IEEE INFOCOM 2025 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) | 979-8-3315-4370-9/25/$31.00 ©2025 IEEE | DOI: 10.1109/INFOCOMWKSHPS65812.2025.11152922

Digital Twins for Identifying Jamming-prone Areas in Smart Cities

Sunday Amatare, Jiayi Meng, and Debashri Roy
Department of Computer Science and Engineering, The University of Texas at Arlington
Emails: {sunday.amatare, jiayi.meng, debashri.roy}@uta.edu

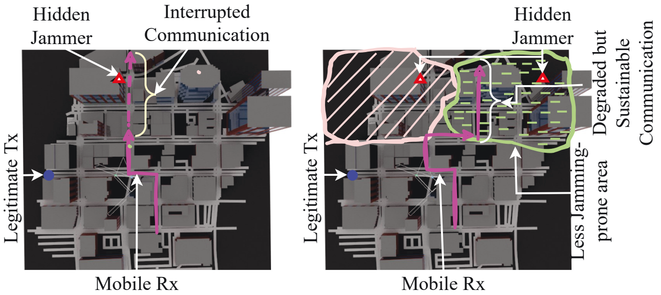
***Abstract*—Jamming attacks pose severe risks to smart cities in the 5G era and beyond, including economic losses and safety threats. Identifying jamming-prone areas within a city is essential for proactive planning and safeguarding the reliability of wireless networks. This paper introduces a novel approach for identifying jamming-prone areas in smart cities using ray-tracing (RT) within a digital twin (DT) framework. The methodology integrates Blender for scene creation, NVIDIA's Sionna RT for propagation modeling, and techniques for jamming identification and severity analysis across various areas of the environment. The results demonstrate the feasibility of this approach, illustrating how high-fidelity replication of real-world scenarios within DTs can effectively identify jamming-prone areas in smart cities. This work highlights the potential of the proposed framework as a reliable and efficient alternative for jamming identification, especially in contexts where privacy concerns or environmental constraints limit the applicability of traditional methods.**

***Index Terms*—Digital twin, Ray-tracing, Jamming Identification.**

I. Introduction

"Jamming-prone area identification" involves determining geographic locations where wireless signals are particularly susceptible to interference or jamming. This is often achieved by analyzing signal strength variations, comparing data from multiple receivers, and using sophisticated algorithms to pinpoint areas where jamming attacks are most likely to occur. These attacks can create significant challenges, including economic losses from operational downtime and potentially life-threatening situations. The issue is particularly critical in smart cities, where wireless communication serves as the backbone for efficient productivity, enabling the seamless integration of technologies, services, and human-robot collaboration. Hence, identifying areas vulnerable to signal interference would allow for the implementation of proactive measures to prevent disruptions and ensure the smooth operation of critical systems, such as GPS navigation, IoT networks, and autonomous vehicles [1].

Machine Learning (ML)-based Jamming Identification. In recent years, ML techniques have gained significant traction for jamming identification and detection due to their ability to handle complex patterns and anomalies in wireless communication systems. By analyzing features such as signal-to-noise ratio (SNR), received signal strength indicator (RSSI), spectral patterns, and packet delivery rates, ML techniques can effectively identify jamming activities. In supervised learning, models are trained on labeled data consisting of both normal and abnormal spectrograms, enabling the algorithm to classify signals and detect jamming effectively [2]. When labeled data is absent, unsupervised learning techniques, such as clustering algorithms, are employed to identify patterns in the data that may indicate jamming activities [3]. Additionally, deep learning techniques, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), along with reinforcement learning (RL), have been explored for their ability to learn from dynamic environments and improve detection over time [4]. The advancement of GPUs and computing technologies has significantly accelerated the adoption of ML approaches, enabling faster processing and improved detection in complex scenarios.



(a) Without the knowledge of a City's Jamming-prone areas

(b) With the knowledge of a City's Jamming-prone areas

Fig. 1. Illustrates the impact of communication without and with knowledge of a city's jamming-prone areas. In (a), a mobile receiver's communication is interrupted because it operates without awareness of areas susceptible to high levels of jamming. In (b), the receiver leverages knowledge of jamming-prone areas to adjust its operations. While some degradation may occur, the transmission remains sustainable due to the strategic awareness of jamming-prone zones.

Concerns with ML-based Jamming Identification. Accurate ML-based jamming detection typically requires large labeled datasets of both normal and abnormal spectrograms or records, which can be resource-intensive and prone to security risks, including adversarial attacks. Additionally, ML approaches often lack integration of contextual information such as the precise locations and number of active regular transmitters within a network. This limitation can hinder the performance of jamming detection systems, especially in dynamic and complex environments like 5G and beyond [5], [6].

Digital Twin (DT)-based Jamming Identification. To overcome previous challenges, researchers are increasingly leveraging DT technology for improved jamming identification and detection in wireless networks [7], [8]. While previous studies have focused on modeling the radio environment and utilizing DT for anomaly detection in wireless networks, our work integrates both the radio environment and the physical structure of the real world. This approach offers a more comprehensive framework, which is critical for efficient network planning and management. Essentially, a DT serves as a virtual representation of the real world, used to predict the behavior and outcomes of its physical counterpart. A wireless DT generally consists of three components: a radio model that represents the transmitter and receiver, a 3D scene that replicates the real world, and a radio propagation engine that simulates radio propagation for specified devices and environments [9], [10]. DTs have emerged as a powerful tool for capturing and analyzing environmental visuals along with their corresponding radio characteristics [11], [12].

Our Contributions. Building on the progress made in DT technology, we propose an innovative framework that accurately identify jamming-prone areas in smart cities which can be leveraged for smart network planning. Our framework achieves this with a minimal dataset, accurately captures the scene's radio environment, and is not affected by the challenges associated with both ML-based and non-ML-based jamming techniques. As shown in Fig. 1, awareness of jamming-prone areas can significantly enhance communication performance by enabling proactive strategies to manage or avoid interference. Fig. 1 (b) illustrates that, by identifying regions prone to jamming, the mobile receiver can strategically navigate toward areas with reduced susceptibility to jamming. Although another jammer may exist in these less jamming-prone areas, its impact differs due to the structural characteristics of the city, thereby enabling sustained communication. Our overall contributions are:

C1. We propose a methodology for accurately identifying jamming-prone areas in smart cities using downtown Dallas and downtown Houston as example scenes. This is achieved by leveraging Blender, Blender OSM and NVIDIA's Sionna tools.

C2. We demonstrate the feasibility of using smaller datasets ($< 0.5MB$) comprising 3D scenes from the example scenarios [13] and propagation modeling to accurately identify jamming-prone areas in smart cities.

C3. We validate our framework through comprehensive analysis and experiments on example scenarios. We release our codebase and dataset for broader community use in [14], facilitating reproducibility and further research exploration.

II. Related Works and Motivation

We underscore existing jamming identification and detection techniques, primarily focusing on both ML-based and non-ML-based approaches. While ML methods leverage algorithms, such as supervised and unsupervised learning, non-ML methods rely on parameters and heuristics, including thresholds, fuzzy logic, game theory, channel surfing, mapping jammed region, and timing channels. Yang *et al.* [15] propose a time series model that monitors the state of the link over time and compares it with historical link data to assess the state of the communication link. Cheng *et al.* [16] introduce a model based on thresholds, which assesses wireless channel performance in time-sensitive applications by analyzing packet loss, throughput, and the message error ratio. Oscar *et al.* [3] introduce a jamming identification method for 802.11 networks that relies on metrics available through standard device drivers and employs random forests for detection. This approach not only supports independent operation but also facilitates collaborative detection. Similarly, Grover *et al.* [17] present a ML-based system for jamming detection that employs support vector machines, adaptive boosting, and expectation maximization algorithms. The framework identifies and detects jamming attacks by analyzing factors such as noise, busy channel ratio, packet delivery ratio, and maximum idle time.

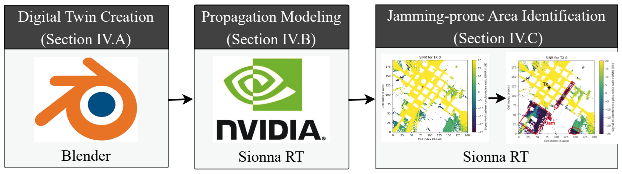


Fig. 2. The proposed framework.

Motivation: The state-of-the-art on jamming identification and detection typically rely on training large datasets containing features such as SNR, RSSI, and spectral patterns. However, these approaches are vulnerable to security risks and prone to accuracy issues, including false positives and false negatives, which undermine their reliability in real-world scenarios. Driven by this motivation, we propose a system that reliably and accurately identifies jamming-prone areas in smart cities using a minimal dataset, leveraging the open-source Sionna RT tool. Our approach integrates environmental features, device interactions, and real-world physical structures, offering significant potential for optimizing the planning and management of wireless network deployments.

III. System Model and Problem Formulation

A. Problem Formulation

We consider a legitimate transmitter TX transmitting with α dBm transmit power in a city $\mathcal{C}$. Each unobstructed point of the city $\mathcal{C}$ is denoted as a cell (c_i, c_j) with i and j indexing the X and Y coordinates of the city $\mathcal{C}$. A mobile receiver RX is modeled to be anywhere in the city, hence denoted as $\texttt{RX}_{(c_i,c_j)}$. The jammer, denoted as JM, is jamming the legitimate transmission of TX by transmitting at the same frequency band as TX with β dBm transmit power. The resulting signal-to-interference-plus-noise ratio (SINR) for each cell of the city is denoted as $SINR_{(c_i,c_j)}$. Overall, we want to mark each of the cells of the city as:

$$\mathcal{C}_{(c_i,c_j)} = \begin{cases} \text{Jam}_{\text{High}} & SINR_{(c_i,c_j)} > \mathcal{T} \\ \text{Jam}_{\text{Low}} & \text{Otherwise} \end{cases} \quad (1)$$

Where $\mathcal{T}$ is a threshold at which the signal from the legitimate transmitter TX is undecodable at the receiver $\texttt{RX}_{(c_i,c_j)}$ due to high interference from the jammer JM.

B. System Architecture

Our framework is illustrated in Fig. 2 and is organized into three main modules as follows:

- **Digital Twin Creation** *(Module 1)***:** We create a virtual replica of each real-world scene by directly extracting its features and strategically positioning RF devices at various locations within each scene (details in Sec. IV-A).
- **Propagation Modeling** *(Module 2)***:** We establish legitimate communication by placing a transmitter at a fixed location and a receiver at other locations within each scene, then propagating a signal between them (details in Sec. IV-B).
- **Jamming-prone Area Identification** *(Module 3)***:** We place a jammer at various location to interfere with the legitimate communication. We analyze the impact of the interfering signal at the receiver's locations (details in Sec. IV-C).

IV. Framework

In this section, we discuss different steps and components of our proposed framework.

A. Module 1: Digital Twin Creation

In the framework, we consider factors such as map accuracy and RF propagation characteristics. Additionally, our model is designed to be adaptable to various environmental configurations in the future. The twin of the city $\mathcal{C}$ initialized as $\mathcal{E}_{\mathcal{C}} = f(\texttt{map}, \mathrm{O}, \rho)$. Here, $\texttt{map}$ represents the imported Blender [18] map, O refers to the existing structures or objects within the twin $\mathcal{E}_{\mathcal{C}}$, and ρ indicates the number of reflections accounted for in the created twin.

B. Module 2: Propagation Modeling

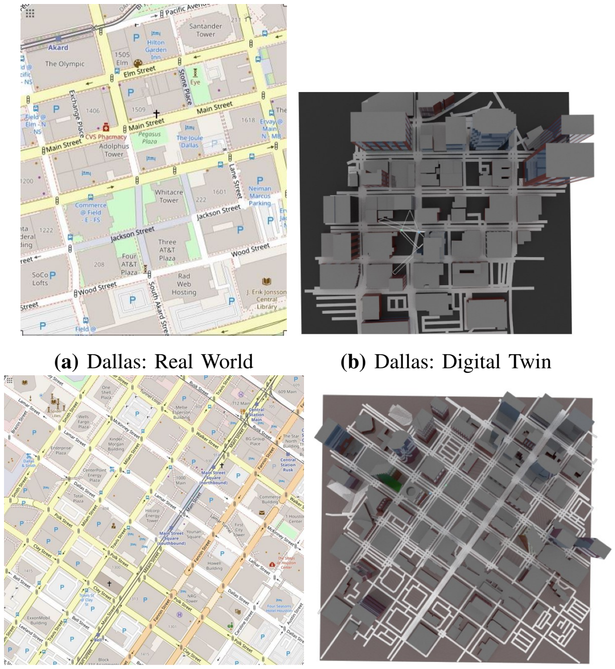
We utilize the off-the-shelf Sionna RT [19] tool to simulate the propagation characteristics of the created digital twin $\mathcal{E}_{\mathcal{C}}$ through RT. For a specified transmitter $\texttt{TX}$, the propagation map is modeled as a rectangular surface with an arbitrary orientation, divided into rectangular cells. The overall propagation map of the created twin $\mathcal{E}_{\mathcal{C}}$ is generated by placing the receiver $\texttt{RX}$ at each cell (c_i, c_j) and running differential raytracing of Sionna RT [19].

C. Module 3: Jamming-prone Area Identification

Upon generation of the propagation map of the digital twin $\mathcal{E}_{\mathcal{C}}$, we simulate unauthorized communication across various regions of the $\mathcal{E}_{\mathcal{C}}$. This is achieved by placing jammer $\texttt{JM}$ at different locations. In the digital twin $\mathcal{E}_{\mathcal{C}}$, for every ray n that intersects a cell (c_i, c_j) of the propagation map, the corresponding SINR is calculated as:

$$SINR_{(c_i,c_j)} = \frac{power(\texttt{TX}, \texttt{RX}_{(c_i,c_j)})}{power(\texttt{JM}, \texttt{RX}_{(c_i,c_j)}) + \mathcal{N}},$$

where $power(\texttt{TX}, \texttt{RX}_{(c_i,c_j)})$ is the power of the transmission going on between the legitimate transmitter $\texttt{TX}$ and the receiver $\texttt{RX}$ at cell (c_i, c_j), $power(\texttt{JM}, \texttt{RX}_{(c_i,c_j)})$ represents the power of the signal coming from the jammer $\texttt{JM}$ at the receiver $\texttt{RX}$ at cell (c_i, c_j), and $\mathcal{N}$ is the noise at cell (c_i, c_j). The jamming-prone cells within the digital twin $\mathcal{E}_{\mathcal{C}}$ of city $\mathcal{C}$ are identified by following Equation 1.



(a) Dallas: Real World **(b)** Dallas: Digital Twin

(c) Houston: Real World **(d)** Houston: Digital Twin

Fig. 3. The scene map and digital twin of our scenarios.

V. Experiments

A. Experimental Dataset

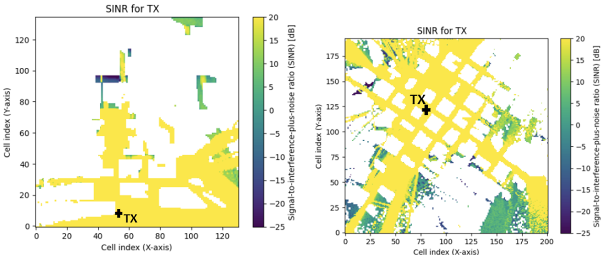
We use real-world 3D maps generated in [13] with Blender OpenStreetMap (OSM) for our outdoor experiments. These maps represent high-fidelity and hyper-realistic replicas of *downtown Dallas* and *downtown Houston*. The downtown Dallas scene covers an area of 0.4×0.5 km^2, comprising 37 buildings, 10 parking lots, and numerous roads that replicate the real world. Similarly, the downtown Houston scene covers an area of 0.8×0.8 km^2, containing 58 buildings, 29 parking lots, and various roads to accurately capture the physical properties of the environment, as shown in Fig. 3. Sionna provides a collection of materials defined by the International Telecommunication Union (ITU), each associated with specific radio properties [9], ensuring both realism and compatibility for every object. Each object in the scenes is represented based on its material properties, categorized as *ITU-marble*, *ITU-glass*, *ITU-concrete*, or *ITU-brick*, using the Blender tool. Note that we only use the generated Blender OSMs of [13] and add material properties to them using Blender.

B. Experimental Settings

In each scenario, we have two transmitters: a legitimate $\texttt{TX}$ and a jammer, along with one $\texttt{RX}$. The legitimate $\texttt{TX}$ is placed at a fixed position, while the jammer is positioned at four distinct locations to analyze how each affects connectivity in different parts of the city. The $\texttt{RX}$ is modeled as a car moving throughout the city. Each jammer is equipped with a dipole

Table I: Simulation Parameters

Parameter	Setting/Value
Dallas Area Dimension	0.4×0.5 km^2
Houston Area Dimension	0.8×0.8 km^2
Carrier Frequency	2.4 GHz
Antennas	Dipole
Regular TX Power	44 dBm
Jammer TX Power	44 dBm
Dallas TX Position	$[-42, -270, 18]$
Dallas JM1 Position	$[-27, 70, 18]$
Dallas JM2 Position	$[73, -249, 18]$
Dallas JM3 Position	$[107, -170, 18]$
Dallas JM4 Position	$[-247, -172, 18]$
Houston TX Position	$[-116, 131, 18]$
Houston JM1 Position	$[-74, 19, 18]$
Houston JM2 Position	$[-103, -245, 18]$
Houston JM3 Position	$[222, 48, 18]$
Houston JM4 Position	$[100, 246, 18]$
Material Properties	ITU-R P.2040 $-$ 2
Number of Rays	$1M$
Rays Maximum Depth (ρ)	5
Reflection	Enabled
Diffraction	Enabled



(a) Dallas

(b) Houston

Fig. 4. Propagation map of the legitimate transmission without any jammer. No signal interference is present. Yellow regions indicate areas with strong signal strength, and the black '+' marks the transmitter's position.

antenna array and transmits at 2.4 GHz with a power output of 44 dBm, identical to the legitimate TX. The configuration of each jammer remains consistent across all experiments.

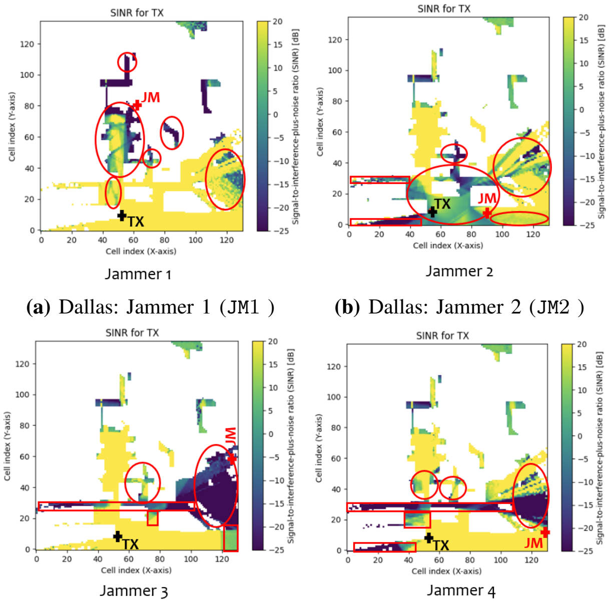
C. Experimental Platform and Performance Metrics

We perform all experiments including scene creation and propagation modeling on an Intel® Xeon® w7-2495x processor, using Blender, TensorFlow, Python, Sionna RT and Matplotlib libraries. We use the SINR to analyze communication between a legitimate transmitter-receiver (TX-RX) pair, both in the absence of a jammer and with a jammer present at various locations in different scenarios.

D. Performance Validation

Depending on the jammer's location in each scenario, we observe its impact on communication through performance metrics such as SINR. To analyze the SINR, we utilize the cumulative distribution function (CDF).

- **Downtown Dallas.** In the Dallas scenario, we begin by positioning a legitimate TX, aimed at a receiver navigating at that region, without introducing a jammer. We then compute the SINR for the legitimate transmitter, labeled as TX. As illustrated in Fig. 4 (a), the area exhibits strong signal strength (yellow region) with minimal interference affecting the signal quality. Next, we position a jammer at distinct locations in the city, targeting both the receiver and the TX. For each jammer position, we calculate the SINR of the TX in the jammer's presence and analyze the resulting signal degradation.



(a) Dallas: Jammer 1 (JM1)

(b) Dallas: Jammer 2 (JM2)

(c) Dallas: Jammer 3 (JM3)

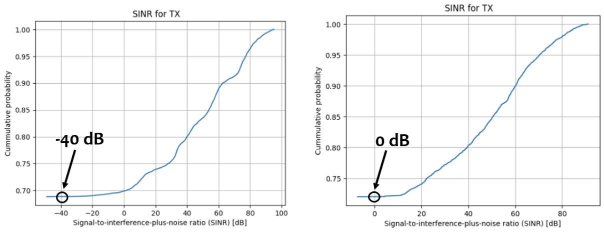
(d) Dallas: Jammer 4 (JM4)

Fig. 5. Dallas scenario with four jammers positioned at different locations: Signal interference is evident, with the dark regions outlined in red representing the jamming-prone areas caused by the jammer. The red '+' indicates the jammer's position.

As shown in Fig. 5, signal interference is evident in comparison to Fig. 4 (a) in all instances where a jammer is present and the SINR is computed for the legitimate TX. The jammer's impact on the city area is highlighted by red shapes, with the red '+' indicating the jammer's position. In Fig. 5 (a), the jammer has minimal impact on signal interference compared to other scenarios. The SINR remains high, as indicated by the yellow region. In Fig. 5 (b), the yellow region is smaller, with a larger green area indicating signal weakness compared to Fig. 5 (a), due to jammer interference, as reflected in the computed SINR for the legitimate TX. In Fig. 5 (c) and Fig. 5 (d), it is evident that the jammer's impact on the signal between the TX-RX pair in each area is substantial, leading to a smaller yellow region and larger dark regions.

Observation 1. *The placement of the jammers,* JM3 *and* JM4*, has more impact on the legitimate transmission of transmitter* TX *than* JM1 *and* JM2 *(see Fig. 5 (c) and (d)).*

Next, we analyze the SINR of the legitimate TX using the CDF. We compare scenarios without a jammer to those where a jammer is positioned at different locations within the city. Fig. 6 (a) shows that in the absence of a jammer, SINR is affected only by background noise and interference from other sources, leading to a broader range of values. At -40 dB, approximately 70% of SINR values are below this level. As SINR increases, the cumulative probability rises steadily, reaching nearly 1.0 around 100 dB, indicating that most SINR values fall below the threshold. The steep rise in the curve, particularly between 20–60 dB, reflects



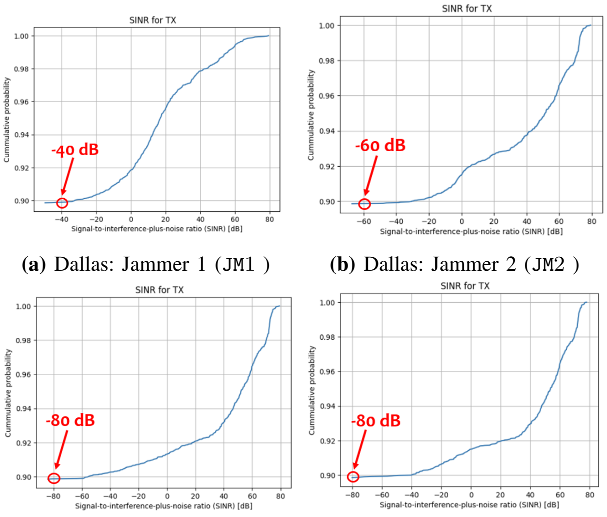
(a) Dallas **(b)** Houston.

Fig. 6. CDF of SINR without any jammer.

a concentration of SINR measurements in this range. Also, Fig. 7 presents the CDF curves of the SINR for the legitimate TX in the presence of jammers located at various positions within the city. In Fig. 7 (a), the SINR begins at approximately -40 dB, indicating moderate levels of interference. The curve rises steeply shortly afterward, showing that the majority of SINR values are concentrated toward higher levels, which suggests better overall signal quality. Additionally, the sharp increase indicates that JM1 has a minimal disruptive impact, allowing many transmissions to achieve acceptable SINR levels. In Fig. 7 (b), the SINR starts at approximately -60 dB, indicating slightly higher interference levels compared to JM1. The curve's gradual slope reflects greater variability in SINR values. These values are spread across a wider range, from around -60 dB to $+80$ dB. Overall, JM2 causes more significant signal degradation than JM1 due to its broader SINR range and slower rise. In Fig. 7 (c), the SINR starts at an extremely low value of -80 dB, signifying substantial interference. The slow rise of the curve in the lower SINR range highlights a high occurrence of very poor SINR levels. This indicates that JM3 is highly disruptive. In Fig. 7 (d), similar to JM3, the SINR values ranges from -80 dB to $+80$ dB, indicating a severe interference environment for JM4.

Observation 2. *The placement of* JM3 *and* JM4 *has significantly higher probability of interfering the legitimate transmission than* JM1 *and* JM2 *(see Fig. 7 (c) and (d)).*

• **Downtown Houston.** Similarly, in the Houston scenario, we begin by positioning a legitimate TX near the center of the scene and establishing TX-RX communication without any jammers. We then calculate the SINR for the scene. As shown in Fig. 4 (b), the majority of the city exhibits good signal coverage, represented by the yellow regions, with minor scattered interference from other sources depicted as green regions. The white areas represent the city structures. Next, we position jammers at four distinct locations across the city and compute the SINR of the TX in the presence of each jammer. We then analyze the individual impact of each jammer on signal degradation and assess their effect on coverage areas within the city. Fig. 8 illustrates the impact of each jammer at different locations within the city, with the affected areas marked by red bounding shapes. In Fig. 8 (a), the jammer has a moderate effect on the overall signal within the area. In Fig. 8 (b), the jammer somewhat degrades the signal quality, particularly in the area it occupies, resulting in a large dark region. In Fig. 8 (c), the jammer causes minimal interference, and the overall SINR remains strong. In Fig. 8 (d), scattered interference is observed across the city when the jammer is positioned in that location.



(a) Dallas: Jammer 1 (JM1) **(b)** Dallas: Jammer 2 (JM2)

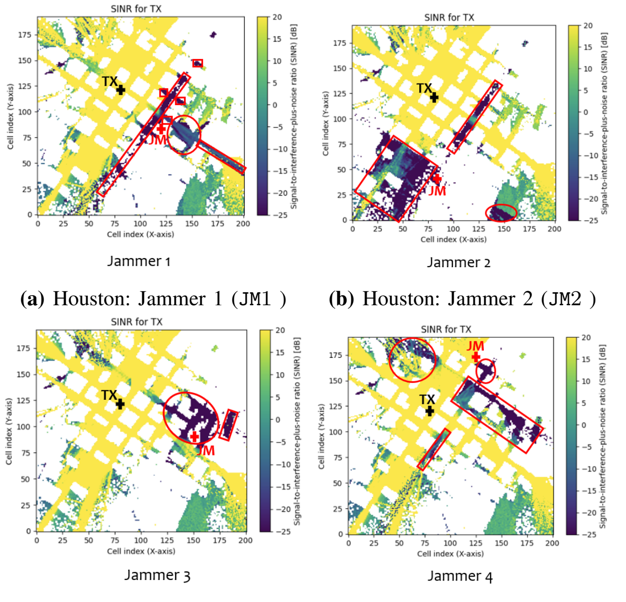
(c) Dallas: Jammer 3 (JM3) **(d)** Dallas: Jammer 4 (JM4)

Fig. 7. CDFs for all jammer locations in Dallas scenario.

Observation 3. *The placement of the jammer* JM4 *has more impact on the legitimate transmission of transmitter* TX *than the* JM1, 2, *and* 3 (see Fig. 8 (d)).

Similar to the Dallas scenario, we next analyze the SINR of the TX using the CDF in the Houston scenario, both without a jammer and with a jammer placed at different locations throughout the city, as shown in Fig. 6 (b) and Fig. 9. In Fig. 6 (b), the cumulative probability starts at approximately 0.75 around 0 dB, indicating that 75% of the SINR values fall below this threshold. As the SINR increases, the curve rises steadily, reflecting the distribution of SINR values and suggesting a gradual improvement in signal quality. In Fig. 9 (a), the SINR values range from approximately -60 dB to $+80$ dB, indicating a moderate level of interference and a diverse range of signal quality. While JM1 introduces noticeable interference, the upward trend in the curve shows that many transmissions still achieve acceptable SINR levels. In (b), the SINR starts at approximately -40 dB, indicating less interference compared to JM1. It spans from about -40 dB to 80 dB, reflecting better overall signal quality. Overall, JM2 is less disruptive. In (c), JM3 is the least disruptive, with the SINR starting at -20 dB. The sharp rise in the curve shows that most SINR values are concentrated at higher levels. In (d), the SINR starts at -75 dB, indicating severe interference. The curve rises slowly initially, highlighting a high occurrence of poor SINR values before improving. JM4 is the most disruptive, causing widespread interference and frequent instances of low SINR.

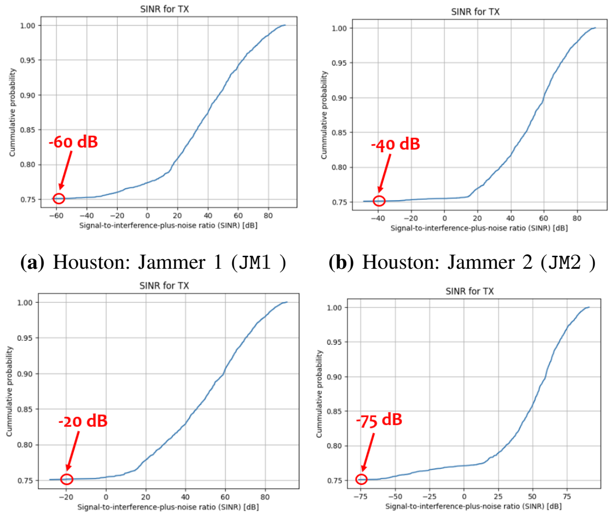
Observation 4. *The placement of the jammer* JM4 *has significantly higher probability of interference than the* JM1, 2, *and* 3 *(see Fig. 9 (d)).*



(a) Houston: Jammer 1 (JM1) **(b)** Houston: Jammer 2 (JM2)

(c) Houston: Jammer 3 (JM3) **(d)** Houston: Jammer 4 (JM4)

Fig. 8. Houston scenario with a jammer placed at various locations: Signal interference is clearly visible, with the red-outlined dark regions indicating the jamming-prone areas caused by the jammer. The red '+' denotes the jammer's position.



(a) Houston: Jammer 1 (JM1) **(b)** Houston: Jammer 2 (JM2)

(c) Houston: Jammer 3 (JM3) **(d)** Houston: Jammer 4 (JM4)

Fig. 9. CDFs for all jammer locations in Houston scenario.

Overall, the proposed framework identifies jamming-prone areas and evaluates the impact levels caused by jammers placed at distinct positions within both cities.

VI. Conclusions

This paper introduces an innovative system for identifying jamming-prone areas in smart cities using DT technology. Our methodology involves creating a digital twin of real-world environments, simulating propagation characteristics to generate RF maps, calculating the SINR of legitimate transmitter-receiver pairs, and analyzing their SINR using CDF. Extensive experimental validation in two outdoor scenarios demonstrates the system's effectiveness in identifying jamming-prone areas and assessing their severity. Future work will investigate the number of jammers required to disrupt an entire network's communication within an environment and explore strategies to mitigate such attacks.

References

[1] N. Suman, M. Sunny, M. S. Menon, N. S. Das, and N. Biju, "Interference detection in iot environment," in *2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT)*, vol. 1, 2024, pp. 1483–1488.

[2] Y. Arjoune, F. Salahdine, M. S. Islam, E. Ghribi, and N. Kaabouch, "A novel jamming attacks detection approach based on machine learning for wireless communication," in *2020 International Conference on Information Networking (ICOIN)*, 2020, pp. 459–464.

[3] O. Puñal, I. Aktaş, C.-J. Schnelke, G. Abidin, K. Wehrle, and J. Gross, "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.

[4] V. Tiwari, A. Agrawal, M. Sharma, P. Chaturvedi, T. Katiyar, and I. Maheshwari, "Mitigation of jamming and spoofing attack on gnss signals using subspace projection," in *2023 3rd International Conference on Emerging Frontiers in Electrical and Electronic Technologies (ICEFEET)*, 2023, pp. 01–06.

[5] B. Upadhyaya, S. Sun, and B. Sikdar, "Machine learning-based jamming detection in wireless iot networks," in *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*, 2019, pp. 1–5.

[6] Y. Wang, S. Jere, S. Banerjee, L. Liu, S. Shetty, and S. Dayekh, "Anonymous jamming detection in 5g with bayesian network model based inference analysis," in *2022 IEEE 23rd International Conference on High Performance Switching and Routing (HPSR)*, 2022, pp. 151–156.

[7] A. Krause, M. D. Khursheed, P. Schulz, F. Burmeister, and G. Fettweis, "Digital twin of the radio environment: A novel approach for anomaly detection in wireless networks," in *2023 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2023, pp. 1307–1312.

[8] W. Wang, Y. Yang, L. U. Khan, D. Niyato, Z. Han, and M. Guizani, "Digital twin for wireless networks: Security attacks and solutions," *IEEE Wireless Communications*, 2023.

[9] J. Hoydis, F. A. Aoudia, S. Cammerer, M. Nimier-David, N. Binder, G. Marcus, and A. Keller, "Sionna rt: Differentiable ray tracing for radio propagation modeling," *arXiv preprint arXiv:2303.11103*, 2023.

[10] S. Amatare, G. Singh, A. Kharel, and D. Roy, "Real-time localization of objects using radio frequency propagation in digital twin," *Available at SSRN 4937841*, 2024.

[11] S. Amatare, M. Samson, and D. Roy, "Testbed design for robot navigation through differential ray tracing," in *2024 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2024, pp. 173–174.

[12] S. Amatare, G. Singh, M. Samson, and D. Roy, "RagNAR: Ray-tracing based Navigation for Autonomous Robot in Unstructured Environment," in *IEEE Global Communications Conference*, December 2024.

[13] S. Amatare, G. Singh, R. Shakya, A. Kharel, A. Alkhateeb, and D. Roy, "Dt-radar: Digital twin assisted robot navigation using differential ray-tracing," 2024. [Online]. Available: https://arxiv.org/abs/2411.12284

[14] https://github.com/TWIST-Lab/Jamming-DTwin2025.

[15] H. Yang, M. Shi, Y. Xia, and P. Zhang, "Security research on wireless networked control systems subject to jamming attacks," *IEEE transactions on cybernetics*, vol. 49, no. 6, pp. 2022–2031, 2018.

[16] M. Cheng, Y. Ling, and W. B. Wu, "Time series analysis for jamming attack detection in wireless networks," in *GLOBECOM 2017-2017 IEEE Global communications conference*. IEEE, 2017, pp. 1–7.

[17] K. Grover, A. Lim, and Q. Yang, "Jamming and anti–jamming techniques in wireless networks: a survey," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 17, no. 4, pp. 197–215, 2014.

[18] B. O. Community, *Blender - a 3D modelling and rendering package*, Blender Foundation, Stichting Blender Foundation, Amsterdam, 2018. [Online]. Available: http://www.blender.org

[19] N. Inc., "Ray tracing," 2024, last accessed 6 April 2024. [Online]. Available: https://nvlabs.github.io/sionna/api/rt.html