JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

11100 Johns Hopkins Road
Laurel, MD 20723-6099

ISART 2020 Plenary Sessions: O-RAN and 5G Design — Resiliency at the Radio Layer

Uplink Jamming and Denial of Service: Push detection and mitigation techniques to the edge

Pam Patton – pamela.patton@jhuapl.edu

Communications at JHU/APL

A Research Division of Johns Hopkins University - University Affiliated Research Center (UARC)

Nuclear Command and Control Communications (NC3)

Since the 1970s, APL has been a leader in NC3 system evaluation to include performance measurement, modeling and simulation, and cyber assessment.

Satellite Communications (SATCOM)

Since the 1980s, APL contributions have been integral in defining new SATCOM systems and developing communications architectures for satellite and payload control.

Cooperative Engagement Capability (CEC) Data Distribution System (DDS)

The DDS was designed by APL to provide several orders of magnitude more communications capability relative to conventional tactical data links for coordinating naval engagements across multiple platforms.

Senior Leader Communications

APL is a leader in US government efforts to evolve and protect strategic national communication systems, including spearheading the initiative that enabled senior national leaders to use the latest commercial mobile devices for critical missions.

Special Users

APL's ability to rapidly prototype operational communications capabilities that meet very specific and tailored requirements has benefited special users across multiple domains.

Advanced Communications Technology Development

APL's early adoption and application of software defined radios (SDRs) is just one example of how APL continuously stays at the forefront of emerging technologies for solving critical challenges.

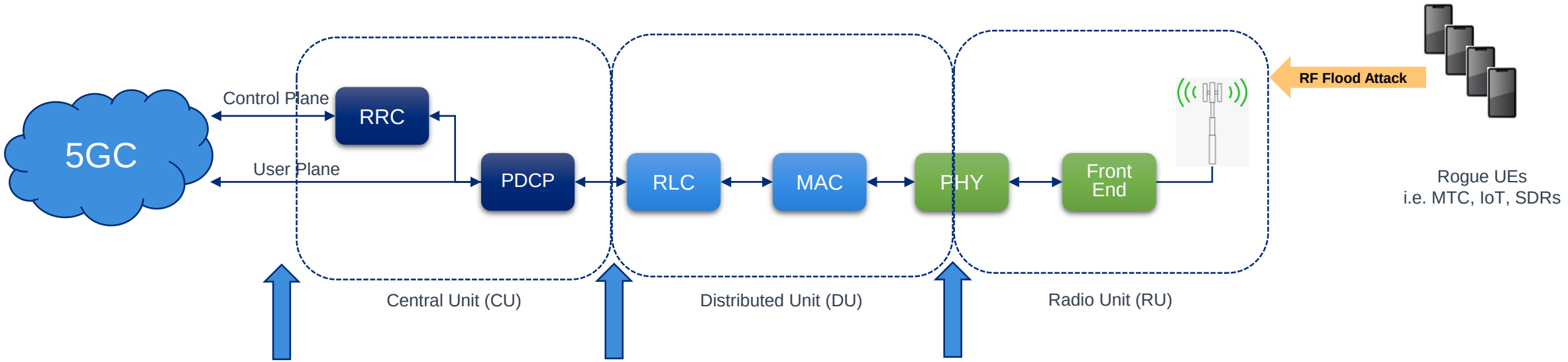
5G Security Advancements - 3GPP Standards and Technical Reports

- 3GPP TS 33.501 5G; Security architecture and procedures for 5G System (Release 15)
  - Focuses on enhancing integrity, confidentiality, and authentication protocols within the network architecture
  - New service based interfaces, signaling procedures, identity protection, key derivation and exchanges
  - Security mechanisms for protecting the internals of the gNB at the F1 and E1 interfaces with a focus on integrity protection, replay protection and confidentiality protection
- 3GPP TS 33.5xx security specifications per network component

- 3GPP TR 33.809 Technical Specification Group Services and System Aspects - Study on 5G Security Enhancement against False Base Stations (Release 16)
  - Addresses the RAN interface security to protect the UE access and confidentiality
  - Does not address interference jamming or RAN attacks

Majority of the security features focus on the network side, after the RAN, for integrity, confidentiality, and authentication. They do not effectively address resiliency of the RF interface

Uplink Jamming and Denial of Service: Push detection and mitigation techniques to the edge



- The introduction of massive machine type communication, massive simultaneous IoT devices, and low latencies can greatly tax a Firewall or DPI system responding OTA threats in the core network.
- Add monitor points in the RAN Management Plane at the CU, DU, and RU to decrease response time in the event of an OTA attack
- The CU will most likely have more compute power for ML and AI algorithms to detect the threat and mitigate the jamming
- Does not rely on an O-RAN architecture but an open interface standard can open up the market for non-RAN vendors to develop security products

JOHNS HOPKINS

APPLIED PHYSICS LABORATORY