QR Code

DO NOT REMOVE

SMARTSAT COOPERATIVE RESEARCH CENTRE

RMIT UNIVERSITY

Adversarial Detection using Deep Learning

Michael Aygur and Kandeepan Sithamparanathan

Introduction

Satellite communication (SATCOM) has enabled global connectivity through various types of satellite constellations. This technology has been widely used in commercial applications for facilitating satellite internet, global positioning, and Earth observation while Defence administrations maintain and command their own satellite fleet for use in military operations. Cybersecurity and physical layer security are used to protect Defence satellite-to-ground and ground-to-satellite networks against unauthorized personnel. Threats to both commercial and defence satellite networks can exist in the form of jamming with an objective of deny accessing or limiting the throughput of the network [1].

Aims

The research project objective is to investigate mitigation strategies to inhibit jamming efforts whilst maximising the achievable throughput and capacity. The project aims to develop advanced physical layer security algorithms and strategies, suitable for defence SATCOM systems. To accomplish this, development of adversarial detection and prediction techniques is required.

Methods

Convolutional neural networks (CNN) have been used for adversarial detection in this research project due to its known image detection capabilities [2]. The features of the proposed CNN consists of power from Inmarsat downlink broadband global area network (BGAN) spectrogram images generated using the short-time Fourier transform (STFT). Additional features will be identified later using advanced signal processing including (but not limited to) [2], [3]. The spectrogram was generated using red-green-blue (RGB), RGB-to-grey, and grey colouring schemes. Combining the CNN detector with another machine learning agent for prediction is next to come.

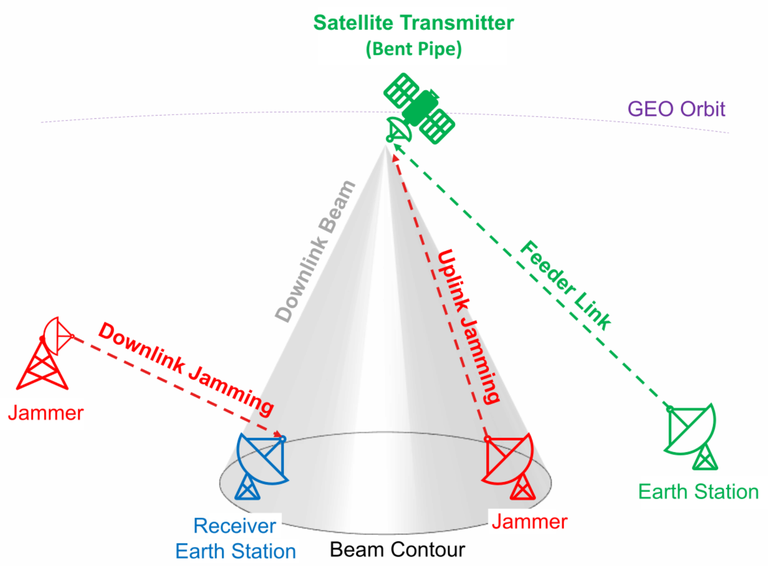

Figure 1: SATCOM Scenario Under Adversarial Attack

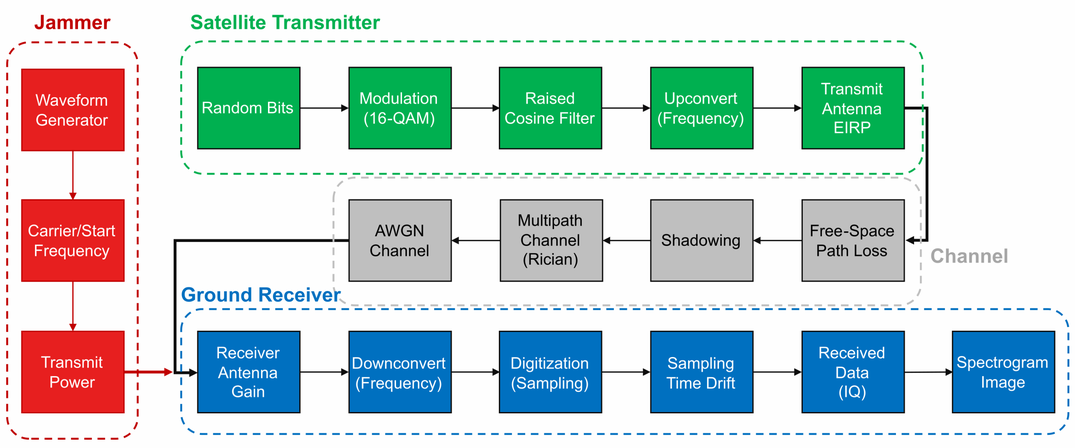

Figure 2: SATCOM Downlink System Model

Results

The SATCOM downlink scenario is described in Figure 1 along with the system model in Figure 2. The downlink system model is operating between 1518-1559 MHz (L-band). Real-world Inmarsat BGAN signals were also measured and saved as spectrogram images using the STFT with minimum power bounds of 15 and 20 dB below the maximum received power.

Three CNNs were trained using the architecture presented in Figure 3. CNN1 requires a 3 channel (RGB) image, CNN2 requires a 1 channel (RBG-to-grey) image, and CNN3 requires a 1 channel (grey) image. The image is passed through the CNN with the most likely classification among the six classifications being outputted at the end.

The CNN accuracy for the training (validation), testing, swapped dataset (RBG-to-grey and grey), real-world measured, and real-world measured swapped dataset (RBG-to-grey and grey) are shown in Table 1. Receiver operating characteristic (ROC) curves and area under the curve (AUC) were generated, with CNN2 yielding slightly better performance. Our results show high performance for both simulated and practical cases using only IQ power values. We are aiming for greater performance using more advanced features.

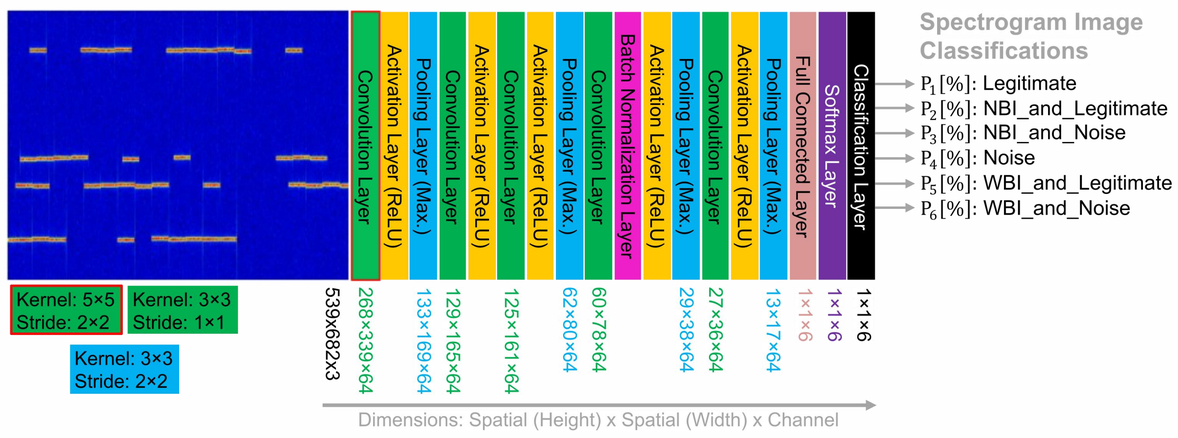

Figure 3: Characteristics for Adversarial Detection CNN Architectures

Table 1: CNN Accuracy under Different Dataset Conditions

Applied Dataset	CNN1	CNN2	CNN3
Training (Validation)	97.21%	98.11%	96.40%
Testing	97.10%	97.99%	96.59%
Swapped Grey Testing	-	15.68%	87.78%
Real-World 15 dB | 20 dB	59.52% | 85.88%	0% | 0%	1.14% | 3.26%
Real-World Swapped Grey	-	-	90.92% | 96.79%

References

[1] F. Fourati and M. -S. Alouini, "Artificial intelligence for satellite communication: A review," in Intelligent and Converged Networks, vol. 2, no. 3, pp. 213-243, Sept. 2021, doi: 10.23919/ICN.2021.0015.

[2] H. Elyousseph and M. L. Altamimi, "Deep Learning Radio Frequency Signal Classification with Hybrid Images," 2021 IEEE International Conference on Signal and Image Processing Applications (ICSIPA), Kuala Terengganu, Malaysia, 2021, pp. 7-11, doi: 10.1109/ICSIPA52582.2021.9576786.

[3] Y. Wei, S. -R. Ou-Yang, C. Li, Q. Liu and Y. -B. Qian, "Hierarchical Jamming Recognition with Spectrum Fusion Feature and Twin-bound SVM for Cognitive Satellite Communications," 2023 IEEE Wireless Communications and Networking Conference (WCNC), Glasgow, United Kingdom, 2023, pp. 1-6, doi: 10.1109/WCNC55385.2023.10119124.

Australian Government Department of Industry, Science, Energy and Resources

AusIndustry Cooperative Research Centres Program