Statistical Methods Based Anti-jamming Signal Recovery Algorithm on Digital Signals

ABSTRACT

Jamming has become a major problem in real-life situations. This type of attack affects numerous wireless networks, causing them to malfunction and even stop working. To mitigate the negative effects of jamming, researchers have proposed different strategies and algorithms to prevent signal contamination. In this paper, we present a new algorithm that is simple to implement and utilizes the additive nature of digital signals and statistical methods. Upon evaluation, our algorithm achieves over 99.5% accuracy rates on simulated datasets.

CCS CONCEPTS

• **Networks** → **Mobile and wireless security**; Wireless access networks; • **Hardware** → *Digital signal processing*.

KEYWORDS

Anti-Jamming, Signal Recovery, Wireless Networking, Signal Processing, Communication Systems.

1 INTRODUCTION

Wireless communication networks play a pivotal role in contemporary society, facilitating a myriad of applications across various domains. From personal communication to industrial automation, these networks underpin essential functionalities. Unfortunately, the ubiquity of wireless networks comes with a vulnerability – the susceptibility to jamming. Jamming disrupts communication channels, leading to service degradation, data loss, and compromised network integrity.

The challenge posed by jamming prompts the question: Can we mitigate its detrimental effects and ensure reliable communication? This paper addresses this question by proposing an innovative solution that strives to recover original signals amidst interference. Our approach, outlined in the subsequent sections, offers a pathway to bolster the resilience of wireless networks.

Creating such a solution is inherently challenging due to the complex dynamics of interference, diverse jamming techniques, and the need for real-time adaptability. Nevertheless, our key insight revolves around leveraging signal recovery algorithms that effectively differentiate between sender-originated signals and jamming-induced noise. Our solution harnesses distinctive properties of sender signals and interference patterns, contributing to accurate signal recovery.

In the subsequent sections, we delve into the methodology of our approach, present experimental results, and offer comprehensive analyses. Through these explorations, we elucidate the algorithm's efficacy in recuperating original signals from the interference-laden environment. Our research not only contributes to the enhancement of wireless communication security but also provides insights into the intricacies of combating jamming-induced disruptions.

The forthcoming sections of this paper will detail the step-by-step methodology, showcase the empirical results obtained, and offer a comprehensive analysis of the proposed algorithm. These facets collectively illuminate the potential of our solution to reinforce the reliability and robustness of wireless networks in the face of adversarial jamming.

2 METHODOLOGY

In this section, we outline the methodology employed to address the challenge of signal recovery in the presence of jammers and develop an efficient algorithm for enhancing the reliability and accuracy of wireless communication networks. Our research revolves around a network comprising six wireless nodes, categorized into two sets: a first set consisting of a good sender, good receiver, and good jammer, and a second set comprising a bad sender, bad receiver, and bad jammer. These nodes operate within the same network channel.

- **Experimental Setup:** We set up a controlled experimental environment with the six categorized wireless nodes to simulate real-world signal transmission scenarios. The nodes are configured to transmit signals at the same carrier frequency, with the good sender and receiver restricted to binary bits (0s and 1s).

- **Data Collection:** We collect data from the experimental setup, capturing the transmitted signals and their corresponding reception at the good receiver. Additionally, we record the interference patterns introduced by the good and bad jammers during the transmission process.

- **Algorithm Development:** Based on the collected data, we develop a novel algorithm to recover the original signals sent by the good sender from the interfered signals received by the good receiver. The algorithm focuses on effectively distinguishing and

extracting the original sender signals from the superposition of sender and jammer signals at the receiver's end.

- **Algorithm Evaluation:** We rigorously evaluate the performance of the developed algorithm using various metrics, such as signal recovery accuracy and computational efficiency. To ensure robustness, we test the algorithm against diverse interference patterns and varying signal strengths.
- **Comparative Analysis:** To assess the algorithm's effectiveness, we conduct a comparative analysis against existing signal recovery techniques and error correction methods. We analyze the strengths and weaknesses of each approach, highlighting the advantages of our proposed algorithm.
- **Simulation and Results:** Using simulation tools, we validate the algorithm's performance under different network conditions, including varying jammer strengths and interference patterns. We present the results in a graphical format, enabling a comprehensive understanding of the algorithm's efficacy.

Through the comprehensive implementation of these methodology steps, we aim to contribute significant insights into the field of wireless communication security. Our research endeavors to pave the way for enhanced data transmission and communication reliability in the presence of jammers, thus fortifying wireless networks against adversarial interference.

2.1 Problem Definition

In this research project, we address the challenge of signal recovery in a wireless network comprising six nodes divided into two sets. The first set comprises a "good sender," "good receiver," and "good jammer," while the second set consists of a "bad sender," "bad receiver," and "bad jammer." All six nodes operate within the same channel of our network.

In our network setup, the senders are responsible for transmitting packets to the receivers. However, the presence of jammers introduces interference, disrupting the signals transmitted by the senders. Consequently, the receivers receive signals that are a superposition of both the original signals from the senders and the interfering signals from the jammers.

Our primary objective is to develop an innovative algorithm capable of recovering the original signals sent by the senders from the contaminated signals received by the receivers. To begin, we simplify the problem by considering only three nodes: the "good sender," "good receiver," and "good jammer." All three nodes transmit signals at the same carrier frequency, limiting their communication to binary bits, i.e., 0s and 1s.

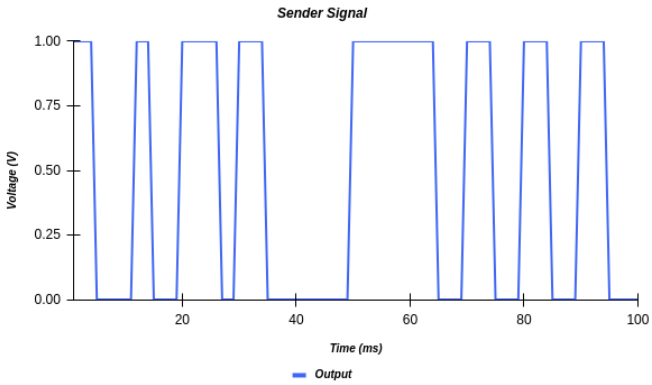

Figure 1: Signal Sent by Good Sender

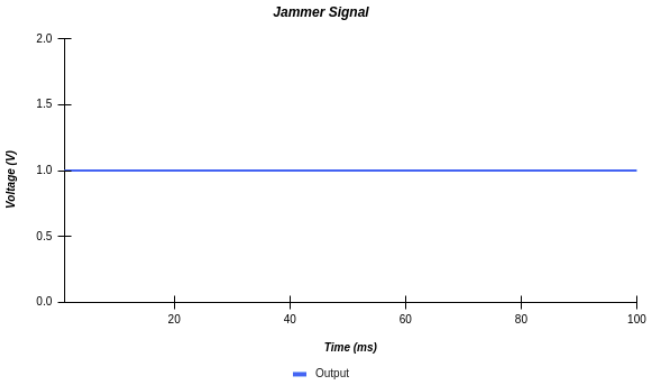

Figure 2: Signal Sent by Jammer

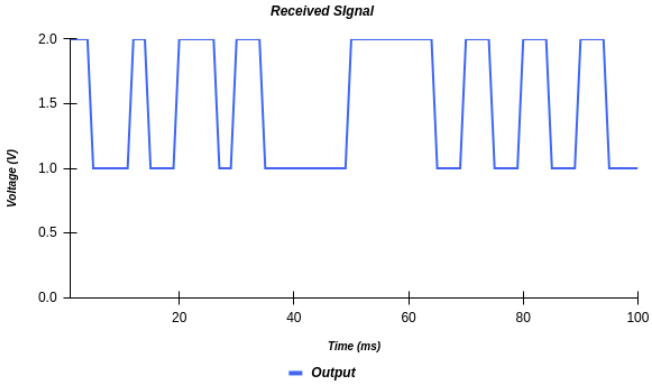

Figure 3: Signal Received by the Receiver

The challenge is further illustrated in Figure 3, which demonstrates the superposition of signals from Figure 1 and Figure 2. Our research project focuses on devising an effective approach to disentangle and recover the signals sent by the sender amidst the presence of contamination depicted in Figure 3.

By exploring innovative algorithms and signal processing techniques, our research aims to contribute to the advancement of signal recovery methods in interference-prone wireless networks. The successful development of such an algorithm has significant implications for improving the reliability and efficiency of communication systems in challenging and dynamic wireless environments.

2.2 Key Ideas

Our algorithm is designed to restore the original signals sent by the sender when the sender's signals are mixed with signals from jammers. This is done by using the sender rates and performing all the necessary calculations on the receiver's end.

At the beginning of this signal recovery process, the sequence of received signals mixed with both the sender's signals and the jammers' signals is split into several subsequences. The length of each subsequence of signals is equal to the number of cycles in which the sender has a constant rate. After splitting into subsequences, for each subsequence, we check if it has at least one bit with an amplitude of 0. If so, this subsequence containing 0s is smoothed to all 0. Similarly, if one subsequence has at least one bit with an amplitude of 1, all bits of this subsequence are smoothed to all 1. In case a specific subsequence does not have either 0 or 1 as mentioned above, we compute the average amplitude of this subsequence and compare it to the expected value of amplitudes to recover signals.

Although dealing with the last case may potentially introduce errors, in real life, the rates of senders and jammers are distinctly different. As a result, our algorithm can still achieve very high accuracy in the long run, which is demonstrated in the evaluation section.

2.3 Implementation

sharedSchedule: which is the schedule of the sender calculated by the pseudorandom seed used to generate pseudorandom sequence and pseudorandom signal rates. The pseudorandom seed is shared with both the sender and receiver.
receivedSignal: which is the sequence of received signals representing bits under the synchronized rate with the sender.
filteredBit: which is the sequence of bits after filtering out signals sent by the jammer.

3 EVALUATION

In the following sections, the signals transmitted by multiple jammers are equivalent to signals with greater amplitudes because of the additive property of digital signals.

Algorithm 1 Signal Recovery

```
1:  procedure FILTER(sharedSchedule, receivedSignal)
2:      filteredBit ← initialization
3:      cycle ← 0
4:      while not pass the end of receivedSignal do
5:          s ← receivedSignal[in the current cycle]
6:          if s has 0 then
7:              filteredBit ← 0
8:          else if s has num_jammer + 1 then
9:              filteredBit ← 1
10:         else
11:             filteredBit ← approx(s)
12:         end if
13:         cycle ← cycle + 1
14:     end while
15:     return filteredBit
16: end procedure
```

Algorithm 2 Approximation

```
    procedure APPROX(signals)
2:      result ← initialization
        if avg(signals) > (num_jammer + 1)/2 then
4:          result ← 1
        else
6:          result ← 0
        end if
8:      return result
    end procedure
```

3.1 Distinct Rates

The four charts in Figure 4 display both PDF and CDF of the accuracy rates from 1000 tests for each case where the numbers of jammers are different. In total, there are 4000 tests conducted where jammers and senders have very different rates, and each test consists of 100 cycles of signals.

The accuracy rates are determined by calculating the number of cycles where the algorithm correctly identifies the original signal sent by the sender divided by the total number of cycles. These results are obtained by using the algorithm mentioned above, which is capable of handling jamming attacks with multiple jammers that randomly change their rates. However, this requires that the sender rates are synchronized.

Overall, our results suggest that the algorithm is very effective at recovering signals under jamming attacks, which can mitigate the negative effects of jamming in wireless communication.

In the detailed graph, labeled as Figure 5, we can observe the accuracy rates of tests conducted with varying numbers of cycles in two different scenarios: one with a single jammer

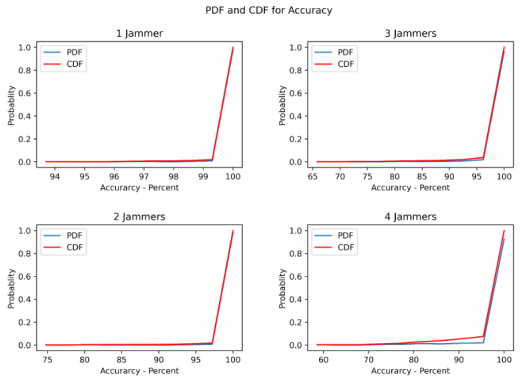

Figure 4: PDF and CDF

in the wireless network and another with two jammers in this network. It is worth noting that sequences of signals with a higher number of cycles, longer sequences in other words, are more realistic and help us better test the performance of our algorithm.

With the simulated data we generated, the algorithm can perform well in both scenarios, regardless of the number of cycles in each session, as long as there is a large difference between the jammer rate and the sender rate. These results demonstrate the effectiveness and reliability of the algorithm in dealing with jamming attacks and maintaining secure communication channels in the long run.

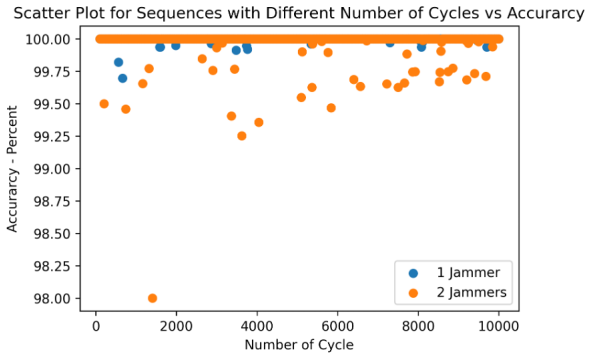

Figure 5: Scatter Plot

Figure 6 displays two accuracy distributions over 100 tests for two scenarios: one with a single jammer and the other with two jammers. Overall, there are 200 tests, each consisting of 10000 cycles.

These two distributions demonstrate that the algorithm works effectively in most cases when there is a large difference between the jammer rate and the sender rate. The algorithm can achieve very high accuracy rates of approximately 99.94% to 100% when one jammer is attacking the wireless network and about 99.8% to 100% accuracy when two jammers are attacking this network. The tails of these two distributions are small, indicating that the algorithm is effective.

Based on these tests, we conclude that the algorithm presented above is both reliable and robust as it can handle a wide range of scenarios.

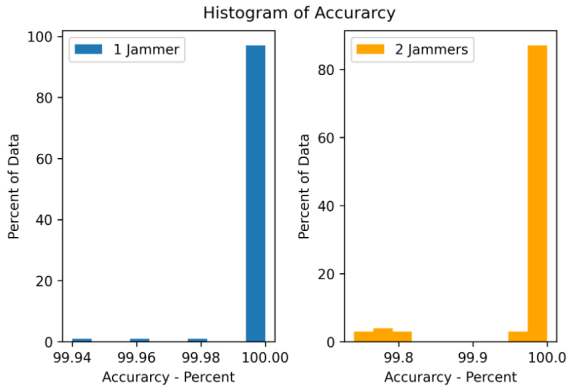

Figure 6: Histogram

3.2 Explaining 4B5B Encoding Technique for Signal Integrity Assurance

In modern communication systems, ensuring the integrity of transmitted signals is of paramount importance. One technique that has gained prominence in this domain is the 4B5B encoding method. The 4B5B technique plays a crucial role in verifying whether a signal has been tampered with, providing a reliable means of detecting alterations. This section elucidates the workings of the 4B5B encoding technique and underscores its significance in ensuring signal authenticity and security.

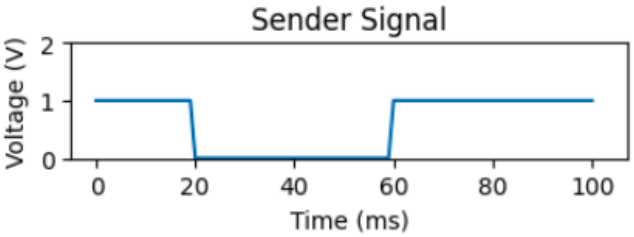

Figure 7: Signal Sent by Sender

At its core, the 4B5B technique involves the conversion of 4-bit sequences into corresponding 5-bit sequences. This process is designed to enhance the robustness of transmitted signals against tampering while simultaneously maintaining compatibility with the original signal. The key premise of

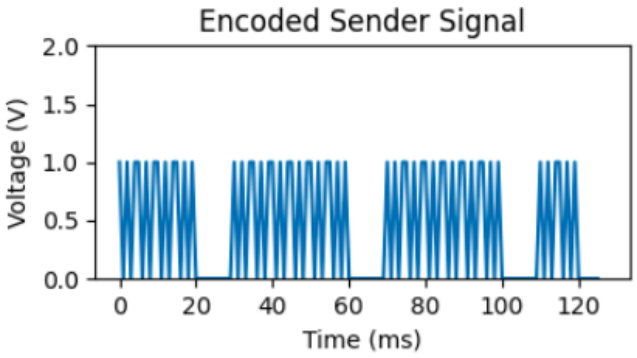

Figure 8: Encoded Sender Signal

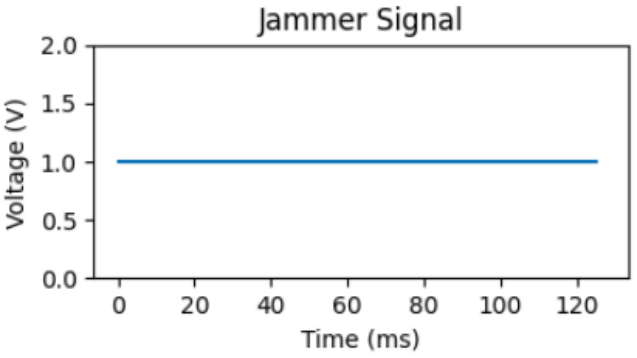

Figure 9: Jammer Signal

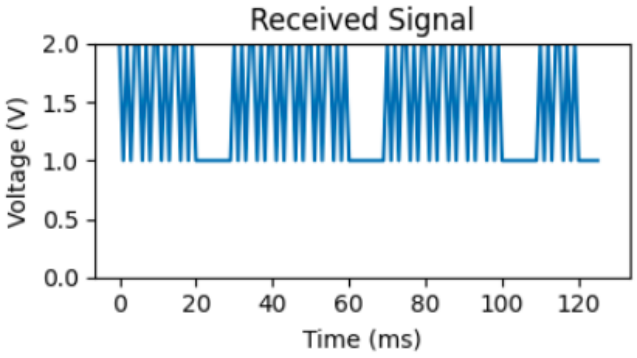

Figure 10: Received Signal

4B5B encoding is to replace each consecutive set of four bits with a unique five-bit sequence, thereby increasing the possible variations.

To enable this conversion, a mapping table is employed, consisting of 16 patterns of 4 bits which are 0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111 , each linked to 32 distinct patterns of 5 bits which are 00000, 00001, 00010, 00011, 00100, 00101, 00110, 00111, 01000, 01001, 01010, 01011, 01100, 01101, 01110, 01111, 10000, 10001, 10010, 10011, 10100, 10101, 10110, 10111, 11000, 11001, 11010, 11011, 11100, 11101, 11110, 11111. This mapping is the cornerstone of the 4B5B technique, ensuring that each 4-bit sequence is uniquely represented by a 5-bit counterpart. The creation of such a mapping table significantly enhances the tamper detection capability of the encoding method.

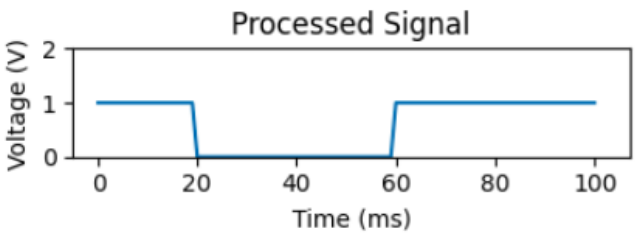

Figure 11: Processed Signal

One of the noteworthy features of 4B5B encoding is its ability to generate an astronomical number of unique mapping tables—specifically, an astonishing 601080390 tables. The sheer enormity of this number underscores the formidable challenge posed to anyone attempting to tamper with the encoded signal. Since each unique mapping encapsulates the relationship between 4-bit and 5-bit sequences, tampering with even a single bit within the signal would lead to an error during decoding, thereby revealing the presence of unauthorized alterations.

A key aspect that contributes to the security of the 4B5B technique is that only the sender possesses the knowledge of the specific mapping employed. This means that an attacker attempting to alter the signal would lack the requisite mapping information to make successful modifications. Consequently, any tampering attempt would result in a mismatch between the expected 5-bit sequence and the altered sequence, immediately raising an error flag during signal decoding.

In conclusion, the 4B5B encoding technique stands as a robust solution for safeguarding the integrity of transmitted signals. By leveraging the intricacies of mapping 4-bit sequences to 5-bit sequences and utilizing an astronomical number of possible mapping tables, 4B5B encoding provides an effective and tamper-resistant means of ensuring signal authenticity. Through its unique characteristics and the clandestine nature of sender-specific mapping, the 4B5B technique forms a vital pillar in the realm of signal security.

3.3 Optimizing Signal Transmission with Alternating Bits

The chart under analysis represents the occurrence of "1 bit" in a sender signal following an alternating pattern, such as 101010, with data for 100 bits.

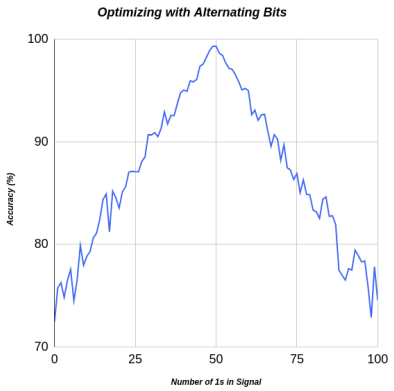

Figure 12: Enhanced Accuracy with Alternating Bits

The signal follows an alternating pattern, such as 101010, and the chart specifically represents data for 1000 bits. In comparison, the provided chart represents the trend based on the number of "1s" in the signal. The data presented in the chart pertains to signals with a length of 1000. However, even with signals of a more extensive data range, such as 10000, it is expected that the highest accuracy will be achieved when the bits alternate consistently. For instance, when there are 5000 alternating occurrences of "1s" and "0s" in the signal.

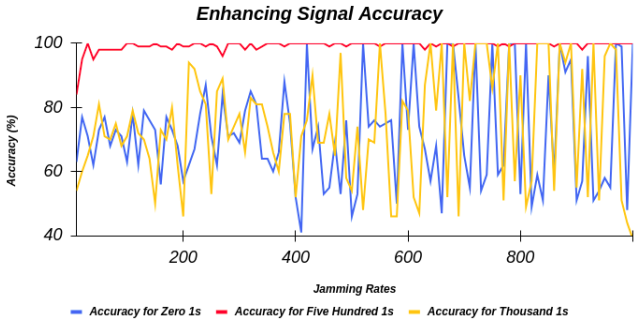

Figure 13: Enhanced Accuracy with Alternating Bits

The provided chart displays three lines indicating the count of "1s" in our signal. Consequently, I have considered instances with 0, 500, and 1000 occurrences of "1s." Notably, the 500 occurrences follow an alternating pattern. As observed, the accuracy of our signal processing improves with increased alternation. Conversely, if our signal lacks alternation, signal jamming is more likely. The unpredictability observed in the accuracies of signals with zero "1s" and signals with one hundred "1s" is attributed to the presence of a jammer signal, which exhibits random behavior in each observation.

4 RELATED WORK

5 CONCLUSION

In conclusion, our algorithm is able to recover bits representing 0 and bits representing 2 from received signals successfully. However, the main challenge affecting accuracy lies in identifying and recovering bits representing 1 based on amplitudes. Based on the two cases we study above, we find our algorithm can achieve very high accuracy when the rates of senders and jammers are very different or when the bits of received sequences alternate consistently. In order to recover bits representing 1 in other cases with high accuracy, we recommend prioritizing the computation or recovery of "1s" at the outset of signal processing. Ongoing efforts involve exploring error correction code methods to address the presence of "1s" from both the sender and jammer. There are several research directions for future work, such as extending our algorithm to recover analog signals, studying more real-life cases, and testing this algorithm with real sensors. The focus of these works should be optimizing signal recovery for bits representing 1 to enhance overall accuracy in practical applications.

ACKNOWLEDGMENTS

A RESEARCH METHODS

A.1 Part One