ADVANCECRT

Centre for Research Training

Science Foundation Ireland sfi For what's next

NB-IoT Battery DEPLETION

USING INTERFERCE

Jamming

Jamming is the intentional disruption of wireless communications, which can be accomplished in a variety of ways. One method is to transmit radio signals that decrease the signal-to-noise ratio of the communications in order to jam them. Another method is to jam selective signals that result in corrupted data packets. These concepts can be applied to wireless data networks to disrupt information flow.

Full Jammer

A simple jammer is a device that can output a continuousv interference signal. Without the ability to analyse communication and adjust the jamming behaviour. A malicious entity can use a simple jammer to force both the Evolved Node B (eNodeB) and NB-IoT devices to allocate more resources in order to communicate. To deploy such an attack, the entity will need to use an "all in one frequency jammer" that is able to jam all signals and be immune to frequency hopping [18,25].

Inteligent Jammer

The attacker will use an intelligent jammer that transmits noise in a burst-like pattern. It only uses energy when it needs to, thus functioning as a duty-cycled device. The intelligent jammer has some understanding of the upper-layer protocols. It can also understand some communication parameters by decoding the unencrypted data elements. The malicious device must be capable of eaves-dropping on the downlink channel while reacting on the uplink channel and the other way around

SDR & SRSRan

- One of the more exciting areas of wireless research in recent years has been the development of software-defined radio (SDR). SDR refers to the use of specialized hardware to perform radio functions that could otherwise be handled by a general purpose processor. SDR opens the door to a world of cheap, miniature radios that can be tailored to the application at hand.

- "srsRAN is a free and open-source 4G and 5G software radio suite. Featuring both UE and eNodeB/gNodeB applications, srsRAN can be used with third-party core network solutions to build complete end-to-end mobile wireless networks. For more information, see www.srsran.com"

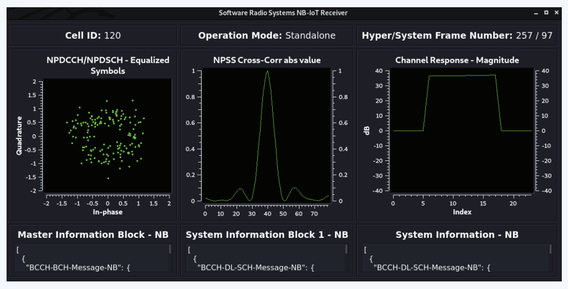
Narrowband IoT

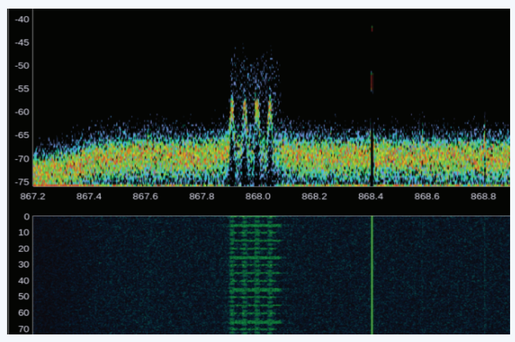
Narrowband-Internet of Things (NB-IoT) is a relatively new Low Power Wide Area Network (LPWAN) technology used to implement large-scale IoT applications. The economic viability of most applications depends on a long battery life of deloyed devices (10 years).

Energy Depletion Attack

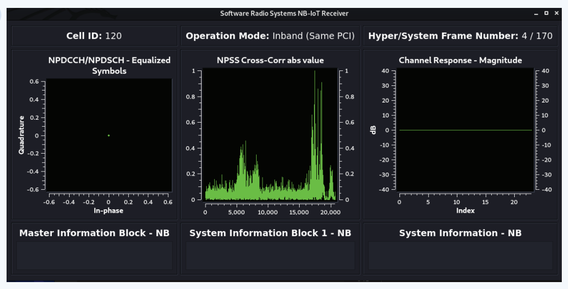
Like traditional wired networks, the devices in a wireless network use energy to transmit data. However, in an NB-IoT network, devices are much more energy-efficient than their traditional counterparts. Because of this, NB-IoT networks are much more susceptible to energy depletion attacks than traditional networks. Using Software Defined Radio (SDR), we've identified multiple types of attacks that deplete the battery.

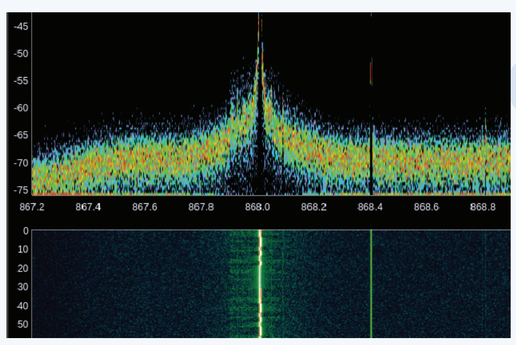
No Jamming



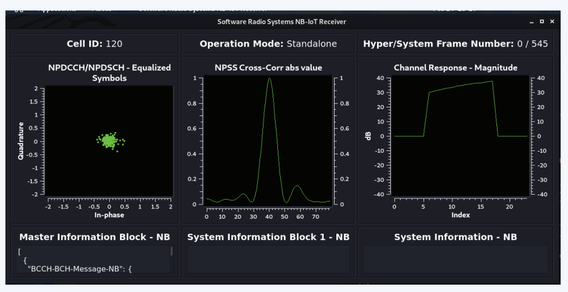


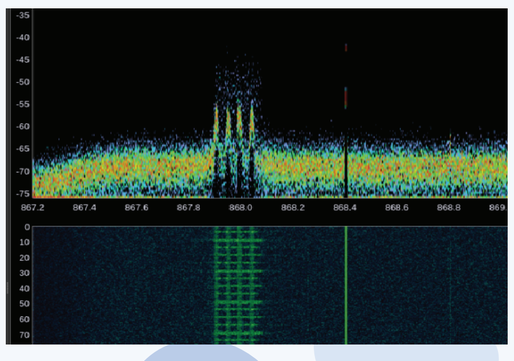
Full Radio Jamming





Forcing checksum failure





References:

1. 3GPP: 3gpp release 16, http://www.3gpp.org/release-16
2. 3GPP: Evolved universal terrestrial radio access (e-utra); physical layer; measurements, https://portal.3gpp.org/
3. Adhikary, A., Lin, X., Eric Wang, Y.P.: Performance evaluation of NB-IoT coverage. In: IEEE Vehicular Technology Conference (2016).
4. Andres-Maldonado, P., Ameigeiras, P., Prados-Garzon, J., Navarro-Ortiz, J., Lopez-Soler, J.M.: Narrowband IoT data transmission procedures
5. Liberg, O., Sundberg, M., Wang, Y.P.E., Bergman, J., Sachs, J., Wikstr om, G.: Cellular internet of things: from massive deployments to critical 5G.
6. SRSRan, https://www.srsran.com/

Host Institution

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

STUDENT: VLAD IONESCU

SUPERVISOR: PROF. UTZ ROEDIG

PROF. DIRK PESCH