Anomaly Detection of AGV Communication Failures in Factory Wi-Fi Network

Sunwoo Bang†, Jae Hong Shin*, and Jeongyeup Paek†

† Department of Computer Science and Engineering, Chung-Ang University, Seoul, Republic of Korea
* Manufacturing SW Platform R&D Team, Hyundai Motor Group, Uiwang-si, Gyeonggi-do, Republic of Korea
layer97@cau.ac.kr, shjh@hyundai.com, jpaek@cau.ac.kr

***Abstract*—With the rapid advances in wireless communication technologies that drive Industry 4.0 and pervasive automation, an ever-increasing share of factory operations is now performed by machines. Automated Guided Vehicle (AGV) is one of the wide-spreading technologies, and has become a cornerstone of modern smart factories, streamlining in-plant logistics and directly impacting on overall manufacturing productivity. As more facilities deploy AGVs, reliable wireless connectivity has emerged as a critical prerequisite for safe and efficient operation. However, field observations of production line AGVs operating over Wi-Fi wireless network reveal recurrent phenomena that point to latent communication failure. This paper defines these anomalies, explores a spectrum of detection strategies, and through a comparative study, identifies an anomaly detection approach well suited to factory Wi-Fi environments.**

***Index Terms*—Automated Guided Vehicle (AGV), Software Defined Factory (SDF), Anomaly Detection, Multivariate Time Series, Industrial Wireless, Industry 4.0**

I. Introduction

Factory automation is undergoing a rapid transformation under Industry 4.0, and the horizon has already extended toward software-defined factory (SDF), or software-defined manufacturing (SDM) [1], [2]. Among the technologies that underpin this transformation, automated guided vehicles (AGVs) have moved from pilot deployments to indispensable shop-floor assets, taking charge of material handling, and delivery. To perform tasks safely and efficiently, an AGV must exchange time-critical commands, status reports, and sensor data with higher-level controllers. To execute such tasks, AGVs must maintain continuous communication with a central controller over the wireless network to receive control commands, making low latency links indispensable. If an AGV experiences high latency or, worse, loses connectivity, its operation may halt. This problem could leads disrupting part or all of factory operations and resulting in severe productivity losses. Indeed, according to prior works [3]–[5], low latency is suggested as one of the key challenges of AGV deployments on factories.

Provisioning a wireless environments for AGVs can be broadly categorized into two approaches: cellular-based methods (LTE/5G) and Wi-Fi-based methods (Wi-Fi 6/6E). While private 5G promises ultra-reliable low latency communication (URLLC) under licensed spectrum, Wi-Fi remains attractive for its low cost and ease of deployment and management, as well as seamless integration with existing infrastructure. During field measurements in a production plant that relies on Wi-Fi, as shown in Fig. 1, we repeatedly observed intermittent disconnections between AGVs and access points (APs). Because link disconnection can trigger cascade into process delays, early detection and mitigation of such disconnections are essential.

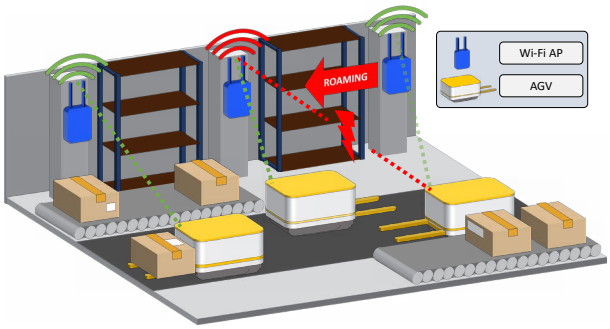


Fig. 1: Overview of AGV disconnection scenario.

AGVs and APs continuously generate diverse metrics such as RSSI, bitrate, and network throughput, and anomaly detection in industrial sensor data remains a challenging research problem [6]. One of the methods for detecting disconnections using these streams is to treat the problem as binary classification. Well-established gradient boosting models such as XGBoost [7] or LightGBM [8] can deliver high accuracy with reasonable computational overhead, provided that representataive positive samples are available. But when the feature space grows complex and the class imbalance gap widens, such supervised classifiers could suffer due to too few fault samples to capture their patterns. Because of this limitation, recent work favors unsupervised or self-supervised anomaly detection models [9]–[12] that train only on normal data. Each method carries its own trade-offs, and the choice depends on the statistics of the data and the constraints of the deployment environment.

This research was supported by the Hyundai Motor Group, also by the MSIT(Ministry of Science, ICT), Korea, under the National Program for Excellence in SW), supervised by the IITP(Institute of Information & communications Technology Planning & Evaluation) in 2025 (2025-0-00032).

J. Paek is the corresponding author.

TABLE I: Total dataset analysis

Disconnection number	1164 times
Total disconnection time	5,489 sec (2,745 timesteps)
Data size (Timestep)	336,292,330 timesteps
Disconnection ratio	0.00082 %

The contributions of this paper are as follows:

- Analyze real-world traces from AGVs and Wi-Fi APs in a real car manufacturing factory and quantify their disconnection phenomena.
- Evaluate both supervised and unsupervised methods for anomaly detection, and identify the method that best balances accuracy and computational overhead.

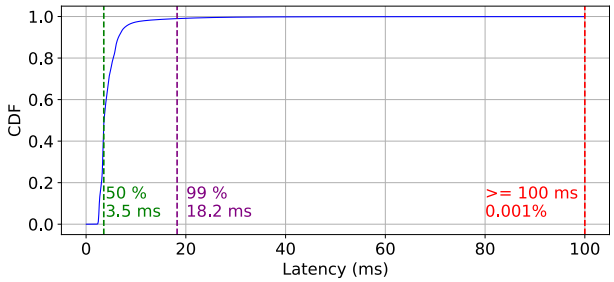
II. Related Work

There are extensive efforts to guarantee the seamless operation of AGVs on the factory floor [13]–[15]. Ohori et al. [13] proposed a method for predicting wireless link quality to detect and avoid AGV communication failure due to AP selection with additional sensors that measure communication metrics. Shi et al. [14] proposed an algorithm that dynamically allocates time slots under strict ordering constraints, ensuring reliable AGV communications. However, these approaches require either additional hardware or a complete overhaul of mechanism, making large-scale deployment and test in real-world AGV fleets highly challenging. Consequently, this paper focuses on the approaches that leverage the telemetry data already produced by AGVs and APs to predict, detect, or prevent communication failures without modifying the control stack.

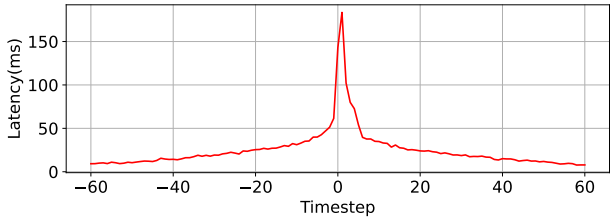
By modeling the telemetry generated by AGVs and APs as a multivariate time series, we can apply state-of-the-art time series anomaly detection techniques directly to factory environments. Su et al. [10] proposed stochastic recurrent neural network model utilizing variational autoencoder to calculate reconstruction error of time series. Nizam et al. [12] proposed two-stage LSTM autoencoder model to detect extremely rare anomalous events on Industrial Internet of Things (IIoT) streaming data. Zhao et al. [9] proposed parallel graph attention network with simple forecasting-reconstruction hybrid model that trying to capture the relationships between different time series. While these models achieve impressive accuracy on public datasets such as server machine dataset (SMD) or secure water treatment (SWaT) dataset, their suitability for latency-sensitive factory Wi-Fi telemetry remains unexplored. In this paper, approaches proposed in prior works will be tested and evaluated on real-world manufacturing AGVs.

III. Methodology

This section presents data analysis, labeling methodology, and the approaches evaluated.



(a) CDF of AGV latency.



(b) Average latency around disconnection.

Fig. 2: Statistics of latency data. For clairity, values are clipped on 200 ms. Fig. 2(b) suggests that high-latency events can be triggered by disconnections.

A. Data Analysis

The data were collected from a real car manufacturing factory in United States for over 108 days from December 2024 to March 2025, involving more than 40 APs and 80 AGVs in operation. Since disconnections exceeding 3 seconds noticeably disrupt factory operations, we counted only such events and the result is shown in Table I.

Although disconnections occur at least once per day and constitute a significant source of productivity loss, the corresponding dataset contains only a handful of examples, making it too sparse for direct use in model training. Consequently, disconnections must be detected through indirect indicators. The key indicator is round-trip latency between an AGV and its AP. Fig. 2(a) shows that in the majority of scenarios, the latency remains under 20 ms. However, there are clearly instances in which the latency exceeds 100 ms. As shown in Fig. 2(b), latency becomes highly unstable immediately before and after each recorded disconnection. This escalation reflects a surge in packet loss rate, providing a reliable warning of an impending communication failure.

Another informative signal is the occurrence of Wi-Fi roaming events. Analysis revealed that approximately 27% of all disconnections and up to 81% of severe disconnection cases exceeding 6 seconds are tightly coupled to Wi-Fi roaming failures. Therefore, roaming events which have clear relationship with disconnections were also treated as anomalies and included in our tests.

B. Approaches

Two approaches are tested and compared on collected dataset. Most edge devices, including AGVs, are constrained in memory and compute. Therefore, a lightweight binary

TABLE II: Result of anomaly detection (P: precision, R: recall).

	Binary Classifier [7]			Deep Learning [9]		
Anomaly	F_1	P	R	F_1	P	R
Roaming	**0.92**	0.87	0.97	0.86	0.76	0.99
Latency	0.63	0.79	0.52	**0.77**	0.72	0.84
All	0.83	0.85	0.81	**0.88**	0.84	0.93

classifier becomes an attractive choice. Among the binary classification algorithms, ensemble methods, especially algorithms based on Gradient Boosting Decision Tree [16] are the most widely adopted and effective in practice. Several classifiers such as AdaBoost [17], XGBoost [7] and LightGBM [8] were evaluated on the collected dataset. XGBoost achieved the highest performance and was therefore selected as the baseline model for comparison with the deep learning approach.

A second possible approach is leveraging contemporary deep learning techniques, which have become central to anomaly detection studies. Accurate anomaly detection depends on a powerful representation of multivariate time series. Graph attention embeddings are particularly attractive because they automatically learn dependencies between features, enabling the model to detect inter-feature anomalies effectively. Consequently, one of the state-of-the-art models, MTAD-GAT [9] has been adopted as the deep learning baseline[1].

IV. Evaluation

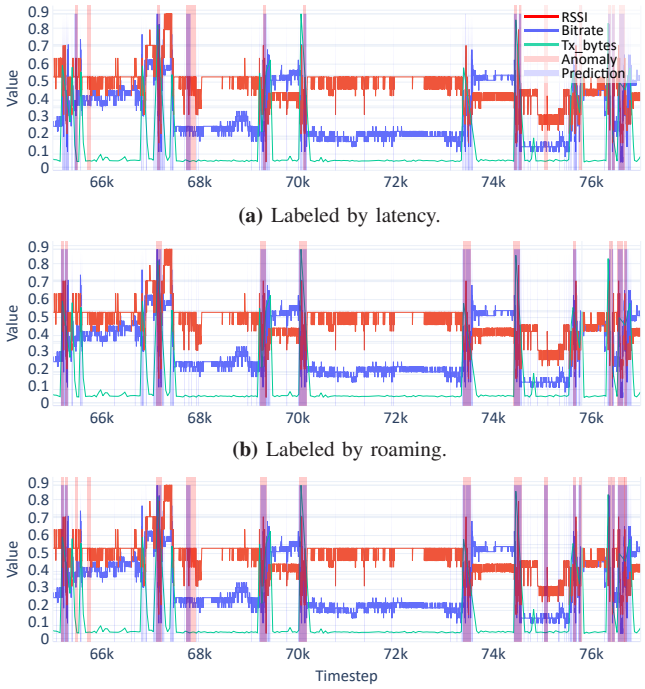
Selected baseline models are trained on the data of a single AGV and their performance is compared in this section. All experiments were conducted on a workstation with an Intel Core i9-9900k CPU, Nvidia RTX 2080 with 8GB VRAM, and 32GB RAM. Operating system was Ubuntu 20.04.6 LTS, running python 3.11 and CUDA 11.8. Hyperparameters such as window size are tuned using a grid-search strategy. Three input features were used, namely received signal strength indicator (RSSI), bitrate, and the bytes transmitted by AGV. Evaluation was conducted using F_1 score, with point adjustment as proposed by Xu et al. [18].

The experimental results are summarized in Table II, revealing the distinct strengths of each model across the evaluated metrics. On the dataset labeled by Wi-Fi roaming events, the binary classifier model significantly outperform the deep learning model, likely because roaming exhibits consistent and distinctive patterns. In contrast, on the dataset labeled by high-latency events and on the dataset labeled by both roaming and latency criteria, the deep learning model demonstrated superior performance. High-latency events arise from a variety of underlying causes and manifest heterogeneous patterns, which makes detection complex. This complexity explains why the deep learning model's ability to learn intricate feature relationships gives it an advantage in these cases. Table III presents the training and inference times for each model. Under a real-time streaming anomaly-detection scenario, it demonstrates that inference times differ roughly between the two approaches. Considering typical sampling rates and the constrained edge device resources, this results underscore the importance of model compression or light-weight strategies when deploying deep learning based models.

[1]https://github.com/ML4ITS/mtad-gat-pytorch.git

TABLE III: Training and inference time of each baseline model.

	Binary Classifier	Deep Learning
Training (sec)	**3.84**	942
Inference (ms)	**0.25**	2.49



(a) Labeled by latency.

(b) Labeled by roaming.

(c) Labeled by latency and roaming.

Fig. 3: Sample results of anomaly detection using a deep learning method on each labeled dataset. Values are normalized between 0 and 1. Red, blue, and green lines denote RSSI, bitrate, transmitted bytes, respectively. Red and blue shaded regions indicate ground truth and predicted anomalies, respectively.

Additionally, it turned out that false positives in the deep learning model on latency-labeled data were strongly affected by roaming events. Fig. 3 shows the sample result of deep learning method. In Fig. 3(a) and Fig. 3(b), false positives occurred at the locations labeled for the other event in each case. Furthermore, when both roaming and high-latency events were treated as anomaly, the model successfully detected anomalies that had gone undetected previously. This indicates that the model confuses the Wi-Fi roaming events with high-latency situations, underscoring the need for a model capable of distinguishing genuine high-latency faults from routine roaming behavior.

V. Conclusion

In this paper, we analyzed real-world manufacturing data from a factory, and explored methods for detecting AGV communication failures within factory Wi-Fi environment.

Comparative experiments demonstrated the detection capabilities and respective strength of each approach across datasets labeled by high-latency and Wi-Fi roaming events. We validated the effectiveness of the deep learning approach under general conditions and identified its remaining weaknesses. Future work will focus on classifying which labeled events actually lead to disconnections and on developing a model capable of distinguishing genuine high-latency fault from routine Wi-Fi roaming events.

ACKNOWLEDGEMENT

We thank the Hyundai Motor Group's Manufacturing SW Platform R&D Team within the Manufacturing Solution Division for providing us with real AGV–AP Wi-Fi communication logs from their car manufacturing factory in operation.

REFERENCES

[1] Y. Koyasako, T. Suzuki, T. Hatano, T. Shimada, and T. Yoshida, "Full Software-Defined Factory Networks by Industrial Ethernet Protocol Softwarization," in *IEEE 20th Consumer Communications & Networking Conference (CCNC)*, 2023, pp. 885–886.

[2] P. Grimmeisen, A. Wortmann, and A. Morozov, "Case study on automated and continuous reliability assessment of software-defined manufacturing based on digital twins," in *Proceedings of the 25th International Conference on Model Driven Engineering Languages and Systems: Companion Proceedings (MODELS)*, 2022, p. 511–518.

[3] Kampen, Anna-Lena and Fojcik, Marcin and Cupek, Rafal and Stoj, Jacek, "The requirements for using wireless networks with AGV communication in an industry environment," in *17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2021, pp. 212–218.

[4] Qiao, Yue and Fu, Yusun and Yuan, Muyun, "Communication–Control Co-Design in Wireless Networks: A Cloud Control AGV Example," *IEEE Internet of Things Journal*, vol. 10, no. 3, pp. 2346–2359, 2023.

[5] Zhou, Ying and Feng, Zhiyong and Song, Zhiqun and Wei, Zhiqing and Ma, Dingyou and Meng, Zeyang and Cui, Yanpeng and Pang, Yashan and Zhang, Ping, "Integrated Sensing, Communication, and Control Driven Multi-AGV Closed-Loop Control," *IEEE Transactions on Vehicular Technology*, 2025.

[6] S. Luo, P. Zeng, C. Ma, and Y. Wei, "Anomaly detection for industrial Internet of Things devices based on self-adaptive blockchain sharding and federated learning," *Journal of Communications and Networks*, vol. 27, no. 2, pp. 92–102, 2025.

[7] Chen, Tianqi and Guestrin, Carlos, "XGBoost: A Scalable Tree Boosting System," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2016, p. 785–794.

[8] Ke, Guolin and Meng, Qi and Finley, Thomas and Wang, Taifeng and Chen, Wei and Ma, Weidong and Ye, Qiwei and Liu, Tie-Yan, "LightGBM: A Highly Efficient Gradient Boosting Decision Tree," in *Advances in Neural Information Processing Systems*, vol. 30, 2017.

[9] H. Zhao, Y. Wang, J. Duan, C. Huang, D. Cao, Y. Tong, B. Xu, J. Bai, J. Tong, and Q. Zhang, "Multivariate Time-Series Anomaly Detection via Graph Attention Network," in *IEEE International Conference on Data Mining (ICDM)*, 2020, pp. 841–850.

[10] Y. Su, Y. Zhao, C. Niu, R. Liu, W. Sun, and D. Pei, "Robust Anomaly Detection for Multivariate Time Series through Stochastic Recurrent Neural Network," in *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2019, p. 2828–2837.

[11] Z. Chen, D. Chen, X. Zhang, Z. Yuan, and X. Cheng, "Learning Graph Structures With Transformer for Multivariate Time-Series Anomaly Detection in IoT," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9179–9189, 2022.

[12] H. Nizam, S. Zafar, Z. Lv, F. Wang, and X. Hu, "Real-Time Deep Anomaly Detection Framework for Multivariate Time-Series Data in Industrial IoT," *IEEE Sensors Journal*, vol. 22, no. 23, pp. 22 836–22 849, 2022.

[13] OHORI, Fumiko and ITAYA, Satoko and OSUGA, Toru and KOJIMA, Fumihide, "Estimating Wireless Link Quality using Multiple Remote Sensors for Wireless Control of AGV in a Factory," in *23rd International Symposium on Wireless Personal Multimedia Communications (WPMC)*, 2020, pp. 1–6.

[14] H. Shi, M. Zheng, W. Liang, J. Zhang, K. Wang, and S. Liu, "Transmission Scheduling With Order Constraints in WIA-FA-Based AGV Systems," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 381–392, 2021.

[15] Y. Qiao, Y. Fu, and M. Yuan, "Communication–Control Co-Design in Wireless Networks: A Cloud Control AGV Example," *IEEE Internet of Things Journal*, vol. 10, no. 3, pp. 2346–2359, 2023.

[16] J. H. Friedman, "Greedy function approximation: a gradient boosting machine," *Annals of statistics*, pp. 1189–1232, 2001.

[17] Y. Freund and R. E. Schapire, "A Decision-Theoretic Generalization of On-Line Learning and an Application to Boosting," *Journal of Computer and System Sciences*, vol. 55, no. 1, pp. 119–139, 1997.

[18] H. Xu, W. Chen, N. Zhao, Z. Li, J. Bu, Z. Li, Y. Liu, Y. Zhao, D. Pei, Y. Feng, J. Chen, Z. Wang, and H. Qiao, "Unsupervised Anomaly Detection via Variational Auto-Encoder for Seasonal KPIs in Web Applications," in *Proceedings of the World Wide Web Conference (WWW)*, 2018, p. 187–196.