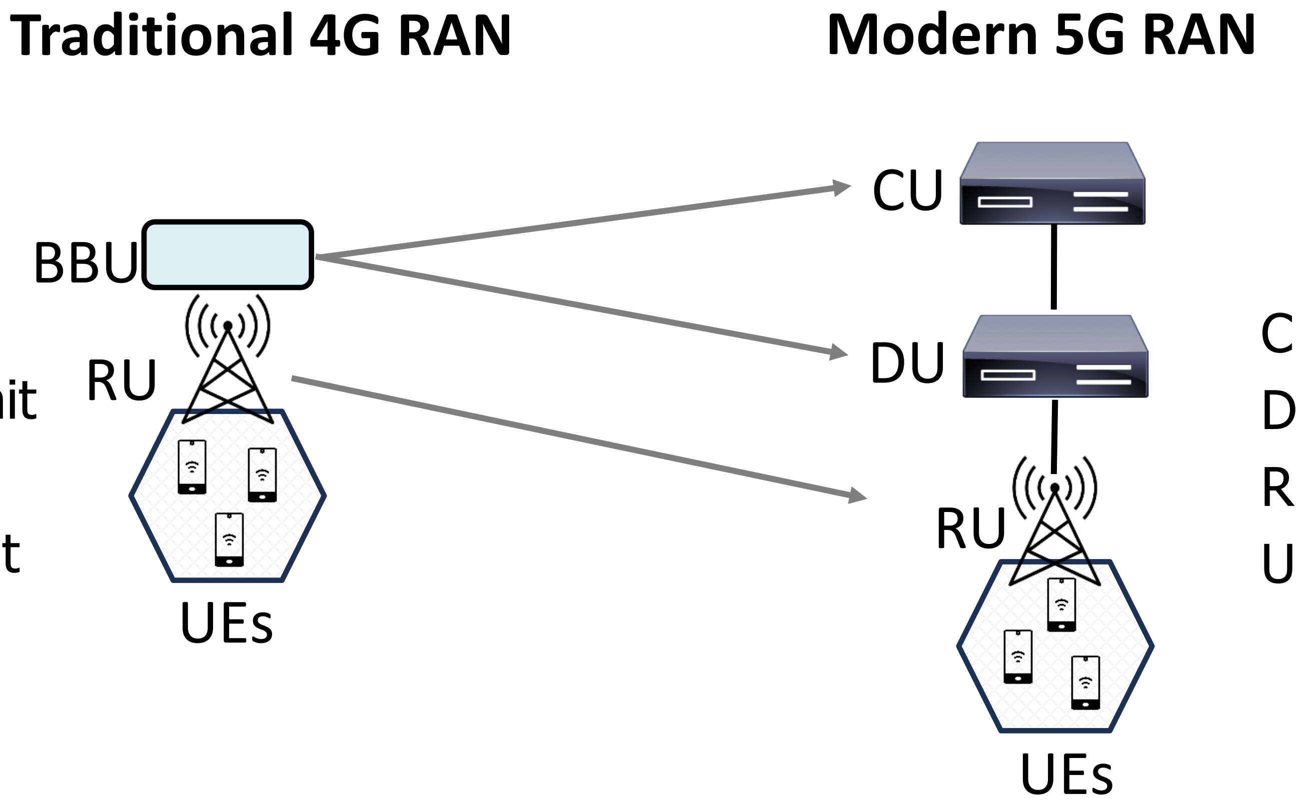
On the Criticality of Integrity Protection in 5G Fronthaul Networks

Jiarong Xing*, Sophia Yoo*, Xenofon Foukas,
Daehyeok Kim, Michael K. Reiter

RICE UNIVERSITY PRINCETON UNIVERSITY Microsoft TEXAS The University of Texas at Austin Duke UNIVERSITY

*Equal contribution

Background: Disaggregated, virtualized 5G RAN

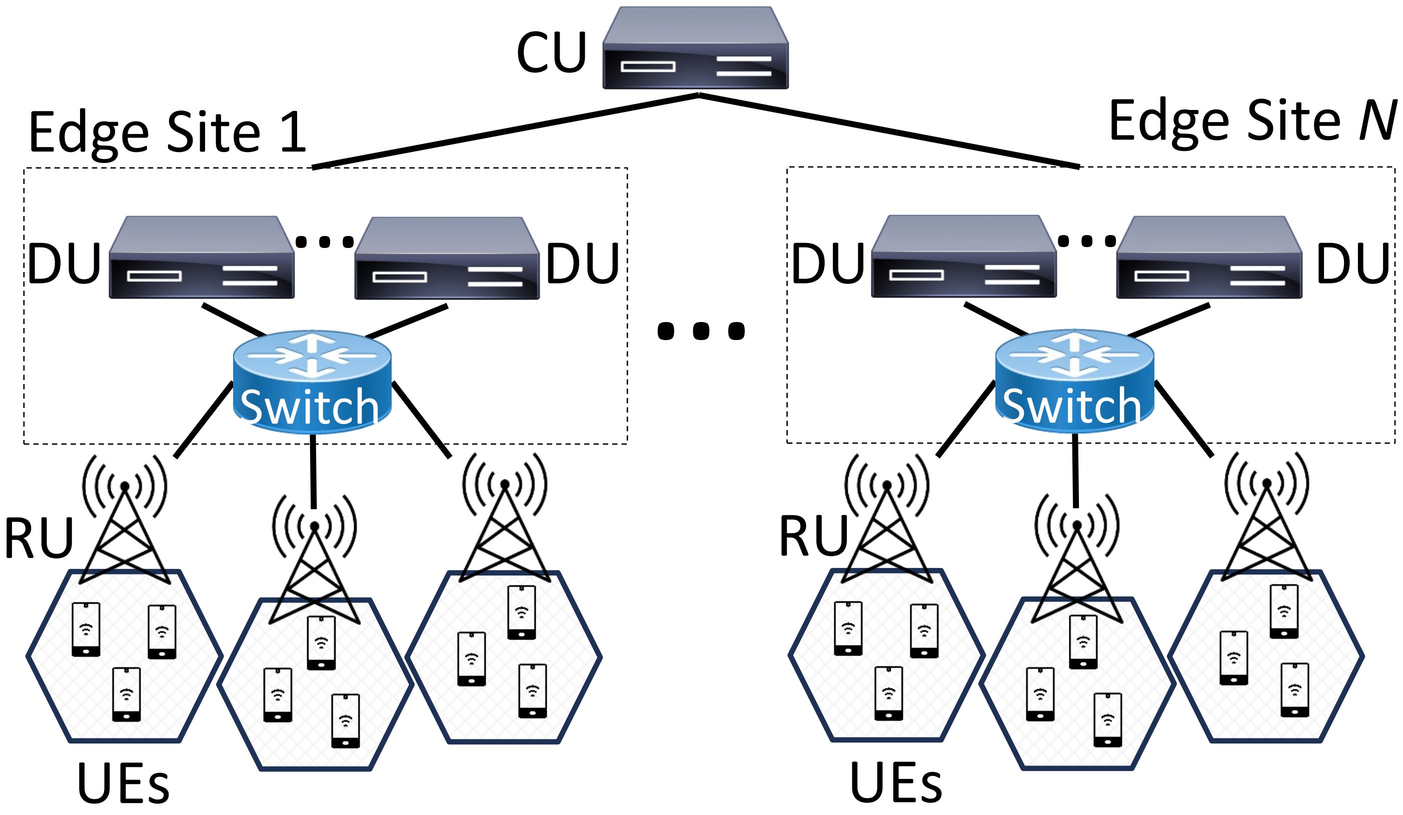


BBU – Base Band Unit
RU – Radio Unit
UE – User Equipment

CU – Centralized Unit
DU – Distributed Unit
RU – Radio Unit
UE – User Equipment

- Disaggregation: Previously centralized RAN components are split into three parts, connected by open interfaces and Ethernet-based protocols
- Virtualization: Functions now run on commodity off-the-shelf (COTS) servers

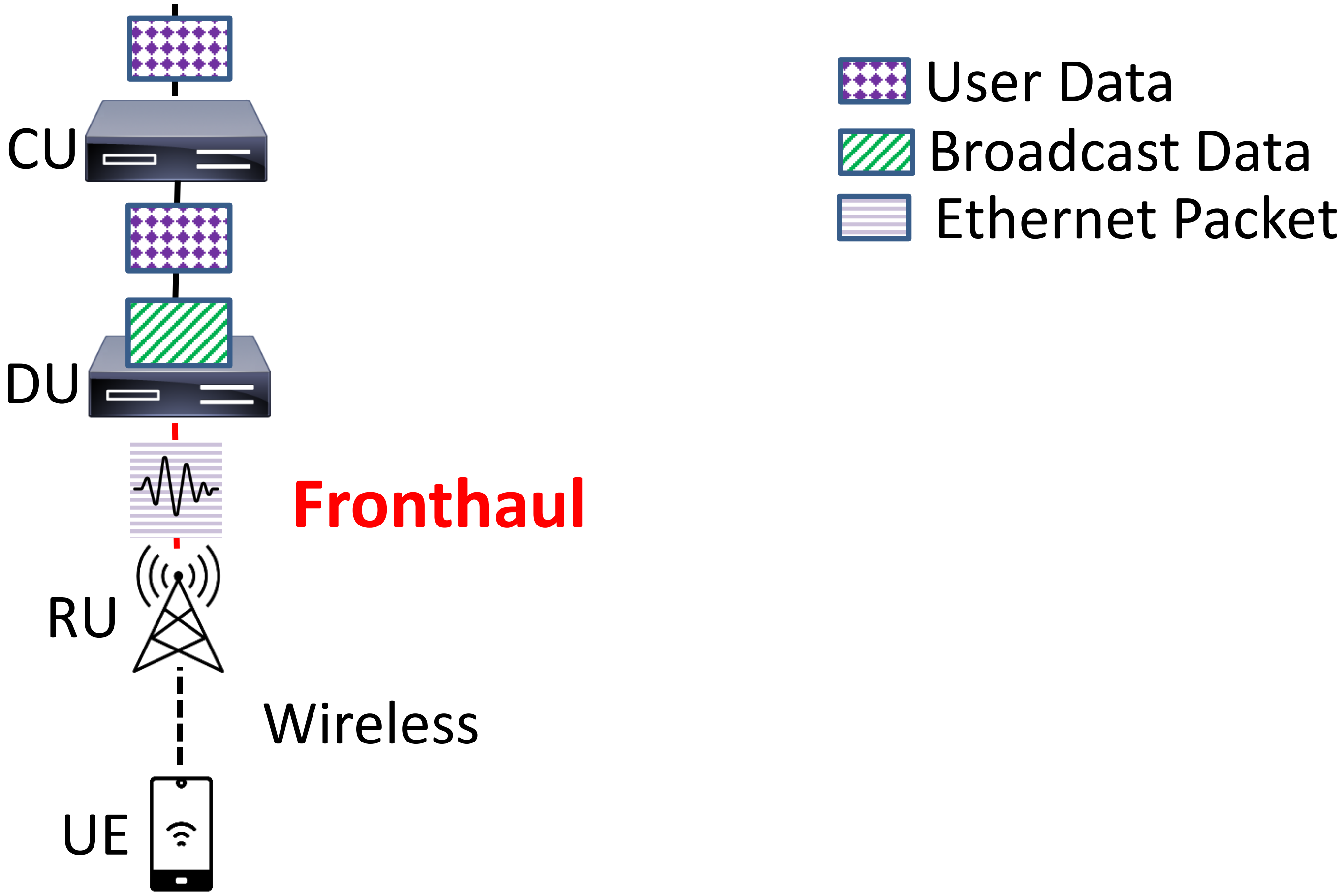
Background: Modern 5G RAN deployment mode



Our focus: The fronthaul network

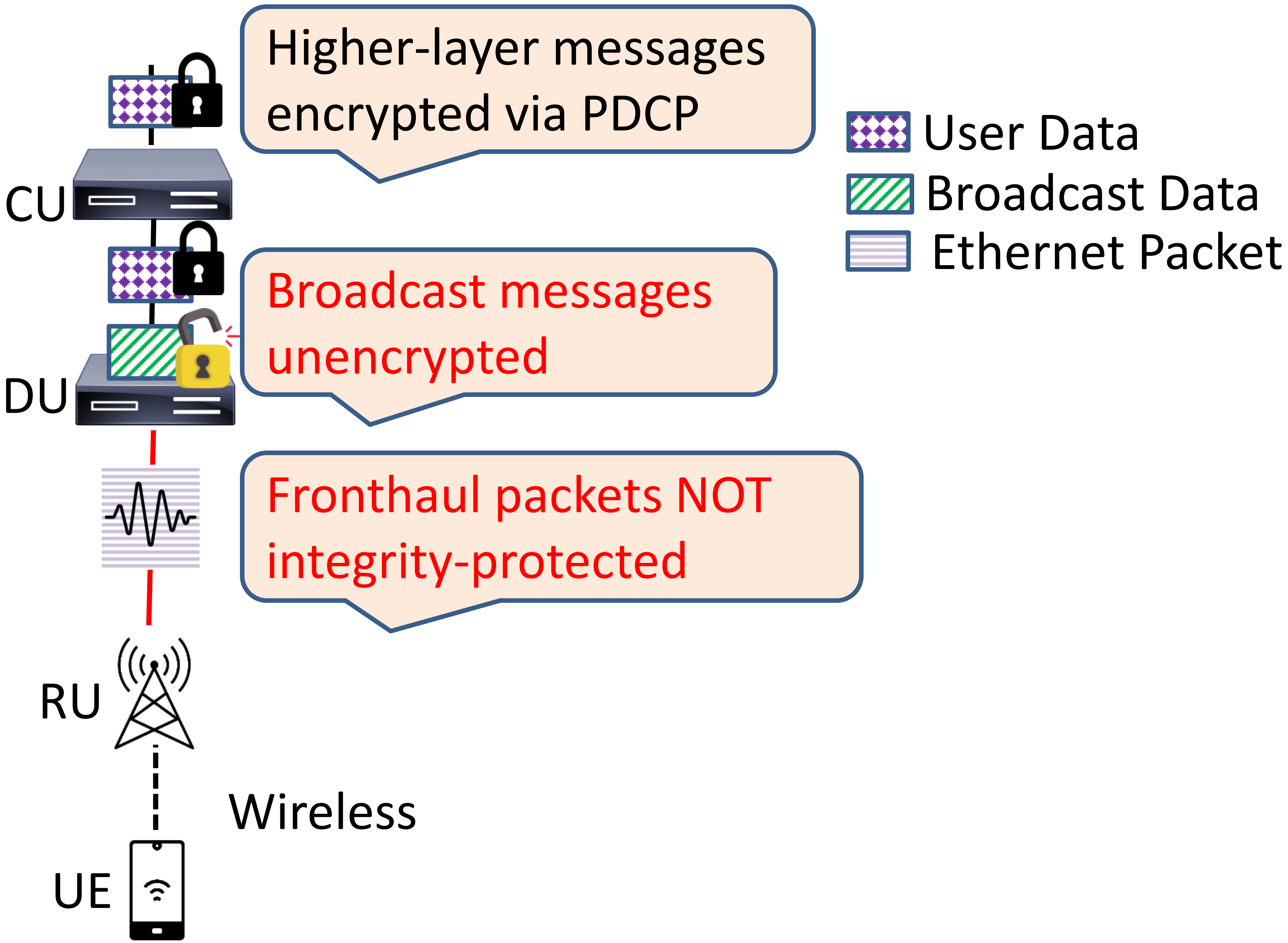
- Fronthaul transports user and control data between DU and RU

- Operates over Ethernet-based eCPRI



Problem: Incomplete integrity protection and MITM attacks

- Fronthaul packets are not integrity protected
- Adversaries can inject and modify fronthaul packets as MITM attackers



Higher-layer messages encrypted via PDCP

Broadcast messages unencrypted

Fronthaul packets NOT integrity-protected

The community undervalues integrity protection

The O-RAN ALLIANCE Security Work Group

O-RAN security specifications view integrity protection as optional:

R1) MITM attacks over fronthaul assumed unlikely (802.1X)

The community undervalues integrity protection

O-RAN ALLIANCE

The O-RAN ALLIANCE Security Work Group

O-RAN security specifications view integrity protection as optional:

R1) MITM attacks over fronthaul assumed unlikely (802.1X)

In contrast to the accepted security stance, we observe that

O1) MITM attacks are practical and feasible over fronthaul

- Public space deployment mode (sidewalks, rooftops, basements)

Source: https://www.lightreading.com/the-edge-network/the-time-i-visited-a-dish-5g-cell-site

Source: https://www.slideshare.net/slideshow/beginners-different-types-of-ran-architectures-distributed-centralized-cloud/249608150

The community undervalues integrity protection

The O-RAN ALLIANCE Security Work Group

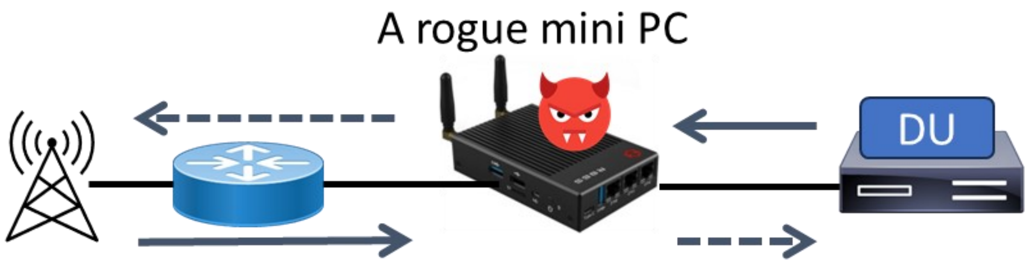
O-RAN security specifications view integrity protection as optional:

R1) MITM attacks over fronthaul assumed unlikely (802.1X)

In contrast to the accepted security stance, we observe that

O1) MITM attacks are practical and feasible over fronthaul

- Public space deployment mode (sidewalks, rooftops, basements)
- Not data center setting
- 802.1X can be bypassed [1]



[1] Alva Duckwall. A Bridge Too Far: Defeating Wired 802.1x with a Transparent Bridge Using Linux. https://av.tib.eu/media/ 40535, 2013.

The community undervalues integrity protection

O-RAN
ALLIANCE

The O-RAN ALLIANCE Security Work Group

O-RAN security specifications view integrity protection as optional:

R1) MITM attacks over fronthaul assumed unlikely (802.1X)

R2) Adversaries assumed to require costly sophistication (PDCP)

In contrast to the accepted security stance, we observe that

O2) Unsophisticated adversaries can directly manipulate traffic

- PDCP is incomplete
- Broadcast messages unprotected
- Pre-attachment messages before key negotiation unprotected

The community undervalues integrity protection

O-RAN ALLIANCE

The O-RAN ALLIANCE Security Work Group

O-RAN security specifications view integrity protection as optional:

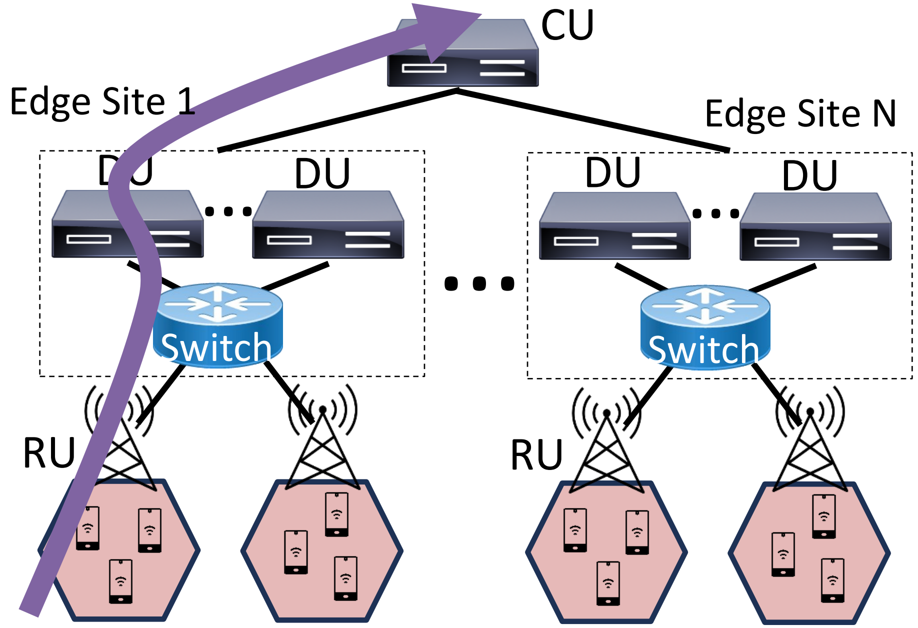
R1) MITM attacks over fronthaul assumed unlikely (802.1X)

R2) Adversaries assumed to require costly sophistication (PDCP)

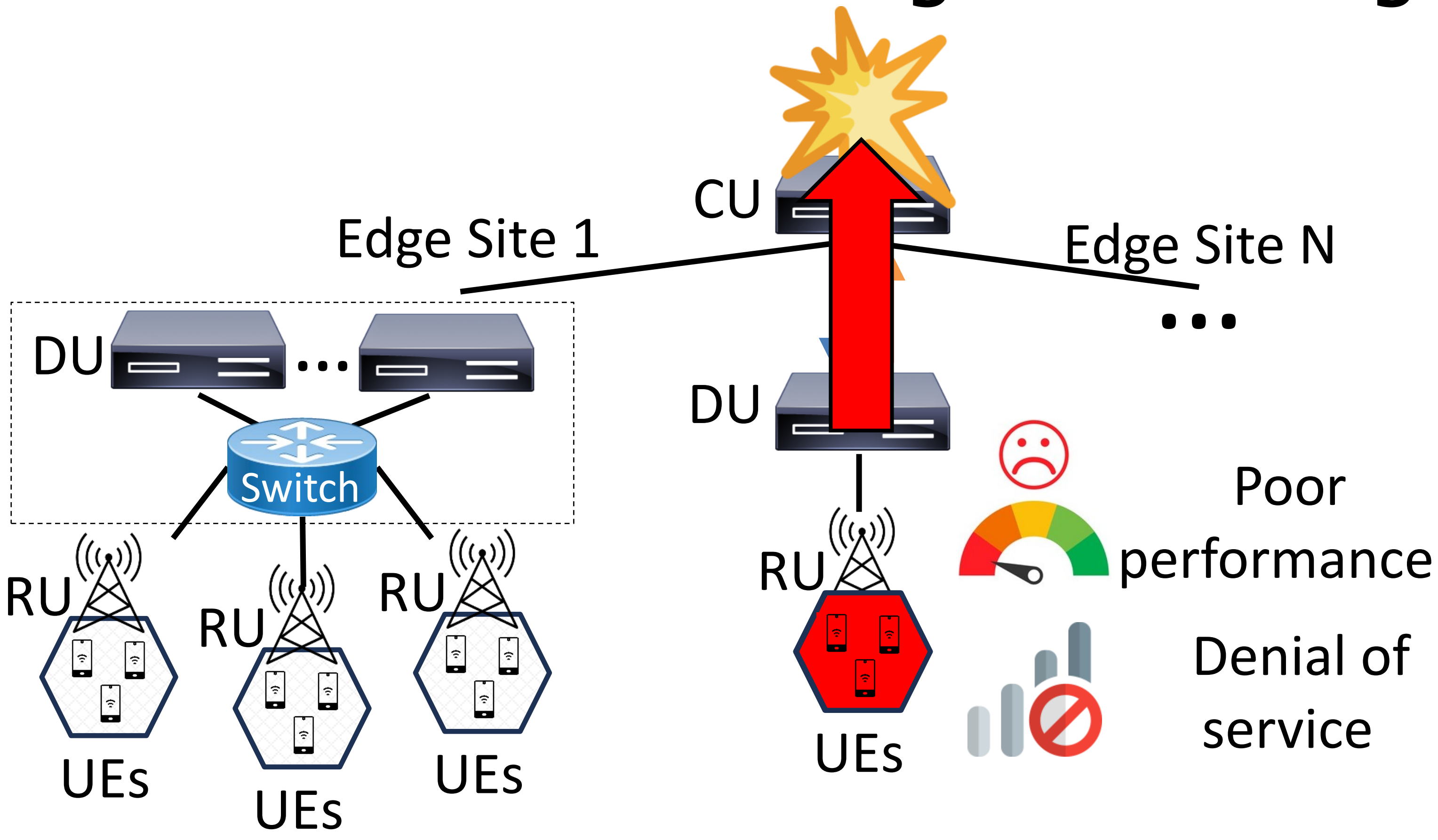
R3) Potential attacks assumed to have low severity (Single DU Impact)

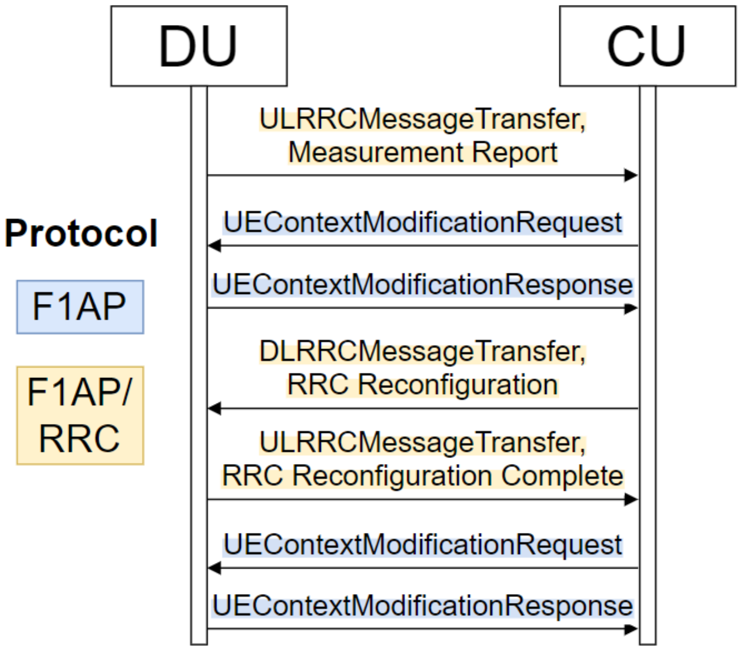
In contrast to the accepted security stance, we observe that

O3) Attacks can be highly severe, impacting large geographical regions



FrontStorm: Flooding CU with signaling storm

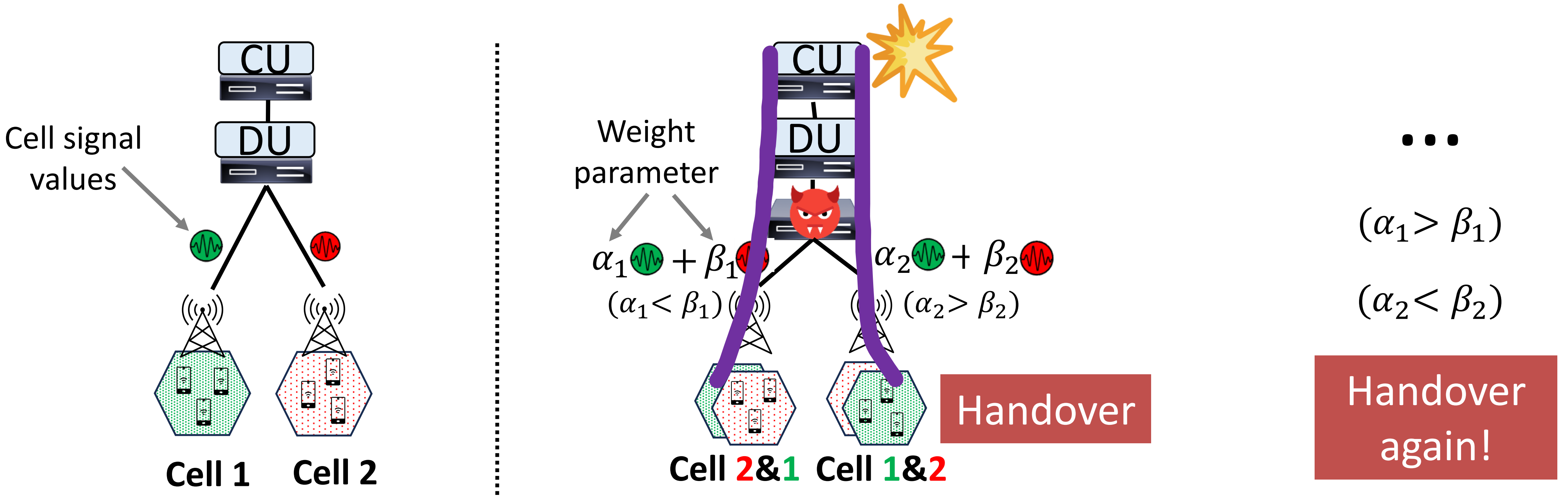



DU
CU
Protocol
F1AP
F1AP/ RRC
ULRRCMessageTransfer, Measurement Report
UEContextModificationRequest
UEContextModificationResponse
DLRRCMessageTransfer, RRC Reconfiguration
ULRRCMessageTransfer, RRC Reconfiguration Complete
UEContextModificationRequest
UEContextModificationResponse

Cell Handover Sequence

- Normally, DU and CU exchange messages infrequently
  - E.g., cell handover, cell reselection
- Attack: Flooding CU with a large amount of messages
  - Degraded performance, DoS, can affect a large geographical area

FrontStorm example: Handover signaling storm



Normal@Time0

L: Only Cell 1

R: Only Cell 2

Attack@Time1

L: Cell2 is better

R: Cell1 is better

Attack@Time2

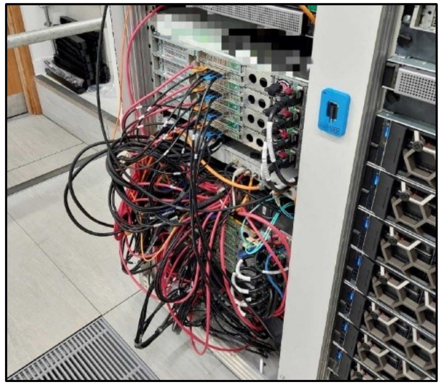
L: Cell1 is better

R: Cell2 is better

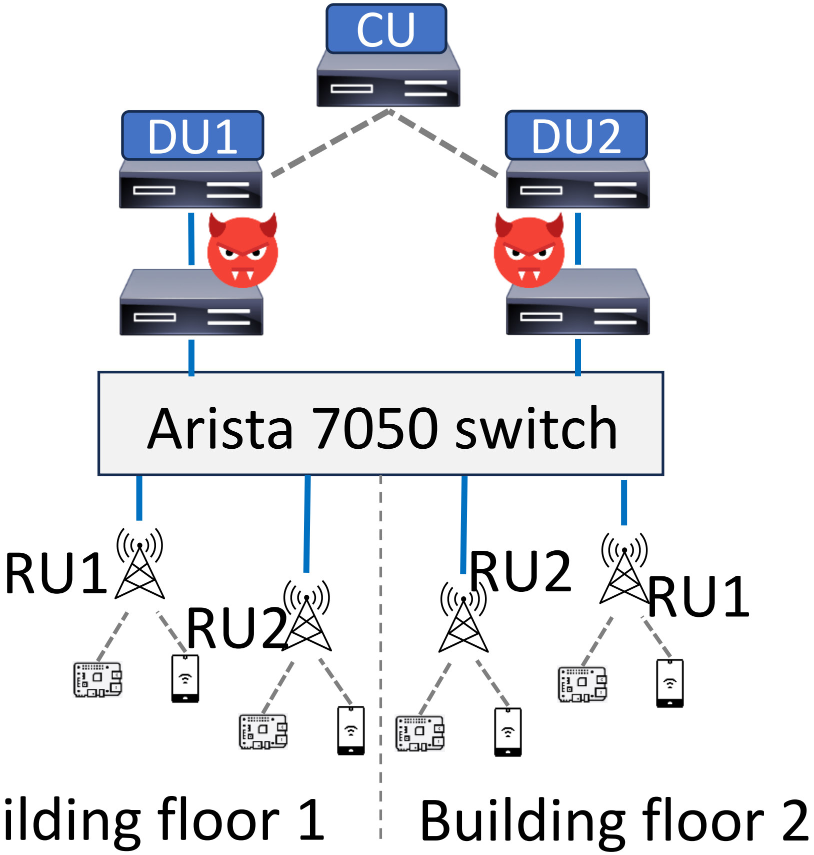
- Multiplexing the signal of cells, creating overlapping cells
- Manipulating the signal quality to trigger UE handover
- Flooding the CU with a large volume of handover messages

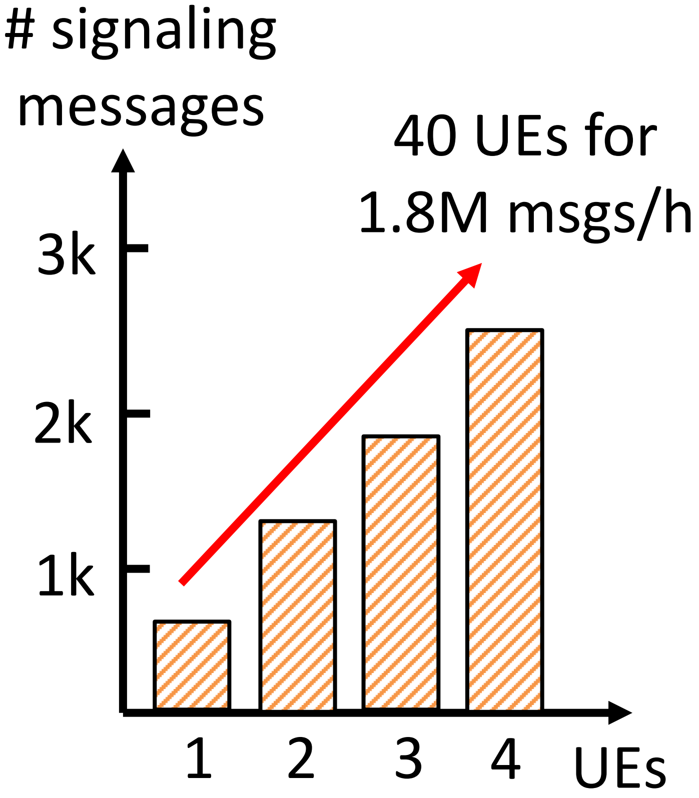
Commercial-grade testbed and FrontStorm results

5G O-RAN cluster



Phone and Raspberry Pi UEs





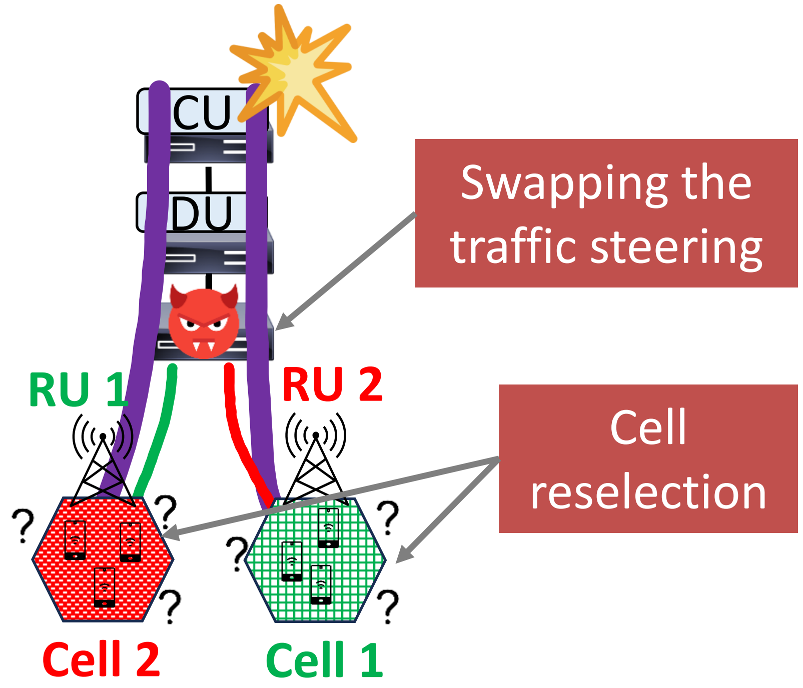
- All testbed components are O-RAN standard compliant
- Attackers manipulate fronthaul packets via a DPDK-based middlebox
- Frontstorm results: 40UEs can generate 1.8M messages per hour

Other high-impact attacks in a nutshell

FrontStorm attacks

A1: Signaling Storm via Handover

A2: Signaling Storm via Cell Reselection



Swapping the traffic steering

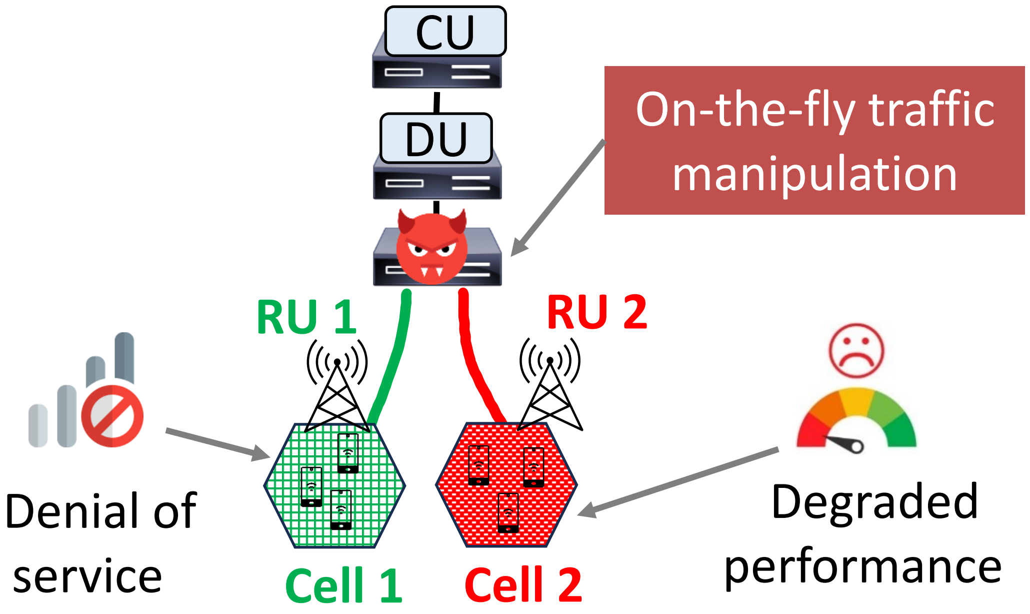
Cell reselection

FrontStrike attacks

A3: Payload Corruption

A4: Downlink SSB Modification

A5: Uplink PRACH Modification



On-the-fly traffic manipulation

Denial of service

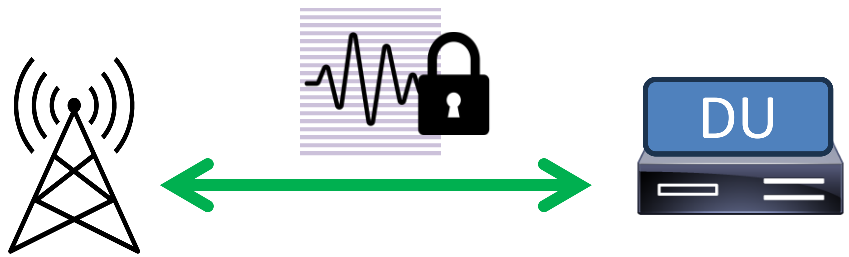
Degraded performance

No need for radio transmitter, can affect many cell simultaneously

Potential countermeasures

Fundamental solution: Fronthaul MACsec

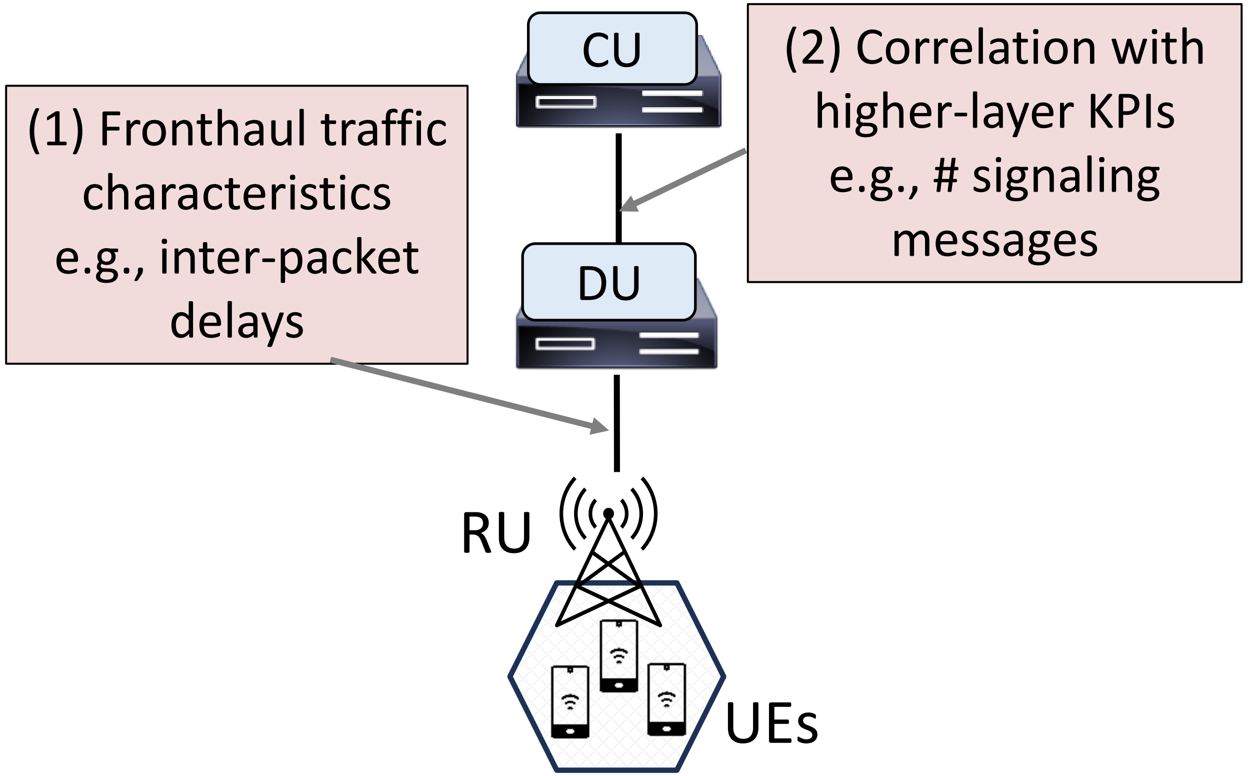
(Media Access Control Security)



Ether Hdr	…	Payload	**ICV**

Could take time to update standards and software/hardware

Immediate solution: Real-time anomaly detection



(1) Fronthaul traffic characteristics e.g., inter-packet delays

(2) Correlation with higher-layer KPIs e.g., # signaling messages

Effective immediate detection

Summary

- Community underestimates 5G RAN fronthaul MITM attacks
  - MITM attacks unlikely? Practical and feasible!
  - Require costly sophistication? Unsophisticated adversaries!
  - Low severity? Impacting large geographical regions!

- Two types of attacks validated on a commercial-grade testbed
  - **FrontStorm:** Introducing signaling storms at CU
  - **FrontStrike:** Manipulating fronthaul packets on the fly
  - No need for transmitter, can affect many cell simultaneously!

- Reassess criticality + mandatory need for fronthaul integrity protection