Vulnerabilities of LTE to RF Interference and Spoofing

Mina Labib, Vuk Marojevic,
Carl Dietrich, Jeffrey H. Reed

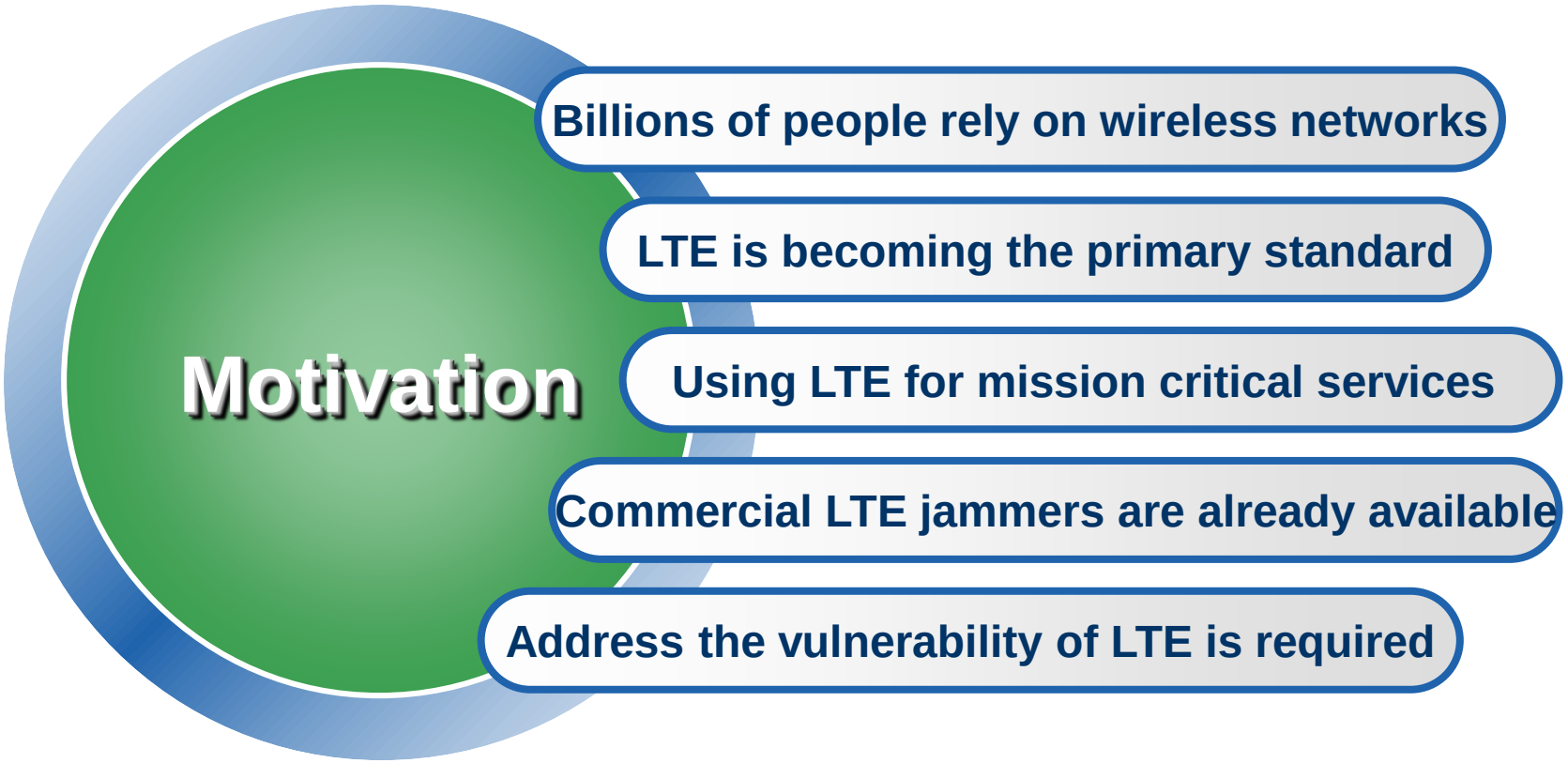
Wireless@Virginia Tech (http://wireless.vt.edu)
Bradley Department of Electrical and Computer Engineering
Blacksburg, VA

VirginiaTech
Invent the Future

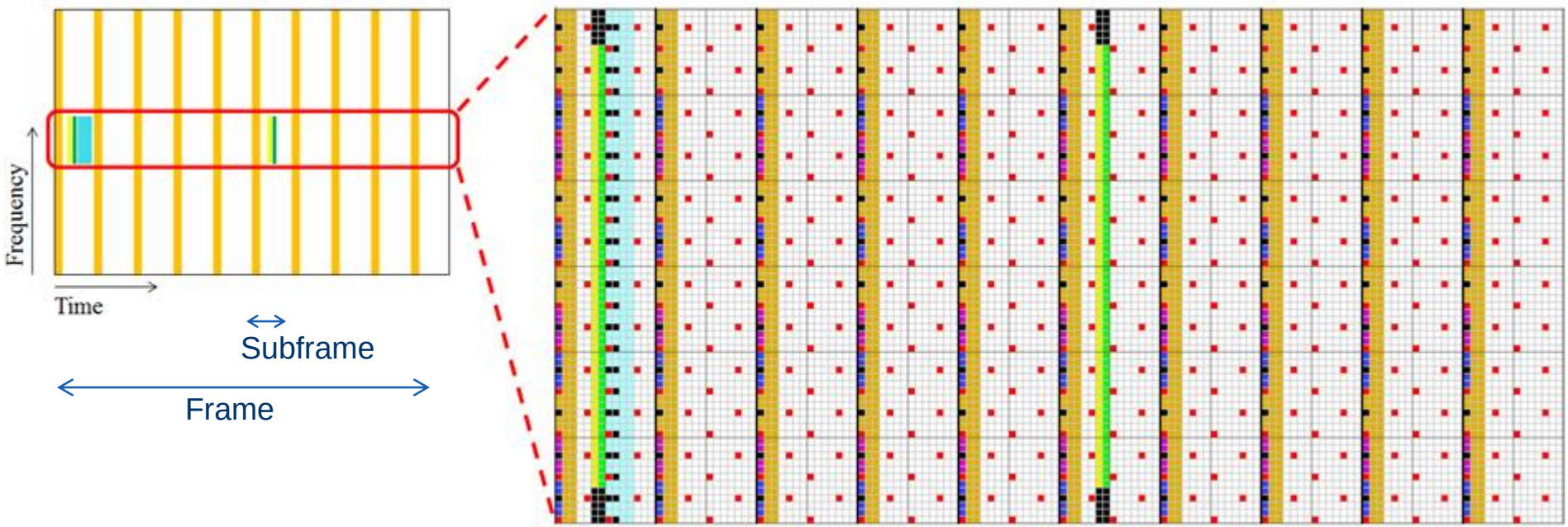
Wireless @ Virginia Tech

Contents

Introduction



LTE Downlink

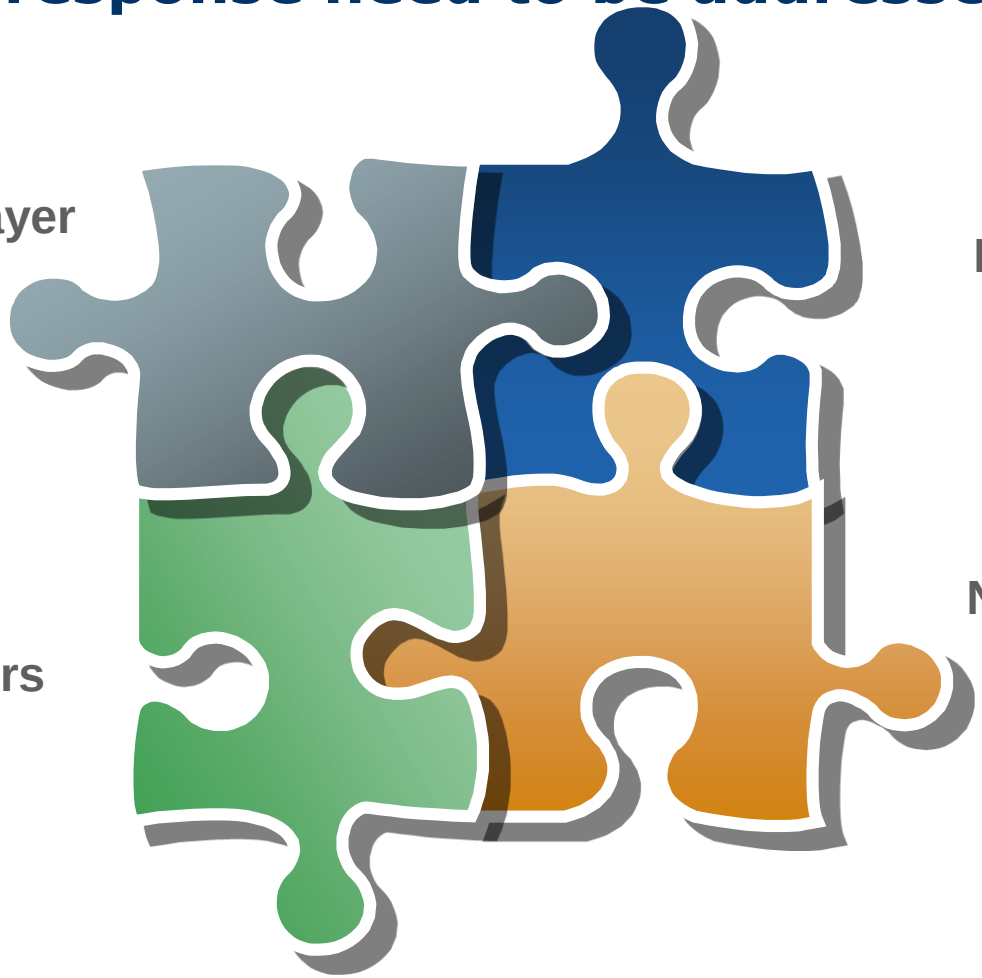


- Control Format Indicator Channel (PCFICH)
- Hybrid ARQ Indicator Channel (PHICH)
- Downlink Control Channel (PDCCH)
- Downlink Shared Channel (a.k.a. Data)
- Primary Synchronization Signal (PSS)
- Secondary Synchronization Signal (SSS)
- Broadcast Channel (PBCH)
- Reference Signals (a.k.a. Pilots)
- Unused

- 32 REs in 1st OFDM symbol of every subframe
- REs in 1st OFDM symbol of every subframe
- 1-4 OFDM symbols every subframe
- Most OFDM symbols
- 1 OFDM symbol (62 subcarriers) every half-frame
- 1 OFDM symbol (62 subcarriers) every half-frame
- 4 OFDM symbols (72 subcarriers) every frame
- 4 REs every RB

Approach

Analysis of the physical layer only is not enough: Upper layers response need to be addressed



Metrics

Interference Power

How to estimate the needed interference power to lead to wrong message decoding channels

Jamming Effectiveness

How to measure the effect of the jammer on the system

Complexity Metric:The Big-O

How to define the complexity of the jamming

Interference Power

Jamming to signal ratio per **resource element** (RE)

The base unit

Jamming to signal ratio per radio **frame**

Power consumption of the jammer (on average)

Jamming to signal ratio per **OFDM symbol** or **instantaneous J/S**

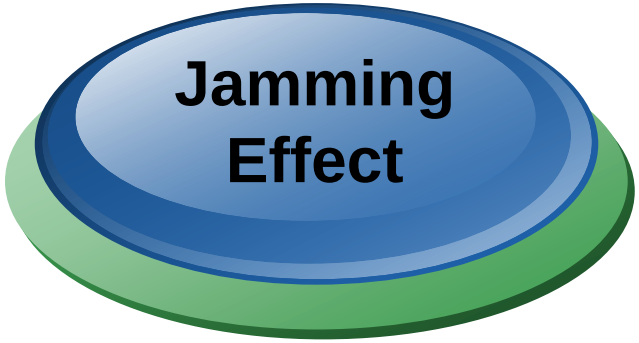
Most accurate way to describe the required J/S.

Mapping between the J/S_{RE} to J/S_{OFS} and J/S_F for 10 MHz BW

10 MHz LTE

	Channel	# of RE per 12 subcarriers (RB) where applies	# of RE per OFDM symbol where applies	# of REs per frame	Ratio of J/S_{RE} to J/S_{OFS}	Ratio of J/S_{RE} to J/S_F
DL	RS	2	100	4000	0.166666667	0.04761905
	PSS	12	62	124	0.103333333	0.00147619
	SSS	12	62	124	0.103333333	0.00147619
	PBCH	12	72	288	0.12	0.00342857
	PDSCH	10 or 12	500 or 600	Dynamic	0.8333 or 1	Dynamic
	PCFICH	4	16	160	0.026666667	0.00190476
	PDCCH	0-12	600	0-1800	1	0.02142857
UL	PUSCH	12	504	70560	0.84	0.84
	PUCCH	12	96	13440	0.16	0.16

Effectiveness of Jamming



Control Message Error Rate

The percentage of incorrectly decoded control channel messages

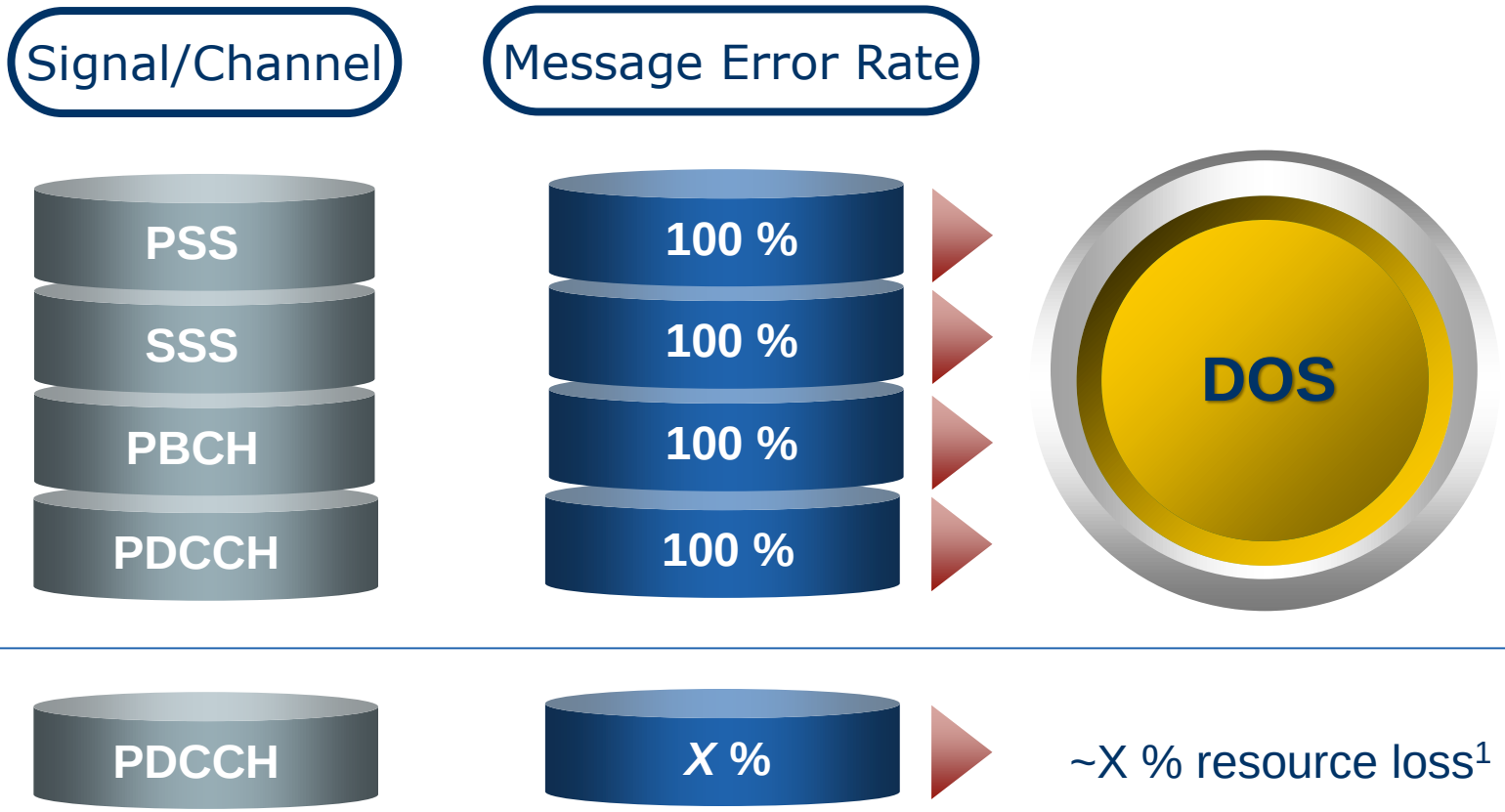
Throughput

More accurate way to measure the effectiveness of the jammer.

E.g.,

- 50% throughput drop
- DOS (0% throughput)

Estimated Message Error Rate for DOS



[1] X % of active UEs wrongly decode PDCCH at uniform resource demand

Complexity Metric

- **We can classify the interference-generation procedures using the following categories:**
  - *Corse Synchronization*: acquire PSS signal
  - *Tight Synchronization*: complete the cell search process
  - *Frequency Discontinuity*: transmit over non-contiguous sub-bands
  - *Time Discontinuity*: <100 % duty cycle

Complexity Analysis

Jamming/ Spoofing	Corse Sync	Tight Sync	Frequency Discontinuity	Time Discontinuity	Big-O	Complexity
RS	Yes	Yes	Yes (extremely)	Yes (extremely)	8	**Very High**
PSS	Yes	No	No	Yes	3	Medium
PDSCH (Barrage)	No	No	No	No	0	Very Low
PBCH	Yes	Yes	No	Yes	5	**High**
PCFICH	Yes	Yes	Yes	Yes	6	**Very High**
PDCCH	Yes	Yes	No	Yes	5	**High**
PUSCH (Barrage)	No	No	No	No	0	Very Low
PUCCH	Yes	Yes	Yes	No	5	**High**
PSS Spoofing	No	No	No	Yes	1	Low
Cell Spoofing	Yes/No	Yes/No	Yes	Yes	(4-8)+	**Extremely High**

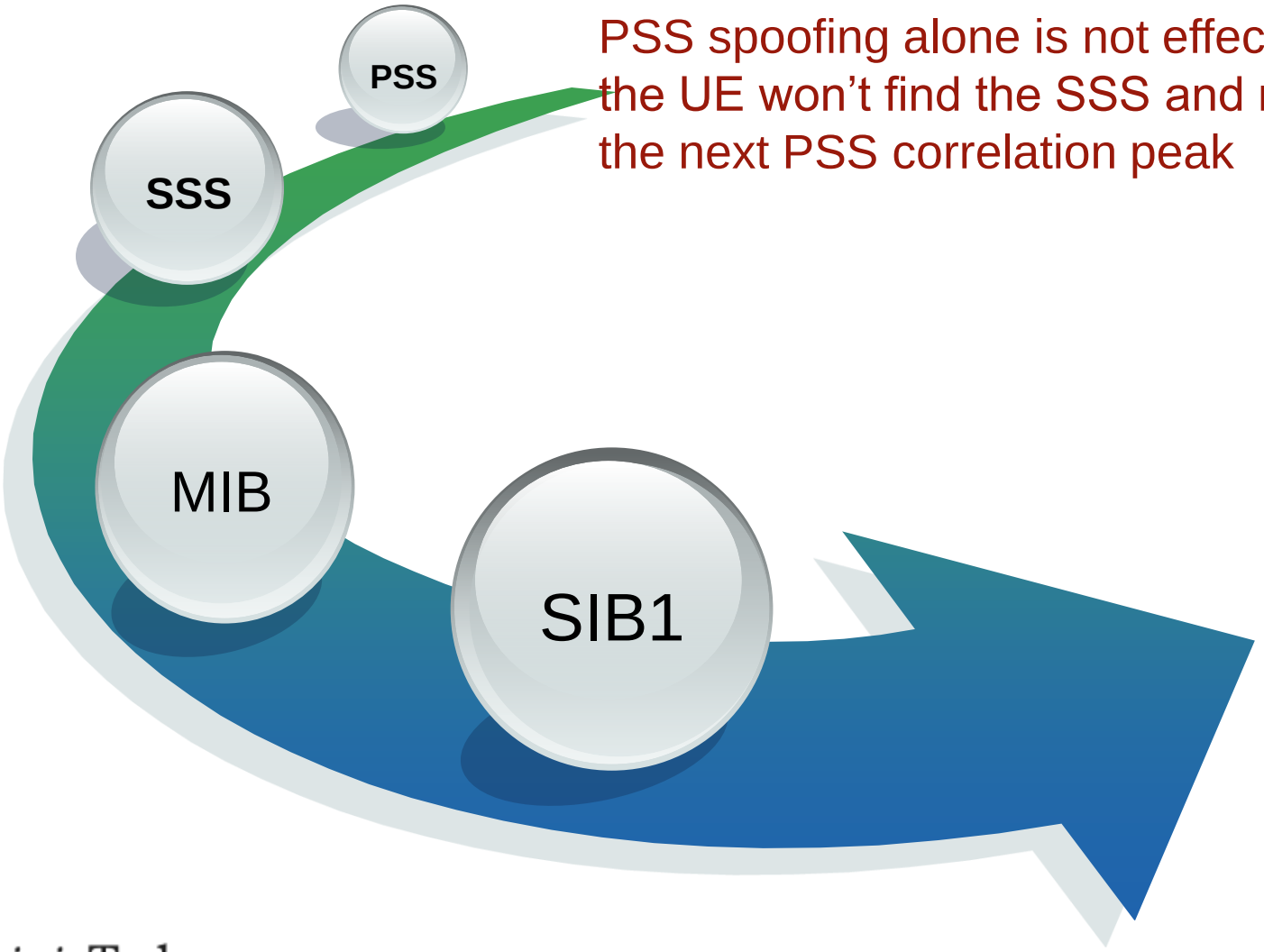
Remarks

- ***Control channel interference: potential threat***
- Different control channel attacks analyzed
- Metrics:
  - J/S_{OFDM}
  - Interference waveform generation complexity
- Findings:
  - **LTE Cell Spoofing:** Potentially critical threat, interesting to explore
  - **PBCH** critical threat
  - **PDCCH** critical threat (once the PBCH is decoded)

LTE Control Channel Spoofing

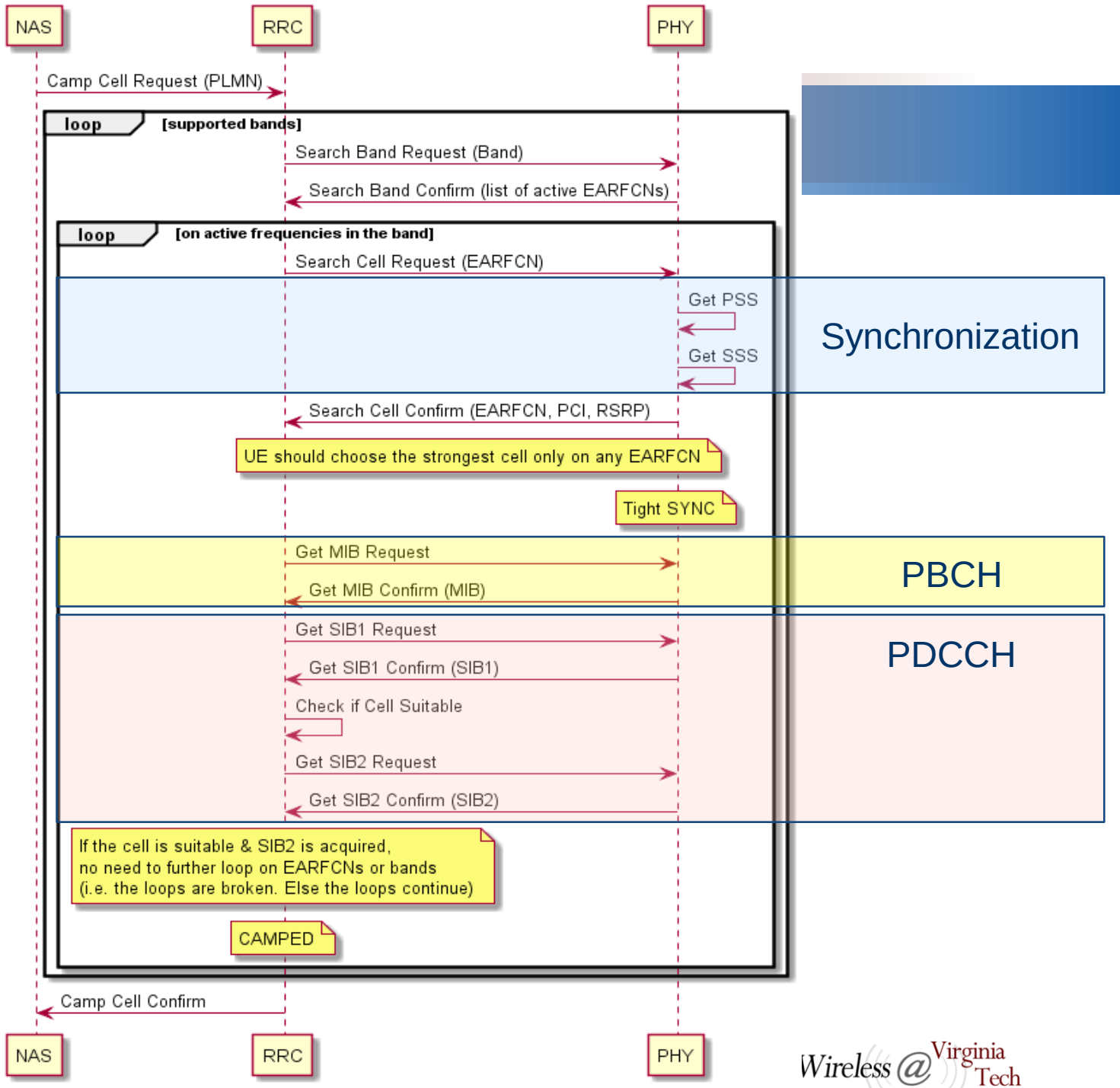
Wireless @ Virginia Tech

Cell Selection at the PHY Layer



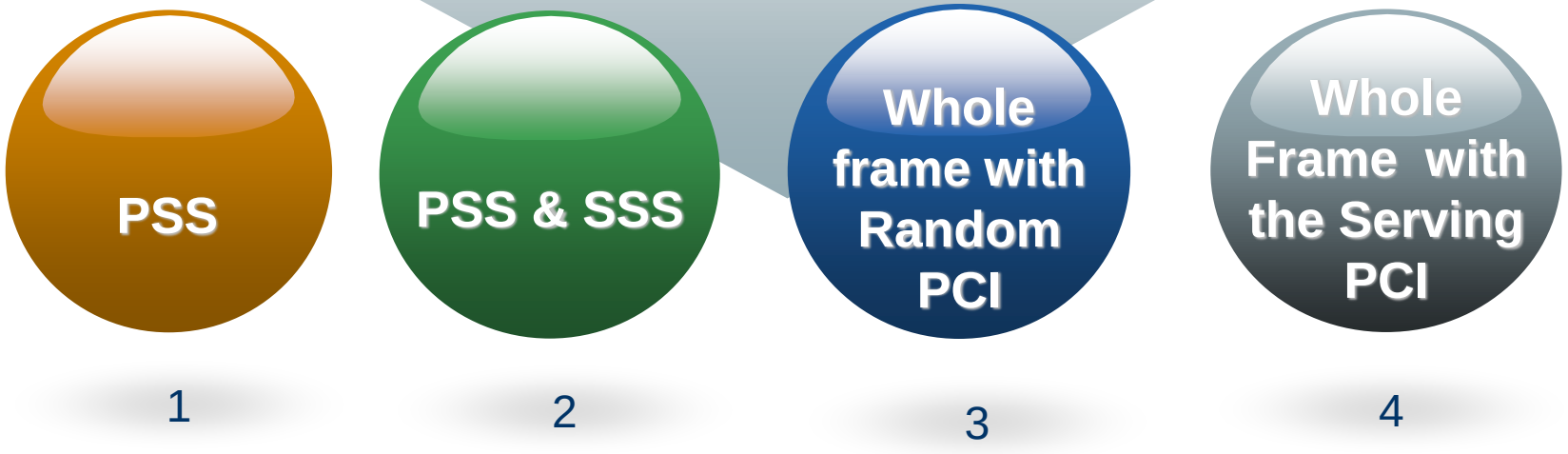
PSS spoofing alone is not effective as the UE won't find the SSS and move to the next PSS correlation peak

Successful Cell Selection



LTE Spoofing

Levels of Spoofing



PSS

PSS Spoofing

- If the PHY detects the highest power coming from the bogus PSS, it will wrongfully assume it is valid LTE PSS signal.
- The PHY won't find the SSS in the expected location, so the it will not be finish the time synchronization.
- The PHY will not be able to report receiving this PSS to the RRC layer and hence it will ignore this PSS and likely consider the second highest correlation peak in the band
- Conclusion: **PSS Spoofing is not viable!**

PSS & SSS

2. PSS & SSS Spoofing

- If the UE detects the highest power coming from the bogus PSS and finds the corresponding SSS, it will wrongfully assume synchronized and transfer the PCI to the RRC layer
- RRC layer will instruct the PHY to get the MIB, which will fail as the jammer doesn't broadcast this channel
- The standard specifies ***"the UE need only search for the strongest cell"***
  - RRC layer will instruct the PHY to move to the next frequency
- Conclusion: **Potential threat!**

Whole frame with Random PCI

3. Cell Spoofing with Random PCI

- The cell selection process will go all the way until confirming the PLMN to the NAS layer
- The NAS will start the registration process with the fake eNB but will fail as there is no security key sent by this eNB
  - The NAS will flag this cell as “barred” and indicate this to the RRC
- The standard states: ***RRC shall keep this cell as barred for 300 seconds***
- The RRC layer reads the SIB1 message…

The SIB1 Message

Only Showing part of the SIB1. Source (3GPP TS 36.331)

***SystemInformationBlockType1* field descriptions**
cellBarred barred means the cell is barred, as defined in TS 36.304 [4].
cellReservedForOperatorUse As defined in TS 36.304 [4].
csg-Identity Identity of the Closed Subscriber Group the cell belongs to.
csg-Indication If set to TRUE the UE is only allowed to access the cell if it is a CSG member cell, if selected during manual CSG selection or to obtain limited service, see TS 36.304 [4].
ims-EmergencySupport Indicates whether the cell supports IMS emergency bearer services for UEs in limited service mode. If absent, IMS emergency call is not supported by the network in the cell for UEs in limited service mode.
intraFreqReselection Used to control cell reselection to intra-frequency cells when the highest ranked cell is barred, or treated as barred by the UE, as specified in TS 36.304 [4].
multiBandInfoList A list of additional frequency band indicators as defined in TS 36.101 [42, table 5.5-1] that the cell belongs to. If the UE supports the frequency band in the *freqBandIndicator* IE it shall apply that frequency band. Otherwise, the UE shall apply the first listed band which it supports in the *multiBandInfoList* IE. If E-UTRAN includes *multiBandInfoList-v9e0* it includes the same number of entries, and listed in the same order, as in *multiBandInfoList* (i.e. without suffix). See Annex D for more descriptions.
plmn-IdentityList List of PLMN identities. The first listed *PLMN-Identity* is the primary PLMN.
p-Max Value applicable for the cell. If absent the UE applies the maximum power according to the UE capability.
q-QualMin Parameter "$Q_{qualmin}$" in TS 36.304 [4]. If *cellSelectionInfo-v920* is not present, the UE applies the (default) value of negative infinity for $Q_{qualmin}$.
q-QualMinOffset Parameter "$Q_{qualminoffset}$" in TS 36.304 [4]. Actual value $Q_{qualminoffset}$ = IE value [dB]. If *cellSelectionInfo-v920* is not present or the field is not present, the UE applies the (default) value of 0 dB for $Q_{qualminoffset}$. Affects the minimum required quality level in the cell.
q-RxLevMinOffset Parameter $Q_{rxlevminoffset}$ in TS 36.304 [4]. Actual value $Q_{rxlevminoffset}$ = IE value * 2 [dB]. If absent, the UE applies the (default) value of 0 dB for $Q_{rxlevminoffset}$. Affects the minimum required Rx level in the cell.

Faking the SIB1 Message

- ***IntraFreqReselection*** enabled:
  - UE will be allowed to find a suitable cell within the same frequency without adhering to the *strongest cell rule*
  - The UE may will eventually find the correct cell and camp on it
- ***IntraFreqRelection*** disabled:
  - UE will not be allowed to search for another cell at the same frequency
- Conclusion: **Potential threat!**

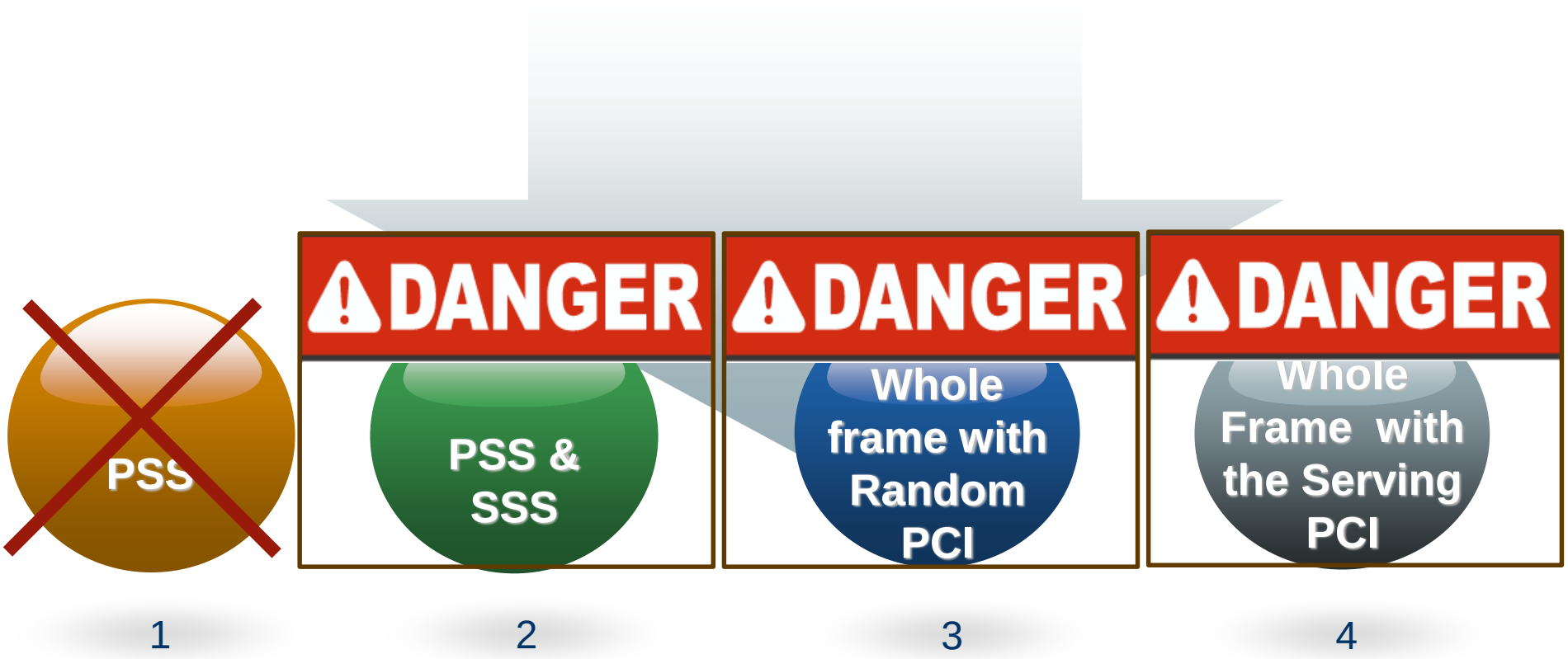
Whole Frame with the Serving PCI

4. Whole Frame with The Serving PCI

- Same as previous…RRC will keep the cell as barred for 300 s
  - Since the RRC labels the cell by frequency and its PCI, the attacker has succeeded to bar the correct cell by copying its PCI
    - requires synchronizing (PSS and SSS)
  - ***IntraFreqReselection*** enabled: UE may find a **neighboring** cell within the same operator and attach to it
  - ***IntraFreqReselection*** disabled: UE will search for a cell at a different frequency
- Furthermore, the attacker can fake the "cellbarred" field in the SIB1 message to prevent the new UEs from attaching to this cell

LTE Spoofing

Levels of Spoofing



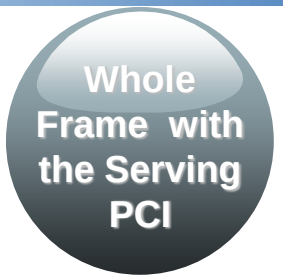
Possible Mitigation Techniques

1

- *"The UE need only search for the strongest cell **except…**"*:

2

- The RRC layer to ignore SIB1 message from any cell that was not authenticated by the NAS



3&4

3- The RRC checks for cells with same PCI.
4- The PHY to identify cells with more parameters than PCI (TOA)

LTE Control Channel Jamming Mitigation

PBCH

PDCCH

VirginiaTech
Invent the Future

Wireless @ Virginia Tech

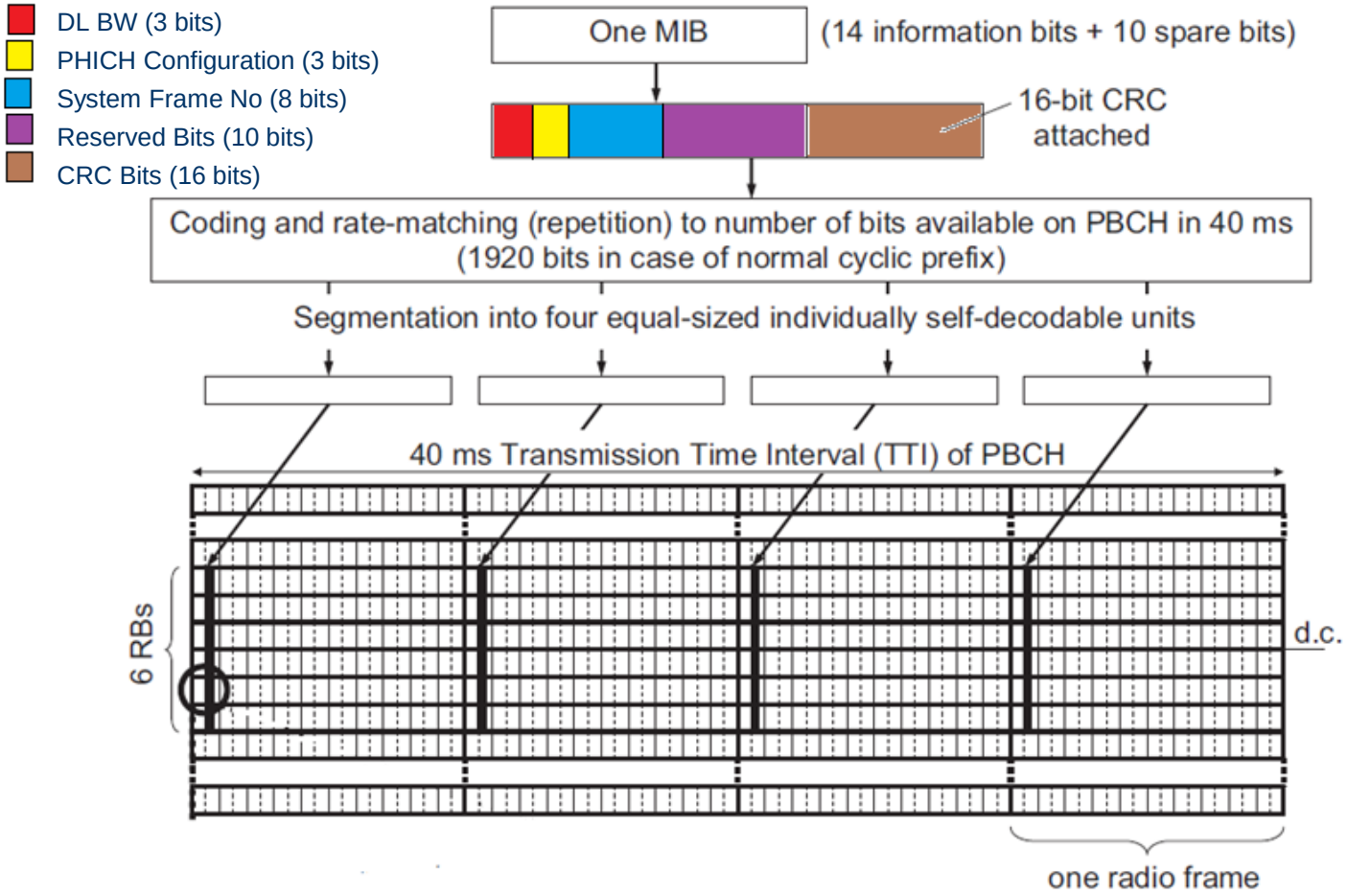
Physical Broadcast Channel (PBCH)

- The purpose of the Physical Broadcast Channel is providing critical access information in the form of the Master Information Block (MIB):
  - Downlink channel bandwidth (3 bits)
  - PHICH configuration (3 bits)
  - System Frame Number (most 8 significant bits)
  - Reserved bits (10 bits)

- The 16 CRC bits are added to the 24 bits in the MIB message. The CRC provides the error-check and provide the number of antenna ports as the CRC bits are masked with a code word representing the number of antenna ports.

- Each PBCH message within one frame is self-decodable. The UE will be able to identify the least 2 significant bits from the phase of the scrambling code.

Physical Broadcast Channel (PBCH)



Source: "LTE: The UMTS long term evolution: from theory to practice" pp. 191

Mitigation Techniques for PBCH (1)

1. **Frequency hopping**:
   - PBCH occupies 72 center sub-carriers, which corresponds to the minimum LTE system BW (1.4 MHz or 6 RBs)
   - UE initially not aware of the system BW, but most can operate on 5, 10, or 20 MHz LTE system => blind BW decoding to decode rest of PBCH

2. **Utilizing the reserved bits**:
   - 10 reserved bits can used to enhance the robustness of the PBCH
   - E.g., repeated transmission of the System Frame Number

3. **Sending the MIB in PDCCH**:
   - 14 MIB bits could be accommodated within the PDCCH (in addition to sending it in the PBCH to check for consistency).

Mitigation Techniques for PBCH (2)

4. **Fixed BW**:
   - BW can be fixed (as UEs will belong to the same military network)
   - Spare 3 bits can be used to repeat the PHICH configuration

5. **Sending the BW in different channels**:
   - UE gets critical information from the PSS & SSS (synchronization, FDD/TDD, cyclic prefix length). Very robust signals.
   - BW information might be included in the PSS/SSS or in a separate signal of similar properties to the SSS) => *robust BW detection*

6. **Subframe Interleaving**:
   - A second level of interleaving can be added by interleaving the REs of the PBCH within the same RB across the whole subframe (14 OFDM symbols) after multiplexing with PDSCH

Mitigation Techniques for PBCH (3)

7. **Changing the convolution coding rate**:
   - Coding rate can be ¼ instead of 1/3 with changes to rate matching to maintain same number of output bits

8. **Space Frequency Block Coding (SFBC)**:
   - eNBs with two or four antennas can transmit the PBCH using SFBC
   - SFBC is the frequency-domain version of Alamouti codes and are designed to create transmit diversity
   - Will improve the SNR at receiver and enhance robustness

Comparison of Mitigation Techniques for PBCH

Technique	Technical Feasibility	Regulatory Aspects
Frequency hopping	Requires UEs to look beyond minimum bandwidth of 1.4 MHz	Major changes needed
Utilizing Reserved Bits	Easy to implement	• Minor changes to the standard • Backward compatible
Sending the MIB in PDCCH	BW is not known to the UE: • Blind decoding • Combining after decoding PBCH first	Major changes to the protocol, but might be backward compatible (?)
BW in different signals	Potentially powerful, but requires designing new signal or redesigning the current sync. signals	Major changes, but might be backward compatible (?)
Subframe Interleaving	PHY layer multiplexing at eNB transmitted, demultiplexing at receiver	Changes to the specs, requires modification of DL receiver processing
Changing coding rate	Easy to implement but effectiveness needs to be analyzed	The final number of bits will remain1920 bits → minimum changes to DL PHY layer processing
Space Frequency Block Coding	Robustness of PBCH will increase by exploiting MIMO	No changes as the feature is included in the standard, since Rel. 8

Physical DL Control Channel (PDCCH)

- The PDCCH carries a selection of the following control information, contained in Downlink Control Information (DCI) messages
  - UE-specific scheduling assignments for Downlink (DL) resource allocation
  - Uplink resource grants
  - PRACH responses
  - UL power control commands
  - Scheduling assignments for signaling messages
- The DCI message first gets CRC attached, then QPSK modulated, then encoded using 1/3 Convolutional coding

Mitigation Techniques for PDCCH (1)

1. **Time Interleaving**:
   - A second level of interleaving can be added by interleaving the REs of the PDCCH in time, within the same RB across the whole subframe (14 OFDM symbols) after multiplexing with PDSCH
   - Requires significant changes to UE chipsets and eNodeBs

Mitigation Techniques for PDCCH (2)

2. **Static Resource Assignments**
   - Enter a mode in which resources are allocated to UEs in a static manner (both UL and DL), so that the UE only has to receive the resource assignment once. They may change on the order of minutes.
   - Negates gain from frequency diversity (although resources on opposite ends of the band could still be assigned to one user)
   - It is inefficient; resources would have to be divided across UEs equally
   - PRACH responses must still be sent as normal

3. **Decreasing Resource Scheduling Granularity**:
   - E.g., every 2 subframes → less flexibility in resource allocation, but more redundancy for PDCCH

Comparison of Mitigation Techniques for PDCCH

Technique	Technical Feasibility	Regulatory Aspects
1. Time Interleaving	Feasible, but would require a special chipset and special eNodeB firmware	No issues
2. Decreasing Granularity	Only requires changes to the eNodeB software	No issues
3. Static Allocations	Only requires changes to the eNodeB software	Lack of uplink power control may cause issues

Conclusion

- **PSS interference not practical**
  - requires tight time-alignment and very high J/S_{OFS} due to the excellent correlation properties of the Zadoff-Chu sequence
- **PSS spoofing alone not viable**
- **LTE Control Channel spoofing can be a potential threat**: Mitigation techniques were proposed to address the several spoofing techniques.
- **PBCH very vulnerable** due to ease of interference and its importance
- We proposed **11 unique mitigation techniques** to improve the robustness of the PBCH and PDCCH

Possible Future Work Plan

- **LTE Control Channel Cell Spoofing**
  - Patent/Publication
  - Demo threat
- **PBCH**
  - Implement one or more mitigation technique and simulate improvement
  - Demo threat and mitigation
- **PDCCH**
  - Further investigate possible mitigation techniques.
  - Implement one or more mitigation technique and simulate improvement
  - Demo threat and mitigation

References

- M. Lichtman, J. H. Reed, T. C. Clancy, M. Norton, "Vulnerability of LTE to Hostile Interference," IEEE Global Conference on Signal and Information Processing, Dec. 2013.
- Sean Ha, "Quantifying Signal Jamming Metrics and Proposing Interference Mitigation Strategies for LTE," White Paper, Virginia Tech, July 2014.
- Shahriar, C.; La Pan, M.; Lichtman, M.; Clancy, T.C.; McGwier, R.; Tandon, R.; Sodagari, S.; Reed, J.H., "PHY-Layer Resiliency in OFDM Communications: A Tutorial," *Communications Surveys & Tutorials, IEEE* , vol.PP, no.99, pp.1,1
- Jaber Kakar, Kevin McDermott, Vidur Garg, Marc Lichtman, Vuk Marojevic, Jeffrey H. Reed "Analysis and Mitigation of Interference to the LTE Physical Control Format Indicator Channel"
- S. Sesia, I. Toufik, and M. Baker, "LTE: The UMTS long term evolution: from theory to practice", 2nd ed., John Wiley & Sons Ltd, 2011
- Marc Lichtman, Thaddeus Czauski, Sean Ha, Paul David, Jeffrey H. Reed, "Detection and Mitigation of Uplink Control Channel Jamming in LTE"
- 3GPP TS 36.331: "Radio Resource Control (RRC)"
- 3GPP TS 36.304: "User Equipment (UE) procedures in idle mode"


Thank You !

"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