Battery Depletion Attacks on NB-IoT Devices using Interference

Vlad Ionescu and Utz Roedig

School of Computer Science and Information Technology, University College Cork, Cork, Ireland
v.ionescu@cs.ucc.ie, u.roedig@cs.ucc.ie

Abstract. 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 deployed devices ($\tilde{1}$0 years). In this paper, we document two interference attacks on the NB-IoT communication link that lead to a battery depletion in devices. These attacks can be carried out without disruption of data delivery and are therefore hard to detect. We describe a Matlab based simulation environment that can be used to investigate interference on NB-IoT communication, and we then use this environment to study the two attacks. For example, we show that battery lifetime can be reduced from 17 years to as low as four months.

1 Introduction

NB-IoT is a relatively new LPWAN technology developed by 3rd Generation Partnership Project (3GPP). NB-IoT aims to provide low-cost devices with long battery life and supports a high connection density. NB-IoT makes use of a subset of the Long-Term Evolution (LTE) standard, limiting the bandwidth to a single narrow-band of 200kHz. As the technology uses the existing LTE infrastructure, deployment of devices is simplified as the existing base station infrastructure can be used. NB-IoT devices are increasingly used to implement Internet of Things (IoT) applications such as smart cities, industrial automation and smart grids. To be commercially viable, these applications require a very long device lifetime. Frequent battery changes in devices are not feasible as this would increase maintenance costs to a point where the application is not viable. Therefore, a device battery lifetime of many years (10 years in most commercial settings) is required.

The energy consumption of an IoT device is in most cases dominated by communication. By choosing a low communication duty cycle, it is possible to achieve the required ten year lifetime of a device. In this case, a duty cycle is chosen where a node wakes once a day to report sensed information via the LTE base station infrastructure to a back-end.

The communication link between the NB-IoT device and the base station is dynamically adjusted to the communication environment. This is done to balance

communication reliability and energy consumption. For example, transmission power and the number of transmission repetitions are dynamically adjusted to compensate for link quality fluctuations. As the communication protocol allows for dynamic adjustments, it provides an angle of attack for an adversary. An attacker can interfere with the communication link such that (i) communication is still possible and (ii) the energy consumption of a device is maximised. An interferer can execute a *battery depletion attack*.

To the best of our knowledge, this work is the first study of energy depletion attacks via an interferer on NB-IoT devices. We present two different methods an attacker can employ to interfere with the communication, increasing device energy consumption. We use a customised Matlab simulation environment to investigate communication between NB-IoT devices and base-station. We show that such attacks can reduce device lifetime significantly. Thus, such attacks can be used to render an IoT deployment commercially infeasible. At the same time, such attacks are hard to detect as data communication from the NB-IoT device is not prevented, and the attacker is not continuously jamming as these activities are carefully timed.

The main contributions of our work are:

- *NB-IoT Battery Depletion Attacks:* We describe in detail two possible attacks on NB-IoT communication via interference that result in energy depletion.
- *NB-IoT Simulation:* We describe our extension to the Matlab simulation environment that can be used to evaluate NB-IoT communication and interference of an attacker with it.
- *NB-IoT Battery Depletion Attack Analysis:* We provide a thorough analysis of the impact of the NB-IoT battery depletion attacks. We show that a device lifetime reduction from 17 years to around four months is feasible.

In the next section, we describe related work. In Section 3 we give a brief overview of NB-IoT, describe the attacker (threat model), and we describe in detail the identified NB-IoT battery depletion attacks. Section 4 describes the evaluation scenario, metrics used for assessment and the simulation environment that was developed. In Section 5 we describe our obtained results and also discuss possible countermeasures. Section 6 concludes the paper.

2 Related Work

Battery depletion attacks on wireless devices is a well-known class of attack that has received a lot of research attention over recent years.

Energy depletion attacks, in general, aim at tricking a device into spending unnecessary effort on tasks that lead to energy depletion. For example, a device can be forced to spend additional computational effort [24] or prevented from entering into an idle or sleep state [22], also known as a sleep deprivation attack. Another common approach is to force a device to perform unnecessary communication as the additional transmissions and receptions require additional

energy [7]. Such an attack is particularly effective on small embedded devices (IoT devices, sensor nodes) where the communication transceiver dominates energy consumption.

Forcing a device into unnecessary communication can be achieved in different ways. An attacker may target an individual device or the network as a whole. To attack an individual device, the attacker may send messages to the device which response, for example, to state that such message is incorrect (see Vasserman et al. [26], and Krejčí et al. [12] for examples). Of course, such an attack is only possible if the protocol allows for such a situation to occur. The attacker may also target the behaviour of the entire network. A popular approach here is to target the routing protocol (see Buttyán et al. [6], and Pu et al. [23] for examples). The attacker may be able to insert a node in the network which modifies routing behaviour such that messages have to travel unnecessary long paths or are frequently dropped, requiring retransmissions. Again here, the used protocols must enable such attack.

The approach investigated in this paper is to use interference as a form of attack leading to battery depletion. An attacker may use an interference signal such that a node is spending additional effort in communication. For example, a node may use increased transmission power or additional transmissions to compensate for the perceived communication channel degradation. If a node does not limit this adaptation, it can lead to significant battery drain. To the best of our knowledge, such interference-based attacks on NB-IoT nodes have not yet been explored.

Hossein et al. [21] review existing jamming attacks and anti-jamming approaches in Wireless Local Area Networks (WLAN) including but not limited to cellular networks, ZigBee networks, LoRa networks, Bluetooth networks, vehicular networks and others. The article presents an in-depth analysis of jamming and anti-jamming techniques, as well as an insight into the design of jamming-resilient wireless networks.

Chiara et al. [20] emphasise the vulnerability of IoT networks with battery-powered nodes against jamming. Moreover, the authors state that an attacker can reduce the lifetime of energy-constrained User Equipment (UE)s by disrupting packet delivery. By considering a scenario as a multistage game, the article determines optimal strategies for both sides and evaluates their impact on network performance. Furthermore, they highlight the compromise between battery lifetime and the reliability of communication and the impact a jamming device has on both.

Andres et al. [4] propose an NB-IoT energy consumption model and validate it in an experimental setup used to measure the energy consumption of UE connected to a base station emulator. The article analyses the latency and battery lifetime needed for the control plane procedure. The energy expenditure estimation resulted in a maximum relative error of 21% between the proposed model and the measurement setup. Furthermore, the authors conclude that the NB-IoT lifespan target of ten years is feasible as long the traffic profile has a

large assumed interarrival time or the radio resources' configuration does not demand an extensive number of repetitions.

3 NB-IoT Battery Depletion Attacks

3.1 NB-IoT

NB-IoT is a LPWAN technology introduced by 3GPP for data gathering designed for low-data-rate applications. [8]. For example, common usage of the protocol might be found in smart metering or intelligent environment monitoring devices. [2].

For communication purposes, NB-IoT can be deployed as standalone, in-band or guard-band as depicted in Figure 1. For in-band and guard-band, the protocol occupies one Physical Resource Block (PRB) of 180 kHz for the downlink and uplink in the LTE spectrum. By "refarming" the GSM spectrum, the standalone deployment inhabits a 200 kHz bandwidth [13, 17]. Furthermore, to support the massive deployment target of 1 million connected devices for every square kilometre, tones (frequency domain) with different time allocations are assigned to the User Equipment (UE). This allows the network to allocate one Resource Unit (RU) to multiple UE, contrary to LTE, where every UE is assigned one RU [27]. One tone can occupy 3.75 kHz or 15 kHz bandwidth for uplink using the Single-Carrier Frequency-Division Multiple Access scheme (SC-FDMA) scheme and 15 kHz bandwidth based on the Orthogonal Frequency Division Multiplexing (OFDM) scheme similar to LTE. While on 15 kHz spacing, either single-tone (8 ms) or multi-tone 12, 6 and 3 tones with a span of 1 ms, 2 ms or 4 ms can be used for various UEs, on the 3.75 kHz spacing, only single-tone allocation is supported to several UEs with the duration of 32 ms [3, 5, 17].

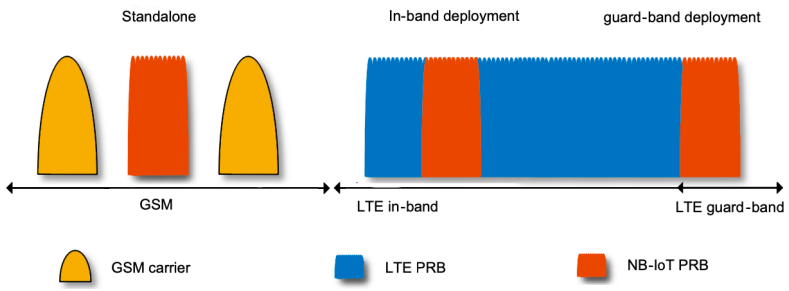

Fig. 1: NB-IoT Deployment Modes

The NB-IoT utilises the frame structure of LTE with 1024 hyper frames. One hyper frame contains 1024 frames, and each frame consists of 10 subframes with two slots of 0.5 ms. In the frequency domain, 12 subcarriers with seven OFDM symbols are mapped to every slot. Furthermore, when the 3.75 kHz spacing is used for the uplink, 48 subcarriers are allocated with a slot span of 2 ms.

Several channels and signals are used for both downlink and uplink to facilitate the communication between the base station and the UE.

Downlink The following are used for the downlink communication, and their allocation is shown in Figure 2

- Narrowband Reference Signal (NRS).
- Narrowband Primary Synchronization Signal (NPSS).
- Narrowband Secondary Synchronization Signal (NSSS).
- Narrowband Physical Broadcast Channel (NPBCH).
- Narrowband Physical Downlink Shared Channel (NPDSCH).
- Narrowband Physical Downlink Control Channel (NPDCCH).

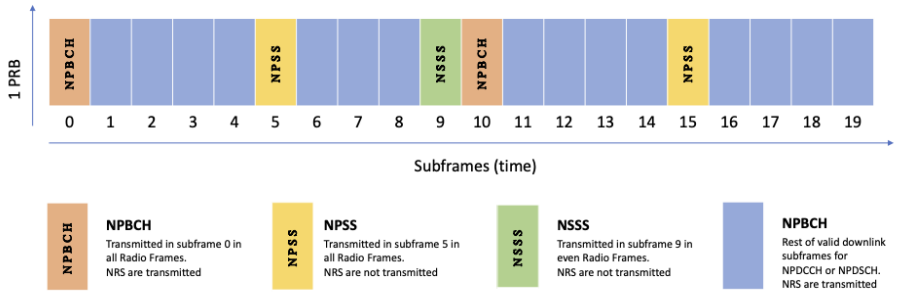

Fig. 2: Subframe Channel Assignments

The UE uses the NRS for cell searching and initial system acquisition. Following this, the NPSS and NSSS are utilised for frequency and timing synchronisation with the base station. After the initial correlation, the UE is ready to acquire the Master Information Block (MIB), which is carried by the NPBCH, as well as the Narrowband System Information Block 1 (SIB1-NB) provided by the NPDCCH, which provides the timing configurations for the remaining System Information Block (SIB)s. Finally, the NPDSCH is used by the base station for transmitting the data packets. [13]

Uplink For the uplink, the following channels and signals are used for communication

- Narrowband Physical Random Access Channel (NPRACH).
- Narrowband Physical Uplink Shared Channel (NPUSCH).
- Demodulation Reference Signal (DMRS).

The UE utilises the NPRACH to conduct the initial access to the network and request the transmission resources or reconnect in case of a link failure. NPUSCH is used to send the uplink data packets, while DMRS is used to estimate the channel accuracy. [17]

One advantage of the NB-IoT protocol is its capability to enhance the coverage area for rural and deep indoor applications. Furthermore, by delivering an extra 20 dB compared to LTE, NB-IoT can operate at 164 Maximum Coupling Loss (MCL) with up to 128 retransmission for uplink and 2048 for downlink, therefore making the protocol suitable for latency insensitive applications with up to ten seconds of transmission delay.

3.2 Threat Model

We assume two scenarios: *simple jammer* and *intelligent jammer*.

Simple Jammer A simple jammer is a device that can output a continuous interference signal. The signal power can be adjusted, but the attacker is not able 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]. Furthermore, the device needs to have configurable transmission power to degrade the signal's quality and not just block communication entirely. In order to perform the attack, a constant power supply is needed as a limited one would not be feasible for an energy depletion attack.

Intelligent Jammer An intelligent jammer is outputting an interference signal at precise times. The device can follow the communication on the channel that it is attacking. Depending on observations, jamming times and signal power can be adjusted. However, they cannot decrypt observed communication; only unencrypted data and aspects such as slot occupancy and transmission times are available to the attacker.

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 eavesdropping on the downlink channel while reacting on the uplink channel and the other way around. Because of the nature of the NB-IoT protocol described in Sectiopn 3.1, data such as NRS, NPSS, NSSS, MIB, SIB1-NB, Narrowband

System Information Block 2 (SIB2-NB), and others are sent unencrypted in order to perform synchronization, and authentication [13], thus making the end device vulnerable to energy depletion attacks. An intelligent jammer can use such exposure to gain more information about the communication and pressure the legitimate devices to increase their transmission power and the number of repetitions while remaining hidden.

3.3 Degradation of Quality of Signal (DQS) Attack

The LTE specification provides a set of data and parameters to estimate the channel between an eNodeB and a UE [2]. In order to properly evaluate the QoS in an NB-IoT network, we have to look at both the downlink radio channel as well as the uplink one. The downlink radio channel is estimated with the help of the Narrowband Reference Signal (NRS), while on the uplink side, the estimation is done using the Single-Carrier Frequency-Division Multiple Access scheme (SC-FDMA) within a resource grid that is configured to use either a 15 kHz or a 3.75 kHz

Downlink Radio Channel Quality of Signal (QoS) Estimation In the downlink channel, the NRS can be found in the last two OFDM symbols of each slots [16]. In Figure 2, an adaptation from [11], a graphical representation depicts the subframes by index from zero to 19 within one PRB. It is worth noting that NPSS, NSSS and NPBCH have set channel assignments according to the NB-IoT standard and that the NRS can be transmitted in all subframes except NPSS and NSSS.

Furthermore, multiple parameters and their relationships have to be described in order to properly assess the impact of decreasing the QoS by adding noise to the transmission.

- Reference Signal Received Power (RSRP), according to the 3GPP definition, is the linear average over the power in Watts of the resource elements that carry NRS [2]. Due to the fact that NB-IoT downlink is an OFDM transmission with 15 kHz carrier spacing, the RSRP will become the power of a single 15 kHz NRS.
- Received Signal Strength Indicator (RSSI) is the linear average of the total power received by a device in Watts only from the configured OFDM symbol and in the measurement bandwidth over N number of resource blocks, by the UE from a multitude of sources, including co-channel, adjacent channel interference, thermal noise and others. Because the downlink is deployed with a 15 kHz spacing and always uses 12 subcarriers, the evaluated bandwidth is equal to

$$15kHz * 12 = 180kHz \tag{1}$$

  or exactly one PRB. Moreover, depending on the cell load, the RSSI varies according to the allocated subcarriers [16].

– Reference Signal Received Quality (RSRQ) is defined as the ratio RSRP and RSSI, with the constraint that both the numerator and denominator shall be measured in the same set of resource blocks.

$$\text{RSRQ} = \frac{\text{RSSI}[W]}{\text{RSRP}[W]} \tag{2}$$

– The Signal-to-Interference and Noise Ratio (SINR) is the ratio between a received signal level and the Interference amount (PI) from other sources, along with the Effective Noise Floor ($P_{N,eff}$).

$$\text{SINR} = \frac{\text{RSRP}[W]}{P_{I,15kHz} + P_{N,eff,15kHz}} = \frac{\text{RSSI}[W]}{P_{I,180kHz} + P_{N,eff,180kHz}} \tag{3}$$

Matz et al. [16] validated the correlation between SINR and RSRQ via the subcarrier activity factor x as the ratio occupied by the Resource Element (RE) in a Resource Block (RB): x=RE/RB, thus proving the relation derived in [19]

$$\text{SINR} = \frac{12}{\frac{1}{\text{RSRQ}} - \text{RE}} = \frac{12}{\frac{1}{\text{RSRQ}} - 12 * x} \tag{4}$$

Uplink Radio Channel QoS Estimation MCL is a parameter calculated by substrating the Receiver Sensitivity ($P_{RX,min}$) from the Power Level at the Antenna Connector (P_{TX}):

$$MCL = P_{TX} - P_{RX,min} \tag{5}$$

MCL is a key metric to estimate the radio coverage, and in the case of NB-IoT, it is used to set up the number of repetitions and the P_{TX}. Furthermore, in the case of uplink for up to two repetitions, the UE adjust the P_{TX} based on multiple cell variables, including coupling loss. In case of more than two repetitions are needed, a maximum cell-specific P_{TX} is used. The receiver sensitivity $P_{RX,min}$ represents the smallest input energy level at the receiver antenna compared to a QoS threshold. To further understand the MCL complexity, the following notions have to be explained. NB-IoT has the capability to dynamically adjust the Modulation and Coding Scheme (MCS) depending on the radio conditions. The MCS is defined as how many useful bits can be carried per RE, resulting in the MCS being directly correlated with the radio link quality and error probability. In other words, MCS is periodically adjusted in order to keep the connection within a Block Error Rate (BLER) threshold, typically 10% for the NPUSCH) and NPDSCH NB-IoT channels [13]. NB-IoT can further extend its range by increasing the number of symbol repetitions NRep. Consequently, the BLER becomes dependent on the MCS and the Nrep used for any given Signal-to-Noise Power Ratio (SNR). The Minimum Signal-to-Noise Power Ratio (SNR_{min}) needed for the aforementioned BLER has to take into consideration firstly the thermal noise as defined below:

$$P_N = 10 * log(kTB/1mW) \tag{6}$$

where k = Boltzmann constant, T = temperature, B = bandwidth. According [16] and [13] the $P_{N,eff}$ is defined as the Noise Figure (NF) of the receiver front-end in addition to the Thermal Noise (P_N). Taking the previous definitions into account the $P_{RX,min}$ can be defined as:

$$P_{RX,min} = P_N + NF + SNR_{min} = P_{N,eff} + SNR_{min}. \tag{7}$$

By understanding the full involvement of the MCL in the NB-IoT capability to adjust the number of repetitions and the power transmission, a malicious entity could exploit it by adding noise to the subframes carrying the NRS on the downlink channel and to the NPUSCH. By doing so, the attack will trick both the base station and the UE into higher coverage levels, increasing power consumption drastically. An example of such noise is the Additive White Gaussian Noise (AWGN). AWGN is a theoretical term for noise that can occur in many natural processes. For example, if we consider the is NPDSCH transmitted at P_{TX} = 35dBm and a scenario at room temperature, T = 290 Kelvin, for a bandwidth of 180kHz with a noise figure equal to 7dB, the effective noise power would be calculated as:

$$P_{N,eff} = 10 * log(k * 290 * 180) + 7dB = -104.4dB \tag{8}$$

Furthermore by considering a SNR_{min} at a medium coverage level at -14dB, we could finally calculate the MCL as:

$$\text{MCL} = P_{TX} - P_{RX,min} \approx 154dB \tag{9}$$

In order to maximise the efficiency of such an attack, an intelligent jamming device can be used. Roger et al. [10] describe a low-power intelligent jamming device that is capable of targeting specific control channels. Another effect of such intrusion would force the carrier to allocate more resources in the form of subcarriers, thus reducing the bandwidth. Because this type of attack does not aim to interrupt the communication immediately, it is harder to detect than full jamming. Additionally, the MCL increase could emerge naturally from the ever-changing environmental conditions, reducing suspicion.

To summarise, in order to effectively perform a Degradation of Quality of Signal (DQS) attack, the malicious device has to estimate the MCL class of the UE and adapt its transmission power to force base station and UE to allocate more resources in terms of the number of repetitions and the energy consumption.

3.4 Random Access Procedure (RAP) Attack

In NB-IoT, the RAP is done with the help of the Narrowband Physical Random Access Channel, also known as NPRACH.

Comparing to the LTE Physical Random Access Control Channel (PRACH), the NPRACH has been completely redesigned [14]. In contrast to the LTE

PRACH, which occupies a bandwidth bigger than the entire NB-IoT carrier up to 1.05 MHz, NPRACH is based on a Single-Tone configuration with frequency hopping and uses 3.75 kHz subcarrier spacing. Furthermore, it supports different cell sizes by providing two cyclic prefix lengths, thus utilising from 45 kHz to 180 kHz depending on the number of subcarriers [15]. In order to enhance the coverage, the transmissions can be repeated up to 128 times.

For the random access procedure to start, the UE needs to receive the SIB2-NB. In Figure 3 a complete procedure is illustrated, including the steps needed before and after.

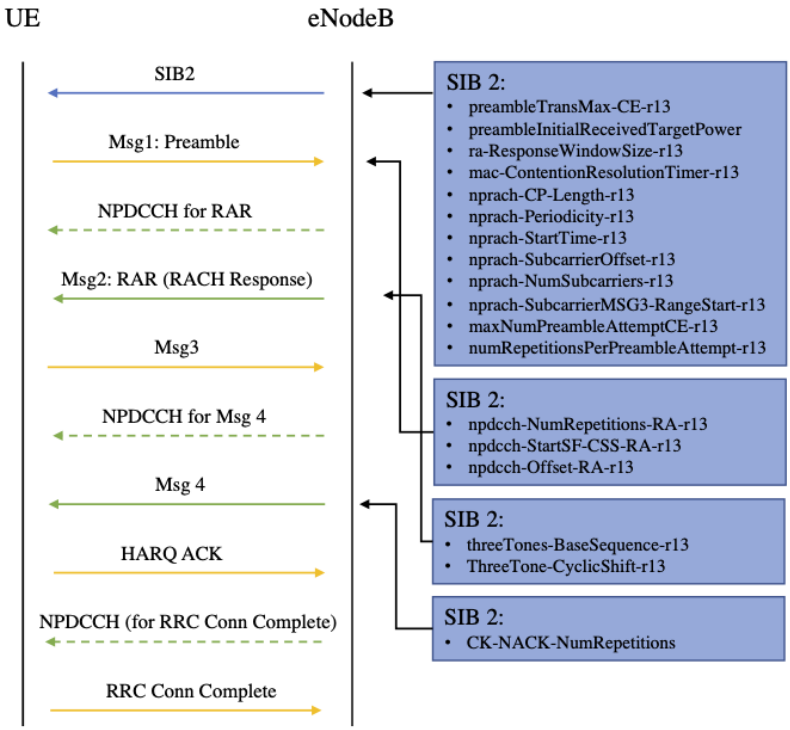

Fig. 3: Random Access Procedure and the related messages.

Because of the coverage enhancement feature, which allows transmissions to be repeated up to 128 times, the random access procedure can be vulnerable to energy depletion attacks. A smart jamming device, similar to the one described in section 3.3 can listen for the preamble message transmitted by the UE and jam the Random Access Response onto the NPDCCH. Another way of taking

advantage of the RAP is to deploy a Man in The Middle Attack by using a fake base station and alter the SIB2-NB in order to maximise the energy consumption used by the UE. It is worth mentioning that with 3GPP release 16 [1] the UE can have preconfigured resources, where up to two users can send NPUSCH simultaneously in the specific case when the latency is greater or equal to 64ms for 12-tone allocation. In case the UE is making use of the Preconfigured Uplink Resources (PUR), it can bypass both the Random Access Preamble Transmission (Msg1) and the Random Access Response (Msg2), thus reducing the power consumption and also reducing the efficiency of the aforementioned attacks [9].

In summary, a malicious entity can deploy a Random Access Procedure (RAP) attack by listening on the downlink channel and jam the Msg1 while counting the number of repetitions so that it will not exceed the configured number sent via SIB2, thus allowing the connection to be completed. Furthermore, to optimise the RAP attack, a MITM can be used to alter the maximum number of transmissions of Msg1 up to 128. The fake base station can also alter the cell ID, therefore invalidating the PUR settings of the UE [9].

4 Evaluation Setup

4.1 Evaluation Scenario

In order to analyse the impact of attacks, we use the following communication scenario: UEs are communicating with an eNodeB. The assumption is that the base station is always able to receive an uplink signal. Devices wake periodically every t hours and send a b_{up} byte-sized payload and receive a b_{down} byte payload. This is a common NB-IoT scenario used in deployments (see Liberg et al. [13]). A typical setting is $t = 2h$, $b_{up} = 200byte$ and $b_{up} = 60byte$.

The scenario is executed without any attack to establish a baseline in terms of the nodes energy consumption. Thereafter we run the same scenario with a present attack and compare the energy consumption with the baseline.

4.2 Evaluation Metrics

We use two parameters to judge how effective an attack is. The first parameter is Energy Depletion Rate (EDR) which describes how much an attack depletes a device battery compared to the baseline scenario without attack. The second parameter is Jammer Duty Cycle (JDC) which captures the percentage of time that the jamming device has to be active.

Energy Depletion Rate (EDR) The EDR is defined as:

$$EDR = 1 - \frac{E_{baseline}}{E_{attack}} \tag{10}$$

Here $E_{baseline}$ is the energy consumed by the UE during normal operation while E_{attack} is the energy consumption under a specific attack scenario. EDR produces

a value between 0 and 1; the attack is not effective for values close to 0, while values close to 1 indicate an effective attack. We use this metric also separately for transmission and reception of the UE in order to see if an attack has more impact on upstream or downstream channels.

Jammer Duty Cycle (JDC) The JDC is defined as:

$$JDC = \frac{T_{active}}{T_{total}} \tag{11}$$

Here T_{active} is the time the jamming device is transmitting a jamming signal while T_{total} is the experiment duration. JDC is a measure for the effort the attacker has to undertake to achieve their goal. It also describes how active an attacker is and how easy it might be spotted.

4.3 Simulation Environment

In order to simulate the battery consumption of NB-IoT devices, we used Matlab together with the LTE-Toolbox as our simulation environment. It is worth mentioning that the LTE-Toolbox implementation of the NB-IoT protocol is not a full end-to-end reactive simulation, thus focusing more on generating modulating, demodulating coding and decoding the appropriate waveform. For this reason, some of the parameters in our environment have to be set prior to executing the simulator (e.g. SIB2-NB maxPreambleTrans). In Figure 4 we can see a simulated waveform with the allocated subframes over the number of subcarriers.

For our scenario, we have chosen the three coupling loss specifications of NB-IoT as outlined by Liberg et al. [13]. These settings were used as the basis for defining the performance requirements and power consumption of the UE. By analysing the latest NB-IoT devices technical specifications, including the Sara N3-NB-IoT from U-Blox, 212 LTE IoT Modem from Qualcomm and averaging their power consumption, the following values were used: maximum $TX_{max} = 330mA$, and maximum $RX_{max} = 30mA$, $idle = 3mA$ and $deepsleep = 0.003mA$. Furthermore, to simulate the environment as close to real-life as possible, we have chosen a $1000mAh$ lithium polymer battery (LiPo) perfect battery at a nominal $3.7V$. The reason for choosing this battery is that it is one of the most popular, standard type LiPo batteries available on the market. However, the actual battery will likely be less reliable as we do not model the battery degradation and external factors such as temperature.

4.4 Jammer

We simulate 4 different jamming attacks:

– The simple jammer for decreasing the quality of the signal: simple Degradation of Quality of Signal Attack (sDQS)

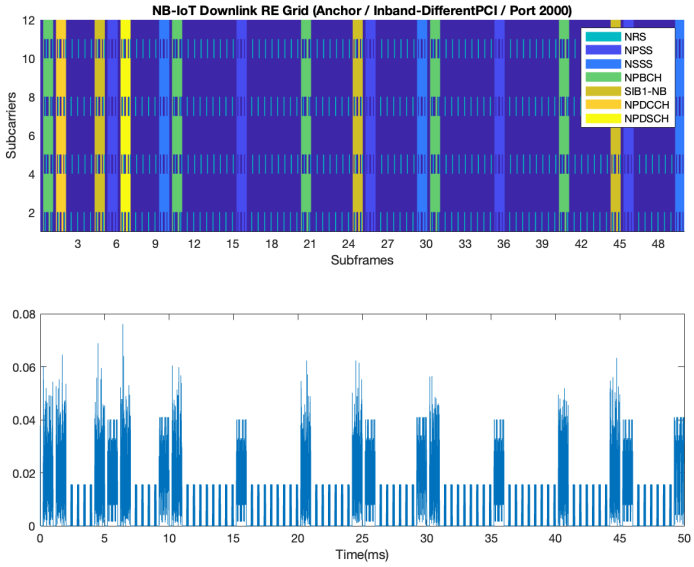

Fig. 4: NB-IoT waveform generated by the Matlab simulation environment. The upper representation displays the channels and signal assign to each subframe. The lower figure display the allocation of the same signals and channels in a time-frequency domain.

- The intelligent jammer for decreasing the quality of the signal: intelligent Degradation of Quality of Signal Attack (iDQS)
- The intelligent jammer targeting the random access procedure: Random Access Procedure (RAP)
- The intelligent jammer for decreasing the quality of the signal and targeting the random access procedure: (iDQS + RAP)

Both the sDQS and the iDQS attack were modelled in Matlab by adapting our base environment to maximise the resources needed to complete the communication. More specifically, setting the number of repetitions for both the downlink and uplink in accordance to the 164 MCL as described in Section 3.1 and the transmission power as specified in Section 4.3. Thus, on the one hand, the sDQS uses a simple AWGN function that adds noise to the legitimate signal depending on the transmission power. On the other hand, the iDQS comprises multiple steps, including but not limited to synchronisation, demodulation, decoding, MIB parsing, and BLER calculation and lastly, adding the AWGN to the signal. Furthermore, we assumed that the intelligent jammer has learned the communication pattern of the UE and that it is able to time the attack.

For the RAP vulnerability described in Section 3.4, we use our baseline environment as a starting point and then model only the access procedure. More

specifically, on the downlink channel, the jammer has to receive and correlate the NPSS and NSSS in order to be able to receive the MIB, which in turn is used for acquiring the other SIBs, especially SIB1-NB and SIB2-NB. After decoding and retrieving the information from SIB2-NB, the malicious device will start jamming on the uplink channel the Random Access Preamble Transmission (Msg1) in order to maximise the number of retransmissions according to the information obtained before. In Matlab, we simulated this by increasing the number of repetitions in the simulated RAP to 120 from the maximum of 128 and calculate the depletion rate and the duty cycle for sending the Msg1 but also for receiving the System Information Block 2 (SIB2).

5 Evaluation Results

5.1 Baseline

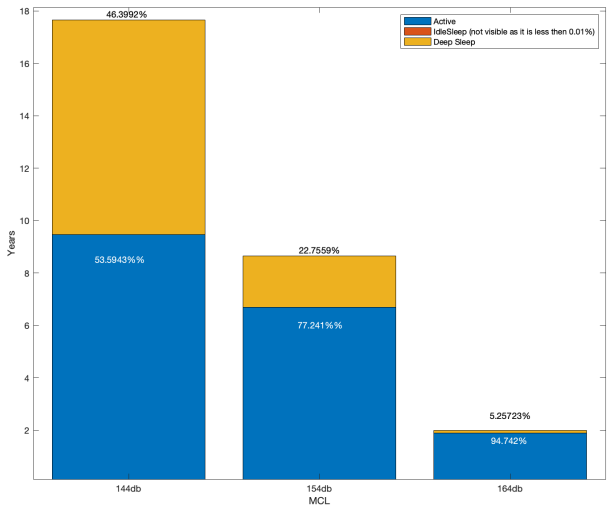

Fig. 5: Achievable battery lifetime of an NB-IoT node in our baseline scenario using communication parameter settings of $t = 2h$, $b_{up} = 200byte$ and $b_{up} = 60byte$ under different MCL scenarios. No jamming attack is present (Baseline Scenario).

The energy efficiency of NB-IoT devices varies a lot depending on the selected MCL. For our scenario presented in Section 4, Figure 5 depicts the years of battery life achieved and the percentage of energy spent in each communication state (Active (TX/RX), IdleSleep and DeepSleep). For this experiment the

communication parameters in our scenario are set to $t = 2h$, $b_{up} = 200byte$ and $b_{up} = 60byte$.

The simulation results for our baseline environment are in line with other results reported in literature [13]. We observe that only the MCL = 144db setting achieves the 3GPP standard requirements in terms of lifetime [2]. It is worth noting that the reporting interval of $t = 2h$ might be considered aggressive, but many real-life applications are requiring such a schedule.

5.2 Jamming

Table 1 summarises the results of our evaluation assessing EDR and JDC for the different attack types considered (sDQS, iDQS, RAP and iDQS + RAP). Communication parameter settings of $t = 2h$, $b_{up} = 200byte$ and $b_{down} = 200byte$ are used here.

Table 1: EDR and JDC for the different attack types considered (sDQS, iDQS, RAP and iDQS + RAP).

Type	EDR	JDC
1.Baseline	0	0.0003
2.sDQS	0.41	1
3.iDQS	0.41	0.0026
4.RAP	0.76	0.0223
5.iDQS + RAP	0.85	0.0246

Simple Jammer The simple jammer executing the sDQS attack is, as expected, the most inefficient approach in terms of JDC. In terms of attack performance it is equivalent to iDQS (see Table 1). However, this is only the case if the transmission power of the jamming signal is set correctly (as we have done in this simulation). If the transmission power is too high, the signal will be entirely blocked instead of degrading it. In this case, the battery lifetime of a UE actually increases as the device is prevented from communicating at all. The simple jammer cannot learn which transmission power to use to effectively jam as it cannot observe the effect of its jamming. Thus, this type of attack may be difficult to execute in practice.

Intelligent Jammer The effectiveness of the intelligent jammer is dependant on the type of attack considered (iDQS, RAP and iDQS + RAP). As expected, the efficiency in terms of JDC is much greater than in the case of a simple jammer (see Table 1). The RAP attack is more efficient from the attackers perspective

than iDQS (achieving an EDR of 0.76 compared to an EDR of 0.41). However, the RAP attack is significantly more energy costly (JDC of 0.0223 compared to a JDC of 0.0026). The combination of both attack types requires a JDC combining the effort for both attacks, which leads to the highest attack success with an EDR of 0.85. Next, we evaluate the effectiveness of the intelligent jammer in more detail, considering variable payload sizes for up and downlink (b_{up} and b_{up}). Figure 6 shows the resulting EDR separately for uplink and downlink (TX/RX). Figure 7 shows the combined EDR together with the JDC.

In Figure 6, we can see the different types of depletion rates based on the chosen attack over the payload size for sending and receiving. The chart is based on multiple simulations with different payload sizes, ranging from 0 to 300 bytes (for b_{up} and b_{up}). The EDR varies from zero to one, where zero represents the baseline with no interference present while 1 expresses an attack with a 100% impact on the battery. On the left side, coloured in blue, we can see the receiving depletion rate for the iDQS, RAP and iDQS+RAP attacks, while at the same time, on the right side, coloured in orange, we show the sending depletion rate. While the iDQS has the smallest impact compared to other attacks, we can observe that its impact is nonlinear, and it increases with payload size. Contrary to iDQS, the RAP attack has a constant impact as it targets only the random access procedure. However, upon further analysing, we can see that the RAP+iDQS attack depletes the most energy for sending and receiving data. As expected, the energy depletion rates have less impact on the receiving side, ranging from zero to approximately 0.55 compared to the sending side, which varies from zero to roughly 0.9. This difference is caused mainly by the fact that the UE spends more energy while transmitting data than receiving.

In Figure 7, we see the combined EDR coloured in blue together with JDC coloured in orange. The iDQS attack though not the most effective in terms of EDR has the most significant difference between the JDC and EDR (A high impact is achieved for little effort). The latter increases significantly over the payload size, thus expanding the gap even further. Identically to the chart presented in Figure 6, the RAP attack has a linear impact on both JDC and EDR, as the payload size does not influence the random access procedures. On the other hand, we can observe that when we combine iDQS+RAP in the same attack, the impact converse compared with only iDQS. The EDR in this case increases slightly with the payload size while the JDC has a steeper ascending trajectory.

5.3 Evaluation Discussions

The simple jammer is easy to construct. However, it requires a constant battery supply, and it will be easy to spot as it is continuously active. Furthermore, as this jammer cannot observe the communication channel, it cannot adjust the power of the interference signal. Thus, it might be challenging to execute this attack efficiently in practice, and by interfering too much, the entire communication may be blocked. In this case, the intended battery depletion attack results in a communication denial of service attack.

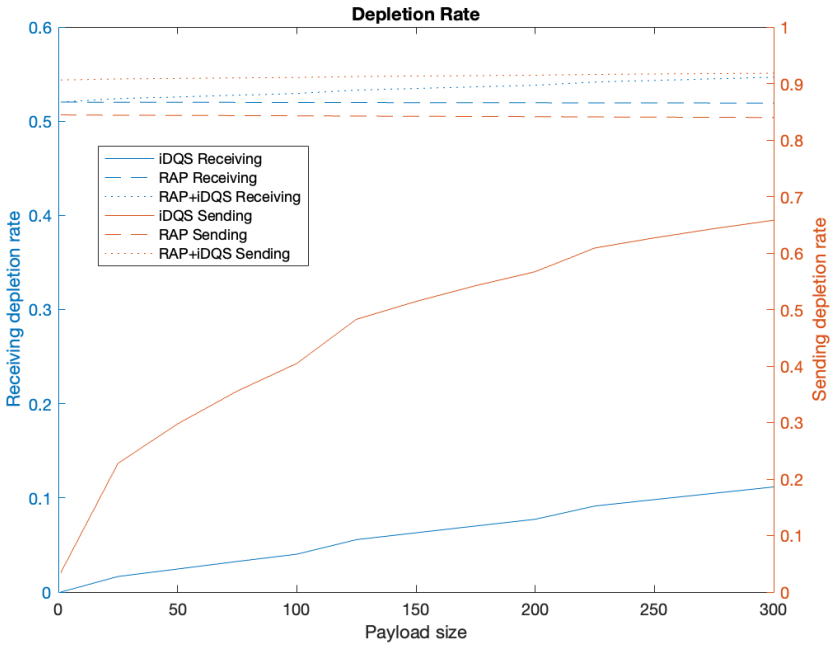

Fig. 6: EDR, separately shown for reception and transmission channel, for the different attack types considered (iDQS, RAP and iDQS + RAP). Communication parameter settings are $t = 2h$, $0 < b_{up} = 300byte$ and $0 < b_{down} < 300byte$.

The intelligent jammer is much more challenging to construct. The communication must be observed, and jamming is executed at specific times. Thus, it is very difficult to spot the attacker as the attacker is only active in very brief time periods. Furthermore, as activity is only briefly necessary, it is possible to deploy the jammer as a battery-powered device. This further enables the attacker to hide their malicious activity. For example, when executing the iDQS attack, the most efficient attack in terms of JDC using $t = 2h$, $b_{up} = 200byte$ and $b_{down} = 200byte$ requires a =JDC of only 0.0026. If the jammer uses the same construction as the NB-IoT device (In terms of transceiver power consumption and battery), a jammer lifetime of two years is possible.

The intelligent jammer can significantly reduce battery life. The baseline scenario shown in Figure 5 supporting over 17 years of operation is only able to support around two years under an iDQS attack, six months under an RAP attack and as little as four months when both attacks are combined.

5.4 Countermeasure

One effective countermeasure that would prevent the intelligent jammer from learning the communication schedule of an NB-IoT device is to become active

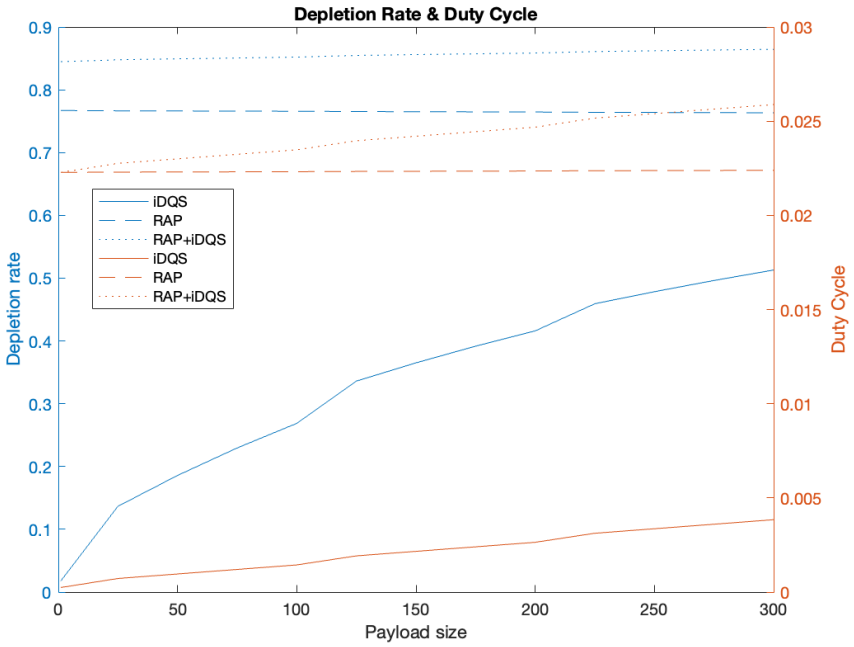

Fig. 7: EDR and JDC for the different attack types considered (iDQS, RAP and iDQS + RAP). Communication parameter settings are $t = 2h$, $0 < b_{up} = 300byte$ and $0 < b_{down} < 300byte$.

to transmit and receive data at random times rather than a fixed schedule (i.e. every two hours). This would force the intelligent jammer to consume more resources in synchronising with the communication. One such example where the UE is required to transmit every two hours would be to keep an average of 12 transmissions per day but randomly select the time slots within an interval.

6 Conclusion

We have shown by simulating the NB-IoT communication that different types of jamming attacks can significantly impact the lifespan of the UE with over 90% energy depletion, resulting in a decrease of device lifetime from over 17 years to around four months. Clearly, a jamming device using the attacks described in this work can be used to render any NB-IoT deployment commercially infeasible. Therefore, more consideration to jamming attacks should be given before rolling out NB-IoT installations on a large scale. Our next steps are to improve the simulation environment to perform a more comprehensive analysis and devise appropriate countermeasures as briefly outlined in the previous section.

Acknowledgement

This publication has emanated from research conducted with the financial support of a grant from Science Foundation Ireland under Grant number 18/CRT/6222. 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

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/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2428
3. Adhikary, A., Lin, X., Eric Wang, Y.P.: Performance evaluation of NB-IoT coverage. In: IEEE Vehicular Technology Conference (2016). https://doi.org/10.1109/VTCFall.2016.7881160, ISSN: 15502252
4. Andres-Maldonado, P., Ameigeiras, P., Prados-Garzon, J., Navarro-Ortiz, J., Lopez-Soler, J.M.: Narrowband IoT data transmission procedures for massive machine-type communications (2017). https://doi.org/10.1109/MNET.2017.1700081
5. Beyene, Y.D., Jantti, R., Ruttik, K., Iraji, S.: On the performance of narrow-band internet of things (NB-IoT). In: IEEE Wireless Communications and Networking Conference, WCNC (2017). https://doi.org/10.1109/WCNC.2017.7925809, ISSN: 15253511
6. Buttyán, L., Csik, L.: 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). pp. 419–424 (2010). https://doi.org/10.1109/PERCOMW.2010.5470633
7. Cao, X., Shila, D.M., Cheng, Y., Yang, Z., Zhou, Y., Chen, J.: Ghost-in-zigbee: Energy depletion attack on zigbee-based wireless networks. IEEE Internet of Things Journal **3**(5), 816–829 (2016). https://doi.org/10.1109/JIOT.2016.2516102
8. Chen, M., Miao, Y., Hao, Y., Hwang, K.: Narrow band internet of things (2017). https://doi.org/10.1109/ACCESS.2017.2751586
9. Hoglund, A., Medina-Acosta, G.A., Veedu, S.N.K., Liberg, O., Tirronen, T., Yavuz, E.A., Bergman, J.: 3gpp release-16 preconfigured uplink resources for lte-m and nb-iot. IEEE Communications Standards Magazine **4**(2), 50–56 (2020). https://doi.org/10.1109/MCOMSTD.001.2000003
10. Jover, R.P., Lackey, J., Raghavan, A.: Enhancing the security of LTE networks against jamming attacks **2014**(1), 7 (2014-12). https://doi.org/10.1186/1687-417X-2014-7, https://jis-eurasipjournals.springeropen.com/articles/10.1186/1687-417X-2014-7
11. Keysight: Downlink channel parameters (nb-iot), http://rfmw.em.keysight.com/wireless/helpfiles/89600B/WebHelp/Subsystems/nbiot/Content/nbiot_dlcontrolchannelproperties.htm
12. Krejčí, R., Hujňák, O., Švepeš, M.: Security survey of the iot wireless protocols. In: 2017 25th Telecommunication Forum (TELFOR). pp. 1–4 (2017). https://doi.org/10.1109/TELFOR.2017.8249286

13. Liberg, O., Sundberg, M., Wang, Y.P.E., Bergman, J., Sachs, J., Wikström, G.: Cellular internet of things: from massive deployments to critical 5G applications. Academic Press (2020)
14. Lin, X., Adhikary, A., Eric Wang, Y.P.: Random access preamble design and detection for 3gpp narrowband IoT systems **5**(6), 640–643 (2016-12). https://doi.org/10.1109/LWC.2016.2609914, http://ieeexplore.ieee.org/document/7569029/
15. Martiradonna, S., Piro, G., Boggia, G.: On the evaluation of the NB-IoT random access procedure in monitoring infrastructures **19**(14), 3237 (2019-07-23). https://doi.org/10.3390/s19143237, https://www.mdpi.com/1424-8220/19/14/3237
16. Matz, A.P., Fernandez-Prieto, J.A., Cañada-Bago, J., Birkel, U.: A systematic analysis of narrowband IoT quality of service **20**(6), 1636 (2020-03-14). https://doi.org/10.3390/s20061636, https://www.mdpi.com/1424-8220/20/6/1636
17. Mwakwata, C.B., Malik, H., Alam, M.M., Moullec, Y.L., Parand, S., Mumtaz, S.: Narrowband internet of things (NB-IoT): From physical (PHY) and media access control (MAC) layers perspectives (2019). https://doi.org/10.3390/s19112613
18. Navda, V., Bohra, A., Ganguly, S., Rubenstein, D.: Using channel hopping to increase 802.11 resilience to jamming attacks. pp. 2526 – 2530 (06 2007). https://doi.org/10.1109/INFCOM.2007.314
19. Nokia: Nokia siemens network. rf measurements quantities and optimization, https://www.academia.edu/8902974/Soc_Classification_level_1_Nokia_Siemens_Networks_Presentation_Author_Date_RF_measurements_quantities_and_optimization_Soc_Classification_level_2_Nokia_Siemens_Networks_Presentation_Author_Date_Content?auto=download
20. Pielli, C., Chiariotti, F., Laurenti, N., Zanella, A., Zorzi, M.: A game-theoretic analysis of energy-depleting jamming attacks. In: 2017 International Conference on Computing, Networking and Communications (ICNC). pp. 100–104 (2017). https://doi.org/10.1109/ICCNC.2017.7876109
21. Pirayesh, H., Zeng, H.: Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey (2021)
22. Pirretti, M., Zhu, S., Vijaykrishnan, N., McDaniel, P., Kandemir, M., Brooks, R.: The sleep deprivation attack in sensor networks: Analysis and methods of defense. International Journal of Distributed Sensor Networks **2**(3), 267–287 (2006). https://doi.org/10.1080/15501320600642718, https://doi.org/10.1080/15501320600642718
23. Pu, C.: Energy depletion attack against routing protocol in the internet of things. In: 2019 16th IEEE Annual Consumer Communications Networking Conference (CCNC). pp. 1–4 (2019). https://doi.org/10.1109/CCNC.2019.8651771
24. Shakhov, V.: On a new type of attack in wireless sensor networks: Depletion of battery. In: 2016 11th International Forum on Strategic Technology (IFOST). pp. 491–494 (2016). https://doi.org/10.1109/IFOST.2016.7884162
25. TORRIERI, D.: Frequency hopping with multiple frequency-shift keying and hard decisions. Communications, IEEE Transactions on **32**, 574 – 582 (06 1984). https://doi.org/10.1109/TCOM.1984.1096105
26. Vasserman, E.Y., Hopper, N.: Vampire attacks: Draining life from wireless ad hoc sensor networks (2013). https://doi.org/10.1109/TMC.2011.274
27. Xu, J., Yao, J., Wang, L., Ming, Z., Wu, K., Chen, L.: Narrowband internet of things: Evolutions, technologies, and open issues (2018). https://doi.org/10.1109/JIOT.2017.2783374