ADVANCECRT

Centre for Research Training

Science Foundation Ireland sfi For what's next

ANOMALY DETECTION IN NARROWBAND INTERNET OF THINGS

Gabriela Morillo, Utz Roedig, Dirk Pesch
University College Cork

Jamming of NB-IoT Synchronisation Signals

In this work we consider an adversary using a jamming device to disrupt NB-IoT communication. We consider an intelligent jammer that targets the initial communication steps of NB-IoT communication to have a maximum impact.

Specifically we describe and investigate how a jammer can interfere with the Narrowband Primary Synchronisation Signal (NPSS) and Narrowband Secondary Synchronisation Signal (NSSS) which are used to initiate the NB-IoT contention-based random-access procedure.

SYSTEM CONSIDERATIONS

NB-IoT provides several security mechanisms based on established mechanisms defined for LTE. However, privacy and security in NB-IoT have yet received little research attention.

- Smart Jammer

We consider an adversary using a jamming device to disrupt NB-IoT communication.
- Narrowband Primary Synchronisation Signal
- Narrowband Secondary Synchronisation Signal

- Denial of Service Attack

We consider an adversary using a jamming device to disrupt NB-IoT communication.

- Spoofing Attack

Our experiments indicate that careful design of the interference signal may allow an attacker to force the UE to recognise a specific eNodeB.

UE AND ENODEB SYNCHRONISATION

01 The UE needs to identify a suitable cell to attach to.

02 Transmission of the NPSS and NSSS.

03 The UE acquires the MIB carried by the Narrowband Broadcast Channel (NPBCH).

04 The random-access procedure initiates when the UE sends a random-access preamble through NPRACH.

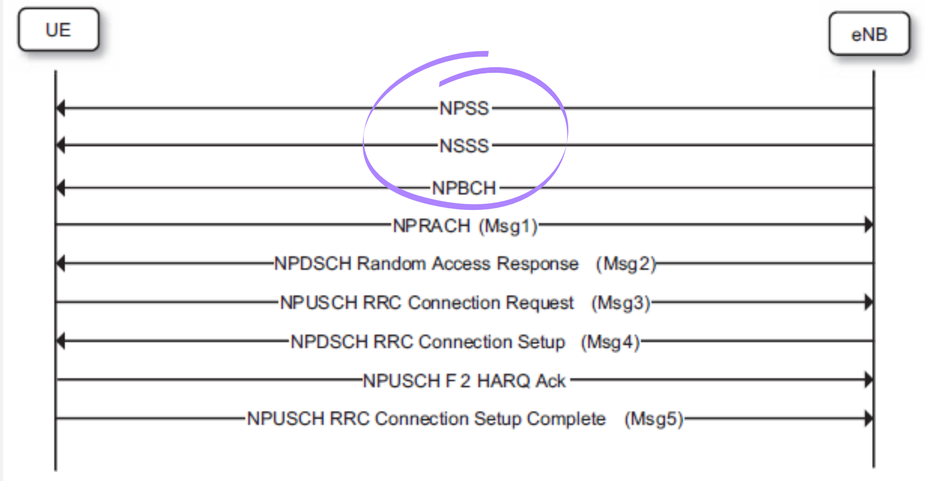

Fig. 1. NB-IoT Random Access Procedure. Initial steps of a UE to establish communication with an eNodeB

RESULTS AND DISCUSSION

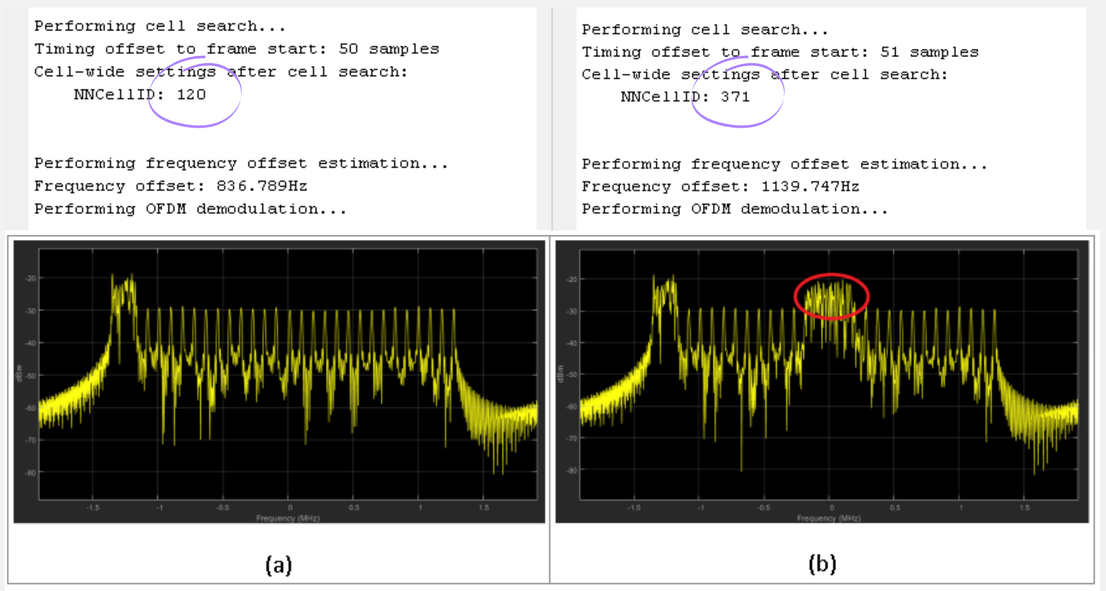

Fig. 2. Jamming Attack on NB-IoT: (a) Standard Transmission (b) Transmission with Jamming Signal

If the power of the interference signal is above 13dB a successful modification of the NB-PCIDs is observed. Cell ID is accurately detected [NNCellID: 120], and the MIB is decoded correctly.

If the power on the jammer is inefficient, the communication with the specific eNodeB is inhibited. It is not possible to decode the MIB, and a wrong cell ID is displayed [NNCellID: 371].

ANOMALY DETECTION IN NB-IOT

- We propose a novel way to detect malicious interference in IoT networks.
- We monitor the network performance in relation to the observed interference.
- Under normal operation interference will have an expected impact on performance for a given observed interference level.
- If there is an impact on network performance much above the expected impact we assume that we are targeted by an interference attack.

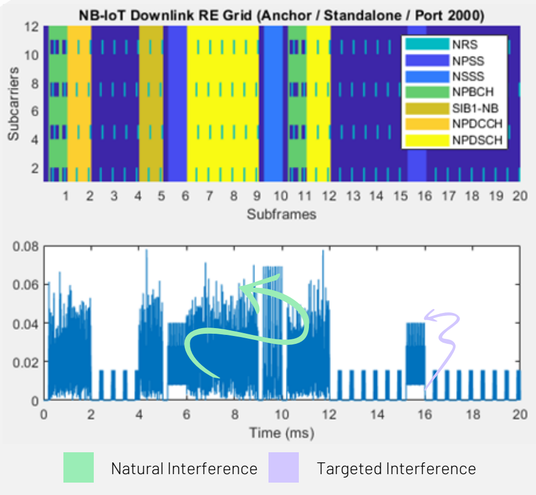

Fig 3. NB-IoT Downlink Standalone Frequency & Time domain + Interference

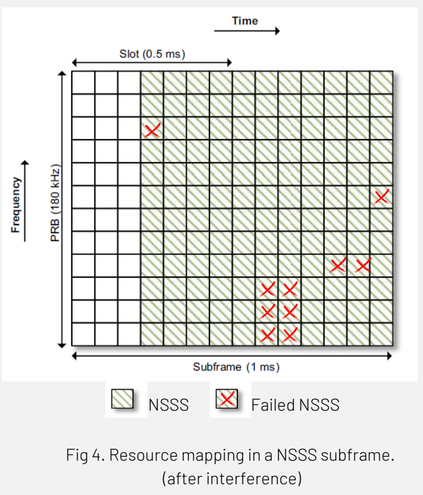

Fig 4. Resource mapping in a NSSS subframe. (after interference)

- Measurement-based method to estimate achievable Packet Reception Rate (PRR) for specific deployment areas based on the characteristics of interference [1].

CONCLUSIONS

- We have shown that it is possible to interfere with the synchronisation signal used by NB-IoT devices (the UE) to establish communication with the base station.
- A simple selective jamming device can prevent communication of NB-IoT devices. Furthermore, our experiments indicate that careful design of the interference signal might enable an attacker to force the UE to recognise a specific NB-PCID.
- In our next steps, we will analyse how the jamming signal should be designed to enable an attacker to force the UE to recognise a specific NB-PCID. We will investigate methods to detect the jamming of synchronisation/control/data signals and make the detection and the prevention more robust.
- SDG: Innovation and Infrastructure / Sustainable Cities and Communities

[1] J. Brown, U. Roedig, C. A. Boano and K. Römer, "Estimating packet reception rate in noisy environments," 39th Annual IEEE Conference on Local Computer Networks Workshops, 2014, pp. 583-591.

Host Institution

UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

MTU Ollscoil Teicneolaíochta na Mumhan Munster Technological University

Maynooth University National University of Ireland Maynooth

TU DUBLIN Ollscoil Teicneolaíochta Bhaile Átha Cliath Technological University Dublin

Trinity College Dublin Coláiste na Tríonóide, Baile Átha Cliath The University of Dublin