**Beyond Traditional RFID: Unveiling the Potential of Wi-Fi, 5G, Bluetooth, and Zigbee for Backscatter Systems**

**Sara El Mattar\***[](https://orcid.org/0000-0001-6429-5686)**, Abdennaceur Baghdad**[](https://orcid.org/0000-0002-0544-2612)

Laboratory of Electronics, Energy, Automatics and Data Processing, Department of Electrical Engineering, Faculty of Sciences and Techniques of Mohammedia, Hassan II University, Casablanca, Morocco

\* Corresponding author. E-mail address: saraelmattar@gmail.com

**Abstract**

Traditional RFID systems rely on dedicated readers, often expensive and bulky, hindering their widespread deployment. This paper proposes an alternative RFID system that leverages ubiquitous radio sources – Wi-Fi, 5G, Bluetooth, and Zigbee – to replace dedicated readers. Our system employs backscatter communication, where RFID tags modulate reflected signals from these readily available sources to transmit data. We investigate the feasibility and performance of this approach through Matlab simulator. Our results show that 802.11ax at 2.45 GHz exhibits the best Symbol Error Rate (SER), followed by 802.11n at the same frequency. However, 5G, Bluetooth, and Zigbee signals demonstrate lower performance even at high Signal-to-Noise Ratios (SNRs). To address this, we introduce error correction coding techniques (BCH and RS) that significantly improve communication reliability. Utilizing these codes, our system achieves a communication range of up to 1 meter. This finding highlights the potential of ubiquitous radio sources as a viable alternative to dedicated RFID readers, opening doors for various applications.

**Keywords:** RFID, backscatter communication, ubiquitous radio sources, WIFI, 5G, Bluetooth, Zigbee, error correction coding

# Introduction

Backscatter technologies have revolutionized wireless communication by enabling ultra-low-power data transmission for battery-free sensors and Internet-of-Things (IoT) devices [1,2]. The most prominent example is the passive RFID tag, a cornerstone of backscatter communication.

At the core of an RFID system lies a two-part interaction: a reader and a tag. The reader, equipped with specified antennas, transmits a strong radio signal to initiate communication with the tag. The tag uses this signal to energize itself and replies with its identification information using a basic modulation technique (such as ON-OFF keying). Although RFID tags are compact, adaptable, and economical, their broad adoption has been hindered by the expensive and bulky nature of dedicated RFID readers. In fact, typical reader prices can range from $1,000 to $20,000 [3].

To address these limitations, researchers have introduced Wi-Fi backscatter systems[4–6]. Their goal is to design tags that can be read using readily available Wi-Fi devices instead of specialized readers. This approach leverages existing Wi-Fi infrastructure, significantly simplifying deployment and reducing costs. A typical Wi-Fi backscatter system involves three components: a Wi-Fi device acting as a sender, a tag, and a receiver (another Wi-Fi device). The sender emits a Wi-Fi packet as a query signal. The tag intercepts and modifies this signal with its data before reflecting it back. Finally, the receiver decodes the tag's data from the modified packet.

Building upon the success of Wi-Fi backscatter, researchers are exploring the potential of other established communication protocols like Bluetooth[7–9], Zigbee[10–12], and 5G[13–15] for backscatter communication. These technologies offer unique advantages based on factors like range, data rate, and power consumption.

While previous research has focused on individual backscatter technologies, this article takes a groundbreaking approach. We present a comprehensive comparison of all these alternative radio frequency (RF) communication technologies (Wi-Fi (including 802.11n, 802.11ac, and 802.11ax), Bluetooth, 5G, Zigbee) in the context of backscatter communication. This comparison will be instrumental for researchers and developers in selecting the most suitable technology for specific applications. We will delve deeper by evaluating an RFID identification system utilizing these alternative sources and explore the integration of error-correcting coding techniques (e.g., BCH and RS) to optimize system performance.

# Evaluated Technologies

From ultrafast internet to seamlessly connected devices, wireless technologies are revolutionizing how we live. This section explores the inner workings and benefits of Wi-Fi, Bluetooth, 5G, and Zigbee.

## Wi-Fi Introduction (IEEE 802.11)

Wi-Fi technology, as we know it today, has come a long way since its introduction in 1997. This advancement has been driven by the need for faster speeds, wider range, and better security in our wireless connections.

The journey began with the 802.11 standard, offering a basic 2 Mbps speed in the 2.4 GHz band. This was followed by a series of improvements:

* **1999:** 802.11b increased the speed to 11 Mbps and operated in the same 2.4 GHz band.
* **1999:** 802.11a offered a faster 54 Mbps speed in the 5 GHz band, but with less range due to the higher frequency.

In 2003, 802.11g combined the benefits of both, using the faster OFDM technology like 11a but in the wider 2.4 GHz range of 11b.

A significant leap came in 2009 with 802.11n, utilizing MIMO technology to achieve speeds of up to 600 Mbps. This standard is still used in some devices today.

The most popular standard, 802.11ac, arrived in 2013, offering gigabit speeds exclusively in the 5 GHz band. It introduced features like Beamforming for better range and MU-MIMO for handling multiple devices simultaneously.

802.11ad, designed for the 60 GHz band, offered very high speeds but with limited range due to signal penetration issues. This standard never gained widespread adoption.

In 2018, 802.11ax (Wi-Fi 6) brought further improvements with wider channels (160 MHz) for increased speeds and lower latency. It also introduced features like OFDMA for better efficiency and 8x8 uplink MU-MIMO for faster uploads for multiple devices.

Wi-Fi continues to evolve, with the Wi-Fi Alliance recently simplifying the naming scheme to Wi-Fi 4 (802.11n), Wi-Fi 5 (802.11ac), and Wi-Fi 6 (802.11ax). This ongoing development ensures that Wi-Fi remains a key player in providing reliable and ever-faster wireless connections for our growing needs.

## 5G Introduction

Each iteration of wireless standards, defining the evolution of mobile networks, is characterized by a "G" symbolizing a substantial improvement in data carrying capacity and latency reduction [16]. This progression spans from first-generation (1G) technology to fifth-generation (5G) technology.

The fifth generation of wireless networks, commonly referred to as 5G, is a major breakthrough, promising remarkably higher data rates and reduced latency compared to its predecessors. The fundamental goal of 5G is to provide substantially increased capacity, enhanced reliability, and a higher density of high-speed mobile users, thus addressing the rapid growth of traffic and the increasing demand for high-speed connectivity [17]. This major advancement will play a pivotal role in accelerating the development of the Internet of Things (IoT), paving the way for an era of unprecedented connectivity.

5G utilizes a variety of frequency bands to deliver high-performance wireless connectivity. Examples of bands in the sub-6 GHz range include n40, covering 2.3 GHz to 2.4 GHz, n78 from 3.3 GHz to 3.8 GHz, and n79 from 4.4 GHz to 5 GHz. These bands offer a balance between range and throughput, making them ideal for wide-area coverage, particularly in urban environments.

On the other hand, millimeter-wave (mmWave) bands like n260 (37 GHz to 40 GHz), n261 (27.5 GHz to 28.35 GHz), n258 (26.5 GHz to 29.5 GHz), and n257 (26.5 GHz to 29.5 GHz) are used to provide extremely fast speeds but over shorter distances. These high frequencies are well-suited for high-density areas where high capacity is crucial.

## Bluetooth Introduction (IEEE 802.15)

Bluetooth provides a way for devices to connect without wires, perfect for short-distance communication. It was developed by Ericsson in 1994 and is named after the 10th-century Danish king, Harold Bluetooth[18]. This short-range radio link aims to connect electronic devices, whether mobile or fixed, with an effective range of 1 to 100 meters. Bluetooth is a combination of software and hardware technology. The hardware is based on a radio chip, while the software controls most of the management and security protocols.

Today, Bluetooth technology uses the protocol defined by the IEEE 802.15 standard, establishing a Personal Area Network (PAN) operating within a room or corridor-sized area. It is a protocol of choice for connecting two or more devices that are not in direct line of sight. Bluetooth uses radio waves to send data. When two devices are trying to pair, they scan for a common frequency over which they can send and receive data. There are 79 2.4 GHz frequency channels in which devices can be paired. A secure association between two devices can be established by physically associating the common Personal Identification Number (PIN) entered by the user on each device. When two devices attempt to connect, a unique key is generated based on the PIN entered on both devices.

ZigBee Introduction (IEEE 802.15.4)

## ZigBee Introduction (IEEE 802.15.4)

ZigBee is a wireless protocol that uses low-power radio signals to connect devices, based on the IEEE 802.15.4 standard, which defines the PHY and MAC layers for low-rate wireless personal area networks (LR-WPANs). Operating through a mesh network, ZigBee creates an environment where each device can act as a router for other devices, ensuring reliable and redundant communication paths, even in harsh environments. ZigBee uses a unique addressing scheme for precise device identification on the network, offering security features such as encryption and authentication against unauthorized access. With a range of up to 100 meters and the ability to support up to 65,000 devices on a single network [19], ZigBee is widely adopted in IoT devices, including smart home appliances, smart lighting, and industrial automation. Due to their low power consumption, ZigBee devices are particularly well-suited for battery-powered devices.

# Principles of BCH and RS Coding

Establishing robust and reliable communication between the information source and the destination is a major challenge in communication systems. Interferences such as noise can compromise the quality of transmitted data, thus requiring effective error correction mechanisms. To ensure stable communication, various strategies are employed, including the use of highly directional antennas, spread spectrum communication, and error-correcting codes. The latter, essential in digital communication systems, are categorized into several types, including block codes, convolutional codes, concatenated codes, Turbo product codes (TPC), among others. Among these categories, block codes hold a prominent position. Among them, BCH codes[20] and RS codes [21] are widely adopted in the fields of digital communication systems and digital storage. Their use ensures consistent data transmission, even in the presence of disturbances, thus ensuring communication reliability.

Bose, Chaudhuri, and Hocquenghem (BCH) codes constitute an extensive category of cyclic codes renowned for their effectiveness in correcting random errors. These codes represent a significant expansion of Hamming codes, particularly in the realm of correcting multiple errors. The discovery of binary BCH codes is attributed to Hocquenghem in 1959 and independently to Bose and Chaudhuri in 1960. These codes are characterized by the block length (n), the number of parity check digits (n-k), and the minimum distance (). The generator polynomial of BCH codes is specified as the least common multiple (LCM) of the minimal polynomials where , being the error correction capacity of the code [22]. For any positive integer m such that and an error correction capacity t such that , a BCH code can be generated with the following parameters:

- Block Length:

- Minimum Distance:

- Number of Parity Check Digit:

The generator polynomial is the least common multiple (LCM) of :

Since every even power of the primitive element (𝛼) has the same minimal polynomial as certain preceding odd powers of (α), equation (1) can be reduced to

Coded words are generated by following these steps:

1. Pre-multiply the k information digits, the message polynomial by ,i.e.,
2. Compute the parity check polynomial by dividing by .
3. Concatenate with to obtain the code polynomia .

In 1960, Irving Reed and Gustave Solomon at MIT came up with a brilliant solution, Reed-Solomon codes, to fix errors in digital information. However, computers weren't powerful enough back then to use them. Today, these codes are widely used in storage devices and communication systems to effectively correct data bursts.

Similarly, in the context of a finite field , an RS error-correcting code with t errors, denoted as , encodes a message of k symbols into a code word of n symbols by adding n − k parity symbols, here , and m is the number of bits per symbol.

The generator polynomial G(x) of the RS error-correcting code is represented by equation (3), where \alpha\ is a primitive element in and i is an arbitrary number [23]. Equation (4) presents the code word polynomial C(x), where D(x) denotes the message of k symbols.

# Modeling an RFID System with Wi-Fi, 5G, Bluetooth, and Zigbee Using MATLAB

## RFID System Communication

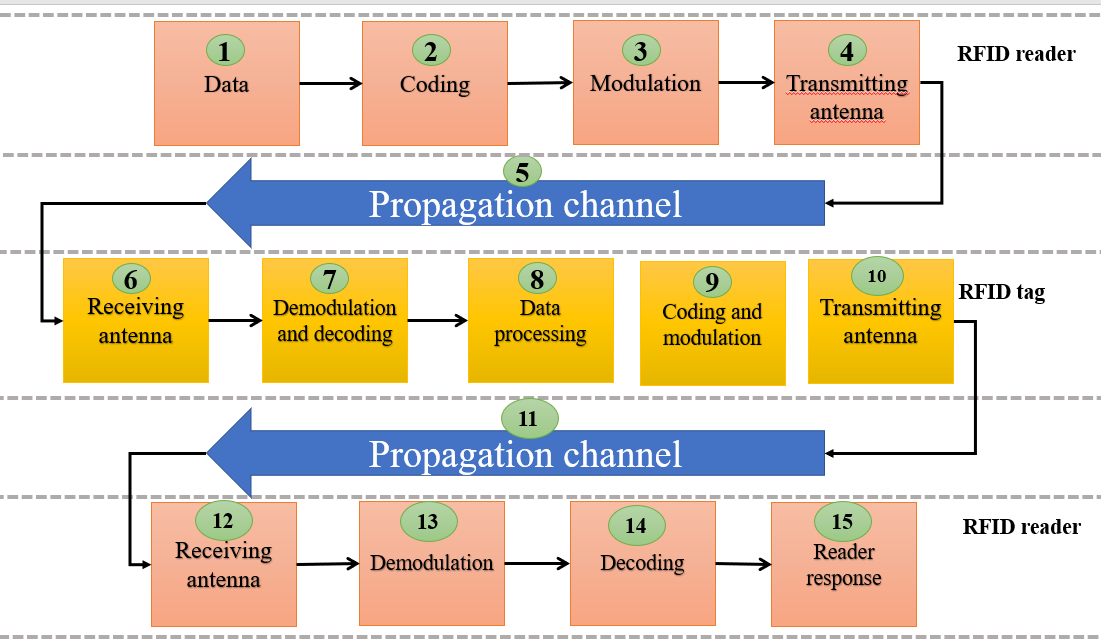


Fig 1. RFID Communication Chain

The RFID communication chain, involving both transmission and reception, is structured into several key functional blocks that ensure the process of transmitting and receiving information between the RFID reader (interrogator) and the RFID tag. Each block plays a specific role, contributing to the overall efficiency of the RFID system. The main blocks of this chain are presented in the Fig 1, and their description is as follows:

RFID Reader Side (Transmission):

1. Data Generation: The data to be transmitted is prepared by the RFID reader's data block. The data can be identification data, configuration data, or control data.
2. Information Coding: Once the data is prepared, the coding block comes into play. This component is responsible for coding the data to ensure its correct and error-free transmission.
3. Signal Modulation: Before transmission, the RF signal is modulated to adjust its properties and enable efficient communication. The modulator transforms the output symbol of the coder into a form suitable for transmission.
4. Signal Emission: This block represents the output point of the modulated signal. The transmitting antenna thus ensures the propagation of the RFID signal, allowing target devices such as RFID tags to receive it and initiate the two-way communication process.
5. Channel: The channel represents the medium through which the signal is transmitted. The quality and characteristics of the channel play a crucial role in the successful transmission of the signal between the RFID reader and the tag, thus influencing the reliability and overall efficiency of wireless communication.

RFID Tag Side:

1. Signal Reception: On the tag side, a specific antenna captures the RF signal emitted by the RFID reader, marking the beginning of the reception process.
2. Signal Demodulation and Decoding: The received RF signal undergoes a demodulation process to make it usable by the following blocks. The demodulated signal is then subjected to a decoding process to extract the original information previously encoded by the reader.
3. Data Processing: The RFID tag's microcontroller in this block can perform the following operations: Data Extraction: The block extracts the data from the decoded data. Data Validation: The block validates the data to ensure it is correct. Data Interpretation: The block interprets the data to determine the meaning of the data. The result of this processing is that the RFID tag has the identity transmitted by the RFID reader.
4. Rebroadcast Coding and Modulation: Before retransmitting the response, the RFID tag encodes the essential information, including its unique identifier. The signal is then modulated for efficient wireless communication with the RFID reader. In the case of passive tags, backscatter modulation is employed, taking advantage of the received signal from the reader as the carrier.
5. Signal Reemission: After modulating the signal with the necessary information, such as its unique identifier, the RFID tag proceeds to retransmit the signal. The tag's antenna plays a central role in transmitting the modulated RF signal, containing the tag's data, to the RFID reader.
6. A propagation channel is used to transmit the signal.

RFID Reader Side (Reception):

1. Reemitted Signal Reception: After emitting a signal to the tag, the RFID reader then switches to reception mode to capture the signal reemitted by the tag. This phase allows the reader to initiate the process of retrieving the information transmitted by the RFID tag.
2. Reemitted Signal Demodulation: The reemitted signal by the tag, carrying the encoded information, is demodulated to recover the coded data.
3. Decoded Information Decoding: The data extracted from the reemitted signal is decrypted to recover the information initially encoded by the tag, such as its unique identifier, for example.
4. Reader Analysis and Response: Once the data is decoded, the RFID reader's processing unit takes over the processing and analysis of the information. This step may involve various operations, such as validating the tag's identifier or updating the database. Based on the data analysis, the RFID reader can generate an appropriate response. This response may include actions such as recording an event, unlocking a door, or other system-specific responses.

Reaching this step, the reader's reception side completes the two-way communication cycle by extracting the information emitted by the RFID tag and performing the resulting actions.

## Description of Our System

Using the power of MATLAB software, we have created a passive RFID communication system. The main difference of our system from traditional passive RFID systems is the use of ubiquitous radio signals in our environment, generated by access points, devices, or base stations (BTS), as an alternative to the signal generated by RFID readers.

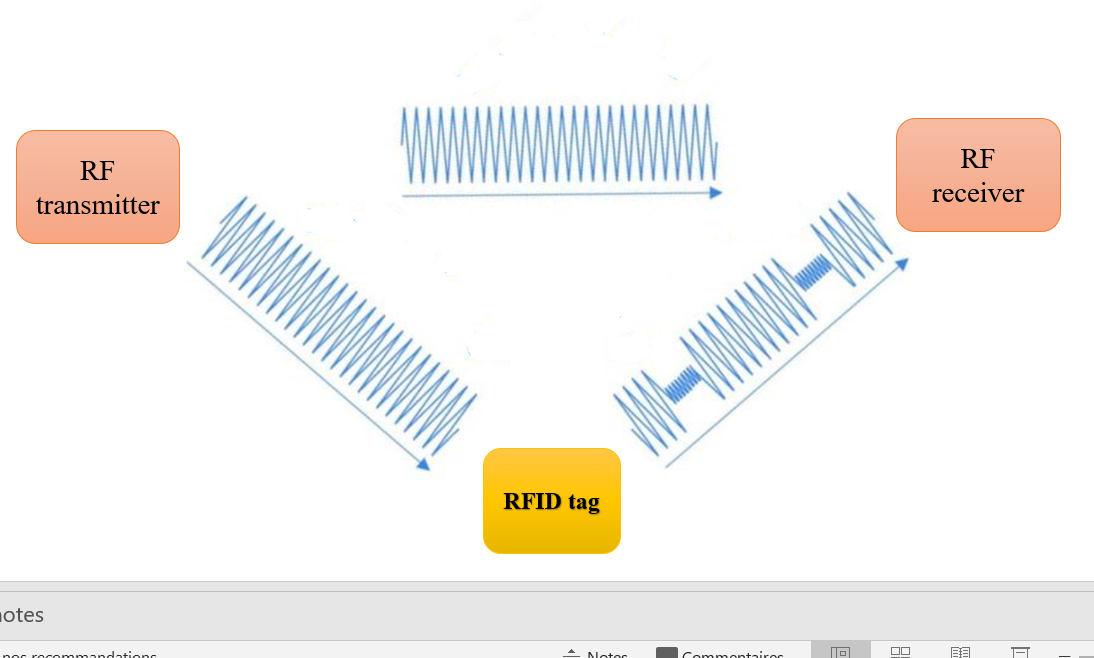


Fig 2. Communication by Backscatter Scheme in our System

We opted for the generation of all emblematic radio signals operating at 2.45 GHz and 5.8 GHz frequencies. The Fig 2 illustrates the system diagram, where the RF transmitters and receivers are specifically dedicated to Wi-Fi, 5G, Bluetooth, and Zigbee technologies. The transmitters generate the RF signal, which is then captured by the RFID tag. This signal carries the tag's unique identifier. The RF receiver receives the signal from the tag and generates a response adapted to the needs of the application.

It is important to note that the RF receiver, in addition to receiving the signal emitted by the RFID tag, is also exposed to interference resulting from the coexistence of this signal with that from the RF transmitter. This superposition of signals can lead to potential disturbances and interference in the reception of the tag's signal, which can influence the quality and reliability of communication.

Our system will follow the communication chain that we have presented, starting with the generation of the RF signal by the transmitter. This signal is then coded and modulated, and then transported through a propagation channel that takes into account the specific transmission properties of each technology. Then, the tag codes its identifier and uses the received signal from the transmitter to modulate the coded identifier by backscatter modulation. The backmodulated signal is then transported by an AWGN (Additive White Gaussian Noise) channel and is collected by the RF receiver, which demodulates and decodes it to extract the identifier sent by the tag. By comparing the sent and received identifier, we can determine the reliability of our system. It is important to note that we did not use the demodulation and decoding block for the commands sent by the RF transmitter. We considered that the RF transmitter's command is a request to send the tag's ID. Thus, the received signal from the RF transmitter is used directly to transport the tag's ID.

Unlike the conventional method that relies solely on RFID readers to emit an interrogation signal, our approach utilizes existing radio signals in the environment. This approach enables more flexible and extensive RFID communication, as it does not require dedicated readers but leverages the already available radio infrastructure.

## RF Source Generation Settings Configuration

We begin our study by exploring the design of RF transmitters/receivers, using technologies such as WiFi, 5G, Bluetooth, and Zigbee. For WiFi, we specifically opted for WiFi 4, WiFi 5, and WiFi 6 versions, recognized as the most recent in this category, and operating on one or both frequencies, namely 2.45 GHz and 5.8 GHz.

·    WiFi 4

For WiFi 4, our configuration is based on the VHT (Very High Throughput) protocol defined by the 802.11n standard. The channel bandwidth was set to 40 MHz, with BPSK (Binary Phase-Shift Keying) modulation and BCC (Binary Convolutional Coding) at a coding rate of ½. We used the transmission channel defined by the wlanTGnChannel function of MATLAB, which represents a channel compliant with the 802.11n standard.

·    WiFi 5

For WiFi 5, our system follows the VHT (Very High Throughput) protocol defined by the 802.11ac standard. The channel bandwidth was set to 160 MHz, with BPSK modulation and BCC coding. We exploited the transmission channel defined by the wlanTGacChannel function of MATLAB, thus ensuring compliance with the 802.11ac standard.

·    WiFi 6

For WiFi 6, our configuration follows the HE-SU (High Efficiency Single User) protocol defined by the 802.11ax standard. The channel bandwidth remains at 160 MHz, but this time we chose BPSK modulation and LDPC (Low-Density Parity-Check) coding. We used the transmission channel defined by the wlanTGaxChannel function of MATLAB, thus ensuring compliance with the 802.11ax standard.

For the transmission channels associated with the WiFi 4, WiFi 5, and WiFi 6 standards, represented respectively by the wlanTGnChannel, wlanTGacChannel, and wlanTGaxChannel functions, it should be noted that they symbolize wireless transmission channels defined by the MATLAB WLAN Toolbox. These channels incorporate large-scale fading effects, including path loss, to realistically reproduce the transmission conditions encountered in real wireless channels.

·    5G

In the context of our system, we developed a 5G signal using MATLAB, operating at the 2.4 GHz frequency. The creation of this downlink single-user 5G waveform was achieved using the MATLAB nrWaveformGenerator function. We set up a PDSCH (Physical Downlink Shared Channel) configuration object, where we specified a 16-QAM modulation scheme, a coding rate of 658/1024, and and a channel bandwidth of 50 MHz. Concerning the transmission channel for 5G, we created a path loss configuration object by adjusting its characteristics to correspond to a rural macrocell scenario. These parameters include an average building height of 7 meters, a street width of 25 meters, the specified carrier frequency, and the geographical coordinates of the base station and the user.

·    Bluetooth

The generation of the Bluetooth signal in our system was performed using the bleWaveformGenerator function, where GFSK (Gaussian Frequency Shift Keying) modulation is employed. It is important to note that we opted for the generation of the classic Bluetooth signal, not using the Bluetooth LE (Low Energy) version.

For the configuration of the transmission channel, we used the bluetoothRangeConfig function. We chose an outdoor environment ("Outdoor") to model the propagation conditions specific to this context. It is important to emphasize that this channel also integrates path loss, thus ensuring realistic modeling of Bluetooth transmission conditions in outdoor environments.

·    ZigBee

The implementation of Zigbee signals in our system was achieved using the lrwpanOQPSKConfig function, which allows the creation of an OQPSK (Offset Quadrature Phase Shift Keying) object compliant with the IEEE 802.15.4 standard, the foundation upon which Zigbee is built. Then, this object was integrated with the lrwpanWaveformGenerator function, which was used to create a Zigbee waveform. For the configuration of the Zigbee transmission channel, we opted for the same parameters as those used for Bluetooth.

This concludes the configuration of the RF source generation settings for WiFi, 5G, Bluetooth, and Zigbee used in our system. The following sections will likely discuss how these generated signals are used to interact with the RFID tags and the overall performance evaluation of the system.

## Backscatter Block Design

After the generation of RF sources and their transmission through the appropriate channels, the signal is received by the tag, where it is directly used to carry the tag's ID through backscatter modulation. There are two types of backscatter modulation: ASK (Amplitude Shift Keying) and PSK (Phase Shift Keying).

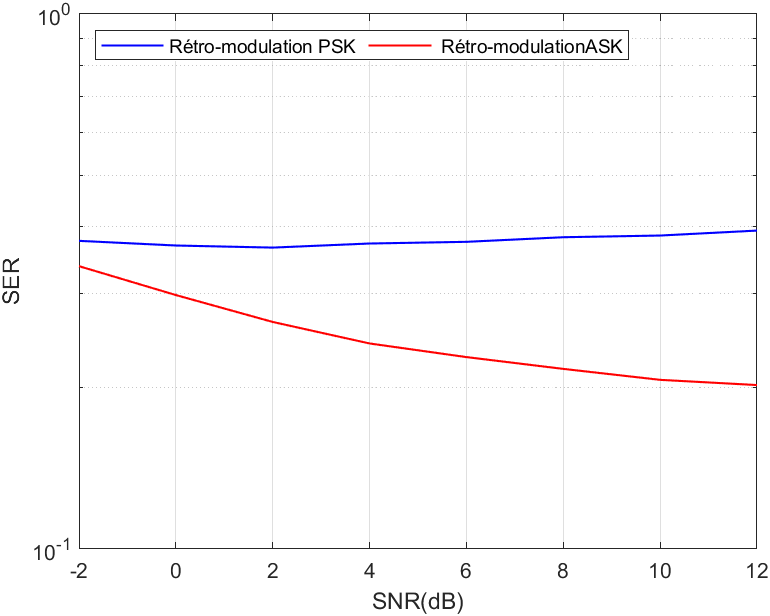


Fig 3. Performance de la Rétro-modulation PSK et ASK : Taux d'Erreur de Symbole (SER) en fonction du SNR (dB)

In order to choose between ASK and PSK modulations, we examined the back-modulation of continuous waves, represented by an unmodulated sinusoidal signal at a frequency of 2.45 GHz. In this investigation, we employed a noisy channel, altering the Signal-to-Noise Ratio (SNR) values within the range of -2 to 12 dB. We calculated the Symbol Error Rate (SER) between the transmitted signal and the received signal after demodulation. The results, presented in theFig 3, demonstrate that ASK back-modulation exhibits significantly superior performance compared to PSK. This performance difference is explained by the demodulation errors induced by the inherent complexity of PSK modulation, which is added to the channel noise. These factors make back-modulation more difficult to detect in the case of PSK.

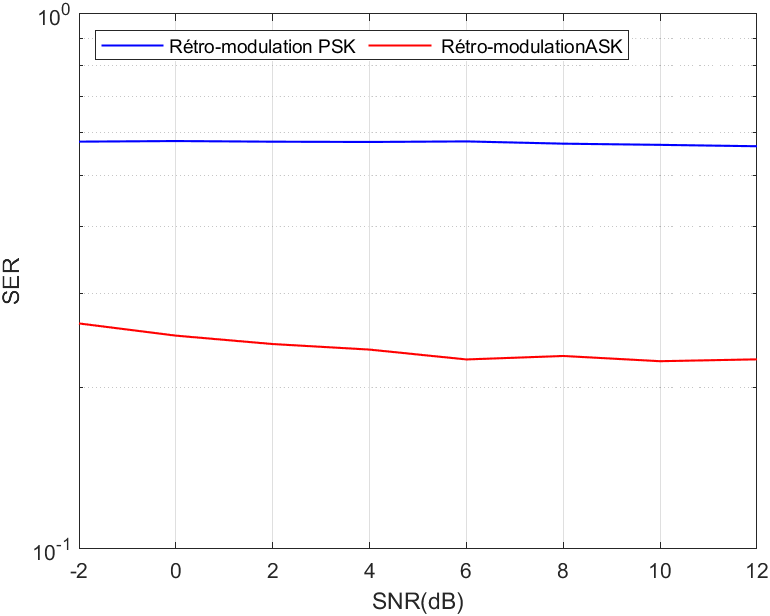


Fig 4. Performance de la Rétro-modulation du Signal WiFi 6 (ax)

To further confirm these results, we conducted additional validation using a WiFi ax signal at 2.45 GHz frequency (Fig 4). A second simulation was performed, and the results presented corroborate the previous conclusions, demonstrating that ASK modulation remains the most appropriate for our system. It can be observed that the Symbol Error Rate (SER) when using the WiFi signal is less performant compared to the signal from the first simulation. It increases from 0.39 to 0.56 for PSK back-modulation at an SNR of 12 dB, and from 0.20 to 0.22 for ASK back-modulation at an SNR of 12 dB. This performance degradation results from the increased complexity caused by using a modulated signal for backscattering, thus introducing complexity into the backscattering demodulation phase. This is particularly noticeable for PSK, which exhibits a more pronounced degradation. It should be noted that these results are obtained without the addition of the interference signal received from the RF transmitter, as explained previously.

# Results and Discussions

## Without Error Correction Coding

In this section, we will evaluate the performance of our system using the generated WiFi, 5G, Bluetooth, and Zigbee RF sources received at a distance of 0.01 meters from the source. ASK back-modulation is employed, and the Symbol Error Rate (SER) between the transmitted ID and the received ID is calculated for a Signal-to-Noise Ratio (SNR) ranging from -5 dB to 20 dB. The results are presented in the Fig 5. The transmitted identifier size is chosen to be 64 bits, and the interference signal received by the sources is added to the received signal from the tag, as explained in Fig 2.

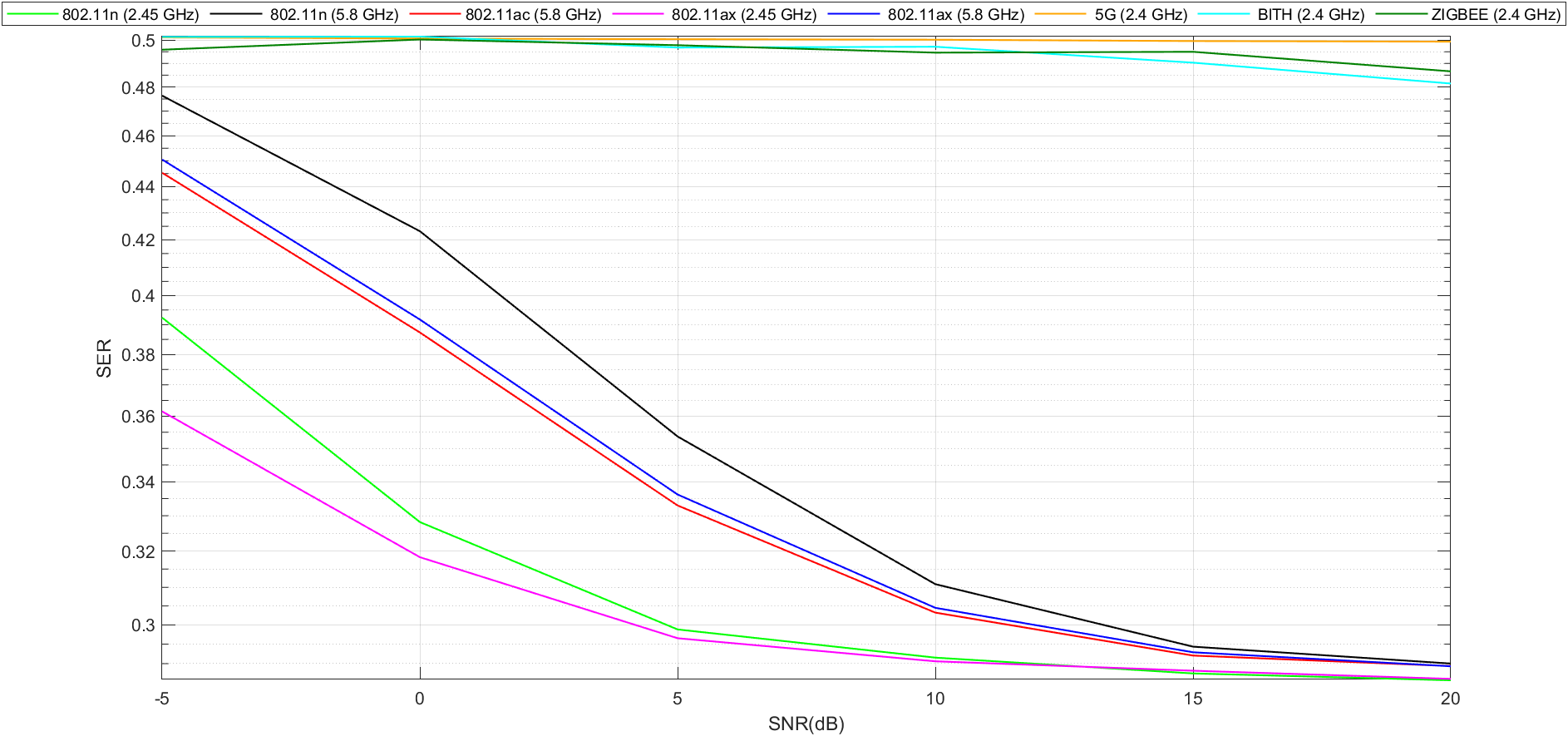


Fig 5. Symbol Error Rate (SER) as a function of Signal-to-Noise Ratio (SNR) for RF sources WiFi, 5G, Bluetooth, and Zigbee

The Fig 5 shows that the Symbol Error Rate (SER) of 802.11ax at 2.45 GHz is the best, followed by 802.11n at the same frequency. This is likely due to the different received power levels of these signals. 802.11ax at 2.45 GHz has a significantly higher received power (60.6011 dBm) compared to 802.11n (57.25 dBm) at the same frequency. This difference is clear for SNRs below 10 dB, but beyond that, the performance becomes similar.

Looking at 5.8 GHz WiFi signals, 802.11ax and 802.11ac have almost identical SER due to their similar received power levels (53.19 dBm and 53.11 dBm respectively). The SER of 802.11n at 5.8 GHz is higher because its received power (49.75 dBm) is lower.

The SER of 5G, Bluetooth, and Zigbee signals is initially very high. However, for Bluetooth and Zigbee, there is a slight decrease in SER when the SNR goes above 15 dB. This is because their received power levels reach 27.3 dBm. The poor performance of the 5G signal is due to its very low received power (-48.91 dBm). ASK modulation relies on the power of the carrier signal, which significantly affects communication performance, as shown here.

## Utilization of BCH Coding

To enhance the performance of our system, we propose implementing an encoding process for the identification (ID) before modulation and transmission. On the reception side, we will compare the sent messages with the received messages after decoding. We begin this step by using BCH (64,57) coding. Fig 6 presents the results of the Symbol Error Rate (SER) between the transmitted message and the received message, calculated for a Signal-to-Noise Ratio (SNR) ranging from -5 dB to 20 dB for different technologies. We chose this code with a coded ID size of 64 to compare it with the results obtained with the same uncoded ID size.

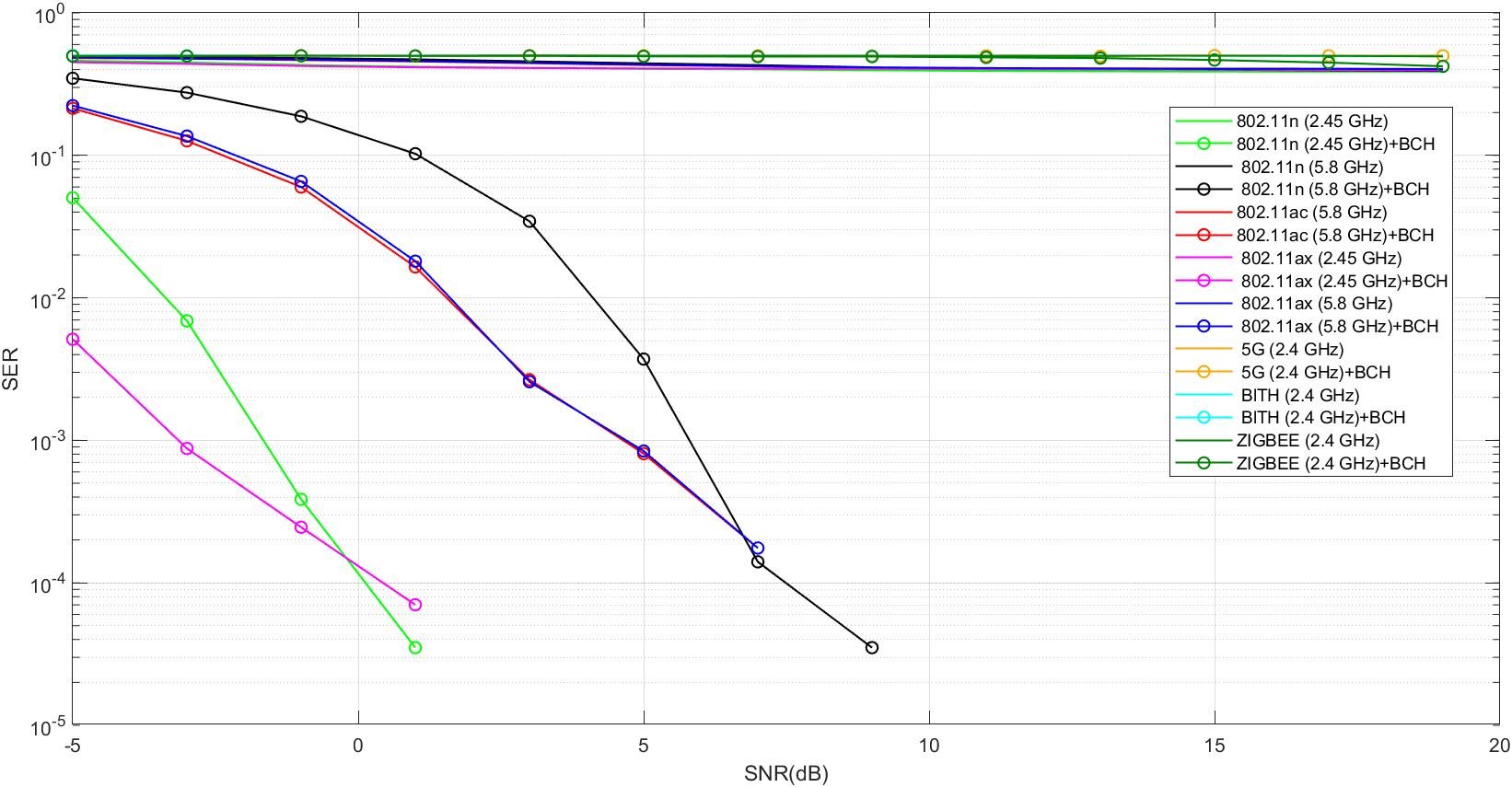
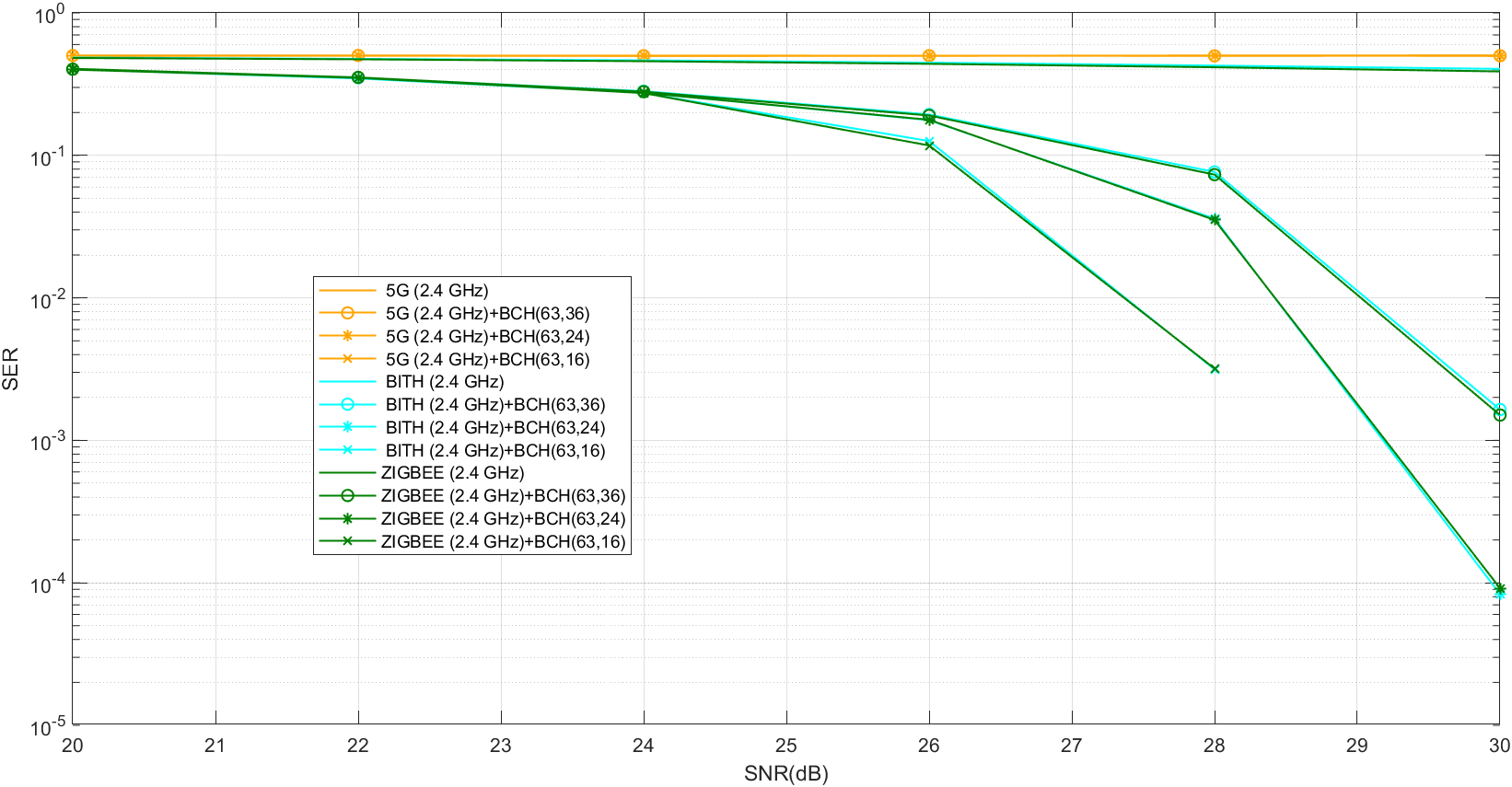


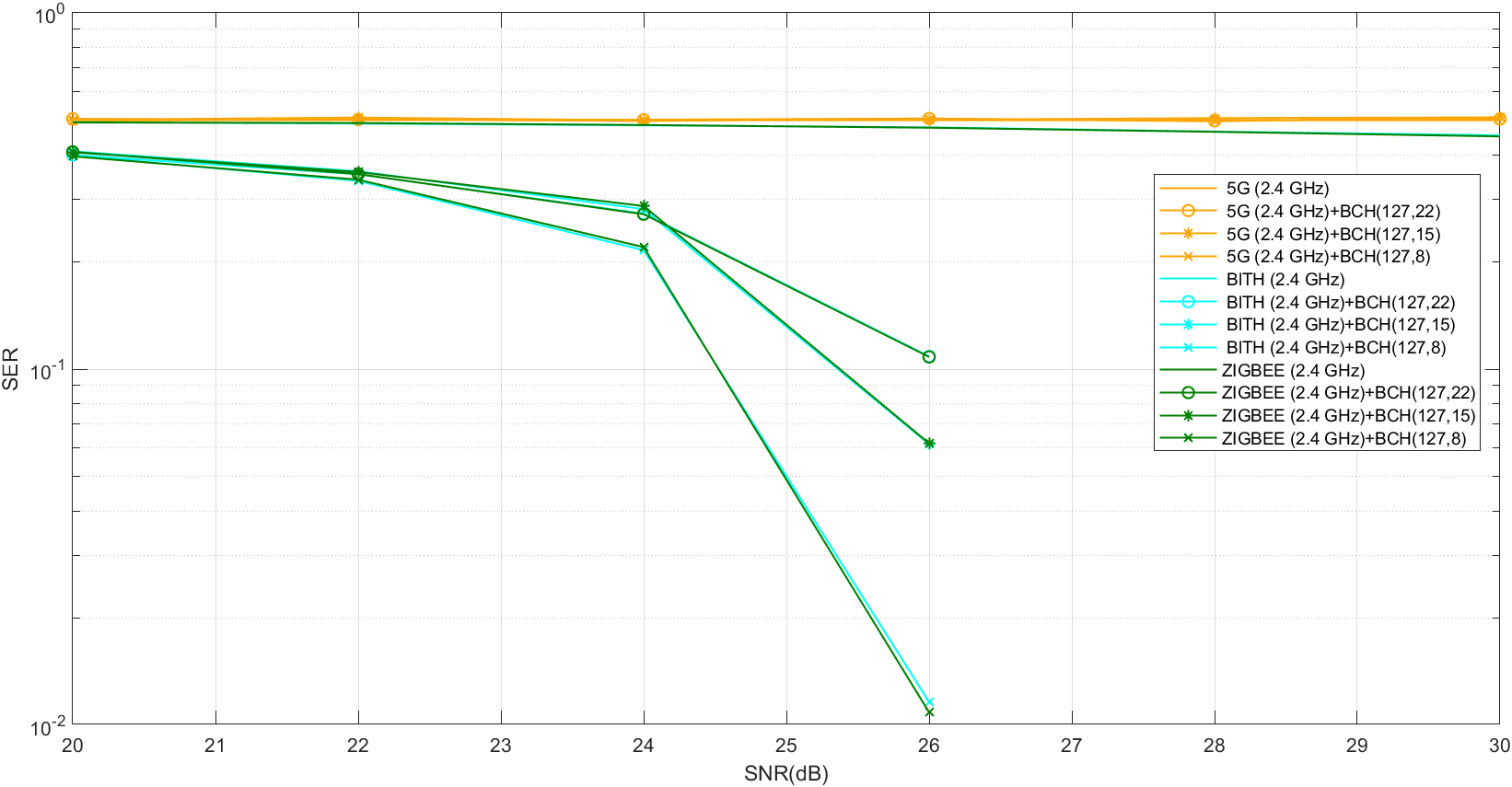
Fig 6. Evolution of SER as a function of SNR for the use of BCH (64,57) coding with different RF sources

The results in the Fig 6 illustrate the Symbol Error Rate (SER) as a function of Signal-to-Noise Ratio (SNR) for using BCH (64,57) coding with different RF sources. It is evident that the use of error-correcting coding has significantly improved the SER. This improvement is particularly notable for the WiFi protocols, with 802.11ax at 2.45 GHz showing the lowest SER for SNR values below 0 dB. There is also a slight improvement in Zigbee and Bluetooth performance with coding, although their SER remains quite high.

The BCH(64,57) code shown in Fig 6 had the capability to correct up to 4 errors. To further enhance performance, it would be beneficial to opt for higher error correction capabilities when using coding. Consequently, we suggest categorizing the RF sources into two groups based on the results presented in Fig 6 to facilitate comparison. The first group will encompass 5G, Bluetooth, and Zigbee, while the second group will comprise WiFi protocols.



(a)



(b)

Fig 7. Evolution of Symbol Error Rate (SER) as a function of Signal-to-Noise Ratio (SNR) for RF sources 5G, Zigbee, and Bluetooth. (a) Using BCH (63,36), BCH (63,24), and BCH (63,16) codes. (b) Using BCH (127,22), BCH (127,15), and BCH (127,8) codes.

The Fig 7 illustrate the Symbol Error Rate (SER) as a function of Signal-to-Noise Ratio (SNR) for 5G, Zigbee, and Bluetooth RF sources, using six different BCH codings: BCH(63,36), BCH(63,24), BCH(63,16), BCH(127,22), BCH(127,15), and BCH(127,8). These codings have error correction capacities \( t \) of 5, 7, 11, 23, 27, and 31, respectively. An important observation is that, in both Fig 7 (a) and Fig 7 (b), increasing \( t \) leads to an improvement in SER, except for 5G, which shows no significant improvement. This behavior can be attributed to the weaker received signal of 5G compared to Bluetooth and Zigbee, which have relatively similar received power levels.

Using BCH(63,36) and BCH(63,24) codings, a 100% improvement is observed with SNR values greater than 30 dB for Bluetooth and Zigbee. Regarding BCH(63,16) coding, a 100% improvement is achieved for SNR values greater than 28 dB, both for Bluetooth and Zigbee, as illustrated in Fig 7 a.

Furthermore, using BCH(127,22), BCH(127,15), and BCH(127,8) codings, a 100% improvement is observed with SNR values greater than 26 dB for Bluetooth and Zigbee, as shown in Fig 7 b. However, achieving these high SNR levels may be challenging under real conditions. It is also noteworthy, as observed in both figures, that even with increasing coding correction capacity, 5G shows no improvement.

We now address the second group of RF sources, namely WiFi sources. As shown in the Fig 6, all versions of WiFi used show a 100% improvement at an SNR of 10 dB with BCH(64,57) coding. It is important to note that these performances are achieved at a distance of only 0.01 m from the source. Therefore, our further objective is to increase this distance to 0.1 m and then to 1 m and test the effectiveness of coding in improving system performance under these conditions.

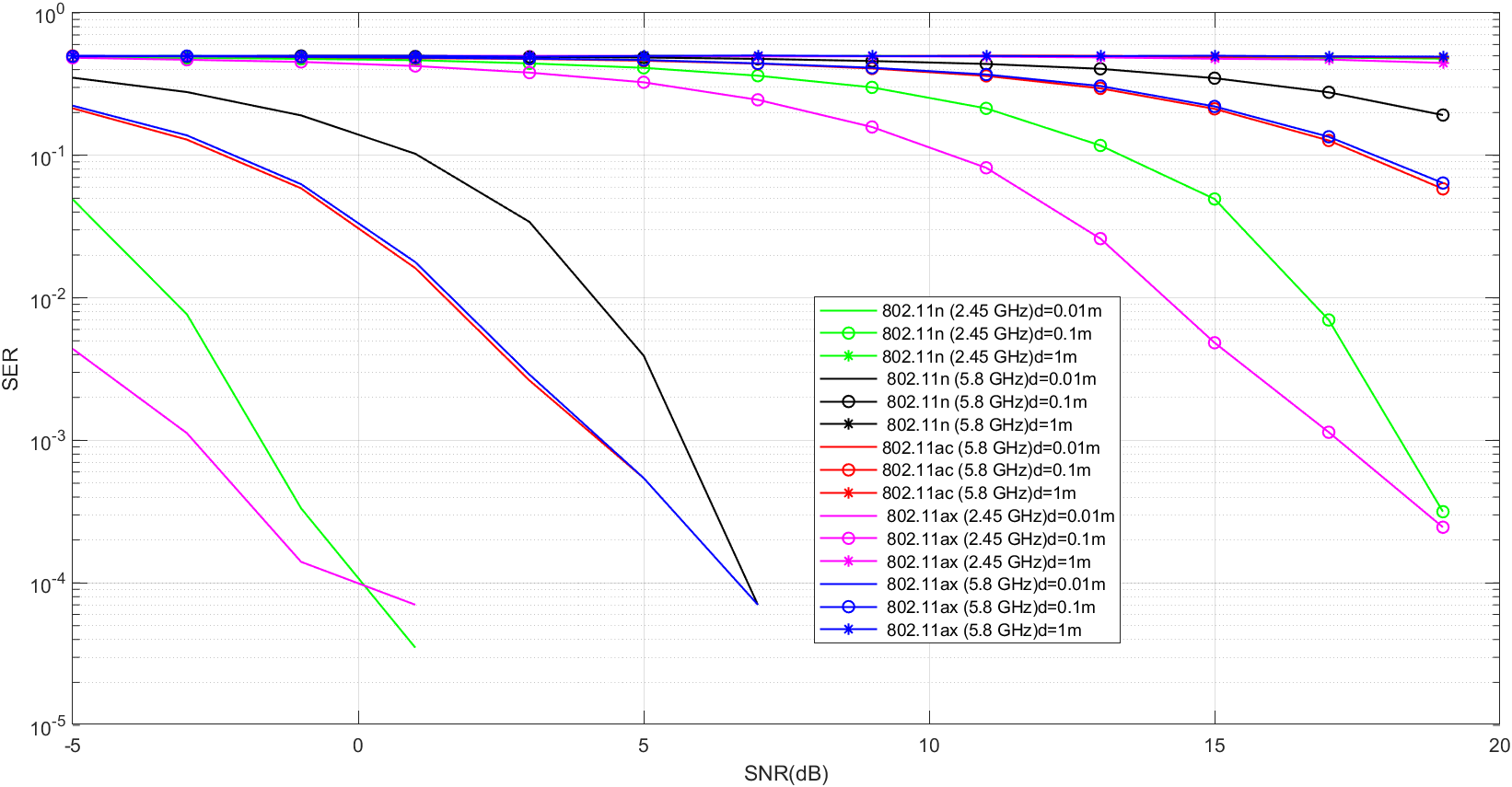


Fig 8. Comparison of SER for different WiFi protocols using BCH (64,57) coding at source distances of 0.01 m, 0.1 m, and 1 m.

The Fig 8 presents simulation results using BCH (64,57) coding for different WiFi protocols, considering distances from the source of 0.01 m, 0.1 m, and 1 m. It can be observed that as the distance increases, the Symbol Error Rate (SER) also increases, and this holds true for all WiFi protocols.

To simplify comparison, we will subsequently focus only on WiFi 802.11ax at 2.45 GHz, as it represents the most improved performance. We will apply other BCH codes to continue the analysis.

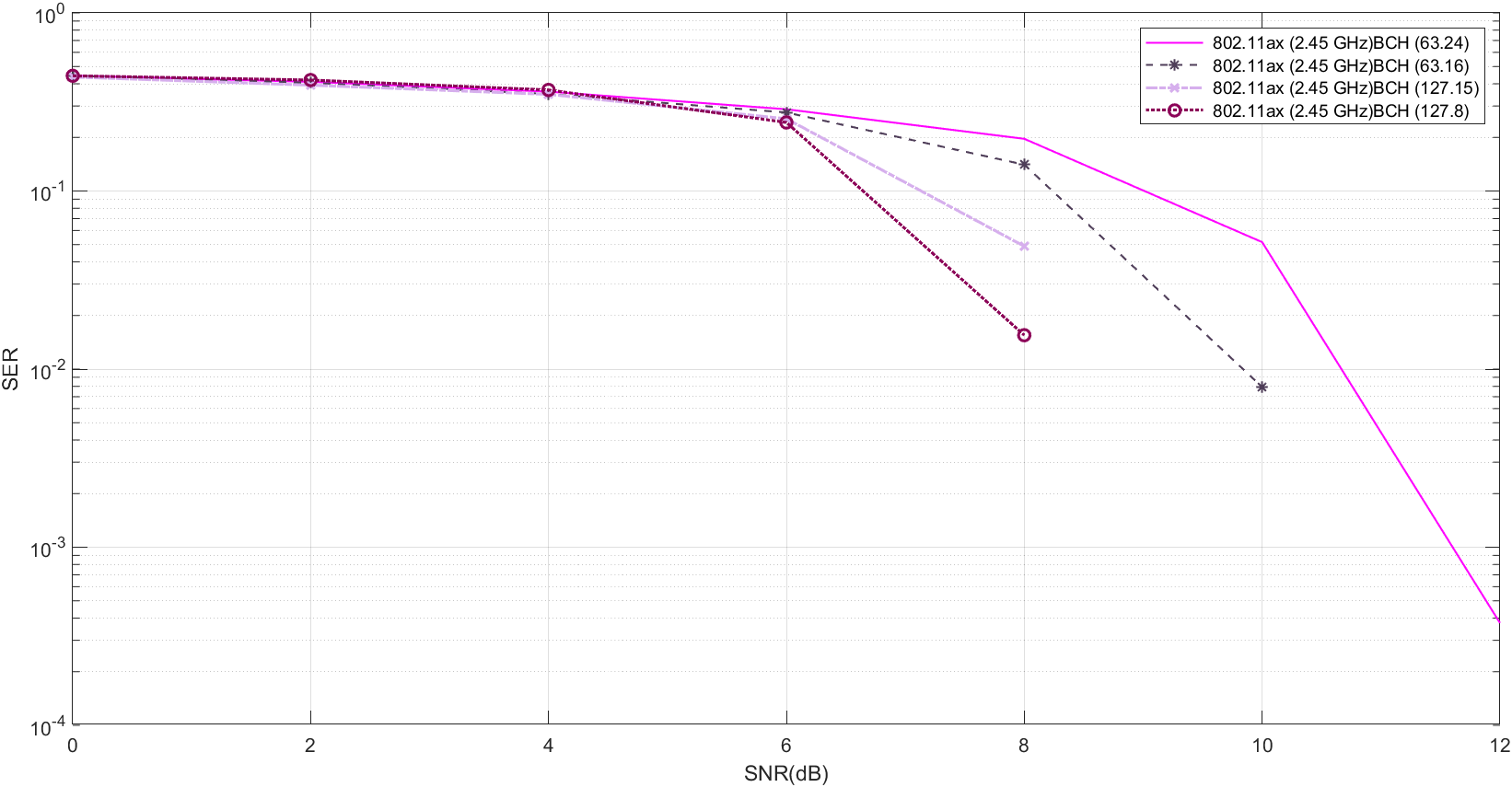


Fig 9. Comparison of the use of BCH codes (127,8), BCH (127,15), BCH (63,16), and BCH (63,24) for a WiFi 802.11ax source at 2.45 GHz, with a source distance of 0.1 m.

The comparison of using BCH codes (127,8), (127,15), (63,16), and (63,24) for a WiFi 802.11ax source at 2.45 GHz, with a source distance of 0.1 m, is presented in Fig 9. As expected, increasing the code's error correction capacity results in improved performance. The most significant performances are observed with BCH(127,8), closely followed by BCH(127,15), then BCH(63,16), and finally by BCH(63,24).

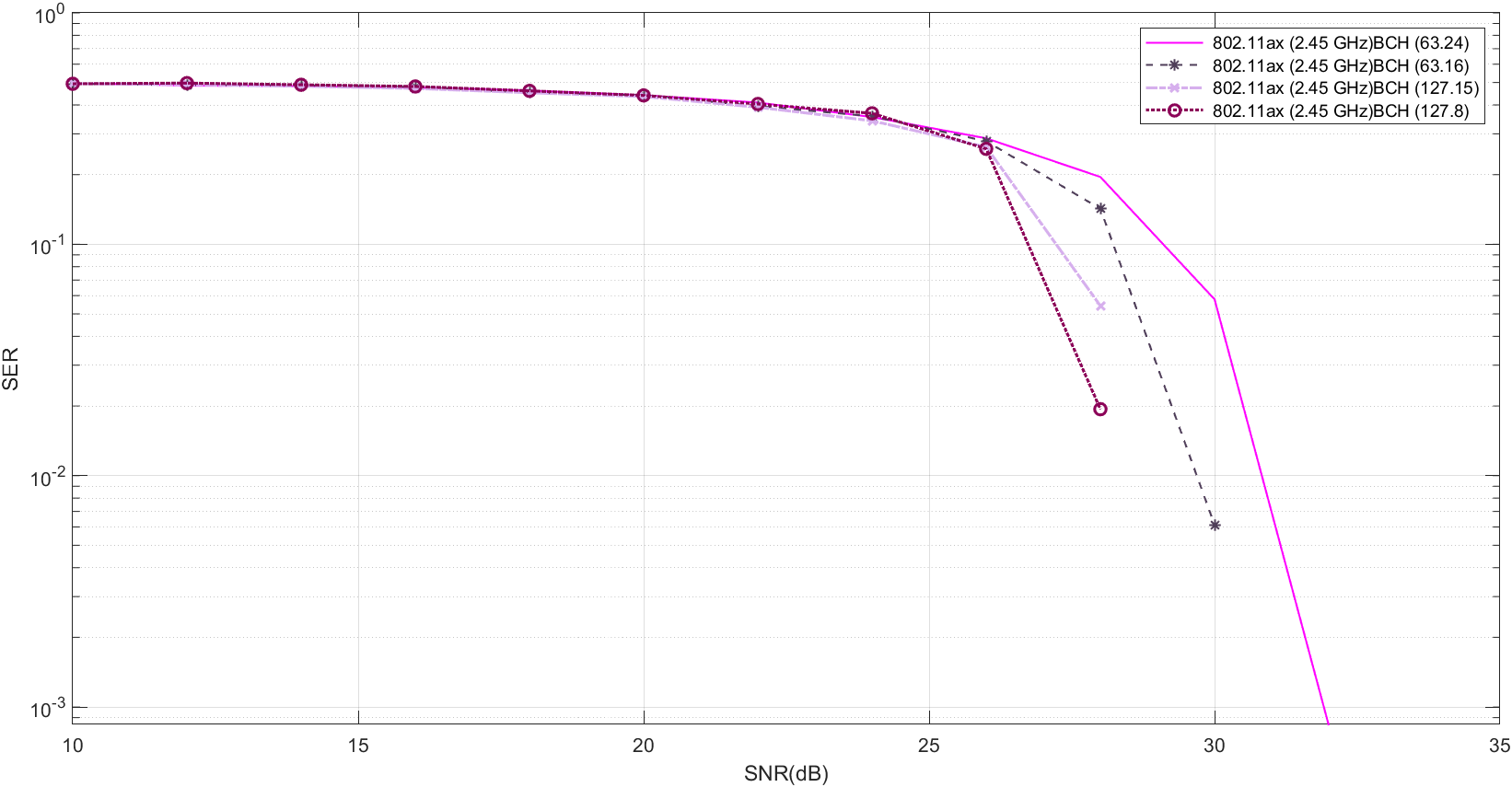
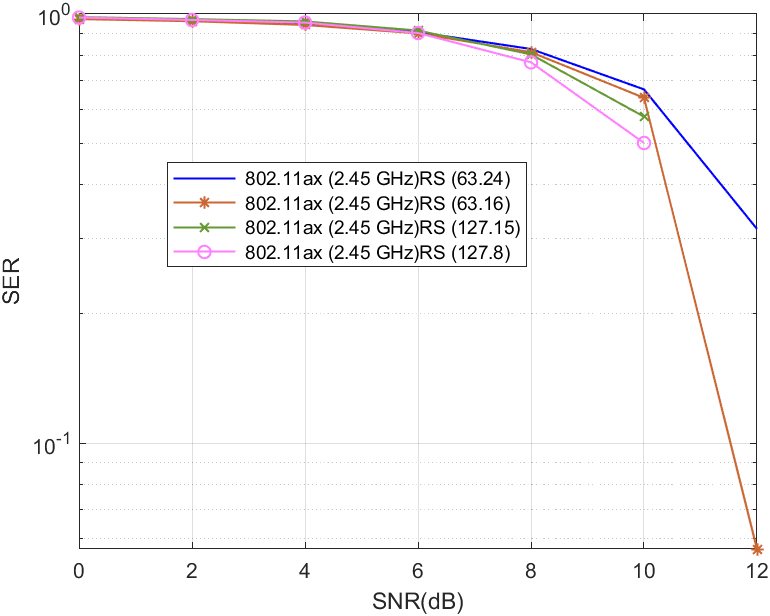


Fig 10. Comparison of the utilization of BCH codes (127,8), BCH(127,15), BCH(63,16), and BCH(63,24) for a WiFi 802.11ax source at 2.45 GHz, with a source distance of 1 m.

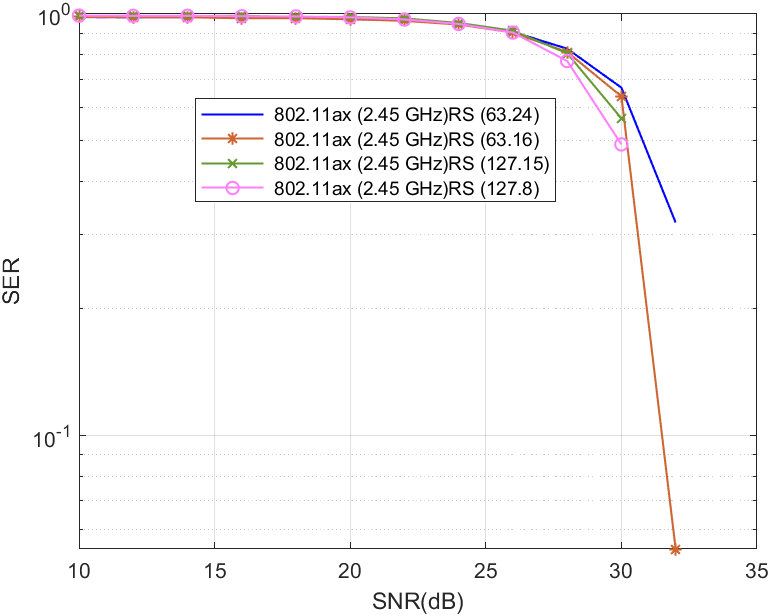
When the source distance was increased to 1 m, the results are presented in the Fig 10. It can be observed that the lowest Symbol Error Rates (SERs) are achieved at SNR values of 28 dB for BCH(127,8) and BCH(127,15), 30 dB for BCH(63,16), and 32 dB for BCH(63,24). However, it is important to note that achieving these high SNR levels may pose challenges in real-world conditions.

## Utilization of RS Coding

Next, we will apply a second type of coding, Reed-Solomon (RS) coding, to evaluate its impact on performance improvement. In this approach, we will begin by using the source distance of 0.1 m, then at 1 m. RS codes (127,8), (127,15), (63,16), and (63,24) will be employed. The values of n and k have been deliberately chosen to match those used in BCH coding, facilitating a direct comparison with the results obtained using the latter.



(a)



(b)

Fig 11. Comparison of the utilization of RS codes (127,8), RS(127,15), RS(63,16), and RS(63,24) for a WiFi 802.11ax source at 2.45 GHz, with a source distance of (a) 0.1 m, (b) 1 m.

In Fig 11 (a) and Fig 11 (b), we present the results obtained at respective distances of 0.1 m and 1 m from the source using RS coding. A common observation in both figures reveals that the lowest Symbol Error Rates (SERs) are associated with RS(127,8), followed by RS(127,15), RS(63,16), and finally RS(63,24). This trend is explained by the error correction capability, which ranges from 19 for RS(63,24) to 59 for RS(127,8).

Table 1. SER for BCH coding at distances of 0.1 m and 1 m

|  |  |  |
| --- | --- | --- |
|  | d=0.1m et  SNR =8 dB | d=1m et  SNR =28 dB |
| BCH(63,24) | 0.19 | 0.19 |
| BCH(63,16) | 0.14 | 0.142 |
| BCH(127,15) | 0.048 | 0.054 |
| BCH(127,8) | 0.015 | 0.019 |

|  |  |  |
| --- | --- | --- |
|  | d=0.1m et  SNR =10 dB | d=1m et  SNR =30 dB |
| RS(63,24) | 0.66 | 0.67 |
| RS(63,16) | 0.63 | 0.63 |
| RS(127,15) | 0.57 | 0.57 |
| RS(127,8) | 0.5 | 0.49 |

Table 2. SER for RS coding at distances of 0.1 m and 1 m

From the results in the Table 1 and Table 2, it is observed that BCH coding demonstrates significantly better performance compared to RS coding, even when parameters such as total length (n) and number of information bits (k) are kept identical for both types of codes. These observations indicate that BCH code effectively corrects the types of errors generated in our system, suggesting that these errors are more likely to be random or short bursts. Generally, BCH code is a binary code designed for correcting random errors, while RS code is symbol-based, capable of correcting burst errors. One disadvantage associated with burst error correction capability is that if the burst is spread over multiple symbols, RS code may not be able to correct it, unlike BCH code, which retains this capability.

# Conclusion

We have presented a promising alternative RFID system capable of utilizing ubiquitous radio sources such as Wi-Fi, 5G, Bluetooth, and Zigbee, replacing dedicated RFID readers. A passive RFID system using these radio signals was modeled using MATLAB. The performance of these signals was compared in terms of Symbol Error Rate (SER) for different Signal-to-Noise Ratios (SNR). 802.11ax at 2.45 GHz stood out with the best SER, followed by 802.11n at the same frequency. However, 5G, Bluetooth, and Zigbee signals showed lower performance, even at high SNRs.

The introduction of BCH and RS coding significantly improved transmission reliability. The BCH(127,8) and RS(127,8) configurations proved to be particularly effective, extending the communication distance up to 1 meter. These results highlight the importance of choosing appropriate coding parameters to optimize system performance.

# References

[1] J. Wang, L. Chang, O. Abari, S. Keshav, Are RFID Sensing Systems Ready for the Real World?, in: Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services, ACM, Seoul Republic of Korea, 2019: pp. 366–377. https://doi.org/10.1145/3307334.3326084.

[2] J. Wang, L. Chang, S. Aggarwal, O. Abari, S. Keshav, Soil moisture sensing with commodity RFID systems, in: Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services, ACM, Toronto Ontario Canada, 2020: pp. 273–285. https://doi.org/10.1145/3386901.3388940.

[3] 7 RFID Costs, From Tags To Implementation | Link Labs, (n.d.). https://www.link-labs.com/blog/rfid-cost (accessed May 16, 2024).

[4] F. Dehbashi, A. Abedi, T. Brecht, O. Abari, Verification: can wifi backscatter replace RFID?, in: Proceedings of the 27th Annual International Conference on Mobile Computing and Networking, Association for Computing Machinery, New York, NY, USA, 2021: pp. 97–107. https://doi.org/10.1145/3447993.3448622.

[5] B. Wang, F. Zhu, L. Zhong, M. Jin, X. Wang, C. Chen, X. Guan, C. Zhou, X. Tian, Enabling Dual-band Wi-Fi Backscatter, IEEE Transactions on Mobile Computing (2024) 1–15. https://doi.org/10.1109/TMC.2024.3400013.

[6] Y. Yang, W. Gong, Universal WiFi Backscatter With Ambient Space-Time Streams, IEEE/ACM Transactions on Networking (2023) 1–11. https://doi.org/10.1109/TNET.2023.3336922.

[7] Z. Huang, Y. Ding, D.O. Wu, S. Wang, W. Gong, Bitalign: Bit Alignment for Bluetooth Backscatter Communication, IEEE Transactions on Mobile Computing (2024) 1–11. https://doi.org/10.1109/TMC.2024.3374815.

[8] M. Jiang, W. Gong, Bidirectional Bluetooth Backscatter With Edges, IEEE Transactions on Mobile Computing 23 (2024) 1601–1612. https://doi.org/10.1109/TMC.2023.3241202.

[9] S. Chen, M. Zhang, J. Zhao, W. Gong, J. Liu, Reliable and Practical Bluetooth Backscatter With Commodity Devices, IEEE/ACM Transactions on Networking 29 (2021) 1717–1729. https://doi.org/10.1109/TNET.2021.3068865.

[10] Z. Xu, W. Gong, Enabling zigbee backscatter communication in a crowded spectrum, in: 2022 IEEE 30th International Conference on Network Protocols (ICNP), IEEE, 2022: pp. 1–11. https://ieeexplore.ieee.org/abstract/document/9940384/ (accessed May 16, 2024).

[11] Z. Xu, W. Gong, Homoscatter: Towards efficient connectivity for ZigBee backscatter system, (2021). http://arxiv.org/abs/2111.02140 (accessed May 16, 2024).

[12] Z. Xu, W. Gong, Bumblebee: enabling the vision of pervasive zigbee backscatter communication, in: 2023 IEEE International Conference on Pervasive Computing and Communications (PerCom), IEEE, 2023: pp. 252–261. https://ieeexplore.ieee.org/abstract/document/10099287/ (accessed May 16, 2024).

[13] Q. Liu, S. Sun, X. Yuan, Y. Zhang, Ambient backscatter communication-based smart 5G IoT network, J Wireless Com Network 2021 (2021) 34. https://doi.org/10.1186/s13638-021-01917-3.

[14] M. Lefki, S. Baccar, H. Shall, M. Ghorbel, M. Kadi, 5G ambient backscatter communications: Achievable range and power levels in an urban environment, in: 2022 IEEE 12th International Conference on RFID Technology and Applications (RFID-TA), IEEE, 2022: pp. 74–77. https://ieeexplore.ieee.org/abstract/document/9924037/ (accessed May 16, 2024).

[15] R. Biswas, J. Lempiäinen, Assessment of 5G as an ambient signal for outdoor backscattering communications, Wireless Netw 27 (2021) 4083–4094. https://doi.org/10.1007/s11276-021-02731-x.

[16] S. Jaiswal, A. Kumar, N. Kumari, Development of wireless communication networks: From 1G to 5G, International Journal of Engineering and Computer Science 3 (2014) 6053–6056.

[17] A. Gupta, R.K. Jha, A survey of 5G network: Architecture and emerging technologies, IEEE Access 3 (2015) 1206–1232.

[18] V. Idi, Bluetooth Technology And Applications, (2019). https://www.theseus.fi/handle/10024/263515 (accessed December 8, 2023).

[19] O.G. Aju, A survey of zigbee wireless sensor network technology: Topology, applications and challenges, International Journal of Computer Applications 130 (2015) 47–55.

[20] F.J. MacWilliams, N.J.A. Sloane, The theory of error-correcting codes, Elsevier, 1977. https://books.google.com/books?hl=fr&lr=&id=nv6WCJgcjxcC&oi=fnd&pg=PP2&dq=%5B1%5D+F.J.+MacWilliams,+N.J.A.+Sloane,+in:+The+Theory+of+Error-Correcting+Codes,+North-Holland+Publishing+Company,+1981,+pp.+80%E2%80%9392.&ots=Re12fknrzG&sig=\_5MGb4148UYVVlJzARFIt54YWR0 (accessed January 1, 2024).

[21] C.K.P. Clarke, Reed-Solomon error correction, BBC R&D White Paper, WHP 31 (2002).

[22] A.U. Mustafa, G. Murtaza, Synthesis-by-analysis of BCH Codes, arXiv Preprint arXiv:1210.7906 (2012). https://arxiv.org/abs/1210.7906 (accessed December 30, 2023).

[23] S.S. Syed, Y. Saqih, S. Faisal, Self-correcting codes conquer noise Part 2: Reed-Solomon codecs., EDN 46 (2001) 107–114.