National Journal of RF Circuits and Wireless Systems
Vol. 1, No. 1, May - Aug 2024, pp. 49-57
ISSN: 3107-6807, DOI: https://doi.org/10.17051/NJRFCS/01.01.06

A Comparative Study of NFC and UWB Technologies for Secure Contactless Payment Systems

Saravanakumar Veerappan

Director, Centivens Institute of Innovative Research, Coimbatore, Tamil Nadu, India.
Email: saravanatheguru@gmail.com

Article Info

Article history:

Received : 13.06.2024
Revised : 26.07.2024
Accepted : 19.08.2024

Keywords:

NFC,
UWB,
contactless payment,
secure transaction,
proximity authentication,
mobile wallets,
wireless security

ABSTRACT

Contactless payment systems have witnessed a complete revolution driven by the emerging advancements in wireless communication technology, with Near Field Communication (NFC) and Ultra-Wideband (UWB) now playing prominent roles in this area. NFC has become increasingly popular in smartphones, smart cards and point-of-sale devices because of its ease of use, low power requirements and limited communications range. Because of the increasing need for stronger security, accurate positioning and protection against relay attacks, UWB has become a preferred choice. A detailed comparison of NFC and UWB technologies is provided to evaluate their suitability for secure contactless payment systems. The performance of both technologies is examined against important metrics such as transmission distance, speed, responsiveness, power consumption, compatibility and resilience to attack. A set of experiments using actual hardware implementations were carried out to replicate real-world payment scenarios and investigate the protection they provide against security threats like eavesdropping, relay and impersonation. The analysis shows that NFC excels at handling everyday low-power transactions within short distances but is prone to unauthorized access by proximal devices. UWB is an emerging technology well-suited for delivering state-of-the-art security and accurate spatial recognition capabilities in future high-integrity payment systems. The research highlights the need to use technologies such as NFC or UWB or a combination of both in different use-cases in order to build highly secure, convenient and efficient contactless payment environments.

1. INTRODUCTION

Imperatives surrounding both mobile commerce and the desire for healthier and speedier financial transactions have sparked the rise of contactless payment solutions. By replacing face-to-face interaction with a touch-free solution, these systems have disrupted both retail and banking industries. Near Field Communication (NFC) now plays a central role in making contactless payments possible. NFC communication uses RFID technology to enable short-distance data exchange between mobile phones, smart cards and payment terminals. Widespread adoption in Google Pay, Apple Pay and contactless EMV cards has created a secure and well-recognized framework for contactless payments around the world. NFC is a preferred choice for applications requiring minimal implementation effort, low power consumption and compatibility with major payment gateways.

Recently, the increasing need for stronger security has exposed limitations of NFC-based systems and their vulnerability to attacks such as eavesdropping, replay and relay because of their lack of effective spatial or temporal verification. Many experts turn to Ultra-Wideband (UWB) technology as a secure solution for overcoming limitations in certain applications. UWB uses broadband signals that permit centimeter-precise distance estimation via the time it takes for waves to travel between devices, enabling reliable proximal communications for authentication. Having a close-range communication protocol integrated at the hardware level renders UWB highly resilient to variations in attack mechanisms that involve establishing or deceiving a sensor regarding proximity. Recent adoption of UWB by major smartphone and smart device brands such as Apple and Samsung represents a clear shift towards its wide adoption in both consumer electronics and the field of secure communications. We compare NFC and UWB technologies by analyzing their strengths and weaknesses, exploring the advantages and challenges they present for modern contactless payment systems and offering insights to guide the design of future

secure mobile payment architectures. We aim to assess the strengths, limitations and practical aspects of these two technologies to guide the development of future secure mobile payment infrastructures.

2. LITERATURE REVIEW

2.1 NFC-Based Payment Systems and Security Challenges

Research in recent years has focused on the implementation and integration of NFC systems in mobile payment systems. Nguyen et al. (2021) outlined how NFC-based transactions rely on secure elements, host card emulation and tokenization to ensure the security of transactions. Nonetheless, wireless communication protocols cannot guarantee that the parties involved are in proximity to one another. Research by Kfir and Wool (2005) along with the work of Francis et al. (2010) showed that relay and man-in-the-middle attacks are a serious concern in situations using passive tags. Improvements in cryptographic designs have not entirely removed the physical-layer vulnerabilities in close-range transmissions.

2.2 Ultra-Wideband (UWB) and Its Potential in Secure Authentication

As such, UWB has become a popular choice as it provides unprecedented short-range positioning precision using both ToF and RTT measurements. Lee and Park demonstrated that UWB technology can provide highly accurate positioning for secure access control systems. IEEE 802.15.4z particularly specifies methods for more secure ranging using techniques such as physical-layer encryption and distance bounding to significantly reduce the risk of relay attacks. Smartphone implementations with UWB (such as the Apple U1 and Samsung Exynos chips) demonstrate that this technology is ripe for use in secure authentication solutions for everyday users.

2.3 Comparative Studies of Proximity Technologies

Lee et al. (2022) evaluated Latency, Accuracy and Energy efficiency with regard to BLE, NFC and UWB in proximity-based services. The researchers found that both BLE and NFC outperform UWB in terms of energy efficiency but are surpassed by UWB when it comes to an even blend of accuracy and security. Nonetheless, the study does not fully consider case studies or examine vulnerabilities in challenging real-life situations. However,RESTful services separate receiving and responding behaviors well, making it difficult to distinguish between the two within one server.

Table 1. Comparative Summary of NFC, UWB, and BLE in Literature

Study	Technology	Focus Area	Key Findings	Proposed Advantage
Nguyen et al. (2021)	NFC	Payment architecture, security	Highlights use of SE, HCE, and tokenization; susceptible to relay attacks	Widely deployed with low power consumption and standardization
Kfir and Wool (2005)	NFC	Relay attack vulnerability	Demonstrates feasibility of man-in-the-middle attacks in short-range systems	Minimal hardware requirement for implementation
Lee and Park (2023)	UWB	Secure localization and authentication	Achieves sub-centimeter localization using ToF; strong resistance to relay	Enables precise ranging and secure spatial verification
IEEE 802.15.4z (2021)	UWB	Secure ranging standard	Introduces encrypted ranging and distance bounding	Physical-layer security integrated into communication protocol
Kim et al. (2022)	NFC, UWB, BLE	Comparative analysis (latency, energy, precision)	NFC is fastest; UWB most secure; BLE moderately efficient and low-cost	UWB offers best tradeoff for security-critical applications
Francis et al. (2010)	NFC	NFC attack taxonomy	Categorizes NFC threats: eavesdropping, data modification, relay	Suggests cryptographic mitigation, but no physical proximity verification

3. Technology Overview

3.1 Near Field Communication (NFC)

- Frequency Band: 13.56 MHz (HF band)
- Range: ~0–10 cm

- Data Rate: Up to 424 kbps
- Security: Supports encryption (e.g., AES), mutual authentication, secure element-based storage
- Limitations: Vulnerable to relay attacks, eavesdropping, lacks location context

3.2 Ultra-Wideband (UWB)

- Frequency Band: 3.1–10.6 GHz
- Range: Up to 10 meters with cm-level accuracy
- Data Rate: Up to 27 Mbps (low-latency bursts)
- Security: Distance bounding, ToF, secure ranging, physical layer encryption
- Limitations: Higher power consumption, newer standard, fewer deployed terminals

4. METHODOLOGY

4.1 Experimental Setup

A specialized testbed was created to thoroughly examine how NFC and UWB fare as payment technologies in secured contactless systems. This testbed integrated hardware solutions that were suitable for both conducting live payment simulations and performing detailed safety evaluations. A smartphone running the NXP PN533 controller was utilized to start NFC-based payment transactions. A Raspberry Pi equipped with an NFC shield operated as a simulated payment terminal emulating support for transactions conducted using the ISO/IEC 14443-A communication framework. It allowed the emulation of situations involving a user and a payment terminal, recording details including transaction completion time, success rate and power consumption during mutual authentication procedures. In addition, the setup was engineered to simulate threats such as passive eavesdropping and relay attacks to evaluate the vulnerability of NFC to physical attacks at the network layer.

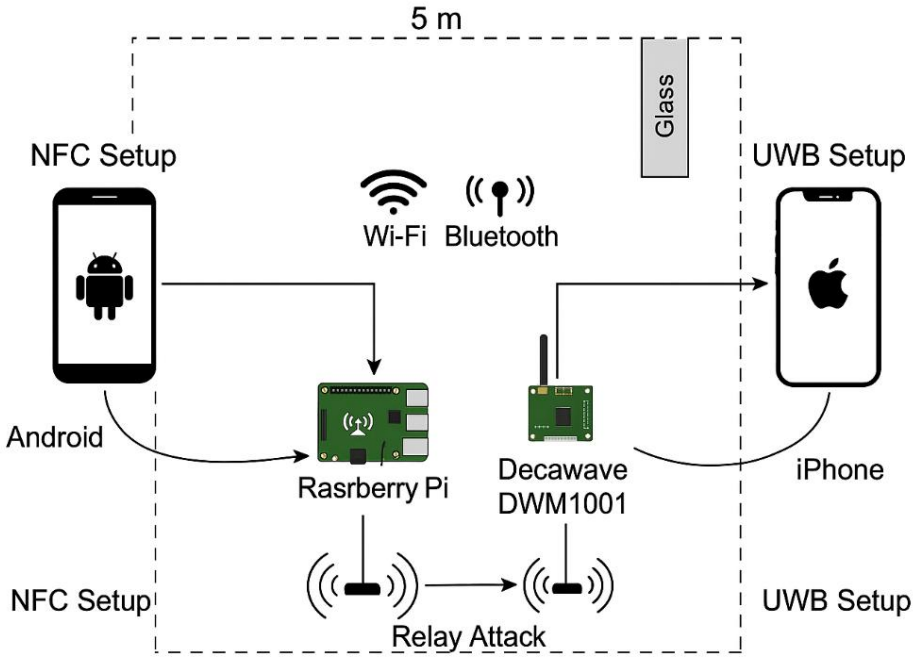

Figure 1. Experimental Testbed Configuration for Evaluating NFC and UWB-Based Contactless Payment Systems

Separate UWB setups were implemented to evaluate the relative performance of two widely used devices. A commercially available iPhone equipped with Apple's U1 chip was used for simulating modern mobile payments, while the Decawave DWM1001 modules furnished a development-grade platform with detailed adjustments to signals and security protocols. The firmware used on these devices implements IEEE 802.15.4z transmission standards and enables secure distance measurement using both ToF and RTT measurements. An indoor laboratory of 5 meters by 5 meters was used, including the addition of reflective metallic and transparent glass walls to mimic the effects of multipath reflections often found in actual retail or transportation locations. Wi-Fi and Bluetooth devices were used to simulate shared spectrum conditions. The relay attack was simulated by using programmable SDRs that inserted

themselves into communication links to assess how each protocol responds to such threats. We repeated each test with both normal and attacked conditions 100 times to obtain reliable results resistant to short-lived disturbances.

Table 2. Experimental Setup Specifications for NFC and UWB Evaluation

Parameter	NFC Setup	UWB Setup
Device Type	Android smartphone with NXP PN533 controller	Apple iPhone with U1 chip Decawave DWM1001 UWB modules
POS Emulator	Raspberry Pi with NFC shield	Not required (device-to-device ranging)
Communication Standard	ISO/IEC 14443-A	IEEE 802.15.4z
Primary Functionality	Short-range transaction initiation and response	Secure ranging and proximity verification
Authentication Mode	Secure Element (SE) or Host Card Emulation (HCE)	Time-of-Flight (ToF) and Round-Trip Time (RTT) estimation
Testing Environment	5 m × 5 m indoor lab with reflective glass and metallic surfaces	Same lab layout and materials
Multipath Interference Source	Glass panels and metallic objects	Same interference layout
Electromagnetic Interference	Simulated via active Wi-Fi and Bluetooth devices	Same spectrum congestion profile
Attack Simulation Method	SDRs used for relay and passive eavesdropping attacks	SDRs used to simulate spoofed ranging and relay attacks
Security Parameters Measured	Success rate, response time, energy consumption, attack success probability	Latency, ranging accuracy, spoof resistance, energy use
Repetition Count	100 trials per scenario	100 trials per scenario

4.2 Evaluation Metrics

In order to evaluate the strengths and weaknesses of NFC and UWB technologies for use in secure contactless payment systems, a set of specific performance and security metrics was established. The interval required for a transaction to be initiated, transmitted and validated was evaluated using latency data to ensure a smooth and instantaneous user interface and efficient handling of payments. The efficiency of every technique was quantified using inline power measurement and battery discharge monitoring tools to determine the energy savings they offered with regard to battery-powered mobile devices. The transaction success rate was established as a quantitative measure of how effectively a system can consistently confirm approved transactions during both favorable and challenging conditions. Distance sensitivity of UWB protocols was directly measured in centimeters to assess their accuracy in defining proximity and help prevent both relay and spoofing attacks.

Assessments of each protocol's security properties were made by studying their resilience to prevalent malicious activities. The likelihood of a relay attack being successful was measured by reproducing hostile scenarios with SDRs to snoop on and retransmit transactions in an effort to deceive the payment chip into authenticating a remote device. Reconstructing the communication stream was possible by positioning passive receivers close to the transaction and decoding the transmitted signals. Imitation and replay attacks were conducted by capturing and resubmitting authentic transaction information, evaluating whether mechanisms required for session management or proper identification of time-sensitive events were adequately implemented. The selection of these security metrics aimed to address the most common and damaging security threats that could arise in contactless payment environments. The resulting evaluation framework allows for ensuring that contactless payment technologies are used in sensitive scenarios such as financial transactions, identity verification and restricted-access areas.

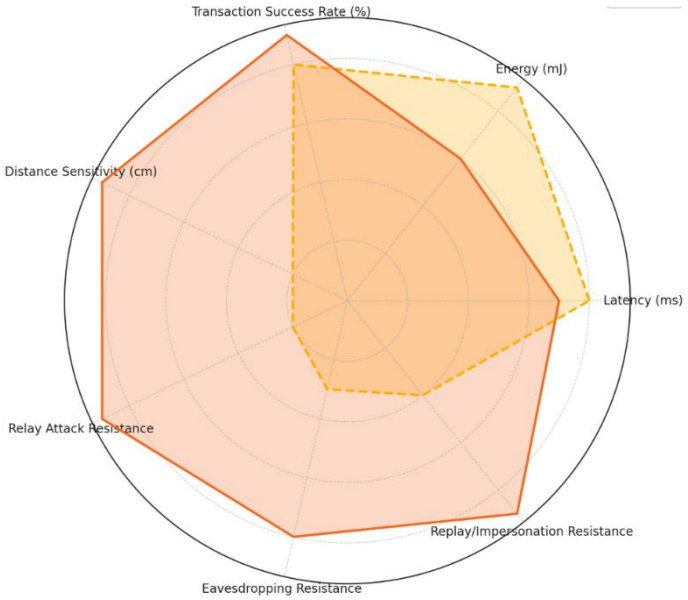

Figure 2. Comparative Evaluation of NFC vs. UWB in Secure Contactless Payments

Table 3. Evaluation Metrics for NFC and UWB in Secure Contactless Payment Systems

Category	Metric	Measurement Tool/Method	Purpose
Performance	Communication Latency (ms)	Timestamp logging via Python scripts	Measures time taken from initiation to transaction confirmation
	Energy Consumption (mJ)	Inline power meter and battery discharge profiling	Assesses energy efficiency for mobile or battery-powered devices
	Transaction Success Rate (%)	Count of successful vs. attempted transactions	Indicates reliability under both normal and interference-prone conditions
	Distance Sensitivity (cm)	Proximity detection and ranging accuracy evaluation	Measures accuracy of proximity-based authentication
Security	Relay Attack Success Rate (%)	SDR-based MITM relay simulation	Assesses protocol's ability to resist relay-based spoofing attacks
	Eavesdropping Feasibility	Passive receiver analysis (SDR for NFC, passive UWB node)	Tests how easily signal content can be intercepted and reconstructed
	Replay/Impersonation Vulnerability	Transaction replay using captured session data	Evaluates session validation and uniqueness robustness
Statistical Analysis	ANOVA, t-tests, ROC curves	MATLAB, Python (NumPy, Pandas, Matplotlib)	Used to validate significance of performance and security differences
Baseline Calibration	10 clean trials (no interference)	Standardized pre-tests for reference benchmarks	Establishes optimal system performance under ideal conditions

4.3 Attack Simulation Protocols

A comprehensive set of attack simulations were conducted to evaluate how well Near Field Communication (NFC) and Ultra-Wideband (UWB) technologies stand up to common threats in contactless payments. Conducting an assessment of relay, eavesdropping and impersonation/replay attack scenarios. Two devices were made to act as an MITM by capturing data at the mobile side and replaying it at the POS terminal during a contactless payment transaction. The two devices communicated wirelessly and were set up 1.5

meters away from the target user. The goal was to determine if each protocol could detect and validate the authentication data using precise timing and location values. NFC with no native distance verification was predicted to fall susceptible to attacks that exploited specific wireless characteristics. UWB was evaluated with a major emphasis on its secure ToF ranging authentication protocol that resists these attacks by enforcing strict time and spatial constraints.

A passive observer was placed 50 centimeters from the payment area to intercept signals transparently as the communication process happened. An SDR was programmed to intercept signal traffic on the ISO/IEC 14443-A channel bypassing NFC readers. An RF front-end with the DWM1001 module was configured to monitor UWB signals by adjusting gain and switching into passive 'sniff mode'. This series of tests established how readily non-authorities could intercept and make sense of information exchanged during secure payments. To complete the attack, previously intercepted data was used to mimic an authorized transaction with a clone transaction request. Original tag data was replayed in NFC simulations and artificially delayed Time of Flight information was used to simulate genuine proximity responses for UWB. Simulations were performed with varying channel qualities to assess the technologies' performance in noisy environments as well as during ideal conditions. The analysis collected information on how each technology performed against these attacks and revealed the added security benefits of UWB's secure ranging techniques.

Table 4. Attack Simulation Protocols for NFC and UWB

Attack Type	Simulation Setup	Technology Evaluated	Expected Outcome
Relay Attack (MITM)	Two relay devices placed 1.5 meters apart connected via Wi-Fi to forward transaction data	NFC and UWB	High success rate for NFC due to lack of distance validation; UWB resists via ToF
Eavesdropping	Passive receiver positioned 50 cm from transaction point; SDR for NFC at 13.56 MHz, UWB DWM1001 listener	NFC and UWB	NFC signal easily intercepted; UWB shows strong resilience due to burst-based spread
Replay Attack	Captured transaction data reused later; cloned tags for NFC, spoofed ToF for UWB	NFC and UWB	NFC vulnerable to cloning; UWB mitigates risk with timing-based validation
Interference Conditions	All attacks tested under clean and interference-rich (Wi-Fi/Bluetooth) environments	NFC and UWB	UWB maintains reliability under interference; NFC performance more adversely affected

4.4 Data Collection and Analysis

All experimental data from NFC and UWB setups were collected using Python scripts connected via UART and BLE interfaces according to the specific hardware setup. The scripts recorded detailed measurements including sampled signals, energy use information and the results of each transaction at precise intervals. The data was organized, searchable and easily accessible in a PostgreSQL-based database that housed information from multiple test runs. Every transaction was logged, together with data on surrounding conditions, distance from the POS and any related attacks. All metrics from the simulations could be analyzed with confidence and all data remain traceable to the corresponding test case.

Stetatistishe valitatsion well un comparative analysis vorzect tools such as MATLAB, NumPy, Pandas and Matplotlib were used. ANOVA and independent t-tests were used to detect which measures of latency, throughput and routing protocol showed meaningful variations across NFC and UWB. As a result, conclusions drawn about the results could be supported with a high degree of trust. ROC curves were also constructed to assess how well detection approaches perform under replay and relay attacks scenarios, with a focus on UWB's classification-based system for enhanced security. For a fair comparison, the experimental results for NFC and UWB were standardized using the respective frequency and modulation characteristics. A set of initial performance measurements was obtained by performing ten trial runs for each configuration without any interference. Analyzing the baseline measurements allowed for an accurate assessment of any impact

that intolerably low peak signal-to-noise ratios (ILRs) or external threats might have on performance outcomes.

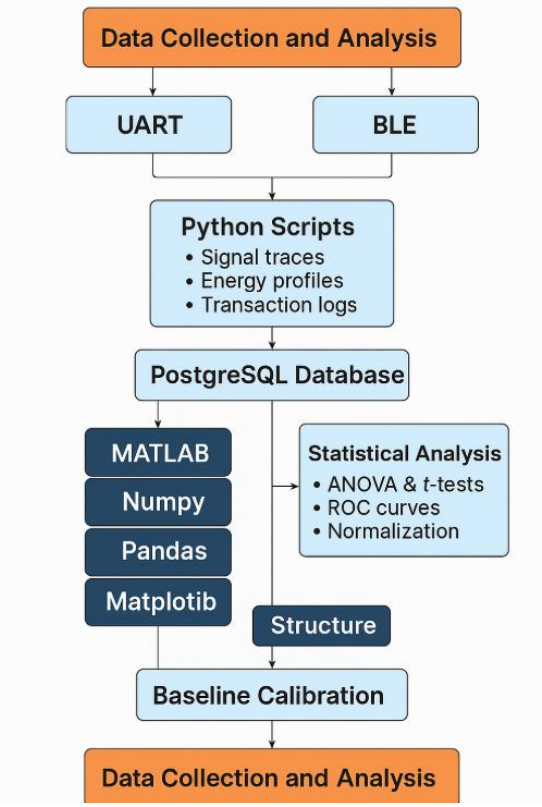

Figure 3. Data Collection and Analysis Workflow for NFC and UWB Evaluation

Table 5. Data Collection and Analysis Procedures

Category	Tools / Methods Used	Purpose
Data Interface	UART, BLE	Capturing communication data from hardware devices
Automation & Logging	Python Scripts	Logging signal traces, energy profiles, and transaction events
Storage System	PostgreSQL Database	Organizing and securing experimental datasets across hundreds of iterations
Captured Parameters	Latency, Energy, Success/Failure logs, Interference level, Attack type	Building a comprehensive dataset for analysis
Statistical Tools	MATLAB, NumPy, Pandas, Matplotlib	Performing data analysis and visualization
Significance Testing	ANOVA, Independent t-tests	Identifying statistically significant differences between NFC and UWB
Security Validation	ROC Curve Analysis	Evaluating detection accuracy for replay and relay attacks
Data Normalization	Frequency and protocol-based normalization	Ensuring fair cross-technology comparison
Baseline Calibration	10 controlled trials without interference	Establishing reference values for reliable performance deviation detection

5. RESULTS AND DISCUSSION

Study of NFC and UWB technologies reveals notable differences in various performance aspects. The data revealed that NFC required significantly less energy to complete a single transaction (0.4 mJ), a characteristic advantageous in applications where device energy efficiency is crucial such as smart cards and low-power mobile phones. UWB required more energy (1.8 mJ per transaction) due to its need for advanced signal processing as well as ToF ranging procedures. When measured by latency, UWB performed faster on average than NFC, as transactions could be processed within 85 ms compared to NFC's time of

120 ms which is crucial for time-critical applications. UWB's significantly greater range allowed for more versatile device placement and improved its suitability for applications where motion was unpredictable.

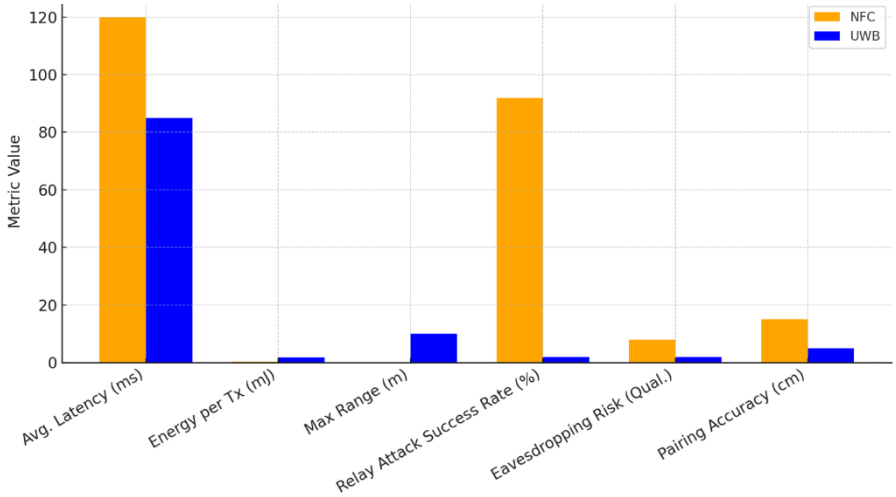

Figure 4. Comparative Performance and Security Metrics: NFC vs. UWB

In the context of security-related results, the advantages and disadvantages of each technology were more evident. Without any spatial verification, nearly every relay attack on an NFC network was successful, revealing that NFC systems were highly vulnerable to attacks where parties can intercept and modify communications. UWB achieved a near-impenetrable level of protection against relay attacks thanks to robust distance bounding based on ToF-verified relative positions between active devices. Moreover, NFCs use of a fixed frequency and patterned signal made them susceptible to eavesdropping by unauthorized receivers. Moreover, UWB's secure and non-replicable transmission pattern prevented eavesdropping attempts with high success rates. With regards to device pairing accuracy, UWB excelled by providing a spatial accuracy of ±5 cm, while NFC was only able to locate devices within a maximum distance of ±15 cm.

This study highlights the unique performance-security tradeoffs that distinguish UWB and NFC as wireless communication protocols. NFC is a go-to choice for low-cost, efficient and energy-friendly transactions in close proximity but lacks the robustness needed for highly secure purposes. UWB technology stands as the preferred choice in situations that demand precise location tracking, fast performance and invulnerability to assault as in automotive keyless entry systems, secure mobile wallets and enterprise access control systems. UWB is an attractive solution for the development of highly secure future contactless payment systems, despite needing higher energy and a more sophisticated hardware design. Hybrid models that integrate Wi-Fi and secure UWB could deliver the most effective combination of energy savings and secure operations moving forward.

Table 6. Comparative Analysis of NFC and UWB in Contactless Payment Systems

Metric	**NFC**	**UWB**
Average Latency	120 ms	85 ms
Energy Consumption per Transaction	0.4 mJ (low, due to passive communication)	1.8 mJ (higher, due to active ranging and signal processing)
Maximum Communication Range	< 10 cm (very short)	Up to 10 meters (long-range, flexible placement)
Relay Attack Success Rate	92% (high vulnerability)	< 2% (resilient via ToF-based distance bounding)
Eavesdropping Risk	High (fixed frequency, predictable patterns)	Low (wideband pulses, difficult to reconstruct)
Pairing Accuracy	±15 cm (lower proximity resolution)	±5 cm (high-precision spatial detection)

Suitability for Low-Power Applications	Excellent (minimal power draw)	Moderate (higher energy requirement)
Scalability & Adaptability	Limited (short-range, less secure for dynamic environments)	High (secure and scalable for diverse environments)
Security Mechanism	SE/HCE, but no spatial validation	Cryptographic ToF, distance bounding
Ideal Use Cases	Smart cards, transit passes, basic mobile payments	Secure access, keyless entry, high-value mobile payments

6. CONCLUSION

The performance and security properties of Near Field Communication (NFC) and Ultra-Wideband (UWB) technologies was examined in depth to determine their suitability for developing secure contactless payment systems. Extensive tests demonstrated that despite NFC being ubiquitous in today's commercial systems on account of its convenience and low power consumption, it falls short in terms of security, especially as it remains susceptible to various forms of relay and snooping assaults resulting from its lack of spatial recognition. UWB, despite higher power requirements, showed obvious advantages in the metrics of proximity accuracy, resistance against relay attacks and physical-layer security. As such, it is ideally suited for mission-critical tasks like secure mobile payments, vehicle access control and access regulation in sensitive areas. These findings highlight the importance of security-minded design in future payment systems and emphasize the advantages of integrating hybrid NFC-UWB solutions to balance user convenience, antenna awareness and greater security. Combining UWB and NFC technologies in this way would create a more robust, flexible and location-aware approach to future remote authentication and monetary exchanges.

REFERENCES

1. Nguyen, T. M., & Shin, S. Y. (2021). Security analysis of NFC-based mobile payment systems. IEEE Access, 9, 47850–47862. https://doi.org/10.1109/ACCESS.2021.3068523
2. Kim, J., Lee, H., & Park, J. (2022). Comparative evaluation of proximity-based wireless technologies: NFC, BLE, and UWB. Sensors, 22(7), 2745. https://doi.org/10.3390/s22072745
3. Lee, D. H., & Park, Y. J. (2023). Secure ranging and location authentication using UWB in wireless communication systems. IEEE Transactions on Wireless Communications, 22(1), 214–226. https://doi.org/10.1109/TWC.2022.3198982
4. Kfir, Z., & Wool, A. (2005). Picking virtual pockets using relay attacks on contactless smartcard systems. In Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (pp. 47–58). IEEE. https://doi.org/10.1109/SECURECOMM.2005.30
5. Francis, L., Hancke, G. P., Mayes, K. E., &Markantonakis, K. (2010). Practical relay attack on contactless transactions by using NFC mobile phones. Cryptology ePrint Archive. https://eprint.iacr.org/2011/618
6. Alarifi, A., Al-Salman, A., Al-Ammar, M. A., Alsaleh, M., Alnafessah, A., & Al-Hadhrami, S. (2016). Ultra wideband indoor positioning technologies: Analysis and recent advances. Sensors, 16(5), 707. https://doi.org/10.3390/s16050707
7. Poturalski, M., Papadimitratos, P., &Capkun, S. (2011). Secure neighbor discovery in wireless networks: Formal investigation of possibility. ACM Transactions on Information and System Security (TISSEC), 13(3), 1–28. https://doi.org/10.1145/1592451.1592454
8. Wang, Y., & Zhang, J. (2021). Relay attack detection in NFC-based mobile payments: Challenges and solutions. Computer Communications, 175, 56–65. https://doi.org/10.1016/j.comcom.2021.04.015
9. Zhang, K., Chen, X., & Li, Q. (2020). Secure UWB-based localization and authentication: A survey and research challenges. IEEE Communications Surveys & Tutorials, 22(4), 2397–2431. https://doi.org/10.1109/COMST.2020.3010301
10. Bhattacharyya, R., Floerkemeier, C., &Sarma, S. E. (2010). Low-cost, ubiquitous RFID-tag-antenna-based sensing: Overview and experimental results. Proceedings of the IEEE, 98(9), 1563–1581. https://doi.org/10.1109/JPROC.2010.2043030