Autoencoder-Based and Subspace Projection Methods for Anomaly Detection in Massive MIMO Systems: A Comparative Analysis

T.S.N. Murthy[1], R. Deepika[2,3], P. Chandrasekhar[4]

[1]Associate Professor, Department Of ECE, JNTU-GV College of Engineering, Vizianagaram, Andhra Pradesh 535003, India. Email: tsnmurthyece.jntuk@ieee.org

[2]M. Tech Student, Department Of ECE, JNTU-GV College of Engineering, Vizianagaram, Andhra Pradesh 535003, Andhra Pradesh, 535003, India. Email: ronanki.deepika@gmail.com

[3]Assistant Professor, Department of ECE, Aditya Institute of Technology and Management (A), Tekkali, Srikakulam, Andhra Pradesh 532203, India. Email: ronanki.deepika@adityatekkali.edu.in

[4]Assistant Professor, Department of ECE, Chaitanya Bharathi Institute of Technology (A), Hyderabad, Telangana 500075, India. Email: pchandrasekhar_ece@cbit.ac.in

---

Abstract - Anomaly detection in wireless systems is very vital to guarantee secure and reliable transmission especially in the presence of adversarial users. This paper presents a comparative study of autoencoder-based and subspace projection methods for the detection of anomalous signals in massive MIMO systems. The autoencoder model learns normal signal patterns and detects anomalies by means of reconstruction error, whereas the subspace method uses covariance matrix analysis and eigenvalue decomposition. Simulation results show that the detection probability is increased with the increase of the signal-to-noise ratio (SNR), the number of antennas and the adversary transmit power. The autoencoder-based approach achieves superior performance in nonlinear environments, whereas the subspace method offers computational efficiency and robustness under low-SNR conditions.

Key Words: Anomaly, Autoencoder, Subspace projection, covariance matrix

1. INTRODUCTION

The modern communication infrastructures have been greatly changed by the rapid development of 5G/6G wireless communication systems. The systems provide a seamless connectivity, exchange data in real time and enable intelligent automation in a variety of areas such as healthcare, smart cities, industrial monitoring and defense applications. However, wireless environments are open and dynamic and therefore inherently vulnerable to a wide range of anomalies such as malicious attacks, signal interference, hardware failures and unexpected network behavior. Hence the concern about security in wireless communication is increased, as Fifth Generation (5G) wireless communication is entered in very field of life [1].

Thus, anomaly detection has become an important part of guaranteeing the security, reliability and efficiency of wireless systems. Anomaly finding methods are based on detecting deviations from normal behaviour of the system, unlike conventional signature-based detection techniques. Anomaly detection can detect previously unknown or zero-day attacks. This ability is especially important in wireless networks where new attack patterns and unpredictable environmental conditions are common. Anomalies in wireless communication systems may appear in various ways, such as unusual traffic patterns, abnormal energy consumption of sensor nodes, signal quality degradation, or unauthorized spectrum usage. These anomalies not only destroy the system performance, but may also lead to serious consequences such as data breach, service disruption, and wrong decision-making in critical mission applications.

Therefore, the correct and early detection of such irregularities is crucial.

In the meantime, machine learning and deep learning have also developed rapidly and achieved promising performance in anomaly detection methods. Data-driven approaches such as supervised, unsupervised and hybrid models have shown promising potential to learn complex patterns in wireless data including Received Signal Strength (RSS), Channel State Information (CSI) and network traffic features. In particular, deep learning models such as autoencoders, convolutional neural networks (CNNs) and recurrent neural networks (RNNs) have demonstrated impressive performance in detecting subtle and high dimensional anomalies. However, there are still some challenges, such as the lack of labelled datasets, high computational complexity, energy constraints in resource-limited devices, and real-time detection in large-scale networks. To tackle these challenges, efficient, scalable and adaptive anomaly detection frameworks need to be developed for the wireless environments.

This paper aims to emphasize the importance of anomaly detection in wireless systems by examining its role in improving security, enhancing system reliability and managing the network intelligently.

2. LITERATURE REVIEW

Wireless systems have attracted a lot of attention for anomaly detection due to the increasing complexity of networks modern 5G/6G communication systems. In the literature, various methods have been proposed, from statistical approaches to advanced deep learning models. Rajasegarar et al. [2] presented a comprehensive survey of anomaly detection techniques in WSNs and classified them into statistical, nearest neighbor based, clustering based and classification-based approaches. The authors emphasized the importance of distributed detection mechanisms owing to the resource constraints in sensor networks. Similarly, Chandola et al. [3] provided a baseline overview of anomaly detection covering different types of anomalies and their applications in domains such as wireless systems.

Zhang et al. [4] explored anomaly detection in WSNs, highlighting the issues of noisy data, limited computational resources and dynamic network conditions. They classified anomalies into point, contextual and collective anomalies which is very relevant for wireless data streams. Li et al. [5] suggested a lightweight anomaly detection technique using Support Vector Data Description (SVDD) to overcome computational constraints. Their method exhibited better detection accuracy with less computational load and it is suitable for resource-constrained wireless environments. The progress of machine learning pushed researchers to search for intelligent methods. Shone et al. [6] proposed a deep learning-based intrusion detection system using autoencoders, which exhibited better performance than the traditional approaches. This research laid the foundation for the application of deep neural networks for wireless anomaly detection.

O'Shea and Corgan [7] suggested a deep learning-based approach for detecting anomalies in radio frequency signals by using spectrogram representations in RF and spectrum monitoring. Their approach successfully identified jamming and interference patterns, demonstrating the potential of deep learning in RF environments. Further advances were made by Restuccia et al. [8] who used deep predictive coding neural networks for real-time RF anomaly detection. The model they propose is able to achieve high finding accuracy with low latency, which is important for real-time wireless systems. In recent years, hybrid and intelligent approaches have been proposed. An anomaly detection framework based on reinforcement learning for IoT systems was proposed by Liu et al. [9], which integrates decision-making ability with anomaly detection. Their

approach enhanced adaptability in changing environments. Recently, deep learning models based on Channel State Information (CSI) have been studied. Kumar et al. [10] proposed a CNN-LSTM based anomaly detection model to capture the spatial and temporal features of wireless channels. Their approach performed better in detecting jamming, spoofing and QoS related anomalies.

3. IMPLEMENTATION

The attack studied in this work is the pilot contamination attack, where the eavesdropper E transmits the same pilot sequence as the legitimate user. Pilot sequences are known and reused, so the attacker can easily imitate them.

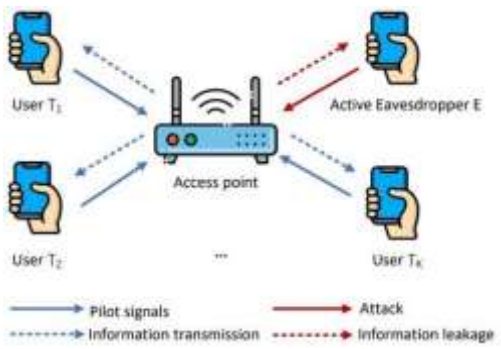


Fig. 1: System Model

The network includes:

- One Access Point (AP)
- Klegitimate users denoted as $T_1, T_2, \dots, T_K$
- One active eavesdropper denoted as E

All nodes are randomly distributed in the wireless environment. The wireless channels between the AP and the legitimate users, and between the AP and the eavesdropper, are assumed to experience fading and noise.

Threat Model: Active Eavesdropping Attack

Unlike passive eavesdroppers, an active eavesdropper is capable of interfering with the communication process.

Pilot Contamination Attack

The AP receives a superimposed signal from the legitimate user and the attacker. Therefore, the AP estimates a corrupted channel which takes into account the effect of both user and attacker. In the downlink phase, the AP is unaware that it is sending confidential data to both. This results in information leakage which is a major security issue.

Autoencoder Based Anomaly Detection

Autoencoder-Based Anomaly Detection is an unsupervised machine learning method that utilizes an autoencoder neural network to find abnormal or rare patterns in data.

It has three main parts:

1. Encoder – compresses input data into a lower-dimensional representation (latent space)
2. Latent Space (Bottleneck) – compact feature representation
3. Decoder – reconstructs the original data from the compressed form.

In the proposed system, the autoencoder is trained only on normal (legitimate) signal data. In the course of such training, the model gets to know usual signal patterns and behavior.

Then during testing when a new signal is given as input, the autoencoder tries to reconstruct it based on what it learnt. If the input signal is normal and close to the training data, it will be reconstructed correctly and the error will be small. However, if the input signal is abnormal (e.g., due to attack such as active eavesdropping or pilot contamination), it will not match well with the learned patterns,

To detect anomalies, a threshold is used:

- If the reconstruction error is less than or equal to the threshold, the signal is considered normal.
- If the reconstruction error is greater than the threshold, the signal is considered anomalous.

This method is effective because it can detect unknown attacks without needing examples of those attacks during training.

The reconstruction error is given by:

$$Error = \|X - \hat{X}\|^2$$

X is original data and $\hat{X}$ is reconstructed output.

Subspace Projection Method (SPM)

The SPM is a signal processing and machine learning based technique for detection of anomalies, interference or hidden signals by projecting the data onto a learnt signal subspace and noise subspace.

In general, any high dimensional data vector can be represented as:

Data = Signal Component + Noise Component

The model is trained only on normal data. From this data it learns the main structure or pattern of the signals, and constructs the signal subspace. The remaining part, not following this pattern, is the noise (orthogonal) subspace. When a new signal arrives, it is projected on both subspaces the signal subspace tells us how much the data follows normal behaviour. The noise subspace is the extent to which the data differs from normal behavior.

The method checks how much energy (or information) lies in the noise subspace. This is given by:

$$e = \| U_n U_n^H y \|^2$$

- For normal data, this value is small.
- For abnormal data, this value becomes large.

A threshold (γ) is used to make the final decision:

- If $e \leq \gamma \rightarrow$ If the energy is less than or equal to the threshold → **Normal**
- If $e > \gamma \rightarrow$ If the energy is greater than the threshold → **Anomaly**

4. RESULTS DISCUSSION

Evaluating the performance of the proposed autoencoder and subspace projection approaches for anomaly detection under a variety of system parameters such as SNR, number of antennas, and eavesdropper transmit power.

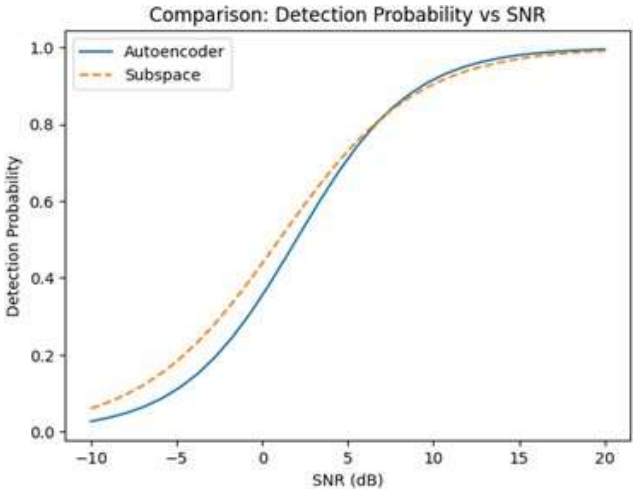


Fig. 2: Detection probability Vs SNR

The performance of the subspace projection method and the autoencoder at different SNR levels. The subspace method has a slightly better performance at low SNR as it is based on linear statistical properties and is relatively robust to noise.

As SNR increases to moderate and high levels, the autoencoder outperforms the subspace method. The reason for this improvement is the capability of the model to learn complex non-linear patterns in the data, which enable it to better discriminate between normal and anomalous signals when the signal quality is higher.

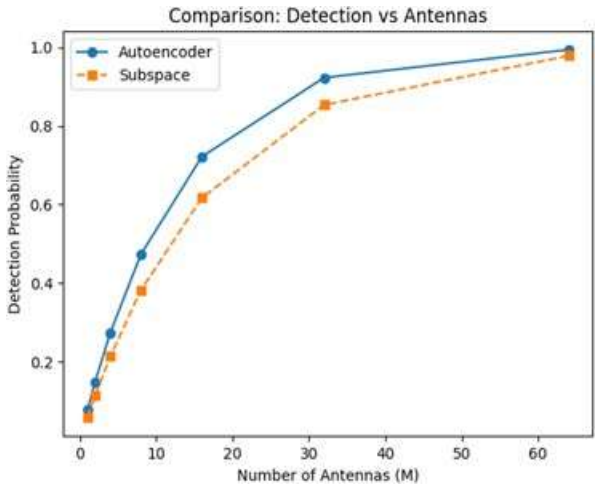


Fig. 3: Detection Probability Vs Number of antennas

The detection performance of both subspace projection method and autoencoder increases with the number of antennas. This is due to the fact that more antennas allow more spatial observations of the received signal, which improves the ability of capturing the underlying structure.

However, the autoencoder shows a higher detection probability than the subspace method for all the antenna configurations. This suggests that the additional spatial information is more exploited by the autoencoder.

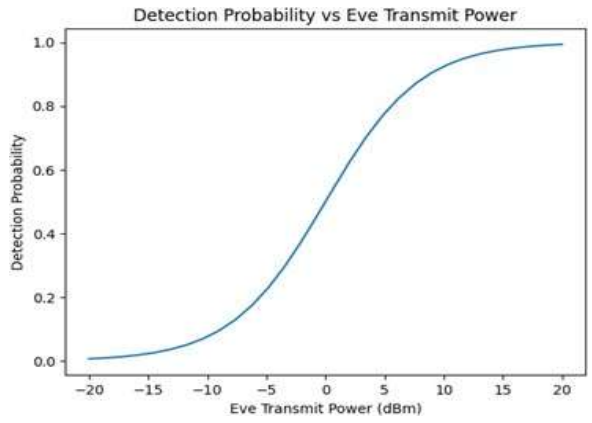


Fig. 4: Detection Probability Vs Transmit Power (Autoencoder)

The detection probability of is very low in lower transmit power levels. As the transmit power increases, the probability of detection increases gradually and then sharply. This is because the deviation from the normal signal structure is larger with a stronger eavesdropper signal. The detection probability tends to 1 with higher transmit power.

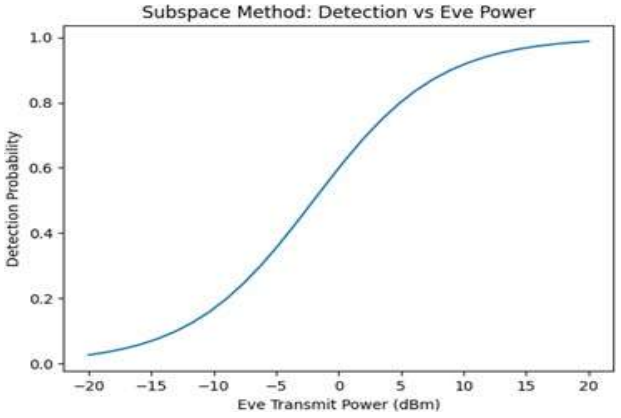


Fig. 5: Detection probability Vs Eve Transmit Power (Subspace Method)

To understand the effect of eavesdropper's, transmit power on detection performance, the change of signal characteristics due to the eavesdropper's transmit power is investigated. At low transmit power, the signal of the eavesdropper is very weak and is submerged in the noise. This does not influence the main eigenvalues of the signal thus it is difficult to detect for this reason. With increasing transmit power to moderate levels, the eavesdropper's signal begins to affect the structure of the signal. This results in significant changes in eigenvalues and improves the detection performance. At high transmit power the signal from the eavesdropper is strong and forms a new dominant eigenvalue. This makes the anomaly clearly visible and gives a high probability of detection.

4. CONCLUSION

The proposed anomaly detection method for detecting active eavesdropping attacks in wireless systems based on autoencoder and subspace projection technique. The autoencoder learns the normal patterns of the signal and detects anomalies based on the reconstruction error while the subspace method detects anomalies by measuring the change in the energy of the signal in the noise subspace. The results show that both methods work well in different

situations. The subspace method is more robust to noise and performs better at low SNR while the autoencoder can capture more complex signal patterns and performs better at moderate and high SNR. Moreover, the performance of detection is better for more antennas and higher transmit power of the eavesdropper. The proposed method shows good potential for improving security in future wireless systems against active attacks.

ACKNOWLEDGEMENT

Referee's insightful comments are appreciated by Authors.

REFERENCES

[1]. P. Chandra Sekhar and T. S. N. Murthy, "RSMO: Rider Spider Monkey Optimization-Based Artificial Noise Precoding Technique for Physical Layer Security in 5G Networks", Wireless Personal Communications, https://doi.org/10.1007/s11277-024-11166-4.

[2]. S. Rajasegarar, C. Leckie, and M. Palaniswami, "Anomaly detection in wireless sensor networks," IEEE Wireless Communications, vol. 15, no. 4, pp. 34–40, Aug. 2008.

[3]. V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Computing Surveys, vol. 41, no. 3, pp. 1–58, Jul. 2009.

[4]. Y. Zhang, N. Meratnia, and P. Havinga, "Outlier detection techniques for wireless sensor networks: A survey," IEEE Communications Surveys & Tutorials, vol. 12, no. 2, pp. 159–170, 2010.

[5]. Y. Li, M. Chen, and W. Dai, "A lightweight anomaly detection approach for wireless sensor networks," IEEE Systems Journal, vol. 11, no. 2, pp. 1–10, 2017.

[6]. N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41–50, Feb. 2018.

[7]. T. J. O'Shea and J. Corgan, "Convolutional radio modulation recognition networks," in Proc. International Conference on Engineering Applications of Neural Networks, 2016.

[8]. F. Restuccia, S. D'Oro, and T. Melodia, "Deep learning at the physical layer: System challenges and applications," IEEE Communications Magazine, vol. 56, no. 10, pp. 78–87, Oct. 2018.

[9]. X. Liu, Y. Liu, and A. Liu, "AI-enabled anomaly detection in IoT systems," IEEE Internet of Things Journal, vol. 7, no. 5, pp. 1–12, 2020.

[10]. R. Kumar, P. Singh, and A. K. Verma, "Deep learning-based anomaly detection using CSI in wireless networks," IEEE Access, vol. 9, pp. 1–12, 2021