KLAIPEDA UNIVERSITY

Faculty of Marine Technology and Natural Sciences

Department of Informatics and Statistics

Location-Aware Cyber Threats and Defenses: Mobile Gaming and Drone Applications

Bachelor’s Final Thesis

Klaipėda, 2025

**Abstract**

This thesis investigates the growing security and privacy challenges in location-based applications, with a focus on mobile augmented reality (AR) games (e.g. **Pokémon Go**) and unmanned aerial vehicles (UAVs, or drones). Modern devices rely on diverse positioning signals (including GPS, Wi-Fi, Bluetooth beacons, and cellular networks) to overlay digital content onto the real world or to navigate autonomous vehicles. In gaming, games apps operate in three connectivity modes: always-connected (fully online), hybrid (a mix of online and offline), and never-connected (entirely offline). While such location-aware technology enables compelling services (from gaming to cargo delivery), it also exposes critical attack surfaces. We analyze how adversaries can spoof or hijack these signals: for example, injecting counterfeit GPS coordinates can covertly redirect a drone’s flight path, or falsify a player’s location in an AR game. Unencrypted radio links and weak authentication in many platforms further permit eavesdropping, hijacking, or data manipulation. Through a combination of literature review, threat modeling, and case analysis, this work catalogs the principal location-based threats in both domains. We identify the most vulnerable systems (e.g. civilian GPS on drones, mobile OS location APIs), dissect attack techniques (GPS spoofing, radio jamming, data injection, and privacy exploitation), and evaluate their impacts on safety, privacy, and economics. Our contributions include a taxonomy of attacks on geo-enabled games and UAVs, an assessment of real-world incidents (including military and civilian demonstrations), and a survey of countermeasures. We discuss both technical defenses (signal authentication, anomaly detection, encrypted telemetry) and policy measures (regulation of geofencing, privacy guidelines). We also evaluate emerging cryptographic strategies, including quantum-resistant (post-quantum) encryption schemes, for future-proofing telemetry and location data on resource-constrained devices. Finally, the thesis examines how emerging trends – such as 5G’s network positioning and AI-driven navigation – may mitigate or exacerbate these risks. By systematically examining location-based vulnerabilities in gaming and drones, this study aims to inform developers, policymakers, and security researchers about safeguarding the safety-critical systems that underpin modern AR experiences and autonomous flight.

**CONTENTS**

**Chapter 1 - Introduction**

1.1 Background and Context

1.2 Problem Statement

1.3 Research Aim and Objective

1.4 Research Questions

1.5 Scope and Delimitations

1.6 Significance of the Study

**Chapter 2 - Location-Aware Technologies and Applications**

2.1 Overview of Location-Aware Technologies  
 2.2 Mobile Gaming and Drone Applications in Context

2.2.1 Modes of Connectivity in Games (Online, Hybrid, Offline)  
 2.3 Common Cybersecurity and Privacy Risks in Location-Aware Systems  
   2.3.1 GPS Spoofing  
   2.3.2 Location Surveillance  
   2.3.3 Game Cheating & Exploits (e.g., Pokémon Go)  
   2.3.4 Unauthorized Data Collection & Third-Party Tracking  
   2.3.5 Drone Hijacking & Control Takeover  
 2.4 Case Studies of Impacted Platforms  
   2.4.1 Pokémon Go  
   2.4.2 AR Glasses (HoloLens, Magic Leap, etc.)  
   2.4.3 Consumer Drones (DJI, Parrot, etc.)  
 2.5 Summary of Literature Gaps

**Chapter 3 - Methodology**  3.1 Research Design (Literature-Based Approach)  
 3.2 Data Sources (Academic Databases, Industry Reports, Cybersecurity Bulletins)  
 3.3 Selection Criteria for Case Studies  
 3.4 Limitations of the Research

**Chapter 4 - Findings and Analysis**  4.1 Categorization of Location-Aware Threats  
 4.2 Threat Vectors in Mobile Gaming  
 4.3 Threat Vectors in Drone Applications  
 4.4 Comparative Risk Analysis (Gaming vs. Drones)  
 4.5 Emerging Trends (e.g., AI-driven Attacks, Cross-Platform Exploits)

**Chapter 5 - Defense Mechanisms and Best Practices**  
 5.1 Existing Technical Countermeasures  
   5.1.1 Anti-Spoofing Technologies  
   5.1.2 Encryption & Secure Communication Protocols

5.1.3 Quantum-Resistant Approaches for Future-Proofing  
   5.1.3 Geofencing  
   5.1.4 Intrusion Detection Systems for IoT Devices  
 5.2 Policy and Regulatory Frameworks  
 5.3 Industry Standards & Compliance (e.g., GDPR, FAA Regulations for Drones)  
 5.4 User Awareness and Education  
 5.5 Limitations of Current Defenses

**Chapter 6 - Conclusion and Recommendations**  
 6.1 Summary of Key Findings  
 6.2 Recommendations for Future Research  
 6.3 Practical Recommendations for Industry and Users  
 6.4 Final Thoughts

**LIST OF FIGURES**

**Fig. 1.** Images of the RQ-170 Sentinel taken from a US Army recognition manual (Source:[**wikipedia**](https://upload.wikimedia.org/wikipedia/commons/thumb/0/09/RQ-170_from_US_Army_recognition_manual.jpg/500px-RQ-170_from_US_Army_recognition_manual.jpg))

**Fig. 2.** Typical architecture for location-aware applications showing GNSS satellites, cellular/Wi-Fi positioning and backend servers (source: [Sumit Dev](https://miro.medium.com/v2/resize:fit:720/format:webp/1*xLzOExtqanGvyjAD_dsLdQ.png)).

**Fig. 3.** FLIR Black Hornet 3

**Fig. 5.** Exploded view of the Hololens 2 to show its components

**Fig. 4.** Geo-Data is used for some core features of Pokemon Go

**INTRODUCTION**

## **1.1 Background and Context**

Global Navigation Satellite Systems (GNSS), such as GPS, provide worldwide positioning and timing. Civilian GPS signals are free and unencrypted, making them universally accessible to consumer devices (smartphones, tablets, UAVs). Indoor and urban positioning often rely on Wi-Fi fingerprinting or cellular-cell triangulation, while Bluetooth Low Energy (BLE) beacons are used for precise local tracking in spaces like malls or offices. Augmented reality (AR) games leverage these technologies to anchor virtual objects in real geography: for example, *Pokémon Go* uses a phone’s GPS and camera to “place” creatures at real-world locations. In parallel, UAVs increasingly permeate both military and commercial sectors. Beyond the early military-reconnaissance roles, drones now perform disaster relief, infrastructure inspection, aerial photography, and even package delivery. These vehicles routinely use GNSS for Guidance, Navigation and Control (GNC). They also employ radio links (e.g. Wi-Fi, LTE, or dedicated RF) to exchange telemetry and video with ground stations.

The convergence of these technologies has enabled innovative applications but also expanded the attack surface. Any system that relies on signal-based positioning can be spoofed or jammed. GNSS signals, for instance, are extremely weak by the time they reach Earth, so attackers with modest equipment can overpower or mimic them. Similarly, radio-control links in consumer drones are often unencrypted and unauthenticated, allowing a nearby adversary to intercept or inject commands. In the AR gaming context, mobile devices continuously broadcast or log their location, which can be harvested to infer users’ movement patterns. Moreover, many AR games integrate user-generated scans of the environment (e.g. Niantic’s Visual Positioning System) to build 3D maps of real-world spaces. This can inadvertently produce detailed imagery of sensitive locations (military bases, private residences) as “fun” game data.

Taken together, these trends highlight a critical security context: the very prevalence of location-based services makes them attractive targets. Drones and AR apps are now widely used by civilians and organizations alike, and any breach of their location integrity can have serious consequences. For example, misdirecting a delivery drone could endanger people or property, and falsifying a player’s GPS position in an AR game undermines fair play and may violate laws (e.g. trespassing).

## **1.2 Problem Statement**

Despite the benefits of location-aware technology, adversaries have demonstrated multiple attack vectors that exploit positioning signals. A primary concern is **signal spoofing and jamming**. In GPS spoofing, an attacker transmits counterfeit satellite signals to deceive a receiver about its true location or time. This can cause an unmanned vehicle to deviate from its intended course or even crash. In fact, research and incidents have shown that drones using standard civilian GPS can be forced to follow false trajectories or violate geo-fences (no-fly zones) once their position is manipulated. Because GPS lacks encryption, any receiver that trusts the strongest signal can be fooled without detecting interference. Jamming is a related threat: high-power interference can deny service by drowning out legitimate GNSS, forcing systems to navigate blind or fall back on potentially unreliable inertial sensors.

Beyond satellite signals, many drone models use unprotected **radio communication links** to their controllers. Security analyses have shown that these RF links can often be intercepted or hijacked with readily available tools. For instance, a hacker intercepting the (typically unencrypted) control channel can issue false commands to the drone – effectively seizing control of the vehicle. Likewise, First-Person View (FPV) video streams from consumer drones are frequently unencrypted, letting eavesdroppers or falsifiers access live camera feeds. The problem extends to AR gaming platforms as well. Malicious apps or man-in-the-middle attacks could potentially alter game data or inject fake virtual objects by tampering with the location API or game server responses. Even if the game server is secure, the **privacy of users** is at stake: continuous location logs and images captured by players can be harvested to build detailed profiles of where people go and what places they photograph.

In summary, the problem addressed by this thesis is the identification and characterization of **location-based threats** in AR games and UAVs. Specifically, we focus on how an attacker can manipulate location signals or data to impact users, operators, and bystanders. This includes

1. Safety hazards (e.g. crashed drones, misled users)
2. Privacy violations (tracking movements or maps of sensitive sites)
3. Economic or policy repercussions (cheating in games, regulatory breaches).

The key challenge is that these attacks exploit fundamental assumptions (e.g. “the GPS signal is correct”) that many applications make implicitly. By systematically exploring the threat models and recent exploits, we aim to illuminate the security flaws inherent in relying on external positioning systems.

## **1.3 Research Aim and Objectives**

The overarching aim of this research is to analyze and mitigate location-based security threats in mobile AR gaming and commercial UAV platforms. We set the following objectives to achieve this aim:

**Threat Taxonomy**: Identify and categorize the main types of location-based attacks relevant to AR games and drones (e.g. GNSS spoofing, radio hijacking, location-faking malware, data harvesting).

**Vulnerability Analysis**: Determine which platforms and technologies are most susceptible (e.g. iOS vs Android location APIs, hobbyist drones with open protocols) and detail the technical root causes of these weaknesses (such as lack of signal authentication or device trust models).

**Impact Assessment**: Evaluate the potential consequences of these attacks on safety (risk of collisions or loss of vehicle), privacy (exposure of user movements or images), and economic factors (e.g. costs of service disruption, liabilities, or cheating).

**Defense Evaluation:** Survey existing defenses – both technical (encrypted positioning, anomaly detection in sensor data, secure communication links) and policy-level (regulations on frequency use, geofencing rules, privacy laws) – and assess their effectiveness for the identified threats.

**Futures Analysis:** Consider emerging trends like 5G network-based localization and AI-driven navigation, and speculate how they may alter the threat landscape (for example, by adding new localization sources or by making spoofing attacks easier/harder to execute).

These objectives guide our investigation of “what can go wrong” and “how to fix it” in these two rapidly growing domains that heavily rely on geography.

## **1.4 Research Questions**

To structure the inquiry, we pose the following research questions:

1. **What are the main location-based security and privacy threats affecting mobile AR games and UAVs?** This includes technical attacks (e.g. spoofing, jamming, data injection) and broader misuse (location tracking, unauthorized surveillance).
2. **Which devices, platforms, or deployment scenarios are most vulnerable?** For example, comparing different smartphone OSes or consumer drone models, and considering factors like GPS chipsets or link encryption.
3. **What underlying technical mechanisms enable these attacks?** (e.g. GPS signal properties, wireless protocol weaknesses, API trust assumptions). We will examine how the attacks are implemented in practice.
4. **What are the potential impacts of location-based attacks in each domain?** This spans user safety, operational reliability, privacy (e.g. user location history exploitation), and economic costs (e.g. replacement of lost drones, regulatory fines).
5. **Which defense strategies (technical and policy) can mitigate these threats?** We will compare countermeasures like cryptographic GNSS enhancements, drone control link security, privacy-preserving data practices, and relevant regulations.
6. **How might upcoming trends (e.g. 5G positioning, AI navigation) influence future vulnerabilities and defenses?** We explore whether new technologies will introduce novel risks or improve resilience.

Answering these questions will yield a comprehensive understanding of location-based attack vectors and protection strategies in AR gaming and drone ecosystems.

## 

## **1.5 Scope and Delimitations**

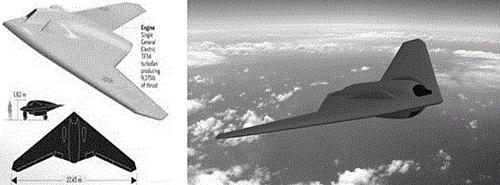
This thesis focuses specifically on **mobile location-based AR games** and **unmanned aerial systems** as representative domains. We selected these because they share intensive reliance on geospatial features and have seen significant adoption and innovation. For AR gaming, our examples center on popular commercial games such as *Pokémon Go*, *Ingress*, and similar apps that integrate real-world mapping and user movement. (This excludes broader AR/VR systems not driven by external location, such as headset-based indoor AR.) For UAVs, we examine consumer and enterprise drones used in civil contexts (recreational quadcopters, photography drones, delivery drones), as well as some military applications for background.

Within these domains, we concentrate on attacks exploiting location technology rather than unrelated drone attacks (e.g. camera hacking unrelated to GPS) or generic mobile malware. In AR gaming, for instance, we emphasize location spoofing, mapping data leaks, or server-side manipulation, not unrelated app vulnerabilities. In UAVs, we emphasize GNSS and radio link attacks, and do not delve deeply into hardware sabotage unless it interfaces with the vehicle’s navigation.

**1.6 Significance of the Study**

As AR games and drones have grown in popularity and capability, their security has become critically important. The **economic scale** is vast: over 100 million monthly users played *Pokémon Go* at its peak, and globally, billions of people now rely on location-based apps. Similarly, the civilian drone industry is expanding rapidly, projections estimate the market will more than triple from 2024 to 2029. These technologies intersect with sensitive domains: for example, mapping of physical sites and automated flights near people or infrastructure, so failures can have serious consequences.

Security research on these topics is also escalating. Recent years have seen dozens of papers and reports on UAV cyber-attacks and spoofing countermeasures. Major incidents have hit the headlines: from demonstration hacks that force drones to land, to the infamous 2011 claim of an RQ-170 Sentinel UAV hijacking via GPS spoofing. On the civilian side, even toy drones have been shown to be easily hijacked using hobbyist gear, raising concerns for both privacy and public safety. Likewise, AR games have drawn scrutiny: security analysts warn that crowdsourced imagery in games can unwittingly reveal military bases or private property.

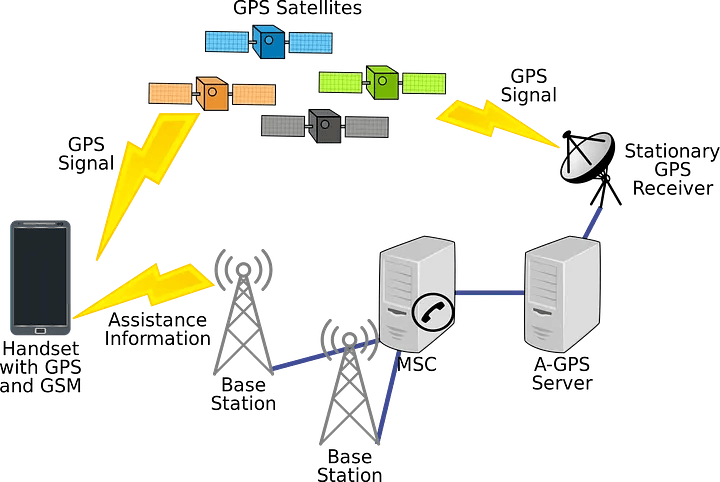


**Fig. 1.** Images of the RQ-170 Sentinel taken from a US Army recognition manual (Source:[**wikipedia**](https://upload.wikimedia.org/wikipedia/commons/thumb/0/09/RQ-170_from_US_Army_recognition_manual.jpg/500px-RQ-170_from_US_Army_recognition_manual.jpg))

This study is significant because it brings together these strands into a unified examination of location-based attacks. Few works have simultaneously addressed the intersection of ubiquitous location signals, game/gaming platforms, and UAV controls. By highlighting vulnerabilities common to both fields (e.g. GPS spoofing affecting drones and location-based apps alike) and those unique to each, we fill a gap in understanding how adversaries exploit physical space in the digital age. The findings will be valuable for security engineers building future AR or UAV systems, for regulators crafting safety standards (like geofencing policies), and for end-users who need to be aware of potential risks. Ultimately, as our society becomes more dependent on positioning services (including emerging 5G/AI-assisted navigation), securing these services against spoofing and privacy violations is paramount.

# **2. Location-Aware Technologies and Applications**

Location-aware systems use sensors and communication methods to determine the geographic position of devices and users. As defined in [5], *“Location-aware technology includes sensors and methods for detecting or calculating the geographical position of a person, a mobile device or other moving objects”*, with common examples being GPS, A‑GPS, Wi‑Fi, and cell-tower triangulation [5].



**Fig. 2.** Typical architecture for location-aware applications showing GNSS satellites, cellular/Wi-Fi positioning and backend servers (source: [Sumit Dev](https://miro.medium.com/v2/resize:fit:720/format:webp/1*xLzOExtqanGvyjAD_dsLdQ.png)).

**2.1 Overview of Location-Aware Technologies**

In practice, modern devices combine multiple techniques (GNSS satellites, inertial sensors, Bluetooth/UWB beacons, etc.) to improve accuracy. Smartphones and wearables (e.g. AR headsets) generally incorporate GPS receivers and motion sensors; for example, Microsoft’s HoloLens 2 includes encrypted storage (BitLocker) and an always-on network firewall as part of its secure design [6]. Similarly, unmanned aerial vehicles (UAVs or “drones”) use GNSS receivers plus IMUs and computer vision to navigate.

In Europe, new GNSS features are enhancing security: for instance, the EU’s Galileo system is rolling out Open Service Navigation Message Authentication (OSNMA) in 2025, which adds a cryptographic signature to satellite signals so receivers can verify they are genuine [7]. This exemplifies the growing emphasis on trusted location data.

**2.2 Mobile Gaming and Drone Applications in Context**

With these capabilities, location-aware technologies have grown in many domains. **Mobile gaming** is a prime example: games like *Pokémon GO*, *Ingress*, or *Harry Potter: Wizards Unite* tie gameplay to real-world movement, using the user’s GPS, camera, and motion sensors to blend digital content with physical space [2][5]. Players wander city streets to “catch” or earn virtual creatures or engage real-world points of interest. Other mobile apps (e.g. fitness games like *Zombies, Run!*) reward outdoor travel via mapped routes. Games may operate entirely online (server-based gameplay and map data) or in **hybrid/offline** modes (some content cached on the device). For example, *Pokémon GO* requires a persistent network connection (to verify location and spawn content), whereas other AR experiences might work offline using local maps. Connectivity mode matters: fully online games can perform server-side cheat detection, whereas offline or hybrid games rely on client-side data and are more susceptible to manipulation.

**Drones** likewise showcase location-aware tech. Consumer drones (DJI, Parrot, Autel, etc.) fuse GPS data, inertial sensors, and computer vision to maintain position, avoid obstacles, and geotag video. They have seen explosive civilian use: commercial drones are now common for aerial photography, surveying, agriculture, search-and-rescue, and even delivery or inspection tasks. As one review notes, modern UAVs are used for “cargo, taxi, agriculture, disaster relief, and risk assessment, or monitoring critical infrastructure” [1]. In Lithuania and globally, hobbyists, businesses, and emergency services deploy drones precisely because of this location tracking and mapping ability. Even advanced concepts like drone swarms rely on accurate location. Thus, location-awareness underpins both popular entertainment (mobile gaming) and emerging tools (consumer UAVs), but it also introduces significant security and privacy challenges as discussed below.

## **2.3 Cybersecurity and Privacy Risks in Location-Aware Systems**

While location-based features enable powerful applications, they also expose new attack surfaces. In general, any system that trusts its geographic data or sensor inputs can be manipulated. We group key risks as follows:

### **2.3.1 GPS and Location Spoofing**

Location spoofing occurs when an attacker falsifies a device’s reported position. A common method is **GPS spoofing**: broadcasting counterfeit satellite signals so that a receiver calculates a wrong location or time. Civil GPS signals lack encryption, so off-the-shelf radios and software can be used to jam or spoof them. Researchers have long warned that civilian drones, cars, and phones are vulnerable to such attacks [1]. For example, one review describes how spoofing can cause a drone to stray off course or crash, bypassing its geofencing and potentially “land in the hands of smugglers.   
In a United States DHS experiment (“Project GYPSY”), GPS spoofing was used to trick a mini-drone (Hornet) into thinking it was somewhere else, and Iran later claimed it commandeered a U.S. RQ-170 stealth drone via fake satellite signals [1]. Even smartphone games are affected: *Pokémon GO* and similar apps rely on GPS, so players often use software or hardware hacks to report fake locations. While Niantic’s developers have worked on anti-cheat measures (see Section 2.4), spoofing remains a cheap and pervasive trick. In summary, without cryptographic authentication (as Galileo’s OSNMA aims to provide [7]), GPS-based systems can be deceived, posing a real security threat to both drones and location-based apps [1].



**Fig. 3.** FLIR Black Hornet 3

Beyond true GPS, software-level **location spoofing** can occur on smartphones by tampering with APIs or developer settings. For example, on Android a malicious app can enable mock locations or hook the location APIs to feed bogus coordinates. Security firms note that “location spoofing in mobile games and other location-based services…should not be merely interpreted as fake data but taken seriously as real human geographic data in new spatial assemblages” [8].

In practice, advanced cheats may run the game in an emulator and script movement, or use Faraday cages with internal GPS transmitters. Defenses against spoofing vary: some apps perform server-side sanity checks (e.g. flagging impossibly fast movement), while others use network triangulation as a cross-check. However, there is no universal solution yet, and location spoofing remains a persistent and evolving threat.

### **2.3.2 Tracking and Location Surveillance**

Location-aware systems can betray user privacy even without overt tampering. **Location surveillance** refers to legitimate or unauthorized tracking of users’ movements by apps, carriers, or governments. Modern smartphones log a torrent of geodata: a New York Times analysis showed that aggregated location “pings” from phones could map individuals’ daily routines (commutes, errands, etc.) with startling clarity [9]. Many consumer apps quietly harvest location: for instance, a U.S. lawsuit accused a popular weather app of tracking users “second by second” and selling that data to advertisers, all hidden in dense privacy policies. The prevalence of sensors means companies (and potentially foreign entities) can build detailed profiles of where people live, work, or congregate. In response, data protection laws treat location as sensitive personal data. The EU’s GDPR explicitly requires **opt‑in consent for location tracking**, viewing it as identifiable personal information. (Similarly, California’s CCPA grants consumers the right to opt out of location data sales.) Despite regulations, enforcement is challenging. Cellular carriers, for example, promised to stop selling location data in 2018 but continued to be fined for leaks.

Public surveillance programs have also leveraged location. During the COVID‑19 pandemic, many governments launched apps to trace contacts via GPS or Bluetooth. While some curtailed outbreaks, security experts warn that most early tracing apps were poorly secured: a study found the vast majority were easy for hackers to breach [9]. One privacy watchdog noted that Norway even banned its official tracking app for collecting excessive data. Beyond pandemics, sensitive use cases abound: leaked “Fitness Tracker” data once allowed researchers to map secret U.S. military bases, and today terrorist or authoritarian governments may try to use location data to monitor or target individuals [10]. In short, any always-on location service risks becoming a surveillance tool. Mitigations (privacy by design, minimal data collection, user transparency) are recommended by experts [9] [10], but gaps remain in user awareness and app practices.

### **2.3.3 Game Cheating and Exploits**

Location-based games are vulnerable to novel cheating and hacking. Beyond GPS spoofing (covered above), attackers can exploit software flaws and user behavior. For example, bots and scripts can automate gameplay in *Pokémon GO* by faking location jumps or simulating screen taps. Niantic has invested heavily in anti-cheat measures (device fingerprinting, behavioral analysis, emulator detection) because *Pokémon GO* “became the poster child for location cheats,” with years of “anti-cheat arms race” against persistent cheat rings according to [8]. Security observers note that some online groups even offer “remote raids” in exotic places - all from players’ couches.

Risks extend beyond fairness. Altered game data can have privacy impacts: spoofing apps may require disabling security (root/jailbreak), exposing phones to malware. In fact, soon after *Pokémon GO*’s 2016 launch, attackers distributed malicious clones of the app: one trojanized version contained the “DroidJack” RAT that could grant full remote control of the victim’s Android device [11]. Even official apps have had issues. Bitdefender reported that early on, *Pokémon GO* for iOS mistakenly requested full Google account access – a bug Niantic quickly patched. Security experts therefore warn players: only install games from official stores and review permissions carefully [11].

More broadly, the “dark art” of location hacks is well-known in the security community. Companies that depend on accurate geodata (ride-hailing, delivery, finance) face concrete scams: organized groups in Brazil used GPS spoofing plus stolen IDs to claim food or taxi jobs miles away [8]. Even if not publicized, any platform that relies on “where you are” must contend with these cheats. Academics emphasize that spoofed location data should be regarded as legitimate user input (not dismissed as noise) in analyses, complicating trust models.  
In summary, location-game cheating encompasses a spectrum of hacks – from simple mock-location flags to sophisticated signal jamming – and remains an active area of concern for developers [8].

### **2.3.4 Unauthorized Data Collection and Third-Party Tracking**

Many location-aware apps include hidden data collection that users do not anticipate. Third-party libraries and analytics SDKs (e.g. ads, social media trackers) embedded in games or utility apps often harvest location and share it widely. In recent years, high-profile incidents have surfaced: for example, a 2022 breach of Gravy Analytics revealed that over 1,000 apps (travel, social, lifestyle) were clandestinely sending fine-grained location data to data brokers [10]. Among the affected apps were Flightradar24, Tinder, and even Muslim prayer apps, illustrating how even “niche” software can leak personal movements. Another study found that the AccuWeather app was persistently transmitting users’ GPS coordinates to an advertising firm, even when the user believed location sharing was off. Advertisers like X-Mode Social have been caught serving location-based tracking SDKs: the U.S Federal Trade Commission (FTC) in 2024 fined X-Mode for sending data about users’ visits to sensitive sites (family planning clinics, places of worship, etc.) to its clients [10].

These cases highlight how location metadata can be sold or combined into surveillance networks. As one industry article warns, installing any app with location permissions and ad SDKs can give unknown data brokers a “mass surveillance” view of a user’s movements. Consumers rarely read privacy policies, so many are unaware that games and utilities might expose their travel patterns to unknown parties. Mitigations include opt‑out laws (CCPA/GDPR), stricter app vetting, and on-device privacy tools (blocking trackers). But currently, the ecosystem is reactive: researchers continue discovering leaks, and regulators sometimes respond (as with the X-Mode case). Overall, unauthorized collection of location data remains a widespread and evolving threat.

### **2.3.5 Drone Hijacking and Control Takeover**

Drones introduce additional threat vectors tied to their wireless control and autonomy. Beyond GPS spoofing, attackers can exploit the drone’s communication link or firmware. A seminal demonstration was **Maldrone** (2015): researchers created a Linux backdoor for the Parrot AR Drone quadcopter. By infecting the drone’s ARM processor, the malware could kill the autopilot and accept reverse-TCP commands, giving the attacker full remote control of the drone’s cameras and sensors [12]. This proof-of-concept showed that even “off-the-shelf” hobby drones can be turned into bots.

More recently, academic and industry teams have reverse-engineered consumer drones. For example, in 2015 security researchers took advantage of a Parrot drone’s open Telnet and Wi-Fi port to gain root access. In one demo at DEFCON, an attacker connected to a Parrot A.R.Drone and forcefully crashed it by killing its flight-control processes [13]. These flaws were not bugs in application code but poor deployment choices (e.g. hardcoded passwords, unencrypted channels). A 2023 academic study similarly found vulnerabilities in DJI’s Enhanced Wi‑Fi protocol. By intercepting the Wi-Fi packets of a DJI Mini SE, researchers were able to send forged commands and hijack the drone mid-flight [14]. In that case the only tools needed were a standard Wi-Fi router and the researchers’ code.

In practice, such remote hijacking has serious implications. Attackers could, for example, intercept and reroute a delivery drone, crash it, or use it to spray chemicals. Even without active hacking, denial-of-service attacks (jamming the control frequency) can make a drone drop from the sky. Given these vulnerabilities, some military and law-enforcement drone programs avoid civilian platforms entirely. However, the consumer market continues to dominate civilian UAVs. As a result, current drones often lack cryptographic protections on their control links, making hijacking “just as easy as hacking any other wireless device,” as one report bluntly notes.

## **2.4 Case Studies of Impacted Platforms**

To ground the above concepts, we consider specific popular platforms where location-aware security issues have emerged.

#### **2.4.1 Pokémon GO**

Niantic’s *Pokémon GO* (2016) was the first truly global location-based AR game, and it exemplifies both the promise and perils of such applications. At its peak, over 100 million people played *GO* each month. The game maps digital monsters onto GPS coordinates, requiring players to physically travel to real landmarks. This meant *GO* collected an enormous trove of location and camera data. Tech analysts have noted that players’ aggregated movement patterns (where and how people travel) become sensitive geospatial intelligence. Indeed, U.S. Marines issued caution to personnel not to reveal unit locations by gaming, and even international incidents occurred (e.g. one oil company’s exercise forcefully reminded attendees not to locate *Pokémon* in secure areas) [2].



**Fig. 4.** Geo-Data is used for some core features of Pokemon Go

Behind the scenes, Niantic has been building what it calls the “Scanverse” – a 3D map of the world derived from images that players collect by taking in-game photos. As of 2024, Niantic reported gathering over a million new environment “scans” per week. While this crowdsourced mapping can improve AR accuracy, it also raises privacy questions: players might inadvertently capture private interiors or sensitive facilities, similar to how users of fitness trackers once mapped military bases. Niantic claims scans are used only for game-related vision processing, but the sheer scale of data means long-term potential for misuse or leakage remains a concern. In fact, when Niantic sold the game to a company owned by the Saudi sovereign fund (2025), commentators immediately questioned how user data might be handled by a foreign authority with a history of surveillance [2].

On the security front, *Pokémon GO* has seen concrete issues. In 2016, just weeks after launch, analysts found rogue APKs of the game containing a known Android RAT (“Droidjack”) that could steal GPS data and other information. Players also discovered that the initial iOS login flow requested full Google account access - a bug Niantic quickly patched after it became public. These incidents underscore that location-based games must manage not only their own data collection, but also defend against malicious clones and permission abuse [11].

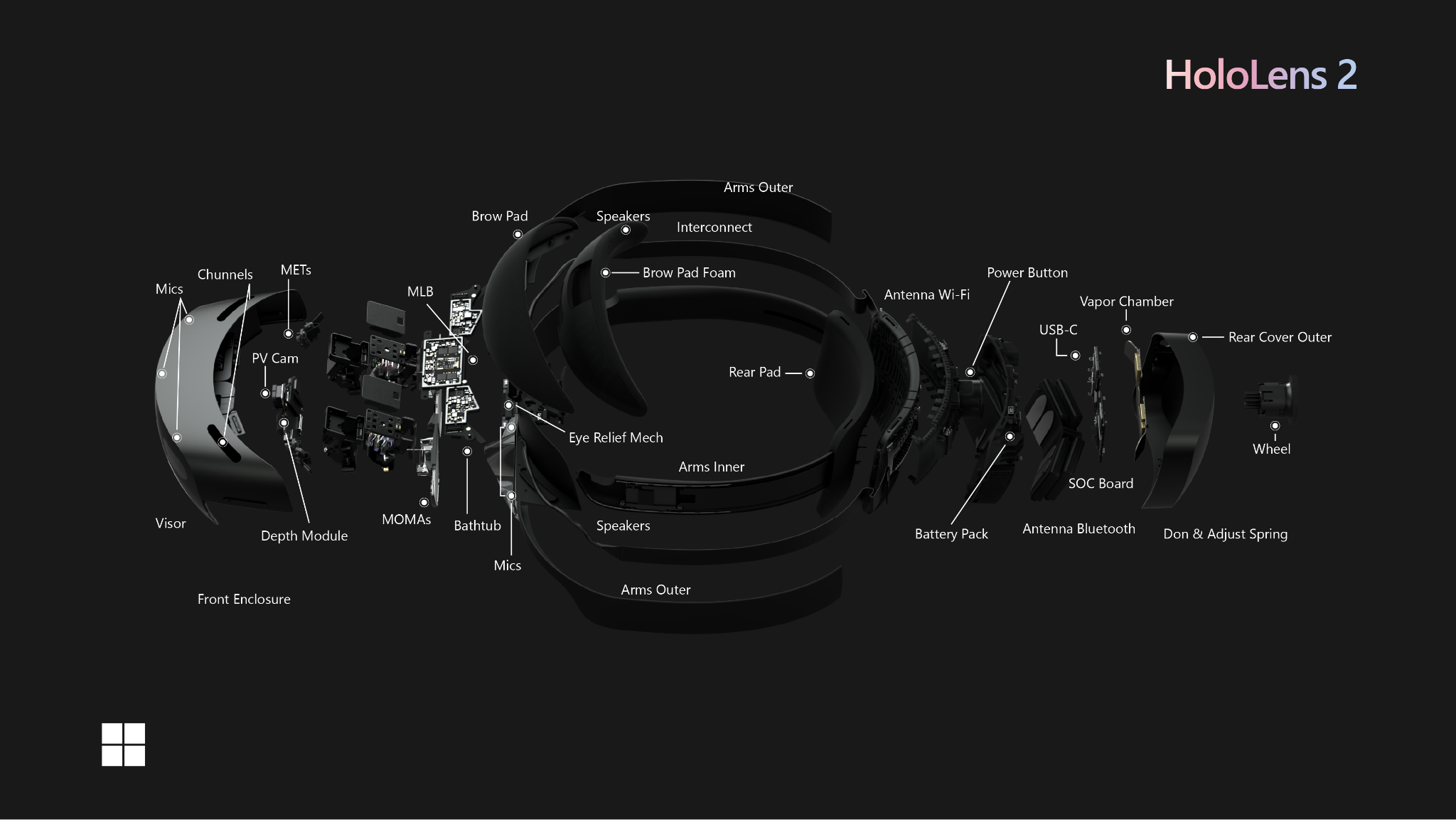
Gameplay itself introduced new risks. Distracted players wandered into dangerous situations: there were reports of thefts and accidents involving game players, from bumping into traffic to trespassing on private property. While not a cyberattack per se, such real-world hazards highlight how integrating location into gaming blurs digital and physical risk.

Finally, cheat prevention has been an arms race. As discussed, Niantic implemented multiple layers of anti-spoofing (server checks, device attestation). Industry commentators note that *Pokémon GO* became the “poster child” for location-game cheats, with long-running efforts to both cheat and detect them. While details of the anti-cheat algorithms are proprietary, security blogs cite Niantic’s own statements that it spent over a year on defenses after *GO*’s release [8]. In practice, cheat communities adapt quickly: new spoofing apps, joystick controllers, and even hardware gadgets continually emerge. Thus, *Pokémon GO* remains a case study of how massive location-based apps must constantly update their security posture.

#### 

#### **2.4.2 Augmented-Reality Glasses (HoloLens, Magic Leap, etc.)**

#### Wearable AR headsets extend location-awareness into the user’s field of view. Devices like Microsoft’s HoloLens or the (now less-visible) Magic Leap One use GPS, IMUs, cameras, and spatial mapping to overlay digital content on the real world. This technology offers powerful enterprise and consumer applications (from navigation aids to immersive gaming), but also severe privacy pitfalls. AR glasses continuously capture video of the environment and bystanders, along with telemetry like gaze direction or heart rate. Researchers have warned that such rich data – eye movements, facial scans, environmental images – can easily reveal sensitive information (users’ health, identity, social graphs) and violate bystanders’ privacy. Indeed, early AR pioneers like Google Glass faced social backlash and bans in public spaces largely due to these concerns [15].



**Fig. 5.** Exploded view of the Hololens 2 to show its components

From a security standpoint, headsets run complex software on powerful chips (for instance, HoloLens 2 is essentially a mobile Windows PC). Manufacturers implement enterprise-grade protections: for example, HoloLens 2 devices have hardware-encrypted storage and always-on firewall as part of their Trusted Computing Base [6]. However, vulnerabilities can and do surface. In July 2017, Microsoft patched a critical bug (CVE-2017-8584) in HoloLens firmware that allowed remote code execution via specially crafted Wi‑Fi packets [16]. Exploiting that flaw would let an attacker take over a headset completely (installing apps, deleting data, etc.). This incident highlights that even cutting-edge AR hardware can be compromised by network-level attacks.

Other risks of AR glasses include social engineering and sensor attacks. A recent insurance-industry write-up enumerates threats like credential theft (stealing network cookies from the headset’s connected smartphone), phishing via deceptive AR content, and denial-of-service attacks on real-time video feeds [17]. As AR devices gain features like eye-tracking (e.g. Meta’s Quest 2) or biometric authentication, the risk of stealing unique biometric profiles increases. In summary, AR glasses (from HoloLens to Magic Leap to upcoming devices like Apple Vision Pro) magnify location-aware concerns: they are rich sensing platforms connected to the cloud, and any flaw in their connectivity or software can expose a trove of sensitive personal and location data [15][16].

#### **2.4.3 Consumer Drones (DJI, Parrot, etc.)**

Civilian drones have become synonymous with GPS-based autonomy, but their vulnerabilities have also been widely publicized. DJI (China) and Parrot (France) dominate the consumer market, selling drones with HD cameras, GPS geofencing, and smartphone apps for control. These platforms illustrate earlier points: they constantly track location and video, and connect wirelessly.

Security researchers have repeatedly found that many such drones trust insecure links. For example, in 2015 a hacking demonstration at DEF CON showed that a Parrot AR.Drone could be easily crashed by exploiting an open Telnet service on its Wi‑Fi module [13]. In that lab test, an attacker gained root on the drone and “killed the processes controlling flight,” causing the drone to drop safely to the ground. Similarly, the “Maldrone” backdoor mentioned above demonstrated that an infected Parrot drone could be completely hijacked, with the malware persisting across reboots [12].

Even DJI products have not been immune. A recent academic paper reverse-engineered DJI’s proprietary Wi-Fi protocol and executed a proof-of-concept hijack on a DJI Mini SE drone. Using only a standard router and custom software, the researchers intercepted and spoofed the control packets, effectively taking control of the drone. The authors stress that their attack required no physical access to the drone or unusual hardware – any moderately-skilled attacker could replicate it. This echoes earlier reports (e.g. Matthew Green’s 2018 talk) that DJI’s Wi‑Fi links were poorly protected. Notably, these findings come even after years of DJI providing “developer kits” and some security guidance; apparently many control channels remain unencrypted or unauthenticated.

Beyond wireless hacking, drones can also be **physically intercepted** via GPS spoofing (as in 2.3.1). Civilian GNSS spoofers (sold online) can mislead drones; once a drone’s autopilot is off-course, an attacker could pick it up or crash it. Indeed, government bodies take such threats seriously. A U.S. DHS exercise and other events (like the mysterious RQ-170 incident) show that drones can be lured or captured with spoofed signals.

Data privacy is another aspect. Some countries are wary of drones transmitting encrypted telemetry to foreign servers. In fact, the U.S. barred federal agencies from using most DJI drones (due to “backdoors” concerns), prompting DJI to add on-device “Privacy Modes” that disable data links. However, consumer apps on smartphones can still upload flight logs or images to the cloud. Users have reported (and researchers confirmed) that non-volatile memory on drones can store sensitive info that later is synced to developer servers.

In summary, consumer UAVs typify the convergence of location tech and security risk. They rely on location for navigation but often lack the cryptographic hardening expected in aerospace. Reported attacks (Parrot telnet exploits, Maldrone backdoor, DJI Wi-Fi hijack) demonstrate that a motivated adversary can seize control. Manufacturers have taken some steps (like DJI’s enhanced encryption on some high-end models, or FIPS-certified chips in certain military drones), but for mass-market devices these protections are often optional.

## **2.5 Summary of Literature Gaps**

Our review shows a rich set of findings across location-aware domains, but also clear gaps. Much existing literature isolates specific threats (e.g. GPS spoofing papers, app-privacy audits, drone pentests) without integrating them into a unified view. For example, academic work on location privacy often focuses on anonymization techniques (k-anonymity, LPPMs) in service data, whereas cybersecurity research emphasizes low-level exploits (spoofers, malware). There is surprisingly little on the intersection: how can we design location-based games or AR experiences that are resilient to both privacy leaks **and** spoofing attacks simultaneously? Similarly, most smartphone app studies analyze trackers in generic apps, but few examine location-tracking in context of gaming or AR specifically.

Another gap is contextual sensitivity. We found scant research on how location-risk varies by region or use-case. For instance, while the EU's GDPR acknowledges location as personal data, there is little region-specific study of how Baltic or Lithuanian users perceive and mitigate these risks. Likewise, case studies abound on *Pokémon GO* and major drones, but smaller or local platforms (e.g. Lithuanian AR startups, local UAV regulations) are underrepresented.

On the technology front, new defenses are emerging but largely untested in consumer markets. Europe’s Galileo OSNMA signal authentication is a major advance against spoofing, but few civilian receivers (smartphones or drones) have firmware that uses it yet. Likewise, we noted industry efforts to build quantum-resistant security into drones: for example, SEALSQ (a Swiss quantum-security company) is embedding post-quantum algorithms into secure chips for professional drones. Academic proposals (like the DroneCrypt IFF system using lattice-based cryptography [19]) show what might be possible. However, there is little literature on evaluating these approaches in practice or extending them to consumer devices. Notably absent are discussions of quantum-safe methods for location data in mobile apps or AR glasses, even though these will ultimately face the same threats to GPS integrity and encryption.

In summary, while the reviewed work provides a solid foundation of known attacks and concerns, there is a lack of holistic, up-to-date analysis on securing location-aware ecosystems end-to-end. Emerging solutions (GNSS authentication, post-quantum crypto) are just becoming available, and their real-world adoption and limitations are not yet well documented. Moreover, the rapid pace of innovation (e.g. new AR devices, drone swarm networks) continues to outstrip formal study. These gaps point to the need for further research into frameworks that combine privacy and security, evaluations of next-generation defenses, and region-specific studies to inform both policy and practice.

## **REFERENCES**

1. Khan, S. Z., Mohsin, M., & Iqbal, W. (2021). “On GPS spoofing of aerial platforms: a review of threats, challenges …,” *PubMed Central (PMC8114815)*, [Online]. Available: [https://pmc.ncbi.nlm.nih.gov/articles/PMC8114815/](https://pmc.ncbi.nlm.nih.gov/articles/PMC8114815/?utm_source=chatgpt.com).
2. Bradshaw, S., & Jackson, D. (2025).“Gotta Track’em All: Data Privacy and Saudi Arabia’s Pokémon Go Acquisition,” *TechPolicy.Press*, [Online]. Available: [https://www.techpolicy.press/gotta-trackem-all-data-privacy-and-saudi-arabias-pokmon-go-acquisition/](https://www.techpolicy.press/gotta-trackem-all-data-privacy-and-saudi-arabias-pokmon-go-acquisition/?utm_source=chatgpt.com). Accessed: 30-july-2025.
3. Marine Corps Base Quantico, “Pokémon Go: Full account access places you and security at risk,” *Quantico Marines — News*, [Online]. Available: [https://www.quantico.marines.mil/News/News-Article-Display/Article/836788/pokmon-go-full-account-access-places-you-and-security-at-risk/](https://www.quantico.marines.mil/News/News-Article-Display/Article/836788/pokmon-go-full-account-access-places-you-and-security-at-risk/?utm_source=chatgpt.com). Accessed: 1-aug-2025.
4. Kaspersky, “Drones and security — What you need to know,” *Kaspersky Resource Center*, [Online]. Available: [https://usa.kaspersky.com/resource-center/threats/can-drones-be-hacked](https://usa.kaspersky.com/resource-center/threats/can-drones-be-hacked?utm_source=chatgpt.com). Accessed: 31-july-2025.
5. Gartner, “Definition of Location-aware Technology,” *Gartner Information Technology Glossary*, [Online]. Available: [https://www.gartner.com/en/information-technology/glossary/location-aware-technology](https://www.gartner.com/en/information-technology/glossary/location-aware-technology?utm_source=chatgpt.com). Accessed: 23-Sep-2025.Accessed: 1-Sep-2025.
6. Microsoft, “HoloLens 2 privacy and data protection,” *Microsoft Learn*, [Online]. Available: [https://learn.microsoft.com/en-us/hololens/hololens2-privacy](https://learn.microsoft.com/en-us/hololens/hololens2-privacy?utm_source=chatgpt.com). Accessed: 1-Sep-2025.
7. European Commission, “Galileo leads the way in GNSS spoofing protection with OSNMA,” *Defence, Industry & Space — European Commission*, 22-July-2025, [Online]. Available: [https://defence-industry-space.ec.europa.eu/galileo-leads-way-gnss-spoofing-protection-osnma-2025-07-22\_en](https://defence-industry-space.ec.europa.eu/galileo-leads-way-gnss-spoofing-protection-osnma-2025-07-22_en?utm_source=chatgpt.com). Accessed: 1-Sep-2025.
8. Guardsquare, “Protect against geo-spoofing in mobile apps,” *Guardsquare Blog*, [Online]. Available: [https://www.guardsquare.com/blog/securing-location-trust-to-prevent-geo-spoofing](https://www.guardsquare.com/blog/securing-location-trust-to-prevent-geo-spoofing?utm_source=chatgpt.com). Accessed: 10-Sep-2025.
9. EY, “How location tracking is raising the stakes on privacy protection,” *EY Forensic & Integrity Services (MENA)*, [Online]. Available: [https://www.ey.com/en\_bh/insights/forensic-integrity-services/how-location-tracking-is-raising-the-stakes-on-privacy-protection](https://www.ey.com/en_bh/insights/forensic-integrity-services/how-location-tracking-is-raising-the-stakes-on-privacy-protection?utm_source=chatgpt.com). Accessed: 11-Sep-2025.
10. NowSecure, “How mobile app location tracking puts executives and enterprises at risk,” 12-Feb-2025, *NowSecure Blog*, [Online]. Available: [https://www.nowsecure.com/blog/2025/02/12/how-mobile-app-location-tracking-puts-executives-and-enterprises-at-risk](https://www.nowsecure.com/blog/2025/02/12/how-mobile-app-location-tracking-puts-executives-and-enterprises-at-risk?utm_source=chatgpt.com). Accessed: 11-Sep-2025.
11. Bitdefender, “Pokémon Go: privacy and security concerns you should be aware of,” *Bitdefender — Hot for Security*, [Online]. Available: [https://www.bitdefender.com/en-us/blog/hotforsecurity/pokemon-go-privacy-and-security-concerns-you-should-be-aware-of](https://www.bitdefender.com/en-us/blog/hotforsecurity/pokemon-go-privacy-and-security-concerns-you-should-be-aware-of?utm_source=chatgpt.com). Accessed: 11-Sep-2025.
12. The Hacker News, “MalDrone — First Ever Backdoor Malware for Drones,” *The Hacker News*, Jan. 2015, [Online]. Available: [https://thehackernews.com/2015/01/MalDrone-backdoor-drone-malware.html](https://thehackernews.com/2015/01/MalDrone-backdoor-drone-malware.html?utm_source=chatgpt.com). Accessed: 23-Sep-2025
13. SoylentNews, “Security researcher demonstrates how Parrot drones are easily taken down or hijacked,” *SoylentNews*, [Online]. Available: [https://soylentnews.org/article.pl?sid=15/08/16/038222](https://soylentnews.org/article.pl?sid=15%2F08%2F16%2F038222&utm_source=chatgpt.com). Accessed: 17-Sep-2025.
14. D. Pratama et al. “Behind The Wings: The Case of Reverse Engineering and Drone Hijacking in DJI Enhanced Wi-Fi Protocol,” *arXiv preprint arXiv:2309.05913*, Sep. 2023, [Online]. Available:<https://arxiv.org/abs/2309.05913>. Accessed: 18-Sep-2025.
15. L. Bauer et al., “Speculative Privacy Concerns About AR Glasses Data Collection,” (PDF), *CMU — PETS 2023 paper*, 2023, [Online]. Available: [https://users.ece.cmu.edu/~lbauer/papers/2023/pets2023-ar-glasses.pdf](https://users.ece.cmu.edu/~lbauer/papers/2023/pets2023-ar-glasses.pdf?utm_source=chatgpt.com). Accessed: 18-Sep-2025.
16. The Register, “It’s July 2017 – and your expensive HoloLens can be pwned over Wi-Fi,” *The Register*, 11-Jul-2017, [Online]. Available: [https://www.theregister.com/2017/07/11/microsoft\_july\_patch\_tuesday](https://www.theregister.com/2017/07/11/microsoft_july_patch_tuesday?utm_source=chatgpt.com). Accessed: 18-Sep-2025.
17. BOXX Insurance, “AR & VR Headsets: Endless Possibilities or the End of Privacy,” *BOXX Insurance Resources*, [Online]. Available: [https://boxxinsurance.com/us/en/resources/ar-vr-headsets-endless-possibilities-or-the-end-of-privacy](https://boxxinsurance.com/us/en/resources/ar-vr-headsets-endless-possibilities-or-the-end-of-privacy?utm_source=chatgpt.com). Accessed: 19-Sep-2025.
18. SEALSQ, “SEALSQ advances post-quantum cybersecurity for defense and public safety drones,” *SEALSQ News Releases*, [Online]. Available: [https://www.sealsq.com/investors/news-releases/sealsq-advances-post-quantum-cybersecurity-for-defense-and-public-safety-drones](https://www.sealsq.com/investors/news-releases/sealsq-advances-post-quantum-cybersecurity-for-defense-and-public-safety-drones?utm_source=chatgpt.com). Accessed: 20-Sep-2025.
19. Decent Cybersecurity, “Quantum-Resistant Cryptography in Drone Identification,” *Decent Cybersecurity*, [Online]. Available: [https://decentcybersecurity.eu/quantum-resistant-cryptography-in-drone-identification](https://decentcybersecurity.eu/quantum-resistant-cryptography-in-drone-identification?utm_source=chatgpt.com). Accessed: 23-Sep-2025. Accessed: 22-Sep-2025.