Over-the-air Signal Protocol and Malicious Alteration/Mimick Recognition

KEWEI CHEN, Department of Electrical and Computer Engineering, UC San Diego, USA

The security of wireless communications is increasingly compromised by sophisticated signal processing attacks, specifically through altered and mimic signals. These attacks modify existing legitimate signals or imitate protocol-bound signals to bypass standard security measures, posing significant threats to systems relying on the integrity and authenticity of wireless communications. This project addresses these security breaches by leveraging Strip Spectral Correlation Analysis (SSCA) features to distinguish between benign, altered, and mimicked signals from noise and single-carrier signals, classify different protocols, and detect signal alterations or mimicry. However, the preliminary results indicate challenges in data reliability due to inaccuracies in the metadata provided by the data collection tool, Searchlight. These inaccuracies lead to shifts in the SSCA features, leveraging a need in re-evaluation of the collected data's integrity and the development of a more accurate data collection method. Despite these challenges.

1 INTRODUCTION

1.1 Motivation and Objectives

Wireless communication security can be compromised by adversaries using advanced signal processing to send malicious signals, either by altering existing signals or mimicking protocol-bound signals. Altered Signals involve the modification of existing legitimate signals in such a way that they carry additional, hidden information. This hidden information is embedded in a manner that makes it undetectable or appears as noise to standard receivers not privy to the alteration technique. However, an attacker with the right equipment and knowledge can decode this hidden information. For example, an attacker might overlay a QPSK modulation on Zigbee's OQPSK signals, allowing the transmission of hidden information that the Zigbee decoder interprets as noise but can be decoded by the attacker.

Alternatively, "Mimick Signals" involve altering the signal's characteristics, such as the preamble, channel frequency, or hopping pattern, to make them appear similar to legitimate signals to bypass decoders or detection mechanisms. This can make the signals undetectable or indecipherable by standard security measures, allowing attackers to exploit systems by bypassing security protocols or creating openings for further attacks. Mimicking can be particularly dangerous in environments where the integrity and authenticity of signals are critical, such as in financial transactions, critical infrastructure, or defense systems. Fig. 1 and 2 illustrate the altered and minick attacks.

To tackle the security breaches caused by such attacks, this project aims at distinguishing over-the-air signal by their modulation and protocols and detects potential alteration and mimicking. Specifically, the following 3 objectives are targeted:

(1) Separation of the protocol-bind singles (benign protocol, altered and mimic signal) from noise and single-carrier signals.

Author's address: Kewei Chen, kec026@ucsd.edu, Department of Electrical and Computer Engineering, UC San Diego, 9500 Gilman Drive, La Jolla, Californa, USA, 92093-0021.

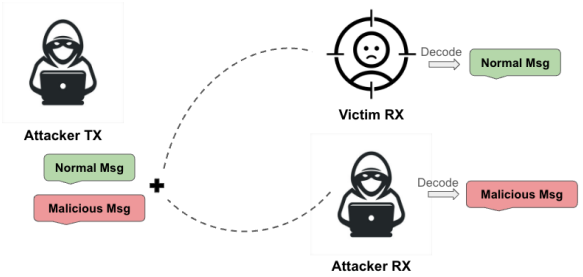

Fig. 1. Altered Attacker

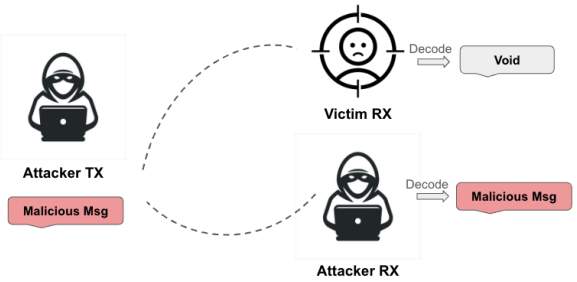

Fig. 2. Minick Attacker

(2) Separation of signals of different protocols (e.g., OFDM, Zigbee, Frequency Hopper etc.).
(3) Detection of whether the protocol-bind signal is altered/minicked.

1.2 Approaches

SSCA, Strip Spectral Correlation Analyzer, is a computationally effective approach for estimating the spectral correlation function throughout the entire cyclic frequency domain [1]. Fig. 3 shows the block diagram of the SSCA extraction process.

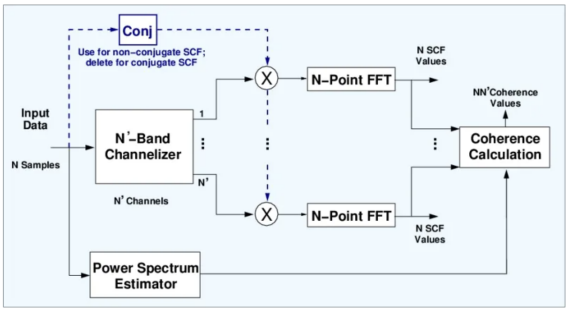

Fig. 3. Block Diagram for SSCA Extraction [2]

The high-level computation process is as follows: the signal is firstly passed through a channelizer that chops the signal into N pieces of narrowband signals. Each of the narrowband signal is then correlated with the original signal to find out the cyclo-stationary features

Note that the SSCA features can be conjugate and non-conjugate. The non-conjugate features, which is computed using the product of conjugated and original signal, reflects the cyclic features. On the other hand, the conjugate SSCA features, which is obtained by multiplying 2 copies of the original signals, mainly reveals the CFO information. The resultant features are 2D, to further compress the features, we can take either the sum of max of each cyclic frequency. This leaves us 4 types of SSCA features: *sum non-conj, sum conj, max non-conj*, and *max conj*. Among these features, we mainly focus on *sum non-conj* as there is little information loss and cyclo-stationary features reveals more signal characteristics than CFO.

Each protocol should revel different SSCA feature given that they have different sampling rate, chirp rate, preamble and etc. This project is completed based on this assumption and we build template for each protocol and compares the testing data SSCA with each of the protocol to accomplish the classification.

2 RELATED WORKS

A lot of works have been carried out to address the modulation classification problem. Most recent works all consider Deep Learning based mechanisms. For example, [3] adopts CNN and uses transfer learning to fix the lack of dataset, and [4] deployed a deep network with dual-stream architecture, namely CNN-LSTM. More advanced methods such as a multimodal approach that uses domain-specific features in the form of Higher Order Cumulants (HOCs) [5] and GAN network [6] also shows promising results. However, the Deep Learning approaches are all computationally expensive and have the problem with the latency. If the dataset is not representive enough, they may also suffer from the problem of over-fitting. Tradition methods, such as likelihood-based methods [7][8], need prior information about the channel and signal model, which are difficult to obtain in practice [9]. In addition, as pointed out by [10], most of works focus on only a subset of modulations, while the multi-carrier signals and protocol-bind signals are mostly ignored, which leaves the gaps of altered/mimick attacks illstruted above.

3 IMPLEMENTATION

3.1 Datasets

So for the following datasets are being used towards this project:

- **Zigbee:** OTA data with arbitrary uncalibrated Gaussian noise and collected at the sampling rate of $4MHz$. The are normal Zigbee protocols, and malicious signals with QPSK over OQPSK type of alteration. There are different alteration power of 0.1, 0.2, 0.3 and 0.4 of the original signal power. The data is transmitted and collected using SDR controlled by GNURadio [11]. The center frequency and sampling frequency is clearly defined before the collection and is therefore accurate.
- **Frequency Hopper:** Normal Frequency Hopper protocols collected using Boxing techniques introduced by Searchlight [12]. The Searchlight scans the spectrum and find out high energy areas with estimated noise floor. The energies are then boxed by uses morphological operations and converted back to IQ samples. The sampling rate and center frequency metadata are therefore not accurate and depends on many random factors such as the noise floor estimation, selective fading, and etc.
- **Lora:** Normal Lora protocols collected using Boxing techniques introduced by Searchlight [12]. The sampling rate and center frequency metadata may not be accurate.
- **Example:** Normal Example protocols collected using Boxing techniques introduced by Searchlight [12]. The sampling rate and center frequency metadata may not be accurate.
- **AWGN:** Random noise generated using MatLab.
- **Single Carrier Signals:** These are taken as LPIs in the testing as they are not protocol-bind. The modulations included are: BPSK, DSSS, FSK, MSK, GMSK, OOK, QAM PSK. They are also collected by the Searchlight [12]

3.2 SSCA Templates

3.2.1 Computation Procedure. The following steps are for building template for sum non-conjugate SSCA feature. The key idea is to find the most common and prominent cyclic features, which is represented as peaks on the 2D SSCA features.

(1) Take half of the dataset as training set and calculate their SSCA features. Normalize them to $[0, 1]$.
(2) Stack the training set and take fft along the stacked axis for each point. Compute

$$common\_pk = fft[0] \times (fft[0]/sum(fft[0:end])) \quad (1)$$

for each point. The $(fft[0]/sum(fft[0:end]))$ term computes the probability that the point is a common peak across the training set, and $fft[0]\times$ further takes the magnitudes into account. This step essentially filtered out common peaks across all the noisy SSCA features over all the training samples.
(3) Apply the peak finder to *common_pk* to find the dominant cyclic features. The key idea of the algorithm is to find thresholds such that

$$threshold = medfilt(common\_pk, w\_size) \quad (2)$$

$$thresh = scale \times threshold \quad (3)$$

where w_size and *scale* are tune-able parameters. Then find continuous ranges above the *thres* and take the midpoints as a peak.
(4) Store *cycle_peaks* (positions of the peaks), *cycle_peak_heights* (heights of the peaks), *range_begin* and *range_end* (ranges that peaks occur). These 4 elements constitute the template.

3.2.2 SSCA Templates for Known Protocols. Fig. 4, 5 6 and 7 shows the the sum non-conj SSCA feature templates for unaltered Zigbee, Frequency Hopper Example and Lora protocol. Note that the red triangles denotes the peaks.

Fig. 8 shows the SSCA feature for the noise. There is no peak except the center one where it is correlating with itself, and the magnitude stays almost constant for the rest of frequencies. This

is expected as there is no cyclic repetition in the noise and the correlation factor remain roughly the same everywhere. The fading at the ends are likely because we are taking finite bandwidth.

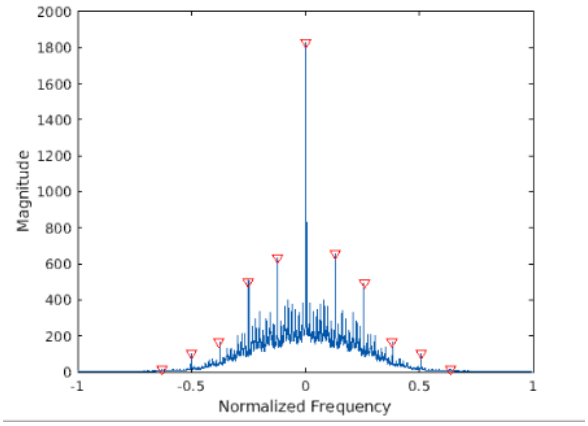

Fig. 4. Sum Non-conj SSCA Feature of the Zigbee Protocol

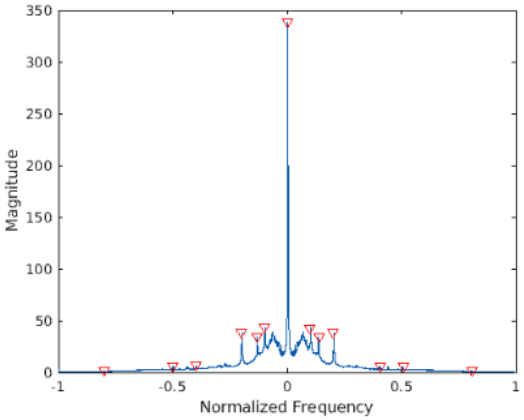

Fig. 5. Sum Non-conj SSCA Feature of the Frequency Hopper

3.2.3 SSCA Similarity Comparison. Given a new signal IQs, we need to firstly extract its SSCA features and then compare it with all the templates we have. Here are the detailed steps to accomplish it:

(1) Compute the sum non-conj feature of the unknown signal. For each template,
   (a) Find the largest values within *range_begin* and *range_end*. Take it as the peak.
   (b) Compute the l2-norm of the extracted peaks with the template peaks.
(2) Classify the unknown signal to the group that has the smallest distance.

Fig. 9 and 10 shows the comparison of Zigbee template to a Zigbee and Frequency Hopper testing data, respectively. The red triangles stand for the template while the green triangles are the peaks extracted from the testing data. It is clear that the peaks of the Frequency Hopper is more "far away" from the template.

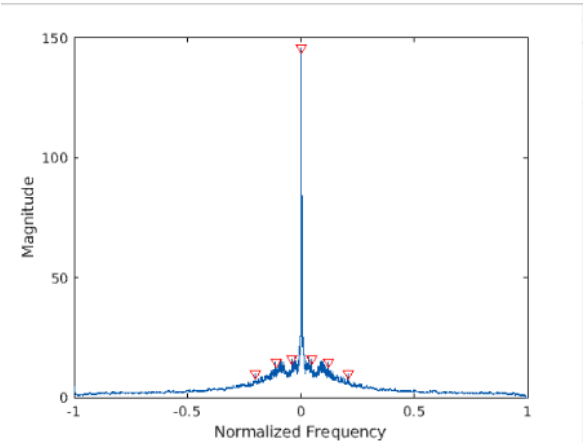

Fig. 6. Sum Non-conj SSCA Feature of the Example Protocol

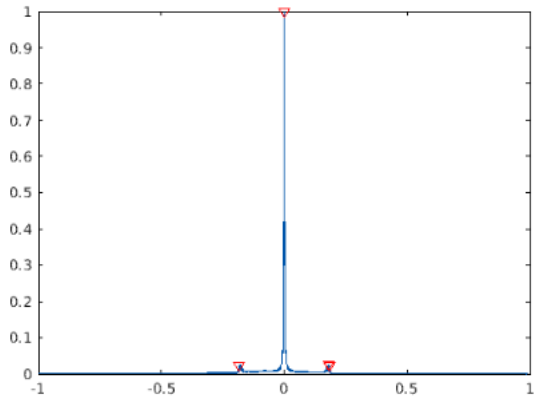

Fig. 7. Sum Non-conj SSCA Feature of the Lora Protocol

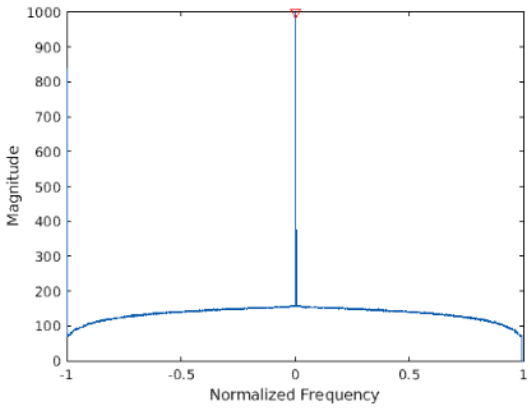

Fig. 8. Sum Non-conj SSCA Feature of the Noise

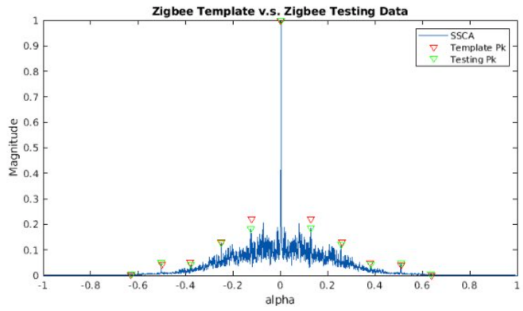

Fig. 9. Zigbee Template and OTA Testing Zigbee SSCA

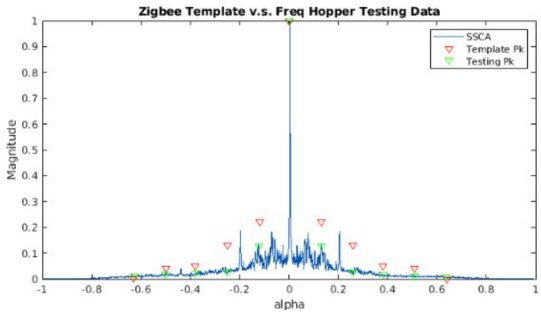

Fig. 10. Zigbee Template and OTA Testing Frequency Hopper SSCA

Fig. 11 shows the similarity distance of different signals when compared with the Unaltered Zigbee template. The Zigbee has the lowest distance while others have higher. If we threshold at 0.1, we can get the following promising results that separates LPIs and different protocol-bind signals:

$$TPR\_zigbee = 87.65\%$$
$$FPR\_noise = 0.00\%$$
$$FPR\_example = 2.74\%$$
$$FPR\_freq\_hopper = 8.88\%$$
$$FPR\_lora = 0.00\%$$
$$FPR\_single\_carrier = 0.44\%$$

3.2.4 SSCA and Altered Signal. Theoretically, the SSCA features of altered/mimick and normal signals should be identical as long as important cyclic features such as sampling rate are not changed. However, we do observe a shift in the similarity distance as the alteration power increases.

Fig. 12 shows the similarity distance of the Zigbbe of different alteration power when compared with the template of unaltered Zigbee. As the alteration power increases, the distance shifts right, getting less similar to the template.

How the observation can be used towards the detection of malicious signals remains unclear will be researched in the future.

3.3 PSD Reveals the Potential Problem in Data Collection

In an attempt to use PSD as side features to assist the classification, we found the misalignment of the PSD collected by Searchlight. Fig. 13 and 14 show the PSDs of Zigbee (collected using GNURadio) and Example (collected using Searchlight) protocol. The PSDs are all calculated with reference to the sampling frequency given in the metadata of the data collection. Although the Zigbee PSDs appear to be reasonable, the Example PSDs suffer from misalignment and long tails on the right. This is probably due to the inaccurate Boxing techniques used by Searchlight. As the estimated sampling frequency and center frequency is not accurate, it may lead to the misalignment in the PSD. It also causes potential problem to the SSCA features which is normalized to the sampling frequency. It may lead to shifts in the SSCA peaks.

4 CONCLUSION

Overall, this project aims at fixing the wireless security breaches caused by Altered and Mimick attack by using SSCA features. The testing within a small set of protocols shows that it can easier distinguish from noise and LPIs, as well as classify different protocols. However, the PSDs shows that the data collected so for is not fully reliable. The collection tool Searchlight gives inaccurate metadata, which potentially lead to shifts in the SSCA feature. Therefore, the integrity of the data collected so far needs to be examined and a better data collection method is needed.

5 ACKNOWLEDGEMENT

This work is part of SCISRS Phase 2 Project from WCSNG Research Group. I want to express my gratitude to Professor Dinesh Bharadia, Professor Fred Harris, and my lab colleagues Gavin Roberts, Hadi Givehchian, Isamu Poy, Radhika Mathuria, Hari Prasad, Raghav Subbaraman, Raini Wu, Richard Bell, Sreevatsank Kadaveru, Jiaming Jin, Dr. Srivatsan Rajagopal, and Dr. Wei Sun.

REFERENCES

[1] L. Izzo and A. Napolitano, "The higher order theory of generalized almost-cyclostationary time series," *IEEE Transactions on Signal Processing*, vol. 46, no. 11, pp. 2975–2989, 1998. DOI: 10.1109/78.726811.

[2] C. Spooner, *A high-level block diagram for the strip spectral correlation analyzer (ssca) method of exhaustive spectral correlation function (scf) estimation. the ssca produces NN' point estimates of the scf with resolution in frequency of $1/N'$ and resolution in cycle frequency of $1/N$. the spacing of the estimates is such that no significant slice (fixed cycle frequency, variable frequency) is missed.* https://cyclostationary.blog/2016/03/22/csp-estimators-the-strip-spectral-correlation-analyzer/, Accessed: 26-Jan.-2024, 2016.

[3] F. Meng, P. Chen, L. Wu, and X. Wang, "Automatic modulation classification: A deep learning enabled approach," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 10 760–10 772, 2018. DOI: 10.1109/TVT.2018.2868698.

[4] Z. Zhang, H. Luo, C. Wang, C. Gan, and Y. Xiang, "Automatic modulation classification using cnn-lstm based dual-stream structure," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13 521–13 531, 2020. DOI: 10.1109/TVT.2020.3030018.

[5] R. Bell, K. Watson, T. Hu, I. Poy, F. Harris, and D. Bharadia, "Searchlight: An accurate, sensitive, and fast radio frequency energy detection system," in *MILCOM 2023 - 2023 IEEE Military Communications Conference (MILCOM)*, 2023, pp. 397–404. DOI: 10.1109/MILCOM58377.2023.10356230.

[6] M. Wang, H. Jia, S. Wu, X. Hu, C. Jiang, and W. Zhang, "Res-gan for behavioral modeling and pre-distortion of power amplifiers in ofdm-based satellite communication system," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 2, pp. 2132–2141, 2024. DOI: 10.1109/TVT.2023.3315016.

[7] C.-Y. Huan and A. Polydoros, "Likelihood methods for mpsk modulation classification," *IEEE Transactions on Communications*, vol. 43, no. 2/3/4, pp. 1493–1504, 1995. DOI: 10.1109/26.380199.

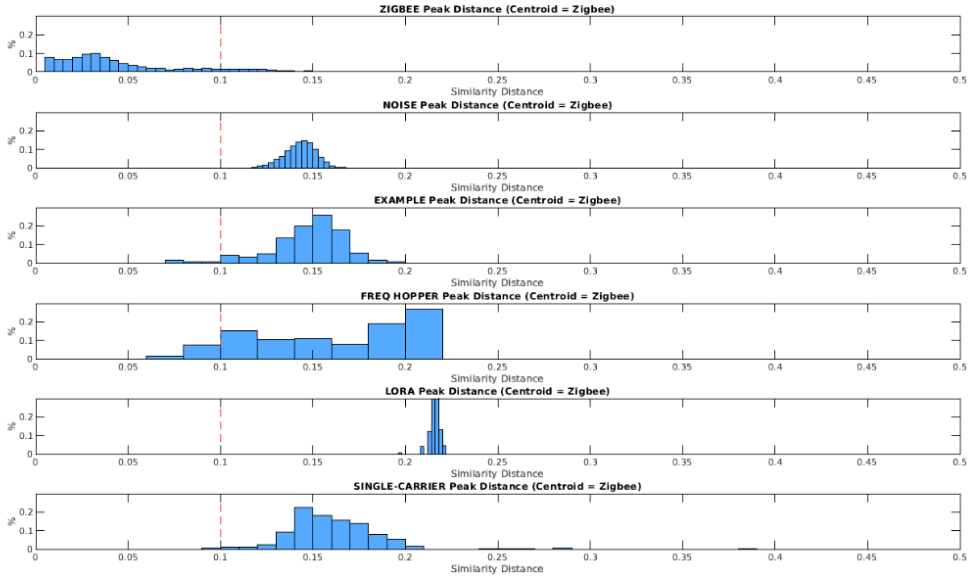

Fig. 11. Similarity of Different Signals Compared with the Zigbee Unaltered Template

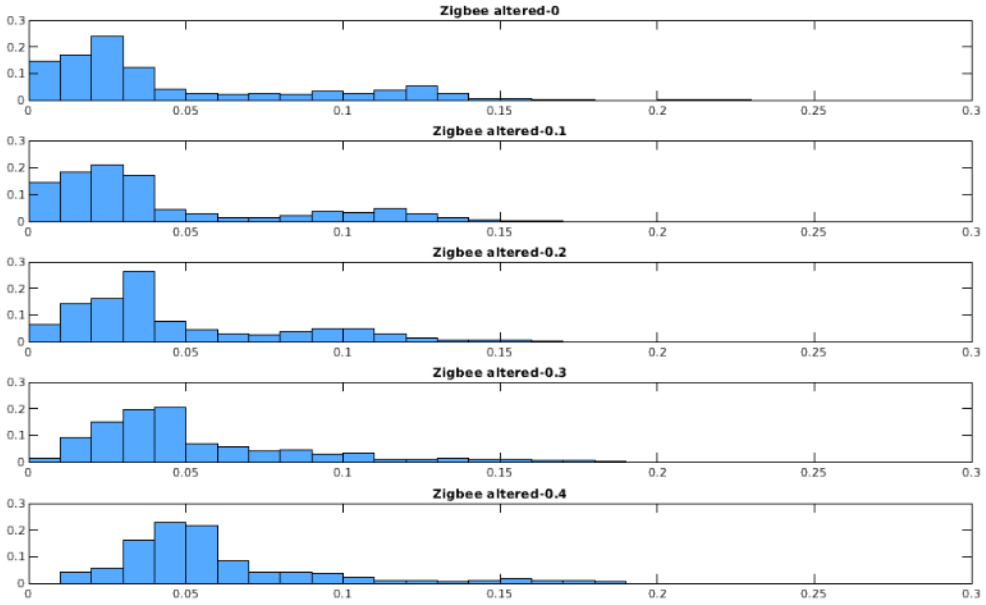

Fig. 12. Similarity Distance Distribution of Zigbee of Different Alteration Power

[8] D. Boiteau and C. Le Martret, "A general maximum likelihood framework for modulation classification," in *Proceedings of the 1998 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP '98 (Cat. No.98CH36181)*, vol. 4, 1998, 2165–2168 vol.4. DOI: 10.1109/ICASSP.1998.681575.

[9] J. L. Xu, W. Su, and M. Zhou, "Likelihood-ratio approaches to automatic modulation classification," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 41, no. 4, pp. 455–469, 2011. DOI: 10.1109/TSMCC.2010.2076347.

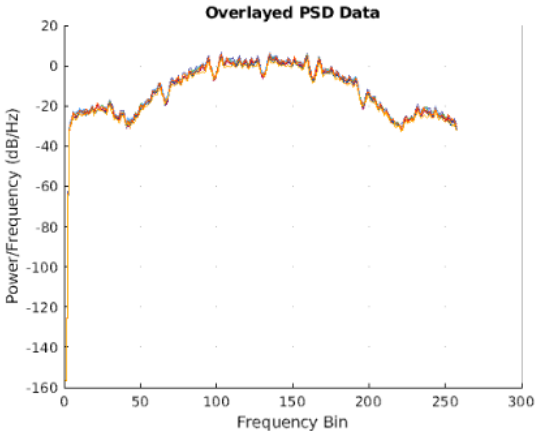

Fig. 13. 10 PSD Sequences of the Zigbee

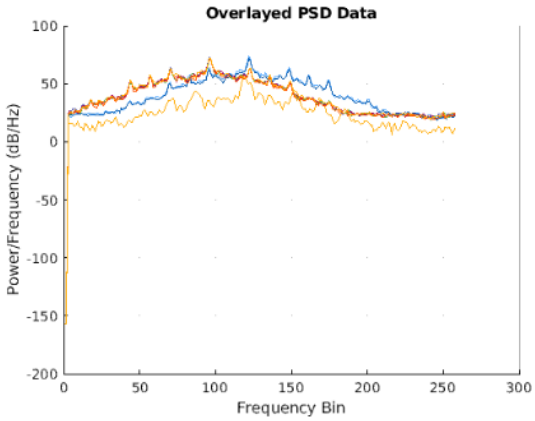

Fig. 14. 10 PSD Sequences of the Example Protocol

[10] T. Huynh-The, Q.-V. Pham, T.-V. Nguyen, *et al.*, "Automatic modulation classification: A deep architecture survey," *IEEE Access*, vol. 9, pp. 142 950–142 971, 2021. DOI: 10.1109/ACCESS.2021.3120419.

[11] GNU Radio Project, *Gnu radio – the free & open source radio ecosystem*, https://www.gnuradio.org/, Accessed: 2024-03-22, 2024.

[12] R. Bell, K. Watson, T. Hu, I. Poy, F. Harris, and D. Bharadia, "Searchlight: An accurate, sensitive, and fast radio frequency energy detection system," in *MILCOM 2023 - 2023 IEEE Military Communications Conference (MILCOM)*, 2023, pp. 397–404. DOI: 10.1109/MILCOM58377.2023.10356230.