Autoencoder-based Smart Jamming Detection in the 5G Radio Access Network

Abate Selamawit Chane and Seong Ho Jeong*
Hankuk University of Foreign studies
selamchane@hufs.ac.kr, *shjeong@hufs.ac.kr

5G 무선 접속 네트워크에서 오토 인코더 기반 스마트 전파방해 탐지

셀라마윗, 정성호
한국외국어대학교

Abstract

One of the key advantages of 5G technology is its ability to support massive connectivity, enabling a wide range of Internet of Things (IoT) services. However, this expanded network of connected devices also introduces new security vulnerabilities. The sheer volume of IoT devices in 5G environments can be exploited by malicious actors, such as jammers, who may introduce noise or selectively target specific devices to disrupt communication. This threat becomes even more severe when the jamming attack is orchestrated by a smart attacker leveraging deep learning techniques as it significantly increases the complexity of detection and mitigation. In this paper, we propose an autoencoder-based jamming detection method designed to counter AI-enabled smart jamming attacks. The objective is to effectively identify these sophisticated jamming attempts and enhance the network's resilience against such threats.

Ⅰ. Introduction

IoT services and AI techniques are increasingly being leveraged to unlock the full potential of 5G networks. However, these same technologies can also be exploited maliciously to execute reactive jamming attacks. Reactive jamming is a sophisticated form of interference where the attacker only transmits disruptive signals upon detecting legitimate activity on a specific frequency. An anomaly detection mechanism is presented at [1] by analyzing radio activities at physical layer. However, in scenarios, where the jammer integrates itself into the network as a legitimate device to gain insights about the network's behavior, it can selectively launch targeted interference in a reactive manner. This strategic approach makes reactive jamming particularly challenging to detect and mitigate.

This paper presents a jamming detection mechanism utilizing autoencoders to identify smart jamming attacks. To validate our approach, we will simulate a scenario where a jammer employs an LSTM-based model. Then, we will evaluate the performance of the proposed autoencoder model by testing its effectiveness against the simulated smart jamming scenario.

Ⅱ. Method

To simulate a reactive jamming scenario, we model a jamming attack that leverages the predictive capabilities of Long Short-Term Memory (LSTM) networks, which are well-suited for processing and forecasting time-series data.

Both the jammer and the detector models use the same network parameters as an input, denoted as x in Fig. 1, which characterize the condition of the channel such as Received Signal Strength Indicator (RSSI), Channel State Information (CSI), time slot usage. These two models are trained independently. The attacker's model, based on LSTM, processes time-series data from these parameters to produce a binary decision, indicating whether an attack should be launched at a specific moment. Meanwhile the autoencoder focuses on the current state of the network to determine whether the system is under attack.

The autoencoder is trained under normal network conditions, where it learns to extract latent features to accurately reconstruct the input data. During this training phase, the autoencoder becomes proficient at reproducing the network's behavior in a non-compromised state. However, during testing, when inputs from a tampered network condition are fed into the autoencoder, the model generates a significantly higher reconstruction error.

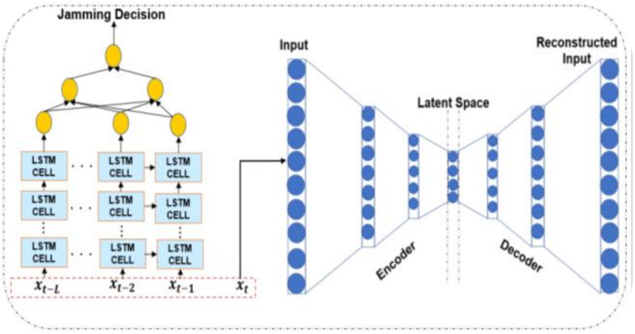

Fig. 1. Smart Jamming Detection using the Autoencoder

Ⅲ. Conclusion

In this paper, we proposed an autoencoder-based jamming detection model to enhance resilience against reactive jamming attacks launched by AI-equipped agents.

ACKNOWLEDGMENT

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation). This research was financially supported by the Ministry of Trade, Industry and Energy (MOTIE) and Korea Institute for Advancement of Technology (KIAT) through the International Cooperative R&D program (Project No. 0028596).

REFERENCES

[1] Martins, P., Reis, A. B., Salvador, P., & Sargento, S. (2020, April). Physical layer anomaly detection mechanisms in IoT networks. In *NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium* (pp. 1-9). IEEE.