CORA Cork Open Research Archive
Cartlann Taighde Oscailte Chorcaí

Title	NB-IoT battery depletion via malicious interference
Authors	Ionescu, Vlad;Roedig, Utz
Publication date	2022
Original Citation	Ionescu, V. and Roedig, U. (2022) 'NB-IoT battery depletion via malicious interference', EWSN '22: Proceedings of the 2022 International Conference on Embedded Wireless Systems and Networks, pp. 244–249. https://doi.org/10.5555/3578948.3578987
Type of publication	Conference item
Link to publisher's version	10.5555/3578948.3578987
Rights	© 2022, Association for Computing Machinery. This is the author's version of the work. The definitive Version of Record is available at: https://doi.org/10.5555/3578948.3578987 For the purpose of Open Access, the author has applied a CC BY public copyright licence to any Author Accepted Manuscript version arising from this submission. - https://creativecommons.org/licenses/by/4.0/
Download date	2026-11-02 08:48:52
Item downloaded from	https://hdl.handle.net/10468/13501

UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

NB-IoT Battery Depletion via Malicious Interference

Vlad Ionescu
School of Computer Science and Information Technology (CSIT)
University College Cork
v.ionescu@cs.ucc.ie

Utz Roedig
School of Computer Science and Information Technology (CSIT)
University College Cork
u.roedig@ucc.ie

Abstract

Narrowband Internet of Things (NB-IoT) is a popular Low Power Wide Area Network (LPWAN) technology for large-scale Internet of Things (IoT) applications. The NB-IoT protocol is designed to conserve energy, so battery powered devices can have a lifetime of several years. However, the protocol design does not assume malicious interference. As we show in this paper jamming can be used to deplete the battery of NB-IoT devices reducing the lifetime from many years to several month. These attacks can be carried out without preventing data delivery entirely and are therefore hard to detect. We consider jamming focused on the initial unprotected downstream communication after a node wakes from sleep. We show that the most efficient interference can be constructed by exploiting the capture effect; the attacker can replace a subframe within the transmission from the base station to the device.

1 Introduction

Narrowband Internet of Things (NB-IoT) is a relatively new Low Power Wide Area Network (LPWAN) technology developed by 3rd Generation Partnership Project (3GPP). NB-IoT aims to provide long-lasting battery life for low-cost devices with support of a high connection density. NB-IoT is a popular industry choice as it uses a subset of the Long-Term Evolution (LTE) standard and devices are integrated with an existing 4G infrastructure. Thus, deployment is greatly simplified and IoT infrastructure cost is reduced.

NB-IoT devices are used to develop IoT applications such as industrial monitoring, smart grids and smart cities. These applications require a long node lifespan to be economically viable. Frequent battery swaps or battery recharging are not possible as this would incur maintenance expenses to the point where the application would be rendered unviable. In most application scenarios communication consumes the majority of energy and it is feasible to achieve the usually required 10 year lifespan by selecting a low duty cycle. A node wakes only a few times per day to relay information to a back-end through the LTE network.

NB-IoT communication is complex and a node waking up has to go through a number of protocol steps (obtaining synchronisation, obtaining network parameters, connection establishment, authentication, ...) before the payload can be transmitted. If any of the protocol steps cannot be completed the payload cannot be delivered.

NB-IoT therefore has mechanisms to ensure that message losses can be compensated. On failure, protocol steps can be repeated, transmission power and the number of message repetitions are constantly adjusted to accommodate for changes in connection quality. However, these mechanisms are designed to deal with natural channel quality fluctuations. They are not designed to deal with malicious interference.

An attacker can use jamming to disrupt communication between an NB-IoT device and a base station. While continuous tampering can be used to prevent all communication a malicious entity may not use such a crude method as it easy detectable. Instead he may interfere with specific messages such that (i) communication is still possible, thus postponing or even evading suspicious and (ii) a device's energy expenditure is maximized. The attacker aims to interfere such that a node uses its adaptation capabilities to the full to compensate, increasing energy consumption. A secondary aim may be to spend as little energy as possible to generate interference as it may be a battery powered device itself. The attacker would like to be active as long as possible.

In our previous work we have conceptually described battery depletion attacks of NB-IoT devices and provided a simulation evaluation [9]. The work presented in this paper considers a refined set of attacks and we use a testbed based on the HackRF One platform [7] and the srsRAN [15] to evaluate jamming based attacks. Specifically, we describe and evaluate interference focused on the initial unprotected downstream communication after a node wakes from sleep. We show that the most efficient jamming can be constructed by exploiting the capture effect; the attacker can replace a subframe within the transmission from the base station to the device.

2 Related Work

Battery depletion attacks aim to force a device into exerting additional effort on tasks resulting in additional energy consumption. For example, a device may be encouraged to exert more computing effort [16], it is stopped from entering an idle or sleep state [13] or forced to perform unnecessary communication [4].

There are several techniques available to force a device to communicate unnecessarily. An attacker may choose to target a single device or the whole network. To launch an attack on a single device, one can inject messages which may result in responses declaring that this message was incorrect (see Vasserman et al. [17], and Krejc et al. [10]). The attacker may also try to alter the behaviour of the entire network. One common method is to target the routing protocol (see Butty et al. [3] and Pu et al. [14]). The attacker may be able to insert a node into the network that alters routing behaviour, causing messages to travel abnormally long distances or to be often lost, forcing retransmissions.

This study investigates interference (often referred to as jamming) as a specific attack resulting in battery depletion. A node may use increased transmission power or additional transmissions to compensate for perceived communication channel degradation. A node may also require more time to receive a required message undisturbed.

Chiara et al. [11], highlight the susceptibility of IoT networks with battery powered nodes to jamming. The work considers battery depletion via interference but does not consider NB-IoT.

Hossein et al. [12] examine current jamming attacks and anti-jamming tactics in Wireless Local Area Networks (WLAN)s such as cellular networks, ZigBee networks, LoRa networks, Bluetooth networks, vehicle networks, and others. The article provides a thorough examination of jamming and anti-jamming methods, as well as insight into the design of jamming-resistant wireless networks. However, NB-IoT networks and battery depletion attacks are not considered.

In our previous work we have conceptually described battery depletion attacks of NB-IoT devices and provided a simulation evaluation [9]. The work presented in this paper considers a refined set of attacks and we use a testbed based on the HackRF One platform [7] and the srsRAN [15] to evaluate the attacks.

3 NB-IoT Communication

NB-IoT operates on a licensed spectrum and uses the existing infrastructure of GSM, LTE and 5G. It may function in one of three different modes: In-band, Guard-band, or Standalone. We focus in this work on the Standalone deployment. However, the results are applicable to the other two operation modes and our testbed setup can also support these.

In a typical NB-IoT scenario, the User Equipment (UE) is configured to report data periodically (e.g. every t hours). The communication flow is illustrated in Figure 1 and further detailed in Section 5. After waking up, the UE must synchronize with the Evolved Node B (eNodeB) (the term for base stations in NB-IoT) in time and frequency by obtaining the Narrowband Primary Synchronization Signal

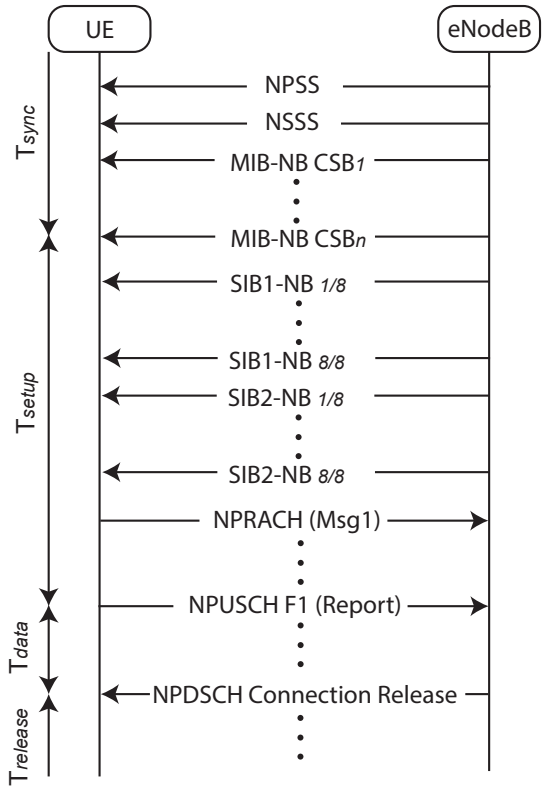


Figure 1. NB-IoT transmission procedure. Messages up to NPRACH (Msg1) are sent unencrypted

(NPSS). Then the Narrowband Secondary Synchronization Signal (NSSS) signal must be received which is correlated with the NPSS to obtain the cell id. With this information the UE can now decode information transmitted in the downlink channel and can encode information in the uplink channel. The next step is to procure the Narrowband Master Information Block (MIB-NB), which is sent in the Narrowband Physical Broadcast Channel (NPBCH). After receiving the MIB-NB, the UE has all of the scheduling information required to obtain next the Narrowband System Information Block 1 (SIB1-NB), which in turn has all of the scheduling information required to obtain the Narrowband System Information Block 2 (SIB2-NB). The SIB2-NB includes all of the settings required procuring following System Information Blocks (SIBs) as well as the information required to initialize the Random Access Procedure (RAP) (connection setup and security handshake). After completing the RAP, the UE is now securely linked to the base station and ready to submit data reports. When the report is acknowledged by the base station, the eNodeB sends a connection release message to the UE, which in turn will go back to sleep.

Extended Discontinuous Reception (eDRX) and Power Saving Mode (PSM), were new features included in 3GPP Releases 12 and 13 that specifically aimed at improving energy consumption of the UE. eDRX is an expansion of the discontinuous reception capability in LTE and allows a

device to go into sleep mode for a length of time. PSM is a UE status that reduces energy consumption further. In essence, a device may shut off its transceiver and only operate a basic oscillator to retain an approximate time reference for when it should quit PSM. However, when a UE wakes from eDRX / PSM it has to perform the aforementioned message processing and exchange. In particular, the UE must process NPSS, NSSS and procure MIB-NB, SIB1-NB and SIB2-NB from the downlink channel. This is where we focus our attack.

4 Threat Model

We assume an attacker that deploys a battery powered device of similar capability to a UE. The device is able to emit an interference signal and it is able to observe communication between a eNodeB and the target UE. We refer to this device as the *Jammer*.

The Jammer aims to use interference such that (i) communication between UE and eNodeB is still possible, thus evading detection and (ii) the target UE's energy expenditure is maximized. Furthermore, the Jammer aims to minimise it's own energy expenditure to prolong jamming activity and to minimise detection.

The Jammer can process NPSS and NSSS, and is able to decode MIB-NB, SIB1-NB and SIB2-NB as this part of the communication is not encrypted. The Jammer can therefore target specific elements of MIB-NB, SIB1-NB and SIB2-NB. We assume the Jammer focuses the effort on jamming these communication elements.

5 Radio Resource Control Procedure

NPSS and NSSS signals and the MIB-NB, SIB1-NB and SIB2-NB information are transmitted on the downlink channel from eNodeB to UE. The frame structure continuously broadcast by the eNodeB is shown in Figure 2.

Narrowband Master Information Block (MIB-NB): The MIB-NB is the first message the UE needs to receive when establishing a connection. This information is transmitted via the Narrowband Physical Broadcast Channel (NPBCH) in a repetitive pattern to improve reliability [5]. The MIB-NB is encoded as eight Code Sub-Block (CSB) that equally divide the message. These CSBs are transmitted in subframe 0. Each CSB is repeated 8 times. Thus, in total 64 subframes equalling to 640 ms are needed for a full MIB-NB transmission. The UE must receive one out of each of the 8 repeated CSB to decode the message successfully. A Cyclic Redundancy Check (CRC) is used to verify a decoded MIB-NB.

In comparison to the LTE MIB, the MIB-NB carries a larger set of information that comprises System Timing, Scheduling Information for SIB1-NB, Access Barring and Operation Mode.

Narrowband System Information Block 1 (SIB1-NB): Similar to MIB-NB, SIB1-NB follows a static repetition pattern. However, the SIB1-NB periodicity is 256 frames (or 2560ms), divided into 16 frame intervals. Depending on the eNodeB configurations, these 16 frames are evenly repeated four, eight or sixteen times. The SIB1-NB is transmitted in eight SIB1-NB subframes always mapped to subframe #4 in every other frame [2] as shown in Figure 2.

The acquisition time can easily add up when the UE is in poor coverage locations. To counteract this, 3GPP introduced an option in release 15 that is able to utilise every subframe #3 preceding subframe #4 for the SIB1-NB transmission as well [1].

The successful acquisition and decoding of the SIB1-NB is essential, as it contains critical information in acquiring the following System Information (SI) and the network configurations that the UE is trying to connect to.

Narrowband System Information Block 2 (SIB2-NB): SIB2-NB is the final piece of data a UE requires before beginning the Random Access Procedure (RAP). SIB2-NB broadcasts on a regular basis based on the configuration transmitted in SIB1-NB. The UE has all Radio Resource Control (RRC) configurations after decoding the SIB2-NB. The RRC includes NPRACH configurations, which are used by the device to select the appropriate parameters for its coverage class based on the Narrowband Reference Signal (NRS). SIB2-NB is periodically transmitted within particular time-domain periods called the *si-WindowLenght*. Furthermore the *si-WindowLenght* starts based on the periodicity defined as *si-RepetitionPattern*, which is the starting radio frame the *si-WindowLenght* becomes active. SIB2-NB can be configured with a TBS in the range of 56, 120, 208, 256, 328, 440, 552, 680 bits to accommodate changing content and future message expansion. The two smallest sizes use two consecutive NB-IoT subframes, while the six biggest use eight. SIB2-NB may be repeated to enable extended coverage. Every second, fourth, eighth, or 16th radio frame might repeat a SIB2-NB.

6 Attack Scenarios

We consider a Jammer that aims to disrupt processing of MIB-NB, SIB1-NB or SIB2-NB information with the aim of increasing energy consumption at the UE. When a UE wakes to transmit a message it requires to receive the MIB/SIB. If the UE is unable to decode these messages it may remain listening for the repetition of these messages in the downstream signal. It will depend on the implementation of the UE how long it will try to decode these messages before it gives up. A jammer can aim to disrupt reception for the longest possible time before the UE gives up and thus prolong the communication duration leading to energy depletion.

There are two distinct jamming approaches we consider: Message Jamming (MJ) and Message Injection (MI).

In case of MJ the Jammer emits a jamming signal during subframes containing MIB / SIB information. It must be ensured that the transmission power of the jamming signal is sufficiently high at the UE. An example MJ jamming signal is shown in Figure 3 (a).

In case of MI the jamming signal is a valid message during a subframe. If the signal strength and timing of the jamming signal is carefully crafted the UE will process within a subframe the message of the attacker instead of the message submitted by the eNodeB. Thus, the attacker injects a false message in place of a valid one. This is possible as this part of the communication is not yet cryptographically secured. Interestingly, compared to MJ less transmission

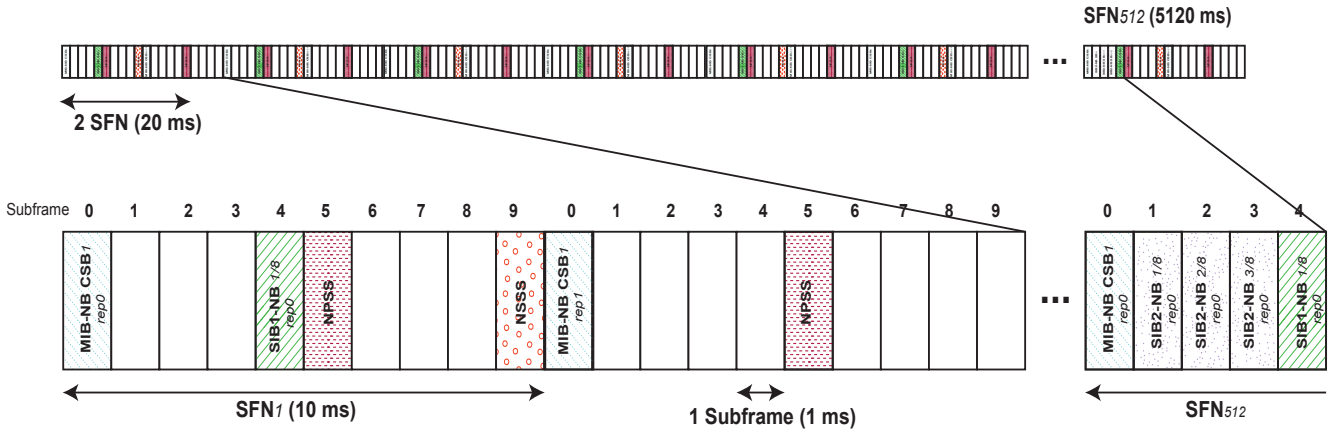


Figure 2. Subframe mapping of MIB-NB, SIB1-NB and SIB2-NB. MIB-NB is split in eight Code Sub-Block (CSB) and repeated in every System Frame Number (SFN). SIB1-NB is transmitted in eight subframes on every other frame and repeated *schedulingInfoSIB1 value* times. SIB2-NB is transmitted in eight consecutive subframes starting from *si-Periodicity* and repeated every *si-RepetitionPattern*

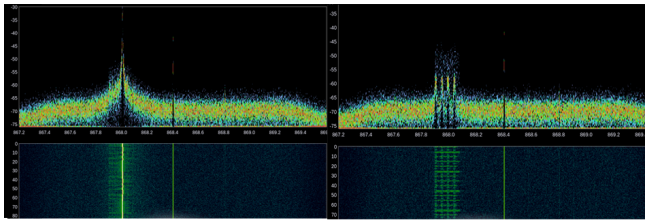


Figure 3. Spectrum of a (a) Message Jamming (MJ) attack and (b) Message Injection (MI) attack.

power is required by the Jammer. An example MI jamming signal is shown in Figure 3 (b).

Both jamming variants can be applied to MIB-NB, SIB1-NB, and SIB2-NB. In case of MJ the Jammer aims to destroy all repetitions of one CSB for MIB-NB and all repetitions of one SIB subframe. It is not necessary for the Jammer to destroy all CSBs or subframe transmissions as a loss of one requires the UE to receive the entire sequence again. In case of MI the Jammer only needs to replace the first CSB or SIB subframe of a sequence. As soon as the UE has obtained a valid CSB or SIB subframe it does not process further repetitions. However, when all parts are received the CRC will fail. The UE will need to receive the entire sequence again.

While MJ and MI have the same consequence (the UE must start receiving the message again) MI is more effective. The Jammer must be active in fewer subframes and the interference signal is indistinguishable from valid eNodeB transmissions.

The **MIB-NB** is always transmitted on the NPBCH on subframe zero of every frame and has a transport block of 50 bits which after modulation consist of eight CSB that are repeated eight times in a Transmission Time Interval (TTI) of 640 ms (see Section 5). This configuration is static as defined by 3GPP [2]. A MJ attack of the MIB-NB message would consist of destroying any CSB and all of its repetitions. To ensure that all repetitions are destroyed, the Jammer needs to send a jamming signal similar to Figure 3(a) for one millisecond and repeat it at least eight times in total eight milliseconds in a 640ms TTI. It is worth mentioning that the CSBs do not provide an index. When observing transmissions it is not possible from the observation of CSBs to determine to which repetition they belong. To synchronise the Jammer it can observe the sequence of CSBs and when adjacent transmitted CSBs are observed it is known when a repetition of a new CSB starts. A MI attack of the MIB-NB message only requires to target the first of the 8 repetitions. Once the UE receives the false CSB it does not process repetitions and the final MIB-NB CRC will fail.

For a **SIB1-NB** attack we are assuming the attacker has obtained the MIB-NB and has now the necessary information to target the SIB1-NB. SIB1-NB, like MIB-NB, follows a static repeating pattern. It always has a TTI of 256 frames (2560ms), which are carried in eight SIB1-NB subframes that are repeated four, eight, or sixteen times depending on the value of *schedulingInfoSIB1* obtained with the MIB-NB. For every other frame, the SIB1-NB is always mapped on subframe four. In our setup, the SIB1-NB repetition is set, which means that the next SIB1-NB is broadcast every 64 frames. Within these 64 frames, eight subframes are used in every other frame to carry the SIB1-NB. Knowing this, targeting the SIB1-NB using MJ or MI requires jamming the subframe four for one millisecond every 64 milliseconds and repeating the process four times.

The **SIB2-NB** targeted attack differs from the SIB1-NB and MIB-NB attack. Unlike the first two messages, the SIB2-NB transmission configuration is dynamic and may be adjusted by the eNodeB, including the transport block size and frequency. In our experimental setup the SIB2-NB is delivered with a periodicity of 512 frames, a transport block size of 440 bits, and a repeating pattern of *si-WindowLenght*

of 960ms and *si-RepetitionPattern every4thRF* resulting in 24 repetitions is used. For this scenario, the MJ Jammer has to interfere with one SIB2-NB subframes (see Figure 2) for a total of 1 milliseconds, and then repeat the operation every other fourth frame for the length of the *si-WindowLength*. Following that, the jammer might idle until the frame count reached the specified periodicity limit (512 frames in our case or 5.12 seconds). The MI works similar to MJ, the main difference being that instead of jamming a subframe, MI transmits a fake subframe and repeats it 24 times (every other fourth frame within 960ms)

7 Testbed

To study the feasability of the aforementioned Message Jamming (MJ) and Message Injection (MI) attacks on MIB-NB, SIB1-NB and SIB2-NB we constructed a tesbed. We use multiple Software Defined Radio (SDR) that act as the eNodeB, the targeted UE and the Jammer. Furthermore we use the srsRan open-source protocol stack which we extended. We also shift operations from the licensed band into the unlicensed frequency band.

Hardware For our testbed we chose three HackRF One SDRs by Great Scott Gadgets [7]. The HackRF One device is a SDR peripheral capable of transmitting and receiving radio wave between 1MHz to 6GHz. The device is an open-source platform that may function as a USB peripheral or programmed as a stand-alone device. In our scenarios all devices were used as peripheral. In terms of setup, the devices are arrange approx. one meter apart. All devices are tuned for the open frequency of 868MHz and calibrated by adjusting the offset in order to maximise the signal quality.

The HackRF One is a half-duplex SDR, meaning it can only transmit or receive data at one point in time. Due to the strict timing constraints that our experiments require we were able to only transmit or receive with one device. This constraint limited the capabilities of the Jammer as it could not react in real time by switching from the receiving to the transmitting state quickly enough. Thus, the Jammer is configured to produce signals relevant to the specific experiment. However, this limitation can be overcome by selecting a more capable SDR

Software srsRAN comprises UE and eNodeB protocol stacks that may be used in conjunction with third-party core network solutions to build full end-to-end mobile wireless networks. All srsRAN software is developed in Linux and runs on standard CPU's and radio equipment [6]. SrsRan provides a partial implementation of the NB-IoT protocol that allows messages to be sent up SIB1-NB [15]. To execute our experiment, we needed to add the capability of sending the SIB2-NB to srsRan. To minimize packet overlapping, we changed the current code to take the Hyper Frame Number (HFN) into account and to verify that the eNodeB is not already delivering other data. The main configuration of the downlink channel for transmitting the SIB2-NB was set as follows: *si_periodicity* = 512; *si_repetition_pattern* = 4 (every fourth frame); transport block size *si_tb* = 440; window length *si_window_length* = 960. We have made the code available via a GitHub repository [8].

Table 1. Measurement of MIB-NB, SIB1-NB and SIB2-NB in terms of Time active receiving (T_R), Time delayed (T_D) and Time active jamming/injecting (T_J)

Target	User Equipment Measurement		MJ	MI
	T_R	T_D	T_J	T_J
MIB-NB	64ms	640ms	8ms	1ms
SIB1-NB	32ms	2560ms	4ms	4ms
SIB2-NB	192ms	5120ms	24ms	24ms

8 Evaluation

We use the aforementioned testbed to evaluate the jamming based battery depletion attacks. We use three HackRF One devices arranged in a line approximate 1m apart. The Jammer is placed in between the targeted UE and the eNodeB.

Jammer Feasibility We use the testbed to verify that the described MJ and MI attacks are feasible.

For the MJ attack we use 802.15.4 Quadrature Phase Shift Keying (QPSK) modulated noise transmitted by the Jammer in the slot as a valid subframe transmitted by the eNodeB. In our setup a jamming transmission power setting of -38db is required to prevent the receiver from decoding a subframe with high success probability (above 99%).

For the MI attack the Jammer is transmitting a valid subframe at the same time the eNodeB transmits a subframe as well. We then test if the UE receives either the subframe transmitted by the eNodeB or the Jammer. At a transmission power level of -57db the UE has a high success probability (above 99%) of decoding the transmission from the Jammer.

The results are interesting for two reasons. First, it is possible for the Jammer to replace individual subframes in the downstream channel. As the initial communication is not cryptographically secured it allows an attacker opportunities byond the battery depletion attacks discussed in this work. Second, the transmission power level required for a MI attack is lower than for an MJ attack. To conserve power a Jammer might therefore choose to inject (malformed) messages instead of blocking messages using simple noise.

We believe that MI attacks are possible due to the capture effect also known as a Physical Signal Overshadowing (SigOver) attack [18].

Energy Depletion The aim of the attacker is to deplete the UE's battery without preventing communication. Interference with MIB-NB, SIB1-NB and SIB2-NB will force the UE to keep listening for longer than necessary which drains the battery. To measure the effectiveness of a jamming attack we determine the additional receive time that the UE is forced to spend receiving. However, the maximum additional time that can be achieved by an attack depends on the implementation specifics of the UE; it is not governed by the NB-IoT standard. For example, if the UE is programmed to allow for a repetition of 5 MIB-NB before the connection is deemed unsuitable then a jamming attack on the MIB-NB can prolong UE listening for as long it takes to receive the MIB-NB components 4 times. At this point it has to be noted that some UE implementations may not define a repetition counter and may try to listen for the MIB-NB infinitely. To assess the effectiveness of the jamming attacks independent of a repetition counter we therefore determine

the additional listening time T_R by preventing the reception of one MIB-NB, SIB1-NB or SIB2-NB. We also determine T_D which describes the additional overall time required to wait for a re-transmission. For an attack on the MIB-NB $T_R = 64ms$ is achieved as the MIB-NB is transmitted over 64 subframes of 1ms length in which the UE must listen. $T_D = 640ms$ as the 64 transmissions are sent in every 10th subframe. Attacking the SIB1-NB results in $T_R = 32ms$ and $T_D = 2560ms$ and attacking SIB2-NB results in $T_R = 192ms$ and $T_D = 5120ms$. The achievable additional listening time T_R is independent of the attack form (either MJ or MI). The results are summarised in Table 1.

If we assume a scenario where the entire communication procedure as shown in Figure 1 requires 23360mW and an additional listening of 1ms costs 80mW and we further assume the UE allows a repetition of 10 for each message type, the following energy depletion results are achieved: Attacking the MIB-NB would expand energy consumption of the UE by 297.2%, attacking the SIB1-NB increases consumption by by 198.6% and attacking the SIB2-NB by 691.7%.

Jamming Efficiency The Jammer aims to remain hidden and also aims to spend as little energy as possible for completing its task. Thus, complementary to the evaluation of the previously outlined energy depletion, it is useful to evaluate the jamming duration. We determine T_J which denotes the time the Jammer must be active to prevent reception of one MIB-NB, SIB1-NB or SIB2-NB. T_J here can be different in case of the attack form (either MJ or MI). In case of MJ attacks on MIB-NB, SIB1-NB and SIB2-NB result in $T_J = 8ms$, $T_J = 4ms$ and $T_J = 24ms$. For MI attacks $T_J = 1ms$, $T_J = 4ms$ and $T_J = 24ms$ are achieved. The results are summarised in Table 1.

In case of an injection of a false MIB-NB CSB the attacker must only be active for one repetition instead of eight repetitions when using MJ.

Using MI attacks is beneficial for the attacker as it requires less energy; less transmission power is required for this type of interference and in case of MIB-NB less subframes must be jammed to be effective.

9 Conclusions

In this paper, we showed a test-bed built on the HackRF One platform [7] and the srsRAN software [6]. We used this setup to test different types of battery depletion attacks and then shared the results. We've shown that these kinds of attacks are feasible and can have a great impact to the end device. We also made the source code available so that it could be used for further research. Our next step is to develop on top of the srsRan software so that the eNodeB and UE can communicate to each other on both the downlink and uplink channels. We also plan to recommend improvements that will help make the NB-IoT and it's implementation more resilient against battery depletion attacks.

Acknowlegement

This publication has emanated from research conducted with the financial support of Science Foundation Ireland under Grant number 18/CRT/6222 and 13/RC/2077_P2. For the purpose of Open Access, the author has applied a CC BY public copyright licence to any Author Accepted Manuscript version arising from this submission.

10 References

[1] 3GPP. 3gpp release 16.

[2] 3GPP. Evolved universal terrestrial radio access (e-utra); physical layer; measurements.

[3] L. Buttyán and L. Csik. Security analysis of reliable transport layer protocols for wireless sensor networks. In *2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, pages 419–424, 2010.

[4] X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou, and J. Chen. Ghost-in-zigbee: Energy depletion attack on zigbee-based wireless networks. *IEEE Internet of Things Journal*, 3(5):816–829, 2016.

[5] H. Fattah. *5G LTE Narrowband Internet of Things (NB-IoT)*. 09 2018.

[6] I. Gomez-Miguelez, A. Garcia-Saavedra, P. Sutton, P. Serrano, C. Cano, and D. Leith. srslte: an open-source platform for lte evolution and experimentation. pages 25–32, 10 2016.

[7] HackrfOne. Hackrf one.

[8] V. Ionescu. https://github.com/ionescuvlad12/srsran-nb_iot.

[9] V. Ionescu and U. Roedig. *Battery Depletion Attacks on NB-IoT Devices Using Interference*, pages 276–295. 01 2022.

[10] R. Krejčí, O. Hujňák, and M. Švepeš. Security survey of the iot wireless protocols. In *2017 25th Telecommunication Forum (TELFOR)*, pages 1–4, 2017.

[11] C. Pielli, F. Chiariotti, N. Laurenti, A. Zanella, and M. Zorzi. A game-theoretic analysis of energy-depleting jamming attacks. In *2017 International Conference on Computing, Networking and Communications (ICNC)*, pages 100–104, 2017.

[12] H. Pirayesh and H. Zeng. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey, 2021.

[13] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. McDaniel, M. Kandemir, and R. Brooks. The sleep deprivation attack in sensor networks: Analysis and methods of defense. *International Journal of Distributed Sensor Networks*, 2(3):267–287, 2006.

[14] C. Pu. Energy depletion attack against routing protocol in the internet of things. In *2019 16th IEEE Annual Consumer Communications Networking Conference (CCNC)*, pages 1–4, 2019.

[15] A. Puschmann. Release srslte 20.04 · srsran/srsran.

[16] V. Shakhov. On a new type of attack in wireless sensor networks: Depletion of battery. In *2016 11th International Forum on Strategic Technology (IFOST)*, pages 491–494, 2016.

[17] E. Y. Vasserman and N. Hopper. Vampire attacks: Draining life from wireless ad hoc sensor networks. 2013.

[18] H. Yang, S. Bae, M. Son, H. Kim, S. M. Kim, and Y. Kim. Hiding in plain signal: Physical signal overshadowing attack on LTE. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 55–72, Santa Clara, CA, Aug. 2019. USENIX Association.