

Characterized parameters:
MinCT/MaxCT
20-100ms,
1-2 PRF/Chan.
Default scan from channel 1
…



MacBook:
Priority Scan

Unique scanning behavior

KU LEUVEN

KU LEUVEN

Thank you very much