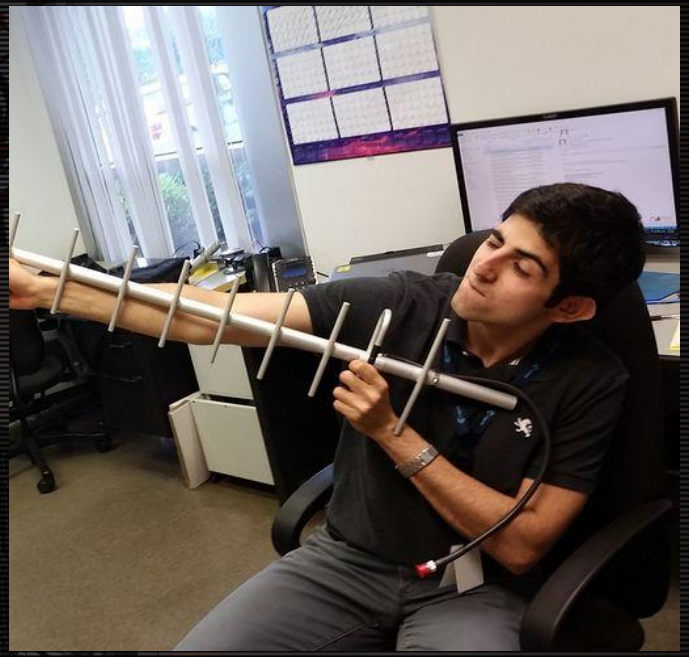
Reza Soosahabi, Chuck McAuley
Application & Threat Intelligence Research Center

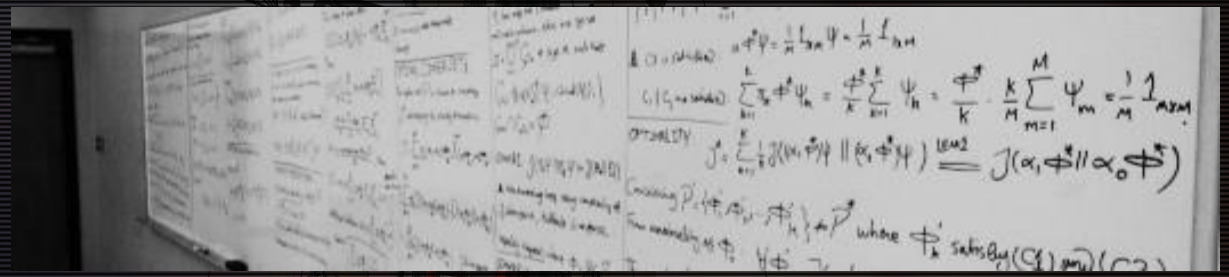
SPARR😈W: A Novel Covert Communication Scheme Exploiting Broadcast Signals in LTE, 5G & Beyond

KEYSIGHT TECHNOLOGIES

WHO

KEYSIGHT TECHNOLOGIES





APPLICATION & THREAT INTELLIGENCE
RESEARCH CENTER
KEYSIGHT TECHNOLOGIES

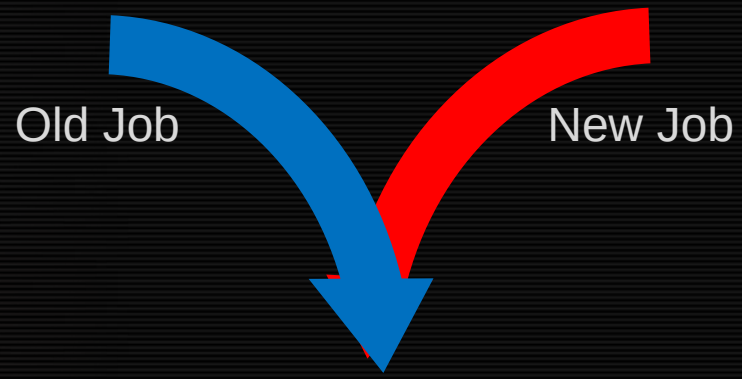
MOTIVATION

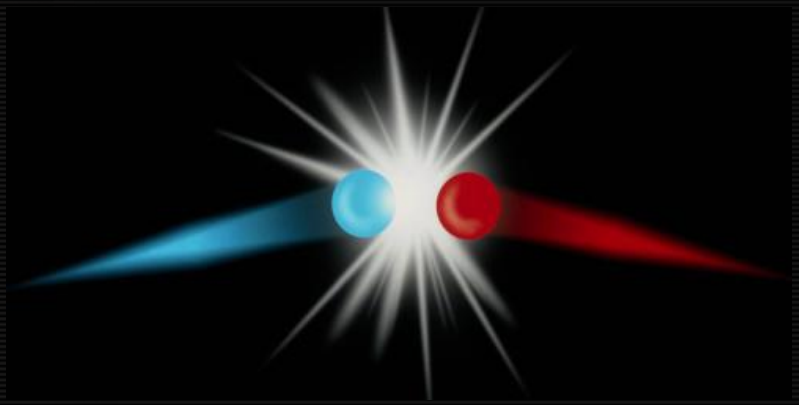
KEYSIGHT TECHNOLOGIES

Motivation

WHAT MADE ME DO IT!

- Past research experience in wireless security
- Worked with US operators before joining Keysight in 2018.
- Researched data exfiltration techniques at ATI that are lesser known in wireless community.
- Trying to impress a cool boss who drops a big money Base-Station emulator equipment on your lap to do open field research!
- The satellite talk in DEFCON 28
  - Whispers Among the Stars: Perpetrating (and Preventing) Satellite Eavesdropping Attacks – James Pavur



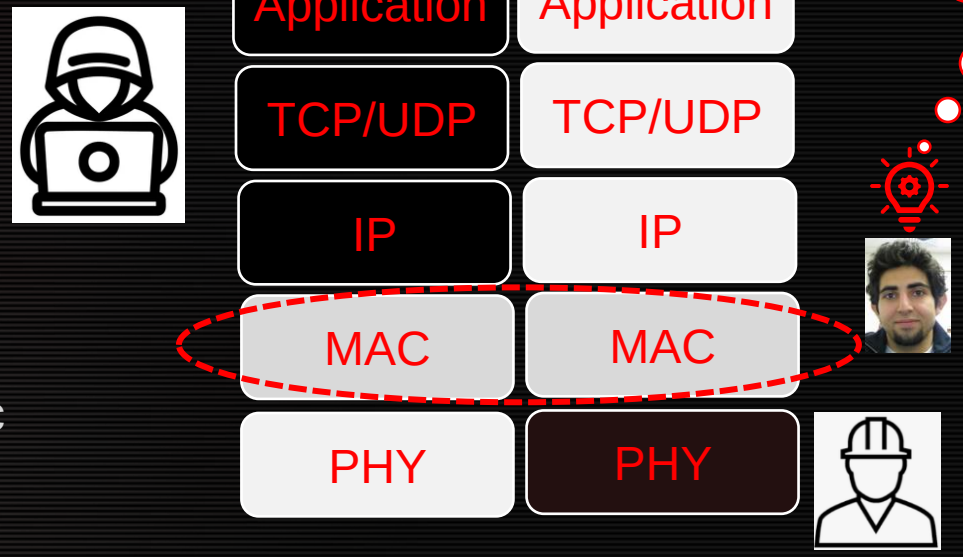


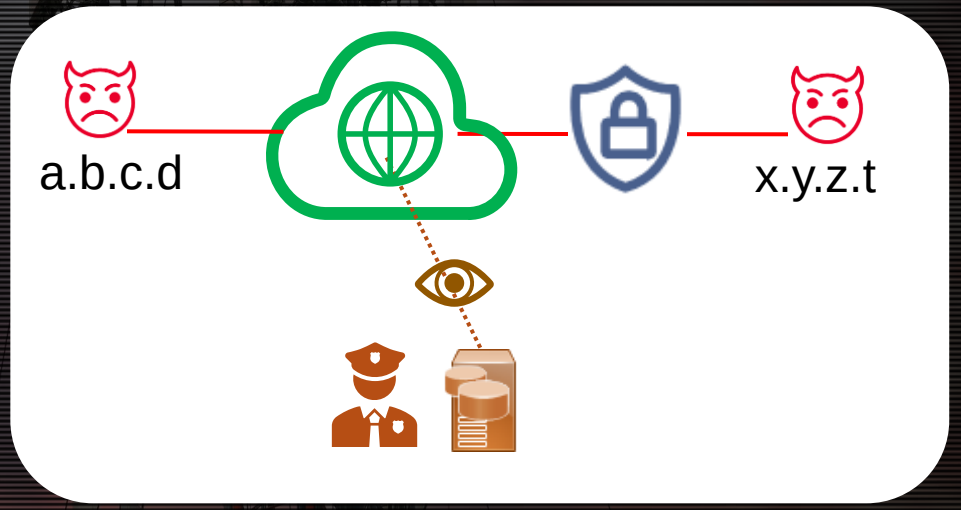
KEYSIGHT TECHNOLOGIES

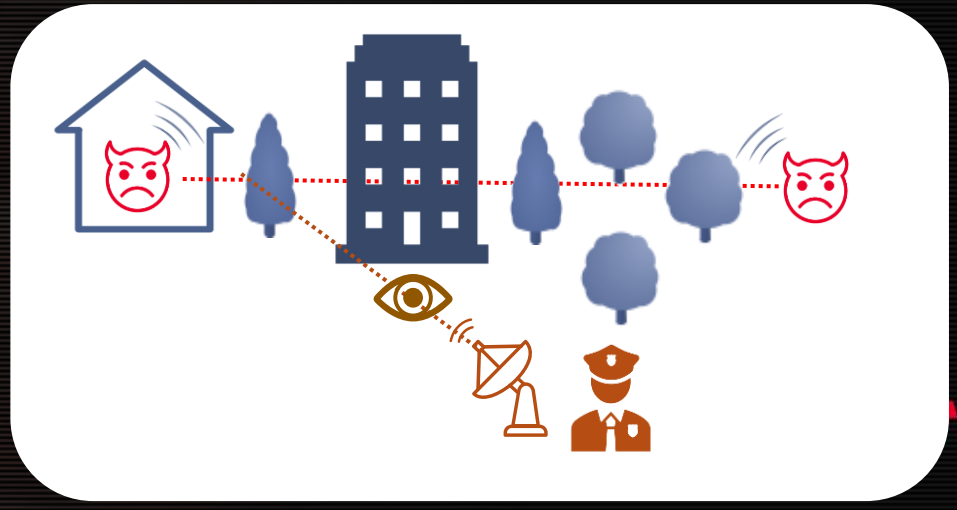
Motivation

FINDING MISSING PIECE

- Covert Communication: a potential threat
- **Hacker Mentality: Exploit [Software]**
  - Tunnelling via 3-7 protos: ICMP, DNS, etc
  - Challenged by Security Boxes: IPS, IDS, LI
- **Engineer Mentality: Build [Hardware]**
  - Building L1 (radios): Spread Spectrum, Ham Radios, etc
  - Signal blocking e.g. indoor to outdoor
  - Avoiding spectrum monitoring





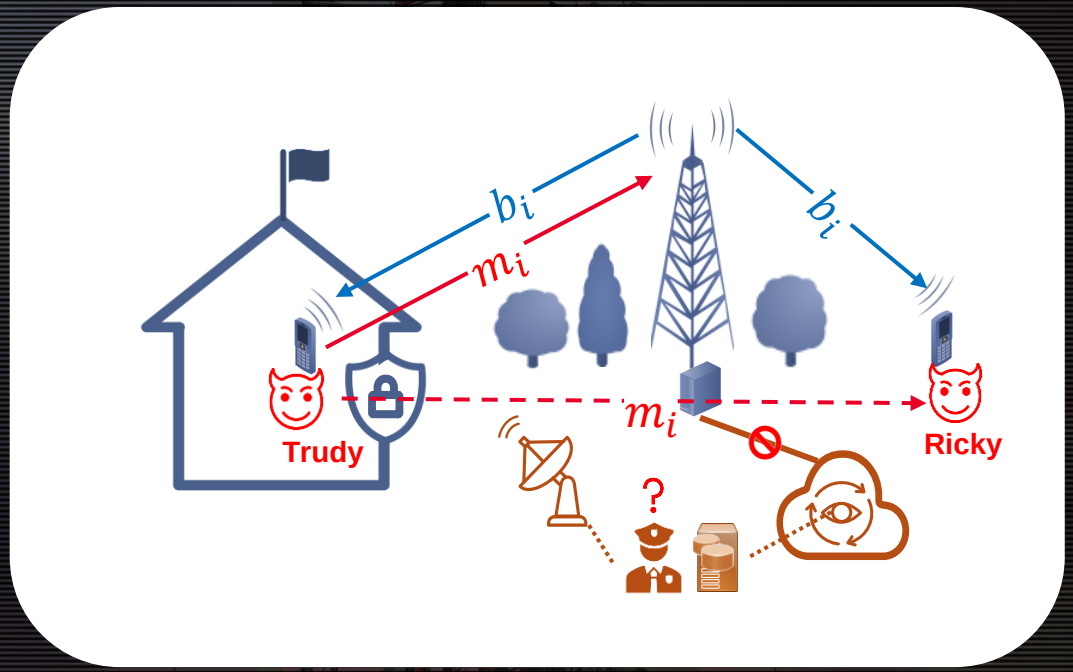


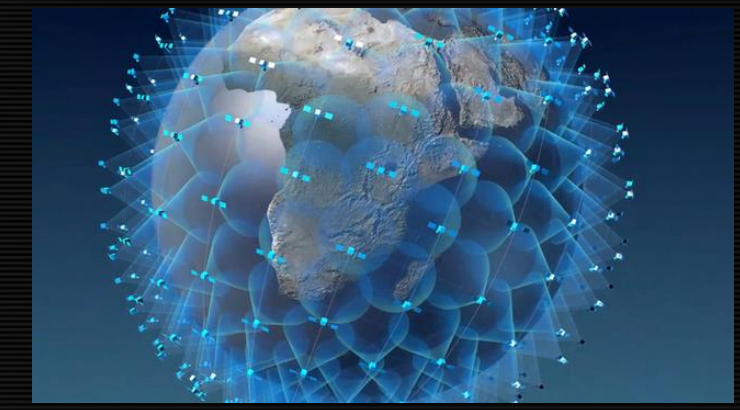
KEYSIGHT TECHNOLOGIES

Motivation

EXPLOITING ACCESS RADIOS

- Exploit MAC standard weakness in cellular & satellite, …
- Radio height makes RF signals unstoppable.
- What if: Trudy bounces a broadcast signal of from ANY powerful Wireless Access Node to Ricky!?





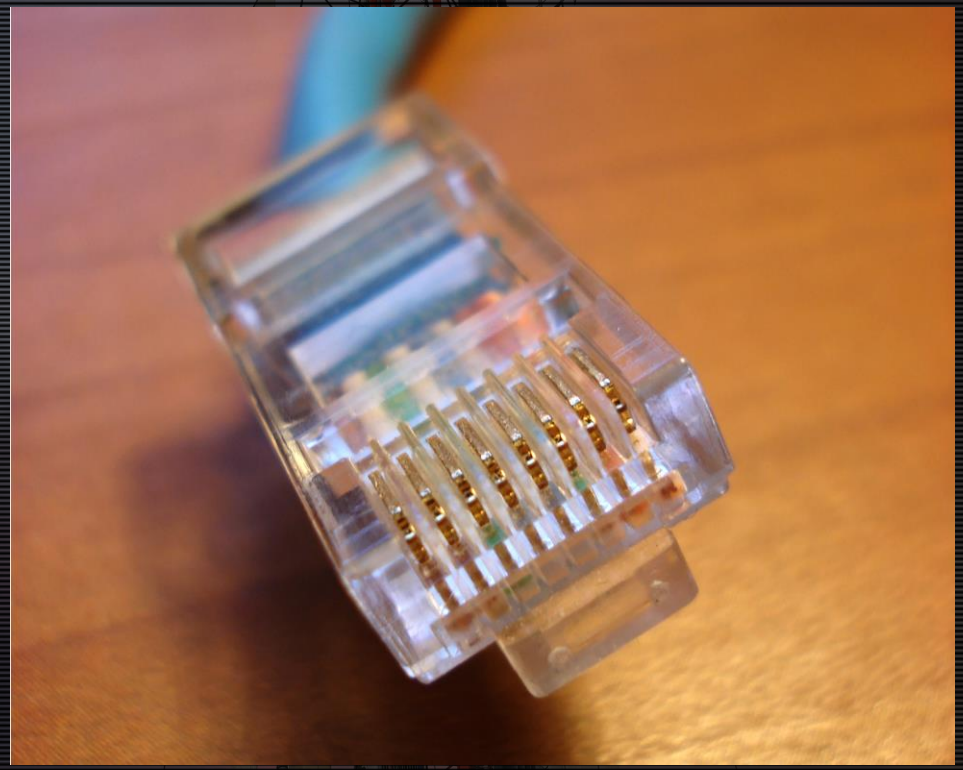
KEYSIGHT TECHNOLOGIES

EXPLOITING LTE & 5G STANDARD WEAKNESS

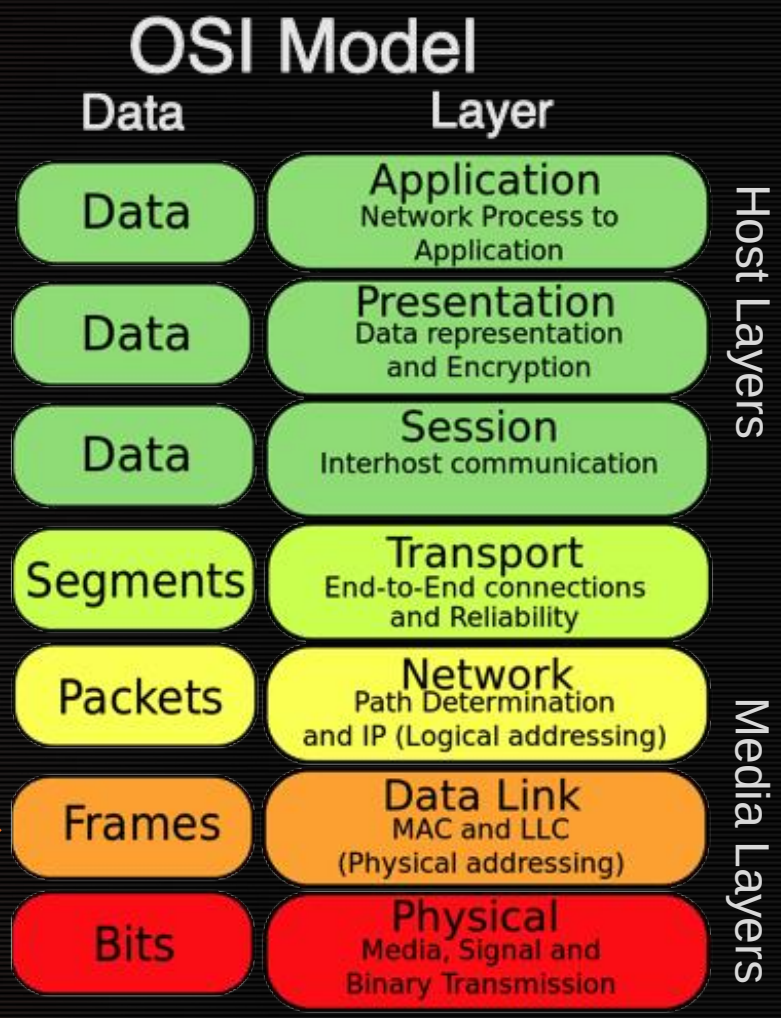
KEYSIGHT TECHNOLOGIES

What is the MAC layer?

MEDIUM ACCESS CONTROL

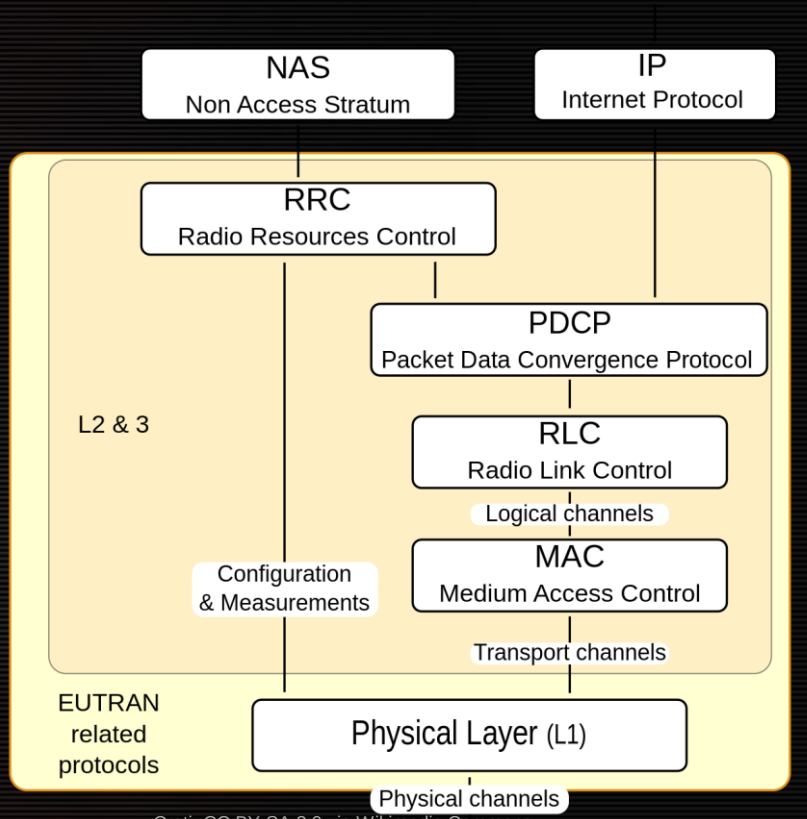


This one



KEYSIGHT TECHNOLOGIES

LTE/5G Big MAC Layers!



Crati, CC BY-SA 3.0 via Wikimedia Commons

Terminology Quick Start:

UE (User Equipment)

- Phone, Tablet, Laptop, Things with SIM!

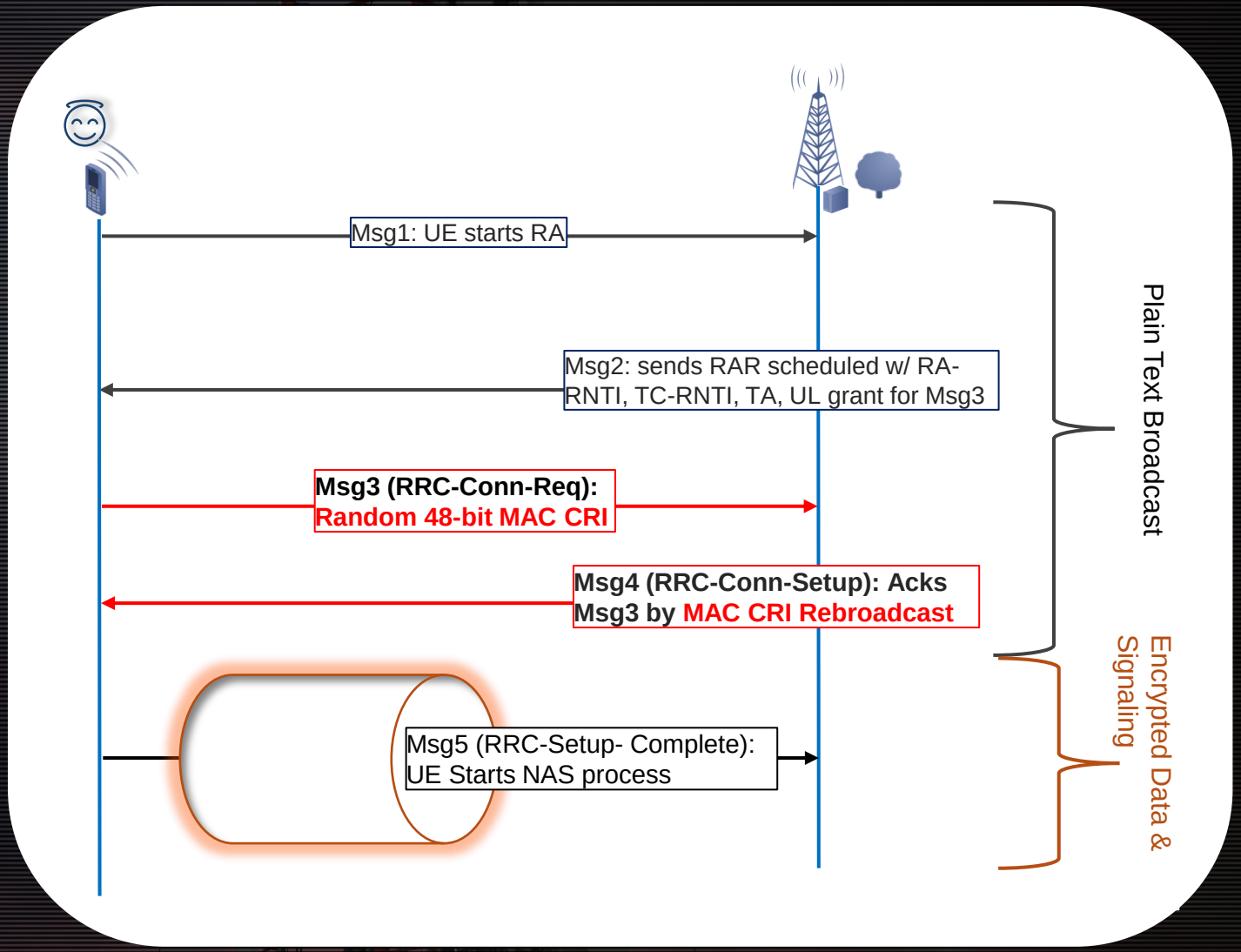
eNodeB / gNodeB

- Cell Tower for LTE/5G
- No one knows what happened to fNodeB!
- **So, I like using fNodeB to refer to both LTE & 5G cells!!**

KEYSIGHT TECHNOLOGIES

Normal RA Procedure

CONTENTION RESOLUTION PING-PONG

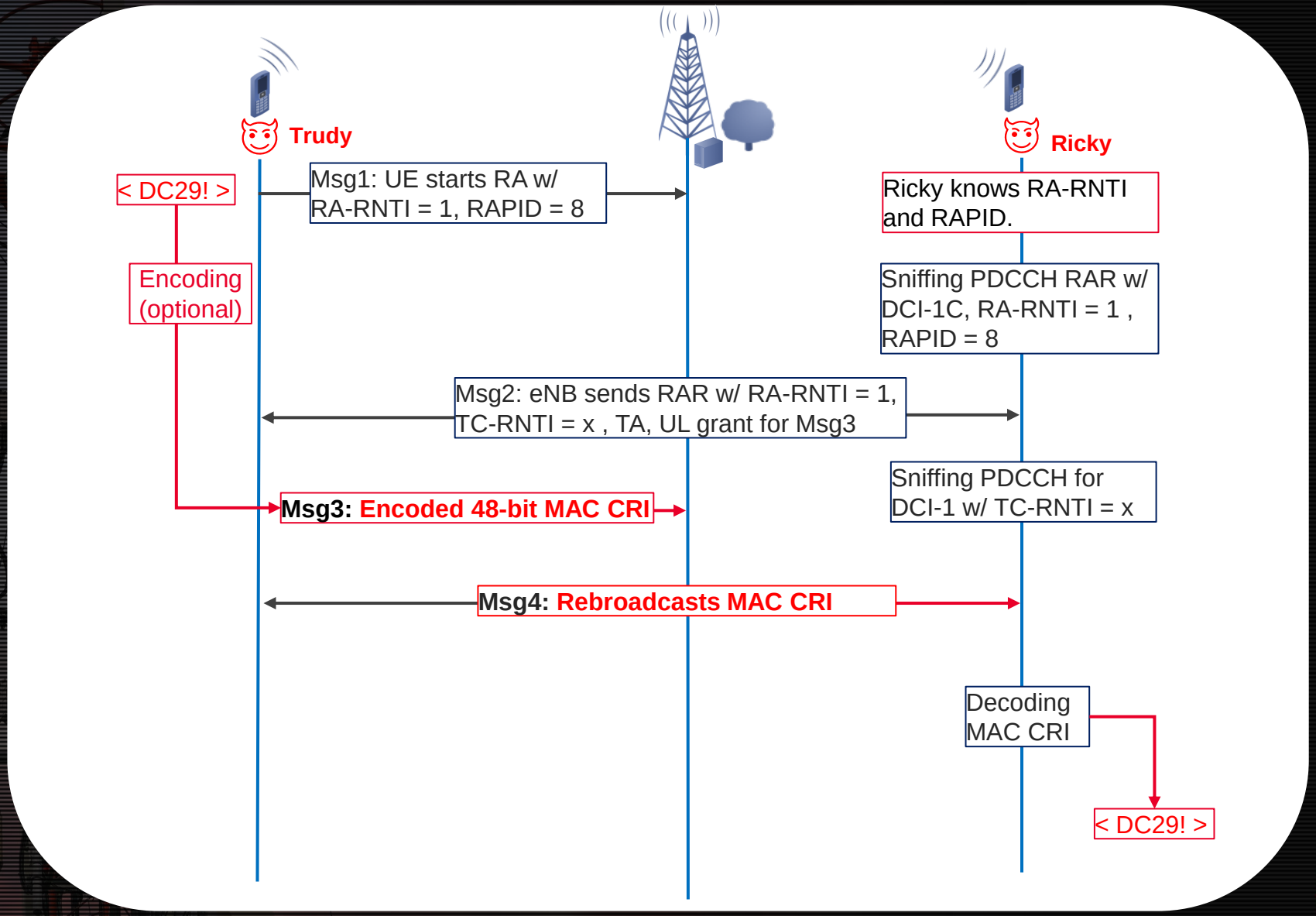


SFN : 403.4	PUSCH - RRC Connection Request
	MAC : 20 06 1F 5C 2C 04 B2 AC F6 Sub Header 0 R = OK E = 1 LCID = 0 (CCCH) F = 0 (False) L = 6 Sub Header 1 R = OK E = 0 LCID = 31 (Padding) CCCH-RLC : 5C 2C 04 B2 AC F6 (RRC Connection Request)
SFN : 403.8	PHICH-ACK
SFN : 404.7	PDCCH (DCI Format 1) + PDSCH (RRC Connection Setup)
	CCE Start = 0 CCE Length = 8 DCI Format 1A (Hex : 47D01E2) Format = 1 Distributed VRB flag = 0 (Local) Resource Allocation = 500 (RB Start = 0, RB Length = 11) MCS = 0 (I_TBS = 0) HARQ Process Number = 7 NDI (New Data Indicator) = 1 (True) RV = 0 TPC Command for PUCCH = 1 MAC : 3C 20 1A 1F 5C 2C 04 B2 AC F6 60 12 98 08 FD 4E ..... Sub Header 0 R = OK E = 1 LCID = 28 (UE Contention Resolution Identity) Sub Header 1 R = OK E = 1 LCID = 1 (CCCH) F = 0 (False) L = 26 Sub Header 2 R = OK E = 0 LCID = 31 (Padding) UE Contention Resolution Identity UE Contention Resolution Identity = 5C 2C 04 B2 AC F6
SFN : 405.1	PUCCH - UCI HARQ ACK

https://www.sharetechnote.com/html/FullStack_LTE.html

KEYSIGHT TECHNOLOGIES

Exploiting CRI Broadcast

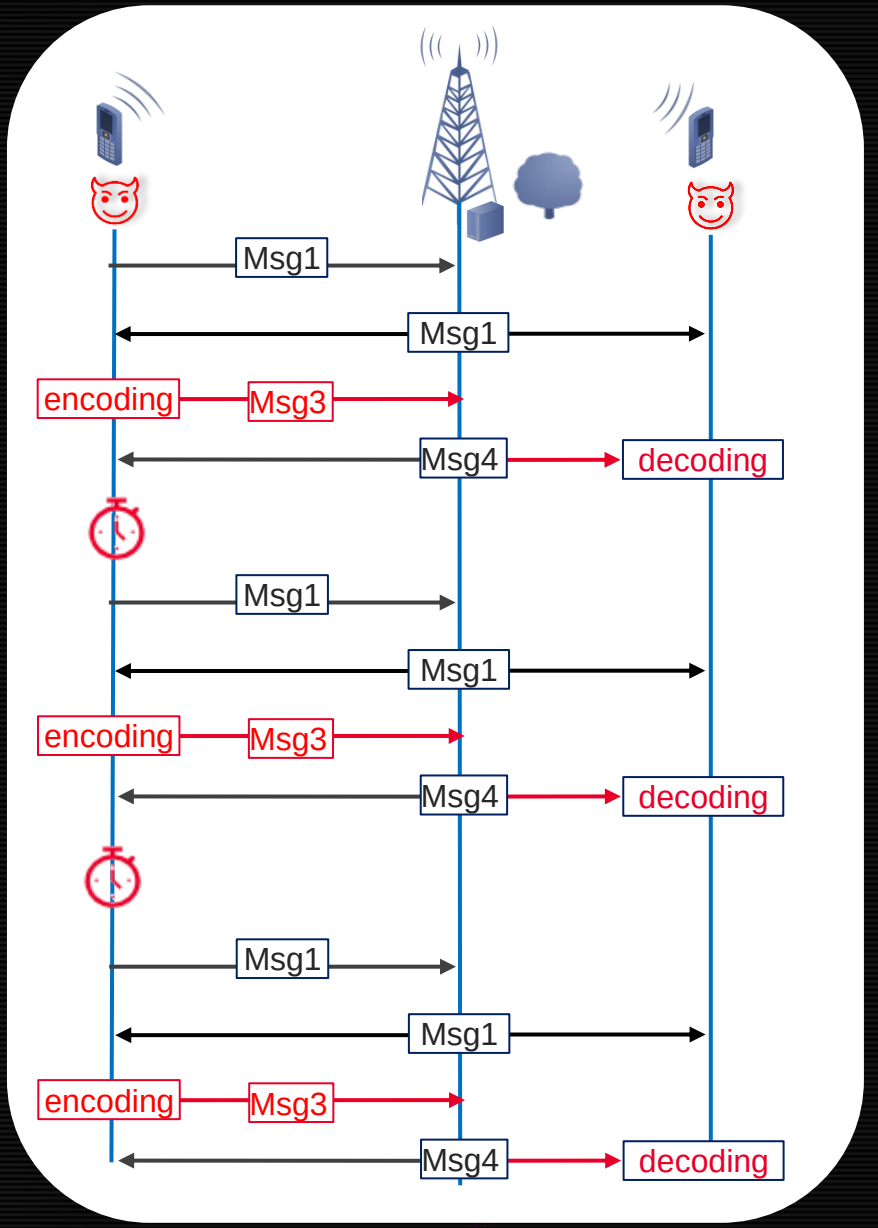


KEYSIGHT TECHNOLOGIES

Exploiting CRI Broadcast

SUCCESSIVE ATTEMPTS

- A SPARROW UE can send successive 40-bits messages
- Successive RACH attempts do not impact other users much.
- Picking low backoff time: like every 40 ms => 1 kbps tput.
- This vulnerability can be traced back to LTE Rel. 8 and still exists in 5G-NR.
- Although less-relevant FR2 (above 6 GHz) due to beamforming it can be easily exploited in LTE lower-bands and FR1 to achieve around 5 miles range.
- Higher ranges achievable in upcoming 5G-NTN (satellite gNBs).



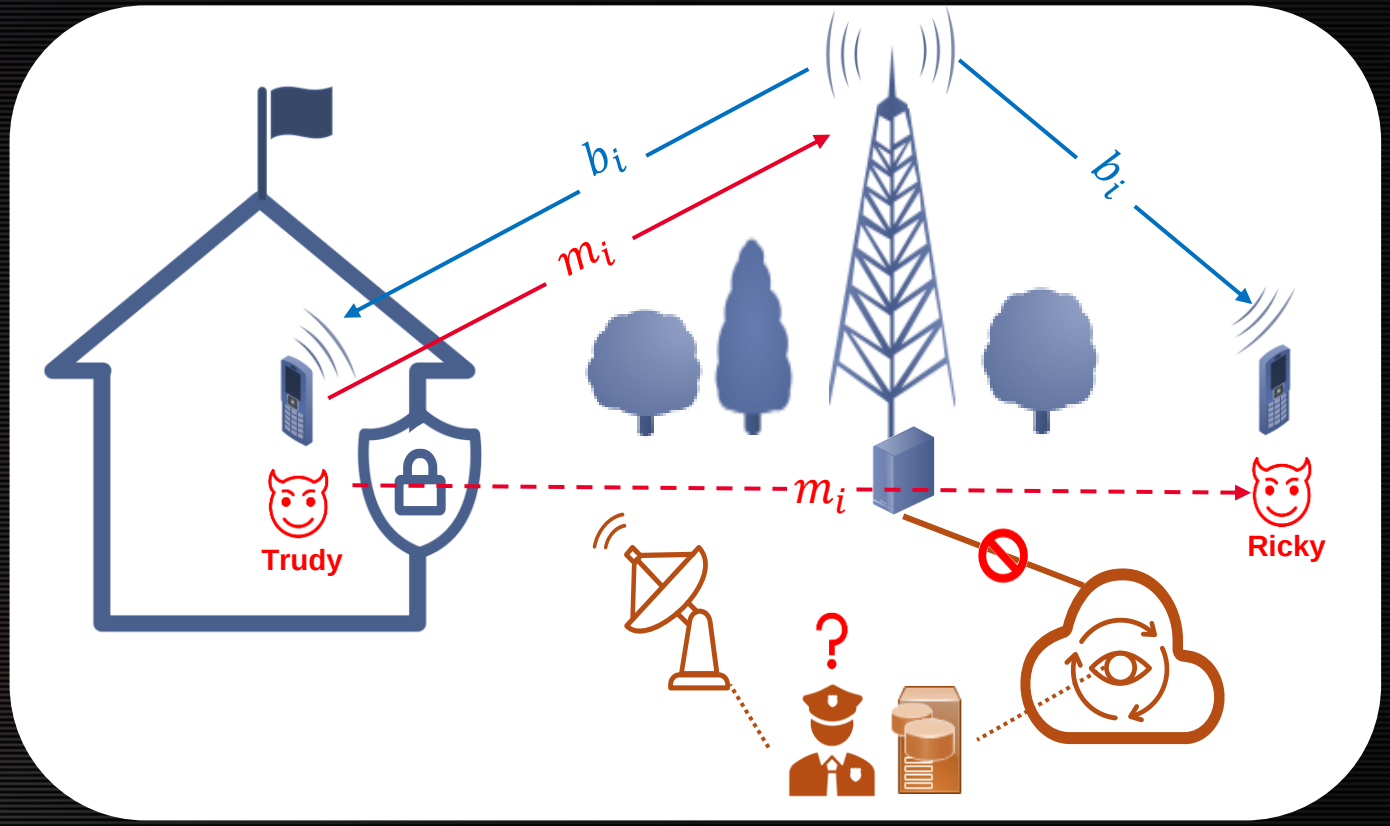
- if in this Random Access procedure, the Random Access Preamble was selected by MAC:
  - based on the backoff parameter in the UE, select a random backoff time according to a uniform distribution between 0 and the Backoff Parameter Value;
  - delay the subsequent Random Access transmission by the backoff time;
- proceed to the selection of a Random Access Resource (see subclause 5.1.2).

Source: 3GPP TS 36.321, sec 5.1.4

KEYSIGHT TECHNOLOGIES

WHY SPARROW?

- No Network or Spectrum Footprint
- Low Hardware Complexity
- More Miles per Watt
- Unstoppable



Sparrow UE

0.2 W / 5 mi

LoRAWAN GW

1 W / 5 mi

2 W / 1 mi

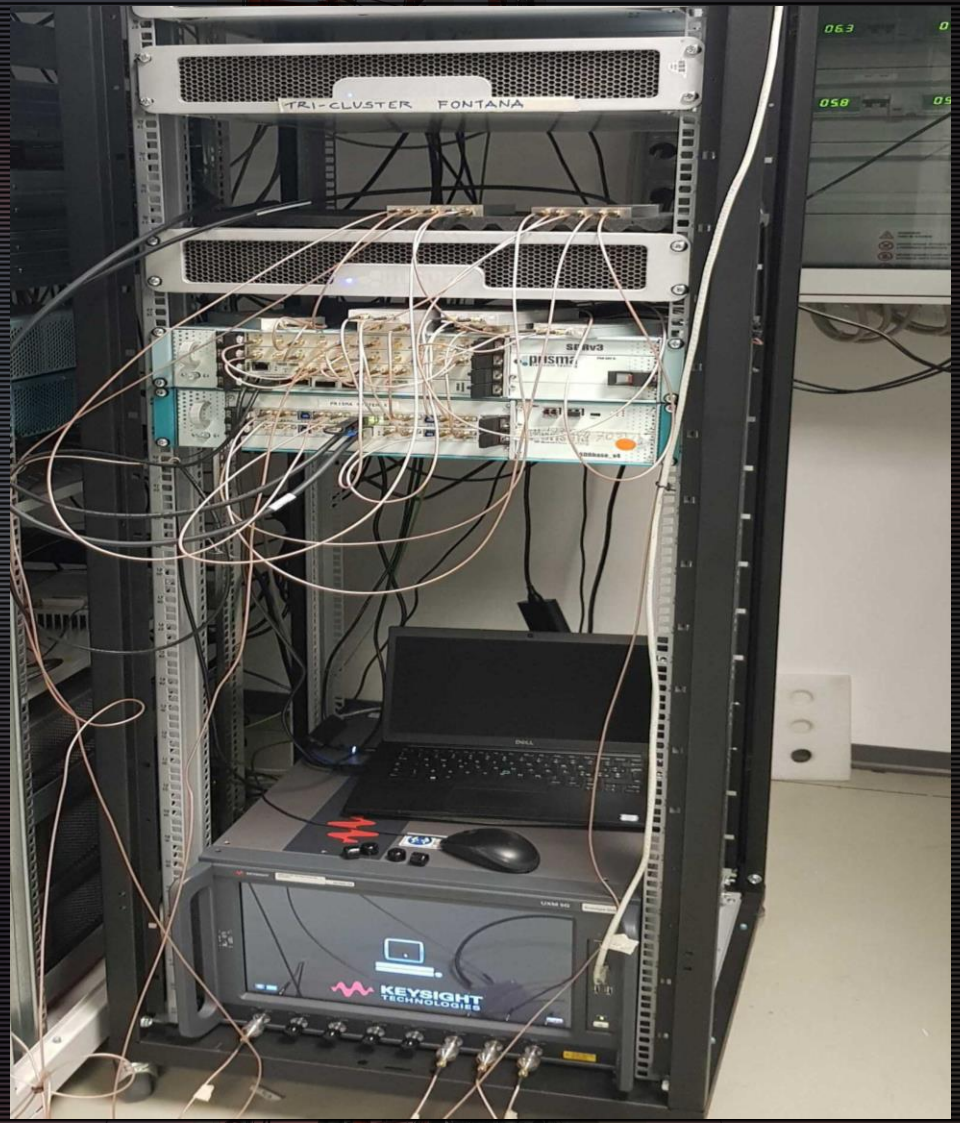
Walkie Talkie

KEYSIGHT TECHNOLOGIES

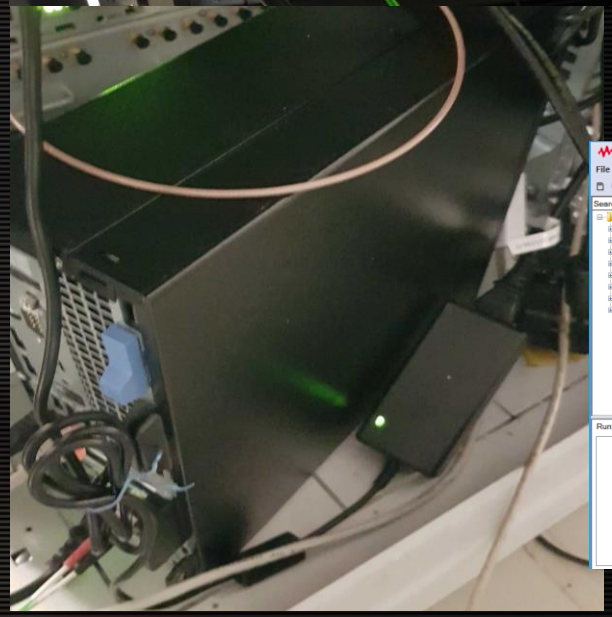
Demo & Use Cases

KEYSIGHT TECHNOLOGIES

SPARROW Testbed Setup

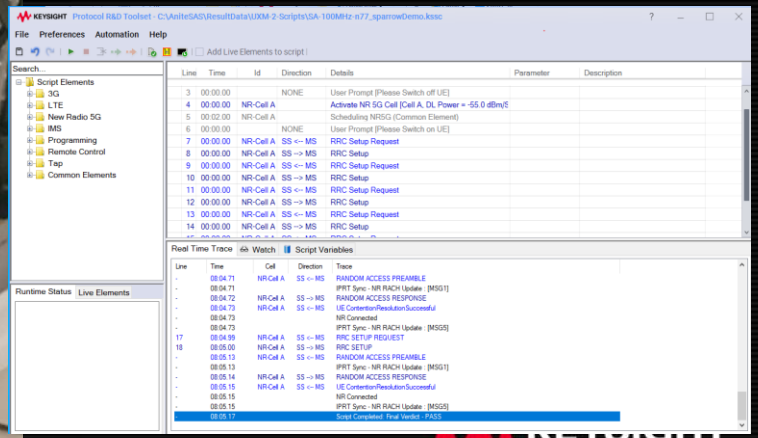


Keysight UXM
Rear side



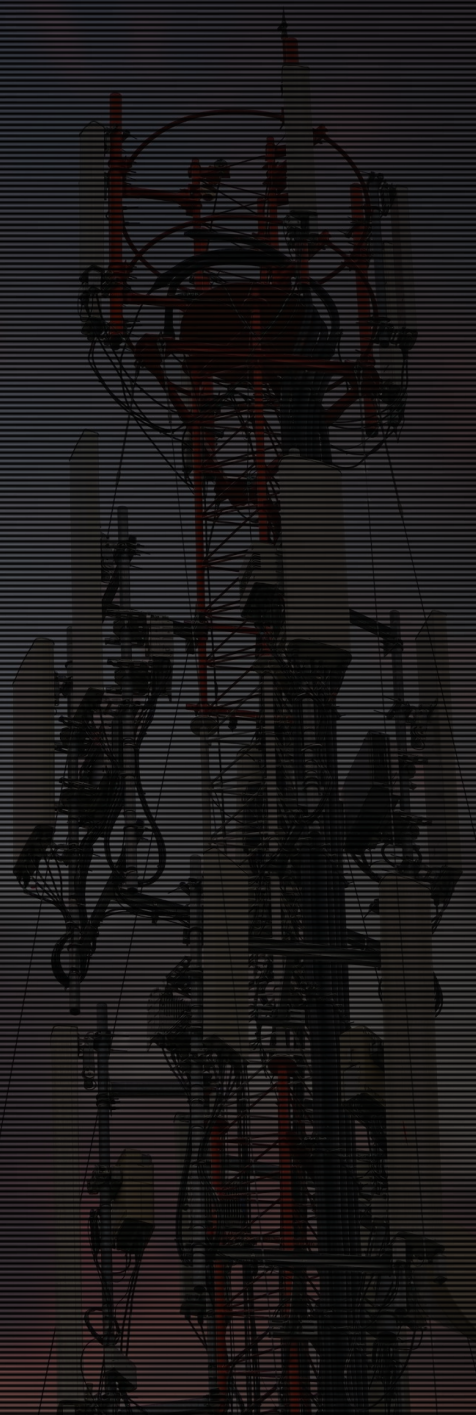
Test PC

PRT
Script



KEYSIGHT TECHNOLOGIES

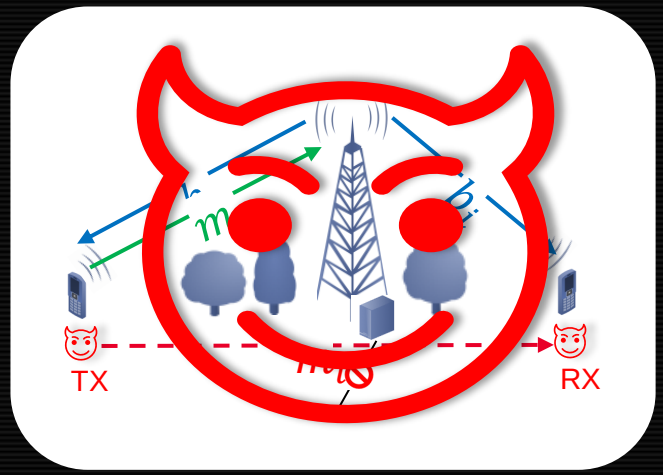
DEMO

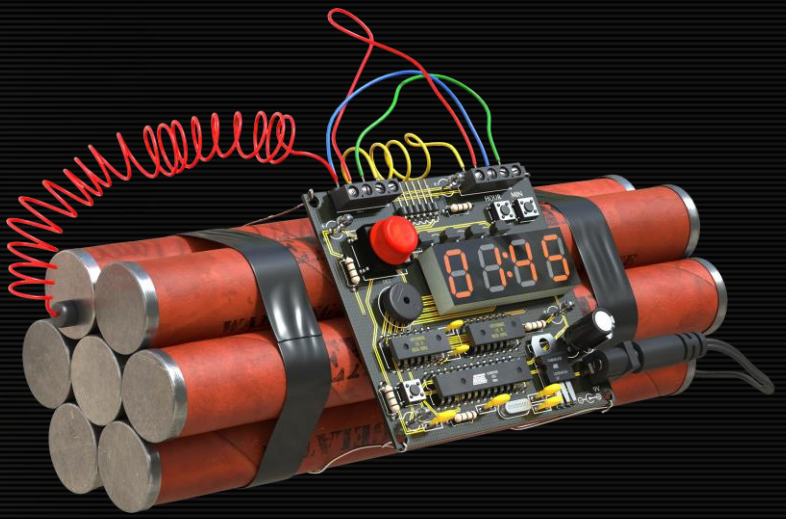


KEYSIGHT TECHNOLOGIES

Application Scenarios

- **Data Exfiltration:** Extract sensitive data out of secure locations
- **Command & Control (CnC):** trigger or monitor events remotely
- **Supply Chain:** Remote access baked into firmware of modem



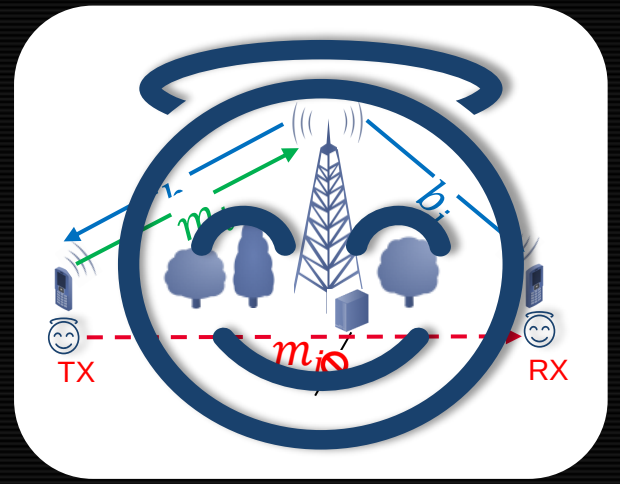


KEYSIGHT TECHNOLOGIES

Application Scenarios

- **Disaster Recovery:** In case of natural disasters, the cellular infrastructure could be operational without backhaul links.

- **Failover Broadcast:** Can utilize this as an alternative for emergency notifications. Connect parties in case of emergency.



KEYSIGHT TECHNOLOGIES

Application Scenarios

- **Extended Network:** Make a lightweight IoT network using someone else's fNodeB

- **Pager Network:** Let everyone know it's dinner time, create a localized medium distance pager network

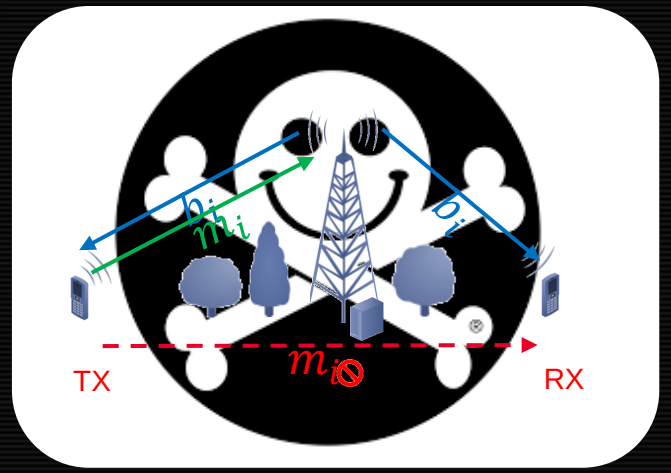
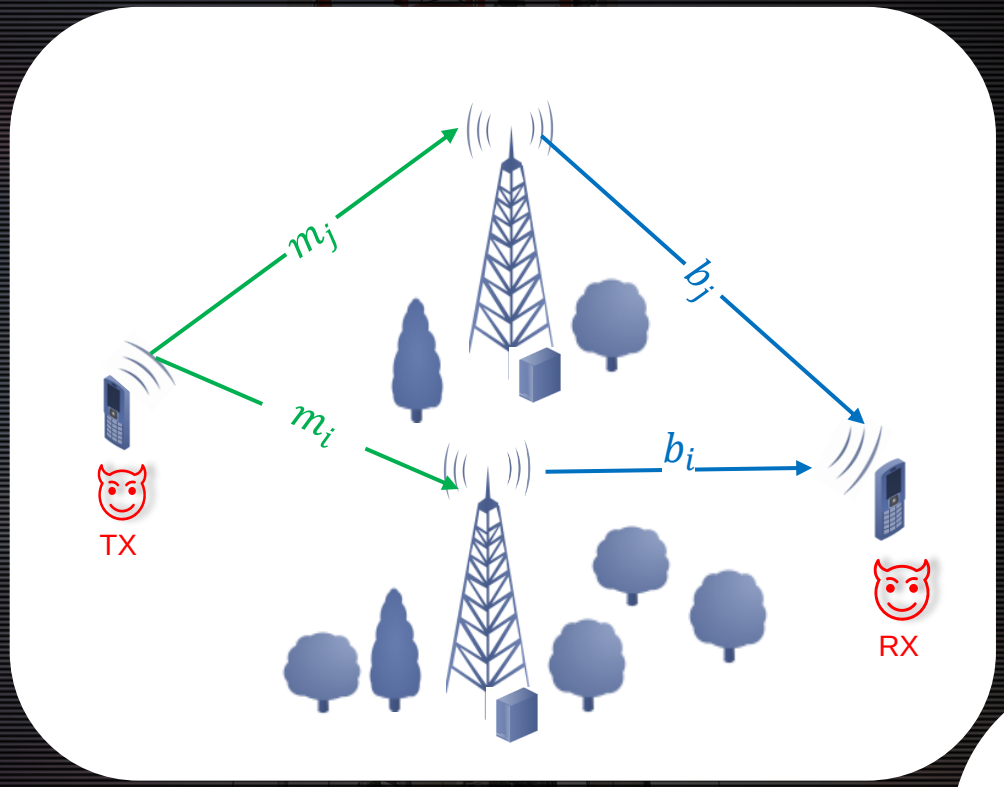


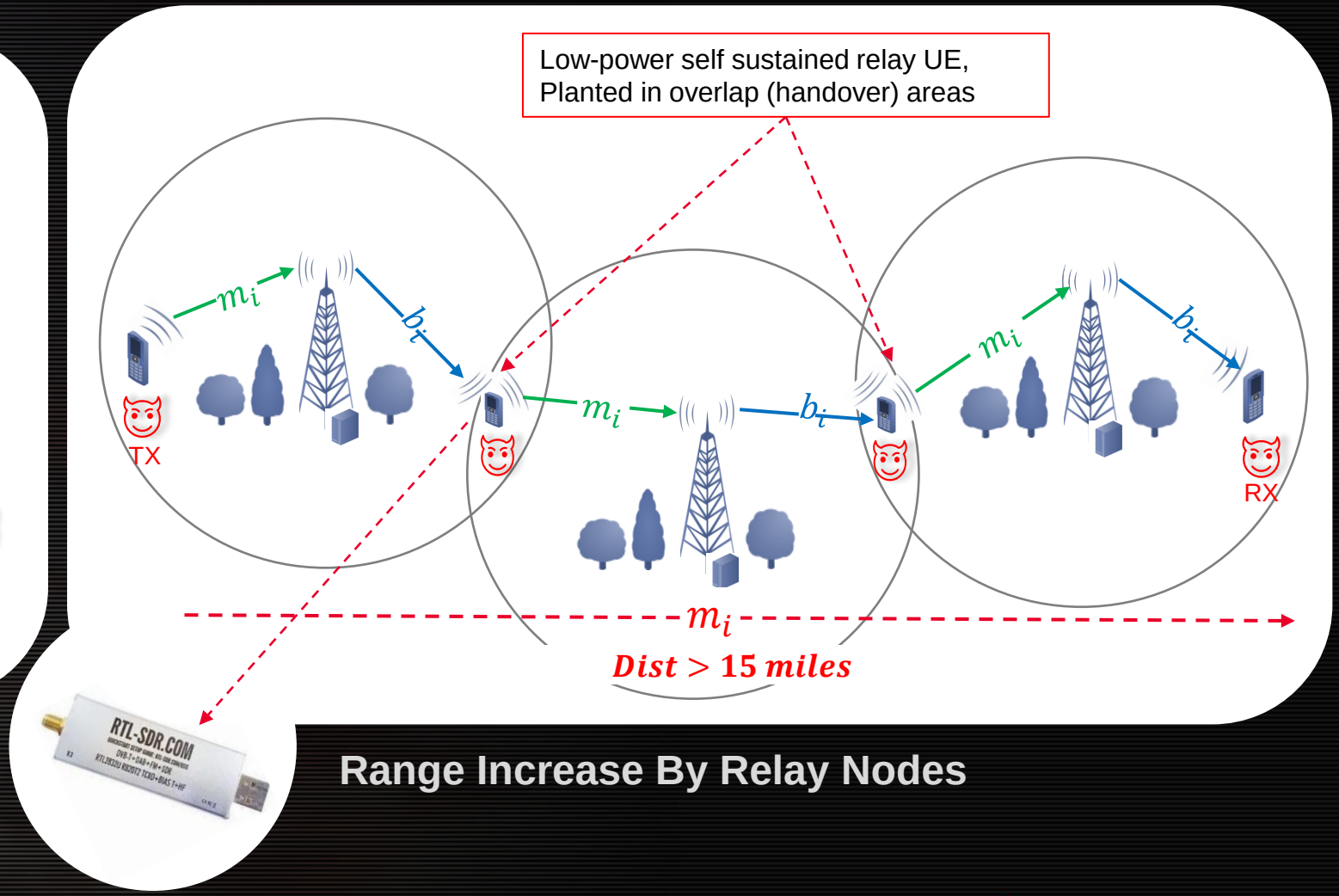
Image provided curtesy of @_naturalfreq of Dirt Simple Comms

KEYSIGHT TECHNOLOGIES

Geographical Enhancements



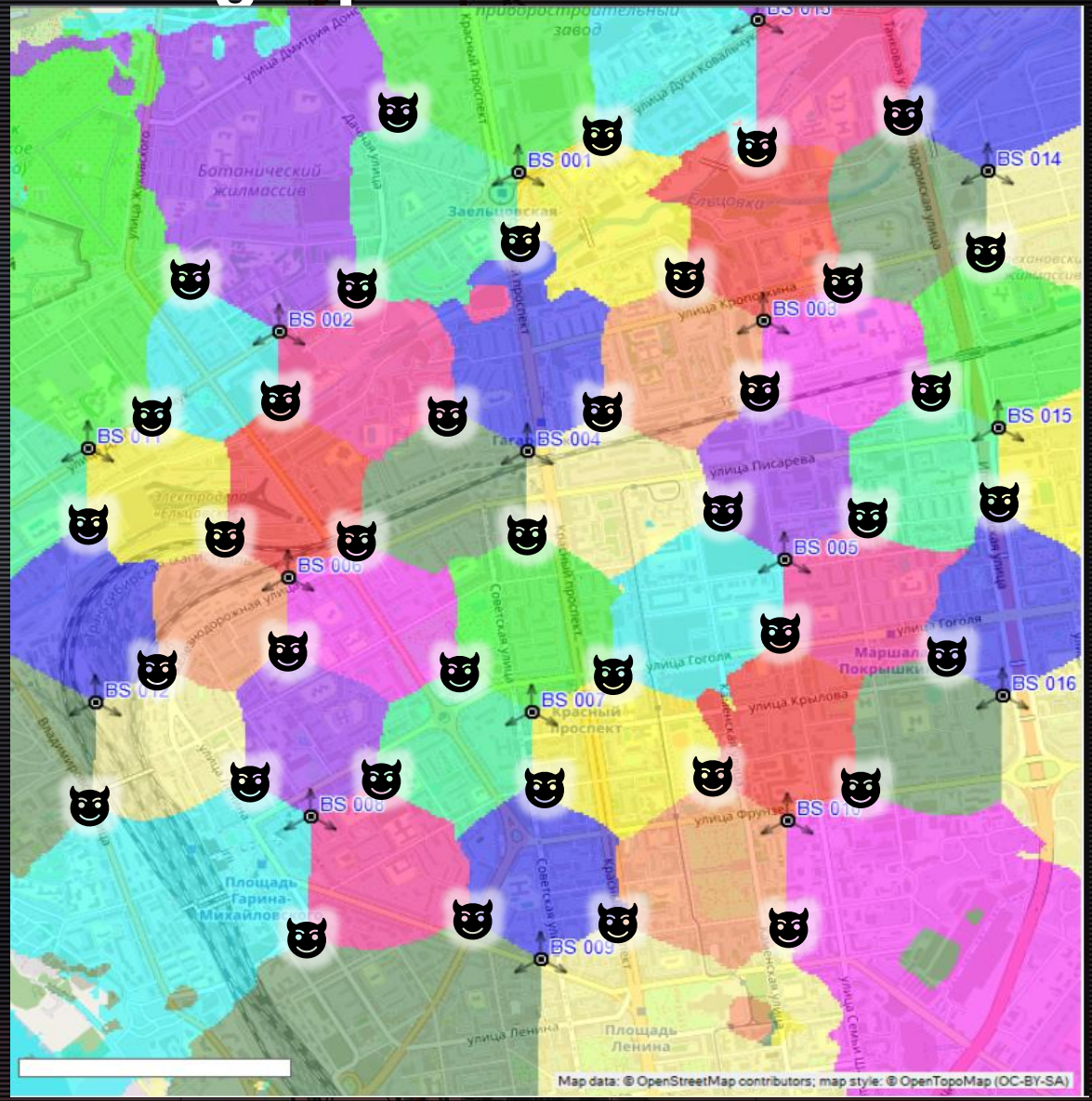
Reliability / Rate enhancement
via parallel PTP links

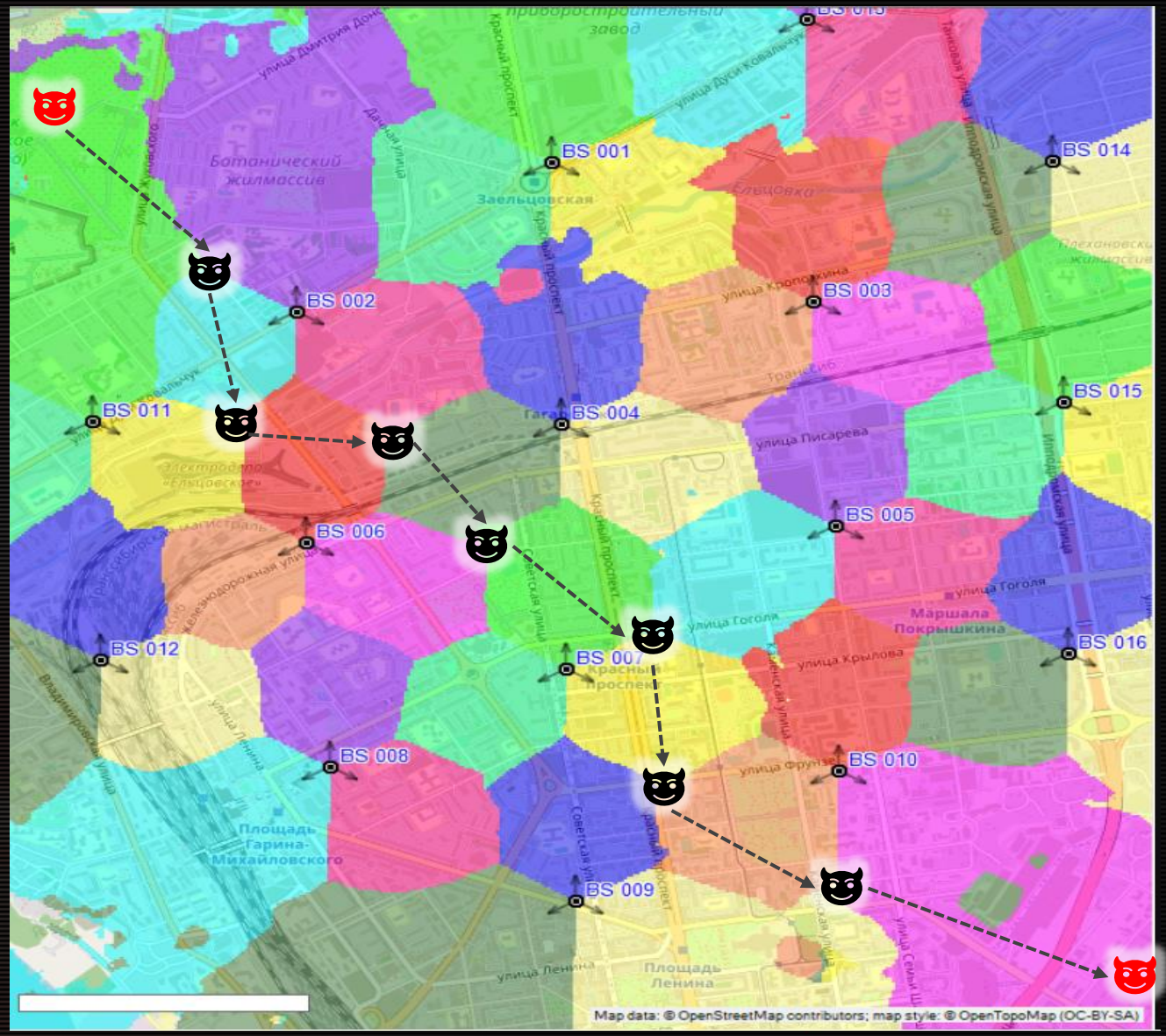


Range Increase By Relay Nodes

KEYSIGHT TECHNOLOGIES

Geographical Enhancements





GENERAL REMEDIATION

KEYSIGHT TECHNOLOGIES

Weakness Model

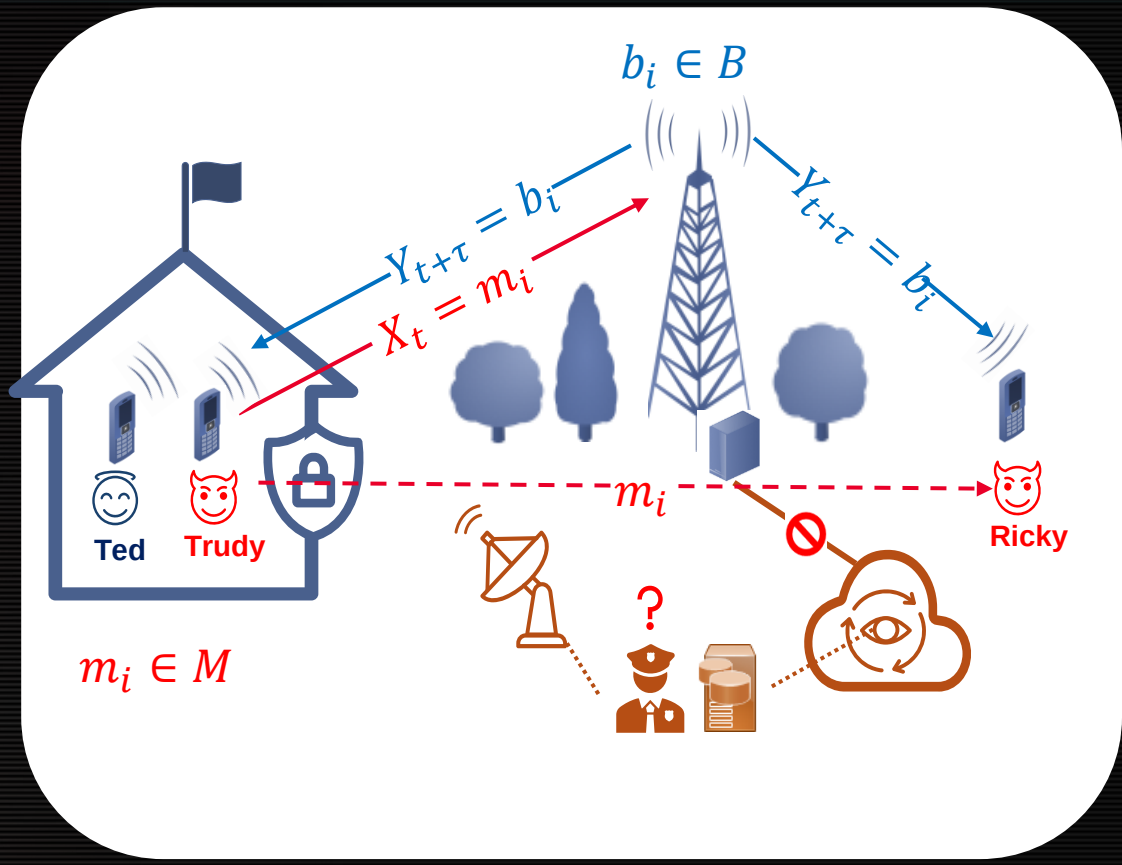
A wireless MAC layer protocol is deemed vulnerable to SPARROW technique, if any of its procedures allows forming two sets of uplink messages (**M**) and the downlink broadcast messages (**B**) satisfying all the following conditions:

1) **Passive Reception:** any signal in (**B**) are anonymously decodable.

2) **Bijectivity:** one-to-one correlation between (**M**) & (**B**).

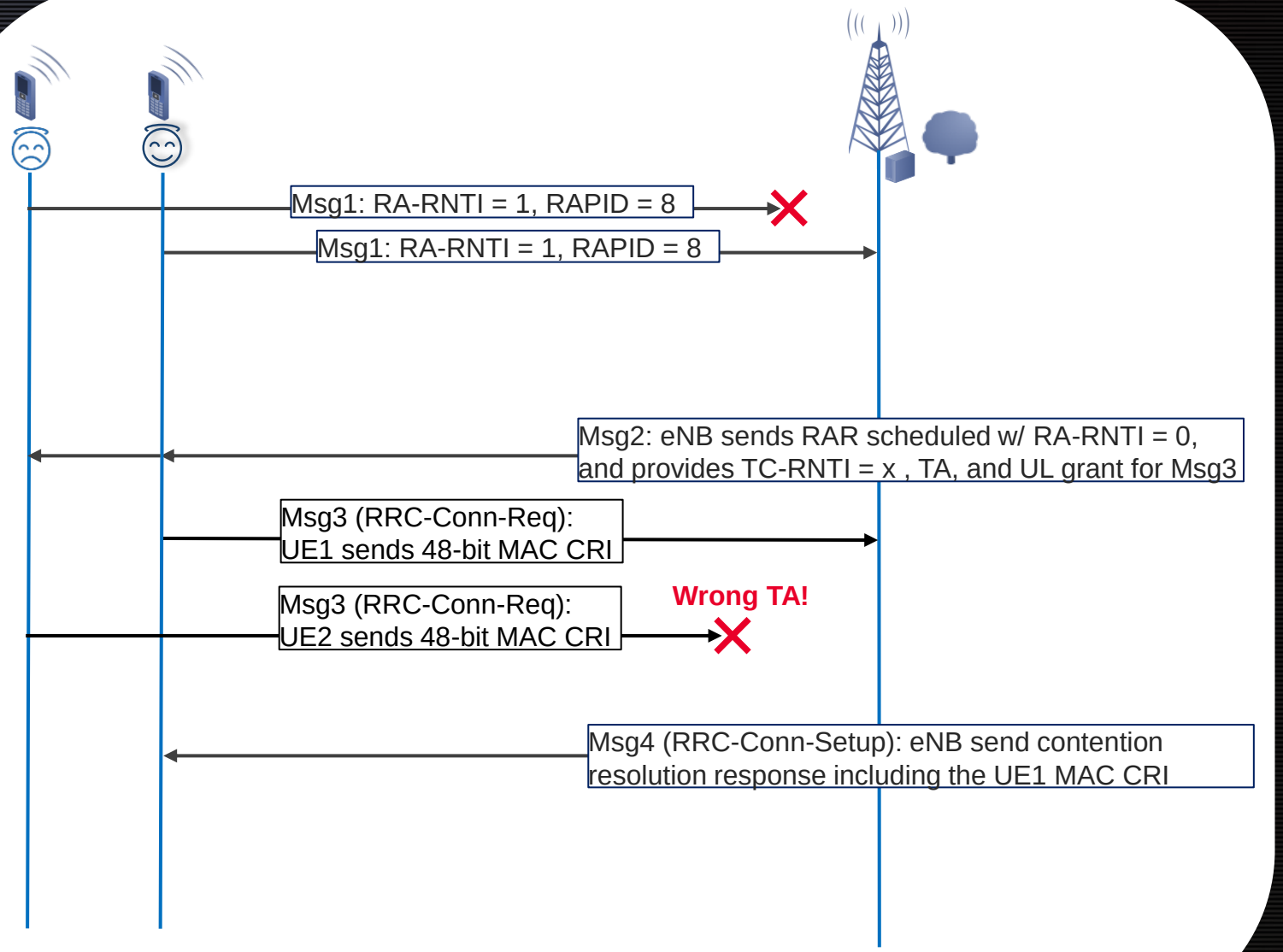
3) **Anonymous Uplink:** no need to attach to the network.

4) **Stateless Uplink:** Trudy can successively send any message from (**M**) without protocol violation.



KEYSIGHT TECHNOLOGIES

Understanding CRI Purpose



- The value is arbitrary by UE
- Think of it as a ping-pong or selective ack

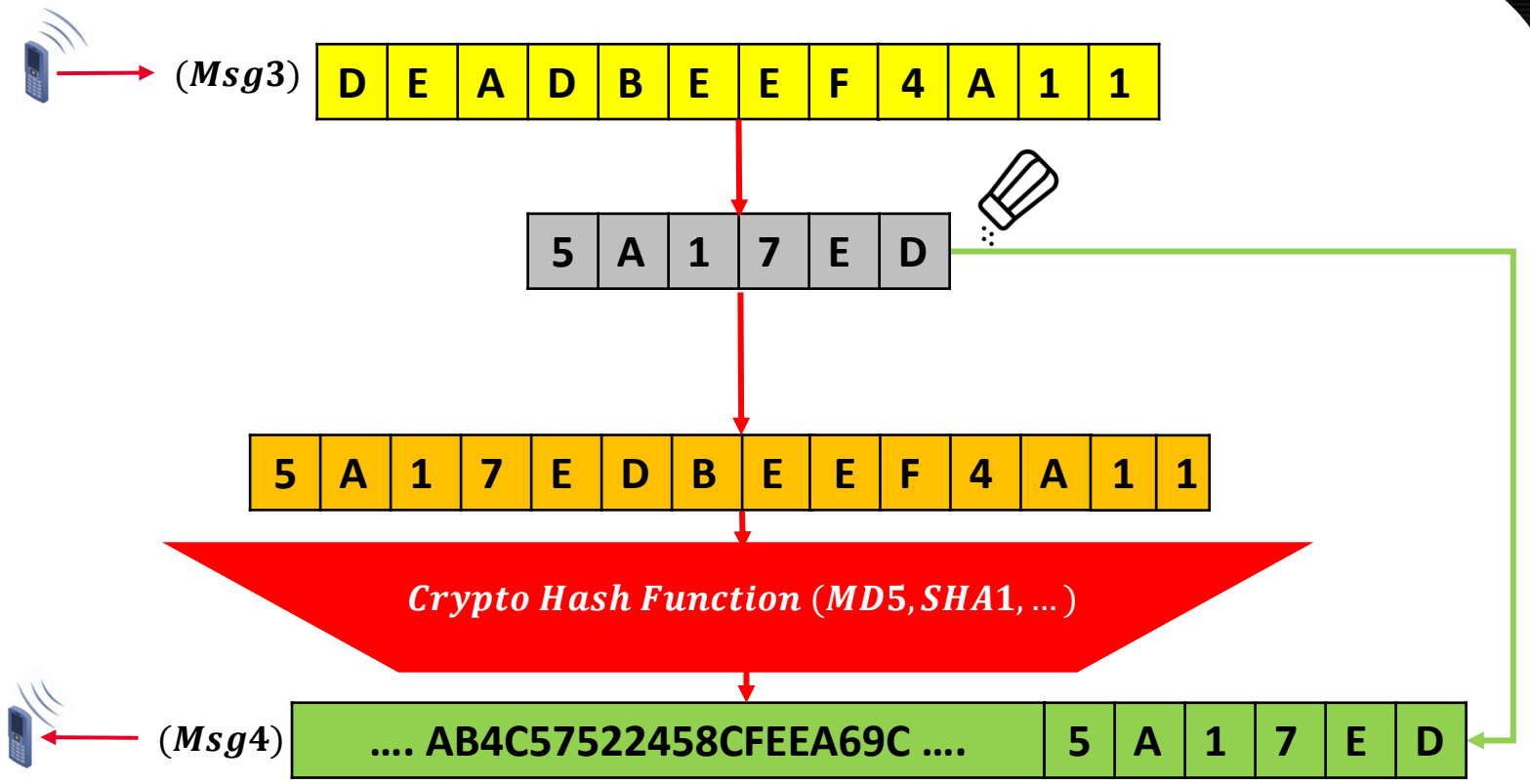
- Rebroadcast in Msg4 is universally decodable (QPSK) by both UE and non-UE devices

- UE identities remain hidden

KEYSIGHT TECHNOLOGIES

Solutions that don’t work

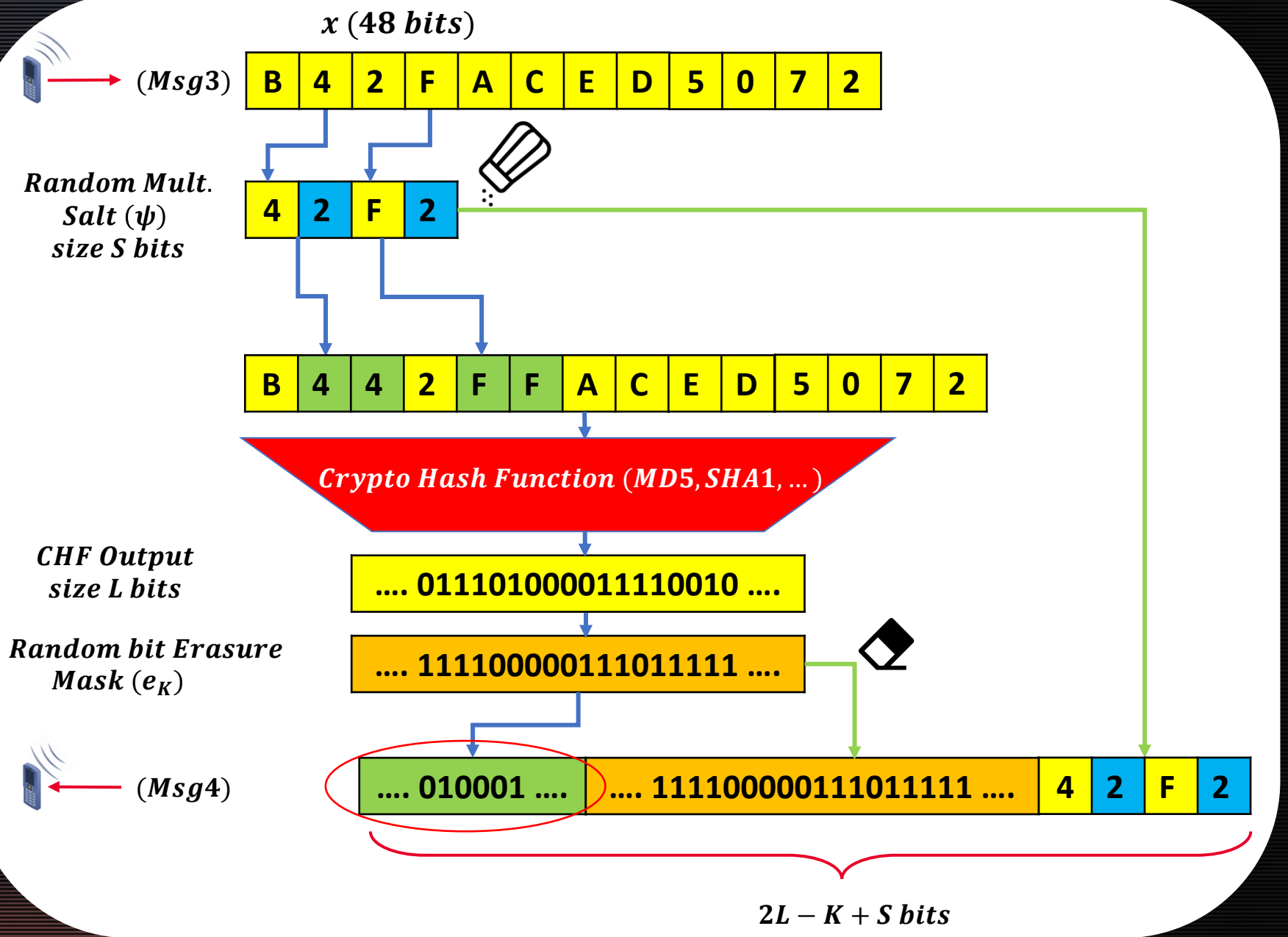
CRYPTO HASH WITH SALT | BLOCKING



- No preset CRI for privacy
- No Shared secret UE & fNB
- Salt must be sent to UE
- Ricky can still map (**B**) to (**M**) by computing hash (rainbow)
- fNB cannot distinguish between Trudy and other users so cannot risk blocking RACH

KEYSIGHT TECHNOLOGIES

Solution That Works: ELISHA



- **Extensible Loss-Induced Security Hashing Algo**
- New Salting to reduce Short-String hash collision
- Infeasible to construct rainbow table or forward-error correction code books
- Could have other applications other than secure RACH

KEYSIGHT TECHNOLOGIES

WRAP UP

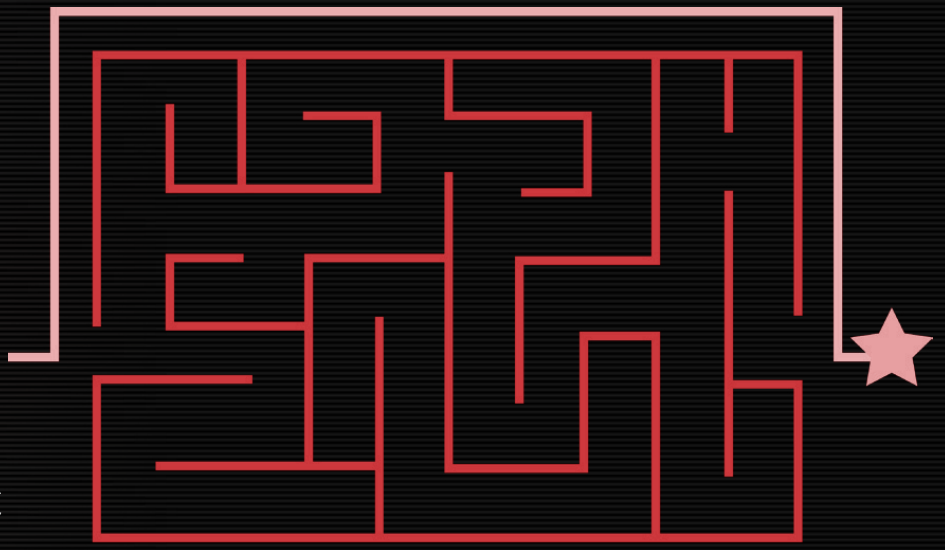
KEYSIGHT TECHNOLOGIES

Disclosure Timeline

KEYSIGHT TECHNOLOGIES

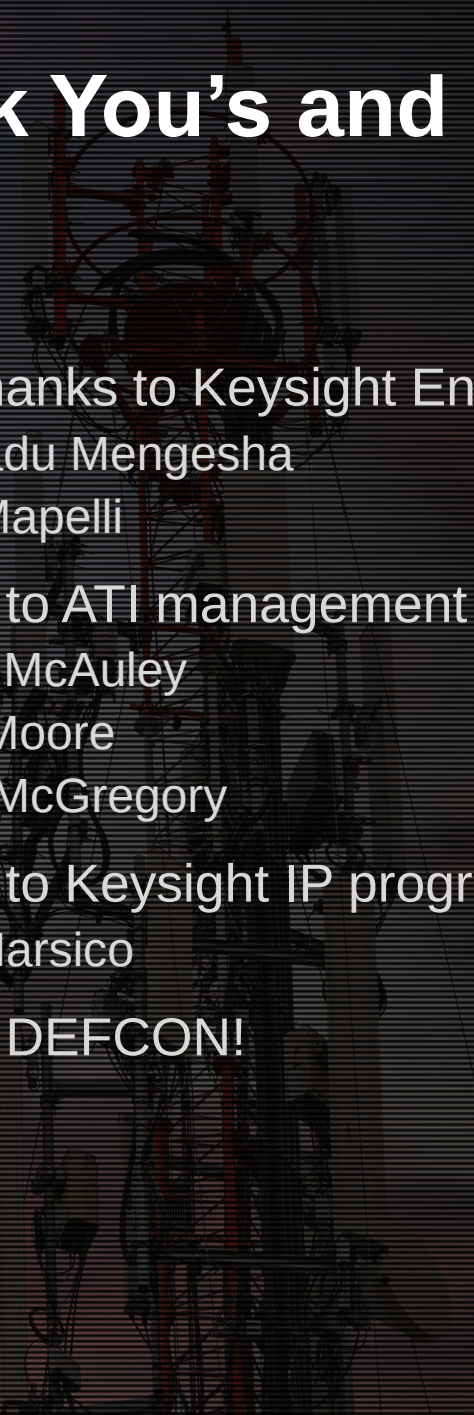
Concluding Bit

- Utilize lateral thinking and your peers!
- There’s a nice sweet spot between building your own wireless protocol or piggy backing on top of the application layer for hidden communication. Just because it’s layer 2 doesn’t mean it’s a short distance.
- We don’t think LTE and 5G are the only radio accessible systems with this kind of problem. Start researching other MAC layer negotiation protocols, notably for wireless systems, like satellites.
- LTE and 5G is for everyone now - CBRS



KEYSIGHT TECHNOLOGIES

Thank You's and Contact



- Many thanks to Keysight Engineering Team in Millan:
  - Befekadu Mengesha
  - Luca Mapelli
- Thanks to ATI management staff:
  - Chuck McAuley
  - Chris Moore
  - Steve McGregory
- Thanks to Keysight IP program coordinator:
  - Pete Marsico
- Thanks DEFCON!

Reza
- https://twitter.com/darthsohos
- https://www.linkedin.com/in/sohos

Chuck
- https://twitter.com/nobletrout

KEYSIGHT TECHNOLOGIES