Supported in part by Oak Ridge National Laboratory

5G NR JAMMING, SPOOFING, AND SNIFFING: THREAT ASSESSMENT AND MITIGATION

Vuk Marojevic
WIRELESS@VIRGINIA TECH
maroje@vt.edu

Marc Lichtman
Vencore Labs

Raghunandan Rao and **Jeffrey Reed**
Wireless@Virginia Tech

Roger Piqueras Jover
Bloomberg LP

RFnest-2

RF Switches

CMW500

RF Switches

RF Switches
+ Filters

RFnest-1

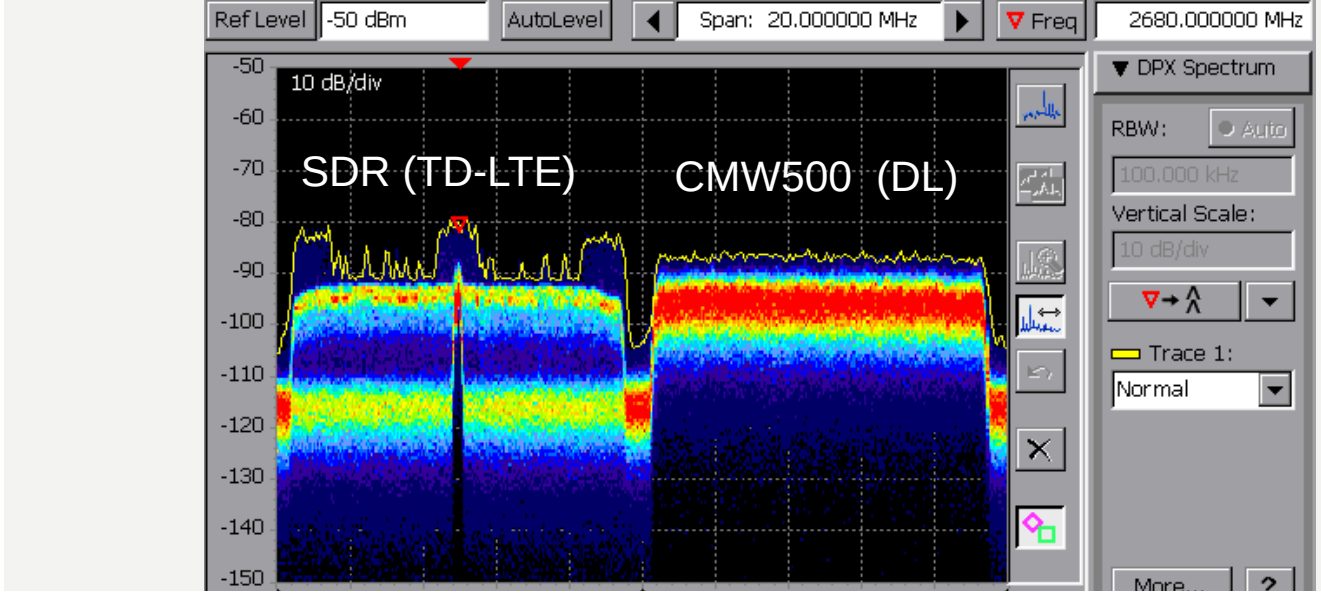
Ethernet Switch

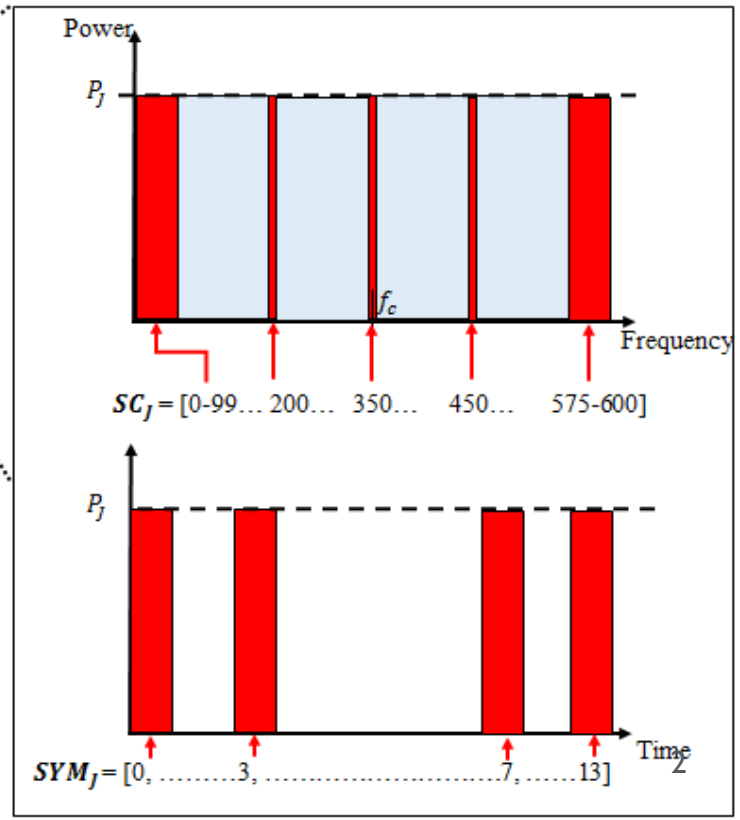
Dir. Couplers
+ RF Switches

N210 USRPs

OctoClock

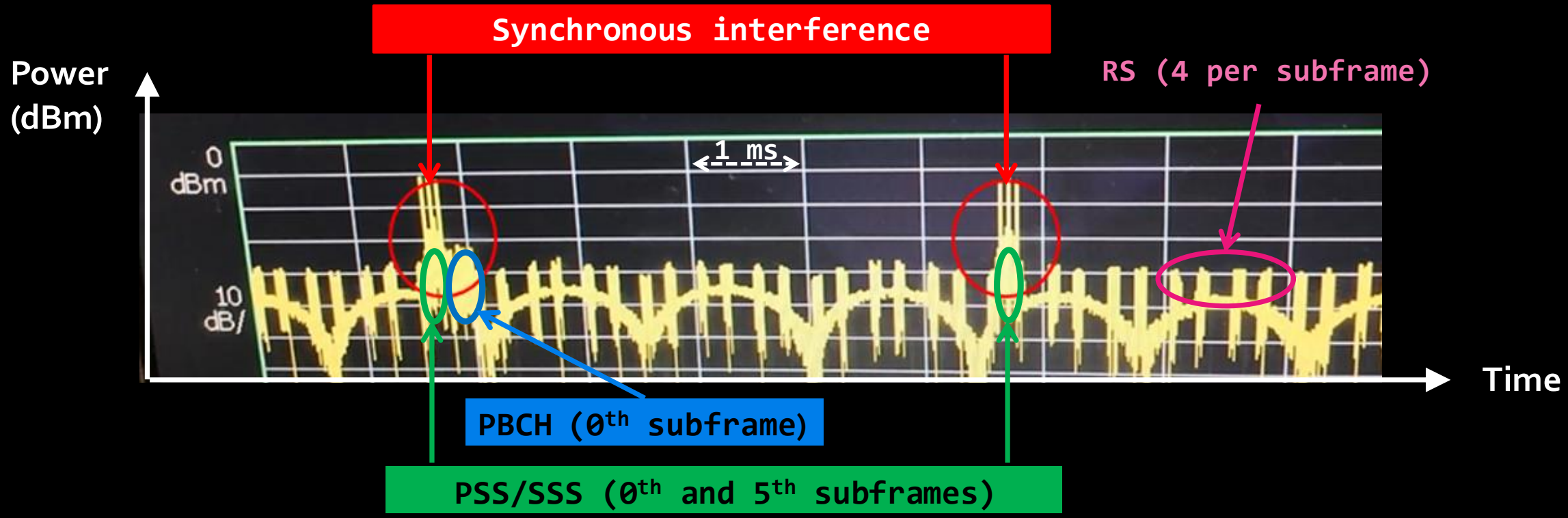
SDR PCs





V. Marojevic, R. Nealy, J.H. Reed, "LTE spectrum sharing research testbed: integrated hardware, software, network and data," *Proc. ACM WiNTECH'17*, Oct. 2017, *https://arxiv.org/abs/1710.02571*

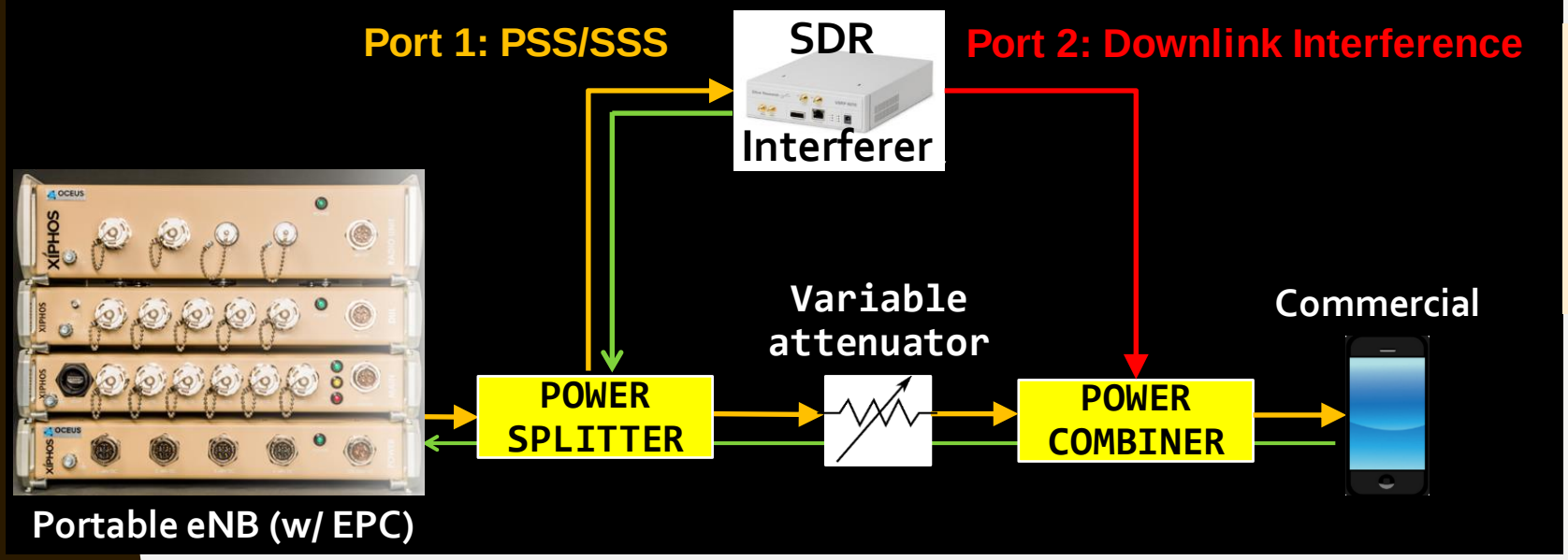
Synchronous Interference – Specific Physical Signals/Channels



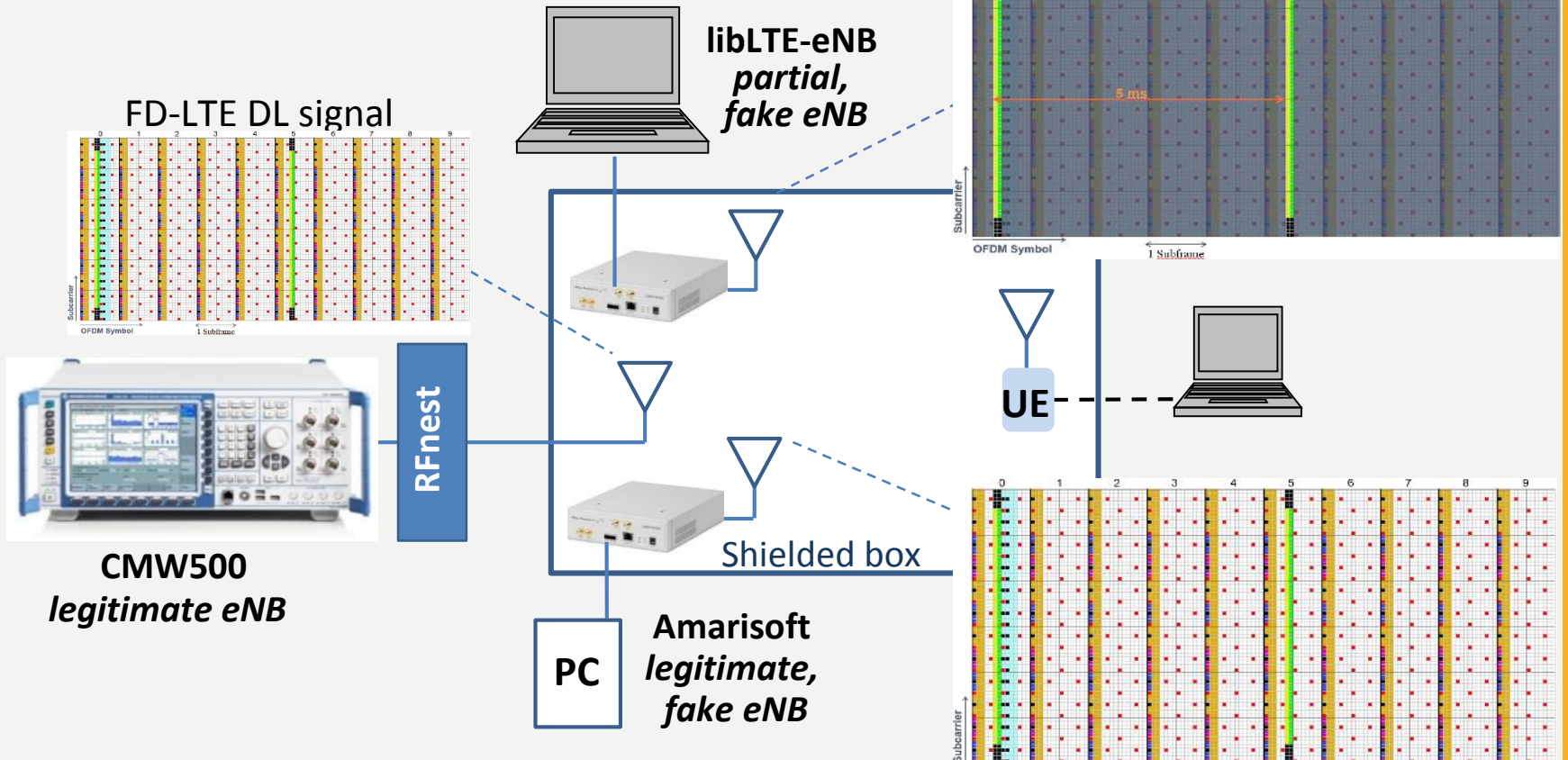
Simplified LTE downlink frame with PSS, SSS, RS, and PBCH

PSS, SSS: Sync. Signals RS: Reference Signal PBCH: Physical Broadcast Channel

R. Rao, et al., "LTE PHY Layer Vulnerability Analysis and Testing Using Open-Source SDR Tools," *Proc. IEEE MILCOM*, Oct. 2017



V. Marojevic, et al., "Performance analysis of a mission-critical portable LTE system in targeted RF interference," *IEEE VTC Fall 2017, https://arxiv.org/abs/1708.06814*



M. Labib, et al., "Enhancing the robustness of LTE systems: analysis and evolution of the cell selection process," *IEEE Commun. Mag., Feb. 2017*

OUTLINE

1. Introduction and Motivation
2. Background on 5G NR
3. Physical Layer Vulnerabilities
4. Overall Vulnerability Assessment
5. Brief Survey of Mitigation Techniques
6. Conclusions

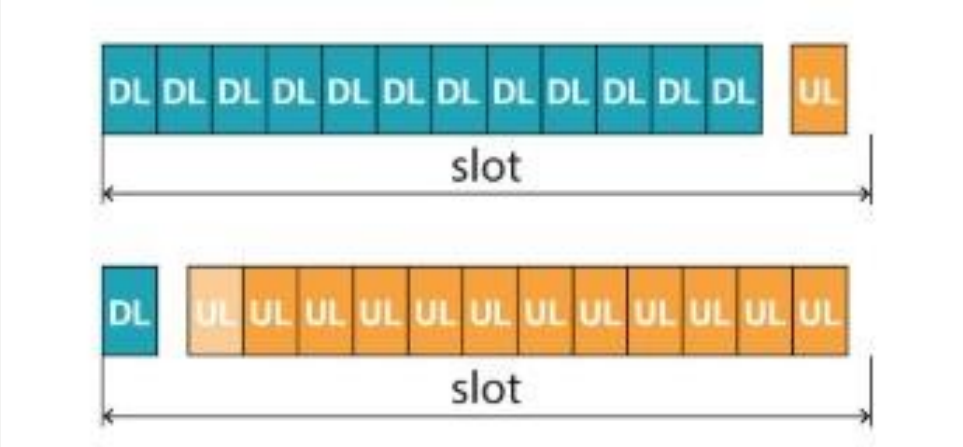
INTRODUCTION AND MOTIVATION

- As we saw with LTE, lower layer security is low on the priorities during creation of specifications
- Commercial cellular is never created with the intention of use in mission-critical contexts
- There is a large community focused on higher layer attacks
- While jamming is always possible, we do *not* want extremely efficient protocol-aware jamming attacks to exist
- This presentation will focus on the PHY layer of 5G NR

FirstNet

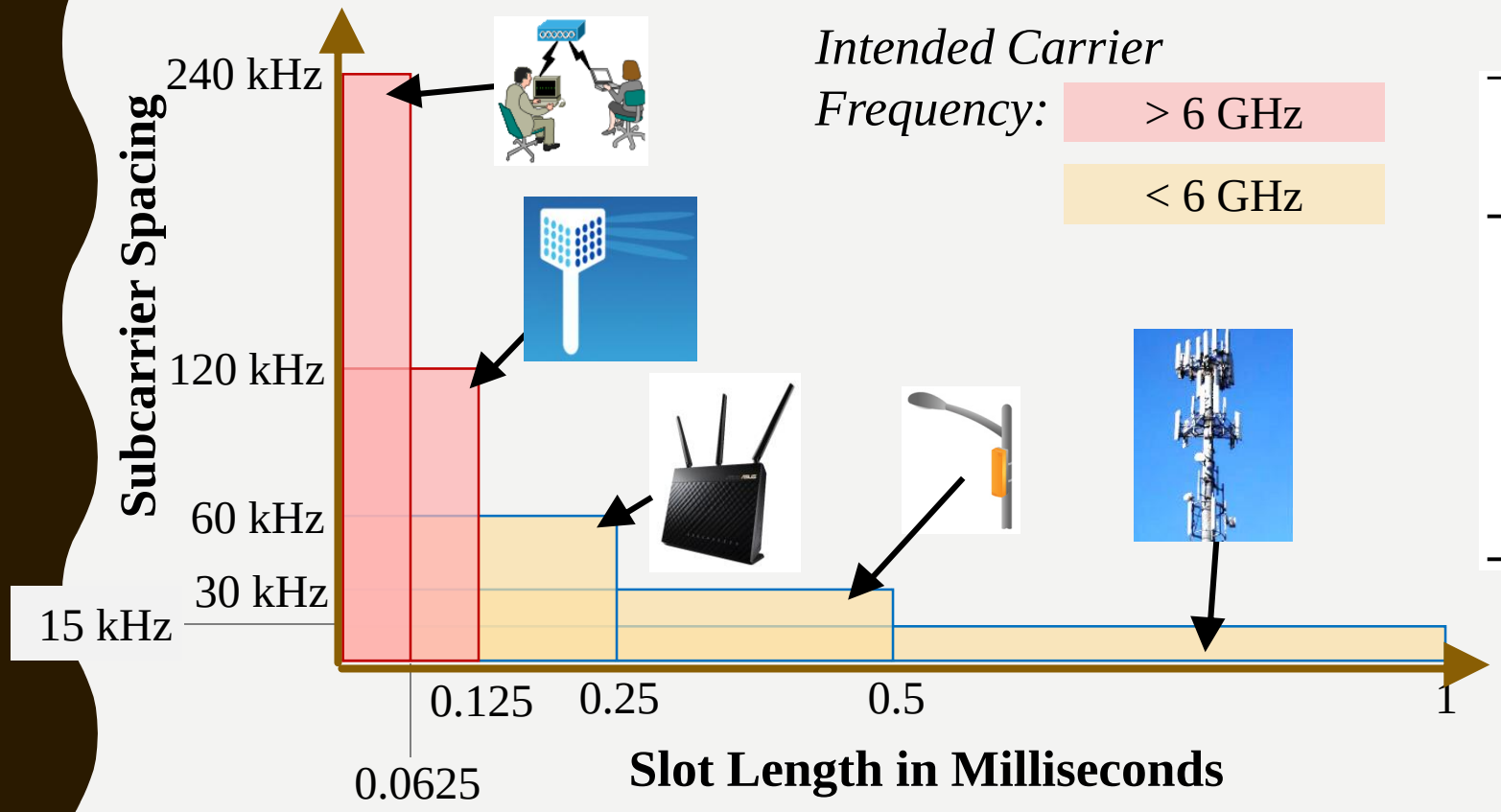
BACKGROUND OF 5G NR

- First set of specs released December 2017
- Largely based on LTE, but with more dynamic aspects
- Intended to operate in *any* spectrum (below 1GHz to 100 GHz)
- Allows for lower latency modes
- More dynamic frame structure, allows different fractions of UL/DL



NUMEROLOGIES

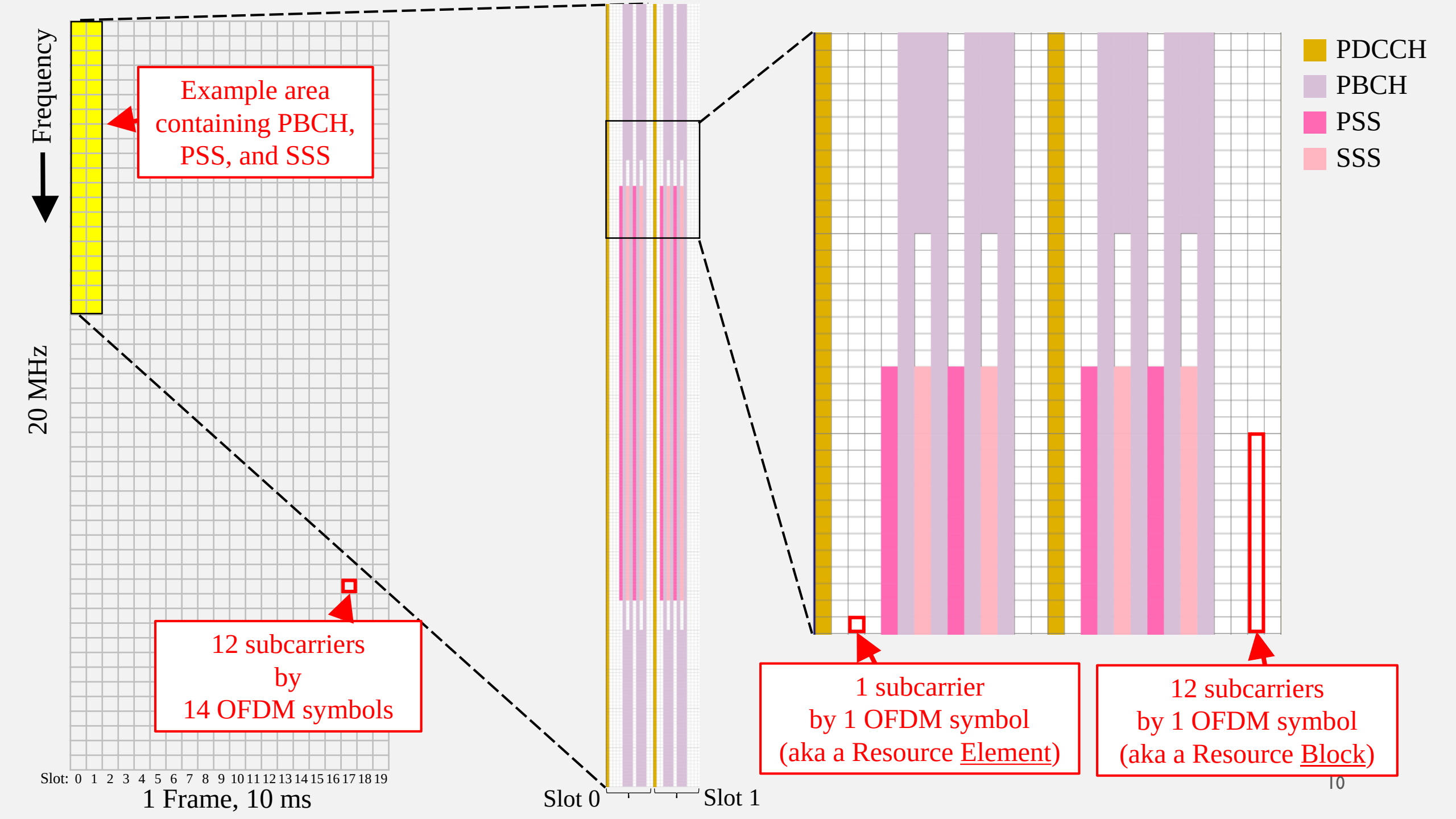
- Several different configurations exist to cover a wide range of applications
- Five different options for subcarrier spacing



Subcarrier Spacing	Slots per Subframe	Meant for Carriers...
15 kHz	1	< 6 GHz
30 kHz	2	
60 kHz	4	
120 kHz	8	> 24 GHz
240 kHz	16	

FRAME STRUCTURE

- Similar to LTE, 5G NR uses OFDM and thus information is mapped onto a time-frequency lattice
- This leads to the ability for a jammer to selectively target physical channels in both time and frequency, to achieve a jamming gain
- Most of the frame consists of data symbols, with pilot symbols mixed in at regular intervals (we do not zoom in enough to show pilots)
- Critical information such as the PSS, SSS, and MIB are allocated to a very small fraction of the entire frame
- On the next slide we show an example mapping of these channels; on the left is the entire frame, and we show 2 stages of "zooming in"


Frequency
20 MHz
Example area containing PBCH, PSS, and SSS
12 subcarriers by 14 OFDM symbols
Slot: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
1 Frame, 10 ms
Slot 0
Slot 1
PDCCH
PBCH
PSS
SSS
1 subcarrier by 1 OFDM symbol (aka a Resource Element)
12 subcarriers by 1 OFDM symbol (aka a Resource Block)

PHYSICAL LAYER VULNERABILITIES

5G NR SYNCHRONIZATION SIGNALS

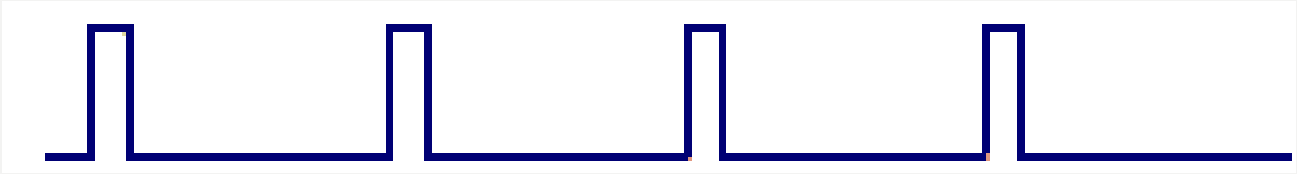
- Largely the same as LTE, although there are more configurations of channel mapping
- PSS and SSS still exist, but are not statically located in frequency
- PSS spoofing is still feasible, although the jammer will now have to transmit more fake PSS's in order to cover all possible PSS locations
- Specific behavior of PSS spoofing is still based on the chipset and the sophistication of the blacklisting mechanism

PHYSICAL BROADCAST CHANNEL (PBCH)

- Transmitted in same slots at PSS and SSS, but over 240 subcarriers
- Carries MIB, which contains the basic parameters such as subcarrier spacing and position of control channels
- Sent in the clear, a smart-jammer would use this information to selectively jam a physical channel
- A jammer targeted the PBCH itself would appear to have a very low duty cycle and only occupy a small fraction (~20%) of the downlink signal bandwidth

DOWNLINK CONTROL CHANNEL (PDCCH)

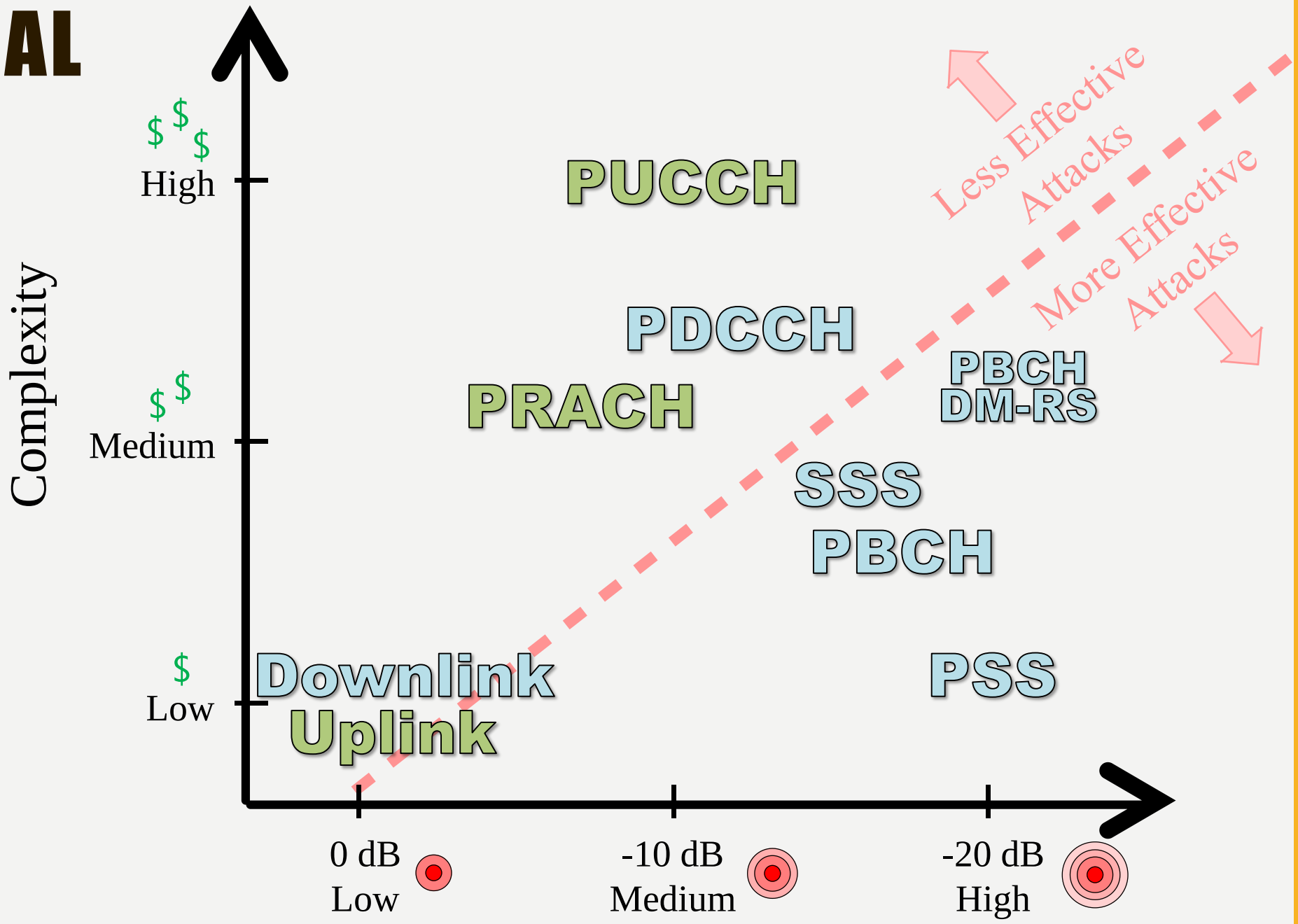
- Used to send control information to the UE on a per-slot basis
- Can appear on any subcarrier, but always starts in the first symbol of each slot
- A jammer selectively targeting the PDCCH would have to decode a couple of system parameters sent in the SIBs
- To target every UE a jammer would have to jam every subcarrier, but only with a duty cycle around 10%
- Such a low-duty-cycle attack could also act as a form of automatic gain control jamming



Channel/Signal	Modulation	Coding
PDSCH (Downlink)	{4, 16, 64, 256}-QAM	LDPC
PBCH	QPSK	Polar
PDCCH	QPSK	Polar
PUSCH (Uplink)	{4, 16, 64, 256}-QAM	LDPC
PUCCH	QPSK	Variety
PRACH	Zadoff-Chu Sequence	N/A
PSS (Spoofing)	M-Sequences	N/A
SSS	Gold Sequences	N/A
PBCH DM-RS	QPSK	N/A

% of REs	Synch. Required	Params. Required	J/S_{CH}	J/S_F
90%	No	None	0 dB	-1 dB
1.7%	Yes	None	0 dB	-17 dB
7%	Yes	Medium	0 dB	-11 dB
$\sim$ 90%	No	None	0 dB	-1 dB
$\sim$ 10%	Yes	High	0 dB	-10 dB
$\sim$ 2%	Yes	Medium	10 dB	-7 dB
0.1% (3 PSSs)	No	None	10 dB	-20 dB
0.3%	Yes	None	10 dB	-15 dB
0.4%	Yes	Low	3 dB	-21 dB

GRAPHICAL RANKING



OVERALL VULNERABILITY ASSESSMENT

- PCFICH in LTE was an extremely sparse downlink control channel that was vital to the link – removed in 5G NR
- Many control channels now have a much more dynamic allocation
- Requires jammer to decode parameters to know channel assignments, adds complexity to the jamming attack
- 5G NR in general has many different configurations
- Uplink control channel is not longer in the same portion of the band

BRIEF SURVEY OF MITIGATION TECHNIQUES

- The most practical mitigation techniques are those that only require changes to base station software
  - UE behavior is baked into the chipset and not easily modified
  - Mitigation at the eNodeB allows for certain mission critical 5G deployments to have additional protection
- **PSS spoofing** can be mitigated using a PSS-only blacklist, and a timer used to identify a PSS without an associated SSS and/or MIB
  - Unfortunately this must be done at the UE side
  - Chipset designers are likely to assume that if there is a PSS then there is an SSS, they are adjunct in time/freq and at the same power level
- **Sniffing** mitigation requires limiting SIB content to strictly what is necessary to establish a radio link with the base station
  - Further network configuration elements should be shared on a secured and integrity protected broadcast channel
- **Detection** of smart-jamming attacks is feasible because the eNodeB can simply monitor for an excess amount of energy on any one specific physical channel (e.g. using masking)

CONCLUSION

- Many improvements made over LTE
- 5G NR is highly dynamic which will provide robustness
- Still a few weak points that should be addressed
- PSS Spoofing mitigation can occur within the chipset implementation
- Detection of PBCH jamming/sniffing and higher layer attacks may be needed in mission-critical applications of 5G NR
- More research is needed, this study did not focus on finding "new" attack vectors

(ONGOING WORK)
5G-SYSTEM NAS VULNERABILITIES

5G-SYSTEM CORE NETWORK

- Work to address some protocol exploits
  - IMSI obfuscation and encryption
  - PKI for message authentication
- Security standards published in March 2018
  - 3GPP TS 33.501 V1.0.0 (2018-03)

5G-SYSTEM SECURITY

- Security cornerstone → Operator public key/certificate on SIM
  - What happens when roaming?
  - Very hard to reach global agreement so an operator "trusts" certificates from all other countries
- Too many vulnerable security edge cases
  - "If the home network has not provisioned the public key in USIM, the SUPI protection in initial registration procedure is not provided. In this case, the null-scheme shall be used by the ME."
  - Null ciphering and null integrity still supported
  - "The provisioning and updating of the home network public key is out of the scope of the present document. It can be implemented using, e.g. the Over the Air (OTA) mechanism."
  - Etc…

QUESTIONS?

REFERENCES

[1] 3GPP, "Study on New Radio Access Technology Physical Layer Aspects," 3rd Generation Partnership Project (3GPP), TS 38.802, 2017. [Online]. Available: http://www.3gpp.org/dynareport/38802.htm

[2] ——, "Physical channels and modulation (Release 15)," 3rd Generation Partnership Project (3GPP), TS 38.211, Dec. 2017. [Online]. Available: http://www.3gpp.org/dynareport/38211.htm

[3] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, "LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation," *IEEE Communications Magazine*, vol. 54, no. 4, 2016.

[4] V. Marojevic, R. M. Rao, S. Ha, and J. H. Reed, "Performance analysis of a mission-critical portable LTE system in targeted RF interference," in *IEEE VTC*, September 2017.

[5] M. Lichtman, J. H. Reed, T. C. Clancy, and M. Norton, "Vulnerability of LTE to hostile interference," in *IEEE Global Conference on Signal and Information Processing (GlobalSIP)*. IEEE, 2013, pp. 285–288.

[6] 3rd Generation Partnership Project, Technical Specification Group Radio Access Network, "NR - Radio Resource Control (RRC) Protocol specification. 3GPP TS 38.331," vol. v1.0.0, 2017.

[7] R. P. Jover, "LTE security, protocol exploits and location tracking experimentation with low-cost software radio," *CoRR*, vol. abs/1607.05171, 2016. [Online]. Available: http://arxiv.org/abs/1607.05171

[8] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical attacks against privacy and availability in 4G/LTE mobile communication systems," in *Network and Distributed System Security Symposium*, 2016.

[9] 3GPP, "NR and NG-RAN Overall Description (Release 15)," 3rd Generation Partnership Project (3GPP), TS 38.300, Dec. 2017. [Online]. Available: http://www.3gpp.org/dynareport/38300.htm

[10] D. Adamy, *EW 101: A first course in electronic warfare*. Artech house, 2001, vol. 101.

[11] F. Ercan, C. Condo, S. A. Hashemi, and W. J. Gross, "On error-correction performance and implementation of polar code list decoders for 5G," in *Allerton Conference on Communication, Control, and Computing*, 2017.

[12] R. M. Rao, S. Ha, V. Marojevic, and J. H. Reed, "LTE PHY layer vulnerability analysis and testing using open-source SDR tools," in *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, Oct 2017, pp. 744–749.

[13] M. Lichtman, J. D. Poston, S. Amuru, C. Shahriar, T. C. Clancy, R. M. Buehrer, and J. H. Reed, "A communications jamming taxonomy," *IEEE Security & Privacy*, vol. 14, no. 1, pp. 47–54, 2016.

[14] M. Labib, V. Marojevic, J. H. Reed, and A. I. Zaghloul, "Enhancing the robustness of LTE systems: Analysis and evolution of the cell selection process," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 208–215, February 2017.

[15] R. P. Jover, "Some key challenges in securing 5G wireless networks," *FCC filling PSHSB 16-353*, January 2017, https://ecfsapi.fcc.gov/file/10130278051628/fcc_submit.pdf.

"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development (NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674, Fax: 202-459-9673, Email: nco@nitrd.gov, Website: https://www.nitrd.gov