

T E C H N I S C H E A N A L Y S E

Technologische und konzeptionelle Analyse von Apple AirTags zur Personenortung

Antistalking-Mechanismen als Sicherheitsrisiko in Entführungsszenarien

mizine.de – Technologie-Redaktion

Februar 2026

Version 1.0 – Research Paper

1. Einleitung

Die fortschreitende Miniaturisierung von Elektronikkomponenten und die flächendeckende kommerzielle Verfügbarkeit von Bluetooth-basierten Ortungssystemen haben in den vergangenen Jahren zu einer signifikanten Veränderung in der Art und Weise geführt, wie Alltagsgegenstände nachverfolgt und gesichert werden. Im Zentrum dieser Entwicklung steht der von Apple im Frühjahr 2021 eingeführte AirTag – ein extrem kompakter, batteriebetriebener Transponder, der das proprietäre „Wo ist?“-Netzwerk (Find My Network) nutzt, um seinen Standort zu übermitteln.¹

Aufgrund der nahtlosen Integration in das Apple-Ökosystem, der vermeintlich globalen Abdeckung durch Milliarden aktiver iOS-Geräte und der fehlenden Abonnementkosten hat sich ein Trend etabliert, der weit über die ursprüngliche Intention des Herstellers hinausgeht. Diese Tracker werden zunehmend über ihren eigentlichen Zweck – das Auffinden von Schlüsseln, Geldbörsen oder Gepäckstücken – hinaus zweckentfremdet und zur vermeintlichen Erhöhung der Sicherheit von Kindern eingesetzt.²

Diese Zweckentfremdung offenbart bei detaillierter technologischer, kryptographischer und konzeptioneller Betrachtung fundamentale Schwachstellen. Die zentrale These lautet: AirTags stellen im Falle einer realen Entführung nicht nur keine zuverlässige Hilfe dar, sondern ein potenzielles Sicherheitsrisiko für das Opfer. Die in die Firmware integrierten Antistalking-Mechanismen verschleiern aktiv die Position des Trackers, verzögern die Aktualisierungsrate extrem und warnen den potenziellen Entführer unmittelbar und proaktiv vor der Überwachung.⁴

Die vorliegende Analyse untersucht diese Hypothese auf Basis der zugrundeliegenden Netzwerkarchitektur, der verwendeten asymmetrischen kryptographischen Protokolle, der neu implementierten herstellerübergreifenden Industriestandards (IETF DULT) sowie empirischer Sicherheitsforschungen führender universitärer Einrichtungen.

2. Systemarchitektur des Apple „Wo ist?“-Netzwerks

Im Gegensatz zu dedizierten, autarken GPS-Trackern verfügen AirTags über keinerlei eigene Hardware zur direkten Positionsbestimmung. Sie besitzen keine Empfangsmodule für globale Satellitennavigationssysteme (GNSS) und weisen keine zellularen Funkmodule zur eigenständigen Datenübertragung auf.⁵ Der AirTag fungiert stattdessen als reines, passives Bluetooth-Funkfeuer (Beacon).

2.1 Offline-Finding und asynchrones Crowd-Sourcing

Die Ortung basiert auf einem parasitären Crowd-Sourcing-Modell, das Apple als „Offline Finding“ (OF) bezeichnet. Der AirTag sendet in regelmäßigen Intervallen Bluetooth Low Energy (BLE) Advertisement-Pakete aus.⁷ Diese Signale sind extrem energieeffizient, was eine Batterielaufzeit von etwa einem Jahr mit einer CR2032-Knopfzelle ermöglicht.⁹ Das BLE-Signal enthält keine geographischen Koordinaten, sondern lediglich eine kryptographische Identifikation.

Jedes Apple-Gerät in der physischen Umgebung (10 bis 30 Meter Radius) fungiert als Finder-Gerät.¹⁰ Der Systemprozess locationd des fremden iPhones empfängt das BLE-Signal und bestimmt seine eigene Position durch GNSS-Daten, WLAN-Kartierungen und Mobilfunkmast-Triangulation.¹²¹³ Das Finder-Gerät kombiniert diese Positionsdaten mit der kryptographischen Identifikation des AirTags, verschlüsselt den Datensatz und lädt ihn anonym auf die iCloud-Server hoch.⁸

2.2 Kryptographische Verschlüsselung und Privacy-by-Design

Das Netzwerkprotokoll nutzt asymmetrische Ende-zu-Ende-Verschlüsselung auf Basis der Elliptischen-Kurven-Kryptographie (NIST P-224 Kurve).¹⁰ Der AirTag rotiert seinen Public Key in regelmäßigen Abständen (historisch alle 15 Minuten).⁷ Die hochgeladenen Standortberichte sind ausschließlich mit diesem rotierenden Public Key verschlüsselt – weder Apple noch das Finder-Gerät können den Inhalt auslesen.¹

Lediglich das autorisierte Master-Gerät des Besitzers kann die Berichte entschlüsseln und den Standort visualisieren.¹⁰ Dieses Design bedeutet zwangsläufig, dass der AirTag vollständig von der Präsenz dritter Apple-Geräte abhängig ist. Befindet sich der Tracker in einem ländlichen Gebiet, einem abgeschirmten Fahrzeug oder an einem Ort ohne iOS-Geräte, bricht die Informationskette sofort ab.¹¹⁴

3. Evolution der Antistalking-Mechanismen

Nach der Markteinführung 2021 wurde durch Opferschutzverbände und Polizeibehörden offensichtlich, dass die Effizienz des Netzwerks eine massive Gefahr für missbräuchliches Tracking darstellt.¹⁷ Die Bauform und das Fehlen optischer Signalgeber prädestinierten den AirTag dazu, unbemerkt in Taschen oder an Fahrzeugen platziert zu werden.¹⁸ Apple erweiterte das System iterativ um proaktive Antistalking-Features.¹⁷

Diese Mechanismen bilden den Kern des technischen Widerspruchs bei der Kinderortung: Das System muss algorithmisch zwischen einem „verlorenen Gegenstand“ und einem

„unerwünschten Tracker“ unterscheiden. Da der AirTag nicht erkennen kann, ob er sich am Rucksack eines Kindes oder im Kofferraum eines Stalking-Opfers befindet, wendet das Netzwerk universelle, hartcodierte heuristische Regeln an.

3.1 Zeitbasierte akustische Warnungen

Der AirTag aktiviert seinen internen Lautsprecher, wenn er für einen definierten Zeitraum vom Besitzer getrennt ist und Bewegung registriert. Ursprünglich betrug die Frist drei Tage; Apple hat sie auf 8 bis 24 Stunden nach Trennung verkürzt.²⁰ Die Audioprofile wurden optimiert, um den Tracker auch tief in Rucksäcken oder hinter Fahrzeugkarosserien auffindbar zu machen.¹⁷

Für ein Stalking-Opfer ist dies eine essenzielle Warnung. In einem Entführungsszenario bedeutet dies jedoch, dass der Täter spätestens nach wenigen Stunden durch den Tracker selbst auf dessen Existenz aufmerksam gemacht wird.

3.2 Smartphone-basierte proaktive Benachrichtigungen

Die iOS-Heuristik erkennt, wenn ein fremder AirTag über längeren Zeitraum mit einem iPhone mitreist, während das Master-Gerät nicht in Reichweite ist. Das System generiert eine „AirTag Found Moving With You“-Warnung mit einer interaktiven Karte der gemeinsamen Wegstrecke.^{21,22}

Der potenzielle Entführer kann über die Benachrichtigung den AirTag zwingen, einen lauten Ton abzuspielen, und ihn per „Precision Finding“ (UWB-Technologie) mit visuellen Pfeilen, Zentimeter-Entfernungsangaben und haptischem Feedback exakt lokalisieren.²³

3.3 Identifizierung und Deaktivierung

Durch NFC-Kontakt wird eine Webseite geöffnet, die die Seriennummer und teils Kontaktinformationen des Besitzers offenlegt.^{24,25} Das Betriebssystem präsentiert zudem eine bebilderte Anleitung zur Batterieentnahme. Sobald die Batterie entfernt oder der Tracker elektronisch blockiert wird, stoppt jegliche Standortübermittlung unwiderruflich.²⁷ Das Tracking ist vollständig neutralisiert.

4. Standortunterdrückung und Latenz

Neben den aktiven Warnungen adressiert die Analyse eine tiefere technische Ebene: die bewusste Verzögerung und algorithmische Unterdrückung der Standortaktualisierungen.

4.1 Die systemische Paradoxie

Wenn ein Kind von einer fremden Person mitgenommen wird, tritt aus algorithmischer Sicht exakt das Szenario ein, das Apple als kriminelles Stalking definiert. Die Heuristik registriert:

1. Der AirTag ist vom verifizierten Besitzer getrennt (Near-Owner-Bit im BLE-Payload von 1 auf 0 gesetzt).²⁸
2. Der AirTag bewegt sich konsistent mit einem unbekanntem Smartphone.
3. Interne Distanz- und Zeitschwellenwerte werden überschritten.⁷

Anstatt die Position in Echtzeit an die Eltern zu senden, priorisiert die Systemlogik den informationellen Schutz der angeblich „gestalkten“ Person – faktisch des Entführers.

4.2 Empirisch belegte Verzögerungen

Feldtests von mizine.de berichten von Verzögerungen bis zu anderthalb Stunden bei der Positionsaktualisierung. Unter bestimmten Bedingungen wurde nach 44 Minuten Bewegung mit einem fremden iPhone keine einzige Position übermittelt.⁴ Diese Latenz resultiert aus opportunistischen BLE-Scans, Caching-Mechanismen und Antistalking-Drosselungen im Backend.

Forschungsarbeiten der TU Darmstadt bestätigen, dass Finder-Geräte und Apple-Server komplexe Aggregations- und Unterdrückungsmechanismen verwenden.⁷ Wenn ein AirTag nur von einem einzigen fremden iPhone gemeldet wird, kann es zu einer bewussten zeitlichen Verzögerung kommen.

4.3 Das asymmetrische Informationsproblem

Während die Eltern oft über Stunden keine verwertbaren Positionsdaten sehen, arbeitet das System auf dem Gerät des Täters an der „Moving With You“-Warnung. Untersuchungen der TU Darmstadt zeigen, dass diese Warnungen innerhalb weniger Minuten nach Ankunft an einer „Signifikanten Location“ generiert werden können.⁷

Das Asymmetrieproblem ist perfekt: Der Täter hat alle Informationen und Hilfsmittel zur Lokalisierung und Deaktivierung, während die legitimen Besitzer im Unklaren bleiben.¹⁹⁴

5. Der IETF DULT-Standard

Die Problematik des unerwünschten Trackings beschränkte sich in den ersten Jahren nach der Markteinführung auf das Apple-Ökosystem. Android-Nutzer stellten einen massiven blinden Fleck in der Sicherheitsarchitektur dar, da ihre Geräte die BLE-Signale der AirTags nicht auswerteten und keine Stalking-Warnungen generierten.²³ Um dieses Asymmetrieproblem zu lösen, veröffentlichte Apple zunächst eine manuelle Scanner-App

namens „Tracker Detect“ für den Google Play Store. Da Nutzer jedoch proaktiv einen Scan anstoßen mussten, erwies sich dieser rudimentäre Schutz in der Praxis als ineffizient und unzureichend.⁷

In einer beispiellosen Zusammenarbeit kündigten die Konkurrenten Apple und Google daraufhin die Entwicklung eines gemeinsamen, verbindlichen Industriestandards an. Dieser Standard wurde unter dem Dach der Internet Engineering Task Force (IETF) formalisiert. Die Arbeitsgruppe „Detecting Unwanted Location Trackers“ (DULT) definiert ein herstellerübergreifendes Protokoll, das mobilen Plattformen ermöglicht, Bluetooth-basierte Ortungsgeräte jedweder Marke (Apple, Tile, Chipolo, Samsung, Pebblebee etc.) als potenzielle Stalking-Werkzeuge zu identifizieren.³¹

5.1 Technische Implementierung

Die DULT-Spezifikation erfordert, dass Tracker ihren Bindungsstatus aktiv über das BLE-Payload kommunizieren. Das „Near-Owner Bit“ signalisiert der Umgebung den Status: Im Near-Owner Mode (Bit = 1) ignorieren Antistalking-Algorithmen den Tracker; im Separated Mode (Bit = 0) startet ein Timer für die Stalking-Heuristik.²⁸

5.2 Globale Abdeckung durch Android-Integration

Mit iOS 17.5 und Google Play-Updates für Android ab Version 6.0 wurde DULT systemweit integriert.³³ Android-Nutzer erhalten native Systembenachrichtigungen („Tracker traveling with you“), wenn ein AirTag mit ihnen reist.³⁴ Der Schutzmechanismus deckt heute nahezu 100 Prozent des globalen Smartphone-Marktes ab.³⁵

Das Argument, ein Entführer könnte ein Android-Gerät nutzen und somit blind für den Tracker sein, ist durch den DULT-Standard vollständig obsolet geworden.

6. Wissenschaftliche Evaluierung

Das Secure Mobile Networking Lab (SEEMOO) der TU Darmstadt hat unter Prof. Dr. Matthias Hollick wegweisende Analysen zu Apples Bluetooth-Crowdsourcing publiziert.¹⁰ Die Forscher entwickelten das Open-Source-Framework „OpenHaystack“ durch Reverse Engineering des Apple-Protokolls.⁷

6.1 Location Correlation Attacks

Die Analysen bestätigen die Robustheit der asymmetrischen Kryptographie gegen klassisches Tracking. Dennoch konnten durch „Location Correlation Attacks“ strukturelle Schwachstellen

identifiziert werden: Apple könnte theoretisch soziale Graphen erstellen, da die Identität des hochladenden Finder-Geräts serverseitig korreliert werden könnte.¹⁰

6.2 Umgehung der Antistalking-Mechanismen

Forscher demonstrierten, dass durch Firmware-Modifikation („cloned AirTags“) die Identifikationsbytes so verändert werden können, dass der Tracker sich als gewöhnliches Apple-Zubehör ausgibt.⁷ Zudem können aggressive Key-Rotationen die Detektionsalgorithmen umgehen. Das akademische System „AirCatch“ wurde vorgeschlagen, um solche Tracker anhand ihres elektromagnetischen Fingerabdrucks zu erkennen.³⁷

6.3 Relevanz für den regulären Nutzer

Für Eltern sind diese Umgehungsmechanismen irrelevant, da sie unmodifizierte AirTags verwenden. Die Forschung unterstreicht vielmehr, dass die fest codierten Schutzmechanismen bei Standardgeräten hochgradig zuverlässig arbeiten.⁴

7. Hardware-Risiken und regulatorische Einschränkungen

AirTags werden durch CR2032-Lithium-Knopfzellen betrieben, die bei Verschlucken eine lebensbedrohliche Gefahr für Kleinkinder darstellen. Im Kontext des US-amerikanischen „Reese’s Law“ rügte die Consumer Product Safety Commission (CPSC) Apple wegen mangelhafter Warnhinweise.³⁹ Apple musste erweiterte Warnsymbole im Batteriefach anbringen und digitale Warnhinweise verschärfen.

Apples EULA schließt die Überwachung von Personen ausdrücklich aus. Die strikte Implementierung der „Moving with you“-Warnungen schützt das Unternehmen vor weitreichenden rechtlichen Konsequenzen und Sammelklagen, die in den USA bereits aufgrund konkreter Missbrauchsfälle – insbesondere Stalking durch Ex-Partner – eingereicht wurden.¹⁷ Es ist technologisch und juristisch ausgeschlossen, dass Apple die Funktionalität zugunsten einer verdeckten Kinderortung anpassen wird.

8. Technologische Gegenüberstellung: BLE-Tags vs. GPS-Tracker

Aufgrund der eklatanten konzeptionellen Schwächen, der unvorhersehbaren Latenzen und der zwingenden Antistalking-Warnungen von AirTags wird bei Sicherheitsexperten und in Verbrauchertests einhellig der Einsatz dedizierter, zellulärer GPS-Tracker empfohlen.⁴ Branchenanalysten vergleichen die Gegenüberstellung eines AirTags mit einem dedizierten GPS-Tracker treffend mit dem Vergleich „zwischen einem Fahrrad und einem Auto: Beide

bringen Sie von A nach B, aber auf völlig unterschiedliche Weise, mit unterschiedlichen Geschwindigkeiten und Zuverlässigkeiten“.⁴¹

Merkmal	Apple AirTag (BLE)	Dedizierter GPS-Tracker
Primäre Positionsbestimmung	Keine eigene Lokalisierungshardware. Zwingend auf aggregierte GPS-Daten fremder Apple-Geräte in BLE-Reichweite angewiesen. ⁴	Eigenständige, direkte Kommunikation mit GNSS-Satelliten (GPS, Galileo, GLONASS). Völlig unabhängig von umgebenden Smartphones. ⁶
Datenübertragung (Uplink)	Parasitär. Benötigt ein internetverbundenes Fremdgerät (iPhone/iPad) in der Nähe. ⁸	Autonom. Nutzt fest verbaute eSIM-Karten und zellulare Netze (LTE-M, 4G, 5G, NB-IoT). ⁴²
Aktualisierungsfrequenz	Hochgradig volatil. Latenzen von Minuten bis zu 1,5 Stunden empirisch belegt. ⁴	Echtzeit (Real-Time Tracking). Update-Intervalle von wenigen Sekunden. ⁵
Antistalking-Warnungen	Ja. Proaktive akustische Warnungen (8–24h) und visuelle Push-Benachrichtigungen an alle Smartphones (iOS/Android). ²⁰	Nein. Vollständig passiv gegenüber der Umgebung. Keine Warnungen an umgebende Geräte. ⁶
Betriebsreichweite	Stark begrenzt durch BLE-Reichweite (ca. 10–30m) zum nächsten kompatiblen Smartphone. Fällt in ländlichen Gebieten massiv ab. ¹¹	Global entsprechend zellulärer Netzabdeckung. Volle Funktionalität unabhängig von Bevölkerungsdichte. ⁵
Geofencing & Aktive Alarmierung	Nicht nativ vorhanden für komplexe Zonenalarme. ⁴⁴	Hochkomplexes Geofencing. Sofortige Push-Benachrichtigungen bei Verlassen definierter Sicherheitszonen. ⁴¹
Energieversorgung	CR2032-Knopfzelle (Verschluckungsgefahr), Laufzeit ca. 1 Jahr. ⁹	Wiederaufladbare Lithium-Ionen-Akkus. Laufzeit je nach Ping-Frequenz mehrere Tage bis Wochen. ⁵
Zwei-Wege-Kommunikation	Nicht vorhanden. Keine Interaktion mit dem Träger möglich.	Oftmals vorhanden. SOS-Tasten, Notrufe, Videotelefonie, Sprachnachrichten. ⁴
Kostenstruktur	Ca. 30 Euro, keine laufenden Abonnementgebühren. ⁵	Höhere Anschaffungskosten plus monatliche Abonnementgebühren für die zellulare Datenübertragung. ⁵

8.1 Technologische Autonomie als entscheidender Sicherheitsfaktor

Die Autonomie dedizierter GPS-Tracker eliminiert die Fehlerquelle der fremden Infrastruktur. Ein professioneller GPS-Tracker kommuniziert direkt mit dem Satellitennetzwerk, berechnet seine Koordinaten autonom und übermittelt diese über eine zuverlässige LTE-M- oder 4G-Verbindung direkt auf die Applikation der Eltern.⁶ Geräte wie der in der Forschung und in Verbrauchertests referenzierte Weenect-Tracker oder GPS-Smartwatches wie die imoo Z7 oder die Garmin Bounce bieten genau diese erforderliche

Unabhängigkeit.⁴⁴⁶⁴⁷ Auch der Jobit-Tracker wird in professionellen Evaluierungen als geeignete Alternative für die Kinderortung genannt.⁴⁰

Entscheidend im Kontext von Entführungen ist das vollständige Fehlen jeglicher Antistalking-Protokolle bei diesen dedizierten GPS-Trackern. Da diese Geräte nicht auf Crowdsourcing basieren, sind sie nicht an die IETF DULT-Spezifikation oder die Apple/Google-Sicherheitsrichtlinien gebunden.⁴³ Ein dedizierter GPS-Tracker piept nicht autonom und sendet keine BLE-Advertisement-Pakete aus, die das Betriebssystem eines modernen Smartphones auswerten könnte. Der Tracker bleibt verdeckt und verschafft den Eltern und Strafverfolgungsbehörden exakt das kritische Zeitfenster für eine unbemerkte Echtzeitverfolgung und ein schnelles, taktisches Eingreifen.⁶

9. Psychologische Effekte: Trügerische Sicherheit

Der Einsatz von AirTags zur Kinderortung erzeugt einen gefährlichen psychologischen Effekt der „trügerischen Sicherheit“ (False Sense of Security).⁴ Die hohe Marktpenetration, das reibungslose Pairing und die geringen Kosten verleiten Eltern zur Annahme, ein vollwertiges Sicherheitssystem erworben zu haben.³

Die positive Alltagserfahrung – Ortung in dicht besiedelten Umgebungen – stützt diese Illusion, da der AirTag in diesen Momenten von einer hohen iPhone-Dichte profitiert oder der Near-Owner-Mode die Antistalking-Maßnahmen temporär deaktiviert.²⁸ Im Notfall greifen jedoch die Drosselungs-, Warn- und Deaktivierungsmechanismen mit algorithmischer Konsequenz.²

10. Fazit und abschließende Bewertung

Die umfassende technologische, kryptographische und protokollare Analyse des Apple „Wo ist?“-Netzwerks, der IETF DULT-Spezifikation sowie der Hardware-Eigenschaften der AirTags bestätigt die Prämisse vollumfänglich: AirTags stellen im Falle einer Entführung keine verlässliche Hilfe dar und wirken aufgrund des hochpriorisierten Stalking-Schutzes kontraproduktiv.⁴

AirTags sind als Asset-Tracker für verlorene Gegenstände konzipiert. Ihr parasitäres Crowdsourcing-Modell macht sie vollständig abhängig von einer hohen Dichte fremder Endgeräte. Sobald ein AirTag zur Personenüberwachung genutzt wird, initiiert die Firmware eine defensive Eskalationskette: proaktive visuelle Warnungen an das Gerät des Täters³³, akustische Alarmer nach 8 bis 24 Stunden²⁰ sowie NFC-basierte Deaktivierungsanleitungen.²⁵ Parallel dazu führt die Netzwerkarchitektur zu Latenzzeiten von bis zu anderthalb Stunden.⁴

Der Einsatz von AirTags zur Sicherung von Kindern vermittelt eine eklatant trügerische Sicherheit. Für sicherheitskritische Anwendungsfälle stellen dedizierte, zellulare GNSS/GPS-Tracker, die unabhängig von Fremdinfrastruktur arbeiten, Echtzeitdaten über das Mobilfunknetz liefern und keine verräterischen Bluetooth-Pakete aussenden, die einzig technologisch belastbare und verantwortungsvolle Alternative dar.

Referenzen

- [1] AirTag – Apple. <https://www.apple.com/airtag/>
- [2] Expert Guide 2025: Can I Put an AirTag in My Kid’s Backpack? – jianglidabag.com. <https://www.jianglidabag.com/expert-guide-2025-can-i-put-an-airtag-in-my-kids-backpack-5-practical-facts-for-parents/>
- [3] Why AirTags Aren’t Safe for Kids: A Parent’s Guide – littlebird.care. <https://www.littlebird.care/journal/why-airtags-arent-safe-for-kids-a-parents-guide-to-child-specific-tracking-solutions>
- [4] Mit AirTag Kinder tracken? So weit geht die Apple AirTag Reichweite – mizine.de. <https://mizine.de/apple/apple-airtags-kinder-orten/>
- [5] GPS Trackers vs. AirTags: A Comprehensive Comparison – GPYes. <https://www.gpyes.com.au/gps-trackers-vs-airtags-a-comprehensive-comparison>
- [6] GPS Trackers vs. Apple AirTag: Key Differences Explained – LandAirSea. <https://landairsea.com/blogs/consumers/gps-trackers-vs-apple-airtag-whats-the-difference-and-why-should-i-care>
- [7] Track You: A Deep Dive into Safety Alerts for Apple AirTags – PoPETs 2023. <https://petsymposium.org/popets/2023/popets-2023-0102.pdf>
- [8] How Does Apple “Find My” Work Even Without Internet? – Ugreen. <https://us.ugreen.com/blogs/smart-finder/how-does-find-my-work-across-devices>
- [9] Apple AirTag vs GPS Trackers: Which One Keeps You Safer? – UTrack. <https://www.utrack.ai/apple-airtag-vs-gps-tracker/>
- [10] seemoo-lab/openhaystack – GitHub (TU Darmstadt). <https://github.com/seemoo-lab/openhaystack>
- [11] How Does AirTag Share Location? – Link Labs. <https://www.link-labs.com/blog/how-does-airtag-share-location>
- [12] Politecnico di Milano – Scuola di Ingegneria Industriale e dell’Informazione. https://www.politesi.polimi.it/retrieve/9631d7a8-0c85-4088-9010-b454274550da/2021_12_Fontana_01.pdf
- [13] Can My Phone Be Tracked If Location Services Are Off? – McAfee. <https://www.mcafee.com/learn/can-my-phone-be-tracked-if-location-services-are-off/>
- [14] Apple introduces new AirTag with expanded range – Apple Newsroom 2026. <https://www.apple.com/newsroom/2026/01/apple-introduces-new-airtag-with-expanded-range-and-improved-findability/>
- [15] How Often Does AirTag Update? – Ugreen. <https://us.ugreen.com/blogs/smart-finder/airtag-update-frequency-tracking-tips>
- [16] My air tag is showing 87 miles away – Reddit r/AirTags. <https://www.reddit.com/r/AirTags/comments/1llttvq/>
- [17] An update on AirTag and unwanted tracking – Apple Newsroom 2022. <https://www.apple.com/newsroom/2022/02/an-update-on-airtag-and-unwanted-tracking/>
- [18] What is AirTag Stalking? – Bitdefender. <https://www.bitdefender.com/en-us/blog/hotforsecurity/airtag-stalking>
- [19] How to know if you’re being tracked by an AirTag – Asurion. <https://www.asurion.com/connect/tech-tips/how-to-stop-an-airtag-from-tracking-you/>

- [20] Apple AirTags and Your Safety – UW–Madison Police Department. <https://uwpd.wisc.edu/apple-airtags-and-your-safety/>
- [21] What to do if you get an alert that an AirTag is with you – Apple Support. <https://support.apple.com/en-us/119874>
- [22] How to locate an unknown AirTag moving with you – Apple Support (YouTube). <https://www.youtube.com/watch?v=mGh7-luPRR4>
- [23] How to detect and disable Apple AirTags – Help Net Security. <https://www.helpnetsecurity.com/2025/02/11/apple-airtags-tracking-detect-disable/>
- [24] How to Protect Yourself from Unwanted AirTag Tracking – Gizchina.com. <https://www.gizchina.com/how-to/how-to-protect-yourself-from-unwanted-apple-airtag-tracking>
- [25] Unwanted Tracking – Apple Support Communities. <https://discussions.apple.com/thread/254341538>
- [26] Why am I getting a detected tracking notification? – Apple Communities. <https://discussions.apple.com/thread/254959656>
- [27] Detect unwanted trackers – Apple Support. <https://support.apple.com/guide/personal-safety/detect-unwanted-trackers-ips139b15fd9/web>
- [28] Detecting Unwanted Location Trackers – IETF Draft (DULT). <https://www.ietf.org/archive/id/draft-detecting-unwanted-location-trackers-01.html>
- [29] Security Now! Transcript Ep. #923 – Gibson Research. <https://www.grc.com/sn/sn-923.htm>
- [30] Revelation of System and Human Vulnerabilities Across MITRE ATT&CK – CMU. <http://reports-archive.adm.cs.cmu.edu/anon/s3d2023/CMU-S3D-23-107.pdf>
- [31] Detecting Unwanted Location Trackers (dult) – IETF Datatracker. <https://datatracker.ietf.org/group/dult/about/>
- [32] DULT Charter – IETF Datatracker. <https://datatracker.ietf.org/doc/charter-ietf-dult/00-01/>
- [33] Apple and Google deliver support for unwanted tracking alerts – Apple Newsroom 2024. <https://www.apple.com/newsroom/2024/05/apple-and-google-deliver-support-for-unwanted-tracking-alerts-in-ios-and-android/>
- [34] Find unknown trackers – Android Help. <https://support.google.com/android/answer/13658562?hl=en>
- [35] Google and Apple deliver support for unwanted tracking alerts – Google Security Blog. <https://security.googleblog.com/2024/05/google-and-apple-deliver-support-for.html>
- [36] Protection mechanisms against unwanted tracking – SEEMOO TU Darmstadt. <https://www.seemoo.tu-darmstadt.de/theses/protection-mechanisms-against-tracking/>
- [37] AirCatch: Effectively tracing advanced tag-based trackers – arXiv. <https://arxiv.org/html/2602.07656v1>
- [38] Okay Google, Where’s My Tracker? – PoPETs 2025. <https://petsymposium.org/popets/2025/popets-2025-0147.pdf>
- [39] CPSC Secures Agreement with Apple for Enhanced Warnings – CPSC.gov. <https://www.cpsc.gov/Newsroom/News-Releases/2025/CPSC-Secures-Agreement-with-Apple-for-Enhanced-Warnings>
- [40] Tracking Devices for Kids Reviews – PCMag. <https://www.pcmag.com/categories/tracking-devices-for-kids>
- [41] AirTag vs GPS Tracking – BrickHouse Security. <https://www.brickhousesecurity.com/blog/airtag-vs-gps-tracking>
- [42] Apple AirTag vs. GPS Trackers – GPX.co. <https://gpx.co/blog/apple-airtag-vs-gps-trackers/>
- [43] Apple AirTags vs GPS Trackers – Logistimatics. <https://logistimatics.com/blogs/guides/apple-airtags-vs-gps-trackers>
- [44] Tune Find My for Travel Tracking – VMUG. <https://vmug.bc.ca/tune-find-my-for-travel-tracking-to-avoid-annoying-airtag-and-apple-device-alerts/>
- [45] Apple AirTag vs. GPS Trackers: Which One is Best for Safety? – TackGPS. <https://www.tackgps.app/blogs/news/apple-airtag-vs-gps-trackers-which-one-is-best-for-safety>
- [46] Best GPS tracker for kids in 2025 – Tom’s Guide. <https://www.tomsguide.com/us/best-gps-child-trackers,review-2884.html>
- [47] The best GPS trackers for kids in 2026 – ZDNET. <https://www.zdnet.com/article/best-gps-trackers-and-devices-for-kids/>