Diagnosing AGV Wi-Fi Disconnection via dmesg Logs: A Real-World Factory Case Study

Suhwan Bae†, 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
bbiddak99@cau.ac.kr, shjh@hyundai.com, jpaek@cau.ac.kr

***Abstract*—Automated Guided Vehicles (AGVs) are fundamental to smart factory operations, yet maintaining stable Wi-Fi connectivity remains a significant challenge, as disconnections disrupt workflows and reduce productivity. We present a log-centric diagnosis method that parses kernel (dmesg) logs from production AGVs, extracts Wi-Fi-related events, and classifies event sequences into patterns. Analyzing a 3.5-month dataset from an automotive manufacturing factory, we identify eight recurring disconnection patterns and map each to its proximate cause. The resulting pattern-to-cause mapping provides practical insights for diagnose and mitigation. To our knowledge, this is the first systematic study to diagnose AGV Wi-Fi disconnections using kernel logs. Our method and findings offer a practical guideline that other plants can apply to address Wi-Fi disconnections, enabling faster diagnosis and more effective remediation of AGV connectivity issues in industrial environments.**

***Index Terms*—Automated Guided Vehicle (AGV), Smart Factory, Wi-Fi Disconnection, Kernel Log Analysis**

I. Introduction

In smart factories, AGVs have come to be essential for improving productivity and operational efficiency [1]. AGVs autonomously transport materials and components between different locations within the factory, being controlled by a central system over a wireless network. However, factors such as roaming between access points (APs), radio interference from multiple devices, and communication failures within either the APs or the AGVs can lead to wireless disconnection events [2]. Such disconnections may cause AGVs to stop unexpectedly or deviate from their intended paths, ultimately resulting in decreased productivity [3], as illustrated in Fig. 1. Understanding the characteristics of these disconnection events is therefore crucial.

Prior studies have primarily examined AGV connectivity at the network level. For example, Ostrowski and Szulewski [4] analyzed Wi-Fi communication of AGVs on a factory shop floor, using network-level metrics such as signal strength, noise levels, and throughput to assess the feasibility of wireless connectivity in industrial environments. While such work provides valuable insights into the radio-level constraints of AGV communication, network-level metrics alone cannot explain the underlying causes of disconnection events, as they provide only performance indicators without revealing whether a failure stems from roaming issues or authentication problems.

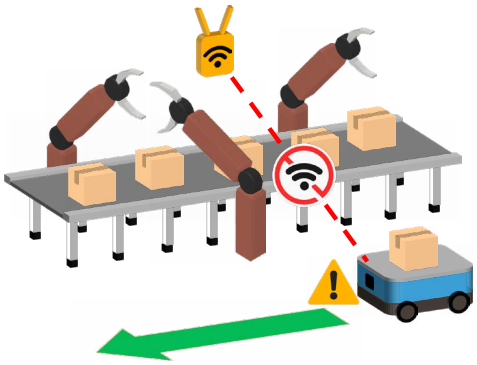

Fig. 1: Illustration of a Wi-Fi disconnection event. The AGV, following its designated path, halts due to the loss of network connectivity.

In contrast, kernel log (dmesg) data provides system-level information that captures device behaviors around disconnection events, such as roaming triggers and disconnection reasons. However, to the best of our knowledge, no prior study has analyzed dmesg logs to examine the underlying behaviors associated with AGV wireless disconnections in a smart factory environment. Therefore, we analyzed over 300 disconnection events recorded in dmesg logs from AGVs operating in a large automotive factory, identifying recurring patterns that characterize these events.

In summary, this study makes three primary contributions:

- Present the first systematic analysis of kernel log (dmesg) data associated with AGV wireless (Wi-Fi) disconnections in a smart factory.
- Identify eight recurring patterns in these logs, transforming raw, unstructured messages into interpretable categories.
- Provide foundational knowledge that can assist engineers in quickly understanding and diagnosing AGV disconnection events, forming a basis for future diagnostic and mitigation strategies in industrial environments.

This work was supported by the Hyundai Motor Group, also by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. RS-2024-00359450), and also by the Institute of Information & Communications Technology Planning & Evaluation(IITP)-ITRC(Information Technology Research Center) grant funded by the Korea government(MSIT)(IITP-2025-RS-2022-00156353).

J. Paek is the corresponding author.

II. Factory Environment & Dataset

In this section, we describe the factory environment in which the AGVs operate and provide details of the dataset used for analyzing Wi-Fi disconnection events.

A. Factory Environment

The dataset we analyzed was collected from the car manufacturing factory, where dozens of APs are installed and several dozen AGVs are in operation. The APs are roughly evenly spaced throughout the factory and communicate with the AGVs using the IEEE 802.11ax (Wi-Fi 6) standard [5]. The AGVs rely on the Wi-Fi network provided by the APs for control and autonomously navigate the factory to transport materials between production zones.

B. Dataset

The dataset used for AGV Wi-Fi disconnection analysis comprises monitor logs and dmesg logs collected from the AGVs over a 3.5 months period. Details of the two log sources are as follows:

- **monitor logs** are generated by user-space scripts (e.g., `network_monitoring.sh`, `network_status.sh`) and record high-level Wi-Fi events, including roaming sequences and disconnection events.
- **dmesg logs** are generated at the kernel level and contain system messages timestamped with millisecond resolution, including roam triggers (e.g., "LOW RSSI"), the result of each roaming attempt (success or failure) with associated failure reasons, and disconnect events with reason codes.

Initially, we defined a Wi-Fi disconnection lasting longer than 6 seconds as a failure condition, but only 181 such events occurred over the 3.5 months period, limiting our ability to conduct an in-depth analysis. In contrast, disconnections of 3 seconds or more occurred 1,131 times and many of these likely extended beyond 6 seconds, so we adopted 3 seconds as our final failure threshold.

We extracted all disconnection events lasting at least 3 seconds from the monitor logs. For each event, we additionally retrieved dmesg logs within a $\pm$5-second window to capture relevant kernel-level events surrounding the disconnection, such as preceding roaming events and subsequent recovery messages. Of the 1,131 disconnection events identified in the monitor logs, only 331 remained after excluding cases with missing or incomplete dmesg logs. These 331 events and their associated dmesg logs formed the basis for analyzing kernel-level log patterns that occur during Wi-Fi disconnections.

III. dmesg Log Analysis Methodology

The dmesg logs are highly variable and largely unstructured, which makes direct log analysis infeasible. To address these challenges, we adopted a three-stage workflow:

1) **Preprocessing:** integrate dmesg timestamps, sort entries, remove duplicate logs, and extract logs within a $\pm$5-second window around each disconnection event.
2) **Keyword Highlighting:** select keywords essential for disconnection analysis and highlight keywords.
3) **Pattern Classification:** classify cases by frequent patterns and define them by the first trigger.

Keyword Type	Percentage	Message
Disconnect Reason Code	97.29%	`DEAUTH_LEAVING, PREV_AUTH_NOT_VALID`
Roam Trigger	89.46%	`LOW RSSI, BEACON MISS`
Roam Result	89.46%	`Disconnect received during handoff`
Authentication	97.89%	`Dauth TX, Deauth RX`
Other Errors	62.95%	`sme_get_beacon_frm failed`

TABLE I: dmesg keywords essential for Wi-Fi disconnection analysis with occurrence percentages during disconnection events and example log entries

The following subsections describe each step in detail.

A. Preprocessing

Raw dmesg logs include two timestamps. We interpret the first as the kernel print time and assume the second corresponds to function execution time. These logs are sometimes out of chronological order and can contain duplicates.

Because the two timestamps in dmesg logs had complementary inaccuracies, with one providing reliable hours but less precise minutes and seconds and the other offering precise millisecond-level resolution but unreliable hours, we combined their accurate components to construct an integrated timestamp for analysis. We then sorted all logs based on this integrated timestamp and finally removed duplicate logs. As described in section II-B, we consider disconnection events lasting at least 3 seconds as the target of our analysis. For each event, we extracted dmesg logs from 5 seconds before the disconnection began to 5 seconds after it ended.

This stage provides the preprocessed dmesg logs required for the next stage of analysis.

B. Keyword Highlighting

dmesg logs contain messages from various kernel subsystems, including the networking stack and device drivers, generating dozens of logs per second. Of the several hundred lines in the dmesg logs extracted in the previous stage, some include keywords that are essential for disconnection analysis. In this stage, we highlight these keywords to focus the analysis on the most informative logs related to Wi-Fi disconnections.

Table I summarizes the keywords we selected for Wi-Fi disconnection analysis. These keywords provide both direct and indirect evidence for diagnosing disconnection events. Disconnect Reason were observed in 323 of 331 events (97.29%) and offer strong clues about the cause of connection loss. Roaming-related messages—both Roam Triggers and Roam Results—appeared in 297 of 331 events (89.46%) immediately before and after disconnections, indicating their likely relevance to disconnection events. Auth messages appeared in 325 events (97.89%) help determine who—AP or AGV—initiated the disconnection. Finally other error conditions like

`sme_get_beacon_frm failed`, which occurred in 209 of 331 events (62.95%), serve as indirect indicators of disconnection behavior.

We highlighted these keywords to focus our analysis on the most informative log segments, which was helpful for the subsequent analysis stage.

C. Pattern Classification

Because dmesg logs exhibit high variability, we concentrated on the most frequent patterns to cluster cases by category. Using the keywords highlighted in the previous stage, we conducted exhaustive manual classification of all 331 disconnection cases. When more than one trigger appears in the same disconnection case, we label the case by the earliest occurring trigger.

The majority of disconnection events (85.84%) began with an AGV roaming attempt, after which a series of logs repeated within a few seconds leading to a disconnect, regardless of roaming result. By focusing on roaming keywords, Disconnect Reason, and Auth/Assoc messages, we identified consistent log-sequence patterns. We also observed necessary-and-sufficient patterns, such as the co-occurrence of `sme_get_beacon_frm failed` and `FORCED SCAN` messages.

This three-stage workflow enabled us to capture the characteristic sequence of each disconnection event. The detailed analysis results are presented in the following section.

IV. Analysis Result: dmesg Log Patterns

In this section, we present the patterns identified by analyzing the dmesg logs from 331 disconnection events. We observed three primary scenarios leading to Wi-Fi disconnection—roaming failure, roaming success, and non-roaming event—which together manifest as eight distinct dmesg log patterns. The following subsections describe these scenarios in detail, presenting the observed log patterns and the direct causes of the Wi-Fi disconnections.

A. Roaming Failure

As shown in Table II, the most frequently observed disconnection pattern (28.91%) occurred when an AGV failed to roam. In this scenario, the dmesg logs exhibit a specific sequence and combination of messages.

First, logs indicating a roaming attempt appear just before the disconnection, followed by the roaming failure reason, `Disconnect received during handoff`. This message indicates that the AGV received an abnormal disconnection notification during the handoff process, where control is passed from the existing AP to a new one.

Subsequently, the disconnect reason is specified as `WLAN_REASON_UNSPECIFIED`. While this field typically records a reason code defined in the IEEE 802.11 standard [6], this pattern tends to show an internal roaming failure code used by the Wi-Fi chipset manufacturer instead.

The combination of these two logs strongly suggests that the disconnection was not caused by an issue with the AP or network infrastructure, but rather by a roaming process failure at the AGV's Wi-Fi chip, firmware, or driver level. Disconnections corresponding to this pattern lasted for an average of 5.1 seconds, with a maximum duration of 24 seconds (see Table II), leading to operational halts for the AGV.

Pattern	Percentage	Duration(s) mean [min–max]
Roaming Failure		
ROAM FAILURE	28.91%	5.1 [3–24]
Roaming Success		
Fail To Get Beacon Frame	23.79%	5.2 [3–23]
DEAUTH LEAVING	19.57%	9.3 [7–30]
DEAUTH RECEIVED	14.15%	5.4 [3–9]
Non-Roaming		
DEAUTH LEAVING	7.53%	7.4 [3–26]
PREV AUTH NOT VALID	4.21%	3.8 [3–5]
Failed to process addba	1.20%	3.0 [3–3]
PER (Packet Error Rate)	0.60%	3.2 [3–4]

TABLE II: Summary of the eight dmesg log patterns identified during disconnection events, showing their categorization, occurrence percentage, and duration statistics.

B. Roaming Success

Our analysis revealed a somewhat counterintuitive finding: the most dominant disconnection scenario, accounting for 57.53% of all disconnection cases, occurs after a successful roam and is categorized into the three main patterns discussed in the following paragraphs.

1) Fail To Get Beacon Frame: The first pattern appears to stem from a discrepancy between a successful chipset-level roam and the final host-level connection establishment. This issue manifests as two specific error logs recorded after roaming: `parse_scan_result failed` and `sme_get_beacon_frm failed`. According to the Wi-Fi chipset's driver code [7], these functions are responsible for retrieving the new AP's beacon information from the scan cache. Their failure indicates that although the Wi-Fi chipset completed its physical handshake, the host driver could not acquire the necessary, up-to-date AP status information required for communication. This incomplete process ultimately leads to a disconnection and forces the AGV to trigger a `FORCED SCAN`, which is an inefficient attempt to re-establish a connection with the same AP.

2) DEAUTH LEAVING: The second pattern is characterized by a specific Disconnect Reason. The AGV reports a `WLAN_REASON_DEAUTH_LEAVING` message, which means the AGV is leaving the network [6]. A subsequent `Deauth TX to AP` log is observed, which clearly indicates that the entity initiating the disconnection is not the AP, but the AGV itself. This suggests that a successful roam does not guarantee a stable connection, as the AGV may terminate the session for internal reasons. Notably, this pattern exhibited the most prolonged disconnections, with both the longest average

duration of 9.3 seconds and the longest maximum duration of 30 seconds.

3) DEAUTH RECEIVED: The final pattern involves initiating another roam using `DEAUTH RECEIVED` as the Roam Trigger, immediately after a successful roam. In the third pattern, after a successful roam, the AGV attempts to initiate another roam using `DEAUTH RECEIVED` as the Roam Trigger. This suggests that the AP is the entity initiating the disconnection. Notably, unlike other patterns that follow a successful roam, this pattern is not prolonged, with a maximum duration of 9 seconds.

In summary, these patterns reveal that a successful roam does not guarantee a stable connection.

C. Non-Roaming

The Non-Roaming scenario, which does not involve any roaming attempts prior to the disconnection, accounts for 13.55% of all disconnection cases. While less frequent than roaming-related disconnections, these events are noteworthy. With the exception of the DEAUTH LEAVING pattern, network connectivity is typically restored within 5 seconds. We identified four distinct patterns within this scenario, which are detailed below.

1) DEAUTH LEAVING: The first pattern is analogous to the one discussed in the Roaming Success scenario (§IV-B). The only significant difference is that this disconnection occurs while the AGV is connected to its current AP, without any preceding roaming attempt. Aside from this, the log sequence is identical, featuring the `WLAN_REASON_DEAUTH_LEAVING` reason code and a subsequent `Deauth TX to AP` log. This pattern is the most severe in non-roaming patterns, exhibiting the longest average and maximum disconnection durations.

2) PREV AUTH NOT VALID: The second pattern begins with a `Deauth RX from AP` message, immediately followed by a `WLAN_REASON_PREV_AUTH_NOT_VALID` reason code. This reason code indicates that the AGV is associated but not authorized, suggesting that the AP terminated the connection, likely because the AGV's authentication had expired. In this case, network connectivity is quickly restored, typically within 5 seconds.

3) Failed to process addba request: In the third pattern, disconnection is preceded by `Failed to process addba request` log. The Add Block Acknowledgment (AddBA) request is an efficiency-enhancing feature of the IEEE 802.11 standard [8] that allows multiple data frames to be acknowledged with a single response. The failure to process these requests appears to be the cause of the subsequent disconnection.

4) PER (Packet Error Rate): The final pattern is unique in that the AGV initiates a roam due to a high Packet Error Rate (PER) approximately four seconds after the initial disconnection. This suggests the initial disconnection was caused by poor link quality or congestion at the connected AP, which subsequently triggered the AGV to seek a better connection.

In summary, these patterns show that disconnections can occur for various reasons, even when an AGV remains connected to a single AP without attempting to roam.

V. Conclusion

This study diagnosed AGV Wi-Fi disconnections in a real-world factory by analyzing dmesg logs. Our analysis of 331 disconnection cases identified eight distinct dmesg log patterns across three primary scenarios including Roaming Failure, Roaming Success, and Non-Roaming. The significance of this work lies in applying these patterns to help determine whether the source of failure is internal to the AGV, the AP, or their interaction, revealing details unavailable through network-level metrics alone. This provides a crucial foundation for faster and more accurate troubleshooting.

We acknowledge, however, that while this dmesg analysis effectively identifies the direct causes of disconnection, determining the ultimate root causes remains beyond the scope of this study. Future work should therefore focus on conducting deeper investigations to determine the ultimate root cause of each identified pattern.

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] Oyekanlu, Emmanuel A. and Smith, Alexander C. and Thomas, Windsor P. and Mulroy, Grethel and Hitesh, Dave and Ramsey, Matthew and Kuhn, David J. and Mcghinnis, Jason D. and Buonavita, Steven C. and Looper, Nickolus A. and Ng, Mason and Ng'oma, Anthony and Liu, Weimin and Mcbride, Patrick G. and Shultz, Michael G. and Cerasi, Craig and Sun, Dan, "A Review of Recent Advances in Automated Guided Vehicle Technologies: Integration Challenges and Research Areas for 5G-Based Smart Manufacturing Applications," *IEEE Access*, vol. 8, pp. 202 312–202 353, 2020.

[2] 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.

[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] I. Ostrowski and P. Szulewski, "The initial analysis of wifi communication (data interchange) for agv on the factory shop floor," 09 2015.

[5] Rohde & Schwarz, "IEEE 802.11ax Technology Introduction," White Paper, 2019. [Online]. Available: https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/premiumdownloads/premium_dl_brochures_and_datasheets/premium_dl_whitepaper/IEEE-802-11ax-Technology-Introduction_wp_3609-9470-52_v0100.pdf

[6] Università degli Studi di Trieste, "Tabella dei codici di deautenticazione WiFi," Web page. [Online]. Available: https://docu.units.it/dokuwiki/tabelle:wifi_deauth_reason

[7] EssentialOpenSource, "qcacld-3.0: Qualcomm Atheros WLAN CLD3.0 Driver," GitHub repository. [Online]. Available: https://github.com/EssentialOpenSource/qcacld-3.0

[8] The INET Framework Developers, "Showcase: Blockack," https://inet.omnetpp.org/docs/showcases/wireless/blockack/doc/index.html, 2022, [Online; accessed 6-August-2025].