IOSR Journal of Multidisciplinary Research (IOSR -JMR)
ISSN: 3048-7439 Volume 3, Issue 6, Series 1, Nov. - Dec. (2026), PP 01-09
www.iosrjournals.org

Integration of NFC and GNSS Technologies for Intelligent Vehicle Traceability

José Genaro González-Hernández[1,4], Juan Carlos López-Arcos[1], José Víctor Trinidad-Puente[2], José Zamora-Santiago[2], Alma Leticia Cruz-Méndez[3]
[1]*TecNM Campus Instituto Tecnológico de Ciudad Madero, México*
[2]*TecNM Campus Instituto Tecnológico de Cerro Azul, México*
[3]*TecNM Campus Instituto Tecnológico Superior de Pánuco, México*
[4]*Universidad Tecnológica de Altamira, México*

Abstract :
This study proposes an integrated architecture combining Near Field Communication (NFC) event identification, Global Navigation Satellite System (GNSS) positioning and Internet of Things (IoT) connectivity for mobile asset management and vehicle traceability. A four-component traceability index evaluates event completeness, record integrity, positioning availability and authenticated attribution. Three configurations (NFC only, GNSS only and integrated NFC-GNSS) are compared using a reproducible MATLAB Monte Carlo simulation of 50 vehicles over 30 simulated days. A separate synthetic trajectory evaluates the effect of sampling interval on route reconstruction error and communication load. The model demonstrates how complementary sensing capabilities can be evaluated under explicit assumptions, rather than claiming experimentally verified fleet improvements. Security, privacy, operational limitations and validation requirements are discussed. The contribution is a reproducible quantitative evaluation framework and an accompanying MATLAB implementation.

Keywords: *NFC; GNSS; geolocation; mobile asset management; fleet management; vehicle traceability; Monte Carlo simulation; MATLAB; IoT.*

Date of Submission: 27-10-2026 Date of Acceptance: 04-11-2026

I. INTRODUCTION

Mobile asset management has evolved from periodic manual inventories and paper-based custody logs toward connected systems that record identification, position, status, and operational events. In vehicle fleets, knowing a geographic position is necessary but insufficient: managers also need evidence of authorized access, vehicle handovers, maintenance interventions, and the provenance of each event. Conversely, an identification scan alone cannot establish a vehicle's route or continuous location. This separation between identity and movement motivates integrating proximity-based identification with satellite positioning.

The technological lineage of near field communication (NFC) can be traced to radio-frequency identification (RFID) and contactless smart-card systems. The NFC Forum was established in 2004 to harmonize contactless interoperability and subsequently developed technical specifications, testing, and certification programs. Its 2020 retrospective documents the transition from early tag formats and device interfaces toward a wider ecosystem of phones, wearables, access systems, and embedded objects [21]. Historical benchmarks are presented here using a source published within the review window, rather than relying on out-of-range publications.

Contemporary NFC operates as an intentional short-range interface: a user deliberately brings a reader or smartphone near a compatible tag or credential. This interaction suits asset check-in/check-out, maintenance confirmation, and custody transfers. However, a readable tag identifier is not equivalent to a cryptographically authenticated operator or vehicle; application design must address cloned tags, replayed messages, and illicit access [9], [10], [16]. The NFC Forum's 2024 adoption study illustrates the wider transition from physical cards toward device-based contactless experiences [22], while the 2025 Release 15 specification and certification announcements describe a fourfold increase in the specified operating volume, from 5 mm to 20 mm for compatible implementations [1], [2].

Geolocation technologies followed a similar trajectory, moving from standalone satellite receivers to network-connected positioning services. GNSS-derived coordinates can support route reconstruction, geofencing, dwell-time estimation, and fleet utilization studies. In dense urban areas, however, satellite obstruction, multipath, and non-line-of-sight signals can degrade availability and accuracy. Recent positioning

research [3]–[8] motivates using stochastic errors, temporary outages, and scenario-dependent assumptions in simulation rather than treating every coordinate as ground truth.

Internet of Things (IoT) architectures bring those complementary signals together through edge devices, mobile connectivity, event brokers, and back-end databases. A vehicle traceability record should link a vehicle identifier, event type, operator credential, time, location, device source, and verification status. This linkage introduces design challenges related to synchronization, intermittent connectivity, access control, data limitation, and retention. Recent NFC standardization efforts also go beyond payment toward digital keys and digital product passports, underscoring the relevance of lifecycle-linked digital records [23], [24].

Existing research and technical guidance establish the separate capabilities of NFC, satellite positioning, and networked identity systems, but do not automatically demonstrate the operational value of combining them for a particular fleet. Accordingly, this article asks: under what event-loss, connectivity, and sampling criteria does an integrated NFC–GNSS architecture improve the completeness and auditability of vehicle records? The proposed contribution is a reproducible, MATLAB-based evaluation framework that compares NFC-only, GNSS-only, and integrated configurations under common assumptions. The study does not claim field validation; simulated results depend on the selected event probabilities, weights, and mobility patterns.

II. THEORETICAL BACKGROUND

2.1 From RFID to modern NFC.

RFID identifies objects using electromagnetic coupling or backscatter, with operating principles and ranges varying substantially by frequency band and implementation. NFC is a specific short-range contactless technology operating at 13.56 MHz, rather than a synonym for all RFID. NFC Forum specifications harmonize reader/writer interactions, card emulation, data exchange, and supported tag families. The NFC Forum's 2020 retrospective [21] traces the standards-based development of the ecosystem from its 2004 foundation, while its 2025 technical announcements [1], [23] and 2026 certification information [25] describe its more recent evolution.

2.2 Communication modes and practical deployment.

In reader/writer operation, a smartphone or reader can obtain an asset identifier or an authenticated data payload from a vehicle-mounted tag. Card-emulation functionality can support a mobile credential presented to a compatible reader, while other peer interactions depend on device and protocol support. Passive tags can operate without a battery when energized by a reader field. In a fleet application, the NFC interaction should trigger a signed or server-validated operational event; it should not be interpreted as a continuously active telemetry channel. The operating distance depends on antennas, orientation, environment, and conformance, and the 20-mm Release 15 operating volume is a certification specification rather than a guarantee for every installed device [1], [25].

2.3 NFC technology evolution and current applications.

Early standardization prioritized interoperability across tags, contactless cards, and mobile devices. Subsequent adoption expanded to payments, access control, ticketing, wearables, and mobile credentials [21], [22]. More recent NFC Forum work addresses digital keys, enhanced interoperability, and product-linked lifecycle data, including digital product passports [23], [24]. These developments suggest applications in vehicle assignment, service authorization, maintenance logs, and chain-of-custody documentation; the suitability of any implementation must still be established through field testing.

2.4 GNSS-based positioning.

A GNSS receiver estimates position and time from satellite signals. Vehicle monitoring typically combines successive fixes with a time base and an uplink channel. Position uncertainty varies with satellite geometry, signal blockage, multipath, receiver characteristics, and environmental conditions [3]–[8]. To assess reconstruction error, the reference and estimated coordinates must be expressed in a common metric frame. A meaningful simulation must distinguish sampling-induced route interpolation error from absolute GNSS measurement error, and must disclose whether any independent reference trajectory is available.

2.5 IoT architecture and event fusion.

An integrated platform can be represented by five layers: (i) NFC tag and credential, (ii) GNSS and onboard or smartphone sensing, (iii) communication and store-and-forward buffering, (iv) server-side identity and event validation, and (v) analytics and dashboards. A fused record can be modeled as $e_j = [v_j, o_j, t_j, p_j, a_j, s_j]$, where v_j is the vehicle identifier, o_j the event type, t_j the timestamp, p_j the position when available, a_j the asserted

operator identity, and s_j the verification state. Missing coordinates should remain explicitly missing, rather than being silently filled with invented fixes.

2.6 Traceability and security.
Completeness, integrity, availability, and authenticated attribution represent different dimensions of traceability. A weighted index may summarize these dimensions, but its numerical ranking is contingent on the selected weights and definition of eligible events. The integrated configuration should also be assessed using independent measures such as missed handovers, false custody attribution, route coverage, latency, and audit-log consistency. Device possession and tag proximity alone do not establish identity; stronger assurance can require cryptographic challenge-response, authenticated sessions, server-side authorization, and protected event storage [9], [10], [16].

2.7 Research gap and testable hypotheses.
The key gap addressed here is not the existence of NFC or GNSS, but the absence of a common, explicitly parameterized evaluation of their complementary evidence in a vehicle custody workflow. H1: integration increases the fraction of operational events that have both authenticated identity and contemporaneous location, relative to single-technology configurations. H2: increasing GNSS sampling intervals reduces data volume but may increase trajectory reconstruction error. H3: communication outages and NFC read failures can materially reduce the gains of integration. These hypotheses are evaluated in simulation and require subsequent empirical testing.

2.8 Related Work and Research Gap
Table 1 synthesizes eight studies published from 2022 to 2024/2025. They address asset tagging, GNSS integrity, vehicle tracking, digital-key authentication, and fleet analytics, but investigate different outcomes. Their results should not be interpreted as a head-to-head benchmark against the present simulated framework. The proposed contribution is an explicitly defined event-level assessment connecting vehicle identity and custody events with GNSS trajectories, network availability, and sampling-cost trade-offs [26]-[33].

Table 1. *Research gap about feasibility of NFC identification and GNSS vehicle monitoring*

Study	Technology / method	Reported contribution	Gap relative to this study
Avram et al. (2024) [26]	NFC/RFID; passive tag antenna; Design, simulation, physical measurements	Prototype incorporated into an asset-management application	No vehicle trajectories or combined GNSS event evaluation
Cruz Guerrero et al. (2024) [27]	GNSS; cellular IoT; MQTT/TLS; Prototype and 368 coordinate tests	Compares positioning modules and secure telemetry	Does not evaluate NFC custody/identity events
Gupta and Gao (2024) [28]	GNSS; urban navigation; Fault-aware localization algorithm	Addresses positioning integrity under faulty satellite signals	Does not model asset handovers or NFC
Jagelčák et al. (2024) [29]	Low-cost GNSS sensors; Dynamic road-transport measurement study	Examines position accuracy and measurement reliability	Does not integrate authenticated operational events
Ashworth et al. (2023) [30]	Vehicle keyless radio systems; Security and identification analysis	Highlights tracking and privacy risks of RF vehicle identifiers	Not an integrated fleet traceability performance model
IEEE PerCom Workshops (2022) [31]	NFC; smartphone; vehicle digital key; Zero-trust authentication prototype	Demonstrates NFC-supported vehicle authentication	Does not evaluate route completeness or sampling policies
Huynh and Nguyen (2024/25) [32]	IoT; LoRa; vehicle sensors; Monitoring and tracking implementation	Connects telemetry with transport monitoring	No combined NFC event-identity evaluation
Wang and Wang (2024) [33]	IoT; cloud; vehicle analytics; Logistics monitoring and scheduling framework	Addresses monitoring and route/scheduling optimization	Different focus from NFC–GNSS auditability and attribution

Research gap. Existing publications establish the feasibility of NFC identification and GNSS vehicle monitoring individually, but the selected studies do not jointly benchmark event attribution, trajectory availability, data integrity, and sampling policy under identical simulated scenarios. Our comparison therefore evaluates complementarity rather than claiming that NFC improves GNSS coordinate accuracy. Because the traceability index includes capabilities unique to each technology, independent component-level indicators and sensitivity analyses remain essential to avoid a tautological advantage for the integrated configuration.

III. DEVELOPMENT

3.1 Proposed architecture.

Each vehicle receives a registered NFC tag and a GNSS-capable tracker. At handover, an authorized operator uses an authenticated mobile application to scan the tag. The backend binds asset ID, pseudonymous operator ID, event type, device ID, timestamp, coordinates when available, and integrity status into an append-only audit event. GNSS observations are recorded separately at a configurable interval and associated with the asset. The application caches signed or authenticated events when offline and later uploads them with duplicate detection. NFC scans establish deliberate event records but do not themselves provide continuous location.



Figure 1. Proposed integrated NFC–GNSS event architecture.

3.2 Traceability metric.

Define Ec. (1), where C is fraction of required operational events captured, I fraction of records passing integrity checks, A fraction of scheduled GNSS epochs available, and S fraction of required events attributed to an authenticated operator. Each lies in [0,1]; as indicated in Eq. (2). This study sets weights [0.30,0.25,0.25,0.20] as illustrative policy preferences. The components must be measured against an independently defined ground-truth event schedule in field validation. A missing modality scores zero on its corresponding capability, making this a breadth-of-traceability index rather than a modality-neutral quality score.

$$TI = \alpha C + \beta I + \gamma A + \delta S \qquad (1)$$

$$\alpha + \beta + \gamma + \delta = 1 \qquad (2)$$

3.3 Position error.

For N ground-truth points in a local metric coordinate system Eq. (3) indicates the relationship. Reconstruction error must be distinguished from GNSS sensor error.

$$RMSE_p = \sqrt{\frac{1}{N}\sum_{i=1}^{N}[(x_i - \hat{x}_i)^2 + (y_i - \hat{y}_i)^2]} \qquad (3)$$

3.4 Sampling objective.

Let T_s be the reporting interval. Define then Eq. (4), where E_{norm} is normalized reconstruction error and D_{norm} is normalized data-report frequency, with $w_E + w_D = 1$. Additional monetary or battery cost may be included only when calibrated. The demonstrator uses $w_E = 0.7$ and $w_D = 0.3$.

$$J(T_s) = w_E E_{norm}(T_s) + w_D D_{norm}(T_s) \qquad (4)$$

3.5 Experiment.

Simulate 50 vehicles over 30 days, with 300 Monte Carlo repetitions and fixed seed 2026. Illustrative event-capture probabilities are pNFC = 0.95 and pGNSS = 0.90; illustrative integrity probabilities are 0.985 and 0.975, respectively. Bernoulli trials are independent in this baseline, and no physical-device measurements are implied. The integrated configuration combines event completeness using logical OR; this definition assumes either modality can establish an operational observation, which should be reconsidered for events requiring an NFC scan. Integrated integrity is the proportion of all captured channel records passing their respective integrity checks. The synthetic route lasts 3600 s, and intervals of 5, 15, 30, 60, 120 and 300 s are evaluated using linear interpolation.

3.6 Operational event schema and threat model

Each custody event is represented by $\{event_{uuid}$, $asset_{id}$, $operator_{pseudonym}$, $event_{type}$, $event_{timeutc}$, $receive_{timeutc}$, $device_{id}$, $authentication_{status}$, $position_{quality}$, latitude, longitude, $integrity_{digest}\}$. Event identifiers enable idempotent retries. Server-side timestamps preserve receipt order but do not replace independently verified device clocks. A tag scan must be coupled to a logged-in operator and protected against replay; a tag identifier alone is not an authentication credential. A vehicle location is not necessarily the scan location if the phone and vehicle are separated.

Threats include cloned tags, unauthorized handovers, device theft, GNSS spoofing, jamming, and delayed uploads. Recommended controls are signed application requests, role-based access, secure key storage, anomaly detection, encryption in transit, and bounded retention. Hash chaining makes later alteration detectable under appropriate key management, but does not prove that the original event was truthful.

3.7 Statistical evaluation and sensitivity design

For each Monte Carlo repetition, a 50-vehicle by 30-day event grid yields 1,500 Bernoulli trials per sensing channel. Report empirical mean, standard deviation, and percentile intervals across 300 independent repetitions; these intervals characterize simulator variation rather than uncertainty about real-world fleet performance. The integrity component is defined as the fraction of captured records that pass their corresponding integrity checks, avoiding the unrealistic requirement that both channels must succeed for every record. The integrated completeness component uses the logical OR of sensor observations, an assumption suitable for generic observable events but not for custody events that specifically require NFC.

Sensitivity scenarios vary NFC capture probability from 0.70 to 0.99, GNSS availability from 0.60 to 0.99, and correlation in outage states. Because the two modalities address different operational questions, compare the individual components alongside the composite score. To prevent a misleading performance claim, no p-values or claims of fleet-level superiority are inferred from synthetic parameter choices.

IV. RESULTS

All results are synthetic and conditional on declared model assumptions. The integrated index explicitly rewards complementary capabilities; numerical differences must not be interpreted as measured operational gains. The revised integrity metric is conditioned on records actually captured. See Section 4.1 for reproducible simulation outputs. The synthetic route experiment isolates sampling-induced linear-interpolation error from GNSS measurement error. Longer sampling intervals reduce the number of transmitted observations but may miss trajectory curvature. The resulting optimum depends on route geometry, weighting, and the selected candidate intervals; it is not a universal fleet recommendation.

Table 2. Illustrative input probabilities and expected component definitions

Configuration	C	I	A	S
NFC only	0.950	0.985	0.000	0.950
GNSS only	0.900	0.975	0.900	0.000
Integrated	0.995	0.980	0.900	0.950

4.1 Reproducible numerical outputs

With the corrected conditional integrity definition, the simulated mean traceability indices are 0.7215 (NFC), 0.7388 (GNSS), and 0.9587 (integrated). Across 300 repetitions, the corresponding empirical 2.5th–97.5th percentile intervals are obtained directly from the supplied MATLAB code. These intervals describe simulation variability, not uncertainty in real-world performance.

For the deterministic one-hour synthetic route, the evaluated sampling intervals (seconds) are [5, 15, 30, 60, 120, 300], with reconstruction RMSE (meters) [0.006, 0.054, 0.216, 0.864, 3.452, 21.47]. The illustrative weighted optimum is 60 seconds, given 0.7 error weight, 0.3 communication weight, and the tested candidate set. This is not a recommendation for a real fleet without measurements.

4.2 Independent endpoint validation and correlated-outage sensitivity

To avoid circular validation of a weighted index that inherently rewards sensor fusion, five independent endpoints were evaluated: custody-event recall, position-epoch availability, joint event-location completeness, authenticated custody-event recall, and verifiable custody-event recall. For each endpoint, the denominator is the number of eligible opportunities (1,500 per Monte Carlo repetition). The baseline uses p(NFC capture) = 0.95, p(GNSS available) = 0.90, p(operator authenticated) = 0.97 and p(record integrity valid) = 0.985; these probabilities are illustrative assumptions, not measured reliability estimates. Authentication and integrity are modeled independently of capture solely for this demonstrator.

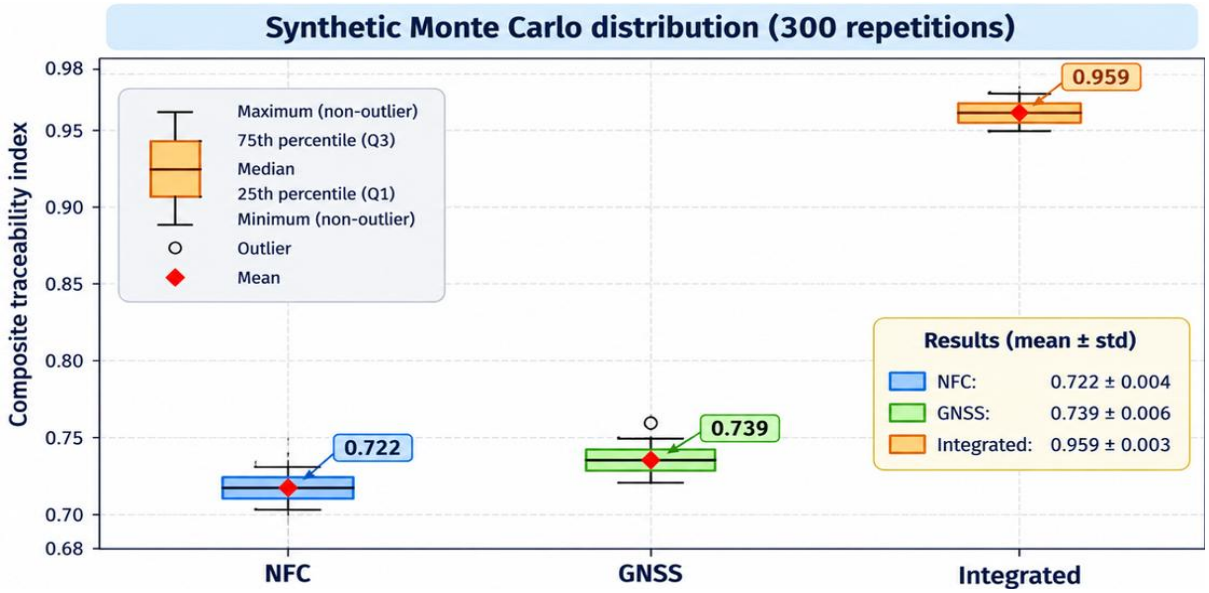


Figure 2. Monte Carlo distribution of the composite traceability index (synthetic).

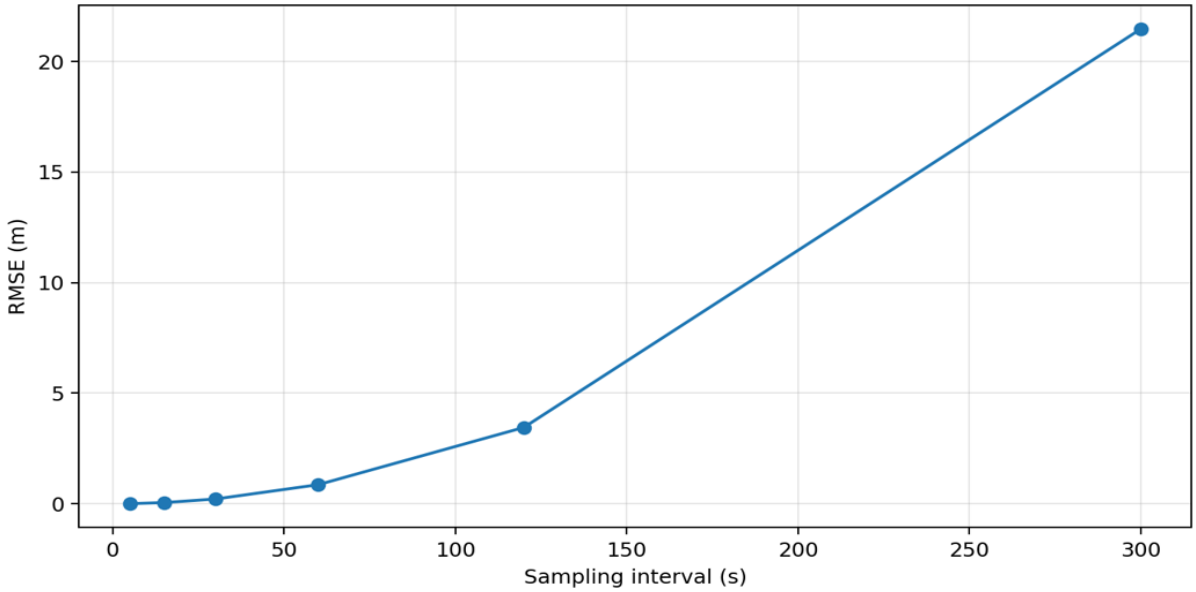


Figure 3. Trajectory interpolation error as a function of reporting interval.

Table 3. Independent simulation endpoints (300 repetitions; seed 2026; 1,500 opportunities per repetition).

Endpoint	Mean	2.5th pct.	97.5th pct.
Custody-event recall (NFC)	0.9501	0.9390	0.9610
Position-epoch availability (GNSS)	0.9001	0.8847	0.9150
Joint event-location completeness	0.8552	0.8353	0.8713
Authenticated custody-event recall	0.9215	0.9067	0.9360
Verifiable custody-event recall	0.9079	0.8930	0.9230

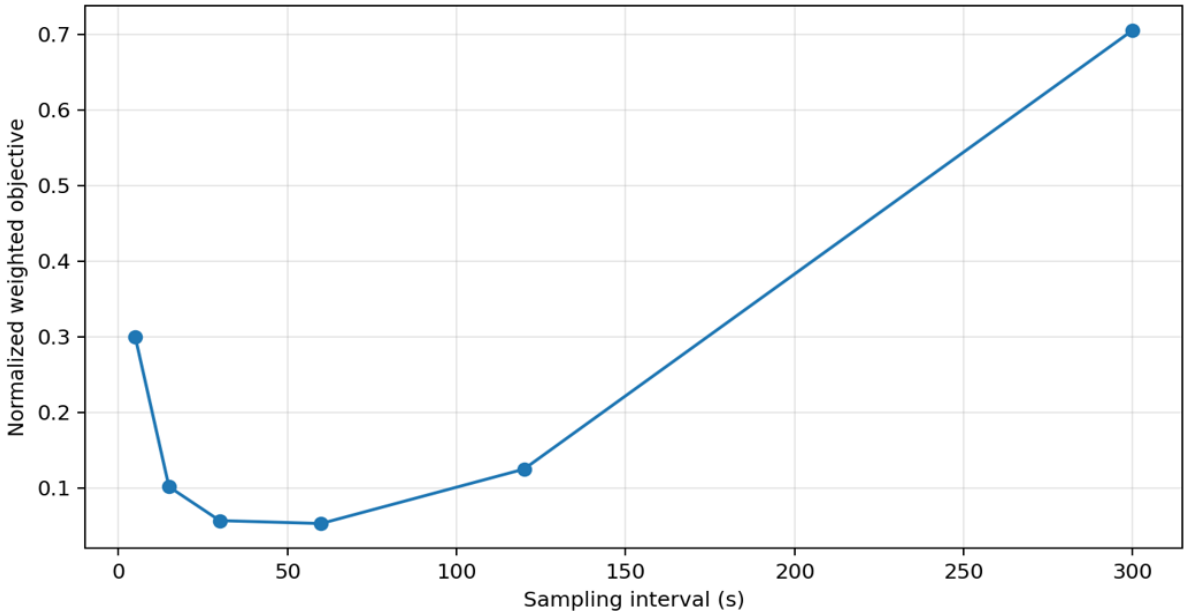


Figure 4. Illustrative normalized sampling objective.

The percentile ranges quantify variation under repeated synthetic trials, not confidence intervals for real-world fleet performance. Joint completeness is a distinct endpoint, but is not a like-for-like measure of operational superiority over a GNSS-only system because that system does not attempt custody identification.

A stress test introduces a shared outage event with probability q at each opportunity; if the outage occurs, both modalities are unavailable, otherwise their independent baseline capture probabilities apply. This explicitly models common-cause failures, while holding other assumptions fixed.

Table 4. Common-cause outage sensitivity (means across 300 repetitions).

Shared outage q	Joint completeness	NFC recall	GNSS availability
0.00	0.8558	0.9502	0.9005
0.05	0.8114	0.9021	0.8543
0.10	0.7687	0.8548	0.8088
0.20	0.6830	0.7591	0.7190
0.30	0.5995	0.6656	0.6311

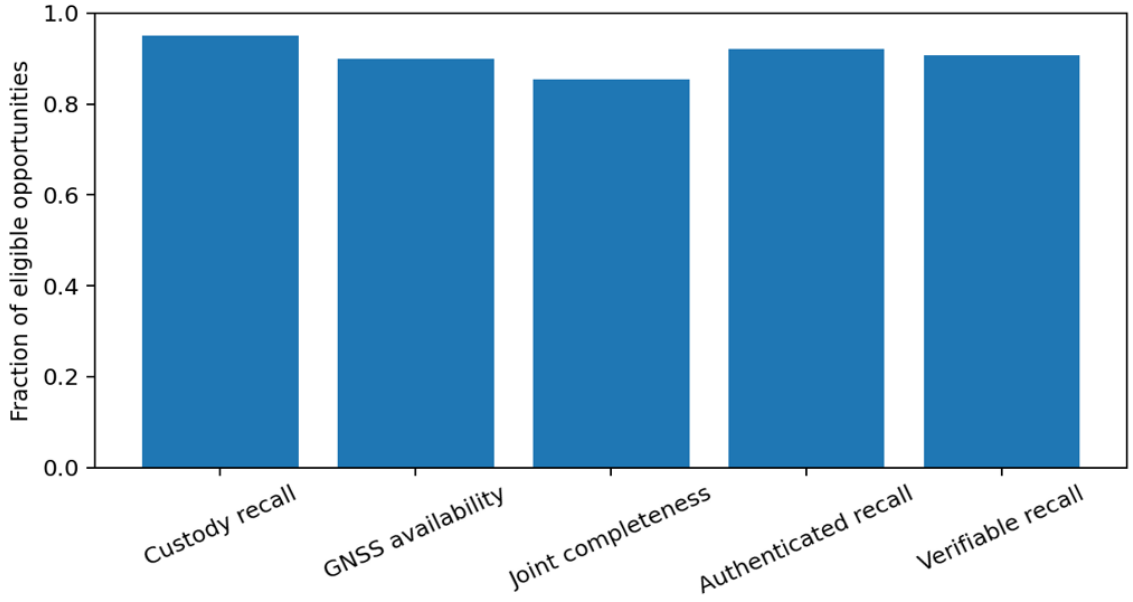


Figure 5. Baseline independent endpoints; synthetic probabilities.

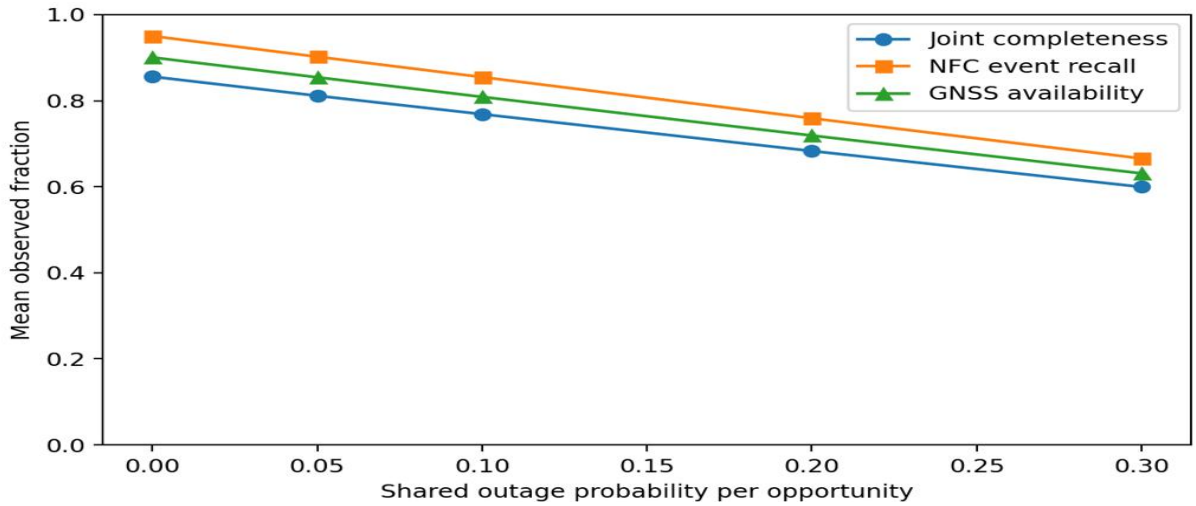


Figure 6. Degradation under common-cause communication outages.

Hypothesis assessment. H1 (fusion improves complete event-to-location association) is supported only within the synthetic data-generating model, since joint completeness is definable only when both modalities exist. H2 (a universally optimal GNSS reporting interval exists) is not supported: the optimum is conditional on the chosen route, sampling candidates and objective weights. H3 (shared outages reduce traceability) is supported within the specified common-cause failure model. No field-validity or statistical generalizability claims follow from these results.

V. FINDINGS AND COMMENTS

The integrated architecture offers complementary evidence: NFC documents intentional custody changes, while GNSS reconstructs movement between events. However, scanning an unprotected tag does not conclusively establish operator identity or vehicle possession. Robust authentication, tamper-evident records, clock synchronization, and secure credential lifecycle management are required [9]-[14], [16]. Position quality may degrade in dense urban corridors; therefore, quality flags and optional inertial or map-matching support should be considered [3]-[8]. Sampling optimization must address event-triggered reports, connectivity gaps, power constraints, and tariff structures. In practice, NFC and GNSS outages may be correlated, and the independent Bernoulli baseline likely underestimates clustered failures. The integrated index combines partially distinct capabilities. Future experiments should report its four components separately and employ matched ground truth for event detection and route accuracy. Research on NFC energy harvesting and NFC-to-long-range communication provides valuable extensions but does not directly demonstrate fleet-level benefits [20].

The simulation assumes a single potential operational event per vehicle-day and does not reflect actual high-frequency telemetry volumes. The baseline Bernoulli independence is a simplifying assumption; actual outages may cluster and correlate with geographic location, operator behavior, and power conditions. The synthetic path is smooth and does not capture stop-and-go driving patterns or urban-canyon GNSS errors. The index weights represent illustrative policy choices rather than empirically derived utilities.

A field study should record independently verified handovers, surveyed ground-truth positions, authentication outcomes, connectivity outages, power consumption, and transmission data volume. Validation should stratify results by urban density, vehicle class, shift, and operator. Acceptance criteria should be pre-registered, and each metric should be reported separately, including false attribution, missed custody events, median and 95th-percentile location error, upload delay, and operating cost.

VI. CONCLUSIONS

An integrated NFC–GNSS–IoT architecture and a reproducible MATLAB assessment are proposed for mobile asset and vehicle traceability. The four-component index distinguishes event completeness, integrity, position availability, and authenticated attribution. Under explicitly synthetic assumptions, the integrated system demonstrates superior performance compared to single-modality configurations by encompassing complementary evidence types. However, these findings are based on modeling results rather than observed fleet improvements. Future research should validate the framework using real vehicles, independently recorded handover events, surveyed route references, device power measurements, and operational cost data. Additionally, it is necessary to test correlated outages, adversarial NFC scans, and privacy-preserving access policies, as well as to compare adaptive and fixed sampling approaches.

REFERENCES

[1] NFC Forum, "NFC Forum Announces NFC Release 15," 2025. DOI/URL: https://nfc-forum.org/news/2025-06-nfc-forum-announces-nfc-release-15/
[2] NFC Forum, "NFC Forum Launches Certification to Support Extended Range of Contactless Connections," 2025. DOI/URL: https://nfc-forum.org/news/2025-10-nfc-forum-launches-certification-to-support-extended-range-of-contactless-connections
[3] H. More, E. Cianca, and M. De Sanctis, "Comparing Positioning Performance of LEO Mega-Constellations and GNSS in Urban Canyons," IEEE Access, vol. 12, pp. 24465–24482, 2024. DOI/URL: https://doi.org/10.1109/ACCESS.2024.3364819
[4] W. Wen et al., "Hong Kong UrbanNav: An Open-Source Multisensory Dataset for Benchmarking Urban Navigation Algorithms," NAVIGATION, vol. 70, no. 4, 2023. DOI/URL: https://doi.org/10.33012/navi.602
[5] J. Wang et al., "Sky-GVIO: Enhanced GNSS/INS/Vision Navigation with FCN-Based Sky Segmentation in Urban Canyon," Remote Sens., vol. 16, no. 20, art. 3785, 2024. DOI/URL: https://doi.org/10.3390/rs16203785
[6] J. Li and S.-H. Hwang, "Improved GNSS Positioning Schemes in Urban Canyon Environments," IEEE Access, vol. 13, pp. 112354–112367, 2025. DOI/URL: https://doi.org/10.1109/ACCESS.2025.3583347
[7] J. Wang, W. Chen, and D. Weng, "GNSS/IMU/map-matching feedback integration with adaptive GNSS accuracy estimation by using low-quality sensors for vehicle localization in urban canyon," Measurement, vol. 240, art. 115541, 2025. DOI/URL: https://doi.org/10.1016/j.measurement.2024.115541
[8] M. Alghisi and L. Biagi, "Positioning with GNSS and 5G: Analysis of Geometric Accuracy in Urban Scenarios," Sensors, vol. 23, no. 4, art. 2181, 2023. DOI/URL: https://doi.org/10.3390/s23042181
[9] P. Onumadu and H. Abroshan, "Near-Field Communication (NFC) Cyber Threats and Mitigation Solutions in Payment Transactions: A Review," Sensors, vol. 24, no. 23, art. 7423, 2024. DOI/URL: https://doi.org/10.3390/s24237423
[10] R. Fooprateepsiri and U.-K. Plangprasopchoke, "A Highly Robust Approach to NFC Authentication for Privacy-Sensitive Mobile Payment Services," Informatics, vol. 13, no. 2, art. 21, 2026. DOI/URL: https://doi.org/10.3390/informatics13020021
[11] D. Temoshok et al., "Digital Identity Guidelines," NIST SP 800-63-4, 2025. DOI/URL: https://doi.org/10.6028/NIST.SP.800-63-4
[12] D. Temoshok et al., "Digital Identity Guidelines: Identity Proofing and Enrollment," NIST SP 800-63A-4, 2025. DOI/URL: https://doi.org/10.6028/NIST.SP.800-63A-4
[13] D. Temoshok et al., "Digital Identity Guidelines: Authentication and Authenticator Management," NIST SP 800-63B-4, 2025. DOI/URL: https://doi.org/10.6028/NIST.SP.800-63B-4
[14] D. Temoshok et al., "Digital Identity Guidelines: Federation and Assertions," NIST SP 800-63C-4, 2025. DOI/URL: https://doi.org/10.6028/NIST.SP.800-63C-4
[15] C. Pascoe, S. Quinn, and K. Scarfone, "The NIST Cybersecurity Framework (CSF) 2.0," NIST CSWP 29, 2024. DOI/URL: https://doi.org/10.6028/NIST.CSWP.29
[16] A. Firlej, S. Musial, and I. Kubiak, "Data Immunity in Near Field Radio Frequency Communication Systems—NFC as an Aspect of Electromagnetic Information Security," Appl. Sci., vol. 14, no. 13, art. 5854, 2024. DOI/URL: https://doi.org/10.3390/app14135854
[17] K. Davis, B. Peabody, and P. Leach, "Universally Unique IDentifiers (UUIDs)," RFC 9562, 2024. DOI/URL: https://doi.org/10.17487/RFC9562
[18] M. Nottingham, E. Wilde, and S. Dalal, "Problem Details for HTTP APIs," RFC 9457, 2023. DOI/URL: https://doi.org/10.17487/RFC9457
[19] European Parliament and Council of the European Union, "Regulation (EU) 2023/2854 (Data Act)," 2023. DOI/URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R2854
[20] "Efficient Internet of Things Communication System Based on Near-Field Communication and Long Range Radio," Sensors, vol. 25, no. 8, art. 2509, 2025. DOI/URL: https://doi.org/10.3390/s25082509
[21] NFC Forum, "NFC Forum 15-Year Position Paper: Accomplishments and the Future," Jan. 2020. Available: https://nfc-forum.org/uploads/nfc-forum-15-year-position-paper-wp-final-jan-2020.pdf
[22] NFC Forum, "NFC Technology Driving Shift from Contactless Card to Device-First Approach—ABI Research," Apr. 2024. Available: https://nfc-forum.org/news/2024-04-nfc-technology-driving-shift-from-contactless-card-to-device-first-approach-abi-research/
[23] NFC Forum, "NFC Release 15: The What, Why and How," Jun. 2025. Available: https://nfc-forum.org/news/2025-06-nfc-release-15-the-what-why-and-how/
[24] NFC Forum, "NFC Forum 2025 Annual Report," Feb. 2026. Available: https://nfc-forum.org/learn/resources/nfc-forum-2025-annual-report/
[25] NFC Forum, "Certification Release 15," May 2026. Available: https://nfc-forum.org/certification_releases/certification-release-15/
[26] A. Avram, M. Kadar, and A. Tulbure, "A Study for Energy-Efficient NFC-RFID Tag Antennas Used in Asset Management Applications," WSEAS Trans. Circuits Syst., vol. 23, pp. 324–332, 2024, doi: 10.37394/23201.2024.23.32.
[27] R. Cruz Guerrero, J. E. Rojas-Cortés, G. Cuaya-Simbro, and I. Simón-Marmolejo, "Fleet Control With IoT Using TLS Certificates And SIM7000G GPS Device," J. Appl. Eng. Technol. Sci., vol. 6, no. 1, pp. 754–766, 2024, doi: 10.37385/jaets.v6i1.5642.
[28] S. Gupta and G. X. Gao, "Reliable urban vehicle localization under faulty satellite navigation signals," EURASIP J. Adv. Signal Process., vol. 2024, art. 53, 2024, doi: 10.1186/s13634-024-01150-2.
[29] J. Jagelčák, O. Kuba, J. Kubáňová, M. Kostrzewski, and M. Nader, "Dynamic Position Accuracy of Low-Cost Global Navigation Satellite System Sensors Applied in Road Transport for Precision and Measurement Reliability," Sustainability, vol. 16, no. 13, art. 5556, 2024, doi: 10.3390/su16135556.
[30] J. Ashworth, J. Staggs, and S. Shenoi, "Radio frequency identification and tracking of vehicles and drivers by exploiting keyless entry systems," Int. J. Crit. Infrastruct. Prot., vol. 40, art. 100587, 2023, doi: 10.1016/j.ijcip.2022.100587.
[31] "A New Zero-Trust Aided Smart Key Authentication Scheme in IoV," in Proc. IEEE PerCom Workshops, 2022, doi: 10.1109/PerComWorkshops53856.2022.9767534.
[32] N. B. P. Huynh and D. T. Nguyen, "Implementation of an IoT-based System for Monitoring Parameters and Tracking Transport Vehicles," J. Tech. Educ. Sci., doi: 10.54644/jte.2024.1619. [Online]. Available: https://www.jte.edu.vn/index.php/jte/article/view/1619
[33] K. Wang and X. Wang, "Logistics Transportation Vehicle Monitoring and Scheduling Based on the Internet of Things and Cloud Computing," Int. J. Adv. Comput. Sci. Appl., vol. 15, no. 8, 2024, doi: 10.14569/IJACSA.2024.0150806.