Literature search on overshadowing and related attacks

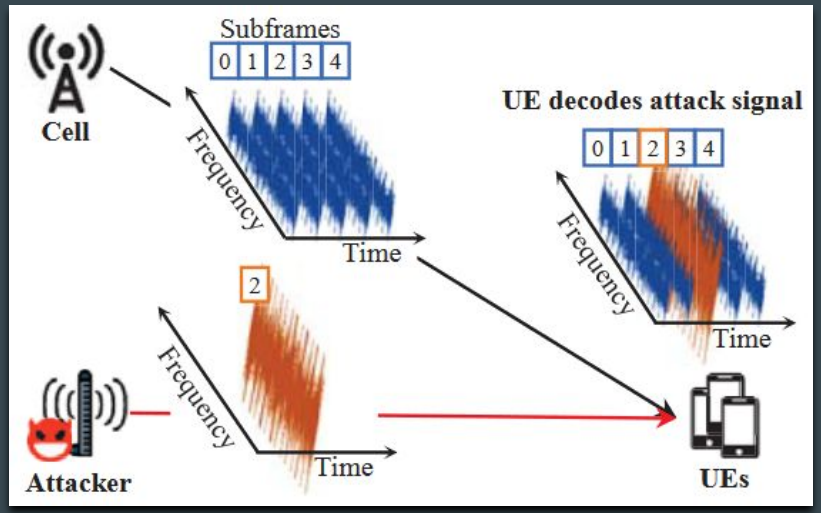
Laura Kolijn — s1025724
Tom Koning — s1020020
Jesse Ravensbergen — s4573560
Denise Verbakel — s1018597

Overshadowing — Introduction

- *Overshadow* a wireless message with your own signal
- Physical property: When waves collide, the stronger is accepted (Capture Effect)
- Exists in many wireless mediums
- Few published attacks (e.g. LTE, IEEE 802.15.4)

SigOver — Overshadowing in LTE

- First paper to introduce the topic of LTE overshadowing
- Targeting LTE subframes
- Crafting (malicious) subframes
- Listening to downlink broadcast messages
- Synchronization on fixed transmission timing
- Relies on capture effect
- Malicious subframe decoded by victim UE



Advancements in LTE Overshadowing — AdaptOver & SigUnder

- Similar technical details as SigOver, with slight differences
- Target only parts of subframe
- Both rely on unencrypted broadcast messages (RRC and MIB respectively)
- AdaptOver promises better DoS persistence
- SigUnder requires less power and is stealthier

Findings and comparison

	SigOver	AdaptOver	SigUnder
Target signal	SIB and paging	RRC	MIB
Required Power	3 dBm over	1.8 dBm over	3.4 dBm under
Type of Attacks	DoS, Network Downgrade	DoS (>12h)	UE detection