Detecting Targeted Interference in NB-IoT

Gabriela Morillo
School of Computer Science and Information Technology
University College Cork
Cork, Ireland
g.morillo@cs.ucc.ie

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

Dirk Pesch
School of Computer Science and Information Technology
University College Cork
Cork, Ireland
d.pesch@cs.ucc.ie

***Abstract*—Many Internet of Things (IoT) applications are considered critical systems, and it is important to guarantee that such deployments are resilient to attacks. An attacker may use radio interference selectively to disrupt communication while minimising the risk of their detection. It is essential to identify such attacks in order to remove the threat. In this work, we propose a novel method of detecting targeted interference in a Narrowband-Internet of Things (NB-IoT) network at the User Equipment (UE). NB-IoT is a recent Low Power Wide Area Network (LPWAN) radio technology used to deploy IoT infrastructures at scale. Network performance data collected at the UE is used to reason about the current interference situation. Subframe loss rates within the downlink channel are monitored and used as input for a statistical anomaly detector. Our evaluation shows that the detector is able to distinguish targeted interference attacks from the impact of naturally occurring interference in cellular networks. This is important as naturally occurring interference requires a different response than targeted interference attacks.**

***Index Terms*—Internet of Things, Narrowband Internet of Things, Jamming, Anomaly Detection.**

I. Introduction

Narrowband-Internet of Things (NB-IoT) is an LPWAN radio technology defined in 3rd Generation Partnership Project (3GPP) standard Release-13 [1]. NB-IoT aims to support a large number of low-cost, low energy consuming, and low data rate devices operated in a large coverage area. NB-IoT is increasingly seen as one of the key future IoT technologies, as it is deployed as part of the existing Long-Term Evolution (LTE) infrastructure and uses a licensed band that enables reliable and future-proof deployments. NB-IoT provides several security mechanisms based on established mechanisms defined for LTE [2].

NB-IoT is used to construct IoT applications in domains such as smart cities, transport systems or smart grids. Many of these IoT applications are considered critical systems, and their secure and reliable operation is paramount. A challenge in IoT deployments is radio interference. Interference may originate naturally within cellular networks such as NB-IoT, from other networks deployed in the same frequency space, electrical machinery or a nefarious actor that aims to disturb communications. While IoT installations and protocols are designed with interference in mind, they usually do not consider deliberate interference from an adversary.

It has been shown that an attacker can use targeted interference to have a significant impact on an NB-IoT deployment [3]–[5]. For example, an attacker can use interference to perform a battery depletion attack [3], [4], to prevent synchronisation [5] or to carry out a Denial of Service (DoS) attack. Such targeted interference attacks are difficult to detect, as communication is not prevented entirely.

It is necessary to determine if a network is subject to such targeted interference attack, as the response to an interference attack is usually different compared to the response to natural interference. For example, in case of natural interference, a communication protocol may use redundant transmissions to deal with a situation. In case of a targeted interference attack, this may not be the appropriate reaction; instead, it might be better not to change communication behaviour, but instead alert the network operator to identify and remove the attacker.

In this work, we propose a novel method of detecting targeted interference in an NB-IoT network at the UE, e.g. a sensor node. We consider an adversary using a jamming device to interfere with NB-IoT communication. Specifically, we assume that the attacker observes and interferes with the downlink channel to achieve maximum impact. Network performance data collected at the UE is used to reason about the current interference situation. Subframe loss rates within the downlink channel are monitored and used as input for a statistical anomaly detector at the UE. The specific contributions of our work are:

- *Targeted Interference Detection:* A UE based detection method using subframe loss rates observed within the downlink channel. Loss rates can be provided by the UE decoding pipeline without modification at the UE.
- *Evaluation of Targeted Interference Detection:* We evaluate the performance of the targeted interference detection mechanism using a Matlab simulation framework. We show that the detector is able to distinguish targeted and non-targeted interference reliably.
- *Optimal Targeted Interference Detection:* We describe the optimal configuration of the detector to balance true positive and false negative detection.

In Section II, we describe the existing related work. In Section III we provide an overview of NB-IoT technology and describe our threat model. Section IV presents the proposed

NB-IoT targeted interference detection model. In Section V, we present the experimental evaluation of the model and discuss results. Section VII concludes the paper.

II. Related Work

In this section, we describe previous works that analyse jamming interference in cellular networks, emphasising those works that addressed jamming interference in cellular IoT networks. Multiple studies have been conducted to describe, model and mitigate interference in wireless communication networks. A more limited number of studies have focused on jamming interference attacks, and even fewer works have concentrated on jamming detection. Jamming detection in LTE and, specifically, NB-IoT has received little attention.

Jamming attacks, which exploit the use of interference generated by an adversary, have been widely conducted in cellular networks such as LTE [16], [22], [25] or the recently deployed 5G [44]–[46]. IoT networks are also subject to a range of potential security attacks. Multiple works have focused on the performance analysis and evaluation of jamming in IoT networks [26], [27], [31], [43] as well as its detection and mitigation [28]–[30], [32]. Similarly, several works have studied jamming interference in LPWANs specifically, which include LoRa [36], [37], Sigfox [44] and NB-IoT. LPWANs are one of the dominant IoT technologies for managing critical infrastructure due to their low-power and long-range capabilities, leading to long-life deployments, e.g. many years up to a decade. A broad literature has focused on IoT security vulnerabilities and signals jamming attacks in LoRaWAN [39], [41], with one of the primary areas being the development of jamming attacks on the LoRa physical layer [34], [35], smart jammers [40], [42], and their mitigation techniques [33], [38].

To understand jamming vulnerabilities in LTE, several works exist that study the impact of the various types of jamming on physical channels, signals, frame structure, and decoding protocols as part of security in the physical layer of LTE [17], [19], [20], [24]. From the attack perspective, various authors studied multiple attacks like partial or total DoS and loss-of-service attacks generated by smart jammers [18], [21]. There is also work that proposes mitigation techniques [13]–[15] and countermeasures [7], [23] for jamming attacks in LTE. However, less work has focused on jamming detection for LTE or NB-IoT. In the following, we describe the most relevant related work.

Topal et al. [6] introduce a system to identify smart jammers in LTE. The model considers two steps, (i) signal pre-processing and (ii) classification. The authors use a wavelet-based pre-processing step to represent the signal as an image. In the classification step, a Deep Convolutional Network (DCNN) and Support Vector Machine (SVM) architecture is considered. The study considers three different jamming attacks: barrage jamming, synchronisation signal jamming and reference signal jamming. The classification performance of the proposed approach demonstrates that the DCNN technique has superior performance compared to SVM. The principal difference between this work and our solution is that it focuses on LTE, not NB-IoT and considers the jamming of synchronisation information and not data transmissions. Furthermore, the proposed detector uses Machine Learning (ML), is heavyweight, requires training and is therefore unsuitable for executing on a low-power NB-IoT UE. Additional equipment co-located with the Evolved Node B (eNodeB) would usually be required.

Eygi et al. [7] consider an LTE smart jamming attack and design a countermeasure mechanism. The attacker observes the downlink transmissions to synchronise timing and transmits resource elements containing malicious synchronisation signals. The work presents a detection and countermeasure technique for this type of jamming based on the Neyman-Pearson theorem using Error Vector Magnitude (EVM) and Cell ID correction percentage. Simulation results show that the proposed countermeasure reduces the jamming effect, and significantly improves Cell ID detection. This work differs from our work as it considers jamming of synchronisation in LTE, whereas the detection of jamming in a more general way on the downlink channel is not considered.

Hachimi et al. [47] present a jamming attack detection method for 5G Cloud Radio Access Networks (C-RAN) using a multi-stage machine learning-based intrusion detector (ML-IDS). The authors used a combination of deep learning and kernelised support vector machine (SVM) to detect four types of jamming attacks: constant jamming, random jamming, deceptive jamming, and reactive jamming. The detection method consists of two stages feature extraction and attack classification. This work differs from ours as it examines the detection of jamming attacks in 5G C-RAN networks using a multi-stage machine learning approach.

Martinez et al. [37] provide a comprehensive analysis of the effects of jamming attacks on the performance of a LoRaWAN network. The authors conducted experiments to model channel-aware and channel-oblivious jammers in LoRaWAN networks. In the former, statistical methods were used to analyse the data collected from the experiments using four performance metrics (packet loss probability, collision probability, packet rejection probability and network throughput). For the latter, two metrics are considered, the gateway (GW) occupancy, defined as the percentage of time the GW is busy processing packets, and the packet forwarding rate, which is the number of packets per minute the GW can process. Although this work focuses on the study of the impact of jamming attacks using statistical methods to evaluate performance metrics, it differs from our research as it focuses on another technology, LoRaWAN networks.

Ionescu et al. [3], [4] describe energy depletion attacks on NB-IoT devices using targeted interference. The work considers a jammer that aims to disrupt the processing of specific information (MIB-NB, SIB1-NB or SIB2-NB information) delivered in the downlink channel from the base station (called eNodeB) to the UE. The UE's energy consumption increases as it aims to receive redundant messages. The results show that this type of jamming attack can impact the lifespan of a NB-IoT UE, e.g. lifetime reduces from 17 years to

approximately four months. This work is complementary to our work as it describes similar attacks to those we consider, but it does not address detection.

III. Background

The core specifications of NB-IoT were completed in June 2016 [8]. NB-IoT is designed to coexist with legacy Global System for Mobile communication (GSM) and LTE technologies [10]. NB-IoT operates in the licensed spectrum and supports three modes of operation: stand-alone, in-band and guard-band. A stand-alone deployment uses any available spectrum with a bandwidth larger than 180kHz. In this case, parts of the GSM spectrum might be used [9]. An NB-IoT in-band deployment uses the existing LTE network, occupying one of the LTE Physical Resource Blockss (PRBs). NB-IoT in guard-band mode, is deployed using the unused bandwidth in the guard-band of LTE networks.

A. NB-IoT PHY Layer

NB-IoT supports Frequency Division Duplex (FDD) and Time Division Duplex (TDD) operations. The NB-IoT frame structure with 15kHz subcarrier spacing has 1024 hyper-frames, each hyper-frame has 1024 frames, and each frame consists of 10 subframes and each subframe is split into two slots of 0.5ms duration. For subcarrier spacing of 15kHz, supported in the uplink and downlink, each frame has 20 slots, while with the additional subcarrier spacing of 3,75 kHz, which is used only in the uplink, each frame contains five slots of 2ms each [9]. PRBs are defined to map the physical channels and signals in NB-IoT. A PRB consists of 12 sub-carriers over 7 Orthogonal Frequency Division Multiplexing (OFDM) symbols, generating 84 Resource Elements (RE), the smallest physical channel unit in the downlink [11], as shown in Figure 1. Table I summarizes the NB-IoT channels and signals in the uplink and downlink that are multiplexed across subframes and REs.

TABLE I
Physical Channels and Signals in NB-IoT

Link	Physical Channel/Signal	Description
Down	Narrowband Primary Synchronisation Signal (NPSS), Narrowband Secondary Synchronisation Signal (NSSS)	Time and frequency synchronization.
Down	Narrowband Reference Signal (NRS)	Reference Time and Frequency.
Down	Narrowband Broadcast Channel (NPBCH)	Master information for system access.
Down	Narrowband Physical Downlink Control Channel (NPDCCH)	Uplink and downlink scheduling information.
Down	Narrowband Physical Downlink Shared Channel (NPDSCH)	Downlink dedicated and common data.
Up	Narrowband Physical Uplink Shared Channel (NPUSCH)	Uplink dedicated data.
Up	Narrowband Physical Random Access Channel (NPRACH)	Random access signalling in the uplink.

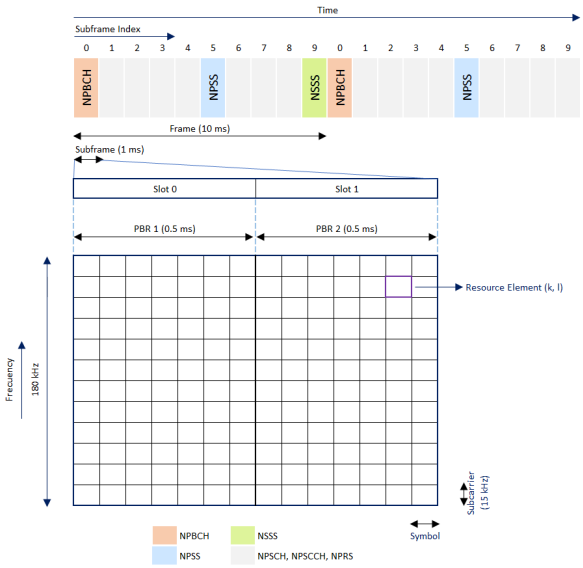

Fig. 1. Time-multiplexing of downlink physical channels on NB-IoT

B. Threat Model and Targeted Interference

We assume that an attacker is equipped with an NB-IoT transmitter. The attacker uses the device to emit a jamming/interference signal. The attacker will apply the interference signal for the shortest duration possible. This approach is used to (i) reduce energy usage (the attacker may operate on a battery powered device), and (ii) reduce the likelihood of detection (the attacker does not want to be found). Thus, the attacker will aim interference at specific protocol elements to achieve maximum impact with a minimum interference effort (a targeted attack).

We assume further that the attacker aims to disrupt the downlink channel with the attack. The attacker can monitor communication between UE and eNodeB. The attacker performs a targeted attack by submitting a jamming signal to disrupt (parts) of a specific physical channel, e.g. NPBCH. For example, the attacker may only target NPBCH to perform a battery depletion attack as described in [3] or NPDSCH to disrupt data transmission between a UE and eNodeB. As a result, the attacker will prevent successful reception of specific subframes (see Figure 1) at the UE. For example, by attacking the NPBCH, most subframes of index 0 are not received while most other subframes are received correctly.

The attacker may not be able to determine the content of all protocol elements, as some are transmitted encrypted. However, not all downlink elements use encryption (e.g. MIB) and interference can also be applied to encrypted signal parts.

IV. Targeted Interference Detection

Our aim is to detect targeted interference as described in Section III-B. Detection should be performed by the UE without hardware modification. Thus, only information already available via the NB-IoT transceiver hardware can be used; specific spectrum measurements are not possible. In addition,

detection should be integrated with normal UE operations to avoid excessive additional energy costs. Detection should be a lightweight implementation to suit an embedded NB-IoT UE.

An NB-IoT UE wakes up periodically from deep sleep, synchronises with the eNodeB, transmits data and then returns to sleep. When waking up, the UE will receive a sequence of subframes via the downlink channel as shown in Figure 1. The UE will decode the subframes and use the information provided to synchronise and attach to the network. A targeted interferer will want to prevent decoding of specific subframes to disrupt communication. Of course, there may also be some subframe decoding failures due to natural interference.

To detect a targeted interference attack, we monitor the subframe loss rate during the wake-up period of the UE. The decoding chain of the UE transceiver can provide this information. The assumption is that a targeted interference attack will lead to a marked increase in subframe losses in the targeted areas compared to loss rates observed in non-targeted areas. We expect natural interference to cause equal loss rates for all subframes, while a targeted attack will cause an unequal distribution of lost subframes. Thus, it is possible to distinguish targeted interference from natural interference.

A. Detector Design

The detector monitors decoding success of a sequence of S subframes in the downlink channel during the active period of the UE (a sequence of subframes as depicted in Figure 1). For each of the subframes η ($\forall \eta \in 0, 1, 2, 3, 4, 6, 7, 8, 9$) within a frame, the loss rate L_η is calculated. We do not consider subframes $\eta = 5$ as these contain only synchronisation information. Thus, a set of loss rates L containing 8 values is collected. As we assume that loss is caused by either a targeted attack or natural interference, L provides a picture of the interference environment that the UE is currently exposed to.

Next, values in the set L have to be adjusted, resulting in the adjusted loss rate set L'. Adjustment is necessary as not all subframes react to interference similarly. Specifically, subframe 0 carries the NPBCH, which uses a different encoding mechanism than the other subframes. Subframe 0 experiences more loss than the other subframes for the same level of interference. To make loss rates comparable across all subframes, we have to adjust the loss rate before performing detection. We discuss this adjustment in detail in the next subsection.

The detector is used to check if a specific subframe η is under targeted attack. For this purpose, the adjusted loss rate L'_η is compared with the average adjusted loss rate $\widetilde{L'}$ computed over all other subframes. If the adjusted loss rate in the investigated subframe L'_η is above the average adjusted loss rate $\widetilde{L'}$, a targeted attack is present. We use a φ to ensure that an attack is only detected if L'_η is significantly above the observed average in order to reduce false alarms. We define φ as a safety margin. The detector decision can be described as:

Algorithm 1 Detection Algorithm

Input: L', η
Output: {0, 1}
1: $\widetilde{L'}$ = AVERAGE(L', η)
2: **if** $L'_\eta > \widetilde{L'} \cdot \varphi$ **then**
3: **return** 1 # subframe η is under attack
4: **else**
5: **return** 0 # subframe η is not attacked
6: **end if**

B. Loss Rate Adjustment

Subframe 0 experiences more loss than the other subframes for the same level of interference. The loss rate must therefore be adjusted to make it comparable with loss rates in other subframes. We use a compensation factor α as follows:

$$L'_0 = L_0 \cdot \alpha(\widetilde{L}) \tag{1}$$

$\widetilde{L}$ is the average loss rate in all other subframes except subframe 0. $\alpha(\widetilde{L})$ is a function, and the necessary adjustment depends on the observed interference level. As we show in the experimental evaluation, $\alpha(\widetilde{L})$ can be described as an exponential function:

$$\alpha(\widetilde{L}) = \delta \cdot e^{\lambda . \widetilde{L}} \tag{2}$$

It has to be taken into account that subframes might be under targeted attack when $\alpha(\widetilde{L})$ is computed. In this case, the adjustment may be incorrect. To account for this issue, it is possible to approximate $\alpha(\widetilde{L})$ by a static α.

V. Evaluation Setup

We use the Matlab simulation environment to evaluate our proposed targeted interference detection method.

A. Simulation Environment

Our simulation environment was developed with Matlab using its LTE Toolbox, implementing the full transmitter and receiver signal processing chains. The receiver chain fully synchronizes, demodulates and decodes an NB-IoT downlink signal sent by a transmitter. The downlink signal can be subjected to interference, and we can detect if subframes are received correctly. In order to do so, we use the decode block defined per each channel at the UE side (the receiver). For this, we use the *lteNPBCHDecode* class and *lteNDLSCHDecode* class in the Matlab LTE Toolbox. The outcome for each channel is a structure with the decoding state indicating 1 if the decoding was successful, and 0 if the decoding failed.

The decoding process for NPBCH in NB-IoT is described in detail in 3GPP TS 36.211 V15.7.0 [12]. We have analysed the overall transmission chain of the NB-IoT eNB as defined in 3GPP specifications [49], [50], [51]. Briefly summarised, the decoding process for NPBCH in NB-IoT starts once the signal has been received by the NB-IoT device. The first step in the process is demodulation, where the received signal is converted from its radio frequency representation to a

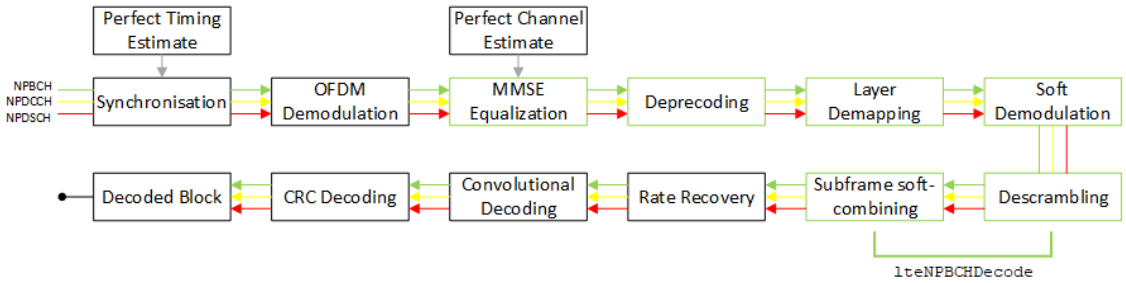

Fig. 2. Communication Chain at the receiver side of the NB-IoT

digital signal using quadrature phase-shift keying (QPSK) demodulation. The next step is channel de-coding, where the demodulated signal is decoded using a rate-1/3 Viterbi decoder to correct any errors introduced during transmission. This is followed by de-interleaving, which further corrects any errors introduced by the channel. The signal is then de-scrambled to obtain the uncoded bits, and an error check is performed on the uncoded bits to detect any errors in the received system information.

Figure 2 depicts in detail the communication chain at the receiver side [52]. We show in the figure the blocks executed for NPBCH, NPDCCH and NPDSCH decoding in Matlab. The decoding procedure is performed for every subframe that arrives within the NB-IoT communication chain at the receiver side. For the NPBCH, a CRC can be evaluated to detect if the subframe was damaged (each NPBCH subframe is self-decodable). For the NPDCCH and NPDSCH, transmitted information (called transport block) may span several subframes and a CRC is only available for the entire transport block. Thus, it is only possible to determine if a subframe used for NPDCCH and NPDSCH is damaged using a CRC if transport blocks fit in a subframe. We make in our simulation this assumption. However, it has to be noted that it is also possible to estimate which subframe was damaged in case a transport block spans multiple subframes if NRS is used for interference estimation.

B. Communication Scenario

We consider communication between an NB-IoT node A and an eNodeB B (base station). B is transmitting subframes in the downlink channel to A and this communication can be subject to interference. We consider three types of interference that can be present:

- *Background Noise (BN):* Additive White Gaussian Noise (AWGN) that is present at all time while the downlink channel is active.
- *Background Traffic (BT):* Noise (interference) that is only present during certain periods of time (on-off noise). The duration of these noise periods and the gaps in between follow a Poisson process. This simulates interference from another communication network deployed in the NB-IoT space.

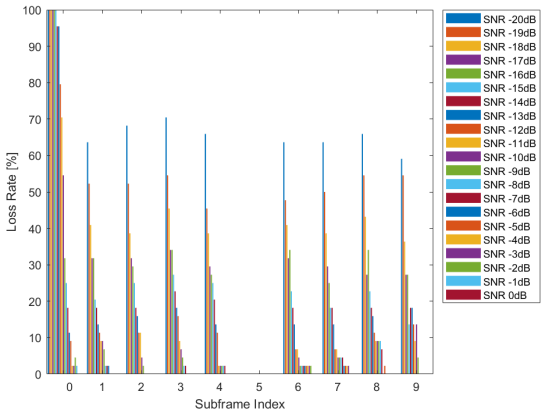

Fig. 3. Loss rate L for continuous background noise (BN).

- *Targeted Attack (TA):* Interference signal that is present only in subframe 0, simulating a targeted attack on the Narrowband Broadcast Channel (NPBCH).

Each interference type can be present at different SNR levels. Different interference types can be present at the same time. The detector must be able to identify situations in which a targeted attack is present and must avoid false alarms, falsely identifying BN/BT as an attack.

VI. Results

In this section, we describe first an experiment that was used to determine the loss rate adjustment. Thereafter we present an evaluation of the detector capability.

A. Loss Rate Adjustment

In this experiment, we subjected the downlink channel to continuous background noise (BN) at different SNR levels. We then determine the subframe loss rate L. Figure 3 depicts the observed loss rate for various SNR values.

It can be clearly seen that for the same noise level, the loss rate L_0 in subframe 0 is significantly larger than the loss rate in all other subframes. For example, for an $SNR = -19dB$ $L_0 = 100\%$ while $L_1 = 40.9\%$. Also, the exponential trend of loss rate depending on the SNR is clearly visible. As discussed previously, subframe 5 carries only timing information and is excluded.

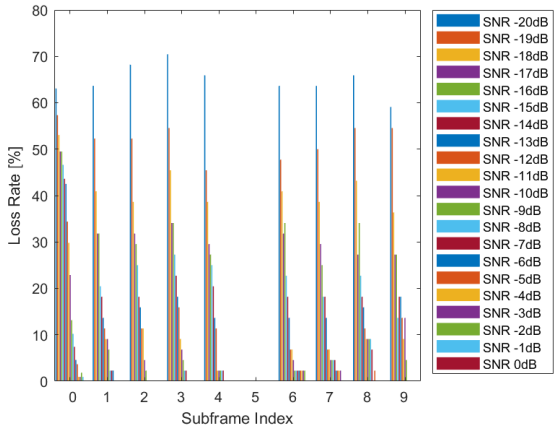

Fig. 4. Adjusted loss rate L' for continuous background noise (BN).

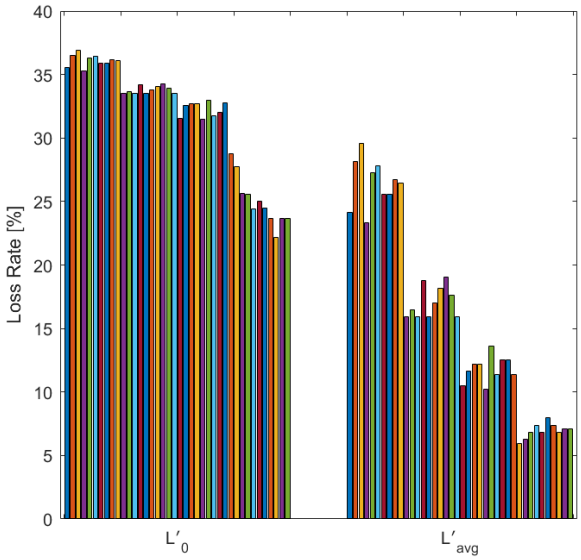

Fig. 5. Loss rate L'_0 and $\widetilde{L'}$ for BA and TA interference (Attack is present).

Using this experimental data, we determine the parameters δ and λ in Equation 2. $\delta = 0.25$ and $\lambda = 0.007$ provide a good fit, and we used these settings to adjust L_0.

The adjusted figure for L' is shown in Figure 4. Using the adjustment, loss rates in all subframes are now comparable; similar levels of interference cause the same loss rate.

B. Detection Capability

In this experiment, we create a number of scenarios with and without targeted interference attacks. We then test if the detector is able to determine that an attack is happening (True Positive) or if the detector falsely claims an attack is present (False Positive).

We combine background noise (BN) and targeted attack (TA) noise to create realistic scenarios; in practice, even when a targeted attack is present, some background noise can be present too. For this purpose, we create interference signals combining BN and TA at different SNR levels. We create 40 attack scenarios with BN based SNR ranging from -10dB to -16dB (steps of 2dB) and TA based SNR ranging from -19.5dB to 0dB (steps of 0.5dB). The interference signal is in most cases stronger than the background noise; a scenario in which the targeted attack is buried in background noise is not a realistic setup.

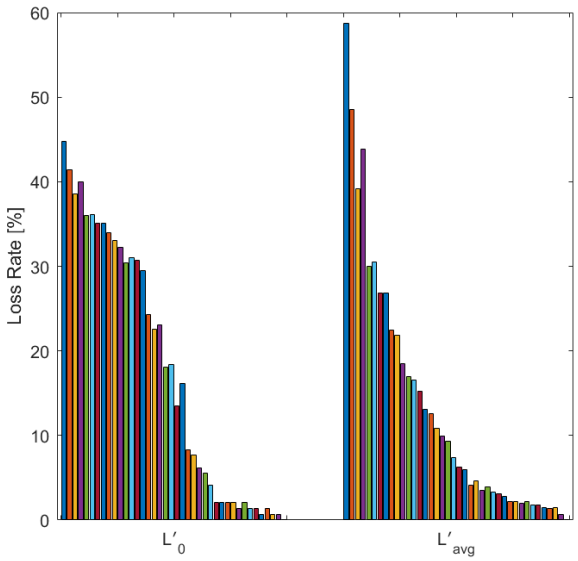

Fig. 6. Loss rate L'_0 and $\widetilde{L'}$ for BN and BT interference (No attack is present).

We then also create 40 scenarios in which no attack is present. We use background noise (BN) based SNR ranging from -10db to -19.5dB (steps of 0.5dB) and background traffic (BT) based SNR ranging from -10db to -19.5dB.

Figure 5 shows the relation between the loss rate in subframe 0 L'_0 and the loss rate average for the other subframes $\widetilde{L'}$ for background noise combined with the targeted attack in the NPBCH channel (Our 40 attack scenarios). It can be seen that with the same interference scenario, the loss rate L_0 in subframe 0 is generally larger than the average loss rate in all other subframes. For example, for an $SNR_{TA} = -17dB$ and $SNR_{BA} = -16dB$ $L_0 = 36.45\%$ while $\widetilde{L'} = 27.84\%$.

Figure 6 shows the comparison between the loss rate in subframe 0 L'_0 and the loss rate average for the other subframes $\widetilde{L'}$ for the background noise (BN) and the Background Traffic (BT) (Our 40 scenarios without attack). For the same interference scenario, the loss rate L_0 in subframe 0 is generally similar to the loss rate in all other subframes. For example, for an $SNR = -18dB$ $L_0 = 39,98\%$ while $\widetilde{L'} = 43,83\%$.

We use the detector as described in Section IV-A and evaluate all possible safety margins φ with the aforementioned 80 interference scenarios. Using a large φ reduces the amount of false positives (classifying an interference scenario without targeted attack as a targeted attack being present). At the same time, an increase in φ reduces the true positives (classifying

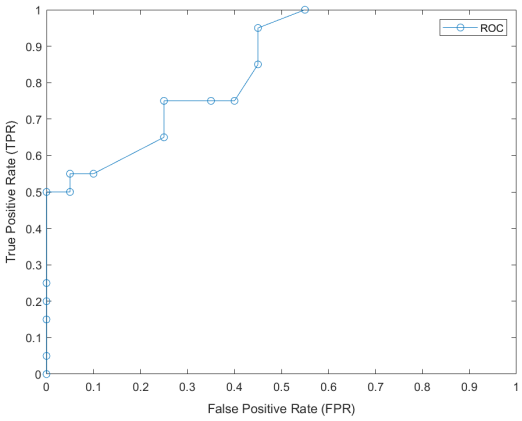

Fig. 7. Receiver Operating Characteristic (ROC) curve

a present targeted interference as a targeted interference). Figure 7 shows the result of this experiment in form of a ROC curve.

As it can be seen in Figure 7 that it is possible to tune the detector such that no false positives occur while still 50% of targeted interference cases are detected ($\varphi = 10$ in this case). This setting would be used if it is necessary to eliminate false alarms, while it is acceptable to reduce detection reliability. It is also possible to tune the detector such that all targeted interference cases are detected; however, in this case, a high false positive rate of 55% is observed. False positive and false negative rates are equal for an EER=25% (for $\varphi = 5$).

In summary, it is possible to distinguish targeted attacks from other interference scenarios using the proposed methods. It would be acceptable in practice to tune the system to not create false positives and therefore miss some attacks. Over time (multiple wake-up periods) an attacker will eventually be detected.

VII. Conclusion

We have demonstrated that it is possible to construct a statistical anomaly detector capable of detecting targeted interference on NB-IoT devices by utilising the available data in the UE as an indirect measure of interference. The detector has an EER=25% and it is possible to detect 50% of attacks without any false positives. For future work, we aim to broaden the capabilities of the detector. At present, the detector is able to detect targeted attacks on NPBCH and NPDSCH but not on NPSS, NSSS and NRS. To include detection for these attacks, additional mechanisms are required. We also plan to evaluate the proposed detection mechanism using a physical testbed setup.

Acknowledgment

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.

References

[1] Third Generation Partnership Project, 3GPP., : Cellular system support for ultra-low complexity and low throughput Internet of Things (CIoT) (Release 13). In: Technical Specification Group GSM/EDGE Radio Access Network, 3GPP TR 45.820 V13.1.0. (2015).

[2] Cao, J., Yu, P., Ma, M., Gao, W., Fast Authentication and Data Transfer Scheme for Massive NB-IoT Devices in 3GPP 5G Network. IEEE Internet of Things Journal, vol. 6, pp. 1561–1575. (2019).

[3] Ionescu, V., and Roedig, U. (2022, October). NB-IoT battery depletion via malicious interference. In 1st Workshop on Unconventional Security for Wireless Communications (UWSC 2022), Co-located with EWSN 2022, Linz, Austria, October 3, 2022.

[4] Ionescu, V., and Roedig, U. (2021, October). Battery depletion attacks on NB-IoT devices using interference. In European Symposium on Research in Computer Security (pp. 276-295). Springer.

[5] Morillo, G. and Roedig, U. (2021) 'Jamming of NB-IoT synchronisation signals', 26th European Symposium on Research in Computer Security (ESORICS) 2021, Virtual Event, 04-08 October.

[6] Topal, O.A., Gecgel, S., Eksioglu, E.M., and Karabulut-Kurt, G. (2019). Identification of Smart Jammers: Learning based Approaches Using Wavelet Representation. ArXiv, abs/1901.09424.

[7] Eygi, M., Karabulut-Kurt, G.: A Countermeasure against Smart Jamming Attacks on LTE Synchronization Signals. In: Journal of Communication, vol. 15, pp. 626–632. (2020).

[8] Standardization of NB-IoT completed, 3GPP, June, 2016 http://www.3gpp.org/news-events/3gpp-news/1785-nb-iot-complete.

[9] Liberg, O., Sundberg, M., Wang, Y., Bergman, J., Sachs, J. and Wikstrom, G., n.d. Cellular internet of things.

[10] Y. . -P. E. Wang et al., "A Primer on 3GPP Narrowband Internet of Things," in IEEE Communications Magazine, vol. 55, no. 3, pp. 117-123, March 2017, doi: 10.1109/MCOM.2017.1600510CM.

[11] R. Ratasuk, N. Mangalvedhe, J. Kaikkonen and M. Robert, "Data Channel Design and Performance for LTE Narrowband IoT," 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), 2016, pp. 1-5, doi: 10.1109/VTCFall.2016.7880951.

[12] ETSI TS 136 211 V14.2.0, LTE Evolved Universal Terrestrial Radio Access (E-UTRA), Physical channels and modulation (3GPP TS 36.211 version 14.2.0 Release 14) (2017).

[13] J. Kakar, K. McDermott, V. Garg, M. Lichtman, V. Marojevic and J. H. Reed, "Analysis and Mitigation of Interference to the LTE Physical Control Format Indicator Channel," 2014 IEEE Military Communications Conference, Baltimore, MD, USA, 2014, pp. 228-234, doi: 10.1109/MILCOM.2014.43.

[14] M. Lichtman, T. Czauski, S. Ha, P. David and J. H. Reed, "Detection and Mitigation of Uplink Control Channel Jamming in LTE," 2014 IEEE Military Communications Conference, Baltimore, MD, USA, 2014, pp. 1187-1194, doi: 10.1109/MILCOM.2014.199.

[15] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic and J. H. Reed, "LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation," in IEEE Communications Magazine, vol. 54, no. 4, pp. 54-61, April 2016, doi: 10.1109/MCOM.2016.7452266.

[16] R. Krenz and S. Brahma, "Jamming LTE signals," 2015 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Constanta, Romania, 2015, pp. 72-76, doi: 10.1109/BlackSeaCom.2015.7185089.

[17] K. Fors, K. Wiklundh and S. Linder, "Interference Impact on Two of LTE's Control Channels," 2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE), Amsterdam, Netherlands, 2018, pp. 309-314, doi: 10.1109/EMCEurope.2018.8485044.

[18] F. M. Aziz, J. S. Shamma and G. L. Stüber, "Jammer-Type Estimation in LTE With a Smart Jammer Repeated Game," in IEEE Transactions on Vehicular Technology, vol. 66, no. 8, pp. 7422-7431, Aug. 2017, doi: 10.1109/TVT.2017.2672682.

[19] N. K. Narcisse, L. Damon and G. Bossard, "Impact of Jamming on Real Life LTE Networks: Experimental Results," 2022 International Wireless Communications and Mobile Computing (IWCMC), Dubrovnik, Croatia, 2022, pp. 248-253, doi: 10.1109/IWCMC55113.2022.9824968.

[20] P. Stenumgaard, K. Fors and K. Wiklundh, "Interference impact on LTE from radiated emission limits," 2015 IEEE International Symposium on Electromagnetic Compatibility (EMC), Dresden, Germany, 2015, pp. 165-170, doi: 10.1109/ISEMC.2015.7256152.

[21] X. Li and Z. Wang, "A Study on Pseudo CRS Signal Jamming Attacks in LTE Network," 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, Brazil, 2018, pp. 1-4, doi: 10.1109/ISCC.2018.8538662.

[22] H. Alakoca, H. B. Tugrel, G. K. Kurt and C. Ayyildiz, "CP and pilot jamming attacks on SC-FDMA: Performance tests with software defined radios," 2016 10th International Conference on Signal Processing and Communication Systems (ICSPCS), Surfers Paradise, QLD, Australia, 2016, pp. 1-6, doi: 10.1109/ICSPCS.2016.7843341.

[23] M. Labib, V. Marojevic, J. H. Reed and A. I. Zaghloul, "How to enhance the immunity of LTE systems against RF spoofing," 2016 International Conference on Computing, Networking and Communications (ICNC), Kauai, HI, USA, 2016, pp. 1-5, doi: 10.1109/ICCNC.2016.7440650.

[24] A. El-Keyi, O. Uereten, T. Yensen and H. Yanikomeroglu, "LTE Physical-Layer Identity Detection in the Presence of Jamming," 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), Toronto, ON, Canada, 2017, pp. 1-6, doi: 10.1109/VTCFall.2017.8288216.

[25] G. Romero, V. Deniau and O. Stienne, "LTE Physical Layer Vulnerability Test to Different Types of Jamming Signals," 2019 International Symposium on Electromagnetic Compatibility - EMC EUROPE, Barcelona, Spain, 2019, pp. 1138-1143, doi: 10.1109/EMCEurope.2019.8872052.

[26] Z. Dou, G. Si, Y. Lin and M. Wang, "An Adaptive Resource Allocation Model With Anti-Jamming in IoT Network," in IEEE Access, vol. 7, pp. 93250-93258, 2019, doi: 10.1109/ACCESS.2019.2903207.

[27] A. S. Ali, M. Baddeley, L. Bariah, M. A. Lopez, W. T. Lunardi, J. P. Giacalone and S. H. Muhaidat. , "Performance Analysis and Evaluation of RF Jamming in IoT Networks," GLOBECOM 2022 - 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 2022, pp. 2745-2751, doi: 10.1109/GLOBECOM48099.2022.10001334.

[28] M. S. Abdalzaher, M. Elwekeil, T. Wang and S. Zhang, "A Deep Autoencoder Trust Model for Mitigating Jamming Attack in IoT Assisted by Cognitive Radio," in IEEE Systems Journal, vol. 16, no. 3, pp. 3635-3645, Sept. 2022, doi: 10.1109/JSYST.2021.3099072.

[29] A. Hussain, N. Abughanam, J. Qadir, and A. Mohamed. 2023. "Jamming Detection in IoT Wireless Networks: An Edge-AI Based Approach". In Proceedings of the 12th International Conference on the Internet of Things (IoT '22). Association for Computing Machinery, New York, NY, USA, 57–64. https://doi.org/10.1145/3567445.3567456

[30] M. Reynvoet, O. Gheibi, F. Quin and D. Weyns, "Detecting and Mitigating Jamming Attacks in IoT Networks Using Self-Adaptation," 2022 IEEE International Conference on Autonomic Computing and Self-Organizing Systems Companion (ACSOS-C), CA, USA, 2022, pp. 7-12, doi: 10.1109/ACSOSC56246.2022.00019.

[31] A. Al Sharah, H. Abu Owida and T. A. Edwan, "Aggressive Jamming Attack in IoT Networks," 2022 4th IEEE Middle East and North Africa COMMunications Conference (MENACOMM), Amman, Jordan, 2022, pp. 235-239, doi: 10.1109/MENACOMM57252.2022.9998231.

[32] S. Yu, C. Lin, X. Zhang and L. Guo, "Defending against Cross-Technology Jamming in Heterogeneous IoT Systems," 2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS), Bologna, Italy, 2022, pp. 702-712, doi: 10.1109/ICDCS54860.2022.00073.

[33] T. Voigt, M. Bor, U. Roedig, and J. Alonso, "Mitigating inter-network interference in lora networks," in EWSN '17 Proceedings of the 2017 International Conference on Embedded Wireless Systems and Networks. ACM Press, Feb. 2017, pp. 323–328, Junction Publishing, 2017.

[34] N. Hou, X. Xia and Y. Zheng, "Jamming of LoRa PHY and Countermeasure," IEEE INFOCOM 2021 - IEEE Conference on Computer Communications, Vancouver, BC, Canada, 2021, pp. 1-10, doi: 10.1109/INFOCOM42981.2021.9488774.

[35] S. J. Moon and W. Lee, "Friendly Jamming in LoRa Physical Layer Using Imperfect Orthogonality of Spreading Factor," 2022 International Conference on Information Networking (ICOIN), Jeju-si, Korea, Republic of, 2022, pp. 423-428, doi: 10.1109/ICOIN53446.2022.9687108.

[36] C. -Y. Huang, C. -W. Lin, R. -G. Cheng, S. J. Yang and S. -T. Sheu, "Experimental Evaluation of Jamming Threat in LoRaWAN," 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 2019, pp. 1-6, doi: 10.1109/VTC-Spring.2019.8746374.

[37] I. Martinez, P. Tanguy and F. Nouvel, "On the performance evaluation of LoRaWAN under Jamming," 2019 12th IFIP Wireless and Mobile Networking Conference (WMNC), Paris, France, 2019, pp. 141-145, doi: 10.23919/WMNC.2019.8881830.

[38] C. Moy, "Artificial Intelligence for Jamming Mitigation in IoT Networks: LoRaWAN Field Measurements Using IoTligent," 2021 XXXIVth General Assembly and Scientific Symposium of the International Union of Radio Science (URSI GASS), Rome, Italy, 2021, pp. 1-4, doi: 10.23919/URSIGASS51995.2021.9560289.

[39] F. Hessel, L. Almon, and M. Hollick. 2022. LoRaWAN Security: An Evolvable Survey on Vulnerabilities, Attacks and their Systematic Mitigation. ACM Trans. Sen. Netw. Just Accepted (September 2022). https://doi.org/10.1145/3561973

[40] Perković, T., Rudeš, H., Damjanovic, S., and Nakić, A. (2021). Low-Cost Implementation of Reactive Jammer on LoRaWAN Network. Electronics, 10, 864.

[41] Viswapriya, S.E., Dinesh, S., and Teja, D.R. (2021). IOT Security Vulnerabilities and Predictive Signal Jamming Attack Analysis in LoRaWAN. International Journal of Computer Science and Mobile Computing.

[42] V. Kalokidou, M. Nair and M. A. Beach, "LoRaWAN Performance Evaluation and Resilience under Jamming Attacks," 2022 Sensor Signal Processing for Defence Conference (SSPD), London, United Kingdom, 2022, pp. 1-5, doi: 10.1109/SSPD54131.2022.9896225.

[43] X. Tang, P. Ren and Z. Han, "Jamming Mitigation via Hierarchical Security Game for IoT Communications," in IEEE Access, vol. 6, pp. 5766-5779, 2018, doi: 10.1109/ACCESS.2018.2793280.

[44] Y. Wang, S. Jere, S. Banerjee, L. Liu, S. Shetty and S. Dayekh, "Anonymous Jamming Detection in 5G with Bayesian Network Model Based Inference Analysis," 2022 IEEE 23rd International Conference on High Performance Switching and Routing (HPSR), Taicang, Jiangsu, China, 2022, pp. 151-156, doi: 10.1109/HPSR54439.2022.9831286.

[45] C. Örnek and M. Kartal, "An Efficient EVM Based Jamming Detection in 5G Networks," 2022 4th IEEE Middle East and North Africa COMMunications Conference (MENACOMM), Amman, Jordan, 2022, pp. 130-135, doi: 10.1109/MENACOMM57252.2022.9998310.

[46] Y. Arjoune and S. Faruque, "Smart Jamming Attacks in 5G New Radio: A Review," 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2020, pp. 1010-1015, doi: 10.1109/CCWC47524.2020.9031175.

[47] M. Hachimi, G. Kaddoum, G. Gagnon and P. Illy, "Multi-stage Jamming Attacks Detection using Deep Learning Combined with Kernelized Support Vector Machine in 5G Cloud Radio Access Networks," 2020 International Symposium on Networks, Computers and Communications (ISNCC), Montreal, QC, Canada, 2020, pp. 1-5, doi: 10.1109/ISNCC49221.2020.9297290.

[48] 3GPP TS 36.212. "Multiplexing and channel coding." 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA).

[49] 3GPP TS 36.104, "Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception (Release 13)".

[50] 3GPP TS 36.141, "Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification (Release 13)".

[51] 3GPP TS 36.321, "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Link Control (RLC) protocol specification (Release 13)".

[52] M. Kanj, V. Savaux and M. Le Guen, "A Tutorial on NB-IoT Physical Layer Design," in IEEE Communications Surveys and Tutorials, vol. 22, no. 4, pp. 2408-2446, Fourthquarter 2020, doi: 10.1109/COMST.2020.3022751.