ADVANCECRT

Centre for Research Training

Science Foundation Ireland sfi For what's next

Narrowband IoT Vulnerabilities

Introduction

Narrowband-Internet of Things (NB-IoT) is a new low power wide area (LPWA) technology for internet of things, developed to significantly improves the energy consumption of end devices, system capacity and spectrum efficiency, especially in deep coverage. There are many advantages for using NB-IoT, among which :

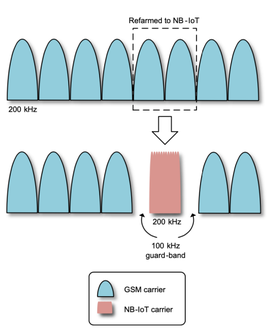
Extended range
Rural and deep indoors

Battery
Battery life expectancy +10 years

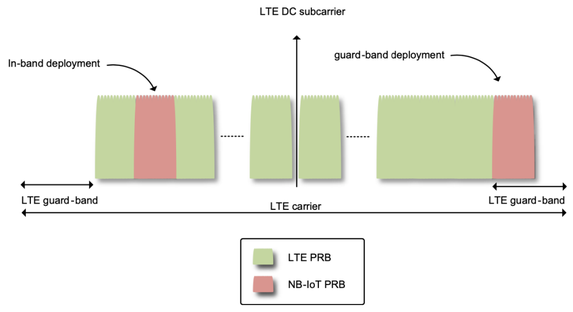
Integration
2G, 3G, 4G and 5G

Infrastructure deployment

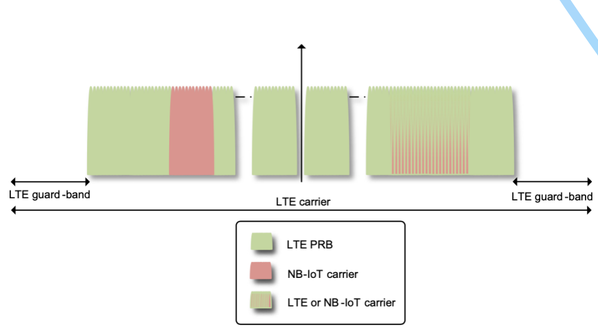
Stand-alone



In-band & guard-band



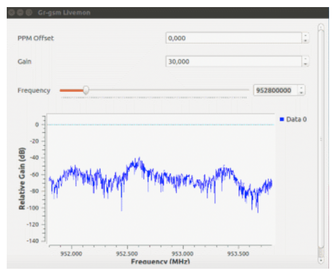
Multicarrier

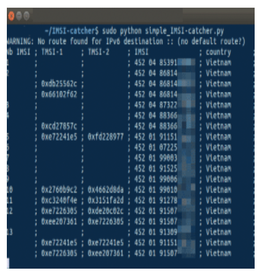


Aims

- Develop and model a baseline scenario in accordance with the latest 3GPP specification
- Simulate a full life cycle of an NB-IoT energy consumption expectancy.
- Simulate different energy depletion attacks, replay attacks and location leak attacks.
- Conclude what would be the optimal threat.
- Provide a solution in order to minimize the impact of an energy depletion attacks

Mockup NB-IoT attack





Energy Depletion Attack

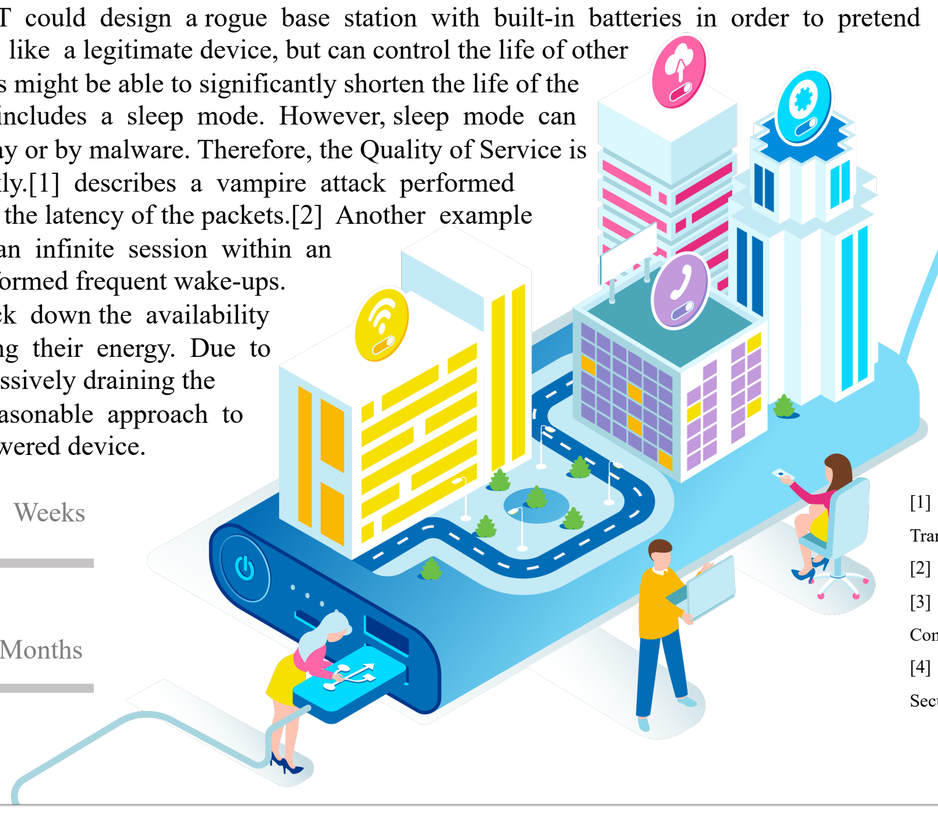
Because one of the main features of NB-IoT is the target life of 10 years, according to 3GPP, battery attacks are dangerous to the network security since adversaries can target battery-powered devices and make them unable to communicate with the base station. Also, a motivated adversary who has the knowledge of the architecture of NB-IoT could design a rogue base station with built-in batteries in order to pretend themselves as end nodes. Such a base could behave like a legitimate device, but can control the life of other nodes that use batteries. In such environment, adversaries might be able to significantly shorten the life of the battery. It is assumed that a mobile sensor duty cycle includes a sleep mode. However, sleep mode can be hindered by design in order to reduce packet delay or by malware. Therefore, the Quality of Service is improved, but the sensor exhausts its battery more quickly.[1] describes a vampire attack performed by implementing a DoB accompanied by an increase in the latency of the packets.[2] Another example of performing depletion of battery is by organizing an infinite session within an attacked node by exploiting the MAC protocols to performed frequent wake-ups. Energy Depletion Attack (EDA) are designed to crack down the availability of battery-powered devices primarily through depleting their energy. Due to the lack of abundant energy source attached, by aggressively draining the battery of these connected sensors, EDAs can be a reasonable approach to degrade the function and further disable a battery-powered device.

Decrease QoS — 2 Years

Jamming — Weeks

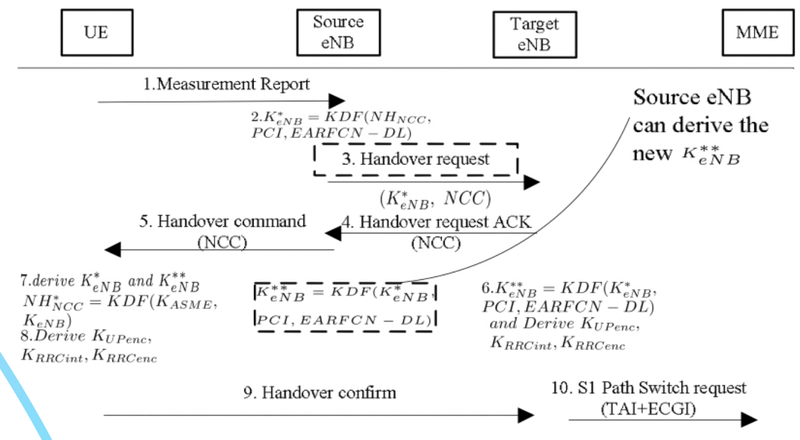
Smart Jamming — < 5 Years

MIM — Months



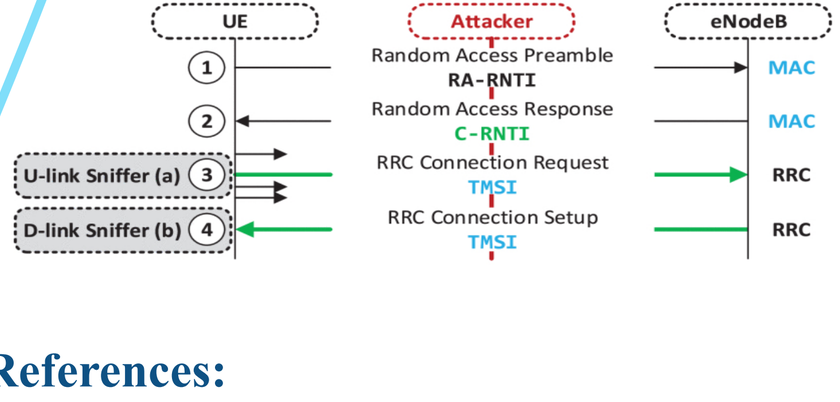
Replay Attack

A replay attack happens when a malicious entity eavesdrops on a protected network connection, intercepts it, and then delays or resends it to deceive the into doing what the cybercriminal wants. The attack can be successful without the need to decrypt the communication. Usually, a replay attack occurs during the authentication messages, and by just resending the auth messages, both entities will recognize the attacker as the legitimate entity and further trust it with future information that might be encrypted or not. More precisely, a malicious entity intercepts the handover request message, also illustrated below that is exchanged between the user equipment and a legitimate eNb. To force a new handover procedure on a targeted eNb, the attacker sends the previously recorded request messages instead of the legitimate one to the eNb. This action makes the targeted eNb recognize the received Key-Nb from the previous messages as the link key and sends the NCC value from the previous message to the UE. The UE will check if the NCC value is the same as the one it has stored and will result in a failed check, forcing the UE to launch anew handover procedure. [3]



Location Leak Attack

The identity mapping attack occurs on layer two by exploiting the temporary identifiers during the radio connection establishment. [4] showed that this type of attack could be performed on an estimate of 94.73% of network connection The attack becomes possible as the MAC layer packets use RNTI to send to the correct UE, which enables matching the C-RNTI and the TMSI. The C-RNTI is received by the UE within the Random Access Response (RAR), which from now on, distinguishes the UE on the MAC layer. Considering that there are only ten possible Random Access RNTIs (RA-RNTIs), all possible RAR can be monitored and determined by the C-RNTI. The information contained in the RAR message is sufficient for matching the C-RNTI and the TMSI by using an uplink sniffer for the RRC connection request or a downlink sniffer for the contention-based resolution of the RRC as shown bellow



References:

[1] E. Y. Vasserman and N. Hopper, "Vampire attacks: Draining life fromwireless ad Hoc sensor networks,"IEEE Transactions on Mobile Com-puting, 2013.

[2] V. Shakhov and I. Koo, "Depletion-of-battery attack: Specificity, mod-elling and analysis,"Sensors (Switzerland),

[3] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspectsfor lte and lte-a networks,"IEEE Communications Surveys Tutorials,vol. 16, no. 1, pp. 283–302, 2014.

[4] D. Rupprecht, K. Kohls, T. Holz, and C. Popper, "Breaking LTE on LayerTwo," inProceedings - IEEE Symposium on Security and Privacy, 2019

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 UCC

Coordinators:
Prof. Utz Roedig
Prof. Dirk Pesch