Enhancing the Security of OFDM-based Radio Interfaces using a Spread Spectrum Underlay Signal

05/01/23

Dr. Nishith D. Tripathi

nishith@vt.edu

Virginia Tech

Acknowledgment. This presentation is based on the research performed by Kumar Sai Bondada (my student).

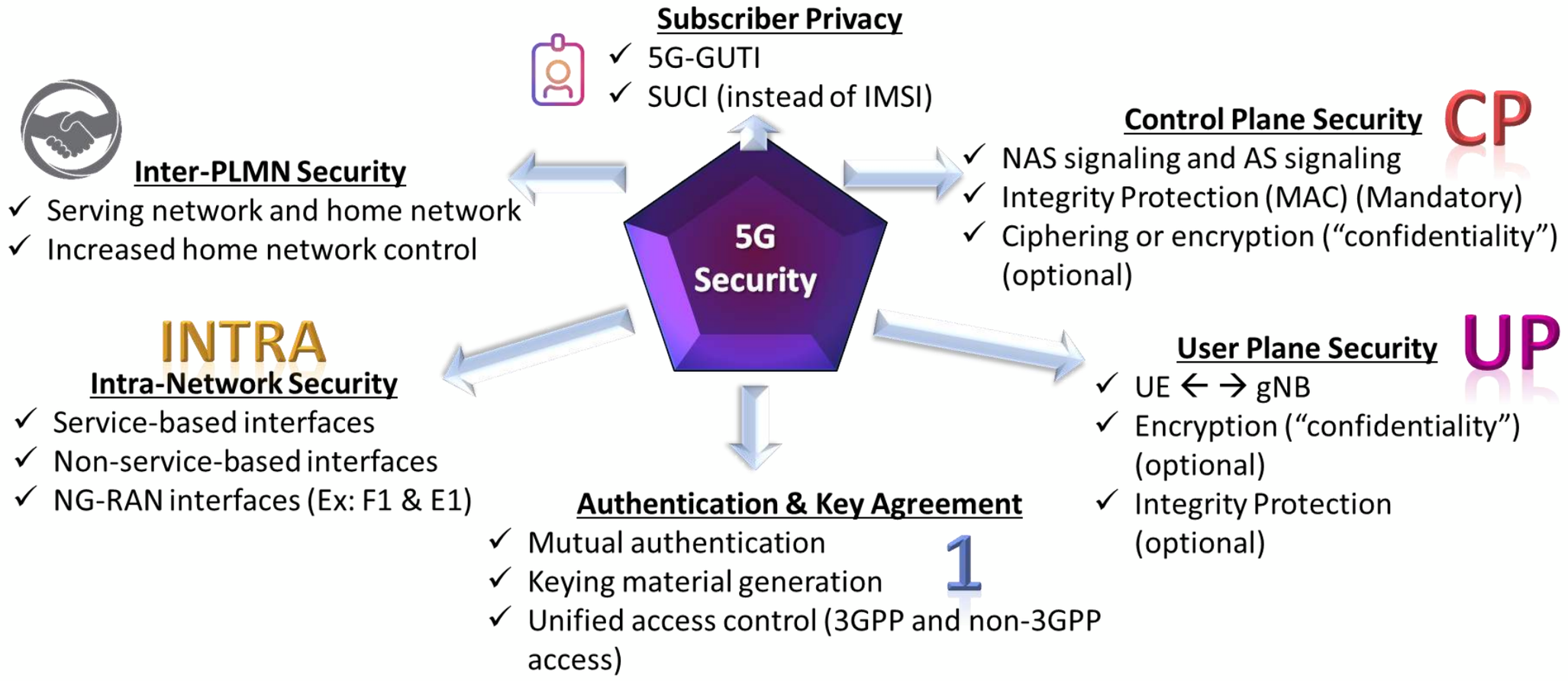
Agenda

- Summarize the security framework of 5G
- Identify strengths and vulnerabilities of the 5G NR radio interface security
- Describe how underlay signaling enhances the security of the 5G NR radio interface while coexisting with the 5G NR radio interface
- Discuss the findings of the underlay signaling analysis

5G Security in a Nutshell

5G Security: A Quick Overview

› 5G is more secure than 4G LTE



Acknowledgment. This figure has been borrowed from the 5G multimedia book: Nishith D. Tripathi and Jeffrey H. Reed, “5G Cellular Communications: Journey and Destination,,” The Wireless University, 2019.

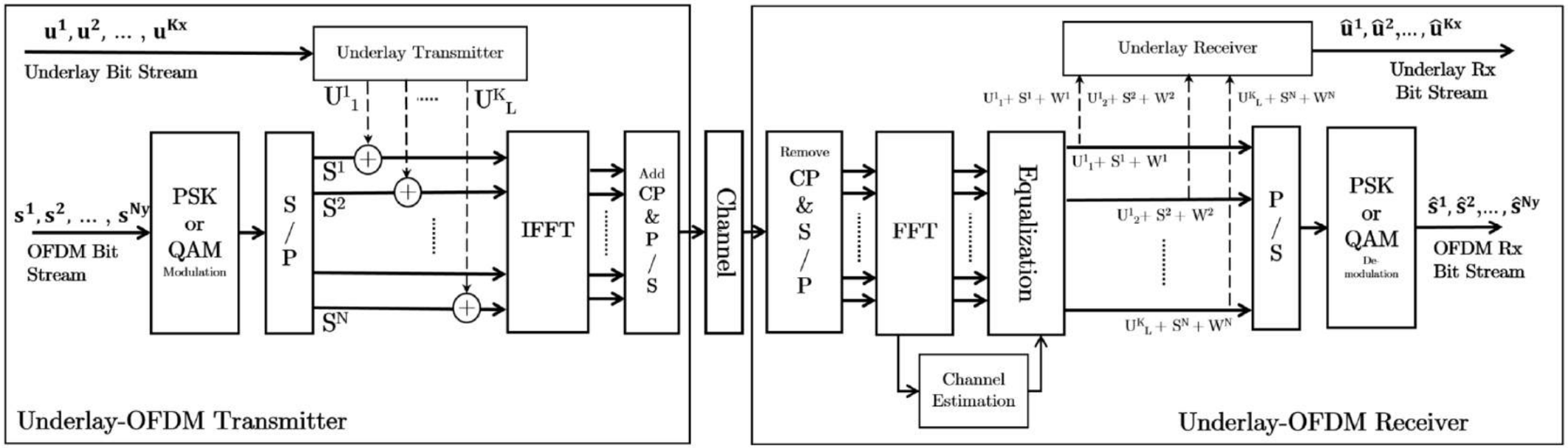
Radio Interface Security in 5G

- Example 5G NR Features for Enhanced Air Interface Security:
  - Wider channel bandwidths in the mmW spectrum
  - Beamforming
  - PDCP duplication
  - Carrier Bandwidth Part
  - Multiple CQI tables
- Example Vulnerabilities of the 5G NR Radio Interface:
  - Easy to detect SS/PBCH Blocks
  - Easy to attack PDCCHs carrying resource allocation
  - Easy to attack System Information Blocks

Underlay Signaling: The Concept

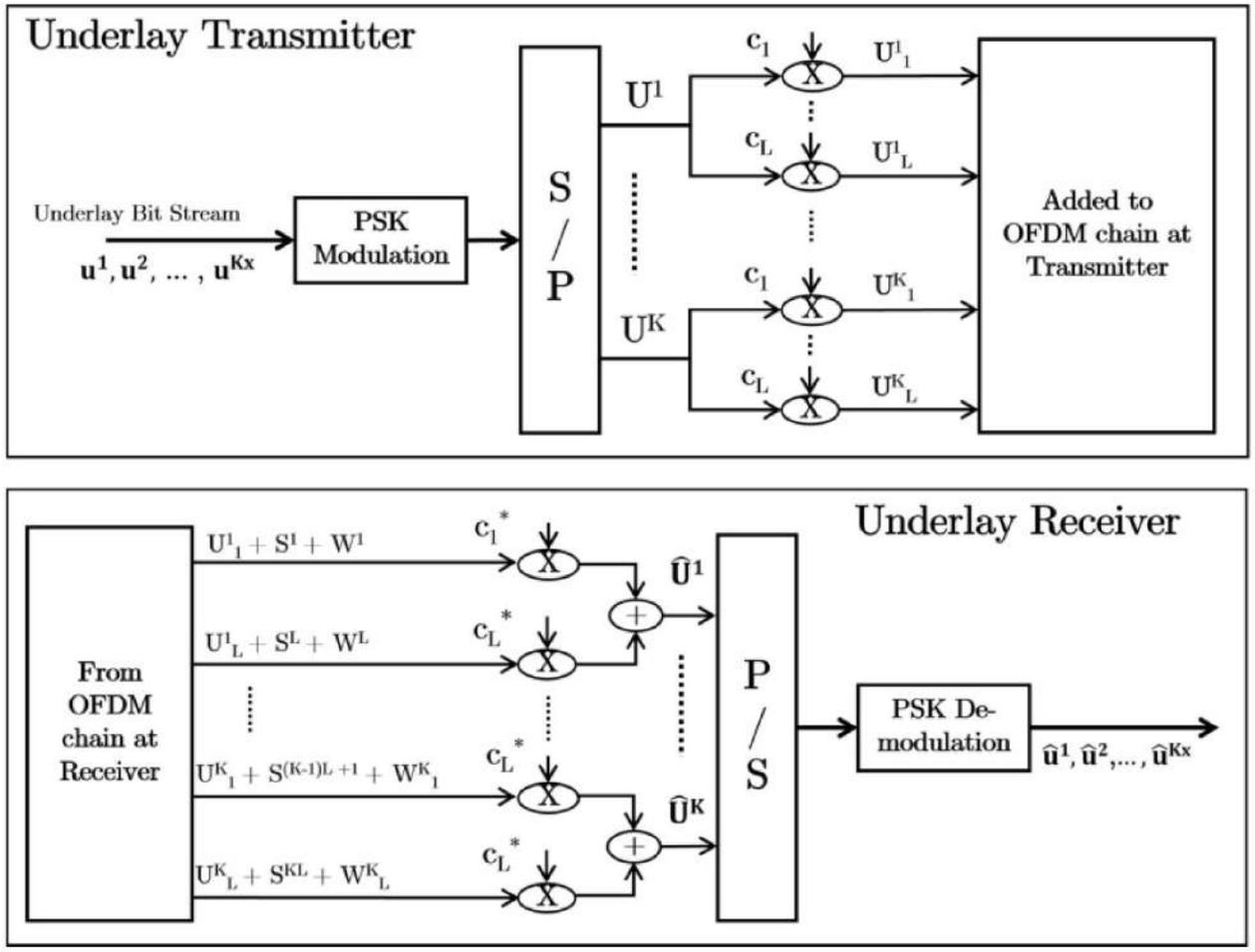
Hybrid OFDM and Underlay Transceiver

- The underlay signal is a spread spectrum signal that occupies the bandwidth of the OFDM signal



Underlay Transmitter and Underlay Receiver: A Closer Look

› The underlay transmitter uses a code such as a Walsh code to spread the signal



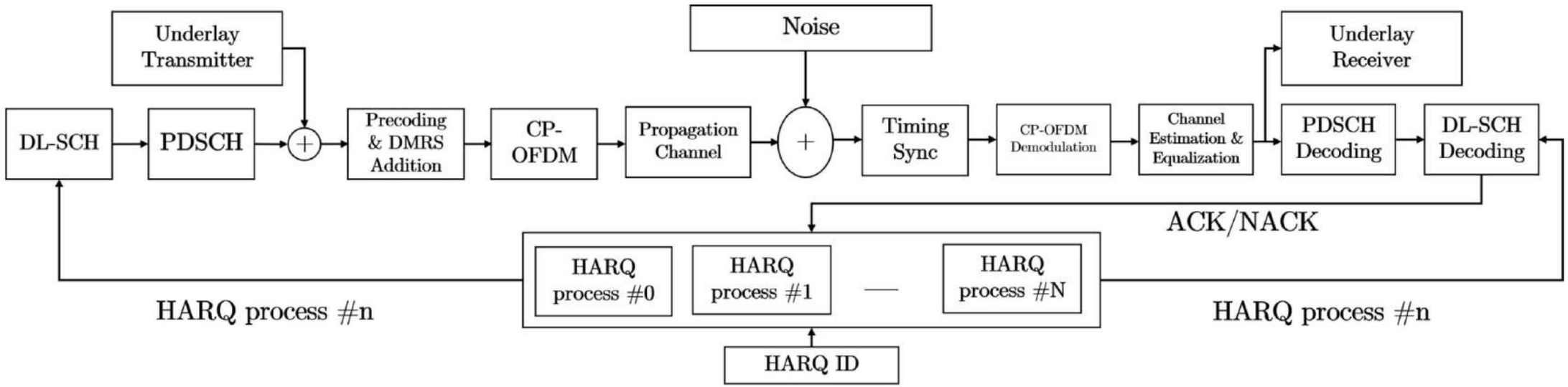
Implications of the Underlay Signal

- Since the underlay signal is using the spread spectrum technique, it appears like noise and hence cannot be easily detected by an adversary.
- Since the underlay signal occupies the same bandwidth as the OFDM signal and since a large spreading factor is needed to hide the underlay signal, the underlay signal is suitable for low data rate use cases (e.g., Physical Downlink Control Channel (PDCCH) signaling such as Downlink Control Information (DCI)).
- The underlay signal can also be used to transport low-latency services without affecting the ongoing transmissions and without requiring preemption of ongoing transmissions.
- Synchronization for the underlay signal is automatically achieved from the accompanying OFDM signal.
- The power would need to be distributed between the OFDM and underlay signals
- The existing 5G NR PHY layer would need to be modified to support the underlay signal.

Underlay Signaling: The Analysis

Analysis Scenario: PDSCH with an Underlay Signal

- Extensive MATLAB simulations are carried out using a 5G NR PDSCH with an underlay signal
- A Proof-of-Concept system has also been developed using srsRAN and USRPs.

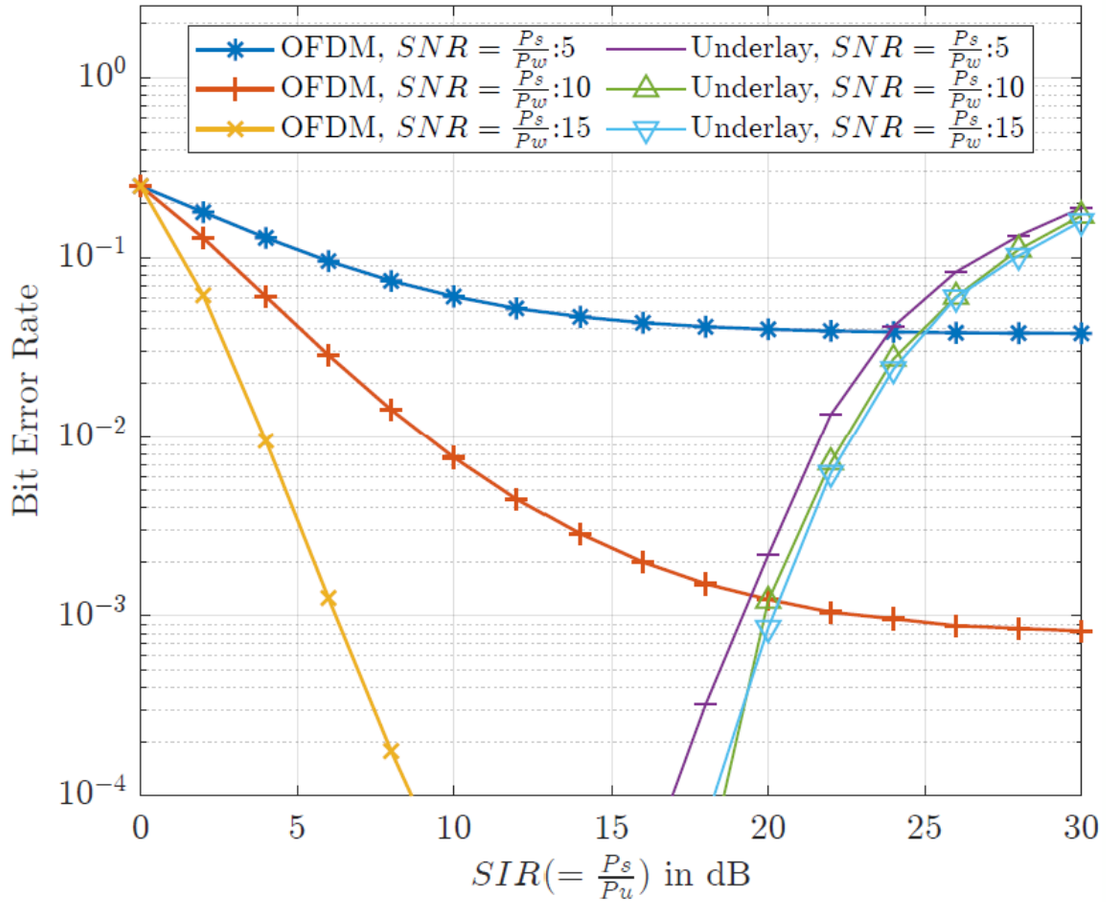


Simulator Features and Key Terms

- Polar coding is applied to the information carried by the underlay signal because of the relatively lower data rates such as those used in the PDCCHs for DCI signaling
- Single Input Single Output (SISO)
- Signal: OFDM signal
- SNR=Ps/Pw, where Ps is the OFDM signal power and Pw is the noise power
- SIR=Ps/Pu, where Ps is the OFDM signal power and Pu is the underlay signal power
- The underlay acts as interference to the OFDM signal and vice versa
- Example Configuration. One QPSK underlay symbol (K=1) is sent during one OFDM symbol (e.g., 1024 subcarriers)

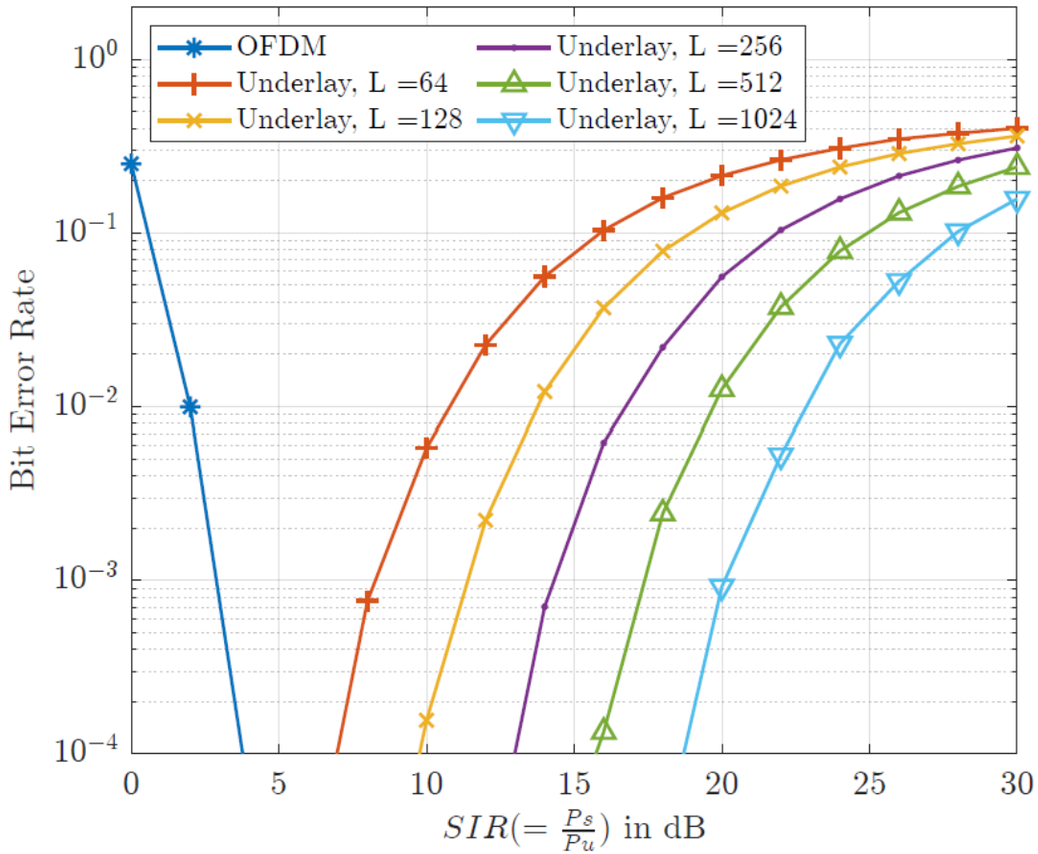
Impact of Underlay Power on OFDM and Underlay Performance

- QPSK for OFDM and underlay with a spreading length L= 1024.
- As the SIR increases, the BER of OFDM improves and eventually flattens out.



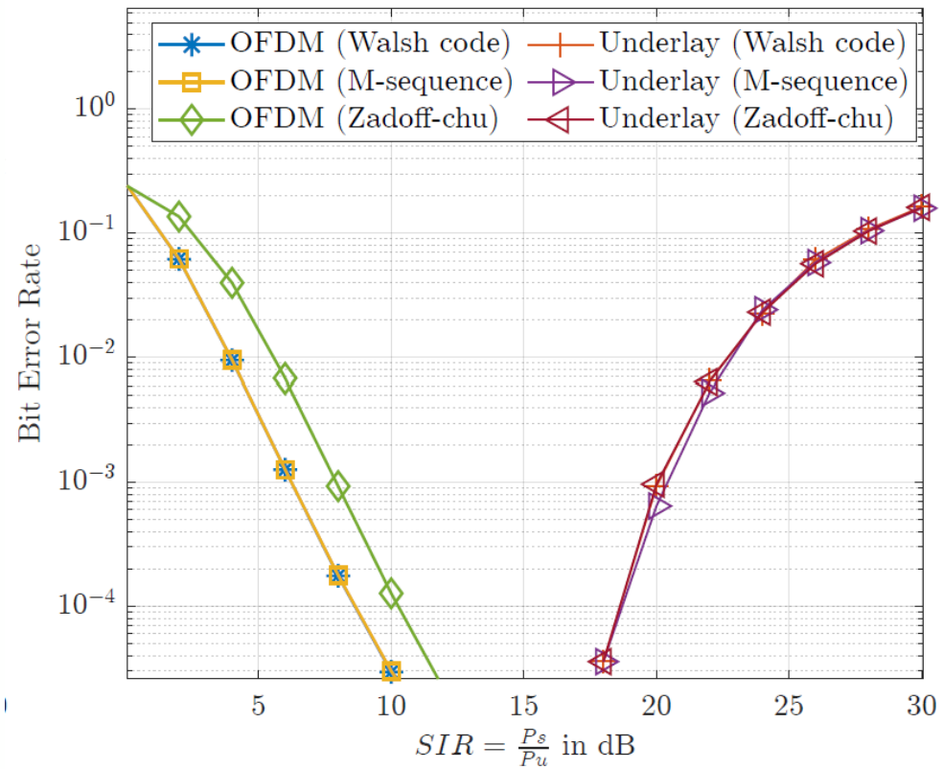
Impact of Spreading Length on OFDM and Underlay Performance

- SNR= 20 dB
- As the spreading length decreases from 1024 to 64, the underlay's BER performance becomes worse.



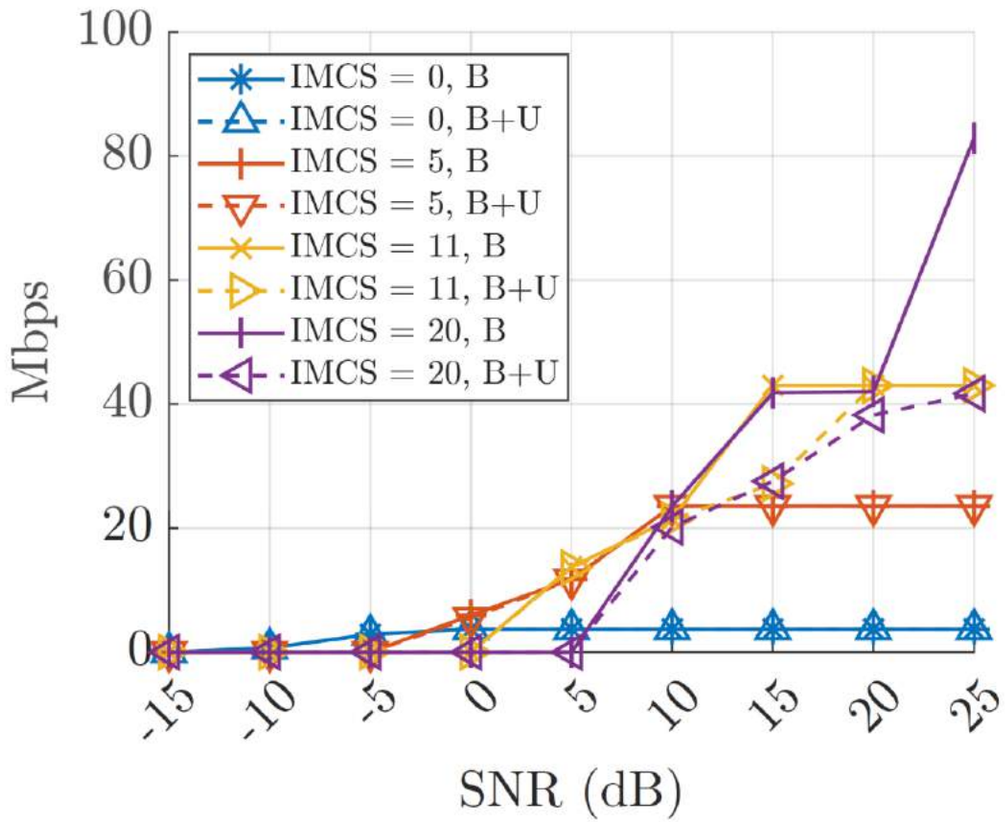
Influence of Different Codes on OFDM and Underlay Performance

- SNR= 15 dB
- Similar underlay performance for different codes
- Similar OFDM performance for Walsh code and m-sequence but slightly worse performance for Zadoff-Chu sequence



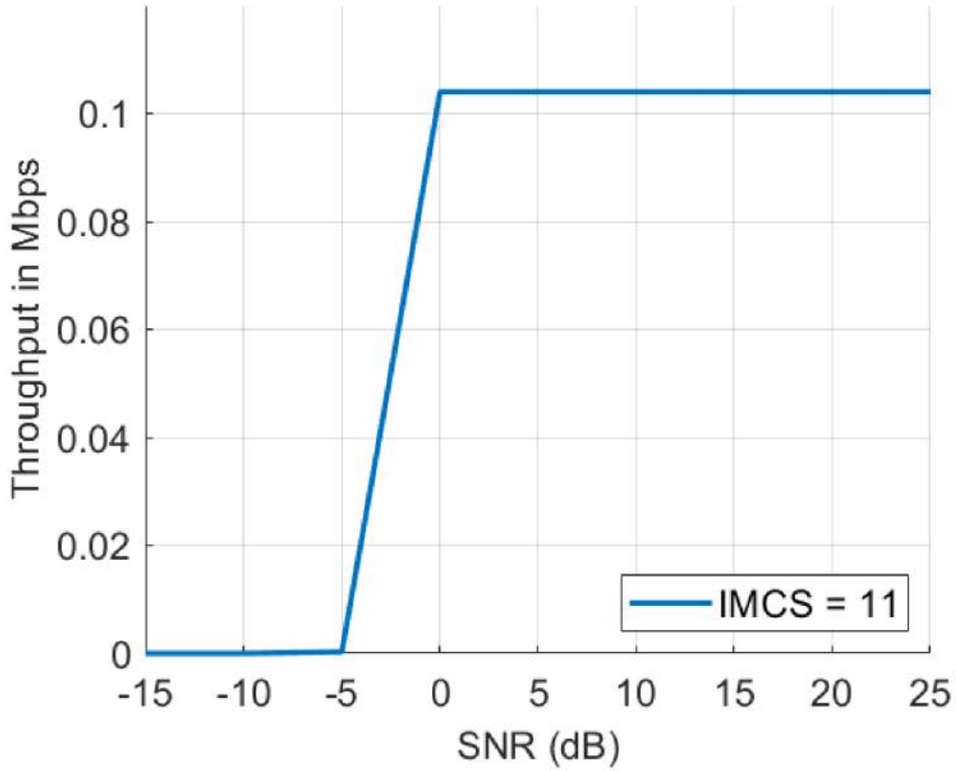
PDSCH Throughput at Different MCS and SNR Levels: Resume

- B: Baseline PDSCH and B+U: underlay plus PDSCH
- Low MCS: Minimal impact of underlay and highest MCS: Significant impact of underlay



Underlay Throughput at Different MCS and SNR Levels

- SIR: 20 dB
- Good underlay throughput can be expected in practice



Conclusion

- A novel frequency-domain spread spectrum underlay signal technique is proposed for enhanced security.
- The proposed underlay signal for sensitive traffic or signaling is transmitted concurrently with the traffic on the 5G NR PDSCH.
- The performance of the proposed underlay technique has been valuated using comprehensive simulations.
- The simulation results demonstrate the ability of the proposed underlay signal to transport sensitive signaling or traffic with the exact degree of degradation in the PDSCH being a function of the MCS values
- The underlay concept has also been demonstrated using open-source software (srsRAN) and USRPs.

Questions?

Thank You