5G Physical Layer Resiliency Enhancements with NB-IoT Use Case Study

Xiang Cheng*, Hanchao Yang*, D. J. Jakubisin†, N. Tripathi*, G. Anderson‡, A. K. Wang‡, Y. Yang*, J. H. Reed*
*Wireless@VT, Bradley Department of ECE, Virginia Tech, Blacksburg, VA
†Virginia Tech National Security Institute, Blacksburg, VA
‡Lockheed Martin, Cherry Hill, NJ

MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM) | 978-1-6654-8534-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/MILCOM55135.2022.10017487

***Abstract*—5G has received significant interest from commercial as well as defense industries. However, resiliency in 5G remains a major concern for its use in military and defense applications. In this paper, we explore physical layer resiliency enhancements for 5G and use narrow-band Internet of Things (NB-IoT) as a study case. Two physical layer modifications, frequency hopping, and direct sequence spreading, are analyzed from the standpoint of implementation and performance. Simulation results show that these techniques are effective to harden the resiliency of the physical layer to interference and jamming. A discussion of protocol considerations for 5G and beyond is provided based on the results.**

***Index Terms*—5G, Wireless Security, Tactical Communications**

I. Introduction

5G technology has received significant interest, from commercial as well as defense industries and the U.S. Department of Defense has outlined a 5G strategy that emphasizes open architectures and network virtualization, citing spurred innovation, competition, and acquisition options [1]. 5G networks are currently being explored and prototyped for a variety of applications in military operations [2], [3].

The growth of low-cost sensor platforms and the advancement of artificial intelligence (AI) and machine learning (ML) enabled sensor data processing is driving the need for collection and dissemination of vast quantities of sensor data spread throughout distributed networks. 5G technology is well equipped to meet the necessary throughput, latency, power, and connection density requirements to support these applications. In particular, 5G supports a diversity of communication modes (terrestrial, non-terrestrial, NB-IoT, D2D, IAB, C-V2X), a flexibility of network design, and AI/ML integration (O-RAN architecture) to support data transport for joint all-domain operations (JADO).

On the other hand, 5G technology is built around a wireless communication standard written for commercial applications, which has a different set of requirements from defense applications, particularly in the case of security and resiliency. While 5G networks have improved security over previous generations in several ways including mutual authentication and increased data integrity and confidentiality (e.g., 5G-AKA and SEPP), physical layer resiliency remains a significant concern. Physical layer resiliency threats for wireless signals fall into two main categories (a) detection and interception and (b) disruption and manipulation.

The first category of threat is related to attacks that seek to determine the presence or location of the communications transmitter or which seek to eavesdrop on the communication. Eavesdropping attackers aim to intercept confidential information from legitimate communications, through monitoring and intercepting unencrypted control channels, or analyzing the encrypted traffic patterns. In response to these threats, there is a need for physical layer waveforms that provide a low probability of interception (LPI), detection (LPD), geolocation (LPG), or exploitation (LPE)—collectively referred to as LPX.

The second category of threat includes attacks that seek to contaminate, spoof, or jam the wireless transmission [4]. Contamination attacks attempt to undermine channel information and the subsequent communication procedures(e.g., through transmissions of identical reference signals [5]). A spoofing attacker's goal is to join or corrupt the legitimate communications by sending forged and injected signals which usually have higher power and carry similar content [6]. Jamming attackers attempt to generate high-power noise to block legitimate communications, decreasing the signal-to-interference-plus-noise ratio (SINR) and making demodulation of the legitimate signals difficult [7]–[9]. Thus, in this case, we are concerned with waveforms and protocols that are resilient under various types of jamming and contamination attacks, sometimes referred to as anti-jamming (AJ) characteristics.

In this paper, we explore physical layer resiliency, taking NB-IoT as a use case. NB-IoT supports scenarios in which a large number of low-cost devices (e.g., sensors) are connected to the 5G Base Station (gNB). NB-IoT, originally designed as an extension of the 4G standards, continues to be the standard of low-cost IoT in 5G. NB-IoT standards support terrestrial networks (TN), and are currently being defined for non-terrestrial networks (NTN). In this paper, we explore several physical layer enhancements to NB-IoT that increase the LPX/AJ characteristics of the waveforms. The techniques considered are adaptations of traditional spreading and frequency hopping approaches. The performance of these techniques in TN and NTN is demonstrated. We provide a discussion of protocol considerations based on our work to inform future research and standards development in this area.

II. Related Works

In recent years, many researchers have proposed different methods to enhance physical layer resiliency in response to the threats discussed in Section I. Conventional countermeasures include frequency hopping and sequence spreading. Frequency hopping can be implemented with 5G systems without fundamentally changing the waveform, and many recent works proposed machine learning-based frequency hopping methods

for adaptive and robust resistance to jamming attacks [10], [11]. On the other hand, sequence spreading—although having desirable LPX/AJ properties—is incompatible with the 5G OFDMA waveform without some degree of modification. For example, Tabatabaefar *et al.* [12] presented a direct sequence spread spectrum (DSSS) method for 5G applications which totally redesigned the 5G physical layer.

Besides these two schemes, power allocation methods [13] are also proposed to mitigate jamming attacks. Power allocation schemes adapt the time and frequency allocation of power (e.g., sub-carrier power allocation) to avoid interference. Like frequency hopping, in recent years many machine-learning-based methods are emerging [14]–[16]. The advantage of this scheme is energy efficiency, and many studies are proposed for IoT systems.

In addition, the secrecy of 5G can benefit from massive MIMO. Elmasry et al. [17] proposed a MIMO hopping method that controls power in different RF paths to hide information. Wang et al. [18] use beamforming to create artificial fast fading in unintended receivers. Apart from that, some studies proposed to use friendly jamming in 5G to interfere with an eavesdropper, assuming that the legitimate receiver can perfectly remove the jammer's interference [19], [20].

III. Overview

A. 5G and NB-IoT: A Brief Introduction

3GPP defined Fifth-Generation technology in Release 15 in 2017-2018. 5G aims to achieve the peak data rate of 20 Gbps, the radio network latency of 1 ms, one million (low-rate and delay-tolerant) devices per square kilometer, and 10 Mbps per square meter [21]. 5G supports three usage categories-enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communications (URLLC), and massive Machine Type Communications (mMTC). 3GPP has defined a new interface called New Radio (NR) that addresses services or applications that possess characteristics of the eMBB and the URLLC usage scenarios. The mMTC usage scenario often necessitates simpler and lower-cost IoT devices and simpler radio interfaces. Thus, 5G aims to use 4G Long Term Evolution (LTE)-based IoT technologies such as LTE-M and NB-IoT. The radio interfaces of both LTE-M and NB-IoT are being enhanced by the 3GPP along with 5G NR radio interface.

NB-IoT, in particular, is intended for very low bandwidth delay-tolerant devices and applications. Benefits of NB-IoT include low cost, long battery life (with the target of 10 years), and enhanced coverage. Data transfer in NB-IoT can be carried out using the User Plane (i.e., using an Evolved Packet System bearer) or the Control Plane (i.e., using Radio Resource Control and Non-Access Stratum signaling).

Like 4G LTE and 5G NR, NB-IoT relies on an Orthogonal Frequency Division Multiplexing (OFDM)-based radio interface. The OFDM radio interface defines a Physical Resource Block (PRB) that consists of twelve subcarriers for the duration of a 0.5-ms slot. The maximum transmission bandwidth in NB-IoT is 1 PRB or 180 kHz. However, the minimum transmission bandwidth in the uplink could be a single subcarrier. A typical NB-IoT UE (e.g., Category NB1 UE) has a single antenna. NB-IoT supports features such as Power Saving Mode (PSM) and enhanced Discontinuous Reception (eDRX) to increase the battery life. Repetitions on the radio interface help enhance coverage. Characteristics such as the support for low-order modulation schemes, a single antenna, and half-duplex Frequency Division Duplex (FDD) simplify the device designs and reduce the cost.

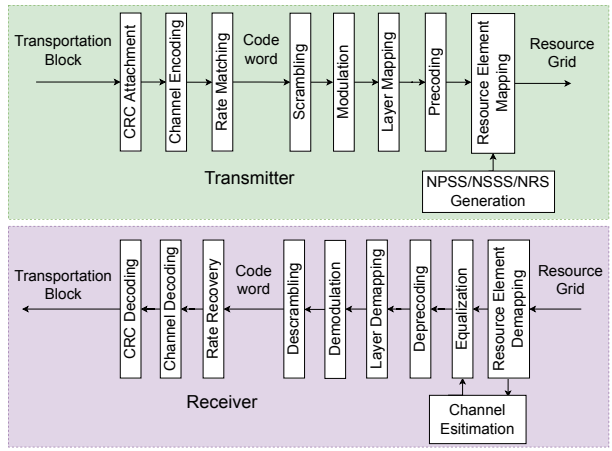


Fig. 1: Signal processing chain in standard NB-IoT system

B. NB-IoT Waveform Details

Each frame in NB-IoT has a duration of 10 ms and contains 10 subframes. One subframe is composed of two slots with a duration of 0.5 ms each, and the dimensions of each slot is 12 subcarriers by 7 OFDM symbols. The downlink subcarrier spacing is always 15 kHz, meanwhile, the uplink subcarrier spacing can be set to either 15 kHz or 3.75 kHz. When the uplink subcarrier spacing is set to 3.75 kHz, a slot contains 48 subcarriers and has a duration of 2 ms.

Fig. 1 shows the signal processing chain for the NB-IoT physical layer. The transportation block from the upper layer passes through the CRC attachment, channel coding, and rate matching for noise and error resistance. Scrambling provides a degree of inter-cell interference protection. Modulation (typically QPSK in NB-IoT) is followed by layer mapping and precoding for beamforming and subsequently resource element mapping to the resource grid. As for the resource grid, the 3GPP NB-IoT standard uses OFDM modulation to transform it into a time-domain signal. In this paper, we provide two alternative methods for creation of the time-domain signal in Section IV: frequency hopping and sequence spreading.

C. Terrestrial and Non-Terrestrial Channel Models

Channel models play an important role in assessing the overall performance of a communication system. NB-IoT standards support TN channel, and are currently being defined for NTN channel. A set of TN channel models has been provided in 3GPP TS 36.101 [22] and 3GPP TS 36.104 [23] in release 14, for testing radio transmission and reception of user devices and base stations. The defined channel models cover different practical scenarios including multipath fading propagation conditions and mobile propagation conditions.

With the growing interest in NTN, 3GPP started working on NR NTN in 2017. In release 15 their focus on NTN is to study deployment scenarios and channel models. The study is documented in 3GPP TR 38.811 [24]. This study selected several deployment scenarios as references and defined key parameters in these scenarios. In addition, it also developed NTN channel models, which include parameters for both link-level and system-level simulations. A tapped-delay-line channel model from the study is used for this paper's simulations. In release 16 a set of necessary features enabling NR support for NTN are identified [25]. It is expected that in release 17 NR-based satellite access will be supported in the specification, serving handheld devices for global service continuity. Release 17 also will support NB-IoT and eMTC-based satellite access to address massive IoT use cases [26].

IV. Physical Resiliency Techniques

To increase the LPX/AJ features of NB-IoT waveforms, we explore the possibility to use two techniques for physical layer hardening: Frequency Hopping Spectrum Spreading (FHSS) and Direct Sequence Spectrum Spreading (DSSS). The details of adopting them in NB-IoT are discussed here.

A. FHSS

Frequency hopping is based on the assumption that the jamming attacker with limited RF power cannot jam all the frequency channels at the same time, thus the legitimate sender and receivers can communicate through the remaining channels. Compared to the standard physical layer in which signals always stay at the same carrier frequency, in frequency hopping, signals hop to another frequency in every slot or subframe based on a pseudo-random sequence only known to the sender and receiver.

To ensure the frequency hopping is compatible with the standard NB-IoT protocol, we can utilize the "in-band" operation mode in which the NB-IoT is allowed to reverse 1 resource block anywhere in the LTE legacy band. For example, if the LTE system bandwidth is 5 MHz, there are 25 resource blocks within it and a maximum of 25 carrier locations available for frequency hopping. In addition, with the "in-band" operation, the first one to three OFDMA symbols of each subframe are reserved for Legacy LTE's PDCCH signal, which provides 71.5-214.5 μs setting time for hopping the frequency. Besides, frequency hopping can also be adopted in the NB-IoT's multicarrier operation which increases the capacity of the cell. In the standard multicarrier operation, a specific anchor carrier is configured for initial connection setup and other non-anchor carriers are used for data communication. When hardening with frequency hopping, the anchor carrier can be fixed while available non-anchor carriers are used for hopping.

In the implementation, the receiver should align precise time synchronization with the transmitter and follow the same hopping sequence to properly reassemble the signal. A pseudo-random method is needed for the hopping sequence for a low possibility of prediction of malicious jammers. The pseudo-random sequence can be generated from seed parameters shared between the gNB and UE. As for time synchronization, it can be aided by the reserved resource for the system. Fig. 2 shows the mechanism of FHSS that we used in the simulation. Where the baseband waveform is the NB-IoT signal after OFDM modulation. Then the transmitter up-converts the signal to a pseudo-random frequency, while the receiver, with the same parameters and time, down-converts the signal from the identical carrier frequency to the baseband.

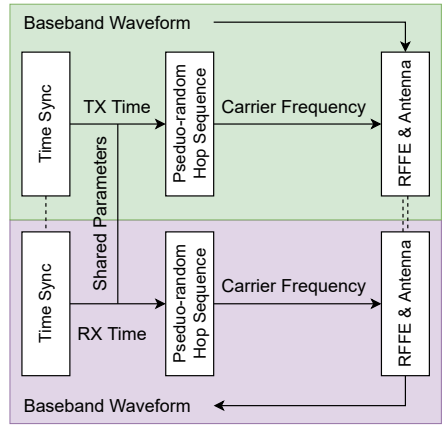


Fig. 2: Frequency hopping spread spectrum diagram

B. DSSS

In DSSS, the transmitter XORs the baseband modulated signal $s(t)$ with a pseudo-random wideband spreading code. In the receiver, the received signal is XORed with a synchronized replica of the spreading code to recover the original signal $s(t)$. Since the spreading code has a much higher chip rate than that of the $s(t)$, the transmitted signal will occupy a much wider bandwidth corresponding to the spreading code. DSSS signals provide LPI as the signal power is spread over a wide bandwidth and is noise-like. It also gives AJ characteristics as the signal is modulated with the pseudo-random spreading code only known to the transmitter and receiver, the spreading code serves as a stream cipher. In addition, in CDMA we can utilize different spreading codes with low cross-correlations to support multiple users to share the channel simultaneously.

The standard protocol doesn't support DSSS. To make minimal modifications to the standard processing chain, we choose not to follow the reference [12] that redesigns the physical layer. We choose to only replace the OFDM modulation block with our alternative spreading block. As shown in Fig. 3, the spreading block spreads modulated symbols in a resource grid, and applies a different spreading code for each subcarrier. After that, we add a chip-level pilot and synchronization signals for the receiver to acquire and synchronize the spreading code. Then the signal is fed to the RF front end and transmitted.

C. Protocol Impact

1) FHSS Considerations: In the case of FHSS, the NB-IoT physical waveform itself remains intact, but is transmitted at a different frequency location at different times such as each subframe (1 ms interval) or another interval. As a result,

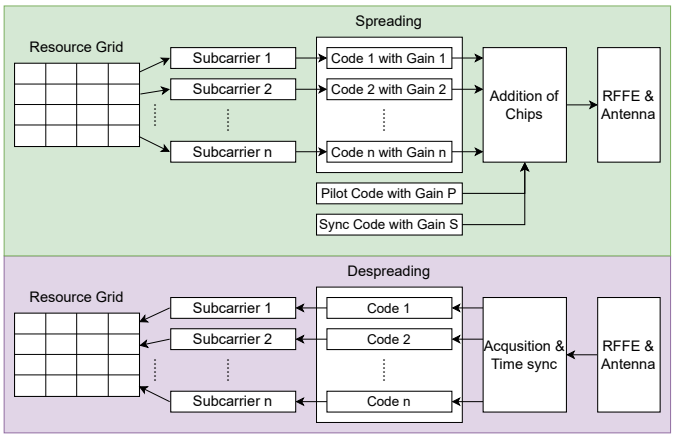


Fig. 3: Direct sequence spread spectrum diagram

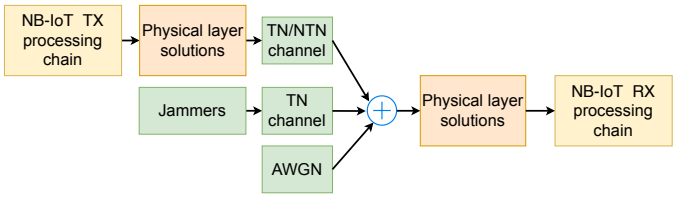


Fig. 4: The simulation framework

acquisition of the downlink carrier by the NB-IoT device must discover the NPSS (or NSSS) at the time (e.g., subframe) and frequency (hopping frequency). Without additional coordination, increased acquisition times are expected. Techniques for anticipating the NPSS time/frequency location (such as GPS-synchronized hopping patterns) are an area for future exploration. In addition, the radio channel will now appear to be time-varying to the modified FHSS physical layer. In other words, each time the NB-IoT waveform is "hopped" to a new center frequency, the radio channel environment is different. As a result, appropriate adjustments for channel estimation, channel quality information reporting, and power control must be made.

2) DSSS Considerations: In the case of DSSS, the signal which would be mapped to a subcarrier is instead spread across a larger transmission bandwidth using a suitable code (e.g., a spreading sequence). As a result, the interleaved placement of reference signals in a resource grid is no longer applicable for DSSS-based signal processing. Instead, pilot and synchronization sequences at the chip rate are needed to estimate and correct for channel impairments. Power management would be needed for the DSSS-based signals. The receiver would need to be a RAKE receiver so that the DSSS signal on the radio interface can be acquired.

V. Simulation Framework

To evaluate effectiveness of the proposed physical layer enhancements on NB-IoT system, we built a MATLAB link-level simulation framework and obtained results for analysis.

As shown in Fig. 4, the two modules with yellow color stand for the portions of the processing chain that retain standard NB-IoT functionality, as shown in Fig. 1 and described in

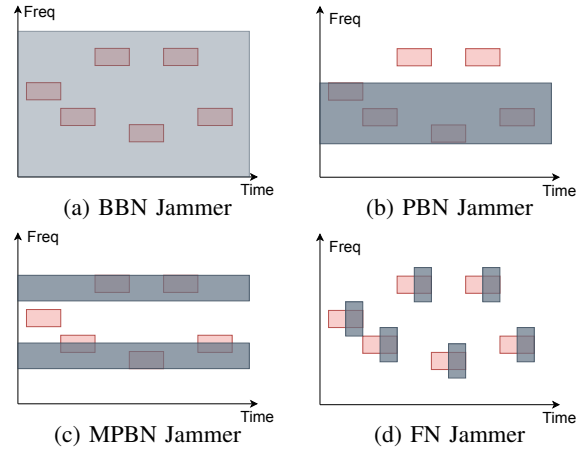


Fig. 5: Illustration of jammer models, pink blocks represent legitimate hopping channels, and gray blocks stand for jamming signals.

Section III-B. The orange modules named physical layer solutions can be either the standard OFDM modulation or the proposed physical layer enhancements, including FHSS and DSSS. The modules with green color represent the analysis and supporting functions for the performance analysis. For example, the blocks named TN/NTN channel represent channel models we built in the simulation. The parameters of TN channel model were set using the Extended Pedestrian A (EPA) model from TS36.101 [22] and TS36.104 [23], and the parameters of NTN channel model were set according to NTN-TDL-D model from TR38.811 [24]. Note that in NTN channel model the maximum Doppler shift is set to 5Hz as we assume that the large Doppler shift caused by satellite movement has been pre-compensated by the receiver's hardware design.

Overall, in the simulation framework, the NB-IoT TX processing chain generates the resource grid, which will be fed into the physical layer solution block to create time-domain waveforms. The waveform then passes through a TN/NTN channel with AWGN added. At the same time, the jammer module synthesizes jamming signals which pass through the TN channel and are added to the legitimate signals. In the next step, the mixed signals are captured by the receiver and processed by the physical layer solutions block. The output is fed into the NB-IoT RX processing chain to determine the bit error rate (BER) or block error rate (BLER) of the system.

A. Jammers

To evaluate the AJ effectiveness of the proposed physical layer solutions, four types of jammers were implemented in the simulation. All the jammers are assumed to have limited power and Fig. 5 illustrates each one of them.

1) Broad-Band Noise (BBN) Jammer: Fig. 5a shows the BBN jammer, which usually creates jamming noise whose energy covers the entire width of the spectrum used by the communication system [27]. In the simulation, we use white Gaussian noise as the BBN jamming signal with configured power. BBN jamming is useful against all kinds of AJ communication, however, it is not power-efficient as the jamming signal power needs to spread across the spectrum.

TABLE I: Key parameters in the simulation

Parameter	Value
Modulation and Coding Scheme(MCS)	4
Spreading factor	FHSS: 26, DSSS: 25
Number of repetitions	2, no HARQ used
Number of antennas	gNB = 2, UE = 1
System bandwidth	Standard = 200 kHZ, FHSS/DSSS = 5 MHz
BBN jamming bandwidth	20 MHz
PBN jamming bandwidth	5 MHz
MPBN jamming bandwidth	2 bands with 1 MHz each
FN re-tracking time	0.4 ms
FN tracking resolution	200 kHz
FN tracking success probability	0.6

2) Partial-Band Noise (PBN) Jammer: Fig. 5b shows the PBN jammer, whose jamming signals are placed across a continuous partial-band spectrum used by the targets [27]. Compared with BBN jammer, PBN jammer is more power-efficient as the jamming power is more concentrated, while its performance is determined by the overlap between the jamming spectrum and legitimately used spectrum.

3) Multi-Partial-Band Noise (MPBN) Jammer: Fig. 5c shows the MPBN jammer, which places its jamming signals over several non-continuous partial-band spectrums. Such jammer is useful to jam signals utilizing multiple spectrums, like multicarrier operation in NB-IoT and frequency hopping.

4) Follower Noise (FN) Jammer: Instead of putting the jamming signal on a constant spectrum over time, as shown in Fig. 5d, the FN jammer first detects the hopping channel used by the legitimate system, then puts the jamming noise on the corresponding channel. Once the legitimate signal hops to another channel, the jamming signal will follow it and start to jam the new channel. FN jammer is especially useful against FHSS, its performance is determined by three parameters: re-tracking time, tracking resolution, and tracking success probability [28].

5) Jammer setting for standard physical layer: when the standard physical layer is used in the NB-IoT, a channel with consistent carrier frequency is utilized for communication. Under the standard physical layer setting, we assume the jammer can detect the channel used by the system accurately and use PBN jamming to jam this channel constantly.

VI. Results

In this section we first analyze the effectiveness of FHSS and DSSS based on the simulation results, then a comparison between FHSS and DSSS in the discussion section is made. Key parameters in the simulation are listed in Table I.

FHSS Performance: We evaluate the FHSS solution against the noise jammers introduced in section V-A. In the simulation, we apply these jammers to the FHSS physical layer and measure the BER and BLER. To analyze how FHSS increases NB-IoT's AJ characteristic we also apply the jamming signals on the standard physical layer and compare its performance with FHSS, the jammer setting for the standard layer is described in section V-A5. The simulation results are present in Fig. 6. These results are for the downlink NTN channel; similar results were observed for the uplink and TN channel.

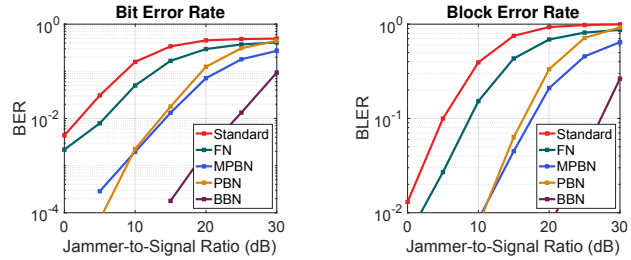
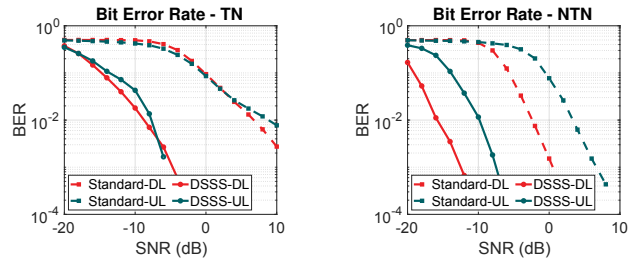


Fig. 6: BER and BLER of FHSS considering different jammer settings, with SNR = 3 dB for all the settings.



(a) BER under TN channel (b) BER under NTN channel

Fig. 7: Comparison between standard NB-IoT PHY and DSSS enhancement without jamming present.

We have two key observations. First, we can compare the effectiveness of different jammers (for a constant jamming signal power higher BER/BLER indicates a more effective jammer). From the figure, FN jammer is the most effective jammer, and BBN jammer is the weakest. PBN and MPBN jammers have similar jamming capabilities as their BER/BLER results are closed over different SNR. Intuitively, FN jammer utilizes its jamming power more effectively than BBN jammer does, as FN jammer adjusts its jamming power on the narrow-band spectrum according to hopping channels while BBN jammer simply spreads its power over a wider spectrum. Second, FHSS outperforms the standard protocol under all the jammer settings. Specifically, under FN jammer FHSS provides around 5 dB gain compared to standard protocol.

DSSS Performance: Here we first evaluate the performance of DSSS in the NB-IoT system when jamming signals are not present, and compare it with the standard physical layer. We run the DSSS simulations with TN and NTN channel models, with both uplink and downlink communication considered. The results are shown in Fig. 7. We observe that the DSSS physical layer has a 10-13 dB gain over the standard physical layer due to the fact that DSSS uses a pseudo-random spreading code to spread its power over a much wider bandwidth.

To analyze how DSSS can improve NB-IoT's AJ characteristic, we also run the DSSS simulation with several jammer types. In the DSSS case, the PBN jammer is effectively an FN jammer due to its overlap with the 5 MHz DSSS signal. In the simulation, the channel model and transmission direction are set to NTN and downlink, respectively. The simulation results are present in Fig. 8. We find that DSSS boosts the performance of NB-IoT in all the jammer settings. DSSS provides around 15 dB processing gain under PBN jammer and above 30 dB under BBN jamming.

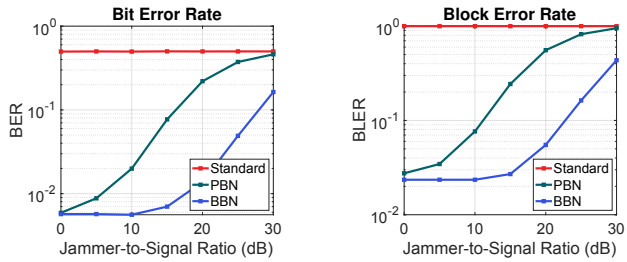


Fig. 8: BER and BLER of DSSS considering different jammer settings, with SNR = -15 dB for all the settings.

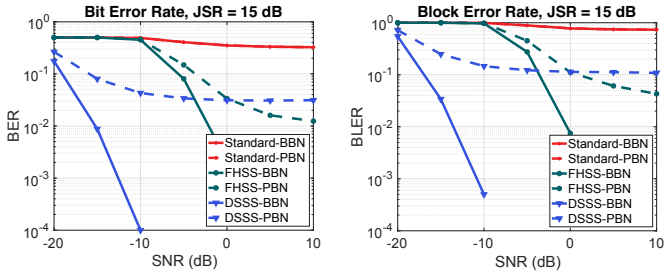


Fig. 9: FHSS and DSSS performance under BBN and PBN, with JSR = 15dB

FHSS and DSSS Comparison: We compared the performance of DSSS and FHSS under jamming with different background SNR, shown in Fig. 9. The simulations are run for PBN and BBN jammers with a jammer-to-signal ratio (JSR) of 15 dB JSR. The DSSS and FHSS signals occupy a 5 MHz spectrum. As the figure shows, the DSSS physical layer has around a 13-15 dB processing gain under BBN jammer compared to FHSS. However, under the PBN jammer, DSSS has a higher error floor than FHSS (after 0 dB SNR). One contributing factor may be self-interference in the DSSS signal since the spreading codes are not perfectly orthogonal (DSSS uses a Walsh code truncated to a length of 25).

VII. Discussion and Conclusions

In this paper, we have described two physical layer modifications that enhance the physical layer resiliency of NB-IoT: FHSS and DSSS. Both techniques are shown to significantly improve the waveform AJ characteristics: 5 dB improvement for FHSS in the worst case of an FN jammer and 10-13 dB improvement for DSSS. While DSSS generally outperformed FHSS, there are situations in which FHSS has a lower error floor (e.g., Fig. 9). In assessing the relative advantages of each approach, implementation complexity and protocol impact must also be considered. Thus, the protocol impacts discussed in Section IV-C should be kept in mind.

References

[1] J. B. Evans, "Department of defense 5G strategy implementation plan," Office of the Under Secretary of Defense (R&E) Washington, Tech. Rep., 2020, https://apps.dtic.mil/sti/pdfs/AD1118833.pdf.

[2] S. Walker, D. Rice, M. Kahn, and J. Clark, "Why the world's militaries are embracing 5G," *IEEE Spectrum*, 2021. [Online]. Available: https://spectrum.ieee.org/lockheed-martin-5g

[3] "Pentagon launches 5G challenge with millions up for grabs," https://www.defensenews.com/battlefield-tech/it-networks/5g/2022/04/06/pentagon-launches-5g-challenge-with-millions-up-for-grabs/, accessed: 2022-05-04.

[4] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet of Things Journal*, 2019.

[5] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Transactions on Wireless Communications*, 2012.

[6] H. Yang, S. Bae, M. Son, H. Kim, S. M. Kim, and Y. Kim, "Hiding in plain signal: Physical signal overshadowing attack on LTE," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019.

[7] S. Erni, P. Leu, M. Kotuliak, M. Röschlin, and S. Čapkun, "Adaptover: Adaptive overshadowing of LTE signals," *arXiv preprint arXiv:2106.05039*, 2021.

[8] G. Morillo and U. Roedig, "Jamming of NB-IoT synchronisation signals," in *26th European Symposium on Research in Computer Security (ESORICS)*, 2021.

[9] Z. Li, Y. Lu, X. Li, Z. Wang, W. Qiao, and Y. Liu, "UAV networks against multiple maneuvering smart jamming with knowledge-based reinforcement learning," *IEEE Internet of Things Journal*, 2021.

[10] P. Sharma, S. Jain, S. Gupta, and V. Chamola, "Role of machine learning and deep learning in securing 5G-driven industrial IoT applications," *Ad Hoc Networks*, 2021.

[11] Q. Zhou, Y. Li, and Y. Niu, "Intelligent anti-jamming communication for wireless sensor networks: A multi-agent reinforcement learning approach," *IEEE Open Journal of the Communications Society*, 2021.

[12] M. Tabatabaefar, M. D. Ardakani, R. Karimian, and S. O. Tatu, "A secure telecommunication link using spread spectrum technique for 5G applications," in *2021 United States National Committee of URSI National Radio Science Meeting (USNC-URSI NRSM)*, 2021.

[13] Z. Xiao, L. Zhu, J. Choi, P. Xia, and X. Xia, "Joint power allocation and beamforming for non-orthogonal multiple access (NOMA) in 5G millimeter wave communications," *IEEE Transactions on Wireless Communications*, 2018.

[14] I. AlQerm and B. Shihada, "Energy-efficient power allocation in multitier 5G networks using enhanced online learning," *IEEE Transactions on Vehicular Technology*, 2017.

[15] C. Zhao, Q. Wang, X. Liu, C. Li, and L. Shi, "Reinforcement learning based a non-zero-sum game for secure transmission against smart jamming," *Digital Signal Processing*, 2021.

[16] A. Gouissem, K. Abualsaud, E. Yaacoub, T. Khattab, and M. Guizani, "IoT anti-jamming strategy using game theory and neural network," in *2020 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE, 2020.

[17] G. Elmasry and P. Corwin, "Hiding the RF signal signature in tactical 5G," in *IEEE Military Commun. Conf. (MILCOM)*, 2021.

[18] T. Wang and Y. Yang, "Enhancing wireless communication privacy with artificial fading," in *2012 IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS)*, 2012.

[19] X. Li, H.-N. Dai, M. K. Shukla, D. Li, H. Xu, and M. Imran, "Friendly-jamming schemes to secure ultra-reliable and low-latency communications in 5G and beyond communications," *Computer Standards & Interfaces*, 2021.

[20] Y. Huo, X. Fan, L. Ma, X. Cheng, Z. Tian, and D. Chen, "Secure communications in tiered 5G wireless networks with cooperative jamming," *IEEE Transactions on Wireless Communications*, 2019.

[21] N. Tripathi and J. Reed, *5G Cellular Communications- Journey and destination*. The Wireless University, 2019.

[22] 3GPP, " Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception," 3rd Generation Partnership Project (3GPP), Technical Specifications (TS) 36.101, 04 2017, version 14.3.0.

[23] 3GPP, " Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception," 3rd Generation Partnership Project (3GPP), Technical Specifications (TS) 36.104, 04 2017, version 14.3.0.

[24] 3GPP, " Study on New Radio (NR) to support non-terrestrial networks," 3rd Generation Partnership Project (3GPP), Technical Report (TR) 38.811, 10 2020, version 15.4.0.

[25] X. Lin, S. Rommer, S. Euler, E. A. Yavuz, and R. S. Karlsson, "5g from space: An overview of 3GPP non-terrestrial networks," *IEEE Communications Standards Magazine*, 2021.

[26] 3GPP, "NTN & satellite in Rel-17 & 18," https://www.3gpp.org/news-events/partners-news/2254-ntn_rel17, accessed: 2022-04-29.

[27] R. Poisel, *Modern communications jamming principles and techniques*. Artech House, 2011.

[28] C. Lee, U. Jeong, Y. J. Ryoo, and K. Lee, "Performance of follower noise jammers considering practical tracking parameters," in *IEEE Vehicular Technology Conference*, 2006.