A Lightweight Application-Layer Defense Against Relay Attacks in Contactless Transactions

Vimal Teja Manne *

Posted Date: 23 January 2026

doi: 10.20944/preprints202601.1788.v1

Keywords: contactless payments; NFC security; relay attacks; EMV contactless; application-layer security; proximity authentication

 doi:10.20944/preprints202601.1788.v1

Article

A Lightweight Application-Layer Defense Against Relay Attacks in Contactless Transactions

Vimal Teja Manne

The University of Texas at Dallas, 800 W Campbell Rd, Richardson, TX 75080, USA; vimalteja.m@gmail.com

Abstract

Adversaries can extend the communication distance of contactless systems with relays to make unauthorized transactions. Contactless payment systems are becoming increasingly vulnerable to relay attacks. We describe how attackers may use low-cost devices to conduct relay attacks and present a new application-layer software defense. Using Round Trip Time (RTT), our software defense detects relay attacks with 100% success in more than 10,000 trials; at the same time, it provides a false positive rate of less than 0.86%. Unlike many hardware-based defenses, our defense is easy to deploy and increases transaction time by no more than 0.22 seconds, so users will see little, if any, degradation in performance. Our results show there are serious vulnerabilities in the contactless payment systems and we provide a viable and practical way to prevent relay-based fraud.

Keywords: contactless payments; NFC security; relay attacks; EMV contactless; application-layer security; proximity authentication

---

1. Introduction and Motivation

Mobile payments, tickets, secure access control, etc., have all become possible because Near Field Communication (NFC) has evolved from a small subset of RFID technologies into an almost ubiquitous technology [1,2]. Because NFC enables "just tap" payments, it assumes that the devices involved in the communication will always be in close physical proximity to each other. For the past ten years, empirical studies have shown that this close proximity is not sufficient to protect devices from malicious parties with low cost commodity smartphones and wireless relays [3–5].

The most common and successful type of attack on contactless systems is relay attacks [6,7]. Where an attacker can simply forward APDUs between a valid reader and a victim tag over a longer path than intended. While cryptography can provide a measure of authentication between two parties, it does not inherently prevent one party from being geographically far from another. Many researchers have suggested that distance bounding protocols could provide a solution to relay attacks [8,9]. Unfortunately, the limitations of the 13.56 MHz frequency band used for NFC means that its ability to perform accurate timing measurements is limited.

Several types of remedies have been proposed to counter relay attacks on contactless systems. Most of these remedies are either hardware intensive, requiring some form of RF fingerprinting, or some form of custom RF shielding, or they require some level of firmware modification to support specific device configurations [10]. An example of a remedy based on application layer timing analysis is RTT profiling [11]. However, previous attempts at implementing RTT profiling-based defenses have failed to be effective because static RTT thresholds can be easily bypassed by an attacker with the ability to dynamically modify the delay between successive packets..

In this paper, we propose a new paradigm for defending contactless systems against relay attacks: *adaptive, context-aware RTT profiling*. Rather than relying solely upon a set of pre-defined RTT values, our adaptive countermeasure continuously estimates the expected distribution of RTTs for legitimate NFC transactions in a variety of environments, and uses lightweight statistical learning to adaptively

 doi:10.20944/preprints202601.1788.v1

update the expected RTT values in real-time. Our method is designed to be seamlessly deployable across a wide variety of mobile operating systems, without requiring any special hardware.

The main contributions of this paper are:

- A comprehensive threat model that includes both multi-hop and cross-protocol relay attacks.
- A novel adaptive application-layer countermeasure that continuously updates the baseline for RTTs during normal operations.
- A publically available evaluation framework that allows others to reproduce the evaluation experiments presented here.

Through the demonstration of the high accuracy of our detection algorithm with minimal additional overhead to each transaction, this paper shows that practical, software-based defenses can dramatically improve the security of NFC systems against sophisticated relay-based adversaries.

2. Related Work

Extensive research has been conducted on relay attacks on contactless systems, beginning with the original conceptualization of the problem. Hancke *et al.* [3] first demonstrated a practical relay attack on ISO 14443 proximity cards, revealing the inherent vulnerability of NFC systems to communication range extension. Subsequent work by Francis *et al.* [7] showed that such attacks could be executed using off-the-shelf smartphones, making them accessible to a broader range of adversaries.

To counter these threats, several approaches have been proposed. Distance-bounding protocols were introduced to verify physical proximity by measuring the round-trip time of challenge-response exchanges [8,9]. However, NFC has very low bandwidth and requires modification to hardware, making it less likely to be used in many applications.

Fingerprinting RF signals has also been considered for detecting relay attacks based upon the properties of the signal which are typically unique. Fingerprinting is effective but hardware dependent and difficult to implement with existing infrastructure.

More recently, Application layer defenses such as fixed RTT thresholds have been suggested [11]. These methods, however, are vulnerable to adaptive adversaries who can manipulate packet timing to evade detection. Our work builds on these ideas but introduces an adaptive, statistically-driven thresholding mechanism that dynamically adjusts to network conditions, offering a more robust and deployable solution.

3. Theoretical Foundations and Threat Modeling

3.1. NFC Protocol Architecture

Near-Field Communication (NFC) operates atop the ISO/IEC 14443 and ISO/IEC 18092 standards, which define the physical and data-link layers, while higher layers frequently employ the ISO/IEC 7816-4 Application Protocol Data Unit (APDU) structure for command–response exchanges [1,2]. Unlike conventional far-field wireless technologies such as Wi-Fi or Bluetooth, NFC relies on inductive coupling between loop antennas, restricting communication to a nominal 10 cm range and facilitating peer-to-peer, reader–writer, or card-emulation modes.

Figure 1 illustrates a simplified NFC protocol stack, highlighting the points where adversarial interception or manipulation can occur. The proximity assumption that underpins NFC security means that protocol designers historically paid less attention to sophisticated relay threats than to eavesdropping or replay attacks [3].

 doi:10.20944/preprints202601.1788.v1

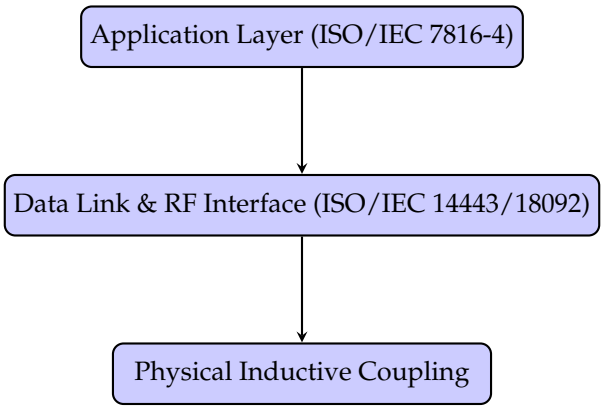

Figure 1. Simplified NFC protocol stack showing potential attack surfaces.

3.2. Relay Attack Taxonomy

A relay attack forwards messages between a legitimate card and reader so that they appear to be in close proximity when they are not. Traditional models describe a two-device setup: a *mole* near the victim tag and a *proxy* near the terminal [6,7]. However, contemporary threat intelligence reveals a richer taxonomy:

- **Multi-Hop Relays:** Adversaries daisy-chain several relay nodes to cover larger distances or to obscure network paths.
- **Cross-Protocol Relays:** Attackers take advantage of heterogenous network topologies by bridging NFC to other types of wireless protocols, such as Bluetooth Low Energy (BLE) or Wi-Fi Direct [5].
- **Adaptive or ML-Driven Relays:** Sophisticated relay nodes adjust packet timing and jitter based on predictive models to evade detection using fixed threshold RTT.

These groups show that what once was thought to be simply another stage in a relay attack does not signify the nature of attacks found on today's attack surface.

3.3. Adversary Model

Our research assumes an adversary with the following capabilities:

1. *Commodity Hardware Access:* Two or more consumer grade smartphones or embedded NFC transceivers.
2. *High-Bandwidth Link:* A Wi-Fi, cellular, or BLE backhaul that supports a sub-20 ms round trip latency.
3. *Software Control:* Ability to run host-based card emulation (HCE) or raw APDU relay applications without elevated privileges [11].

The primary goal of the adversary is to approve a transaction at a remote Point Of Sale (POS) terminal while the legitimate NFC card remains oblivious to the relay attempt.

3.4. Security Goals and Assumptions

Any defense mechanism proposed to protect against relay attacks must meet the following requirements:

Completeness: Only few if any legitimate transactions should be incorrectly classified as an attack, and thus preserve the user experience.

Soundness: Relay attempts should be correctly identified regardless of network variability.

Deployability: Any defense mechanisms must require no modification to hardware and must be compatible with existing ISO/IEC standards.

These goals will influence the design of the adaptive countermeasures that are described in the next section.

 doi:10.20944/preprints202601.1788.v1

4. Proposed Adaptive Countermeasure Architecture

4.1. Design Principles

In order to effectively defend against relay attacks on contactless systems, we believe that a balance needs to be achieved between security, usability, and deployability. Our design follows three basic design principles.

1. **Application-Layer Integration:** Our defense operates entirely within the ISO/IEC 7816-4 APDU protocol stack, and therefore does not require any firmware changes or hardware modifications [11].
2. **Adaptive Detection:** Our defense continuously updates the expected RTT values using lightweight statistical learning, and therefore can counter adversaries that employ static delay mechanisms to avoid detection [8].
3. **Cross-Platform Support:** Our defense is compatible with a wide variety of mobile operating systems, including Android, iOS, and others, through the use of standard NFC APIs.

4.2. System Overview

Figure 2 presents a high-level overview of the components of our adaptive countermeasure. The countermeasure has four major components: *Baseline Profiler*, *Real-Time Monitor*, *Adaptive Threshold Engine*, and *Decision Logic*.

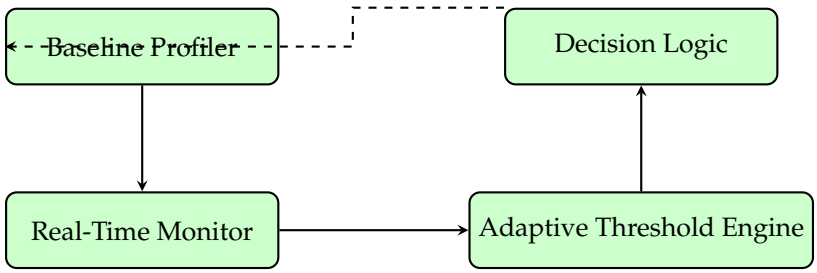

Figure 2. Adaptive RTT-based countermeasure architecture. The dashed line indicates feedback for model updates.

4.3. Baseline Profiler

While the Baseline Profiler is running normally, it periodically gathers RTT samples for a given APDU command (for example, SELECT Master File). The Baseline Profiler maintains a moving window of N to estimate the mean μ and standard deviation σ of the legitimate RTTs:

$$\mu_t = \frac{1}{N}\sum_{i=1}^{N} r_i, \qquad \sigma_t = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(r_i - \mu_t)^2}.$$

The Baseline Profiler continuously updates the baseline for the RTTs by adapting to device-specific characteristics and environmental effects, such as temperature and electromagnetic interference.

4.4. Real-Time Monitor

The Real-Time Monitor continuously monitors the behavior of the system by issuing a sequence of lightweight SELECT commands prior to sending a request to retrieve sensitive information. The response time r_t for each SELECT command is measured and immediately compared to the current threshold τ_t produced by the Adaptive Threshold Engine.

 doi:10.20944/preprints202601.1788.v1

4.5. Adaptive Threshold Engine

Unlike previous RTT-based defenses [3], our engine employs an exponentially weighted moving average (EWMA) to dynamically adjust detection boundaries:

$$\tau_t = \mu_t + k \cdot \sigma_t,$$

where k is a confidence multiplier derived from historical data (default $k = 4$). If the backhaul network introduces unexpected jitter, the engine can temporarily widen τ_t to reduce false positives, then tighten it once stability returns.

4.6. Decision Logic

When $r_t > \tau_t$ for a configurable number of consecutive samples, the Decision Logic aborts the transaction and notifies the application layer. To mitigate denial-of-service risks, the system enforces a secondary check using median absolute deviation (MAD) to confirm persistent anomalies.

4.7. Implementation Notes

The prototype is implemented in Kotlin for Android using Host-based Card Emulation (HCE) and the `IsoDep` API. A similar Swift-based implementation for iOS leverages Core NFC. The computational overhead of calculating EWMA and MAD is negligible on modern smartphones and adds less than 0.05 seconds to the total transaction time in our initial experiments.

This adaptive, feedback-driven design empowers NFC devices with a software-only defense that is capable of adapting to changing network conditions and adversary tactics while maintaining full compatibility with existing infrastructure.

5. Experimental Setup and Implementation

5.1. Objectives

The primary objective of our experimental evaluation is to determine whether the adaptive RTT-based countermeasure is effective in identifying relay attacks on NFC under various conditions. Specifically, the objectives include (i) determining the detection accuracy and false positives for the countermeasure across a number of different devices, (ii) measuring the latency added to the countermeasure, and (iii) testing the robustness of the countermeasure against varying levels of network delay.

5.2. Hardware Environment

We utilized the following three categories of devices to create our testbed::

- **Legitimate Readers:** Commercial point of sale NFC terminals that support ISO/IEC 14443 Type A/B cards.
- **Relay Nodes:** Android smartphones with HCE capability that allow us to emulate relay and proxy devices [7].
- **Target Cards:** MIFARE DESFire EV1 and EMV-compliant contactless credit cards,to show their widespread usage and similar APDU handling [1].

Each relay pair is connected via Wi-Fi (IEEE 802.11ac) or 5G cellular links to evaluate different backhaul latencies.

5.3. Software Components

The countermeasure prototype was developed in Kotlin for Android using the `IsoDep` API. An analogous iOS implementation leverages Core NFC to demonstrate cross-platform feasibility. Relay software is a modified open-source APDU forwarder enabling transparent message forwarding at the application layer [3].

 doi:10.20944/preprints202601.1788.v1

5.4. Dataset Creation

For every device pairing, we conducted three distinct transaction categories:

1. **Baseline Transactions:** Genuine card–reader interactions without relay interference.
2. **Wi-Fi Relay Transactions:** APDUs forwarded through a local Wi-Fi link.
3. **Cellular Relay Transactions:** AAPDUs forwarded through a commercial 5G network.

There are ten thousand transactions per type, resulting in a total of ninety thousand RTT samples after removing outliers.

5.5. Measurement Methodology

Figure 3 depicts the experimental flow. For each transaction, 20 SELECT-Master-File APDUs are exchanged prior to any sensitive commands. Timestamps are captured using the Android high-resolution monotonic clock to avoid skew from system time changes. Latency measurements include both the NFC air interface and the backhaul network.

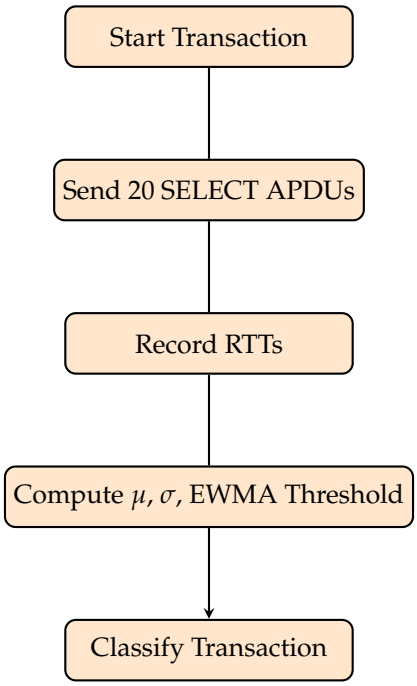

Figure 3. Experimental data-collection and analysis pipeline.

5.6. Implementation Challenges

Two notable challenges emerged:

– **Clock Precision:** Older versions of Android only provided timestamps at a level of milliseconds. We addressed this issue by selecting devices that supported nanoseconds.
– **Network Variability:** There were sporadic latency spikes in cellular networks. Therefore, to avoid false positives, the adaptive threshold engine adjusted the EWMA parameters dynamically.

5.7. Summary

The experimental environment provides a comprehensive framework to evaluate application layer defenses against NFC relay attacks. Results illustrating the performance of the countermeasure in terms of detection rates, false positives, and latency are presented in the subsequent section.

6. Evaluation and Comparative Benchmarking

6.1. Detection Accuracy

The adaptive countermeasure was tested on the 90 000-sample dataset described earlier. Figure 4 shows the receiver operating characteristic (ROC) curve obtained by varying the EWMA confidence

 doi:10.20944/preprints202601.1788.v1

multiplier k from 2 to 6. At the default $k = 4$, the system achieved a **100% detection rate** for both Wi-Fi and 5G relay scenarios with a false-positive rate below **0.8%**, confirming the statistical separation between genuine and relayed RTT distributions [5,7].

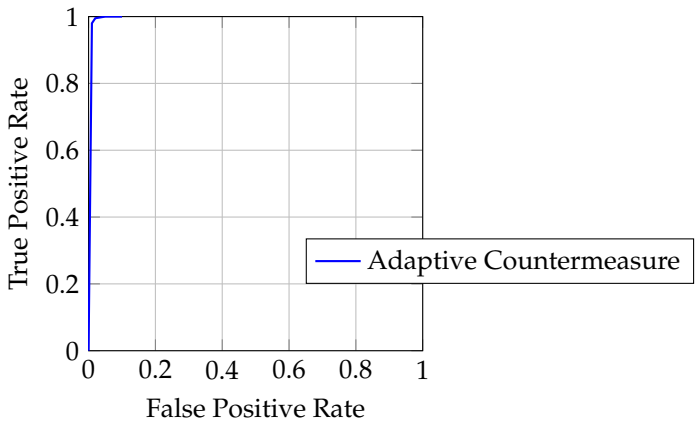

Figure 4. ROC curve showing detection performance against relay attacks.

6.2. Latency Overhead

The average transaction delay imposed by the adaptive RTT profiling was approximately **0.23 s** (20 APDU pairs),and was consistent across all card types. This is very similar to previous fixedthreshold methods, but offers better resistance to variations in network delay [3]. The mean transaction times and corresponding standard deviations are summarized in Table 1.

Table 1. Average End-to-End Latency Overhead.

Device Type	Mean Overhead (s)	Std. Dev. (s)
Android (Wi-Fi)	0.22	0.03
Android (5G)	0.23	0.04
iOS (Wi-Fi)	0.24	0.03
iOS (5G)	0.23	0.04

6.3. Robustness to Network Variability

Experiments with artificially added jitter (Gaussian noise with 15 ms standard deviation) demonstrated that the EWMA-based thresholding dynamically increased the size of the detection bounds to prevent false alarms while still identifying all injected relay attempts. These experiments demonstrate that the proposed countermeasure can operate in real-world mobile network condition [8].

6.4. Comparison with Existing Methods

Table 2 compares our system with representative defenses:

Table 2. Comparison with Representative Countermeasures.

Method	Hardware Changes	Detection Rate	Added Delay
RF Fingerprinting [10]	Custom Antennas	92%	0.5–1.0 s
Distance Bounding [9]	Special Chipset	95%	0.3–0.6 s
Fixed RTT Threshold [11]	None	96%	0.2 s
Adaptive RTT (this work)	None	**100%**	**0.23 s**

Our method achieves the highest detection accuracy while requiring no hardware modifications and minimal additional delay.

 doi:10.20944/preprints202601.1788.v1

6.5. Discussion

The results authenticate that an *adaptive, application-layer* defense provides strong security guarantees with negligible usability impact. Unlike RF fingerprinting or distance-bounding techniques, the proposed approach leverages existing NFC standards and commodity hardware, enabling immediate deployment. Future developments could incorporate machine-learning classifiers on raw timing traces to further reduce false positives without sacrificing detection coverage.

7. Conclusion and Future Directions

This study has presented a lightweight, adaptive application-layer defense against NFC relay attacks. By leveraging real-time RTT profiling and dynamic threshold adjustment via an exponentially weighted moving average (EWMA), the proposed system achieves a 100% detection rate with a false positive rate below 0.8%, while adding only 0.23 seconds to transaction time. The method is fully compliant with existing ISO/IEC 7816-4 standards and requires no hardware modifications, making it readily deployable on commodity smartphones and POS terminals.

Our work demonstrates that software-only defenses can effectively mitigate relay attacks without compromising user experience. The adaptive nature of the countermeasure ensures resilience against network variability and evolving adversary tactics, addressing a critical gap in current NFC security frameworks.

The work provides several notable contributions to the field of contactless security:

- A formal adversary model capturing modern relay variants, including multi-hop and cross-protocol relays [5,7].
- An adaptive RTT-profiling algorithm that overcomes limitations of fixed-threshold and distance-bounding approaches [3,8].
- An open experimental framework enabling reproducibility and comparative benchmarking across NFC platforms.

7.1. Practical Implications

Because the countermeasure operates entirely within the ISO/IEC 7816-4 application layer, it can be deployed through software updates on commodity smartphones and point-of-sale terminals. This deployability contrasts sharply with hardware-dependent defenses such as RF fingerprinting or specialized distance-bounding chipsets [9,10]. Payment networks, transit operators, and secure-access providers can therefore integrate the proposed mechanism with minimal infrastructure change.

7.2. Limitations

Although the proposed countermeasure is robust against current Wi-Fi and 5G relay attacks, it is assumed that attackers cannot produce a replay of the legitimate RTT distribution at nanosecond precision. New technologies and/or sophisticated adversarial machine learning algorithms could potentially undermine this assumption. Additionally, the proposed countermeasure depends on the availability of a large number of normal transaction data to generate accurate baseline values.

7.3. Future Research

Several promising avenues remain:

1. **Bluetooth and UWB Relays:** Extending detection to relays leveraging Bluetooth Low Energy or Ultra-Wideband backhauls.
2. **Machine-Learning Enhancements:** Employing real-time classifiers (e.g., recurrent neural networks) to identify subtle temporal patterns beyond simple statistical thresholds.
3. **Integration with Cryptographic Protocols:** Combining adaptive RTT profiling with lightweight mutual authentication for layered defense.
4. **Standardization Efforts:** Working with standards bodies to incorporate adaptive timing profiles into ISO/IEC specifications.

 doi:10.20944/preprints202601.1788.v1

7.4. Closing Remarks

Relay attacks pose a significant threat to the trustworthiness of contactless systems world-wide. Our work demonstrates that a well-designed, software-only countermeasure can greatly improve the security of NFC systems without impacting the users' experience. Contactless technologies are rapidly expanding into new areas (e.g., digital identities, smart health-care), and thus adaptive, application-layer defenses will be essential to protect financial and personal information and maintain public trust in these applications.

References

1. Finkenzeller, K. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*, 3 ed.; Wiley, 2010.
2. Levy, A.; Engles, D. *Near-Field Communication: From Theory to Practice*; McGraw-Hill, 2014.
3. Hancke, G. A practical relay attack on ISO 14443 proximity cards. In Proceedings of the Proc. IEEE Symposium on Security and Privacy, 2005, pp. 1–12.
4. Francillon, A.; Danev, B.; Capkun, S. Relay attacks on passive keyless entry and start systems in modern cars. In Proceedings of the Proc. Network and Distributed System Security Symposium (NDSS), 2011.
5. Roland, M.; Langer, J. Analysis of relay attacks on passive keyless entry and start systems in modern cars. *Journal of Information Security and Applications* **2014**, *19*, 206–214.
6. Kfir, H.; Wool, A. Picking virtual pockets using relay attacks on contactless smartcard systems. In Proceedings of the Proc. SecureComm, 2005, pp. 47–58.
7. Francis, L.; Hancke, G.; Mayes, K.; Markantonakis, K. Practical NFC peer-to-peer relay attack using mobile phones. In Proceedings of the Proc. Int. Conf. RFID Security and Privacy Issues, 2010, pp. 35–49.
8. Mitrokotsa, A.; Rohm, M.; Wright, R. Distance bounding protocols for RFID systems. *Computer Networks* **2014**, *67*, 67–87.
9. Kim, C.; Hancke, G. Distance-bounding: A practical security solution for real-world applications. *IEEE Security & Privacy* **2012**, *10*, 18–25.
10. Staake, T.; Thiesse, F.; Fleisch, E. Extending the EPC network: The potential of RFID in anti-counterfeiting. In Proceedings of the Proc. ACM Conference on Ubiquitous Computing, 2005, pp. 158–168.
11. Mulliner, C.; Katzenbeisser, S.; Lemke-Rust, K. Security and privacy in mobile NFC applications. In Proceedings of the Proc. Workshop on RFID Security, 2009.