On Jamming Detection: A Unified Method for Real-Time Detection Across Multiple Protocols & Attack Types

Alexandros I. Papadopoulos *†, Konstantinos Nikiforidis*, Odysseas Grosomanidis*, Eleni Chamou*,
Savvas I. Raptis *‡, Aristeides D. Papadopoulos *, Antonios Lalas*, Konstantinos Votis*,
*Information Technologies Institute, Centre for Research and Technology Hellas (CERTH), Greece
†Computer Science and Engineering Department, University of Ioannina, Greece
‡School of Electrical and Computer Engineering, Aristotle University of Thessaloniki, Greece
alexpap@iti.gr,lalas@iti.gr

***Abstract*—Jamming attacks continue to pose a significant threat to next-generation wireless networks, including Beyond 5G (B5G) and 6G, by disrupting communication through intentional interference. In this paper, we introduce JAmming detection method baSed on Modulation scheme IdeNtification and Outlier Detector of un-jammed data (JASMIN), a novel jamming detection method designed to operate effectively across a broad range of network protocols and jamming scenarios. JASMIN relies solely on unjammed data during its training phase and utilizes two primary components in its detection phase: a Modulation Scheme Identification (MSI) model that classifies the legitimate signal's modulation format, and an Outlier Detector (OD) that quantifies channel noise. By comparing the predicted modulation scheme over multiple time windows with the OD's measurements of noise, JASMIN identifies abnormal interference that indicates the presence of jamming—regardless of the specific jamming strategy (e.g., constant, periodic, reactive). We demonstrate the efficacy of JASMIN on an SDR-based testbed implementing an IEEE 802.11p (V2X) communication network, employing three USRP B210 devices operating at 5.9 GHz. Evaluation results show an overall accuracy of 99.92% under a wide range of SNR levels. Additionally, JASMIN's real-time compatibility and minimal computational overhead make it a compelling solution for modern wireless systems. To foster further innovation, we publicly release the dataset utilized in our experiments.**

***Keywords*—Jamming Detection, SDR, V2X, Datasets**

I. Introduction

The advent of Beyond 5G (B5G) and 6G networks marks a significant advancement in communication technologies, offering ultra-low latency, enhanced bandwidth, and high-speed connectivity. These networks are tailored to meet the demands of advanced applications such as autonomous driving, wireless power transfer, and extended reality. However, despite progress across various layers of communication, vulnerabilities in the physical layer pose a critical risk, potentially undermining the transformative potential of these technologies. Among physical-layer threats, jamming attacks stand out as both highly effective and challenging to counteract. These attacks disrupt communication by introducing interference on the same frequency as the target signal, and they manifest in three primary forms with distinct characteristics.

Constant jamming, the simplest form, involves continuous high-power interference across the transmission bandwidth, causing a significant reduction in the Signal-to-Noise Ratio (SNR). Its simplicity makes it easy to implement and, simultaneously, highly disruptive to network operations. In contrast, periodic jamming introduces interference at regular intervals, allowing brief periods of normal communication. This approach can exploit timing vulnerabilities in the network and demands precise synchronization with the target signal. Its intermittent nature complicates detection, as it may mimic normal network fluctuations and appear less conspicuous. Reactive jamming represents the most sophisticated type of attack. It transmits interference only when legitimate signals are detected, thereby conserving energy and enabling targeted disruptions. This approach remains passive until legitimate transmissions occur, making it particularly difficult to detect and requiring advanced mechanisms to pinpoint the source of interference.

The timely and accurate detection of jamming attacks is critical for the implementation of effective countermeasures, ensuring the performance and security of networks, especially in the domain of autonomous vehicles. To address this issue, various detection techniques have been proposed in the literature. Advanced artificial intelligence (AI) models, such as Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, Random Forest, and XGBoost [1]–[5], have demonstrated significant potential in detecting jamming attacks across diverse network performance scenarios. Despite these advances, existing methods lack universal effectiveness, particularly against sophisticated jamming techniques like periodic and reactive jamming. Furthermore, many approaches rely on training datasets that are not readily available from real-world systems, limiting their adaptability to specific channel conditions. In order to overcome these limitations, we propose JAmming detection method baSed on Modulation scheme IdeNtification and Outlier Detector of unjammed data (JASMIN), a novel jamming detection method designed to address all types of jamming attacks. JASMIN is agnostic in respect of the used communication protocol and central operating frequency and eliminates the dependency on jamming data during the training phase.

In this context, our research contributions are as follows:

- We propose and introduce JASMIN, a novel jamming detection method capable of achieving high detection accuracy across various communication protocols.
- We evaluate the proposed method using a physical,

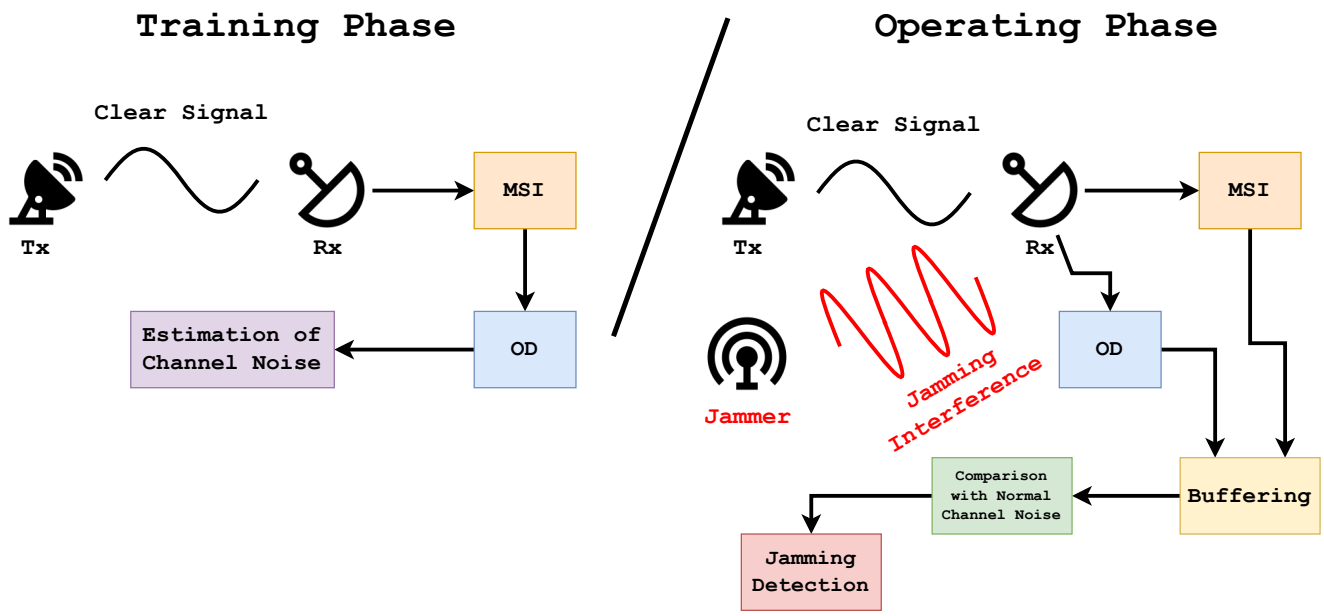

Fig. 1: The training (left) and the operating phase (right) of the JASMIN method

software-defined radio (SDR)-based setup that emulates a Vehicle-to-Everything (V2X) testbed.

- We publicly release the training and evaluation data to foster collaboration and further advancements in the field.

The rest of this paper is organized as follows. Section II presents an overview of related studies. In Section III, we detail the workflow of the proposed method. Section IV describes the SDR-based setup and the generated data used for training and evaluation purposes. In Section V, we explain the process of fine-tuning the components of JASMIN using un-jammed data. Section VI evaluates the performance of the proposed method in detecting jamming attacks. Finally, Section VII provides concluding remarks and insights derived from this study.

II. Related Studies

The proposed jamming detection method relies on the receiver's ability to identify the modulation scheme used by the transmitter. Consequently, we review the current state of the art in both modulation scheme identification (MSI) and jamming detection techniques. Furthermore, we provide the accuracy levels of existing methods as a benchmark to evaluate the performance of our solution. As concernts MSI, various neural network architectures have been applied achieving high accuracy across diverse SNR conditions. For example, a ResNet model with six residual blocks was trained on a combination of real and synthetic datasets covering 24 modulation schemes, attaining 99.8% accuracy for SNRs above 10 dB and maintaining 90% accuracy near 0 dB [6]. Alternatively, a CNN with custom layers designed for Automatic Modulation Classification was trained on synthetic data with varying SNR levels using a two-step pre-training and fine-tuning process. This CNN-based model achieved 100% accuracy for SNRs exceeding 4 dB and retained 70% accuracy close to 0 dB [7].

In addition to CNNs and ResNets, LSTM networks have been effectively utilized for this task. One such model consists of three stacked LSTM layers followed by four fully connected layers, trained on the In-phase and quadrature (I/Q) samples of signals under various noise conditions. This LSTM architecture delivers 98% accuracy for SNRs above 12 dB and sustains 60% accuracy as the SNR approaches 0 dB [8]. Another LSTM-based approach employs a two-layer configuration with 128 units, trained on amplitude and phase inputs using the RadioML2016.10a synthetic dataset. This model demonstrates an average accuracy of 90% across an SNR range from 0 to 20 dB, highlighting its robustness in varying noise environments [9]. A variety of machine learning and deep learning techniques have also been effectively utilized for jamming detection, consistently achieving high accuracy across different scenarios. One method employs features such as bad packet ratio, received signal strength, and clear channel assessment, utilizing algorithms like Random Forest, SVM, and MLP to reach 97.5% accuracy [1]. Another approach leverages channel and performance metrics, including Noise and Channel Busy Ratio and Packet Delivery Ratio, with Random Forest classifiers achieving over 95% accuracy [2].

Advanced deep learning models further enhance jamming detection performance. For instance, two-layer LSTM networks using Quality of Services (QoS) metrics attain 95.5% accuracy [3]. Shallow feed-forward neural networks that incorporate delivery rate and SNR metrics have demonstrated accuracies between 95% and 99% [4]. Additionally, combining statistical features with algorithms like XGBoost and LightGBM achieves up to 99% accuracy [10]. Convolutional approaches utilizing spectrograms with CNNs and conventional encoders identify jammed cases through significantly higher reconstruction errors, while autoencoders processing I/Q components achieve 99.7% accuracy [5], [11]. These studies underscore the robustness of both traditional machine learning and deep learning techniques in detecting jamming under various conditions. In several studies, the datasets include

jamming signals generated by reactive jammers, simulating more realistic and dynamic interference patterns. For example, the method proposed in [2] specifically addresses both constant and reactive jammers in 802.11 networks, achieving over 94% accuracy even in outdoor mobile scenarios. Moreover, some works [12] extend beyond detection to classify the type of jamming attack, such as distinguishing between constant and smart (reactive) jammers.

Building on existing knowledge, we propose a method designed to achieve high effectiveness and accuracy across all types of jamming attacks while being applicable to all communication protocols. The workflow of JASMIN is depicted in Fig. 1. During the training phase, the MSI module is trained across various SNR levels to reliably identify the modulation scheme employed by the transmitter (Tx). Concurrently, an Outlier Detector (OD) component is trained to quantify the noise introduced by the communication channel, thereby establishing a baseline profile for normal noise levels. In the operational phase, if interference caused by a jammer affects the signal received by the receiver (Rx) in any manner, the outputs of the MSI and OD modules are evaluated over a specific timeframe. If the Rx does not detect the same modulation scheme consistently during this period, or if the OD identifies a noise level exceeding the predefined normal threshold, a jamming attack is detected. The dual-decision process distinguishes true jamming from non-malicious disruptions like distance or non-line-of-sight conditions.

III. JASMIN: A Unified Method for Jamming Detection

JASMIN is designed to provide robust and accurate jamming detection in real-time across various network protocols, including those aimed at B5G and 6G applications. The method integrates two complementary modules—an MSI and an OD—which together form a two-stage decision process. A notable advantage of JASMIN is that it is trained solely on unjammed data, thereby avoiding the challenges associated with acquiring representative jamming datasets.

At its core, the MSI model (M) is responsible for determining the modulation scheme (e.g., BPSK, QPSK, 16-QAM, 64-QAM) of the received signal by analyzing sequences of I/Q samples. This module is typically implemented using a deep learning architecture which has been fine-tuned to handle varying SNR conditions while maintaining high classification accuracy. In normal operation, the MSI consistently identifies the modulation scheme employed by the transmitter. Complementing the MSI, the OD module is tasked with quantifying the channel noise through anomaly detection. For each supported modulation, a dedicated OD model $OD(m)$ is trained to capture the characteristic noise profile of unjammed signals. This involves computing metrics between the observed constellation points and those expected from an ideal, noise-free signal. During normal operation, the OD reports noise levels that remain within a well-defined baseline range.

In the operational phase, that is illustrated in Alg. 1, the receiver continuously buffers I/Q data over a preset time window (T) and, once enough data are accumulated, the MSI module generates multiple predictions (P). The prevalent modulation scheme is then determined from these predictions, and the corresponding OD model is employed to evaluate the noise level across successive data segments. The decision to trigger a jamming alert is based on two concurrent conditions:

Algorithm 1: Operating Phase of JAmming detection method baSed on Modulation scheme IdeNtification and Outlier Detector of un-jammed data (JASMIN)

Given:
  Pretrained MSI model M.
  Pretrained OD models $\{OD(m)\}$.
  Scaler function S.
  Time-window length T
  Number of predictions in sequence P.
Initialize: An empty data buffer $\mathcal{B}$.
while new I/Q samples are received **do**
  Append incoming samples to $\mathcal{B}$.
  Apply normalization: $\mathcal{B} \leftarrow S(\mathcal{B})$.
  if the size of $\mathcal{B}$ reaches $P \times T$ samples **then**
    Modulation Identification:
    for $i = 1$ to P **do**
      Let $\mathbf{x}^{(i)}$ be the i-th packet of T samples.
      Obtain the modulation prediction $m_i \leftarrow M(\mathbf{x}^{(i)})$.
    end for
    Determine the prevalent modulation scheme:

$$\hat{m} = \text{mode}\{m_1, m_2, \ldots, m_P\}.$$

    Calculate the consistency ratio:

$$\gamma = \frac{\text{Number of packets with } m_i = \hat{m}}{P}.$$

    Outlier Analysis:
    for $i = 1$ to P **do**
      Compute the outlier label for packet $\mathbf{x}^{(i)}$ using $OD(\hat{m})$:

$$\ell_i \leftarrow OD\big(\hat{m}, \mathbf{x}^{(i)}\big),$$

      where $\ell_i = 1$ indicates a normal (unjammed) packet and $\ell_i = -1$ indicates an anomalous (potentially jammed) packet.
    end for
    Aggregate the outlier labels:

$$L = \text{mode}\{\ell_1, \ell_2, \ldots, \ell_P\}.$$

    Decision Rule:
    if $\gamma < 1$ **or** $L = -1$ **then**
      Set `jamming_detection` $\leftarrow True$
    else
      Set `jamming_detection` $\leftarrow False$
    end if
    Reset $\mathcal{B}$ for the next batch.
  end if
end while

(i) if the MSI predictions are inconsistent over the observation window, or (ii) if the OD detects noise levels significantly above the normal baseline. Meeting either of these criteria results in a flagging of the current data batch as potentially jammed.

This approach has several clear advantages. First, because it does not depend on predefined jamming signatures or protocol-specific features, JASMIN can be applied across many communication standards. Second, training exclusively on unjammed data simplifies deployment in environments where jammed signals are rare or unavailable. Moreover, using two independent yet complementary detection methods boosts overall robustness; if one module fails to detect an attack,

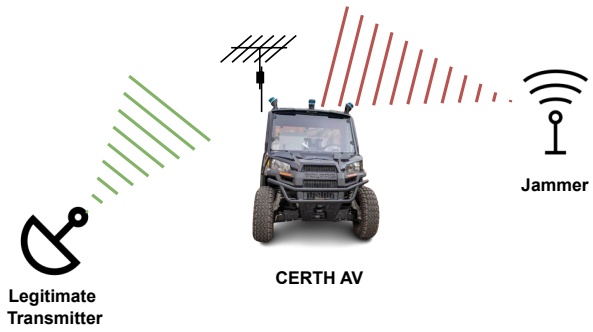

Fig. 2: Simulated scenario by SDR-setup.

the other can still identify it. Finally, the efficient design and optimal parameter tuning allow JASMIN to generate thousands of predictions per second, meeting the demands of real-time security in dynamic wireless settings.

IV. Experimental Setup & Data Collection

JASMIN is evaluated within the IEEE 802.11p protocol [13], which is specifically designed for V2X networks. The physical layer implementation employs three SDRs: one as the base station, one representing the autonomous vehicle, and one functioning as the jammer mainly simulated the scenario illustrated in Fig. 2. These SDRs are primarily USRP B210 devices[1], equipped with omnidirectional antennas operating at 5.9 GHz. Each USRP connects to a host computer via USB 3.0 and is configured using GNU Radio[2]. The host computers are NVIDIA Orin Jetson units[3], selected for their high performance, energy efficiency, and compatibility with GNU Radio's Linux-based signal processing framework. These units manage critical SDR tasks, including real-time signal processing, modulation, demodulation, and jamming detection.

The transmitter and receiver simulations are based on WiMe [14]. The jammer replicates the transmitter flowgraph, injecting white Gaussian noise with amplitude similar to the transmitter to mimic interference. Detecting the jammer under these conditions ensures straightforward identification of stronger interference typical in jamming attacks. The transmitter employs OFDM with BPSK, QPSK, 16-QAM, and 64-QAM modulation. Captured signals at the receiver are stored via API into a shared database, enabling post-processing and jammer detection model training. To ensure generalization, GNU Radio dynamically varies transmitter, receiver, and jammer distances. Transmission occurs under both jammed and unjammed scenarios across all modulation schemes. The UDP listener handles data packets limited to 128 I/Q sample pairs.

A summary of the data is provided in Table I including the number of packages and SNR levels' description. For the clear signal data, captured during both training and evaluation, a wide range of SNR levels is observed, including also negative values. This ensures that the dataset effectively simulates scenarios where the communication link experiences significant noise without the presence of a jamming attack. Regarding the jamming attack data, the system is evaluated under a combination of reactive and periodic jamming. Specifically, the jammer activates as soon as the receiver begins detecting the transmitter's signal and operates with a periodicity matching that of the transmitter. This behavior results in packets with highly positive SNR values, reflecting the jamming impact on the communication link. The dataset is publicly available on Zenodo[4].

[1]https://www.ettus.com/all-products/ub210-kit/

[2]https://www.gnuradio.org/

[3]https://www.nvidia.com/en-eu/autonomous-machines/embedded-systems/jetson-orin/

V. Fine Tuning of JASMIN Components

As previously noted, JASMIN comprises two primary components: the MSI and the OD. Before deploying JASMIN for a specific protocol, the training phase must be conducted. During this phase, the AI tools selected by the network operator are configured and fine-tuned according to the characteristics of the protocol and normal data. This preparation ensures that JASMIN is optimally adapted for effective operation within the designated network environment. In our case, we have selected an LSTM model for MSI and the Isolation Forest (IF) as OD. The tools are fine-tuned based on the data extracted by the SDR-based setup, fully described in Sec. IV.

A. MSI model

As already mentioned, the selected AI tool for the MSI is an LSTM model. It is designed for sequence classification tasks and operates on input sequences with a shape of (128, 2), representing a data package of I/Q samples. The LSTM consists of 128 units to learn temporal dependencies in the data, followed by a dropout layer with a rate of 0.5 to reduce overfitting. The output layer is a dense layer with a softmax activation function for multi-class classification. The model is trained using the categorical cross-entropy loss function, the Adam optimizer, and accuracy as the evaluation metric. Training is performed over 100 epochs, with early stopping employed to halt training when the validation performance stops improving. Figure 3 displays the confusion matrix for the MSI, while Table II summarizes the performance metrics and accuracy for each modulation scheme. The MSI achieves high accuracy across all schemes. The model achieves high accuracy (overall: 97.57%), performing robustly even at low SNR (BPSK: -1.2 dB, QPSK: -17.3 dB, 16-QAM: -28.24 dB, 64-QAM: -15.16 dB). At SNR below 0 dB, accuracy (75%) aligns with existing literature; above 0 dB, accuracy reaches 99.5%. The model remains lightweight and efficient.

B. Outlier Detector

An IF is employed as the primary outlier detector for jamming identification. The IF is trained exclusively on normal data to learn the typical noise characteristics of each modulation scheme, and once trained, it flags any samples with noise levels significantly deviating from these norms as potential jamming attacks. To assess how closely the received I/Q samples match the expected constellation points, the relative square error (RSE) is computed as follows:

$$\mathrm{RSE} = \frac{\sum_{i=1}^{N} \left(y_i - \hat{y}_i\right)^2}{\sum_{i=1}^{N} \left(y_i - \bar{y}\right)^2}$$

In this equation, the term $\left(y_i - \hat{y}_i\right)^2$ represents the squared distance between the observed sample and its nearest point in the ideal constellation of each modulation scheme, while $\left(y_i -\right.$

[4]https://doi.org/10.5281/zenodo.15145234

TABLE I: Summary of the training & evaluation data

Modulation	Clear Signal					Jamming Signal				
	Num of Packages	Mean SNR (dB)	Var SNR (dB)	Max SNR (dB)	Min SNR (dB)	Num of Packages	Mean SNR (dB)	Var SNR (dB)	Max SNR (dB)	Min SNR (dB)
Training Data										
BPSK	7617	15.12	17.93	18.88	−1.2					
QPSK	12 775	14.93	25.21	23.44	−17.34					
16-QAM	9188	13.85	30.12	23.64	−28.21					
64-QAM	3876	11.29	27.52	19.6	−15.16					
Evaluation Data										
BPSK	2539	15	17.76	18.47	−6.83	8465	−5.59	22.4	18.94	−52.82
QPSK	4259	15.1	25.01	22.41	−16.36	9098	−2.34	27.68	19.6	−51.31
16-QAM	3063	14.16	30.12	23.35	−25.43	16 539	−5.89	24.64	22.47	−51.84
64-QAM	1292	10.95	27.49	19.11	−14.47	22 978	−6.97	19.72	19.4	−50.71

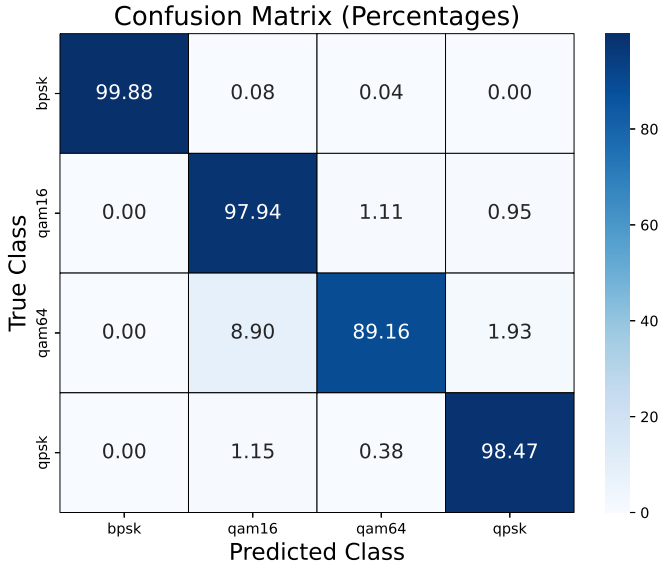

Fig. 3: Confusion Matrix of MSI (%)

TABLE II: Modulation Scheme Identification Results

Modulation Scheme	Precision	Recall	F1-Score	Accuracy
BPSK	1.0000	0.9988	0.9994	-
QAM16	0.9476	0.9794	0.9632	-
QAM64	0.9576	0.8916	0.9234	-
QPSK	0.9873	0.9847	0.9860	-
Macro Avg	0.9731	0.9637	0.9680	-
Weighted Avg	0.9758	0.9757	0.9756	-
Overall Results	**0.9758**	**0.9757**	-	**97.57%**

$\bar{y})^2$ quantifies the squared distance from the observed sample to the average point of the packet. Packets, each consisting of 128 samples, are analyzed using this measure, and empirical results indicate that an RSE below 0.1 is generally associated with unjammed packets.

The proportion of packets with an RSE exceeding 0.1 is utilized to set the contamination parameter in the IF, which reflects the assumed fraction of outliers in the training data. This parameter is adapted to each modulation scheme based on the observed outlier rates: while lower rates are seen with schemes like BPSK (0.12%), higher modulation orders such as QAM16 and QAM64 exhibit rates of 14.56% and 25.15%, respectively, with QPSK observing a moderate rate of 5.64%.

Each IF model is trained on packets comprising 128 constellation points where each point is described by its real and imaginary parts, yielding an initial shape of $(128, 2)$. However, a point-wise Manhattan distance is computed to transform these points into an input feature with a shape of $(128, 1)$. This approach was adopted without decoupling the real and imaginary components, and because the various constellations are symmetric, the reduction of points to the first quadrant simplifies the procedure. In particular, for BPSK packets, only the real component is used. To further enhance the training process, random intra-packet point permutations are employed as an augmentation strategy, acknowledging that jamming detection is primarily influenced by the spatial location of the constellation points rather than their order. The IF is implemented with 150 base estimators (trees), a configuration that ensures the model is well-tuned to detect anomalies based on the inherent noise and structural characteristics of the channel across different modulation schemes.

VI. Evaluation

To evaluate JASMIN, we use the second dataset, which contains both normal (clear) and jammed data for all supported modulation schemes. This dataset was not available during the training phase of the models. Also in this case, the clear signals were captured under various SNR levels, while the jammed signals were generated using a combination of reactive and periodic jamming attacks. In Alg. 1, we integrate the LSTM model, denoted as M, with the Isolation Forest for each modulation scheme, denoted as $OD(m)$. The time window T is set equal to the data package size of 128 I/Q samples, and the parameter P was fine-tuned and selected to be 21. Given that the receiver operates at 10 MHz, JASMIN can generate more than 3,500 predictions per second, thereby ensuring the physical security of the network. The scaler of the LSTM model is integrated as S.

When testing the outlier detection models on the jammed data, the percentages of outliers detected for each modulation scheme are as follows: 87.21% for BPSK, 76.19% for QPSK, 94.08% for QAM-16, and 96.52% for QAM-64. These figures indicate that the models are effective in anticipating the increased noise due to the presence of jamming.

Table III presents the performance metrics for each modulation scheme, showing that the model achieves perfect detection of jamming attacks in BPSK, 16-QAM, and 64-QAM. In

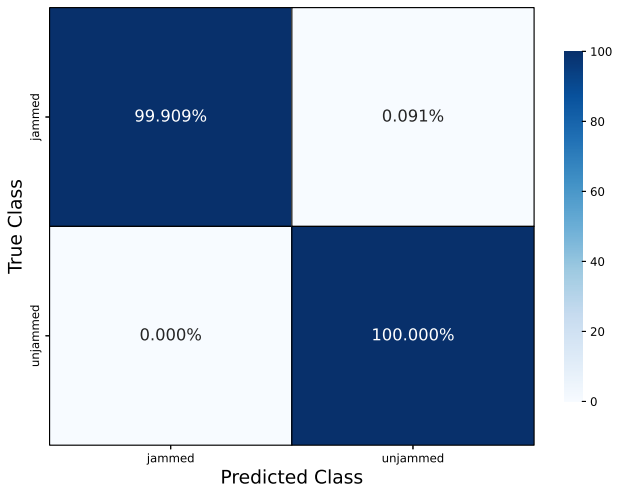

Fig. 4: Confusion Matrix of JASMIN (%)

TABLE III: JASMIN Results Per Modulation Scheme and Overall

Modulation	Class	Precision	Recall	F1-Score	Accuracy
BPSK	Clear	1.00000	1.00000	1.00000	**100%**
	Jammed	1.00000	1.00000	1.00000	
QPSK	Clear	0.98239	1.00000	0.99112	**99.63%**
	Jammed	1.00000	0.99536	0.99767	
16-QAM	Clear	1.00000	1.00000	1.00000	**100%**
	Jammed	1.00000	1.00000	1.00000	
64-QAM	Clear	1.00000	1.00000	1.00000	**100%**
	Jammed	1.00000	1.00000	1.00000	
Overall	Clear	0.99318	1.00000	0.99658	**99.92%**
	Jammed	1.00000	0.99909	0.99954	

the case of QPSK, the accuracy is slightly lower at 99.63%. Overall, the model exhibits a precision of 0.99318 for clear signals and 1 for jammed signals, with a recall of 1 for clear signals and 0.99909 for jammed signals, leading to an overall accuracy of 99.92%. Figure 4 presents the confusion matrix for JASMIN, which further underscores its high accuracy. Notably, only small portion of QPSK packages (76 out of 9098) were incorrectly labeled as clear signals when they were, in fact, subject to a jamming attack, and no clear signal package was mistakenly identified as jammed.

VII. Conclusion

This paper has introduced JASMIN, a unified jamming detection method capable of detecting a wide variety of attack strategies—constant, periodic, and reactive—while remaining agnostic to specific network protocols. By leveraging a two-stage decision process that integrates Modulation Scheme Identification (MSI) and a dedicated Outlier Detector (OD), JASMIN reliably discerns abnormal interference in real time without relying on jammed data for training. Our evaluation on an SDR-based IEEE 802.11p (V2X) testbed, comprising multiple USRP devices operating at 5.9 GHz, demonstrates the method's high effectiveness, achieving a detection accuracy of 99.92% across a broad range of SNR conditions. These results underscore the method's versatility and robustness, confirming its suitability for beyond-5G networks and other critical wireless systems. In an effort to encourage broader exploration of physical-layer security, we publicly release our dataset, inviting the research community to further refine and extend jamming defense strategies in modern communication infrastructures.

Acknowledgment

This work has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme, in the frame of the NATWORK project (Net-Zero self-adaptive activation of distributed self-resilient augmented services) under Grant Agreement No 101139285 and ULTIMO (Advancing Sustainable User-centric Mobility with Automated Vehicles) project under Grant Agreement No 101077587. In the context of the ULTIMO project, the primary components of the SDR setup have been installed to establish a realistic simulation environment for the V2X protocol, and AV applications. In the context of the NATWORK project, the methodology has been fully defined, and the tools have been fine-tuned and evaluated based on the SDR setup.

References

[1] Y. Arjoune *et al.*, "A novel jamming attacks detection approach based on machine learning for wireless communication," in *2020 International Conference on Information Networking (ICOIN)*, pp. 459–464, 2020.

[2] O. Punal *et al.*, "Machine learning-based jamming detection for ieee 802.11: Design and experimental evaluation," in *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, pp. 1–10, 2014.

[3] F. T. Zahra *et al.*, "Lstm-based jamming detection and forecasting model using transport and application layer parameters in wi-fi based iot systems," *IEEE Access*, vol. 12, pp. 32944–32958, 2024.

[4] E. Testi *et al.*, "Machine learning-based jamming detection and classification in wireless networks," in *Proceedings of the 2023 ACM Workshop on Wireless Security and Machine Learning*, WiseML'23, (New York, NY, USA), pp. 39–44, Association for Computing Machinery, 2023.

[5] M. Varotto *et al.*, "Detecting 5g signal jammers using spectrograms with supervised and unsupervised learning," *arXiv preprint arXiv:2405.10331*, 2024.

[6] T. J. O'Shea *et al.*, "Over-the-air deep learning based radio signal classification," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 1, pp. 168–179, 2018.

[7] F. Meng *et al.*, "Automatic modulation classification: A deep learning enabled approach," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 10760–10772, 2018.

[8] S. Hu *et al.*, "Robust modulation classification under uncertain noise condition using recurrent neural network," in *2018 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–7, 2018.

[9] S. Rajendran *et al.*, "Deep learning models for wireless signal classification with distributed low-cost spectrum sensors," *IEEE Transactions on Cognitive Communications and Networking*, vol. 4, no. 3, pp. 433–445, 2018.

[10] A. S. Ali *et al.*, "Rf jamming dataset: A wireless spectral scan approach for malicious interference detection." TechRxiv, November 11 2022.

[11] S. Sciancalepore *et al.*, "Jamming detection in low-ber mobile indoor scenarios via deep learning," *IEEE Internet of Things Journal*, vol. 11, no. 8, pp. 14682–14697, 2024.

[12] M. Murshed *et al.*, "Vehicular network security against rf jamming: An lstm detection system," *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, pp. 599–604, 2024.

[13] A. M. Abdelgader *et al.*, "The physical layer of the ieee 802.11 p wave communication standard: the specifications and challenges," in *Proceedings of the world congress on engineering and computer science*, vol. 2, pp. 22–24, 2014.

[14] B. Bloessl *et al.*, "Performance assessment of ieee 802.11.p with an open source sdr-based prototype," *IEEE Transactions on Mobile Computing*, vol. 17, pp. 1162–1175, 05 2018.