Security Limitations of the CAN Bus and Detection through Power Fingerprinting

Ken Broden
brod0268@morris.umn.edu
Division of Science and Mathematics
University of Minnesota, Morris
Morris, Minnesota, USA

Abstract

This paper examines the vulnerabilities of the Controller Area Network (CAN), the standard communication protocol used in most modern vehicles. It explains why CAN is widely adopted and outlines key security weaknesses in its design. The paper then reviews recent research efforts to detect and mitigate these vulnerabilities, with particular focus on an approach to origin authentication that relies on the unique power consumption patterns of each individual electronic control unit on a CAN bus.

Keywords: CAN, automotive software, cybersecurity, embedded systems

1 Introduction

Modern vehicles rely on Controller Area Network (CAN) for fast and reliable communication among many embedded Electronic Control Units (ECUs). As automotive technology has advanced, vehicles now depend on dozens of ECUs for safety, performance, and convenience functions. CAN was originally developed in the 1980s and remains the industry standard today because it is lightweight and robust [5]. However, it was not designed with modern connectivity or cybersecurity requirements in mind. As vehicles continue to gain wireless interfaces and increasingly complex software, the absence of built-in message authentication has become a significant security concern for both manufacturers and consumers [3].

1.1 Motivation

Concerns about CAN security grew sharply after researchers Miller and Valasek demonstrated a remote compromise of a Jeep Cherokee in 2015 [4]. They were able to control several critical functions, including braking behavior, dashboard displays, radio output, and lighting systems by injecting unauthenticated CAN messages. This incident made clear that once an attacker gains access to a vehicle's internal network, they can influence many safety-relevant subsystems. As vehicles continue to add more ECUs and remote connectivity features, these attack opportunities will continue to expand. Because of this, the automotive industry needs methods to verify whether a CAN message truly originates from the ECU that claims to have sent it.

1.2 Purpose of Paper

The purpose of this paper is to explain and evaluate a research strategy developed by engineers at the University of Waterloo that aims to detect unauthenticated CAN messages by identifying the physical origin of each transmission. To support this discussion, the paper first introduces relevant CAN background and explains how typical attacks are performed. It then evaluates how effectively the proposed technique identifies spoofed or unauthenticated messages and discusses the strengths and limitations. This research strategy, referred to as the Controller Area Network Origin Authentication (CANOA) technique, is examined here from the perspective of an external analyst.

1.3 Scope

This paper evaluates the CANOA technique developed by Thakur, Moreno, and Fischmeister and examines how effectively it can verify whether a CAN message was sent by its claimed ECU. The technique focuses solely on origin authentication and does not address encryption or message confidentiality. CANOA is a detection method, not a mitigation strategy, so determining how a vehicle should respond to an unauthenticated message is outside the scope of both the source work and this paper.

CANOA relies on power side-channel measurements rather than cryptographic or network-layer defenses, and the results reported by the researchers represent a proof of concept. Accordingly, this paper explains the technique and evaluates its feasibility, not a deployable security solution.

2 Background: CAN Bus Basics

This section introduces what CAN is, why it is used, how it works at a basic level, and the main security limitations of the CAN protocol.

2.1 What CAN Is

The Controller Area Network (CAN) is a communication system made up of multiple devices, called nodes, that are all connected to a shared set of wires known as a bus. Each node can send and receive messages through this common connection. CAN is most widely recognized for its use in automobiles, where it serves as the main communication network linking ECUs that manage various vehicle functions.

2.2 Why CAN Is Used

As electronic systems became increasingly common in automobiles, the number of individual wires needed to connect each component grew rapidly. This resulted in large, heavy, and complex wiring harnesses that were difficult and expensive to build and maintain. To address this problem, Bosch introduced CAN as a lightweight communication bus designed specifically for embedded automotive systems [5].

CAN significantly reduces wiring complexity by allowing all ECUs to share a common pair of wires rather than using dedicated connections between components. This shared network simplifies vehicle design, lowers manufacturing costs, and reduces overall vehicle weight. It is also highly robust. CAN uses differential signaling, described in Section 2.3, which provides strong resistance to electromagnetic interference [5], an essential property for automotive environments.

CAN's message arbitration mechanism enables real-time communication so safety-critical data, such as braking or engine control signals, can be transmitted reliably even when multiple ECUs attempt to communicate. Because the network is message-based rather than point-to-point, manufacturers can add or modify ECUs without redesigning the entire electrical system, making CAN flexible and scalable for modern vehicle architectures.

2.3 How CAN works

The Controller Area Network (CAN) uses a broadcast architecture, meaning every node on the network can see every message sent, including the ones it transmits itself. All nodes are connected to a shared "backbone," which consists of a twisted pair of wires known as CAN High (CAN H) and CAN Low (CAN L). These two wires carry the same information in opposite voltage directions – a method called differential signaling. This design is what makes CAN communication highly resistant to electrical noise.

Unlike simpler systems that send data as voltage pulses, where a higher voltage might represent a 1 and zero volts represents a 0, CAN determines bits based on the difference in voltage between CAN H and CAN L. When a node transmits a dominant bit (logic 0), CAN H rises to about 3.5 V while CAN L drops to about 1.5 V, creating a voltage difference of roughly 2 V. When a recessive bit (logic 1) is sent, both lines rest at about 2.5 V, so the difference between them is close to zero.

Because the wires are twisted together, they experience nearly the same amount of interference from external electromagnetic noise. Any interference that affects both wires equally cancels out when the voltage difference is measured, keeping the signal reliable even in the harsh electrical environment of a vehicle.

Data on the CAN bus is transmitted in units called frames or data packets. Each frame includes several parts: a start of frame bit, a control field, a 64-bit data section, error checking bits, an end of frame, and most importantly for this discussion, an 11-bit identifier (ID) [5]. The ID defines the message's type and also determines its priority on the bus.

When two nodes attempt to send data at the same time, CAN uses a bit-by-bit arbitration process to decide which one continues. This works because the 11-bit identifier (ID) is transmitted immediately after the start-of-frame bit, before any data or control fields. The ID field therefore determines message priority [5].

During arbitration, all nodes transmit and listen to the bus at the same time. The bus's idle state is recessive (logic 1). If a node sends a recessive bit but detects a dominant bit (logic 0) instead, it knows that another node is transmitting a lower numerical ID, which has higher priority. The losing node stops transmitting immediately and retries later, while the highest-priority message continues without interruption.

This "non-destructive" arbitration ensures that no data is corrupted during collisions, and it guarantees that high-priority messages, such as braking or engine control signals, always win access to the bus.

2.4 Security Limitations

The speed and reliability that make CAN so effective also come with important security trade-offs. Because CAN uses a broadcast design, every message is visible to every node on the network. This means that if even one ECU becomes compromised, it can potentially affect all others connected to the bus [3].

Another limitation is that CAN messages are not encrypted. All data is transmitted as plain, unprotected bits, making it possible for anyone with access to the bus to view the information being exchanged. This lack of encryption was not a concern when CAN was first developed, since vehicle networks were originally isolated and physical access was limited. However, as modern vehicles have become increasingly connected through wireless systems and external interfaces, the absence of encryption has become a clear weakness.

In addition, CAN provides no message authentication. Each node on the network is assigned one or more message identifiers (IDs), and all frames sent from that node use those IDs. However, the CAN protocol itself does not verify that a message with a given ID was actually sent by the correct node. In other words, while the ID is intended to represent the sender, there is no built-in mechanism to confirm its authenticity. As a result, other nodes on the network cannot be certain that a received message truly originated from the expected source. This lack of verification is a fundamental weakness in CAN security and forms the basis of the research explored later in this paper.

3 Attacks

While the CAN protocol provides fast, efficient, and reliable communication for automotive systems, its design also leaves several security gaps. The same features that make CAN lightweight and responsive, such as its broadcast architecture and lack of message authentication, also make it vulnerable to different forms of malicious interference.

This section explores how these weaknesses can be exploited through message injection and spoofing, and then examines the consequences these attacks can have on vehicle safety, reliability, and data privacy.

3.1 Message Spoofing & Injection

Message injection occurs when an attacker adds unauthenticated messages onto the CAN bus [3]. These messages can take several forms. An attacker might send entirely new frames that do not normally exist on the network, replay legitimate frames at different times, or interrupt normal communication by overwriting it with their own data. Because CAN is a broadcast system, every node can see all traffic on the bus. This means an attacker can easily observe legitimate messages, copy them, and resend them later [3]. In simple terms, message injection means placing any frame on the bus that should not be there.

A more targeted form of this attack is called message spoofing. In a spoofing attack, the attacker sends fake messages that pretend to come from a legitimate ECU by using that ECU's identifier (ID). Instead of sending random or meaningless traffic, the attacker carefully crafts messages that look valid by matching the expected structure and ID of real frames. As a result, other ECUs on the network accept these messages as genuine.

CAN is especially vulnerable to spoofing because it has no built-in authentication to verify the sender's identity, and its arbitration process gives priority to messages with lower ID values [4]. An attacker can therefore send spoofed frames with a low ID to win arbitration and dominate the bus, disrupting or delaying legitimate communication.

3.2 Consequences

When a CAN bus is attacked, the consequences can be serious and far-reaching. The most immediate concern is safety, because many vehicle systems rely on CAN messages to coordinate critical functions. Interference with this communication can have direct physical effects on the vehicle and its surroundings.

A widely cited example is the remote compromise of a Jeep Cherokee by Miller and Valasek [4]. After exploiting software vulnerabilities in the infotainment system, they gained access to the internal CAN network and issued commands to ECUs controlling braking, steering, and engine behavior, along with non-critical systems such as radio volume. Their work demonstrated how much control an attacker could obtain once the CAN bus was breached.

There are also reliability and financial implications. An engine control unit may enter a failsafe or "limp" mode when it observes irregular CAN traffic [3], which protects mechanical components but can disrupt driving and potentially leave a vehicle inoperable. Repeated or malicious interference could also cause damage requiring costly repairs.

Privacy is another concern as modern vehicles collect and store personal data through connected systems [3]. If an attacker compromises a connected ECU and reaches the CAN bus, they might access phone contacts, call logs, or navigation history.

Overall, CAN bus attacks threaten safety, reliability, and privacy, which highlights the need for practical and effective security mechanisms for in-vehicle networks.

4 Power Fingerprint Monitoring (CANOA)

Researchers Shailja Thakur, Carlos Moreno, and Sebastian Fischmeister from the University of Waterloo developed a novel strategy to detect spoofed messages on the CAN bus. CANOA introduces a new way to identify message senders without modifying the CAN protocol or adding cryptographic overhead.

4.1 Concept Overview

The researchers proposed a detection technique that authenticates ECUs on the CAN bus by monitoring their power consumption patterns. Each ECU draws a slightly different amount of electrical current due to small variations in its internal hardware [6]. These differences are consistent and measurable, allowing a unique power fingerprint to be created for each ECU.

Once these fingerprints are established, CANOA compares them to the power signals observed during normal CAN communication. When a message appears on the bus from a specific ECU ID, the system checks whether the current draw matches the fingerprint associated with that ECU. If the signature aligns as expected, the message is verified as legitimate; if it differs, the message is flagged as spoofed. In this way, CANOA uses power consumption as a physical identifier to confirm message origin.

The main advantage of this approach is that it relies on a physical side channel rather than encryption or digital signatures. This means it introduces no additional communication overhead or latency, which is important for time-sensitive automotive systems [6]. CANOA does not use the voltage differential on the CAN H and CAN L lines to create its fingerprints; the power signatures come only from monitoring the current drawn by each ECU's power supply. Although it does not depend on the CAN data signals themselves, CANOA still reads the CAN frames to identify the message's claimed ID. This allows the system to compare the ID in the frame

with the ECU whose power fingerprint most closely matches the observed transmission.

4.2 CANOA Architecture

To implement CANOA, electrical current sensors are first attached to the ECUs that will be monitored. These sensors record power usage data over time, allowing the system to establish a unique fingerprint for each ECU. Once this baseline is created, CANOA uses two algorithms to detect spoofed messages and verify legitimate ones.

The first algorithm operates offline and is responsible for building the reference fingerprint for each ECU. It collects power traces, removes noise, aligns timing, and averages multiple readings to produce a stable signature.

The second algorithm runs in real time while the vehicle is operating. Each time a message appears on the CAN bus, the algorithm compares the ECU's current draw to its stored fingerprint. If the signal correlation is high, the message is accepted as authentic. If not, it is flagged for further inspection as potentially spoofed.

This two-step process: first learning each ECU's electrical signature, then verifying messages live during operation, is the foundation of the CANOA technique. The following algorithms are simplified and adapted from Thakur et al. [6].

Algorithm 1 Reference Signal Generation

1: **Signal capture:** Collect many power traces for each ECU.
2: **Preprocessing:** Filter out noise and align the signals in time.
3: **Segmentation:** Split traces based on CAN frame boundaries.
4: **Averaging:** Compute average waveform for each ECU/message type.
5: **Storage:** Save averaged waveforms as reference profiles.

The reference signal generation algorithm begins by collecting power traces for each ECU while it transmits CAN messages (see Algorithm 1). These traces capture the small changes in electrical current that occur during transmission.

First, the algorithm removes electromagnetic noise from the collected data and aligns the power signals in time so that each sample lines up with the moment an ECU is sending a CAN frame. The traces are then divided according to CAN frame boundaries, meaning that each message transmission is matched with its corresponding section of the power signal.

To make the signals comparable across different ECUs, the algorithm normalizes the measurements, bringing all power readings onto a common scale. Then, each trace is passed through several processing steps:

- A Tukey window [7] is applied to smooth the edges of the signal and reduce sudden jumps or distortions.
- A Fast Fourier Transform (FFT) [2] converts the signal from the time domain to the frequency domain, helping to remove unwanted noise and highlight useful patterns.
- Finally, a Principal Component Analysis (PCA) [1] extracts the most important features of the signal by selecting the parts of the waveform that carry the most variation.

After these steps, the algorithm computes an average waveform that represents the ECU's typical power signature during message transmission. This averaged waveform forms the ECU's reference fingerprint. During real-time operation (see Algorithm 2), incoming power traces are compared against these stored fingerprints to verify whether a message truly came from its claimed ECU.

Algorithm 2 CANOA Verification

1: **Signal capture:** Record ECU power waveform on message transmission.
2: **Preprocessing:** Clean and align data.
3: **Comparison:** Compute correlation coefficient to reference profile.
4: **if** signal correlates highest with claimed ECU reference **then**
5: Mark as *legitimate.*
6: **else**
7: Mark as *spoofed.*
8: **end if**
9: **Output:** Return inferred ECU and confidence value.

Algorithm 2 performs the real-time classification of CAN messages to verify which ECU actually sent each one. Once the reference fingerprints have been created by Algorithm 1, this algorithm runs continuously during vehicle operation, checking every new CAN transmission against those stored power profiles.

When a CAN message appears on the bus, the system records the current power consumption of every monitored ECU. From these power measurements, it extracts a set of features in the same way that was done during the fingerprint creation process. Each ECU's data is then passed through its corresponding trained classification model, which calculates how likely it is that the ECU produced the observed transmission.

For every ECU–ID pair, CANOA generates a probability value showing how confident the model is that this ECU sent a message with that identifier. The system then compares all probabilities and identifies the ECU–ID pair with the highest probability that also exceeds a predefined threshold. That ECU is marked as the true source of the message.

Table 1: CANOA Classification Outcomes and Attack Interpretation

Condition	CANOA's Interpretation	Detected Attack Type
Fingerprint of claimed ECU matches	Message is legitimate	Normal transmission
Claimed ECU does not match, but another ECU does	Message sent by compromised ECU	Compromised ECU
No ECU matches (all probabilities below δ)	Message came from unrecognized device	Added or external ECU

If no ECU–ID pair passes the threshold, CANOA concludes that the transmission did not originate from any legitimate ECU on the network. In other words, none of the ECUs' fingerprints match the power behavior recorded during that message. This result indicates that the message came from an unknown or unrecognized device, such as an external module attached to the CAN bus.

Table 1 summarizes the possible outcomes from Algorithm 2 and how CANOA interprets each situation.

4.3 Lab and Field Testing

The researchers from the University of Waterloo conducted a real-world experiment to test the CANOA system. They built a hardware setup that tapped into a live CAN bus and monitored the power consumption of three different ECUs: the Engine Control Module (ECM), the Transmission Control Module (TCM), and the Anti-Lock Brake System (ABS). A simplified diagram of this prototype system is shown in Figure 1.

Each ECU was equipped with a shunt resistor to measure voltage drop across its power line. This measurement allowed the researchers to determine the ECU's power consumption in real time while it was transmitting CAN messages. The setup also included signal capture probes connected to the CAN High (CAN H) and CAN Low (CAN L) lines to monitor bus traffic simultaneously.

4.4 Results

In the laboratory prototype, four simulated ECUs were placed on a 125 kbps CAN bus and more than one thousand spoofed frames were injected [6]. CANOA successfully detected nearly all spoofed transmissions and produced stable, repeatable power fingerprints for each ECU. In the field test on a commercial truck, the researchers monitored five real ECUs and collected roughly one hundred thousand CAN messages during normal operation. In this setting, the technique achieved an authentication accuracy of approximately 99.9 percent with sub–0.05 millisecond per-message verification latency [6]. These results indicate that the method can distinguish ECU power signatures reliably in both controlled and real-world environments.

5 Discussion

5.1 Strengths

CANOA has several strengths that make it a promising method for authenticating messages on the CAN bus while keeping communication fast and efficient. One of its key advantages is that it operates entirely outside of the CAN protocol [6]. It does not require any changes to the existing message format or timing, so it can work with current vehicle systems and hardware without modifying the protocol.

Another major strength is that CANOA identifies each ECU using its unique power consumption pattern. These power "fingerprints" are based on the natural electrical behavior of the ECU's hardware during message transmission. Because this behavior comes from physical properties of the ECU itself, it is difficult for an attacker to imitate or reproduce through the CAN bus.

CANOA is also effective at detecting different types of threats. It can recognize when a legitimate ECU has been compromised, as well as when an external device is attempting to impersonate another ECU on the network. At the same time, it does not rely on cryptographic operations or message tagging to verify authenticity. Instead, it uses side-channel power measurements that require no extra data on the bus, which helps keep communication latency low and allows messages to be verified in real time without adding extra traffic.

5.2 Limitations

CANOA also has several important limitations. Most fundamentally, it is a detection method only. It can identify when a message was likely sent by a legitimate ECU, but it does not specify how a vehicle should react once an unauthorized transmission is detected. Any real deployment would need a separate mitigation strategy, which is outside the scope of this research.

Another limitation involves compromised ECUs. CANOA verifies the physical source of a message, not whether the sender is behaving maliciously. If an attacker gains control of an ECU and transmits frames using its legitimate identifier, the power trace will still match the stored fingerprint, and CANOA will classify the message as valid. This would allow

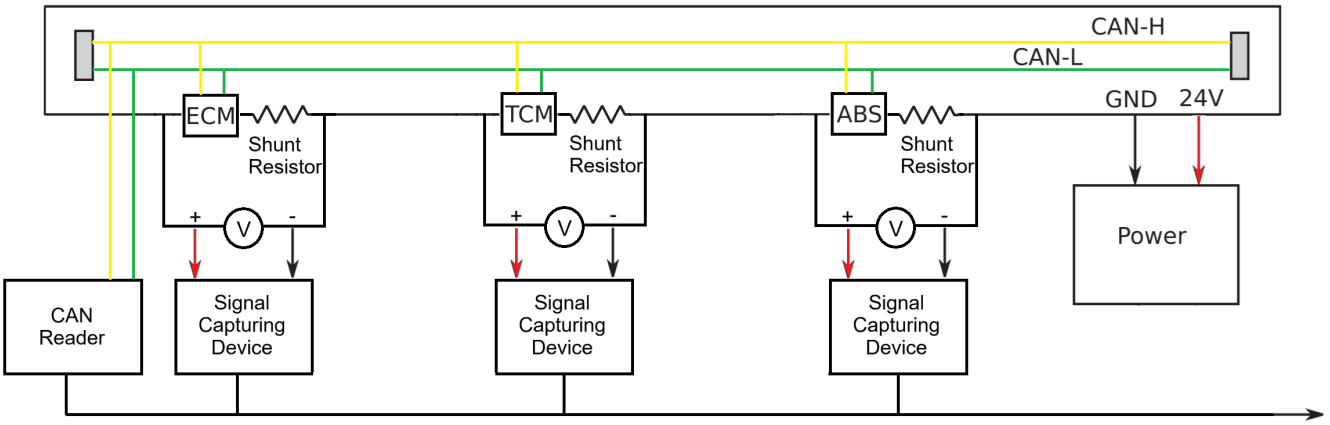

Figure 1: Hardware architecture for capturing CAN signal from the bus and power consumption measurements of the ECUs [6].

the attacker to misuse that ECU's functions or even flood the bus with high-rate traffic that appears legitimate.

Environmental and operational conditions may also affect performance. Because CANOA depends on small variations in ECU power consumption, electrical noise, temperature changes, or fluctuations in supply voltage can alter the shape of the measured traces. Since fingerprints are learned under normal conditions, large deviations may reduce matching accuracy.

Finally, CANOA adds complexity to maintenance. Replacing an ECU, even with an identical model, may introduce a different power signature, requiring the system to be retrained to capture the new fingerprint. This additional step could complicate routine repairs and limit practicality in real service environments.

5.3 Integration and Future Improvements

The researchers who developed CANOA outlined several directions for future improvements that could enhance both practicality and accuracy. One area of interest is simplifying the hardware design. Instead of measuring the power consumption of each ECU individually, a future version of CANOA could monitor the total power usage of the entire system to reduce wiring complexity and installation effort. The challenge is that aggregate power measurements contain more noise and provide fewer distinct features, so isolating which ECU is transmitting may become more difficult and could reduce authentication accuracy.

Another key consideration is system reliability under different environmental and operational conditions. Temperature fluctuations, electrical noise, and long-term ECU aging can all influence the shape of power traces. These factors may cause gradual fingerprint drift over time, which would lower authentication accuracy unless the system is periodically retrained.

The researchers also highlighted the potential benefits of using lower sampling rates for power measurements. If the sampling rate can be reduced without significantly affecting accuracy, CANOA could use simpler sensors and become more cost-effective, which is essential for any solution intended for large-scale deployment in production vehicles. Finally, they suggested strengthening the system by incorporating additional physical side channels, such as acoustic measurements, alongside power-based fingerprints.

6 Conclusion

The Controller Area Network remains the dominant communication protocol in the automotive industry because it enables fast, reliable, and lightweight real-time data exchange, which is essential in safety-critical systems. Despite these strengths, CAN lacks built-in message authentication, which leaves it open to several types of attacks.

CANOA offers a practical and promising direction for addressing this gap by verifying the physical origin of transmitted messages without altering the CAN architecture or adding meaningful computational overhead. By using power side-channel measurements, CANOA can potentially identify the transmitting ECU with high accuracy and minimal delay based on the results shown in controlled experiments [6].

Although CANOA is not intended to serve as a complete security solution on its own, it could fit well within a layered defense strategy. When paired with other cybersecurity measures, it may provide an additional physical layer of verification that strengthens overall system resilience and makes unauthenticated message injection more difficult to carry out.

References

[1] Hervé Abdi and Lynne J. Williams. 2010. Principal Component Analysis. *Wiley Interdisciplinary Reviews: Computational Statistics* 2, 4 (July 2010), 433–459. doi:10.1002/wics.101

[2] E. Oran Brigham. 1988. *The Fast Fourier Transform and Its Applications*. Prentice-Hall, Inc., Englewood Cliffs, NJ, USA.

[3] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak N. Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage. 2010. Experimental Security Analysis of a Modern Automobile. In *Proceedings of the 2010 IEEE Symposium on Security and Privacy (SP 2010)*. IEEE Computer Society, San Francisco, CA, USA, 447–462. doi:10.1109/SP.2010.34

[4] Charlie Miller and Chris Valasek. 2015. *Remote Exploitation of an Unaltered Passenger Vehicle*. Technical Report. IOActive, Seattle, WA, USA. https://ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf

[5] Robert Bosch GmbH. 1991. *CAN Specification Version 2.0*. Bosch, Stuttgart, Germany. https://www.bosch-semiconductors.com/media/ip_modules/pdf_1/can2spec.pdf Controller Area Network (CAN) Specification, Version 2.0.

[6] Shailja Thakur, Carlos Moreno, and Sebastian Fischmeister. 2024. CANOA: CAN Origin Authentication through Power Side-channel Monitoring. *ACM Trans. Cyber-Phys. Syst.* 8, 2, Article 13 (May 2024), 30 pages. doi:10.1145/3571288

[7] John W. Tukey. 1997. *The Practice of Data Analysis: Essays in Honor of John W. Tukey*. Princeton University Press, Princeton, NJ, USA. doi:10.1515/9781400851607 Course Book.