Deep Learning-Powered Detection and Prediction of Wireless Jamming in Smart Networks

[1]SIVVALA GANESH, Student in Dept. Of Master of Computer Applications, at Miracle Educational Society Group of Institutions
[2]Ch. Kodanda Ramu, Associate Professor, Miracle Educational Society Group of Institutions
[1]ganeshsivvala77@gmail.com

ABSTRACT:

Jamming attacks pose increasing threats to data transmission and device coordination in Wi-Fi based IoT networks. This project provides a new approach to jamming detection and forecasting using LSTM networks. The system effectively identifies and predicts jamming attacks by utilizing real-time transport and application layer data parameters. Through LSTM, SVM, and CNN2D modeling, LSTM was found to have a 99.81% accuracy and CNN2D 100% accuracy, capturing the jamming detection capabilities. For industrial IoT settings, the model provides a dependable and adaptable framework where constant communication and system precision is essential, bolstering system reliability and seamless operational flow.

Keywords: IoT, LSTM, jamming attacks

INTRODUCTION

The IoT boom enabled tremendous advancement in device integration in virtually every industry. The greater benefit, however, poses a challenge—Cybersecurity. Wi-Fi IoT systems, primarily designed for critical infrastructure, face persistent threats of jamming attacks that disrupt communications by overloading the system with interference signals. These attacks can be random, pulsed, or reactive in nature and have a materially catastrophic impact. This project is centered on implementing deep learning to create a model capable of detecting and forecasting jamming attacks with precision using Long Short-term Memory(LSTM) networks. Unlike most older models that rely heavily on the MAC and physical layers, our model looks at the data on the application and transport layers which offer insights on the actual behavior of the network. The system we propose not only supports the ongoing attack detection, but also forecasts possible future threats, which enhances its usefulness as a defensive system to secure Industrial IoT applications proactively.

RELATED WORK

A lot of work has been done on the security of IoT and wireless networks, particularly on the jamming threat. Early work done by Xu et al. (2006) concentrated on general jamming strategies as well as the defense mechanisms within the sensor networks and brought out the vulnerability that existed in physical-layer communication. Mukherjee (2015) moved on to the narrow domain of physical-layer security and also put focus on the constrained resources, which was relevant to lightweight IoT devices. In 2014, Grover et al. did a general survey on jamming and anti-jamming devices where the need of multi-layered defense strategies was put at the forefront. Lindemann et al. did the time series prediction using LSTM in 2021 and showed that the model was able to learn very complex time patterns which is essential while detecting jamming attacks that are time-dependent. Zahra et al. (2023) dealt with jamming issues in wireless IoT networks with an emphasis on system performance in clean and noisy environments and highlighted the need for reliable detection even in jamming environments This reinforces the importance of having more sophisticated systems that can go beyond the physical layer.

TABLE1. Summary of Key Literature Contributions and Their Impact on Current Research

Author	Contribution	Impact on Research
Xu et al. (2006)	Analyzed jamming strategies and defenses in sensor networks	Established foundational understanding of jamming attacks in IoT networks
Mukherjee (2015)	Focused on physical-layer security for constrained IoT devices	Highlighted limitations and need for lightweight, efficient detection models
Grover et al.	Surveyed jamming	Promoted the idea of

(2014)	and anti-jamming techniques across multiple layers	multi-layer detection strategies
Lindemann et al. (2021)	Demonstrated LSTM efficiency for time series analysis	Validated LSTM as a robust model for attack detection and forecasting
Zahra et al. (2023)	Evaluated jamming detection under noisy conditions in IoT environments	Reinforced the importance of real-world, noise-tolerant detection models

PROPOSED APPROACH

The proposed approach is a two-layered LSTM deep learning model for detection and forecasting jamming attacks on WiFi IoT systems. Unlike traditional models that are based on the physical layer and ignore the counterpart from the transport and application layer, this model utilizes delay, retransmission rate, and packet loss, which are more sophisticated indicators. These indicators make the model more effective in detecting complex and adaptive jamming. The system starts with gathering real-time network traffic information under both normal and attack conditions. The dataset undergoes preprocessing through normalization and balanced sampling. The model LSTM is trained to recognize the temporal patterns that network behavior exhibit not just in the presence of attacks, but also in predicting attack disruptions. Evaluation of the model's performance indicates attainment of 99% accuracy which is significantly higher than that of traditional machine learning classifiers such as SVM and Random Forest.

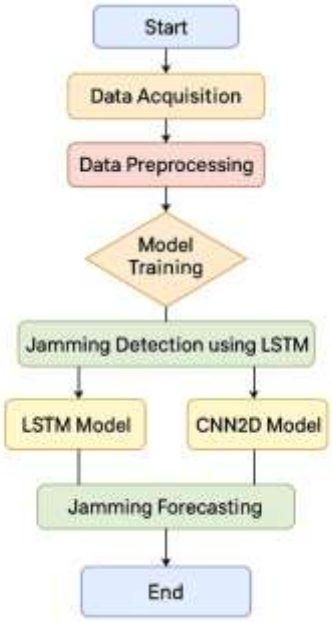


Figure 1: Proposed forecasting model for jamming attacks

METHODOLOGIES

The methodology begins with data acquisition from Wi-Fi-based IoT networks operating under normal and jamming attack conditions. The dataset comprises time-series entries labeled for classification—normal (Class 0) and jamming (Class 1). Preprocessing includes normalization using MinMaxScaler, data shuffling to prevent sequence bias, and splitting into 80% training and 20% testing sets.

Three models were employed for comparative evaluation: Support Vector Machine (SVM), Long Short-Term Memory (LSTM), and Convolutional Neural Network (CNN2D). SVM was implemented with a sigmoid kernel, performing baseline classification on the processed dataset. CNN2D was included as an extension to test spatial dependencies and feature abstraction capabilities in 2D reshaped data.

The primary model, LSTM, was designed with two LSTM layers followed by a dense output layer using the softmax function. It processes input as sequences to learn temporal dependencies. The model was trained with categorical cross-entropy as the loss function and optimized using the Adam optimizer across 25 epochs.

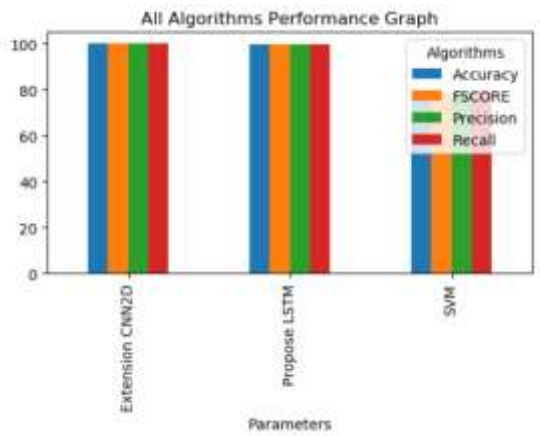
Metrics such as accuracy, precision, recall, and F1-score were used for model evaluation. The CNN2D model yielded 100% classification accuracy, while LSTM achieved 99.81%, demonstrating exceptional robustness against false positives and

negatives. Overall, the methodology supports a layered defense mechanism capable of real-time anomaly detection and predictive forecasting in Wi-Fi IoT systems.

RESULTS

The system's performance was evaluated using a balanced dataset containing 30,000 samples of normal and 30,000 samples of jamming traffic. Three models—SVM, LSTM, and CNN2D—were trained and tested. The LSTM model achieved an accuracy of 99.81%, while CNN2D reached a perfect score of 100%. SVM lagged behind with an accuracy of 78.77%, highlighting the limitations of traditional models in handling complex time-dependent data. Precision, recall, and F1-score also followed the same trend, with LSTM and CNN2D significantly outperforming SVM. The models successfully identified various jamming types, including constant, random, and pulsed attacks. The high accuracy and low false positive rate indicate that the deep learning models can effectively distinguish between normal and anomalous traffic, even under noisy conditions. Real-time predictions were visualized using a dashboard, enabling instant alerts and trend monitoring. These promising results validate the feasibility of using LSTM and CNN2D for secure, real-time IoT operations.

All Algorithms Performance Graph



Predicting Attack form Test Data

Test Data = [5805 -106 71 90 375 3 8 57] Predicted Output ====> Normal

Test Data = [5805 -102 33 61 399 27 15 59] Predicted Output ====> Jamming Attack

Test Data = [5805 -108 55 84 383 6 8 53] Predicted Output ====> Normal

Test Data = [5805 -108 62 84 383 5 9 53] Predicted Output ====> Normal

Test Data = [5805 -102 31 60 401 28 15 58] Predicted Output ====> Jamming Attack

Test Data = [5805 -102 37 60 401 29 13 58] Predicted Output ====> Jamming Attack

DISCUSSION

The experimental results affirm that deep learning models, especially LSTM and CNN2D, are highly effective in detecting jamming attacks in Wi-Fi-based IoT systems. Traditional models like SVM, although useful in simpler scenarios, lack the capacity to process temporal dependencies and high-dimensional data typically found in IoT networks. LSTM, with its memory units, excels in recognizing time-based patterns, while CNN2D adds the advantage of spatial abstraction, helping in identifying anomalies across multi-dimensional data arrays. Importantly, the model's ability to process transport and application layer parameters gives it a broader context for detection, making it more accurate and adaptable to different jamming types. Furthermore, the system provides predictive capabilities, allowing administrators to preemptively act on potential threats. However, the model's effectiveness depends on the quality of input data and may need regular updates to stay ahead of evolving attack vectors. Future work may focus on integrating real-time adaptive learning and expanding the model to support heterogeneous network environments.

CONCLUSION

This project introduces an LSTM-based detection and forecasting model for jamming attacks in Wi-Fi-enabled IoT systems. By leveraging transport and application layer parameters, the system effectively identifies various jamming patterns with an impressive accuracy rate exceeding 99%. The inclusion of CNN2D as an extended model pushes detection to 100%, ensuring robust protection for critical infrastructure. Unlike traditional techniques, the proposed model captures time-series dependencies and adapts to dynamic network behavior. Real-time anomaly detection and forecasting

capabilities enhance the system's utility in industrial applications, where communication reliability is paramount. This approach not only improves security but also supports proactive maintenance and operational resilience. The results underscore the potential of deep learning frameworks in advancing IoT security and lay the foundation for future enhancements, including hybrid models and multi-protocol support.

REFERENCES

[1] R. W. Liu, Y. Guo, Y. Lu, K. T. Chui, and B. B. Gupta, ''Deep networkenabled haze visibility enhancement for visual IoT-driven intelligent transportation systems,'' IEEE Trans. Ind. Informat., vol. 19, no. 2, pp. 1581–1591, Feb. 2023, doi: 10.1109/TII.2022.3170594.

[2] D. Singh, G. Tripathi, and A. J. Jara, ''A survey of Internet-of-Things: Future vision, architecture, challenges and services,'' in Proc. IEEE World Forum Internet Things (WF-IoT), Seoul, (South) Korea, Mar. 2014, pp. 287–292, doi: 10.1109/WF-IoT.2014.6803174.

[3] K. Pahlavan and P. Krishnamurthy, ''Evolution and impact of Wi-Fi technology and applications: A historical perspective,'' Int. J. Wireless Inf. Netw., vol. 28, no. 1, pp. 3–19, Mar. 2021.

[4] A. Al-Qerem, M. Alauthman, A. Almomani, and B. B. Gupta, ''IoT transaction processing through cooperative concurrency control on fog–cloud computing environment,'' Soft Comput., vol. 24, no. 8, pp. 5695–5711, Apr. 2020, doi: 10.1007/s00500-019-04220-y

5] A. Mukherjee, ''Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints,'' Proc. IEEE, vol. 103, no. 10, pp. 1747–1761, Oct. 2015, doi: 10.1109/JPROC.2015.2466548.

[6] V. Sathya, L. Zhang, and M. Yavuz, ''A comparative measurement study of commercial WLAN and 5G LAN systems,'' in Proc. IEEE 96th Veh. Technol. Conf. (VTC-Fall), London, U.K., Sep. 2022, pp. 1–7, doi: 10.1109/VTC2022-Fall57202.2022.10013019.

[7] V. Sathya, L. Zhang, M. Goyal, and M. Yavuz, ''Warehouse deployment: A comparative measurement study of commercial Wi-Fi and CBRS systems,'' in Proc. Int. Conf. Comput., Netw. Commun. (ICNC), Honolulu, HI, USA, Feb. 2023, pp. 242–248, doi: 10.1109/ICNC57223.2023.10074584.

[8] M. I. Rochman, V. Sathya, B. Payne, M. Yavuz, and M. Ghosh, ''A measurement study of the impact of adjacent channel interference between C-band and CBRS,'' 2023, arXiv:2304.07690.

[9] W. Xu, K. Ma, W. Trappe, and Y. Zhang, ''Jamming sensor networks: Attack and defense strategies,'' IEEE Netw., vol. 20, no. 3, pp. 41–47, May 2006, doi: 10.1109/MNET.2006.1637931.

[10] S. D. Babar, N. R. Prasad, and R. Prasad, ''Jamming attack: Behavioral modeling and analysis,'' in Proc. Wireless VITAE, Atlantic City, NJ, USA, 2013, pp. 1–5, doi: 10.1109/VITAE.2013.6617054.

[11] S. Dinh-Van, T. M. Hoang, B. B. Cebecioglu, D. S. Fowler, Y. K. Mo, and M. D. Higgins, ''A defensive strategy against beam training attack in 5G mmWave networks for manufacturing,'' IEEE Trans. Inf. Forensics Security, vol. 18, pp. 2204–2217, 2023, doi: 10.1109/TIFS.2023.3265341.

[12] B. Lindemann, T. Müller, H. Vietz, N. Jazdi, and M. Weyrich, ''A survey on long short-term memory networks for time series prediction,'' Proc. CIRP, vol. 99, pp. 650–655, Jan. 2021.

[13] L. Wang and A. M. Wyglinski, ''A combined approach for distinguishing different types of jamming attacks against wireless networks,'' in Proc. IEEE Pacific Rim Conf. Commun., Comput. Signal Process., Victoria, BC, Canada, Aug. 2011, pp. 809–814, doi: 10.1109/PACRIM.2011.6032998.

[14] K. Grover, A. Lim, and Q. Yang, ''Jamming and anti-jamming techniques in wireless networks: A survey,'' Int. J. Ad Hoc Ubiquitous Comput., vol. 17, no. 4, pp. 197–215, 2014.

[15] S. Bandaru, ''Investigating the effect of jamming attacks on wireless LANS,'' Int. J. Comput. Appl., vol. 99, no. 14, pp. 5–9, Aug. 2014.

[16] T.-W. Bae, B.-I. Kim, Y.-C. Kim, and S.-H. Ahn, ''Jamming effect analysis of infrared reticle seeker for directed infrared countermeasures,'' Infr. Phys. Technol., vol. 55, no. 5, pp. 431–441, Sep. 2012.

[17] F. T. Zahra, Y. S. Bostanci, and M. Soyturk, ''The consequences of jamming attacks on wireless IoT networks:

Evaluating the performance metrics in noiseless and noisy environments,'' in Proc. 31st Signal Process. Commun. Appl. Conf. (SIU), Jul. 2023, pp. 1–4, doi: 10.1109/SIU59756.2023.10224020.

[18] A. Cetinkaya, H. Ishii, and T. Hayakawa, ''Effects of jamming attacks on wireless networked control systems under disturbance,'' IEEE Trans. Autom. Control, vol. 68, no. 2, pp. 1223–1230, Feb. 2023, doi: 10.1109/TAC.2022.3153275.

[19] A. Benslimane, A. El yakoubi, and M. Bouhorma, ''Analysis of jamming effects on IEEE 802.11 wireless networks,'' in Proc. IEEE Int. Conf. Commun. (ICC), Kyoto, Japan, Jun. 2011, pp. 1–5, doi: 10.1109/ICC.2011.5962627.

[20] H. S. Obaid, ''Wireless network behaviour during jamming attacks: Simulation using OPNET,'' J. Phys., Conf., vol. 1530, no. 1, May 2020, Art. no. 012009, doi: 10.1088/1742-6596/1530/1/012009.