IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 29 July 2023, accepted 2 September 2023, date of publication 7 September 2023, date of current version 13 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3313117

RESEARCH ARTICLE

A Spectrum Injection-Based Approach for Malware Prevention in UHF RFID Systems

AHMED F. ASHOUR[1], **CALVIN CONDIE**[1], **CADE POCOCK**[1], **STEVE C. CHIU**[1], **ANDREW CHRYSLER**[1], **(Member, IEEE), AND MOSTAFA M. FOUDA**[1,2], **(Senior Member, IEEE)**

[1]Department of Electrical and Computer Engineering, Idaho State University, Pocatello, ID 83209, USA
[2]Center for Advanced Energy Studies (CAES), Idaho Falls, ID 83401, USA

Corresponding author: Ahmed F. Ashour (ahmedashour@isu.edu)

This work was supported by Idaho State University funding for the Center for Advanced Energy Studies (CAES).

ABSTRACT Radio frequency identification (RFID) is a technology that uses electromagnetic waves (EMW) to send, process, and store data by using a built-in integrated circuit and antenna. However, its susceptibility to malware attacks poses a threat to data privacy and system performance. Thus, there is a need to develop techniques to protect RFID systems from malware injection and improve efficiency through spectrum optimization. An approach for improving the efficiency and data privacy of RFID systems operating in the ultra-high frequency (UHF) band is proposed for multiple data rates of 160, 256, 320, and 640 kbps. Firstly, a method is introduced for reconstructing regular data in a malware-free RFID system with optimized spectrum usage, which reaches up to 50% of the total spectrum and improves efficiency. Secondly, a spectrum injection-based approach (SIBA) is proposed by incorporating a bandpass filtering (BPF) technique to inject the missing spectrum of regular data with a portion of the malware-injected data spectrum. This approach results in faster and more precise data reconstruction with higher accuracy and overcomes the malware. A noise reduction technique based on BPF is also proposed to reduce the noise effects and enhance the accuracy of data reconstruction at different signal-to-noise ratio (SNR) levels. This technique is evaluated through extensive analysis with various metrics such as reconstruction accuracy, robustness to noise, bandwidth utilization factor (BUF), and computational complexity, making it suitable for resource-constrained environmental settings. These approaches address the challenges of malware injection and spectrum optimization, resulting in more efficient and secure RFID systems.

INDEX TERMS Baseband signal reconstruction, BPF, BUF, data privacy, RFID, EMW, malware attacks, malware detection, noise reduction, SIBA, SNR, spectrum injection, spectrum optimization, UHF band.

I. INTRODUCTION

In communication systems, it is important to reconstruct baseband signals from their digital samples. This is typically accomplished through digital signal processing (DSP) techniques. There are two main approaches for baseband signal reconstruction: continuous-time and discrete-time techniques. Continuous-time methods use anti-aliasing filters and sample-and-hold circuits to reconstruct the original analog signal from its samples. Discrete-time approaches employ various DSP algorithms to extract the original analog signal from its digital samples [1].

Some popular baseband signal reconstruction techniques include ideal reconstruction, interpolation, oversampling, noise shaping, and signal extrapolation. Ideal reconstruction involves converting the discrete-time signal to a continuous-time signal using a zero-order hold before running it through a low-pass filter to remove high-frequency components [2]. This technique provides highly accurate results but can be difficult to implement due to limitations in anti-aliasing filters and sample and hold circuits [3].

The associate editor coordinating the review of this manuscript and approving it for publication was Ding Xu.

Interpolation estimates the signal value between two samples using linear, polynomial, or spline interpolation methods. Oversampling involves sampling the signal more frequently than the Nyquist rate to improve the signal-to-noise ratio and reduce quantization noise. Noise shaping reduces quantization noise by shaping the quantization noise spectrum and moving noise energy to higher frequencies. Signal extrapolation estimates the signal when it is outside the range of available samples and is frequently used to increase the length of the signal in digital audio systems [1], [4].

Radio frequency identification (RFID) technology facilitates data exchange between a reader and a tag through electromagnetic waves [5]. In RFID systems, the reader transmits a signal that energizes the tag, enabling it to send its own signal back to the reader. This signal contains relevant information, such as a product ID [6]. To ensure precise transmission of this data between the reader and tag, signal reconstruction techniques are employed [7]. Precisely interpreting the tag's signal is necessary to retrieve the stored data, requiring signal evaluation and the use of appropriate signal processing techniques [8]. Demodulating and decoding the tag signal using digital signal processing methods is a common approach to signal reconstruction in RFID systems [9]. By processing the received signal, data transmission can be recovered and applied for various purposes, including authentication, asset tracking, and inventory management [10], [11]. Increasing the precision of signal reconstruction can be achieved by utilizing multiple antennas and beamforming strategies, allowing the system to focus on the tag's signal reception, reducing interference, and improving the signal reconstruction process's accuracy [12], [13].

Many research papers have discussed the implementation of signal reconstruction schemes in RFID systems. In [14], the authors discuss compressed sensing (CS), which enables accurate signal reconstruction from lower sampling rates. The authors introduce two algorithms, base pursuit (BP) and orthogonal matching pursuit (OMP), for signal reconstruction. They analyze the Sparse Representation principle and its methods, emphasizing its application in CS using the Gabor dictionary. The study shows that the BP algorithm has higher accuracy than the OMP algorithm for signal reconstruction, making it a valuable tool for applications such as RFID-based Internet of things (IoT).

The paper [15] proposes a passive RFID-based system, called RF-3DScan, for the 3D reconstruction of tagged packages in a warehouse. The system uses a moving antenna to obtain RF signals from the tags, while it extracts phase differences to determine the relative positions of the tags, enabling the determination of package orientation and coarse-grained stacking with 1D scanning. The authors evaluated the prototype system's performance and achieved high accuracy and low error rates. In [16], authors presented a new passive RFID real-time tracking system (PRTS) for tracking RFID-tagged mobile objects on conveyor belts under the conditions of sparse measurements. The system uses a novel sparse signal reconstruction method and leverages simplified particle filters to facilitate real-time tracking. In the article [17], an in-depth analysis is presented on the inclusion of RFID tag antennas and sensors in health monitoring (SHM) applications. The authors highlight the benefits of utilizing RFID antenna sensors and systems in SHM, underscoring their passive characteristics, compact form factor, and versatility in accommodating various modes of operation. Furthermore, the article delves into the existing obstacles and cutting-edge approaches concerning RFID antenna sensors and systems,

TABLE 1. List of abbreviations.

Abbrev.	Meaning
AES	advanced encryption standard
AIS	artificial immune systems
AWGN	additive white Gaussian noise
BP	base pursuit
BPF	bandpass filter
BRF	band-reject filter
BUF	bandwidth utilization factor
CS	compressed censing
DSP	digital signal processing
EMW	electromagnetic waves
HF	high frequency
IFT	inverse Fourier transform
IoT	internet of things
ISDN	integrated services digital network
JRIP	Java-based implementation of the RIPPER
LAN	local area networks
LF	low frequency
NFC	near-field communication
NMSE	normalized mean square error
OMP	orthogonal matching pursuit
PART	partial rule-based trees
PRTS	passive RFID real-time tracking system
RCS	radar cross section
RF	random forest
RFID	radio frequency identification
RIDOR	ripple down rule
RMSE	root mean square error
RSSI	received signal strength indicator
SHM	sensors in health monitoring
SIBA	spectrum injection-based approach
SNR	signal-to-noise ratio
SQLI	SQL injection
SQLIA	SQL injection attacks
UHF	ultra-high frequency
XSS	cross-site scripting

with a focus on sensing capabilities and communication methods from a holistic system standpoint. The study in [18] introduces a novel method for accurately estimating the distance of indoor passive UHF RFID tags. It leverages the correlation between radar cross-section (RCS) and received signal strength indicator (RSSI) ratios to achieve high precision in two stages. To further enhance accuracy, a percentage polynomial curve is employed in the second stage. The suggested approach attains accuracy rates that range from 90.3% to 100%, and exhibits a root mean square error (RMSE) of 0.02. This approach holds potential for application across different technological domains.

While this paper mainly focuses on reconstructing regular data from malware-injected data in RFID systems, it's crucial to acknowledge the importance of safety and security in the overall design and operation of such systems. Ensuring the integrity and confidentiality of data transmitted over RFID networks heavily relies on safety and security measures at the layer. Measures like encryption, authentication protocols, and secure communication channels are vital to mitigate risks and prevent unauthorized access. Although our primary goal in this paper is data optimization and reconstruction techniques, it's worth noting that a comprehensive analysis of safety and security, in RFID systems falls beyond the scope of our research. Future studies could delve deeper into these aspects to provide a holistic understanding of RFID system design and operation.

In this paper, we introduce several contributions to enhance the efficiency and security of RFID systems operating in the UHF band. Firstly, we propose a method for reconstructing regular data in a malware-free RFID system, optimizing spectrum usage, and achieving up to 50% spectrum savings. Secondly, we present a spectrum injection-based approach that leverages a BPF filtering technique to inject missing spectrum and improve data reconstruction accuracy while mitigating the effects of malware injection. Additionally, we propose a noise reduction technique based on bandpass filtering to enhance the signal-to-noise ratio (SNR) and improve data reconstruction accuracy. Through extensive analysis and evaluation, our contributions demonstrate improved reconstruction accuracy, robustness to noise, efficient bandwidth utilization, and suitability for resource-constrained environments. A list of abbreviation is shown in Table 1. Section II provides an introduction to the existing techniques for detecting and preventing malware. Section III explains the fundamental principles of baseband signal reconstruction, which are utilized in the paper, along with the proposed scheme for reconstructing regular data from both malware-free and malware-injected data. In Section IV, the paper presents the simulation and results of the proposed schemes, evaluating their performance in terms of normalized mean square error (NMSE) and time complexity. Additionally, the proposed schemes are analyzed in the presence of additive white Gaussian noise (AWGN), and a noise reduction scheme is investigated. Various performance metrics are employed for evaluation. Finally, Section V concludes the article, summarizing the key findings and contributions of the research.

II. RFID MALWARE DETECTION AND PREVENTION TECHNIQUES

RFID systems are exposed to harmful attacks called malware. It comes in three types: RFID viruses, RFID worms, and RFID exploits [19]. RFID malware causes harm or gains unauthorized access to data. So those systems need to be protected against such attacks. Many research papers explore many techniques to detect and protect RFID systems against malware attacks [20].

Many research papers propose techniques for malware detection and/or protection. In [21], the authors discuss a method for detecting malware in UHF RFID tags with SQL injection virus code in their user memory banks. The study used signal strength data in the frequency domain obtained from a spectrum analyzer while an RFID reader read the tag. The data is then used to train a random forest model for malware detection. Also, in [22], the authors proposed a method for detecting and preventing SQL injection attacks (SQLIA) in RFID systems. The proposed method includes a SQL query matching approach that uses string comparisons and a tag data validation and sanitization technique to provide security against second-order SQLIA. Another approach to protecting RFID systems from malware and ensuring the privacy of tag data is presented in [23]. This framework uses a technique for analyzing individual components of the RFID tag to detect malware-infected tags and sanitize them to remove the malware. An authentication-based protocol is used for privacy protection and identifying rogue readers. In [24], the authors proposed a method for detecting malware in RFID tags operating in low-frequency (LF), high-frequency (HF), and UHF bands. The method involves spectrum monitoring of both normal and malware data in user memory banks and detecting malware based on the measured signals' power.

Tables 2 and 3 provide a comprehensive review of relevant studies focused on techniques utilized for the detection and prevention of malware. The article in [25] examines three main approaches to identifying and combating malware: signature-based detection, behavior-based detection, and specification-based detection. It then focuses on the use of artificial immune systems (AIS) as a lightweight and adaptable technique for preventing malware in IoT networks. The study in [26] provides an analysis of the security measures and techniques employed in a proposed system to secure a smart home access control system by employing RFID cards. The paper acknowledges the use of the advanced encryption standard (AES) algorithm. A robust password policy, Google captcha, and measures to prevent SQL injection (SQLI), cross-site scripting (XSS), and session hijacking in order to thwart unauthorized access and safeguard sensitive data. Additionally, the suggested system utilizes RFID

TABLE 2. Review of relevant studies on techniques for detecting and preventing malware.

Ref., Year	Malware		Used Techniques	Applications	Pros	Cons
	Detect	Prevent				
[25], 2021	✓	✓	- Detection: Signature-based detection technique, behavior-based detection technique, and specification-based detection technique. - Prevention: Artificial Immune Systems (AIS).	Securing IoT Networks.	- Lightweight and adaptive. - Able to detect malware attacks without prior knowledge. - Ideal for detecting unknown malware files. - Inspired by the human immune system. - Effective in dynamic and ever-evolving environments.	- Lack of standardization. - Limited scalability. - Limited accuracy. - Limited robustness. - Limited efficiency. - Limited adaptability. - Limited flexibility.
[26], 2020	×	✓	AES algorithm, strong password policy, google captcha, and prevention of SQLI, XSS, and session hijacking.	Web applications.	- Enhanced security for residents. - Helps increase safety by minimizing theft and accidents. - Facilitates better control and monitoring of movement within a commercial organization. - Utilizes RFID technology. - Protects the privacy of data.	- Invasion of user privacy. - system's ineffectiveness against some cyber-attacks.
[27], 2021	×	✓	Active Jamming, Shielding tag, and Authentication.	Access control, animal identification, inventory control, and smart cards.	- The active jamming technique effectively blocks unauthorized access to RFID tags. - Shielding tags offer an efficient solution to prevent unauthorized reading of RFID tags. - Authentication methods provide a reliable way to prevent unauthorized access to RFID tags.	- Active jamming has the potential to disrupt legitimate RFID communication. - The use of shielding tags can unintentionally hinder legitimate reading of the tags. - Authentication methods are susceptible to security vulnerabilities such as replay attacks.
[28], 2022	✓	×	J48, Random Forest, RIDOR, JRIP, and PART.	Improving the efficiency and security of large RFID networks.	- Identification of previously unidentified attacks. - Flexibility in adapting to evolving attack patterns. - Potential to minimize false positives.	- Necessity for substantial amounts of training data. - Risk of bias in the training data. - Vulnerability to potential manipulation of training data or the system by attackers, enabling evasion of detection.
[21], 2022	×	✓	Random Forest Classifier on signal strength data in the frequency domain.	Supply chain management, medicine, transportation, IoT, localization, and environmental sensing.	- The technique is cost-effective as it uses existing parts in the RFID system. - It can detect malware during the reading stages of the RFID tag, allowing for preventive measures. - The technique achieves a high detection rate of over 80%. - The use of a Random Forest Classifier enhances the accuracy and reliability of the detection process.	- The technique requires a spectrum analyzer, which may not be available in all RFID systems and can add additional costs. - It may not be as effective against new or unknown types of malware, as the detection model might not be trained to identify them.

TABLE 2. *(Continued.)* **Review of relevant studies on techniques for detecting and preventing malware.**

Ref., Year	Malware		Used Techniques	Applications	Pros	Cons
	Detect	Prevent				
[24], 2023	×	✓	Spectrum-based malware detection.	Inventory tracking and management.	- The technique can identify malware in RFID tags that operate at low-frequency (LF), high-frequency (HF), and ultrahigh-frequency (UHF). - It involves monitoring the power of each signal to detect malware, without interfering with the tag's functionality. - The technique can successfully detect malware, even if the specific malware was not previously identified.	- The technique only focuses on detecting malware and does not have the capability to stop it from infecting systems. - It might not be able to effectively detect advanced malware that has the ability to evade detection. - There is a possibility that the technique could produce inaccurate results, either by generating false positives (flagging harmless tags as malware) or false negatives (failing to detect actual malware).
Our Work	✓	✓	- Detection: Any proposed technique used in previous literature. - Prevention: Spectrum injection-based approach (SIBA).	Any real-life application, such as inventory management, supply chain management, IoT, and access control.	- It optimizes the usage of bandwidth, resulting in significant spectrum savings of up to 50%. - This innovative system effectively protects RFID systems from malware-infected data by preventing and reducing their impact. - The system also enhances data reconstruction, enabling faster and more precise results with higher NMSE accuracy in just a few iterations. - The proposed schemes work efficiently in noisy environments. - Flexibility, adaptability, and applicability to diverse RFID systems.	Transmitting small windows requires a high number of iterations to reconstruct the signal, resulting in increased computational complexity in terms of time and memory requirements for the system.

technology for monitoring and controlling access at the main gate. Thereby preventing unauthorized entry. In [27], the aim is to assess the security measures integrated into a suggested system for safeguarding a smart home access control system with the use of RFID cards. The authors delve into the utilization of encryption algorithms, robust password policies, and preventive measures against prevalent web vulnerabilities. In [28], the article delves into the utilization of machine learning algorithms for intrusion detection in network security, with a specific focus on the detection of malware. Techniques such as J48, random forest (RF), ripple down rule (RIDOR), Java-based implementation of the RIPPER (JRIP) algorithm, and partial rule-based trees (PART) are discussed. The paper highlights the necessity for enhanced methods given the incessant evolution of attack methods, the proliferation of connected devices, the difficulties in detecting zero-day attacks, and the inadequacy of existing prevention methods. The paper [21] presents a method for detecting malware in UHF RFID tags by analyzing the signal strength data in the frequency domain using a Random Forest Classifier. By dividing the observed spectrum into 15 ranges and detecting the number of maxima in each range, the malware-infected tags can be detected with an accuracy of over 80%. The authors in [24] proposed a spectrum-based malware detection technique for RFID memory banks in LF, HF, and UHF bands. The technique involves monitoring the power of each signal and identifying the difference between the malware and normal signal data.

TABLE 3. Research problems, contributions, and outcomes of the relevant studies in Table 2.

Ref., Year	Research Problems	Contributions	Outcomes
[25], 2021	- Concerns regarding the security and privacy of RFID systems. - Different types of security threats like replay, disclosure, tracking, offline guessing, denial of service attacks, and more.	- A detailed classification of security and privacy concerns in RFID systems. - Categorization of potential attacks into confidentiality, integrity, and availability. - Classification of various security measures proposed to tackle these attacks. - Discussion of security approaches based on cryptography, privacy, authentication, authorization, and availability. - Identification of challenges and issues related to RFID security. - Insights into future research opportunities in this field.	- Enhanced understanding of the security and privacy challenges in RFID systems. - Comprehensive classification of security and privacy concerns in RFID systems. - Valuable resource for researchers and practitioners involved in this area. - Emphasizing the necessity for further research to address RFID security challenges and issues.
[26], 2020	- Security concerns in a smart home access control system using RFID cards. - Risks of unauthorized access, theft, and accidents in smart homes are addressed. - Web application security issues, such as SQL injection and brute force attacks, are highlighted.	- It proposes using a web application and database to manage access and information. - The paper suggests using RFID cards to control entrance through the main gate and access to individual houses. - It recommends AES encryption, strong passwords, Google captcha, and other security measures for data protection.	- The system takes stringent measures to prevent unauthorized access, significantly reducing the risk of hacking. - It provides top-notch protection for data in smart homes, ensuring optimal security. - The proposed approach employs advanced encryption techniques to secure electronic case data and classified information, making the authentication process simpler and stronger. - The system effectively minimizes vulnerabilities to unauthorized access, enhances safety, prevents thefts and accidents, and ensures the utmost security of sensitive information within smart homes.
[27], 2021	- For years, RFID security has been neglected, resulting in numerous vulnerabilities that can even affect human functionality. - The absence of a robust standard for RFID devices exposes end-users to increased risks.	- The article provides a comprehensive overview of RFID technology. - It examines 23 well-known RFID attacks, including Reverse Engineering, Buffer Overflow, Eavesdropping, and Malware. - The paper proposes security measures and defenses to protect RFID devices, such as Active Jamming, Shielding tags, and Authentication.	- The article seeks to raise awareness about the security vulnerabilities in RFID systems. - It advocates for the development of more secure RFID devices.
[28], 2022	- The constant evolution of attack methods in network security. - The increasing number of connected devices transitioning from interpretation to operation. - The challenge of detecting zero-day attacks with traditional signature-based intrusion detection systems. - Existing prevention and security methods are insufficient in providing comprehensive protection against complex attacks and malware.	- The article presents a framework for intrusion detection systems that utilize machine learning, enabling the use of regularly updated network traffic and reproducible attacks. - It conducts a survey of methodologies and technologies used in intrusion detection systems, covering both signature-based and anomaly-based approaches. - The article reviews various machine learning algorithms utilized in intrusion detection, including J48, Random Forest, RIDOR, JRIP, and PART.	- The proposed framework holds promise in enhancing the efficiency and security of large-scale RFID networks. - The survey and review of intrusion detection system methodologies and technologies provide researchers and practitioners with a better understanding of the strengths and weaknesses of different approaches. - The review of machine learning algorithms used in intrusion detection assists researchers and practitioners in selecting the most suitable algorithm for their specific requirements.
[21], 2022	- Lack of encryption throughout the entire system makes the RFID data vulnerable to unauthorized access. - There are multiple avenues through which malware can be injected into the RFID system, increasing the risk of attacks. - Detecting malware in the RFID system is challenging due to various factors, making it harder to identify and mitigate potential threats.	- The method discussed focuses on detecting UHF RFID tags that are infected with a SQL injection virus code in their user memory banks. - A Random Forest Classifier is applied to analyze the signal strength data in the frequency domain, aiding in the identification of malware in the RFID system. - Feature reduction is achieved by dividing the observed spectrum into 15 ranges, each with a bandwidth of 344 kHz, and counting the number of maxima in each range, effectively simplifying the analysis process.	- The proposed technique utilizes spectrum analysis to detect malware in RFID systems. - By analyzing the frequency ranges, particularly the low bands around 903 MHz, the technique successfully detects malware-infected tags. - The detection rate achieved by this technique is more than 80%, making it effective in identifying and preventing malware attacks on RFID systems.

TABLE 3. ***(Continued.)*** **Research problems, contributions, and outcomes of the relevant studies in Table 2.**

Ref., Year	Research Problems	Contributions	Outcomes
[24], 2023	- The network of RFID technology is at significant risk from malware attacks. - Current methods to prevent malware attacks on RFID technology are cumbersome and may involve updating low-level reader protocol (LLRP) protocol, which can be challenging. - The typical approach of using a blacklist in the database to detect common blocks present in malware code cannot differentiate between regular code and malware.	- The paper suggests a new method for detecting malware in RFID memory banks in different frequency bands. - The technique focuses on monitoring signal power and distinguishing between normal and malicious data. - The paper includes a simulation using MATLAB to show how the proposed technique can detect a SQL injection virus.	- The proposed technique offers a way to detect malware in RFID tags operating at varying frequencies. - It relies on analyzing the power of the signals to detect malware, without interfering with the tags. - The malware causes a decrease in signal power, which can be detected through spectrum analysis. - This technique can identify malware even if its specific characteristics are unknown. - The paper focuses solely on the detection aspect and does not discuss any prevention methods.
Our Work	- Malware attacks on RFID systems. - The need for complex hardware to reconstruct the signals. - The limited spectrum available. - Noise effects on the RFID systems.	- A reconstruction technique is proposed for regular data reconstruction in a malware-free environment. - A spectrum injection-based approach for preventing the malware effect on the reconstructed regular data. - A noise reduction scheme is proposed to reduce the noise effects on the reconstructed signals.	- The proposed method achieves spectrum optimization up to 50%. - The introduced SIBA technique enables signal reconstruction in just a small number of iterations (N=2) instead of 50 iterations, effectively mitigating the impact of malware on regular data. - The proposed noise reduction scheme demonstrates effective performance in handling noise at various signal-to-noise ratios (SNRs).

In our research, we recommend using any existing malware detection technique in the literature but introduce three strategies. The first approach concentrates on optimizing spectrum usage through signal reconstruction. The second approach, known as the spectrum injection-based approach (SIBA), focuses on preventing malware by efficiently reconstructing regular data from malware-infected data, minimizing the computational complexity. Furthermore, we propose merging this technique with a proposed noise reduction method to combat the effects of AWGN. In our research, we can use any existing malware detection technique in the literature but introduce three strategies. The first approach concentrates on optimizing spectrum usage through signal reconstruction. The second approach, known as the SIBA, focuses on preventing malware by efficiently reconstructing regular data from malware-infected data, minimizing the computational complexity. Furthermore, we propose merging this technique with a proposed noise reduction method to combat the effects of AWGN. We summarize the research problems, contributions, and outcomes in Table 3. Furthermore, we provide a detailed explanation and analysis of them in the remainder of the paper.

So, compared to other literature, we have introduced a novel method that overcomes the limitations observed in previous approaches mentioned in Tables 2 and 3. Unlike those methods, our technique offers greater flexibility and does not compromise on accuracy. We achieve this by allowing for adaptable adjustments in the size of the transmitted window and the number of iterations utilized in the algorithms. By fine-tuning these parameters, we can optimize the accuracy of our technique to meet the specific requirements of the RFID system. Moreover, our proposed techniques have the added advantage of being applicable to any RFID system, regardless of its band or bit rate. Unlike other systems that are restricted to certain applications and tailored for specific bands or bit rates, our approach can be implemented across a wide range of RFID systems, making it a more versatile and practical solution. Another crucial aspect of our methods is the flexibility they offer in selecting the appropriate malware detection techniques. We are not limited to a particular technique but have the capability to incorporate any existing malware detection approach from the literature into our framework. This adaptability allows us to leverage the strengths of different techniques and customize them to suit the specific requirements of the RFID system we are working with.

III. BASEBAND SIGNAL TRANSMISSION AND RECONSTRUCTION

A. INTRODUCTION

In the realm of communication systems, the transmission of signals is classified into two primary mechanisms: baseband and bandpass transmission. Baseband signals are directly generated from the source of information and do not undergo modulation or shifting to higher frequencies [29]. They can be analog or digital and are commonly known as low-pass signals, as they possess frequencies that are situated near zero in relation to their highest frequency, which represents their bandwidth. An example of a baseband signal is human speech, which exhibits its most powerful frequency range between 0 and 4 kHz, as illustrated in Fig. 1 [30]. The baseband channel can transmit information at frequencies

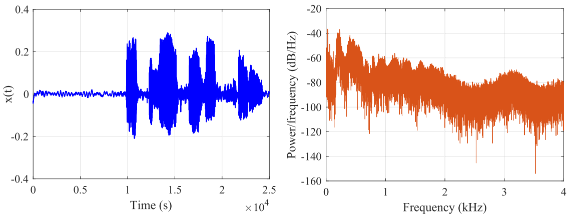


FIGURE 1. An example of a human speech signal (on the left) and its spectrum (on the right).

close to zero and is regularly used in short-range communication networks, including near-field communication (NFC), integrated services digital network (ISDN), industrial control systems, and local area networks (LANs) [31].

To produce a bandpass signal, the baseband signal undergoes modulation with a carrier signal (f_c). This process results in the upward shift of the baseband signal towards higher frequencies and the transmission of a passband signal. In contrast, the bandpass signal is not generated directly from the baseband signal but rather through this modulation process [32]. Passband signals are a type of signal that is preferred for long-distance transmission because they have a higher information-carrying capacity than other signal types. This is due to the use of multiple frequency bands, which allows for a greater amount of information to be transmitted [33].

B. THE BASEBAND TRANSMISSION TECHNIQUE

A proposed technique for transmitting and reconstructing a baseband signal [34], [35] is shown in Fig. 2, which refers to regular data without any malware. The baseband signal, $x_{reg}(t)$, is generated by a signal generator, which is the RFID tag and must have a bandwidth smaller than the channel to prevent distortion during transmission. The technique involves transmitting a window of the spectrum of a time-limited signal instead of the entire spectrum, allowing a selective BPF with starting and ending frequencies of f_s and f_e to choose the window from the spectral information of the signal to be sent over a channel with limited bandwidth. However, this approach results in a distorted signal, $g_{reg}(t)$, since some of the original spectral information and energy are lost due to the windowing process.

Assuming the transmission of regular data without malware, denoted by $x_{reg}(t)$ and representing the binary form of the word "*Orange*" (in HEX=4F72616E6765), a selective BPF is employed at the transmitter. This filter sets a window of the original signal's spectrum $X_{reg}(f)$ to be transmitted, ranging from (20-520) kHz and containing 44.8% of its total average power. Notably, the (0-20) kHz band of $X_{reg}(f)$ comprises 55.2% of the original signal's power. The transmitted signals $g_{reg}(t)$ inevitably undergo distortion due to energy loss from their spectra, as depicted in Fig. 3.

C. THE RECONSTRUCTION ALGORITHM

The manuscript [35] presents an algorithm 1, which outlines a proposed methodology for reconstructing the baseband signal at the receiver. The aim here is to obtain the regular signal $x_{reg}(t)$ through extrapolating the original regular signal's spectrum, utilizing a segment $G_{reg}(f)$ of the main signal's spectrum $X_{reg}(f)$ and prior knowledge of the time extent of the transmitted signal.

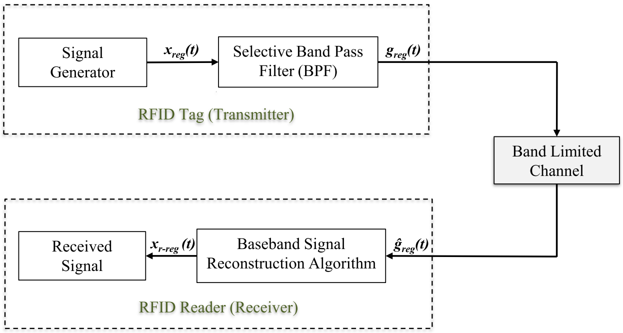


FIGURE 2. The baseband signal reconstruction block diagram.

Algorithm 1 Baseband Signal Reconstruction Algorithm (without noise)

```
Input: $\hat{G}_{reg}(f)$, $f_s$ and $f_e$
Output: $x_{r-reg}(t)$
Calculate $\hat{g}_{reg}(t)$ by performing the IFT of $\hat{G}_{reg}(f)$
for ($i$=$1$ to $N$) do
    Multiply $\hat{g}_{reg}(t)$ and $p(t)$ to get $s(t)$
    Compute $S(f)$ by performing the FT of $s(t)$
    Apply $S(f)$ to BRF with $f_s$ and $f_e$ to get $C(f)$
    Add $C(f)$ to $\hat{G}_{reg}(f)$ to get $X_{reg,1}(f)$
end
Calculate IFT of $X_{reg,N}(f)$ to get $x_{r-reg}(t)$
End
```

The process of reconstructing the baseband signal comprises several steps. First, the inverse Fourier transform (IFT) is performed on the received signal's spectrum $\hat{G}_{reg}(f)$, which results in a non-time-limited signal $\hat{g}_{reg}(t)$. Subsequently, a gate ($rect$) function $p(t)$ is applied to $\hat{g}_{reg}(t)$, with the same time extent as the original signal $x_{reg}(t)$, to produce $s(t)$. An FT is then applied to $s(t)$ to obtain a non-bandlimited signal $S(f)$, which is filtered using a band-reject filter (BRF) with starting and ending frequencies equal to those of the transmitter (f_s and f_e), yielding the filtered function $C(f)$. Next, the known spectrum $C(f)$ of the received signal is inserted into the dead space of the received signal's spectrum $\hat{G}_{reg}(f)$, resulting in an initial estimate of the reconstructed signal's spectrum $X_{reg,1}(f)$ (for 1-iteration). The IFT of $X_{reg,1}(f)$ is calculated, and the loop is repeated for N iterations until the desired shape of the spectrum is achieved. Finally, the IFT of $X_{reg,N}(f)$ is calculated to obtain the reconstructed signal $x_{r-reg}(t)$ after N-iterations.

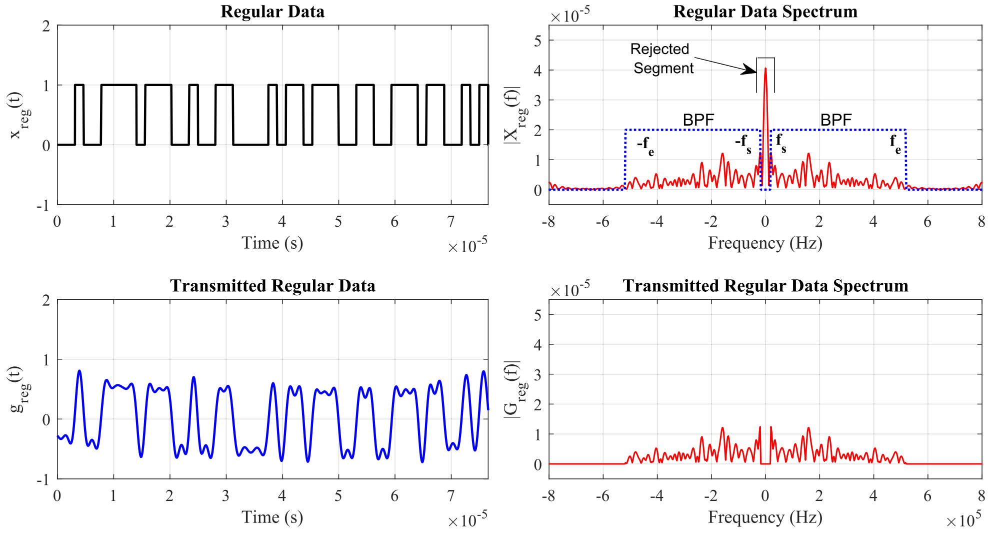


FIGURE 3. The generated $x_{reg}(t)$ and transmitted $g_{reg}(t)$ signals (on the left) and their corresponding spectra $X_{reg}(f)$ and $G_{reg}(f)$, respectively (on the right) with f_s= 20 kHz and f_e= 520 kHz.

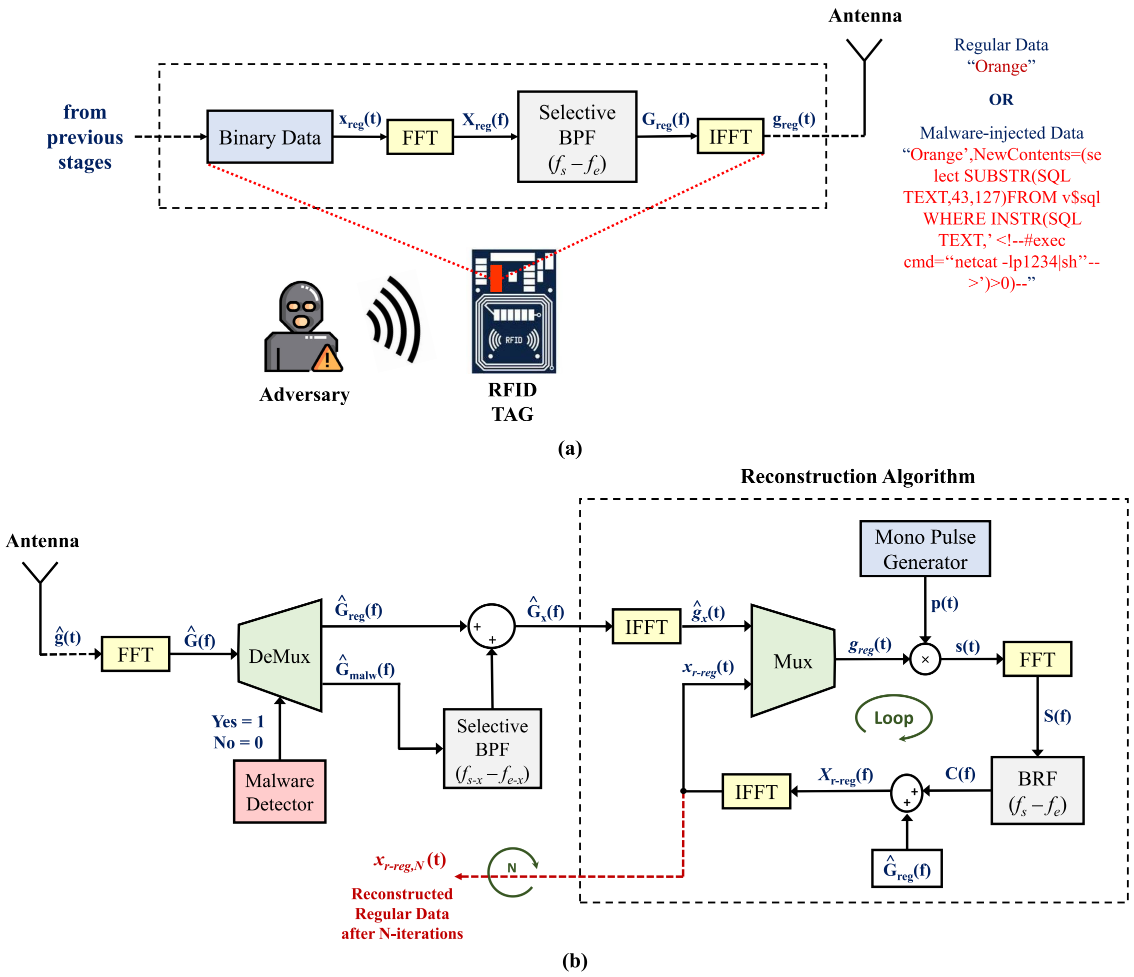


FIGURE 4. The proposed system's block diagram. (a) The transmission concept in the RFID Tag (b) The reconstruction algorithm in the RFID reader.

TABLE 4. Features of the computer used for the simulation.

Parameter	Specifications
System Manufacturer and Model	Micro-Star International Co., Ltd. MSI, raider GE76 12UE
Processor	12th Gen Intel(R) Core (TM) i9-12900H, 2900 MHz, 14 Core(s), 20 Logical Processor(s)
Memory	16 GB
Storage	SSD 1 TB
Operating System	Microsoft Windows 11 Home Edition
Matlab Version	R2022b, Update 4(9.13.0.2166757)

IV. RESULTS AND DISCUSSIONS

The computer hardware utilized to simulate the proposed scheme for routinely reconstructing data by injecting a portion of malware's spectrum is detailed in Table 4. These hardware specifications played a significant role in determining the simulation time and results.

A. PERFORMANCE METRICS

The evaluation of the reconstruction status' performance will rely on the NMSE, a prevalent performance metric for such systems. This measure provides insight into the degree of similarity between the reconstructed signal, represented as $x_{r-reg}(t)$, and the original signal generated by the tag, represented as $x_{reg}(t)$. The NMSE is defined in the work of Ghannouchi et al. [36] and is widely adopted in signal processing research. It is calculated as the ratio of the mean square error between the two signals to the mean square value of the original signal. The NMSE is defined as:

$$NMSE = \frac{\sum_{t=1}^{L} \left|x_{reg}(t) - x_{r-reg}(t)\right|^2}{\sum_{t=1}^{L} |x_{reg}(t)|^2} \tag{1}$$

where L is the signal's length (in samples). A lower NMSE value indicates a higher degree of similarity between the transmitted and reconstructed signals, resulting in improved performance. This suggests that the reconstruction process is more accurate and efficient.

B. THE PROPOSED TECHNIQUE FOR REGULAR DATA RECONSTRUCTION

1) SYSTEM'S BLOCK DIAGRAM

The proposed system's block diagram is presented in Fig. 4, which aims to reconstruct the regular data spectrum using the spectrum of malware-injected data. The RFID tag transmission concept is shown in Fig. 4(a), which is similar to the transmitter concept presented in Fig. 2. The generated binary data of the tag is denoted by $x_{reg}(t)$, which passes through the FFT block and the selective BPF to select the window with starting and ending frequencies f_s and f_e, respectively, to obtain $\hat{G}reg(f)$. The output signal of the BPF is fed to the IFFT block to generate the baseband signal $g_{reg}(t)$, which is then transmitted through the antenna. It is assumed that the system operates on the baseband concept. In Fig. 4(b), we illustrate our proposed receiver in the RFID reader, which operates under two reception scenarios: receiving without any malware and receiving with malware-injected data. Our assumption is that the reader initially received a malware-free signal that was later infected by malware. The received signal $\hat{g}_(t)$ is processed by the FFT block, resulting in $\hat{G}_(f)$. We use a malware detection technique, as explained in Section II, to determine if the received data is free of malware or not. If the data is malware-free, the malware detector block outputs (0) to the selector control line of the demultiplexer (DeMux) block, and the signal is passed to the first line to become $\hat{G}_{reg}(f)$, leading to the first scenario in our assumptions. If the data is infected with malware, the malware detector block outputs (1), and the signal is passed to the second line to become $\hat{G}_{malw}(f)$, leading to the second scenario.

In the first scenario, the malware-free signal spectrum $\hat{G}_{reg}(f)$ is processed by the adder block, which adds zero $(\hat{G}_{malw}(f))$ from the malware-injected path. The result is then processed by the reconstruction algorithm proposed in [34], allowing for the regular data to be reconstructed after N-iterations $x_{reg,N}(t)$. In the second scenario, where the data is identified as malware-infected $\hat{G}_{malw}(f)$, it is processed by a selective BPF with starting and ending frequencies of f_{s-x} and f_{e-x} respectively. The BPF only allows the missing spectrum portion of the regular data to pass through, which is then injected into the missing part of the regular data spectrum $\hat{G}_{reg}(f)$ via the adder block. The resulting spectrum $\hat{G}_x(f)$ is then processed by the reconstruction algorithm, allowing for the regular data to be reconstructed again after a smaller number of iterations (N) to get the original regular data $x_{reg,N}(t)$.

C. RECONSTRUCTING DATA FROM A MALWARE-FREE RFID TAG

Figure 6 displays the NMSE performance of the reconstructed regular data without malware versus the number of iterations (N) for 5 different transmitted window spectra ranges, with a fixed bandwidth of 500 kHz with a data rate of 640 kbps. Table 5 shows the corresponding performance metrics of Fig. 6. The table includes different transmitted window ranges represented by (f_s and f_e) and evaluates accuracy using the NMSE. The average power contained in each window is also shown. The performance is measured for different iterations, ranging from 5 to 2000. As shown in Fig. 6, the first window (10–510) kHz, which represents 48.5% of the total regular signal's power, can achieve a very good NMSE value of 0.0487 after only 50 iterations and maintain this value thereafter.

For the second window (20-520) kHz, it represents around $\approx$ 45% of its total average power. It achieves an acceptable NMSE value of 0.0622 after 1000 iterations, resulting in a good reconstruction status, but it can achieve almost the same NMSE as the first window (0.0478) after 2000 iterations. The corresponding reconstructed signals compared to the original regular transmitted data and

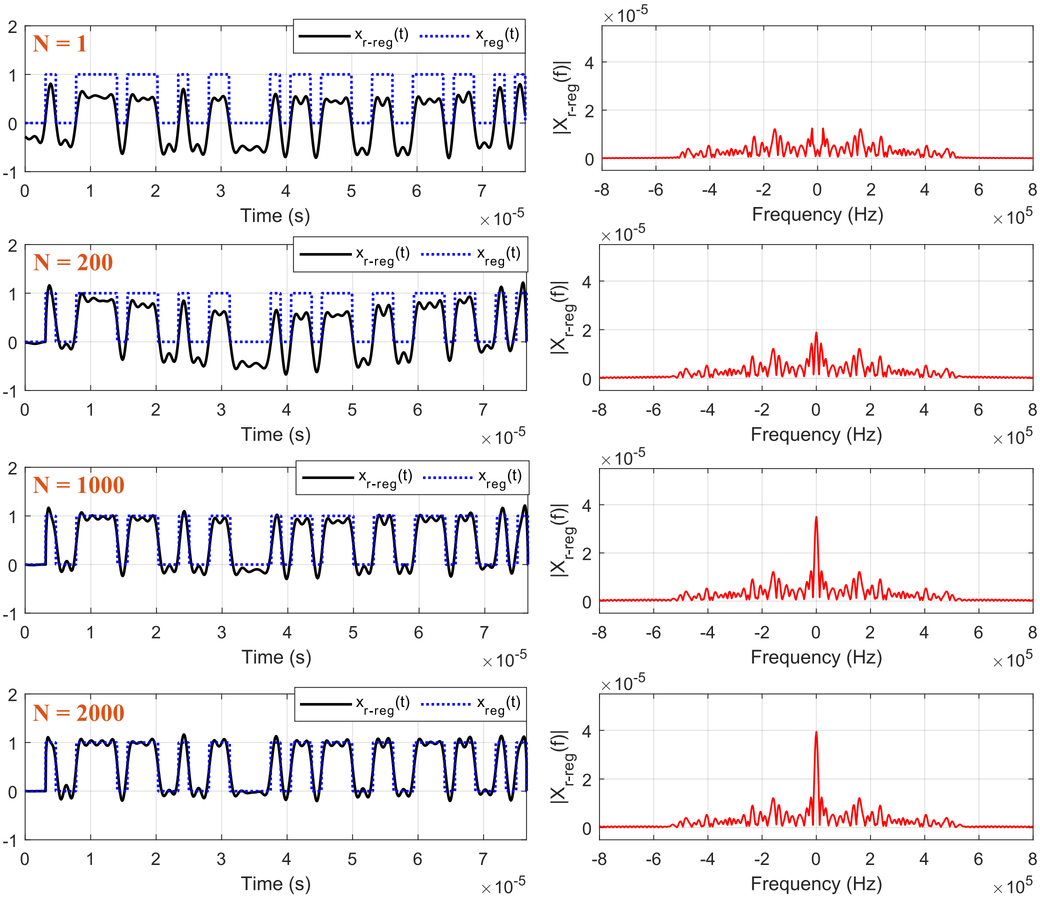


FIGURE 5. Reconstructed malware-free regular data $x_{reg}(t)$ (on the left) and their spectra $|X_{reg}(f)|$ (on the right) for different iterations with a transmitted window (20-520 kHz).

TABLE 5. Performance metrics of reconstructed regular data without malware using a fixed window bandwidth (500 kHz) for different iterations: NMSE and Average Power.

Δf (kHz)		P (%)	NMSE						
f_s	f_e		N=5	N=50	N=100	N=200	N=500	N=1000	N=2000
10	510	48.5	0.2334	**0.0487**	0.0479	0.0472	0.0468	0.0467	**0.0466**
20	520	44.8	0.4499	0.3863	0.3309	0.2472	0.1204	0.0622	**0.0478**
30	530	40.6	0.5412	0.3977	0.3731	0.3668	0.3623	0.3559	0.3446
40	540	38.1	0.5656	0.5040	0.4935	0.4777	0.4424	0.4021	0.3593
50	550	37.7	0.6016	0.5632	0.5347	0.4993	0.4622	0.4515	0.4471

their spectra are shown in Fig. 5. The first two subfigures (N = 1 and 200) show a bad reconstructed regular data status, as their NMSE is around 0.4. However, when increasing N to 1000 iterations or more, the reconstructed signals are more accurate and of high performance. For the remaining transmitted windows, their average power ranges from 37.7% to 40.6%, which is lower than the previous windows. However, their corresponding NMSE values are high (around ≈ 0.4) after 2000 iterations, and they cannot reach the acceptable range of 0.06. Therefore, the signal cannot be fully reconstructed until a very high number of iterations is reached, such as 10,000 or more.

The time consumption of the proposed scheme to reconstruct the regular malware-free data $x_{reg}(t)$ for the same transmitted windows as shown in Fig. 5 in the receiver is presented in Fig. 7. It is observed that all windows have almost similar reconstruction times, except for the last window (50-550 kHz), which takes longer to reconstruct than the other three windows after 1000 iterations. Additionally, the window (40-540 kHz) exhibits higher time consumption

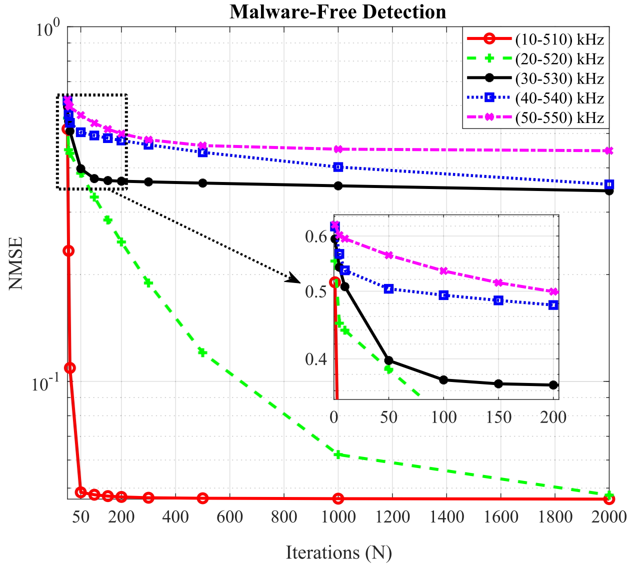


FIGURE 6. NMSE of reconstructed regular data without malware with W= 500 kHz and R_b = 640 kbps.

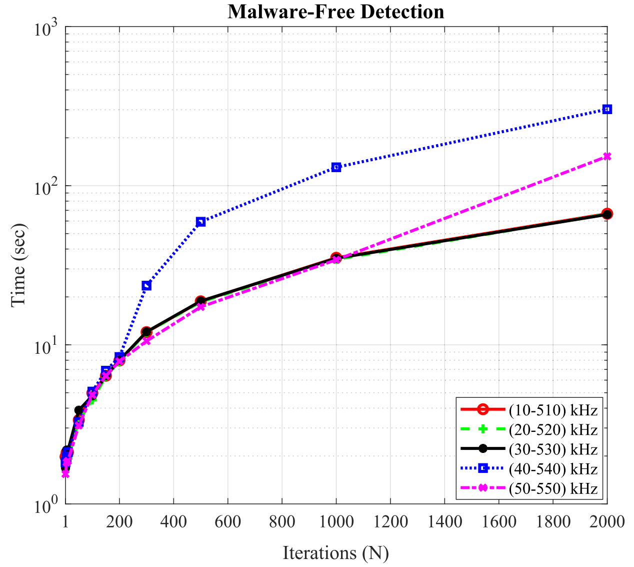


FIGURE 7. Time consumption for reconstructing the regular data without malware with W = 500 kHz and R_b = 640 kbps.

compared to the others after 200 iterations. It appears that the reconstruction time does not follow a specific criterion based on the transmitted window. Consequently, when sending more than 45% of the total signal's average power and running the algorithm for a certain number of iterations, around 50% of the used spectrum can be saved for reconstructing the regular data. However, reconstructing low average power signals requires a high number of iterations, which leads to a more complex system and a longer reconstruction time.

D. RECONSTRUCTION OF REGULAR DATA USING MALWARE-INJECTED SIGNALS

The proposed scheme outlines the procedure for regular data reconstruction and the injection of malware-infected data.

TABLE 6. NMSE of reconstructed regular data with malware injection using fixed window bandwidth (500 kHz) for various iterations.

Δf (kHz)		NMSE				
f_s	f_e	N=1	N=2	N=3	N=4	N=5
10	510	1.2467	0.0514	0.0484	0.0481	0.0480
20	520	1.2558	0.0535	0.0494	0.0487	0.0483
30	530	1.2647	0.0533	0.0506	0.0493	0.0484
40	540	1.2700	0.0508	0.0479	0.0470	0.0466
50	550	1.2808	0.0501	0.0472	0.0467	0.0465

This process is illustrated in Fig. 4, while Fig. 8 showcases the signal reconstruction and injection stages. The proposed approach, based on spectrum injection, involves combining the received regular data spectrum $G_{reg}(f)$ within the frequency range (f_s and f_e) with the bandpass-filtered malware-injected spectrum $G_{malw}(f)$. By utilizing the complementary band of $G_{reg}(f)$, the empty spectrum space is filled, resulting in the formation of the signal $\hat{G}_x(f)$. The spectrum $G_{malw}(f)$ exhibits a similar shape to the original regular data spectrum $G_{reg}(f)$, as observed in the top-left subfigures of Fig. 8. The newly formed spectrum $\hat{G}x(f)$ closely resembles the original transmitted regular data spectrum $Xreg(f)$. As a result, when applying the new signal $\hat{G}x(f)$ to the baseband signal reconstruction algorithm, a reduced number of iterations are required to reconstruct $xreg - r, N(t)$, as shown in the bottom-left subfigure of Fig. 8.

Figure 9 displays the NMSE of the reconstructed regular data obtained using the spectrum injection approach for the same transmitted windows depicted in Fig. 6, considering N=1 to 30 iterations. Table 6 presents the recorded NMSE values for N=1 to 5 iterations. Both the figure and table indicate that the NMSE achieves high performance, approximately 0.05, after only two iterations for all transmitted windows. This signifies that leveraging the malware-infected data enables speedy and accurate reconstruction of the original regular data, surpassing the reconstruction speed of the regular malware-free RFID system (which requires 50 iterations) by a factor of 25.

The reconstructed regular data after malware-infected data injection for different windows after two iterations is shown in Fig. 10. It is seen that the data is perfectly restored and has achieved a very high reconstruction status compared to the previously discussed conventional reconstruction method in section IV-C.

E. EFFECTS OF NOISE ON THE PROPOSED SCHEME

1) INTRODUCTION

In this section, we will examine the impact of AWGN on the regular signal being transmitted and evaluate the performance of the proposed algorithm for noise reduction. Our objective is to illustrate that the underlying challenge of the proposed algorithm lies in the inherent difficulty of the extrapolation problem. One key factor to highlight is

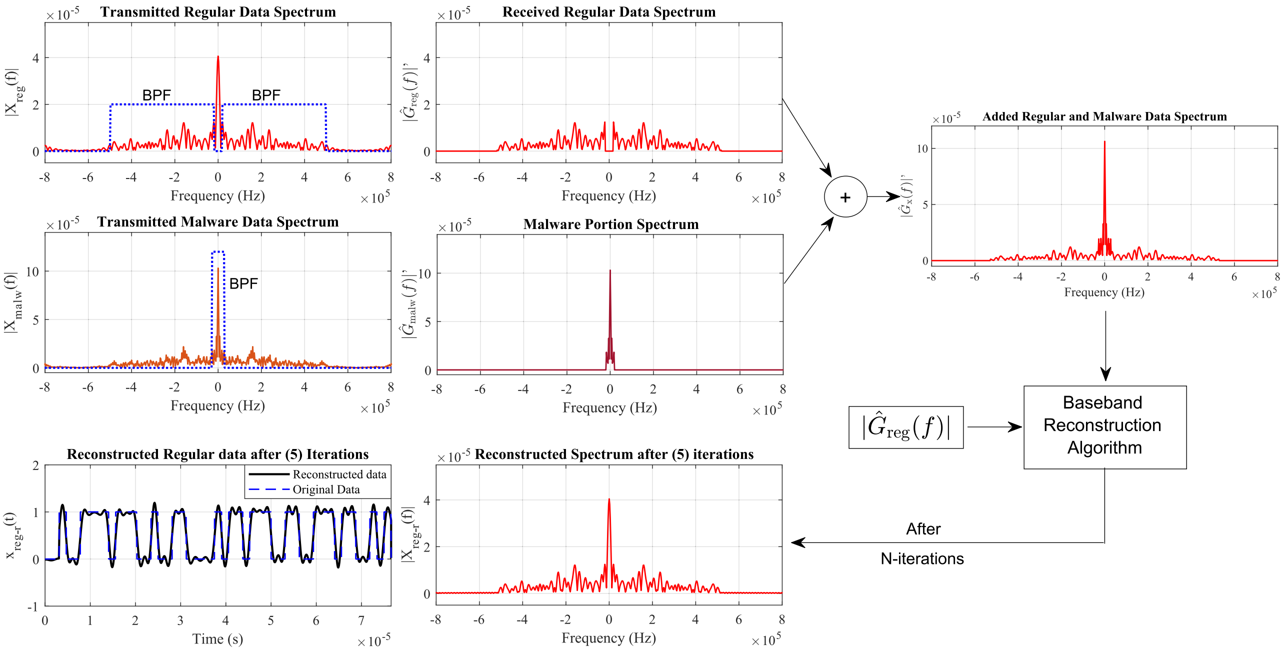

Transmitted Regular Data Spectrum
|X_reg(f)|
BPF
BPF
Frequency (Hz)
×10^5
×10^-5
Received Regular Data Spectrum
|Ĝ_reg(f)|'
Transmitted Malware Data Spectrum
|X_malw(f)|
BPF
Malware Portion Spectrum
|Ĝ_malw(f)|'
+
Added Regular and Malware Data Spectrum
|Ĝ_x(f)|'
|Ĝ_reg(f)|
Baseband Reconstruction Algorithm
After
N-iterations
Reconstructed Regular data after (5) Iterations
Reconstructed data
Original Data
x_reg-r(t)
Time (s)
Reconstructed Spectrum after (5) iterations
|X_reg-r(f)|

FIGURE 8. Signal stages of malware-infected data spectrum injection into the regular data spectrum.

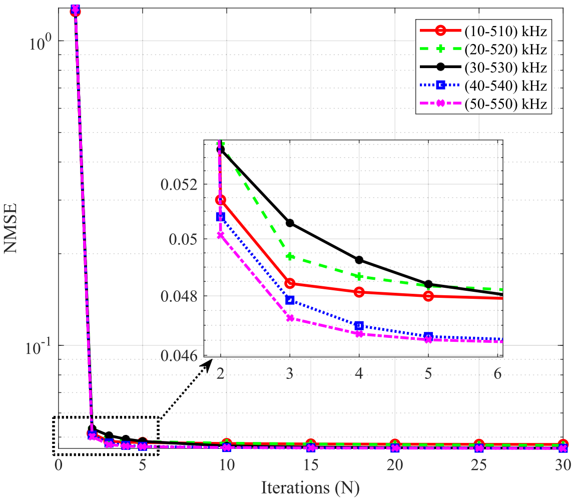


FIGURE 9. NMSE of reconstructed regular data with malware-infected data injection.

the difficulty in extrapolation due to the lack of a definitive maximum threshold for restoration noise. This is expected, as the uncertainty in restoration is likely to increase as we move away from the known portion of the signal spectrum. Specifically, the uncertainty in restoration, given knowledge of a signal spectrum that only extends to a length of W Hz, will be significantly higher at a distance that is, for example, 10^{10} times greater than W Hz. However, we can still anticipate favorable outcomes in the vicinity of the known signal spectrum, as evidenced by the examples provided in the study.

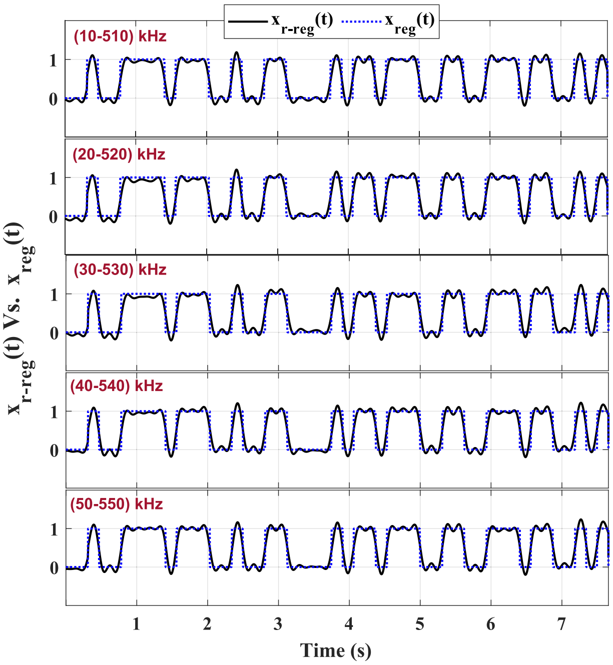


FIGURE 10. Reconstructed regular signals after injection of malware-infected data for different windows and 2-iterations.

2) IMPACT OF PARAMETER VARIATION ON RECONSTRUCTED SIGNALS

In Fig. 11, we observe the impact of various states on the reconstructed signal $x_{r-reg}(t)$ of the regular data stream (640 kbps) in the presence of AWGN. The reconstructed signal is represented by different colors, while the transmitted signal $x_{reg}(t)$ is depicted in black. Each column in the figure corresponds to a specific parameter change, namely the transmitted window bandwidth (W), the number of iterations (N), and the SNR while keeping the other two parameters constant. The associated average power and NMSE for each state are recorded in Table 7.

Specifically, Fig. 11(a) demonstrates the effect of increasing the transmitted window bandwidth from 200 kHz to 500 kHz while maintaining N and SNR at constant values. The subfigures indicate a decrease in NMSE from 0.2156 to 0.0997 by increasing the transmitted window bandwidth. Additionally, there is an increase in the average power of the signals from approximately 80% to approximately 95%. This suggests that the algorithm converges effectively, with the NMSE improvement primarily dependent on the transmitted window bandwidth rather than the average power of the transmitted signal. The reason behind this outcome is that the noise is distributed across the signal's frequency band. Consequently, increasing the transmitted signal's bandwidth reduces the impact of noise.

Figure 11(b) illustrates the effect of increasing the number of iterations from 2 to 10, while keeping the transmitted window bandwidth and SNR constant, with an average transmitted power of approximately 95%. It is evident that the NMSE increases, resulting in algorithm divergence. This occurs due to the addition of the received spectrum with noise $\hat{G}_{reg-n}(f)$ in each iteration, as depicted in step 6 of Algorithm 1.

Figure 11(c) illustrates the impact of increasing the SNR from 15 dB to 30 dB, while keeping the transmitted window bandwidth (W) and the number of iterations (N) constant. Notably, as the SNR increases, the NMSE decreases, leading to algorithm convergence. This indicates that a higher SNR helps overcome the effects of noise. Hence, we observe that the proposed reconstruction algorithm effectively operates by selecting an appropriate bandwidth for the transmitting window, optimizing the number of iterations, and adjusting the SNR at the receiver. Through these mechanisms, we can effectively handle the presence of noise, ensuring successful extrapolation and reconstruction.

3) A PROPOSED APPROACH FOR NOISE REDUCTION

As observed in the previous section, the inclusion of AWGN in the signal causes a notable decline in the effectiveness of the reconstruction algorithm. This leads to a gradual increase in the amount of noise present in the recovered signal with each successive iteration. To overcome this challenge, a solution is proposed in this study to mitigate the adverse effects of noise. Fig. 12 illustrates the block diagram that demonstrates the proposed technique for noise reduction, and Fig. 13 displays the corresponding signals. The proposed technique encompasses the following sequential steps:

Step (1): Calculating the FT of the received signal with noise $\hat{g}_n(t)$ to obtain the spectrum $\hat{G}_n(f)$ as shown in Fig. 13 a and b, which is unknown as to whether it corresponds to regular data or malware-injected data, but needs to be noise filtered first and assumed for simplicity to be the regular data without any malware.

TABLE 7. Impact of parameter variations on the NMSE of reconstructed regular data under AWGN noise.

Variable W (N= 5, SNR= 20 dB)		Variable N (W= 0-500 kHz, SNR= 20 dB)		Variable SNR (N= 5, W= 0-500 kHz)	
P%	**NMSE**	**N**	**NMSE**	**SNR**	**NMSE**
W= 0-200 kHz		**2**	0.0639	**15 dB**	0.2119
80.14	0.2156				
W= 0-300 kHz		**5**	0.1002	**20 dB**	0.1005
88.58	0.1447				
W= 0-400 kHz		**8**	0.1679	**25 dB**	0.0648
91.93	0.1229				
W= 0-500 kHz		**10**	0.2293	**30 dB**	0.0541
94.82	0.0997				

Step (2): The next step involves utilizing $\hat{G}_n(f)$ on a NRF that consists of a BPF. The BPF should have the same starting and ending frequency ranges as the transmitter and receiver, denoted as (f_s,f_e). The purpose of this step is to eliminate all noise in the signal spectrum in regions A, B, and C while maintaining the remaining spectrum as it is. This results in a spectrum, namely $\hat{G}_{filtered}(f)$, which contains less noise and exhibits zero noise in the pre-mentioned regions, as illustrated in Fig. 13d. In comparison, the original signal's spectrum, denoted as $\hat{G}_{free}(f)$, represents the noise-free regular signal's spectrum.

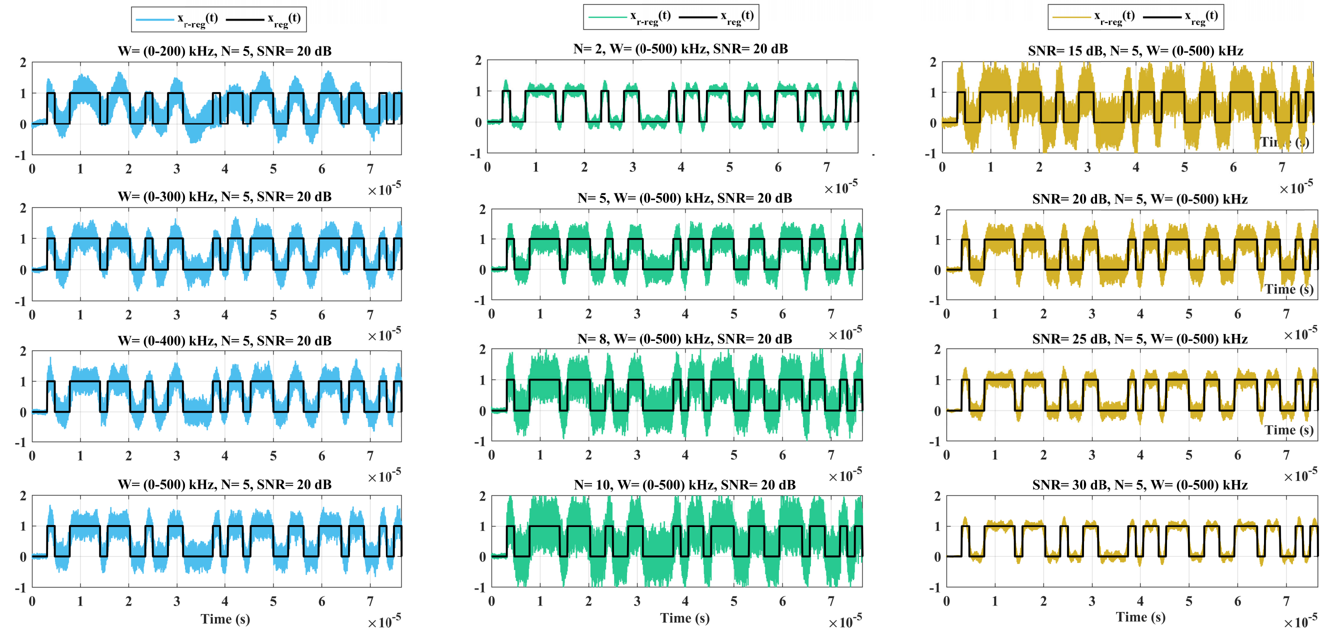
Steps (3 and 4): This stage involves the same malware detection, injection, and reconstruction process described in Section IV-(B, C, and D), resulting in the reconstructed regular data signal $x_{r-reg,filtered}(t)$ after N iterations, as shown in Fig. 13b. This signal is compared to the reconstructed regular data $x_{r-reg,free}(t)$ in a noise-free environment, and they appear to be highly similar, indicating a reduction in noise.

A comparison is shown in Fig. 14 of the NMSE for the reconstructed regular data without noise and with noise when the noise reduction scheme is implemented at different SNR values. This comparison is conducted with a transmitted window band of (20-520) kHz and up to 3000 iterations. The figure illustrates the effectiveness of the proposed noise reduction scheme when applied to a received signal that is corrupted by noise. It can be observed that the proposed scheme performs remarkably well, exhibiting a high level of accuracy in reconstructing the original signal even in scenarios with low SNR. Impressively, the achieved NMSE closely approximates the NMSE obtained when no noise is present.

F. DEMONSTRATION OF NOISE REDUCTION IN VARIOUS UHF BANDS

1) INTRODUCTION

In this section, we will evaluate how well the noise reduction technique works in reducing noise effects across different



(a) Different window bandwidth (W).

(b) Different number of iterations (N).

(c) Different SNR.

FIGURE 11. Reconstructed 640 kbps regular data with the presence of AWGN using different parameter values.

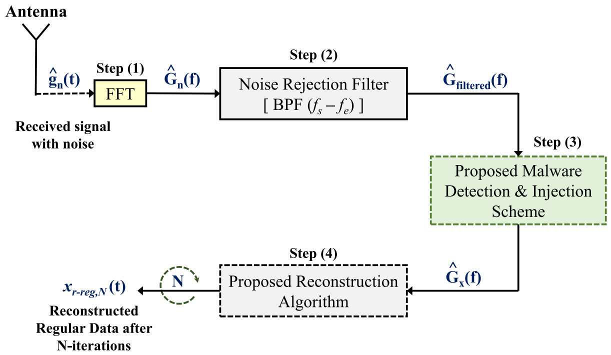


FIGURE 12. Block diagram of the proposed noise reduction technique.

UHF bands and how it can be applied to different data rates in UHF RFID systems. According to the ISO 18000 Part 6C standard [37], [38], FM0 supports discrete data rates such as 160, 256, 320, and 640 kbps. We will conduct a thorough assessment of the proposed technique by examining its impact on reconstruction accuracy, its ability to handle noise, its utilization of bandwidth, its average power consumption, its computational complexity, its processing time, and its memory usage. By considering all of these factors together, we will gain valuable insights into how effective and practical the noise reduction technique is in real-world UHF RFID scenarios across various UHF bands and data rates.

2) PERFORMANCE EVALUATION

a: RECONSTRUCTION ACCURACY

To evaluate the efficiency of the suggested noise reduction technique, we implemented it at different data rates (160, 256, 320, and 640 kbps). We then analyzed and plotted the NMSE for various transmitted windows (W_1, W_2, W_3, and W_4) as shown in Fig. 15. These windows represent different percentages (70%, 80%, 90%, and 100%) of their respective main lobe bandwidths. Additionally, we ensured a fixed SNR of 5 dB throughout the analysis. The corresponding received signals with noise $\hat{g}_{reg-n}(t)$ and their reconstructed regular data $x_{r-reg}(t)$ compared with the original transmitted regular data without malware $x_{reg}(t)$ are shown in Fig. 16.

For all data rates shown in the subfigures of Fig. 15, we can see that the NMSE is decreased by increasing N until it reaches a constant value at 50 iterations. When the window W_1 is transmitted in the AWGN noisy channel, the NMSE of all rates is around 0.062 at 50 iterations, which is an acceptable value, as shown in Fig. 16(a), which shows the reconstruction signals for a 160 kbps data rate. The second window W_2 achieves an NMSE of 0.047 for all rates too at 50 iterations, and its corresponding reconstructed signal for 256 kbps rate is shown in 16(b), which is also acceptable for digital signals. Also, for the third and fourth transmitted windows W_3 and W_4, the NMSE curves are almost the same and achieve a 0.045 NMSE value at 50 iterations, where their corresponding reconstructed signals for 320 kbps and 640 kbps are shown in Fig. 16(a and b). So, we can see that for transmitted windows ranging from 70% to 100% of the total main lobe bandwidth, we can reconstruct the transmitted signal well.

By observing the NMSE plots for different data rates displayed in the subfigures of Fig. 15, it is evident that increasing N leads to a decrease in NMSE until it levels off at 50 iterations. When the window W_1 is sent through an AWGN noisy channel, the NMSE for all rates remains around 0.062 at 50 iterations, which is deemed acceptable. This can be seen

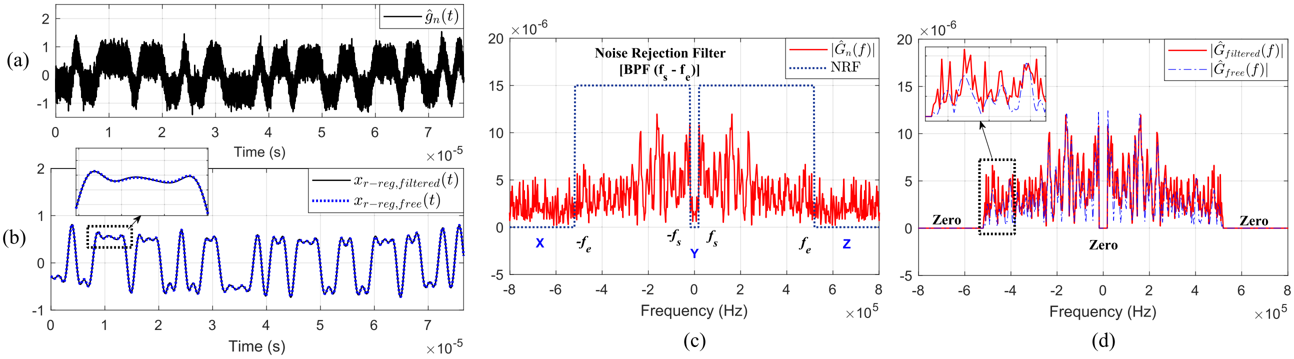


FIGURE 13. Signals associated with the proposed scheme for noise reduction (a) Received signal with noise. (b) Reconstructed signals without noise and with noise reduction. (c) Received signal spectrum. (d) Spectra of reconstructed signals without noise and with noise reduction.

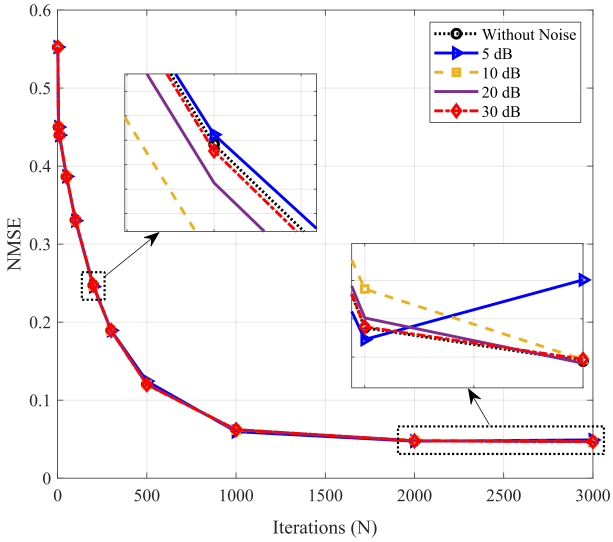


FIGURE 14. Comparing NMSE for the Reconstructed 640 kbps regular data with a transmitted window of (20-520) kHz, with and without AWGN at various SNRs.

in Fig. 16a, showcasing the reconstructed signals for a data rate of 160 kbps. Similarly, the second window W_2 attains an NMSE of 0.047 across all rates after 50 iterations, with its corresponding reconstructed signal for a rate of 256 kbps depicted in 16b in an acceptable manner for digital signals. Furthermore, for the third and fourth transmitted windows, W_3 and W_4, the NMSE curves maintain a nearly identical pattern and achieve an NMSE value of 0.045 at 50 iterations. The reconstructed signals for rates of 320 kbps and 640 kbps are illustrated in Fig. 16(c) and (d) respectively. Thus, it is clear that we can effectively reconstruct the transmitted regular data when the transmitted windows span from 70% to 100%.

b: ROBUSTNESS TO NOISE

In real-life situations, RFID systems are commonly utilized in environments with random noise levels. The deterioration of signals can adversely impact the effectiveness of data restoration techniques. Hence, it is crucial to evaluate the performance of the proposed noise reduction method and determine its efficacy in mitigating the influence of channels. So, in this section, we will examine how the proposed noise reduction technique fares when subjected to varying SNR conditions. Our objective is to assess the accuracy of reconstructing data and compare it to the reconstruction achieved in noise-free channels. By studying the behavior of the proposed technique across different SNR values, we can gain valuable insights into its noise reduction capabilities and ascertain its suitability for practical RFID applications operating in demanding and noisy environments.

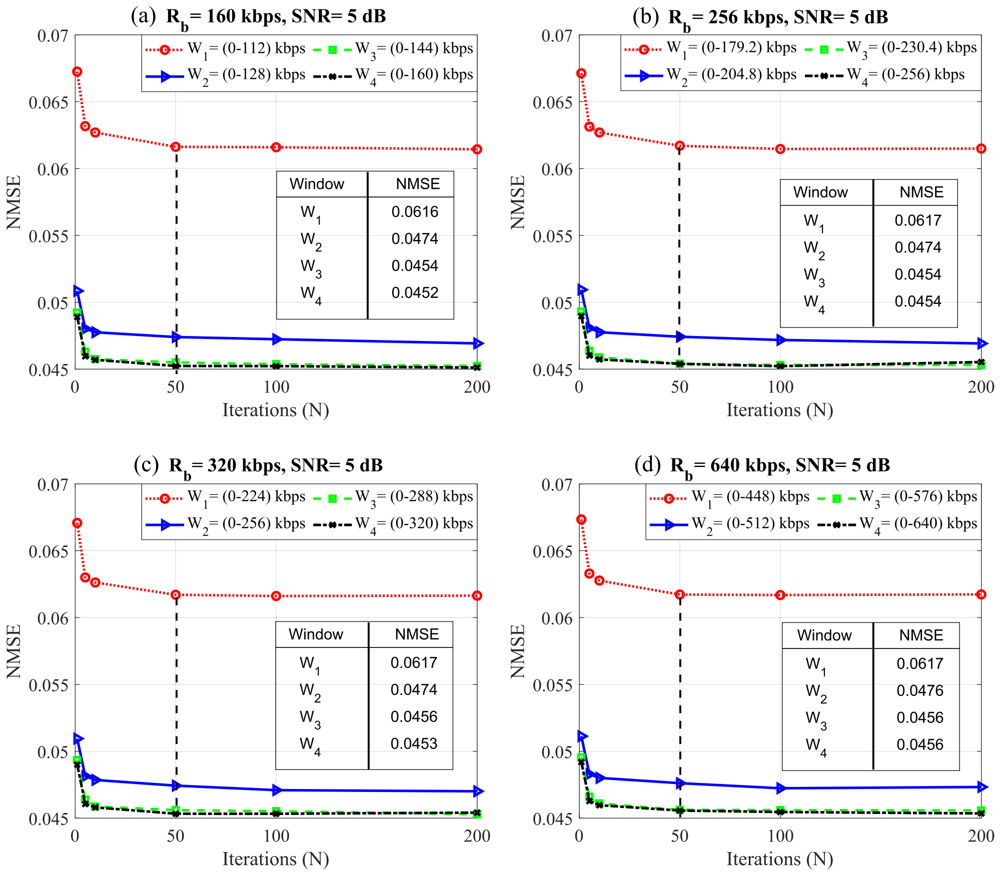
Figure 17 illustrates the NMSE of various reconstructed regular data in both noisy and noiseless channels. The comparison is made at different data rates, transmitted window sizes, and SNRs. The transmitted window sizes, denoted as W_A, W_B, W_C, and W_D, correspond to percentages (70%, 80%, 90%, and 100%) of the total main lobe bandwidth of their corresponding signals with data rates of 160, 256, 320, and 640 kbps, respectively. The figure illustrates that irrespective of the data rate, the size of the transmitted window, or the SNR, the proposed technique for noise reduction yields an NMSE that closely aligns with the corresponding NSME curve in the absence of noise in the channels. This indicates that the proposed technique is highly effective in terms of its ability to withstand noise and provide efficient results.

c: BANDWIDTH UTILIZATION AND AVERAGE POWER

Table 8 presents an overview of the bandwidth utilization factor (BUF) and average power of the noise-rejected reconstructed regular data at SNR of 5dB for different data rates and varying transmitted window bandwidths. The BUF evaluates how effectively the signal reconstruction algorithm uses the available bandwidth by comparing the bandwidth needed for signal transmission and reconstruction to the total accessible bandwidth. A higher BUF suggests better utilization of the available resources. The average power represents the average power within each transmitted spectrum portion. The BUF can be calculated using the following formula:

$$BUF = \frac{\text{Transmitted Window Bandwidth } (W)}{\text{Total Available Bandwidth}} * 100\% \tag{2}$$

where the total available bandwidth is the UHF bandwidth (860-930) MHz.



(a)

Window	NMSE
W_1	0.0616
W_2	0.0474
W_3	0.0454
W_4	0.0452

(b)

Window	NMSE
W_1	0.0617
W_2	0.0474
W_3	0.0454
W_4	0.0454

(c)

Window	NMSE
W_1	0.0617
W_2	0.0474
W_3	0.0456
W_4	0.0453

(d)

Window	NMSE
W_1	0.0617
W_2	0.0476
W_3	0.0456
W_4	0.0456

FIGURE 15. Comparison of NMSE for various transmitted window bandwidths at different UHF data rates and 5dB SNR (a) $R_b = 160$ kbps. (b) $R_b = 256$ kbps. (c) $R_b = 320$ kbps. (d) $R_b = 640$ kbps.

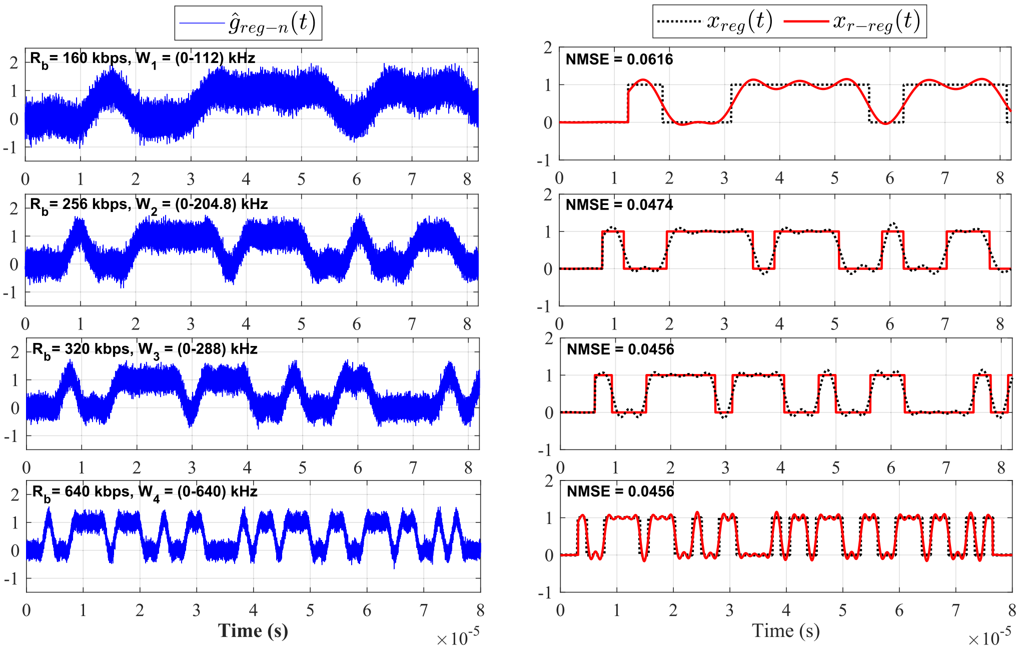


FIGURE 16. Received regular signals with noise (on the left) and their corresponding reconstructed signals (on the right) at 5dB SNR and different data rates with varying transmitted window bandwidths.

The table showcases results for four data rates: $R_{b1} = 160$ kbps, $R_{b2} = 256$ kbps, $R_{b3} = 320$ kbps, and $R_{b4} = 640$ kbps. Furthermore, the BUF and average power are displayed for different window bandwidths: W_A (70%),

TABLE 8. BUF and average power of noise-rejected reconstructed regular data at 5dB SNR and different data rates with varying transmitted window bandwidths.

	Bandwidth Utilization Factor (BUF)							
	$\mathbf{W}_A(70\%), P_A\%$		$\mathbf{W}_B(80\%), P_B\%$		$\mathbf{W}_C(90\%), P_C\%$		$\mathbf{W}_D(100\%), P_D\%$	
$\mathbf{R_{b1}}$ = 160 kbps	0.16	93.38	0.18	94.92	0.21	95.09	0.23	95.12
$\mathbf{R_{b2}}$ = 256 kbps	0.25	93.36	0.29	94.92	0.32	95.09	0.37	95.12
$\mathbf{R_{b3}}$ = 320 kbps	0.32	93.36	0.36	94.92	0.41	95.09	0.45	95.12
$\mathbf{R_{b4}}$ = 640 kbps	0.64	93.32	0.73	94.92	0.83	95.08	0.91	95.12

TABLE 9. Processing time of noise-rejected reconstructed regular data at 5dB SNR and 50 iterations with different data rates and varying transmitted window bandwidths.

	Processing Time (s)				Mean Time (μ_t)	
	$\mathbf{W}_A(70\%)$	$\mathbf{W}_B(80\%)$	$\mathbf{W}_C(90\%)$	$\mathbf{W}_D(100\%)$		
$\mathbf{R_{b1}}$ = 160 kbps	3.06	3.10	3.14	3.16	3.12	3.2
$\mathbf{R_{b2}}$ = 256 kbps	3.17	3.19	3.21	3.21	3.2	
$\mathbf{R_{b3}}$ = 320 kbps	3.21	3.24	3.22	3.19	3.22	
$\mathbf{R_{b4}}$ = 640 kbps	3.22	3.18	3.29	3.26	3.24	

TABLE 10. Memory usage of noise-rejected reconstructed regular data at 5dB SNR an 50 iterations with different data rates and varying transmitted window bandwidths.

	Memory Usage (MB)				Mean Memory (μ_m)	
	$\mathbf{W}_A(70\%)$	$\mathbf{W}_B(80\%)$	$\mathbf{W}_C(90\%)$	$\mathbf{W}_D(100\%)$		
$\mathbf{R_{b1}}$ = 160 kbps	146.30	146.15	146.16	147.43	146.51	146.63
$\mathbf{R_{b2}}$ = 256 kbps	146.30	146.15	147.21	145.30	146.69	
$\mathbf{R_{b3}}$ = 320 kbps	147.20	146.13	148.12	146.20	146.91	
$\mathbf{R_{b4}}$ = 640 kbps	146.19	146.21	146.15	147.09	146.41	

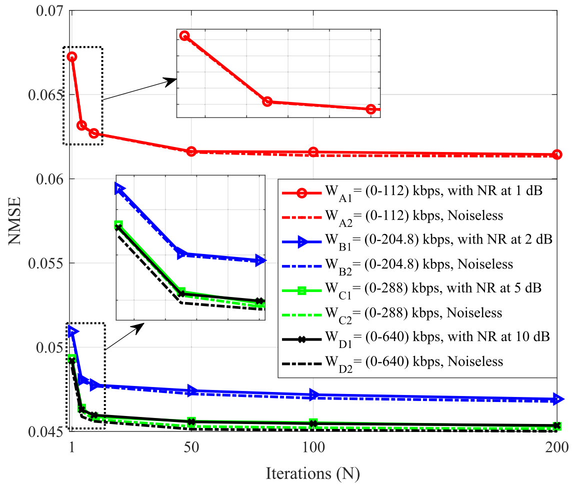


FIGURE 17. Comparison of NMSE for noiseless and noise-rejected reconstructed regular data at 5dB SNR and different data rates with varying transmitted window bandwidths.

$\mathrm{W_B}$ (80%), $\mathrm{W_C}$ (90%), and $\mathrm{W_D}$ (100%). The table shows that increasing the data rate also increases the BUF, indicating higher utilization of the available bandwidth. However, the average power of each transmitted window remains almost constant across different data rates but increases with larger window bandwidths. This suggests that higher data rates and wider bandwidths lead to more efficient spectrum utilization, resulting in increased power in the transmitted signal.

d: COMPUTATIONAL COMPLEXITY

It plays an important consideration when working with signal reconstruction algorithms. It quantifies the computational resources, such as processing time and memory, needed for the algorithm to reconstruct the signal. A lower computational complexity denotes a more efficient algorithm [39].

Processing Time: It is the amount of time that the algorithm spends to process or reconstruct the signals when applying input data. The shorter the processing time, the faster the signal reconstruction, resulting in quicker analysis and decision-making. Table 9 displays the time it takes to process reconstructed regular data with noise rejection. The data has an SNR of 5 dB and undergoes 50 iterations. This table aims to investigate how various data rates and window bandwidths affect the processing time for the noise reduction technique used in regular data reconstruction. It contains four rows with different data rates, while the columns indicate the processing time (in seconds) for four different window bandwidths. To calculate the average time, the processing times for the four window bandwidths are averaged for each data rate. The findings suggest that as the data rate increases, there is a small rise in processing time. Similarly, increasing the transmitted window bandwidth also leads to a slight increase in processing time. However, the mean processing time remains relatively consistent across all four data rates, averaging around 3.2 seconds. This information can be valuable in understanding the computational resources required for processing regular data under different conditions.

Memory Usage: It is an important consideration when implementing algorithms that reconstruct signals. Specifies how much memory space the algorithm uses to store temporary or final data while the program is running. Algorithms with low memory usage work best for machines with limited memory capacity or situations where available memory is limited. The memory usage of reconstructed regular data with noise rejection was analyzed in Table 10. The data was tested at 5 dB SNR and 50 iterations with different data rates and transmitted window bandwidths. Each row represents a specific data rate, while the columns represent different window bandwidths. The table provides the memory usage in MB for each combination, along with the mean memory usage for each data rate. The results show that as the data rate increases, the memory usage remains relatively consistent. However, as the transmitted window bandwidth increases, the memory usage also increases. On average, the memory usage across all data rates is around 146.63 MB. This information is valuable for understanding the resource requirements and limitations when implementing signal reconstruction algorithms. It helps in optimizing the algorithm to minimize memory usage, especially in scenarios where available memory is limited or when developing resource-constrained machines.

V. CONCLUSION

This paper presents a new way to reconstruct regular data from a malware-free and malware-injected RFID system in the UHF range with different data rates. The proposed method optimizes bandwidth usage by sending only a portion of the original signal's spectrum and using it to reconstruct the entire signal, saving up to 50% of the spectrum compared to conventional schemes. Moreover, a new technique was introduced to use the malware-injected data spectrum in the empty space in the received regular data spectrum to reconstruct the regular signal more quickly and with better performance. The new scheme could reduce the number of iterations from 1000 to 2 iterations to achieve the same reconstruction performance. The proposed scheme can be considered in reconstructing regular data with the aim of other signals' spectra, not malware-injected data only. The impact of AWGN on the reconstructed signal was also analyzed. Various techniques were explored to mitigate the noise effect, including adjusting the transmitting window's bandwidth, optimizing the number of iterations, and modifying the SNR at the receiver. The findings indicated that widening the bandwidth of the transmitting window can decrease the influence of noise. However, caution should be exercised as increasing the number of iterations excessively may cause the algorithm to diverge. Additionally, a higher SNR helps overcome the effects of noise. Also, a proposed noise reduction technique for UHF RFID systems was evaluated across various UHF bands and data rates and showed that the technique effectively reduced noise and improved reconstruction accuracy, with the NMSE closely approximating the NMSE obtained when no noise was present. The BUF and average power of the noise-rejected reconstructed regular data at SNR of 5dB for different data rates and varying transmitted window bandwidths are presented, and increasing the data rate also increases the BUF, indicating higher utilization of the available bandwidth. The proposed technique is highly effective in terms of its ability to withstand noise and provide efficient results. Future work could investigate the applicability of these methods in more noisy and complex environments to make them more practical for real-world applications.

REFERENCES

[1] L. Tan and J. Jiang, *Digital Signal Processing: Fundamentals and Applications*. New York, NY, USA: Academic, 2018.

[2] J.-N. Juang and R. W. Longman, "Identification of the dynamics in the singular vectors of the system Toeplitz matrix of Markov parameters," *J. Astron. Sci.*, vol. 69, no. 4, pp. 1115–1148, Jun. 2022, doi: 10.1007/s40295-022-00324-0.

[3] M. B. Mashhadi, N. Salarieh, E. S. Farahani, and F. Marvasti, "Level crossing speech sampling and its sparsity promoting reconstruction using an iterative method with adaptive thresholding," *IET Signal Process.*, vol. 11, no. 6, pp. 721–726, Aug. 2017, doi: 10.1049/iet-spr.2016.0569.

[4] S. D. Stearns and D. R. Hush, *Digital Signal Processing with Examples in MATLAB*. Boca Raton, FL, USA: CRC Press, 2016.

[5] L. Profetto, M. Gherardelli, and E. Iadanza, "Radio frequency identification (RFID) in health care: Where are we? A scoping review," *Health Technol.*, vol. 12, no. 5, pp. 879–891, Sep. 2022, doi: 10.1007/s12553-022-00696-1.

[6] J. Zhang, S. C. Periaswamy, S. Mao, and J. Patton, "Standards for passive UHF RFID," *GetMobile, Mobile Comput. Commun.*, vol. 23, no. 3, pp. 10–15, Jan. 2020, doi: 10.1145/3379092.3379098.

[7] C. Zang, C. Zhang, M. Zhang, and Q. Niu, "An RFID-based method for multi-person respiratory monitoring," *Sensors*, vol. 22, no. 16, p. 6166, Aug. 2022, doi: 10.3390/s22166166.

[8] C. J. N. Syazwani, N. H. A. Wahab, N. Sunar, S. H. S. Ariffin, K. Y. Wong, and Y. Aun, "Indoor positioning system: A review," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 6, pp. 1–14, 2022, doi: 10.14569/IJACSA.2022.0130659.

[9] F. Muralter, F. Muralter, H. Landaluce, and A. Perallos, "Polarization-diversity-based rotation sensing methodology using COTS UHF RFID tags," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 12728–12735, Jul. 2023, doi: 10.1109/JIOT.2023.3253709.

[10] X. Guo, L. Shangguan, Y. He, J. Zhang, H. Jiang, A. A. Siddiqi, and Y. Liu, "Efficient ambient LoRa backscatter with on-off keying modulation," *IEEE/ACM Trans. Netw.*, vol. 30, no. 2, pp. 641–654, Apr. 2022, doi: 10.1109/TNET.2021.3121787.

[11] J. Aliasgari, M. Forouzandeh, and N. Karmakar, "Chipless RFID readers for frequency-coded tags: Time-domain or frequency-domain?" *IEEE J. Radio Freq. Identificat.*, vol. 4, no. 2, pp. 146–158, Jun. 2020, doi: 10.1109/JRFID.2020.2982822.

[12] F. Liu, C. Masouros, A. P. Petropulu, H. Griffiths, and L. Hanzo, "Joint radar and communication design: Applications, state-of-the-art, and the road ahead," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3834–3862, Jun. 2020, doi: 10.1109/TCOMM.2020.2973976.

[13] T. Yin, L. Li, W. Lin, H. Hu, D. Ma, J. Liang, T. Bai, C. Pan, and Z. Han, ''Joint active and passive beamforming optimization for multi-IRS-assisted wireless communication systems: A covariance matrix adaptation evolution strategy,'' *IEEE Trans. Veh. Technol.*, vol. 72, no. 7, pp. 9281–9292, Jul. 2023, doi: 10.1109/TVT.2023.3253505.

[14] L. Fen, P. Xuefeng, and M. Gang, ''RFID signal reconstruction of Internet of Things based on compressed sensing,'' in *Proc. 8th Int. Comput. Syst. Educ. Manage. Conf. (ICSEMC)*, 2017, pp. 1–4, doi: 10.25236/icsemc.2017.43.

[15] Y. Bu, L. Xie, Y. Gong, J. Liu, B. He, J. Cao, B. Ye, and S. Lu, ''RF-3DScan: RFID-based 3D reconstruction on tagged packages,'' *IEEE Trans. Mobile Comput.*, vol. 20, no. 2, pp. 722–738, Feb. 2021, doi: 10.1109/TMC.2019.2943853.

[16] R. Zhao, Q. Zhang, D. Li, H. Chen, and D. Wang, ''PRTS: A passive RFID real-time tracking system under the conditions of sparse measurements,'' *IEEE Sensors J.*, vol. 18, no. 5, pp. 2097–2106, Mar. 2018, doi: 10.1109/JSEN.2018.2789350.

[17] J. Zhang, G. Tian, A. Marindra, A. Sunny, and A. Zhao, ''A review of passive RFID tag antenna-based sensors and systems for structural health monitoring applications,'' *Sensors*, vol. 17, no. 2, p. 265, Jan. 2017, doi: 10.3390/s17020265.

[18] M. Omer and G. Y. Tian, ''Indoor distance estimation for passive UHF RFID tag based on RSSI and RCS,'' *Measurement*, vol. 127, pp. 425–430, Oct. 2018, doi: 10.1016/j.measurement.2018.05.116.

[19] P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, ''Internet of Things: Security and solutions survey,'' *Sensors*, vol. 22, no. 19, p. 7433, Sep. 2022, doi: 10.3390/s22197433.

[20] J. B. Awotunde and S. Misra, ''Feature extraction and artificial intelligence-based intrusion detection model for a secure Internet of Things networks,'' in *Illumination of Artificial Intelligence in Cybersecurity and Forensics*, vol. 109. Cham, Switzerland: Springer, 2022, pp. 21–44, doi: 10.1007/978-3-030-93453-8_2.

[21] S. M. N. Hasnaeen and A. Chrysler, ''Detection of malware in UHF RFID user memory bank using random forest classifier on signal strength data in the frequency domain,'' in *Proc. IEEE Int. Conf. RFID (RFID)*, May 2022, pp. 47–52, doi: 10.1109/RFID54732.2022.9795967.

[22] H. Fernando and J. Abawajy, ''Malware detection and prevention in RFID systems,'' in *Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence*. Berlin, Germany: Springer, 2013, pp. 143–166, doi: 10.1007/978-3-642-34952-2_6.

[23] B. Ray, S. Huda, and M. U. Chowdhury, ''Smart RFID reader protocol for malware detection,'' in *Proc. 12th ACIS Int. Conf. Softw. Eng., Artif. Intell., Netw. Parallel/Distrib. Comput.*, Jul. 2011, pp. 64–69, doi: 10.1109/SNPD.2011.41.

[24] A. F. Ashour, C. Condie, C. Pocock, S. C. Chiu, A. Chrysler, and M. M. Fouda, ''Spectrum-based malware detection for RFID memory banks in LF, HF, and UHF bands,'' in *Proc. IEEE Int. Opportunity Res. Scholars Symp. (ORSS)*, Apr. 2023, pp. 70–73, doi: 10.1109/ORSS58323.2023.10161830.

[25] A. Kumar, A. K. Jain, and M. Dua, ''A comprehensive taxonomy of security and privacy issues in RFID,'' *Complex Intell. Syst.*, vol. 7, no. 3, pp. 1327–1347, Jun. 2021, doi: 10.1007/s40747-021-00280-6.

[26] M. Baykara and S. Abdullah, ''Designing a securable smart home access control system using RFID cards,'' *J. Netw. Commun. Emerg. Technol.*, vol. 10, no. 12, pp. 1–12, 2020.

[27] L. Gavoni, ''RFID exploitation and countermeasures,'' 2021, *arXiv:2110.00094*.

[28] C. Nagarathna, B. M. Kumar, N. Bhavana, T. Manjushree, and D. Pattan, ''Improve the efficiency of large rfid network using enhanced security data delivery model for machine learning based network intrusion detection system—A survey,'' *Int. J. Hum. Comput. Intell.*, vol. 1, no. 4, pp. 10–17, 2022.

[29] E. Krouk and S. Semenov, *Modulation and Coding Techniques in Wireless Communications*. Hoboken, NJ, USA: Wiley, 2011.

[30] A. Gody, R. A. Seoud, and M. E. El-Din, ''Using mel-mapped best tree encoding for baseline-context-independent-mono-phone automatic speech recognition,'' *Egyptian J. Lang. Eng.*, vol. 2, no. 1, pp. 10–24, Apr. 2015, doi: 10.21608/ejle.2015.60254.

[31] R. E. Blahut, ''Baseband modulation,'' in *Modem Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2009, doi: 10.1017/CBO9780511811401.004.

[32] R. L. Haupt, *Wireless Communications Systems: An Introduction*. Hoboken, NJ, USA: Wiley, 2019.

[33] A. Lapidoth, *A Foundation in Digital Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2017.

[34] A. Ashour, A. Khalaf, A. Hussein, H. Hamed, and A. Ramadan, ''A proposed signal reconstruction algorithm over bandlimited channels for wireless communications,'' *Adv. Electr. Comput. Eng.*, vol. 23, no. 1, pp. 19–32, 2023, doi: 10.4316/AECE.2023.01003.

[35] A. F. Ashour, ''A new algorithm for baseband pulse transmission over band-limited channels for wireless automotive communications,'' *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 4, pp. 5222–5228, Aug. 2020, doi: 10.30534/ijatcse/2020/151942020.

[36] F. M. Ghannouchi, O. Hammi, and M. Helaoui, *Behavioral Modeling and Predistortion of Wideband Wireless Transmitters*. Hoboken, NJ, USA: Wiley, 2015.

[37] *18000-63 Type C (Gen2) and 18000-63 Type C/18000-64 Type D (Gen2/TOTAL) RFID IC*, EM Microelectron., La Tène, Switzerland, 2015.

[38] S. A. Ahson and M. Ilyas, *RFID Handbook: Applications, Technology, Security, and Privacy*. Boca Raton, FL, USA: CRC Press, 2017.

[39] J.-I. Agulleiro and J. J. Fernández, ''Evaluation of a multicore-optimized implementation for tomographic reconstruction,'' *PLoS ONE*, vol. 7, no. 11, Nov. 2012, Art. no. e48261, doi: 10.1371/journal.pone.0048261.

AHMED F. ASHOUR received the B.Sc. degree in electrical and computer engineering from the Higher Technological Institute (HTI), Egypt, in 2009, and the M.Sc. degree in electronics and communications engineering from the Arab Academy for Science, Technology, and Maritime Transport (AASTMT), Egypt, in 2017. He is currently a Teaching and Research Assistant with the Department of Electrical and Computer Engineering, Idaho State University, ID, USA. He held the position of Senior Teaching Engineering II with The American University in Cairo (AUC), from 2021 to 2022. He was an Assistant Lecturer with AASTMT, in 2022, and with HTI, from 2017 to 2020. He was a Teaching Assistant with HTI, from 2011 to 2017. He held other technical positions as a Senior Research and Development Electronics Engineer with Falcon Electronics and Electrical Industries, Egypt, from 2018 to 2022, and an Executive Director with Fast Fix Company for Construction and Maintenance, Egypt, from 2014 to 2017. His research interests include analog and digital signal processing, machine learning, and mobile and wireless communication networks (5G and 6G).

CALVIN CONDIE received the B.Sc. degree in electrical engineering from Idaho State University, in May 2023. He is going to pursue his master's degree. He has been very active in participating in clubs on campus, such as the Institute of Electrical and Electronics Engineers and the Tau Beta Pi Honor Society. His research interests include further development of RFID technologies as well as antennas and network security.

CADE POCOCK received the AAS degree in instrumentation engineering technology from Idaho State University, in 2019, where he is currently pursuing the degree in electrical engineering with Idaho State University. His research interests include RFID communication and control systems.

STEVE C. CHIU received the B.S. degree in electrical engineering from the University of Illinois at Chicago, and the master's degree in engineering management and the Ph.D. degree in electrical and computer engineering from Northwestern University. He is a Professor and the Chair of Electrical and Computer Engineering with Idaho State University (ISU). His research interests include high-performance computing, embedded control systems, communications, and microelectronics. He was affiliated with ISU's Measurement and Control Engineering Research Center. He has published more than 70 refereed conference papers and journal articles, including a book on control system modeling and simulation with MATLAB. He is a member of the Tau Beta Pi Engineering Honor Society. He was a selected attendee at the National Academy of Engineering's 2013 Frontiers of Engineering Education Symposium. He was the 2019 Fulbright-NSF U.S. Scholar in cybersecurity and critical infrastructure. Prior to his academic career, he worked in the certification and telecommunication industries as the Standards Project Manager and a Research and Development Engineer. He was a referee for several publications in computer science and engineering, including *IEEE Computing in Science and Engineering*, the *Journal of Parallel and Distributed Computing*, the *Journal of Future Generation Computing Systems*, and *Lecture Notes in Computer Science*. He serves on the Editorial Review Board of the *International Journal of Handheld Computing Research*. He is a Guest Editor of the *Journal of Supercomputing*.

ANDREW CHRYSLER (Member, IEEE) received the B.S. degree in chemical and biological engineering with a minor in mathematics from Colorado State University, Fort Collins, CO, in 2011, and the M.S. and Ph.D. degrees in electrical and computer engineering from The University of Utah, Salt Lake City, UT, in 2017 and 2018, respectively. He was with IM Flash Technologies, Lehi, UT, as a Semiconductor Manufacturing Engineer and as a Co-Op with the NASA Glenn Research Center, Cleveland, OH. He has also conducted research at Daegu University, Daegu, South Korea. He is an Assistant Professor with Idaho State University. His research interests include dielectric properties of materials, implantable antennas, millimeter wave antennas, and international engineering education. He is an NSF EAPSI Korea Fellow ('15) and received the IEEE APS Doctoral Research Award ('13).

MOSTAFA M. FOUDA (Senior Member, IEEE) received the B.S. degree (as the valedictorian) and the M.S. degree in electrical engineering from Benha University, Egypt, in 2002 and 2007, respectively, and the Ph.D. degree in information sciences from Tohoku University, Japan, in 2011. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, Idaho State University, ID, USA. He is a Full Professor with Benha University. He was an Assistant Professor with Tohoku University and a Postdoctoral Research Associate with Tennessee Technological University, TN, USA. He has (co)authored more than 190 technical publications. His current research focuses on cybersecurity, communication networks, signal processing, wireless mobile communications, smart healthcare, smart grids, AI, and the IoT. He has guest-edited a number of special issues covering various emerging topics in communications, networking, and health analytics. He is currently serving on the editorial board of IEEE Transactions on Vehicular Technology, IEEE Internet of Things Journal, and IEEE Access. He has received several research grants, including NSF Japan–U.S. Network Opportunity 3 (JUNO3).