Smart indoor evacuation using real-time beacons

Oleksandr Muzychuk[1,†], Victoria Vysotska[1,2,†], Viktor Vasylenko[1,†], Mykhailo Tsuranov[1,*,†], Heorhii Zemlianko[1,†], Inna Khavina[1,†] and Yurii Gnusov[1,†]

[1] *Kharkiv National University of Internal Affairs, L. Landau Avenue 27 61080 Kharkiv, Ukraine*
[2] *Information Systems and Networks Department, Lviv Polytechnic National University, Stepan Bandera Street 12 79013 Lviv, Ukraine*

Abstract

The proliferation of «smart» environments raises the question of the need for accurate and reliable indoor positioning systems (IPS) for critical applications in logistics, health care and security. Traditional technologies, such as GPS and Wi-Fi, demonstrate their inadequacy due to signal attenuation and multibeam propagation in the rooms. This paper provides an in-depth analysis of positioning systems based on mobile beacons, with a focus on Bluetooth Low Energy (BLE) and Ultra-Wideband (UWB) technologies, as well as assessing their resistance to cyber attacks. The study systematizes key technologies, breaking down in detail the trade-offs between economical and scalable BLE and UWB centimeter accuracy. The solution is a hybrid deployment model that uses artificial intelligence (AI) to compensate for signal and adapt to dynamic changes in the environment. The vulnerability analysis reveals serious threats to unencrypted beacon protocols, including spoofing, signal cloning and denial of service (DoS) attacks. To counter these risks, a comprehensive cyber protection model is proposed. It includes functions such as dynamically changing identifiers, the use of AI to detect anomalies and the integration of cyber-physical systems (CPS) with digital doubles for proactive monitoring and simulation of attacks. The effectiveness of the proposed system was tested under a pilot evacuation scenario. The results show that the use of a special pre-configured mobile application in conjunction with the beacon infrastructure reduces the evacuation time for people unfamiliar with the building's layout by 30% and for people who know the building's internal structure efficiency 8%. This confirms the practical relevance of the system for improving safety of life in emergency situations.

Keywords

indoor positioning system (IPS); Bluetooth low energy (BLE); ultra-wideband (UWB); cybersecurity; emergency evacuation; anomaly detection; autonomous navigation

1. Introduction

The modern world is undergoing a rapid transformation toward "smart" environments, where accurate and reliable positioning of objects, assets, and people is becoming a critically important element of infrastructure. While in the past "smart" referred primarily to household appliances, in the modern world, entire cities are becoming smart. The concept of "smart" cities, university campuses, industrial enterprises, and medical institutions is based on the systems' ability to collect and analyze real-time data, which is unachievable without precise spatial referencing and stable connectivity among smart system components [1].

In the field of logistics and industry, the need for positioning manifests in asset management, work process control, and inventory optimization. The application of mobile sensors allows for tracking the location of costly equipment, tools, and inventory, preventing their loss or misuse. This contributes to increasing operational efficiency and reducing capital and operating

AISSLE-2025: International Workshop on Applied Intelligent Security Systems in Law Enforcement, October, 30–31, 2025, Vinnytsia, Ukraine
* Corresponding author.
† These authors contributed equally.
o.muzychuk23@gmail.com (O. Muzychuk); victoria.a.vysotska@lpnu.ua (V. Vysotska); Vasylenko_Viktor@ukr.net (V. Vasylenko); kaf-kdt@univd.edu.ua (M. Tsuranov); manfred.jeusfeld@acm.org (H. Zemlianko); t.princesales@utwente.nl (I. Khavina); manfred.jeusfeld@acm.org (M. Jeusfeld)
0000-0001-8367-2504 (O. Muzychuk); 0000-0001-6417-3689 (V. Vysotska); 0000-0002-9313-861X (V. Vasylenko) 0000-0002-2115-7029 (M. Tsuranov); 0000-0003-4153-7608 (H. Zemlianko) 0000-0002-1856-1186 (I. Khavina); 0000-0002-9017-9635 (M. Jeusfeld)

expenditures (CAPEX and OPEX) [2]. Similar systems are used for condition monitoring of objects, for example, in the food and pharmaceutical industries, where beacons equipped with temperature and humidity sensors ensure compliance with storage conditions [3].

In medicine, positioning technologies are used for tracking personnel, such as doctors and nurses, which allows for a quick response to emergencies. Furthermore, these systems help locate critical equipment (wheelchairs, infusion pumps), thereby improving patient safety and staff operational efficiency [1]. Positioning also plays a key role in ensuring the accessibility of the urban environment for people with disabilities, guiding them to exits, elevators, or safe zones using acoustic and light beacons [4].

For educational institutions, beacon-based systems create "smart campuses," providing interactive navigation, automating the process of attendance tracking, and enabling targeted distribution of educational materials and emergency alerts [5]. These technologies allow for process optimization, reduction of administrative costs, and enhancement of student and faculty safety in emergencies by quickly determining the location of every individual [5].

Society has become accustomed to relying on Global Navigation Satellite Systems (GNSS), which ensure the safety of road transport, container shipping, and even food delivery. However, satellite positioning systems provide virtually no accurate results indoors, nor do they function reliably in combat conditions due to the active use of Electronic Warfare (EW) countermeasures.

The relevance of the topic thus extends beyond a simple technological capability. It is driven by economic and operational feasibility, as automation based on precise positioning allows companies and organizations to minimize labor costs, increase productivity, and ensure a high level of safety, while also enhancing the efficiency of informing and evacuating employees during hostilities and air raids.

The use of beacon technologies is extensive and widespread, but the crisis situation in Ukraine opens up new opportunities for targeted technology in the field of human security.

The goal of this article is to conduct a comprehensive analysis of the current state of technologies and solutions based on mobile beacon sensor infrastructure. The study will present a classification of existing standards and technologies, review their key characteristics and application areas, and perform a comparative analysis of their effectiveness.

A central element of the work will be a detailed analysis of vulnerabilities and threats to such systems, based on which a comprehensive approach to their cyber defense will be proposed, including innovative mechanisms such as the application of cyber-physical systems and digital twins.

The article will also consider the possibility of applying beacon technology for the evacuation of personnel during air raid alerts.

2. Related works

Ensuring accurate and reliable positioning is one of the key tasks in creating intelligent urban environments and infrastructure. Before the advent of beacon technology, classical navigation methods (GPS) or common wireless networks (Wi-Fi) were used, and some organizations tried to adapt infra-red technologies for intra-positional navigation. More advanced industrial enterprises and companies tried to develop their own technologies for navigation inside buildings and offices. However, the shortcomings of the above technologies have led to the emergence of beacons [6].

In this paper we consider the fundamental shortcomings of classical technologies, their limitations: the physical propagation of their signals, which were presented graphically in Figure 1, with a more detailed description. It is also justified to use technologies based on mobile beacons (beacons) as a more promising direction for the organization of navigation in closed spaces and in real time.

The GPS (Global Positioning System), which operates in the decimeter wavelength range, is critically dependent on a direct line of sight to satellites. Its signal is easily attenuated or completely blocked by physical obstacles, such as thick building walls, dense foliage, and even

heavy cloud cover. This renders GPS unsuitable for accurate navigation in "urban canyons," basements, tunnels, and inside buildings, where the signal is reflected or completely lost [7].

Wi-Fi-based positioning also faces a number of fundamental challenges that reduce its accuracy and reliability. The key one is multipath propagation, where radio waves are repeatedly reflected off walls, furniture, and other objects indoors before reaching the receiver. Unlike GPS, where the signal propagates via line of sight, in Wi-Fi environments the measured signal path length is always greater than the actual distance, which introduces significant error into calculations. This is a fundamental obstacle because technologies of IEEE 802.11n/ac standards (MIMO, MRC, BF) deliberately use reflections to enhance throughput, creating a contradiction between optimization for data transmission and for positioning [8].

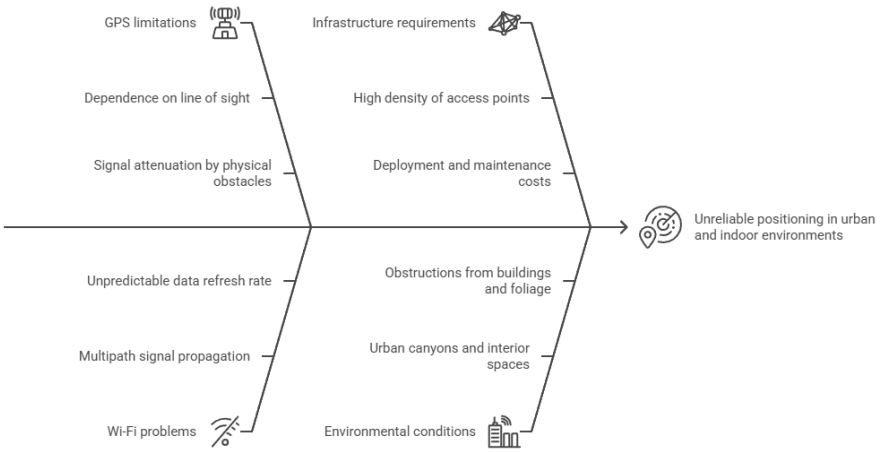

Figure 1: Problems of traditional navigation techniques (author's development).

Furthermore, Wi-Fi positioning is characterized by an unpredictable data update frequency, which can reach tens of seconds or even minutes, rendering the system unreliable for critical applications requiring real-time tracking. Achieving acceptable accuracy (approximately 2–3 meters) necessitates a very high density of access points, which must be distributed in a dense, staggered pattern throughout the entire perimeter, significantly increasing deployment and maintenance costs [8].

To overcome the limitations of traditional navigation systems, technologies based on mobile beacon sensors (beacons) have been actively developed and implemented. These devices are inexpensive, energy-efficient transmitters that utilize short-range technologies, such as Bluetooth Low Energy (BLE), to determine location with accuracy up to several meters in environments where GPS and Wi-Fi prove ineffective [9].

BLE beacons are capable of operating autonomously for extended periods on small batteries, making them ideal for high-density indoor deployment. They can be easily integrated into existing infrastructure or deployed from scratch with minimal capital expenditure. Their ability to provide accurate and reliable indoor positioning opens up new opportunities for a wide range of applications—from navigation and marketing to asset management and security.

The initial configuration process for beacons is quite complex and lengthy, and there is also a need for preliminary setup of user devices. However, if these processes are automated and a training procedure for beacon usage is organized, it could significantly enhance the efficiency of personnel in emergency situations. This is because the technology is capable of providing the most relevant information, not only about an employee's location within a facility but also about their subsequent actions for successful evacuation. Furthermore, the technologies discussed in the article will significantly simplify the work of law enforcement and rescue services personnel in critical situations.

Beacon-based technologies are already successfully applied in various fields, solving specific tasks.

Indoor Navigation and Wayfinding: Beacons assist visitors in navigating large and complex spaces, such as shopping centers, museums, railway stations, and university campuses (Figure 2). In conjunction with mobile applications, they provide interactive maps and step-by-step instructions, making it easy to locate required auditoriums, stores, or emergency exits [5].

Asset Tracking and Logistics: In industry and healthcare, beacons are used for tracking valuable equipment, inventory, and even personnel. Beacons attached to objects allow for real-time determination of their location, which optimizes inventory processes, reduces search time, and helps prevent theft [2]. For example, in hospitals, beacons enable the rapid location of necessary medical equipment, and in schools, they track laptops and laboratory instruments (Figure 2) [5].

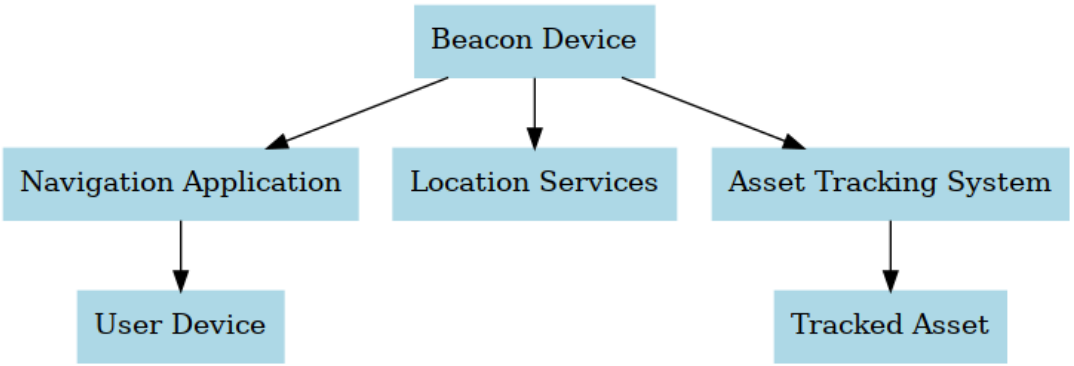

Figure 2: Chart of the sequence of navigation and asset tracking (author's development).

Interactive Marketing and Customer Engagement: In retail environments, beacons are employed for contactless marketing (Figure 3). When a shopper approaches a specific product, the system can send a contextual notification to their smartphone containing product information, a discount, or a special offer. This enables the personalization of the shopping experience, influencing decisions at the "moment of truth," and collecting valuable data on customer behavior [10].

Security Systems: Beacons play a crucial role in ensuring safety and access control. They can be utilized for the automated verification of employee entry into designated areas [5] or for emergency incident notification [9]. In the event of a fire or other emergency, beacons can guide people toward the nearest exits, ensuring rapid and safe evacuation (Figure 3) [7].

Despite their diversity, all these use cases rely on the same fundamental functionality: the system's ability to accurately determine location and initiate an action based on this data. This underscores the versatility of beacon technology as a foundational component for creating context-aware smart environments.

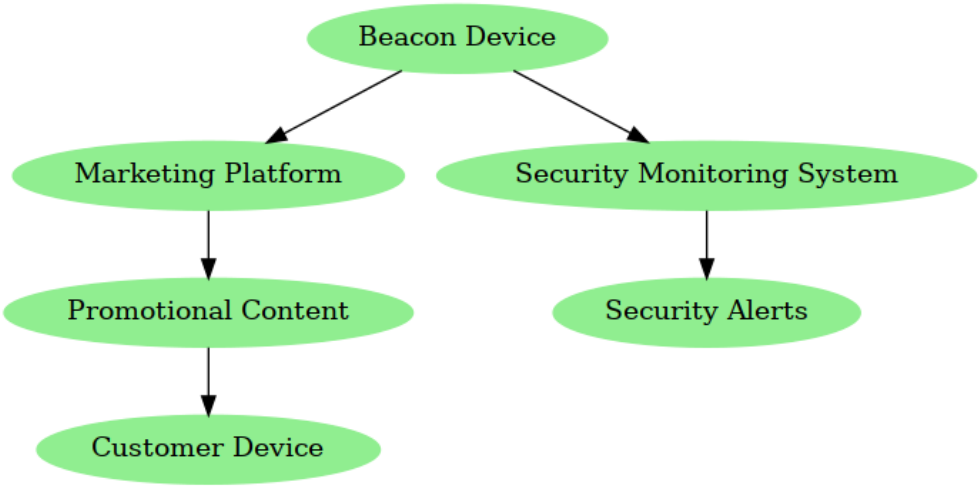

Figure 3: Marketing and security flowchart (author's development).

3. Materials and methods

3.1. Comparative analysis of positioning technologies

The choice of positioning technology is always a trade-off between accuracy, cost, power consumption, and scalability. None of the existing technologies is universally superior for all scenarios. This paper presents a comparative study of key beacon-based positioning technologies (BLE, UWB, Wi-Fi RTT), as well as the modern RFID tag technology [11].

The comparative analysis is presented in a table format, which allows for an objective assessment of the strengths and weaknesses of each technology and determining their applicability in various practical tasks:

1. BLE (Bluetooth Low Energy) technology is characterized by low latency (less than 10 ms) and high energy efficiency, which ensures a long battery life in devices. BLE is supported by most modern smartphones, facilitating its widespread adoption in consumer applications. Scalability is achieved through the use of mesh networks, allowing coverage of large areas and supporting simultaneous interaction of a large number of devices. For security, AES-128 encryption is used. Ease of deployment and integration with IoT platforms make BLE an attractive solution for mass-market scenarios, such as indoor navigation in shopping centers and contextual marketing, where positioning accuracy at the level of 1–3 m is considered sufficient [12]. However, the technology is sensitive to electromagnetic interference and multipath effects, which can reduce operational stability in complex radio environments [13, 14].

Table 1
Comparative analysis of positioning technologies

Parameter	BLE (Bluetooth Low Energy)	UWB (Ultra-Wideband)	Wi-Fi RTT (IEEE 802.11mc/az)	RFID (UHF/Active/Passive)
Positioning Accuracy	1–3 m (up to 1 m with AoA/AoD)	10–30 cm (up to 10 cm ideally)	1–2 m (1.1 m RMSE, 1.5 m 90% quantile)	1–5 m (Zonal, type-dependent)
Operating Range	Up to 100 m (BLE 5.x)	50–100 m (Indoors)	30–50 m (AP dependent)	3–10 m (UHF passive), >100 m (Active)
Update Rate	Variable (up to 10 Hz, mesh up to 100 Hz)	10–200 Hz (Realistically 10–100 Hz)	1–10 Hz (Typically 1–5 Hz)	1–10 Hz (Active), <1 Hz (Passive)
Latency	<10 ms (Connection), <100 ms (Update)	Milliseconds (Low)	100–500 ms per determination	Sub-second (Passive), <100 ms (Active)
Power Consumption	Low (Beacons are inexpensive)	High (Anchors/Tags are expensive)	Low (If Wi-Fi 6 is available)	Low (Passive), Higher (Active/Reader)
Infrastructure Cost	Low (Beacons are inexpensive)	High (Anchors/Tags are expensive)	Low (If Wi-Fi 6 is available)	Low (Passive), Higher (Active/Reader)
Interference Robustness	Low (Sensitive to multipath)	High (Resistant to multipath)	Medium (Environment	Medium (Frequency/Method

			dependent)	dependent)
Ease of Deployment	High (Simple installation)	Complex (Requires calibration)	Medium (AP dependent)	High (Passive), Medium (Active)
Device Compatibility	Very High (Smartphones, IoT)	Growing (Smartphones, IoT, automotive)	High (Android 9+, Wi-Fi 6 AP)	Requires RFID readers
Security	AES-128, ECDH, Regular updates	High (Distance-bounding, Encryption)	WPA2/WPA3, FTM Authentication	Encryption, Authentication, Kill-commands
IoT Integration	Excellent (Mesh, standard profiles)	Excellent (Sensor networks, API)	Excellent (Wi-Fi, API, sensor fusion)	High (Standards, middleware)
Scalability	High (Mesh, thousands of devices)	High (100+ tags/anchors)	Medium (Channel/AP limited)	Very High (Thousands of tags)
Standardization	Bluetooth SIG, ISO/IEC 18305	IEEE 802.15.4z, FiRa, ISO/IEC 18305	IEEE 802.11mc/az, Wi-Fi Alliance	ISO/IEC 18000, 24730, 18305
Applicability	Navigation, Marketing, Healthcare	Industry, AGV, Security	Offices, Smart Buildings, Navigation	Logistics, Warehouse, Inventory
Privacy	Implementation dependent, BLE-privacy	High (Low power, short pulse)	Requires access control, privacy API	Deactivation, Pseudonymization
Throughput	Up to 2 Mbps (BLE 5.x)	High (Wide spectrum)	40/80 MHz (Wi-Fi 5/6)	Low (Passive), Higher (Active)
Infrastructure Requirements	BLE Beacons, Gateways	Anchors, Controllers, Tags	Wi-Fi 6 AP with FTM	RFID Readers, Tags
Tag/Device Power Supply	Months/Years (Battery)	Months (Accumulator), Low power	Mains (AP), Battery (Client)	None (Passive), Battery (Active)
Multipath/NLOS Resistance	Low/Medium	Very High	Medium (Improved by ML/filtering)	Medium (Environment dependent)
Sensor fusion	Yes (IMU, PIR, Ultrasound)	Yes (IMU, other sensors)	Yes (IMU, BLE, UWB)	Yes (Temperature, Humidity, etc.)
Implementation Examples	Shopping centers, Hospitals, Smart homes	Factories, Warehouses, Automotive, Medicine	Offices, Campuses, Airports	Warehouses, Retail, Medicine

2. The Ultra-Wideband (UWB) technology provides high positioning accuracy at the level of 10–30 cm and is characterized by low latency (within milliseconds). A key advantage of UWB is its high resistance to radio interference and multipath propagation, which is due to wideband signal transmission. This technology supports distance-bounding and encryption functions, which increases the security level of localization. In recent years, there has been rapid growth in UWB support in smartphones and Internet of Things (IoT) devices. However, the deployment of UWB systems requires significant capital investments and is accompanied by high infrastructure implementation complexity. Due to these features, UWB is primarily used in industrial and critical scenarios, such as for the navigation of Autonomous Guided Vehicles (AGVs) or the tracking of tools on assembly lines [15–17].
3. Wi-Fi RTT (Round Trip Time) is a technology that implements location determination based on measuring the signal propagation time between a device and Wi-Fi 6 access points supporting FTM (Fine Timing Measurement). Positioning accuracy reaches 1–2 m, and latency is 100–500 ms. The advantages of Wi-Fi RTT include a high degree of compatibility with devices on the Android platform, as well as the possibility of integration with existing IoT systems and support for modern security protocols (WPA2/WPA3). Operational reliability can be reduced due to interference and multipath effects, however, the technology demonstrates moderate resilience to these phenomena. To increase accuracy, calibration is required, aimed at eliminating systematic errors. Due to the low infrastructure costs (where Wi-Fi 6 is already present), Wi-Fi RTT is often used in offices and smart buildings, where optimization of capital expenditure is important [15, 18, 19].
4. Radio Frequency Identification (RFID) technology allows for zonal positioning with an accuracy of 1–5 meters. Passive RFID tags are characterized by an operating range of up to 10 meters, while active tags can reach over 100 meters. The main advantages of RFID include the low cost of passive tags, high scalability, and ease of integration with existing industrial IoT systems. Standardization according to ISO/IEC ensures compatibility between devices from various manufacturers. Privacy concerns are addressed through tag deactivation and the use of data pseudonymization. This technology is effective for tasks involving zonal object tracking, especially in warehouse and production logistics, where the identification of a large quantity of goods or equipment is required [20, 21].

As can be seen from Table 1, UWB technology is the most accurate and promising; however, its power consumption is relatively high, which is critical in emergency situations. Furthermore, the application of UWB technology is constrained because it necessitates the use of modern smartphones, which significantly reduces the effectiveness of the alerting under extreme conditions. Therefore, to ensure maximum user coverage in emergency circumstances, BLE (Bluetooth Low Energy) technology is the optimal choice, as its long market presence ensures maximum coverage of user devices and offers sufficiently low power consumption. It should also be noted that the widespread use of fitness trackers, smartwatches, and wireless headphones encourages users to keep the BLE transmitter constantly activated.

3.2. Conceptual model for deployment and use of lighthouse-based infrastructure

Multi-Layer System Architecture. An effective beacon-based positioning system features a complex multi-layered architecture, where each component performs its unique function.

Physical Layer: this layer comprises the mobile sensor-beacons themselves, which are placed within the physical environment (e.g., on walls, shelves, or equipment). In addition to stationary beacons, this layer also includes wearable devices (tags) attached to assets or personnel to track their movements. The beacons transmit signals with unique identifiers and, in some cases, with sensor data (temperature, humidity) [2].

Network Layer: this layer consists of receivers that capture the beacon signals. The receivers can be either specialized BLE Beacon Gateways or common mobile devices (smartphones, tablets).

These receivers collect data, such as the beacon ID, Received Signal Strength Indicator (RSSI), and reception time, and transmit them to the server layer for further processing [10].

Server Layer: this layer is the "brain" of the entire system. Data received from the receivers is processed centrally at this level. Complex positioning algorithms (e.g., tri-lateration, fingerprinting, or tri-angulation) are executed here to calculate the precise coordinates of the beacons in real time. The server layer is also responsible for database management, historical data storage, analytics, and integration with other information systems [10, 22].

Application Layer: this is the end-user interaction interface. It can be implemented as a mobile application, a web dashboard, or specialized software. At this layer, location data is visualized, and various actions are initiated, such as sending notifications, activating interactive content, or generating analytical reports [5].

Technology Selection and Deployment Strategy (Hybrid Approach). Effective deployment of beacon infrastructure requires not a blind choice of a single technology, but a strategic, hybrid approach that leverages the strengths of each one. For instance, within a single facility, such as a “smart” university campus, the following multi-layered strategy can be applied:

- UWB (Ultra-Wideband) can be used in zones requiring sub-meter accuracy and high reliability: in laboratories for tracking high-value scientific equipment or in areas adjacent to chemical storage for personnel safety assurance [15].
- Wi-Fi RTT (Round Trip Time) is ideally suited for navigating students and faculty within common areas, such as classrooms and libraries, as well as for people flow analytics. Since Wi-Fi infrastructure often already exists in most campuses, this approach provides savings on capital expenditures [15].
- BLE (Bluetooth Low Energy) beacons can be placed at points of interest, such as bookstores, cafes, or information stands. Their low cost and energy efficiency make them ideal for contextual marketing and sending notifications about events, schedules, or promotions, as well as for alerting users about emergency situations and evacuation routes [5].

Thus, instead of relying on a single protocol, the hybrid approach allows for the optimization of performance and costs, ensuring the necessary level of accuracy and reliability for each specific task.

Mitigating Multipath Propagation and Dynamic Interference. Traditional RSSI-based positioning methods are extremely sensitive to multipath propagation and interference. AI offers intelligent approaches to combat these problems.

Human Body “Shadowing” Compensation: One of the main sources of dynamic interference in indoor environments is the human body. Research indicates that an AI model can be trained to recognize the characteristic pattern of simultaneous signal attenuation that occurs across three BLE advertising channels (37, 38, and 39) when a person passes between the beacon and the receiver. Thus, the model can distinguish this "shadowing" from other types of interference and correct the RSSI values, which significantly increases positioning accuracy in dynamic and crowded environments [23].

Filtering and Algorithms: AI enables the optimization of traditional filtering methods. Kalman filters, median filters, and moving averages can be integrated with AI algorithms to stabilize unstable RSSI readings. Instead of merely discarding anomalous values, AI learns to treat interference not as errors, but as a complex, yet recognizable, part of the input data that can be utilized to improve the model [23, 24].

Adaptation to Changes and Device Heterogeneity. Traditional positioning systems require frequent manual recalibration. AI renders these systems autonomous and self-adapting:

1. Self-Adapting Models: AI enables the creation of models that can dynamically adapt to environmental changes (e.g., furniture rearrangement or changes in pedestrian flow) without the necessity of manual recalibration. Machine learning models continuously train

on new data, allowing them to adjust their internal parameters to maintain accuracy. This significantly enhances the reliability and scalability of the system [25].

2. Addressing Device Heterogeneity: Device heterogeneity is a key problem that reduces positioning accuracy. Deep learning-based solutions, for instance, utilizing autoencoders, allow for the creation of "device-agnostic" RSSI (Received Signal Strength Indicator) representations. These models learn to extract the essential characteristics of the signal while ignoring variations caused by the unique features of a specific device. This ensures consistent positioning accuracy regardless of the smartphone model or other device [26].

AI also plays a vital role in optimizing the energy consumption of devices, which is critical for battery-powered beacons and mobile devices.

Intelligent algorithms can analyze the device's state and activity to determine the optimal time for position updates. For example, if a user is in a static position, the scanning frequency can be reduced, saving battery power. This extends the autonomous operating time of beacons and mobile devices, making the solutions more practical and economically beneficial [25].

Optimal beacon placement is a complex task that affects the accuracy, coverage, and cost of the entire system. Traditional methods often lead to inefficient solutions.

The problem of optimal beacon placement belongs to the class of NP-hard problems, making it virtually unsolvable manually. To address it, AI algorithms such as evolutionary algorithms (e.g., OPTILOD), genetic algorithms, or Particle Swarm Optimization (PSO) are applied. These algorithms automatically determine the minimum number of beacons and their best location to achieve maximum coverage and minimize positioning error [27].

AI algorithms optimize several interconnected parameters simultaneously, including the number of beacons, coverage area, and Geometric Dilution of Precision (GDOP). Thus, AI finds a balance between deployment cost (by minimizing the number of beacons) and positioning accuracy, allowing for the achievement of the best results. This differs from the naive approach of "the more beacons, the better," since, after reaching a certain threshold, increasing their number can, conversely, negatively affect accuracy due to increased interference [24, 27].

3.3. Cyber Protection and Security of Beacon-based Positioning Systems

Vulnerabilities and threats to lighthouse-based systems. Despite their advantages, lighthouse-based systems are exposed to a number of serious vulnerabilities, many of which stem from the very nature of their operation – data transmission «in open form» for simplicity and energy efficiency.

1. Signal Interception and Spoofing (Spoofing): since many protocols, such as iBeacon, broadcast their identifiers without encryption, an attacker can easily intercept and record them. The attacker can then create a fake beacon with the same identifier and retransmit the signal, potentially at a different physical location. A user application receiving the fake signal cannot distinguish it from the genuine one, which can lead to user redirection to a malicious site, data compromise, or even financial loss [28]. Another type of attack, “piggybacking”, involves an attacker using the infrastructure of legitimate beacons for their own purposes without the owner’s consent [29]. These vulnerabilities extend to various forms of deception, including spoofing and jamming, which can severely compromise the integrity and availability of positioning services by introducing false signals or disrupting legitimate ones [30, 31]. Furthermore, sophisticated attackers may leverage hardware behavioral fingerprinting techniques to impersonate legitimate devices, thereby circumventing traditional security measures and enabling data exfiltration or privilege escalation within IoT ecosystems [32].
2. Denial of Service (DoS) Attacks: beacon-based systems can be attacked by creating radio interference on the same frequency as BLE, which disrupts the operation of both beacons and receivers. A more sophisticated DoS attack, known as "silencing," involves an attacker using cloned beacons with higher transmitter power to flood the airwaves with fake signals.

This distorts the distance estimation to the real beacon, rendering the positioning system inoperable [29]. Such denial-of-service attacks, especially those involving signal spoofing, present a significant challenge for autonomous systems, akin to GPS spoofing where fake signals manipulate perceived location [33, 34]. This vulnerability extends to broader cyber-physical systems, where the injection of forged commands or the generation of malicious network traffic can impair system functionality and integrity, thereby affecting the availability of critical services [34].

3. Privacy Concerns: beacon systems collect user location data, which raises serious ethical and legal issues. The key problem is that users may feel that their movements are being tracked without their explicit consent [35]. This necessitates system developers to ensure transparency and mandatory consent for data collection. Moreover, the aggregation of such location data, especially when combined with other personal identifiers, raises concerns about mass surveillance and potential misuse by centralized service providers. This highlights a critical need for robust data governance frameworks that prioritize user control over personal information and ensure transparency in data collection and utilization practices [36].
4. Lack of Encryption and Authentication: a fundamental vulnerability is that many beacons do not utilize built-in encryption mechanisms to protect transmitted data [37]. This not only makes them susceptible to spoofing but also allows for the interception of confidential information if it is transmitted via the beacon. The “hijacking” attack, in which an attacker intercepts the password sent for beacon configuration and changes it, completely deprives the legitimate owner of control over the device [37]. The vulnerability is also evident in the possibility of “over-the-air” reprogramming of beacons without proper authentication, which can lead to DoS attacks or content substitution [29]. These vulnerabilities are exacerbated in cloud-based SCADA systems, where the public cloud environment introduces additional threats such as distributed denial-of-service and man-in-the-middle attacks, further compromising data integrity and system availability. Consequently, unauthorized access to sensitive data and improper access control mechanisms represent critical attack vectors that can lead to severe operational disruptions and privacy breaches within these interconnected environments [38].

Existing threats are not merely isolated hacking incidents, but fundamental risks inherent to the technology itself, as the simplicity and low cost that make beacons attractive are also the source of their vulnerability. With the increasing complexity and interconnectedness of hybrid positioning systems, cybersecurity risks also escalate. Beacon devices, especially BLE (Bluetooth Low Energy), are vulnerable to various attacks. A spoofing attack involves faking the beacon’s identifier, which can lead to providing false information or redirecting the user to malicious resources. Other threats include cloning (copying identifiers) and jamming—signal suppression that can cause a Denial of Service (DoS) [28]. Furthermore, side-channel attacks, which exploit information leakage from the physical implementation of beacon devices, pose a significant threat, enabling the extraction of sensitive data like cryptographic keys through analysis of power consumption, electromagnetic emanations, or acoustic signatures [40].

Many IoT devices feature weak authentication mechanisms, use unencrypted communication channels, and possess firmware vulnerabilities, making them easy targets. Malicious actors can exploit these vulnerabilities for data theft, network hacking, or launching distributed DoS attacks [41]. This expanded attack surface, coupled with the resource constraints and diverse design of many IoT devices, renders them particularly susceptible to compromise, making them prime targets for botnets or espionage [40, 42]. To develop an effective cyber defense strategy, it is necessary to systematize the main threats faced by beacon-based systems (Table 2) [references to our two articles, conceptual security model, and smart city]. This classification provides a foundation for understanding the various attack vectors and vulnerabilities inherent in beacon technology, enabling the development of targeted security countermeasures.

Table 2
Classification of cyber threats and countermeasures

Threat Class	Threat Description	Possible Consequences	Attack Examples	Countermeasures and Protocols	Notes/Standards
Spoofing (Impersonation)	An attacker broadcasts fake beacon signals, mimicking legitimate devices.	Positioning errors, unauthorized access.	Starbucks spoofing, Taipei Main Station	Rolling code encryption, AES, EID, mutual authentication	BLE Secure Connections, Eddystone-EID, STRIDE
Replay (Signal Repetition)	Interception and re-broadcasting of legitimate beacon signals.	False events, bypass of access control.	Experiments with iBeacon	Rolling code, timestamps, EID.	STRIDE, NIST SP 800-121
Piggybacking	Unauthorized devices use the beacon infrastructure.	Data leakage, service manipulation.	Described in systematic reviews.	Access control, whitelisting, mutual authentication	ACL, BLE security modes
Eavesdropping (Listening In)	Interception of open beacon radio signals.	Privacy violation, collection of movement data.	Real-world cases in retail and transport.	AES encryption, ephemeral identifiers, data minimization	ISO/IEC 27001, LINDDUN
Denial of Service (DoS)	Mass generation of fake signals or jamming of the radio channel.	Violation of service availability, navigation failures.	BNT-attack, laboratory attacks.	Monitoring, anomaly detection, physical protection, frequency redundancy.	ISO/IEC 18305, AI-based detection
Man-in-the-Middle (MitM)	Interception and modification of data between the beacon and the client.	Data manipulation, information theft.	Experimental attacks.	Mutual authentication, TLS/SSL for backend, integrity checks.	NIST, STRIDE
Tampering (Physical Interference)	Physical access to the beacon for reprogramming or disabling.	System malfunction, injection of malicious code.	Described in reviews.	Tamper-resistant hardware, restricted access, monitoring	ISO/IEC 27001, STRIDE
Privacy Attacks	User tracking, profiling based on beacon signals.	GDPR violation, personal data leakage.	Systematic reviews.	Ephemeral IDs, data minimization, user consent, privacy policies	LINDDUN, GDPR
Replay/ Piggybacking	Repetition or use of legitimate signals to bypass control.	False events, unauthorized access.	Experiments with BLE.	Rolling code, timestamps, access control.	STRIDE, BLE security modes
Jamming (Suppression)	Disruption of the radio channel, blocking of signal transmission.	Loss of coverage, positioning failures.	BNT-attack, laboratory attacks.	Channel hopping, monitoring, physical protection.	ISO/IEC 18305

Beacon-based positioning systems are susceptible to a wide range of cyberthreats, including spoofing, replay, DoS, MitM, privacy attacks, and physical tampering. Effective protection requires a comprehensive approach: the implementation of cryptographic protocols (rolling code, AES, EID), authentication, monitoring, physical security, and adherence to industry standards [43]. The heterogeneous nature of IoT devices, coupled with their often limited computational resources and extended operational lifecycles, exacerbates these vulnerabilities, making conventional security paradigms inadequate. Vulnerabilities in beacon-based systems require a comprehensive approach to cybersecurity that extends beyond traditional methods and includes both software and organizational measures (Figure 4).

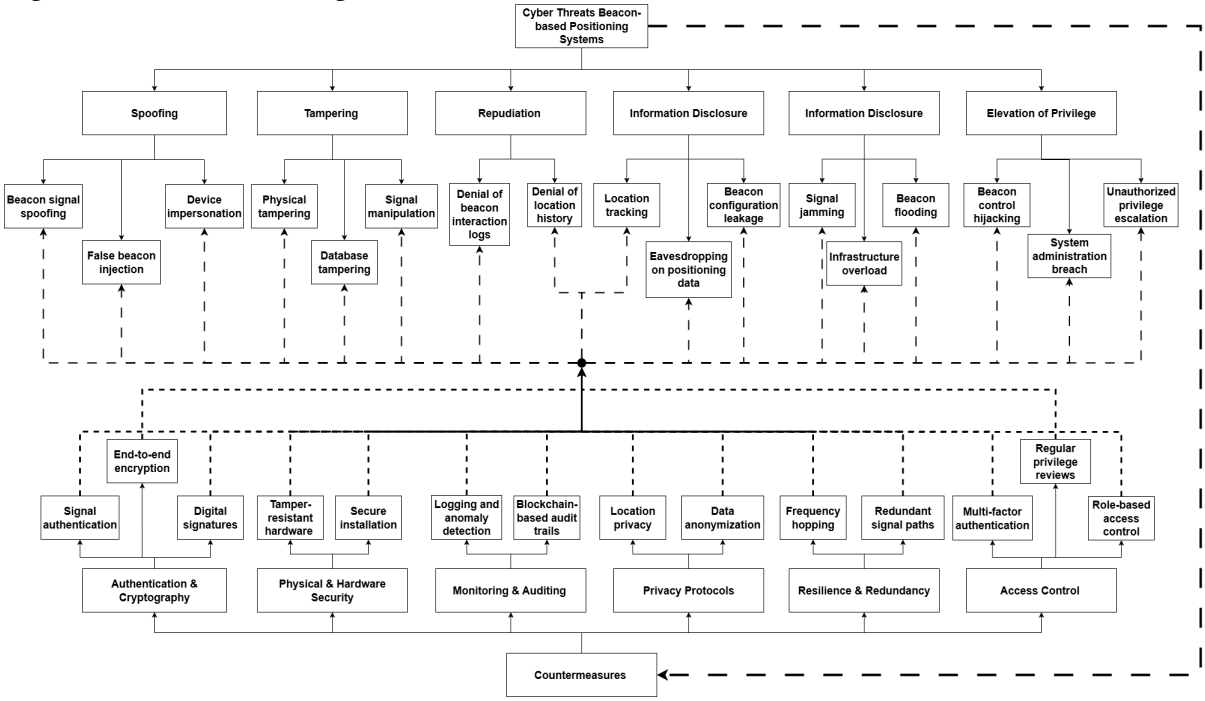

Figure 4: Cyber protection scheme for positioning systems (author's development).

1. Encryption and Authentication: one of the most effective methods is the use of end-to-end encryption for data transmitted between beacons and receivers. This makes signal interception and substitution virtually impossible [37, 45]. Authentication mechanisms guarantee that only authorized devices can interact with beacons, preventing "hijacking" attacks [37, 45].
2. Dynamic Identifier Changing (Secure Shuffling): to counteract "piggybacking" and spoofing attacks, it is recommended to use technology that regularly and randomly changes beacon identifiers (UUID, Major, Minor). This makes it impossible to use intercepted identifiers to create fake beacons, as they quickly become obsolete [37]. Integration with a centralized control system allows these changes to be synchronized with applications, ensuring seamless operation.
3. Software Lock: to protect against physical compromise of beacons and data extraction from them (cracking), some manufacturers use a software lock at the firmware level. Upon an attempt to gain access to the device memory, all confidential data is automatically deleted, rendering the attack pointless [37]. Furthermore, robust access control mechanisms, coupled with continuous behavioral monitoring and anomaly detection, are crucial to identify and neutralize sophisticated threats like unauthorized device impersonation and various forms of data manipulation [44, 45].
4. Anomaly Detection: proactive protection includes real-time analysis of system behavior. For example, the time intervals between beacon signal transmissions can be monitored. If the system detects that the intervals between consecutive signals from the same beacon are

too small, this may indicate a DoS or spoofing attack [45]. Comparing the time and location of signal transmission with reference data also allows for the identification of counterfeit beacons [28, 45].

5. The Role of Cyber-Physical Systems (CPS) and Digital Twins (DT): integrating beacon-based systems into the architecture of Cyber-Physical Systems and Digital Twins is an advanced approach to ensuring security. A Digital Twin is a virtual, real-time synchronized copy of the physical environment. It enables:

- Remote monitoring: modeling the physical environment and the status of beacons in a virtual space, which allows for prompt identification of anomalies without the need for physical inspection [6].
- Reducing personnel risk: using autonomous data-collecting robots, controlled via the Digital Twin, to monitor dangerous or hard-to-reach environments (e.g., at nuclear facilities). This allows for accurate positioning data collection, significantly increasing personnel safety [6]. Furthermore, AI/ML-powered defense systems can leverage this real-time analysis from digital twins to automatically update existing software and prevent large-scale cybersecurity attacks, while also enhancing forensic capabilities for post-incident analysis.
- Proactive defense: simulating various types of attacks and testing the effectiveness of countermeasures in a virtual environment before their implementation in the real system.

This approach shifts the paradigm from reactive defense to proactive risk management. It should be noted that when using beacons as means of notification and evacuation assistance, the most effective measures will be organizational security measures, such as inconspicuous placement of beacons so that the majority of users are unaware of their location, territorial control, and regular patrols to monitor the information being broadcasted by the beacons.

Of the technical means of protection, the possibility of establishing a video surveillance system should be noted, which will allow for the identification of a potential intruder and significantly reduce the possibility of unintentional insider interference.

4. Case study

In order to test the possibilities of using beacons for navigation, the authors decided to install them on the first floor of the training building, which is characterized by a narrow, dark corridor with no natural light (Figure 5). The beacons are shown as dots on the diagram, near the exits from the classrooms.

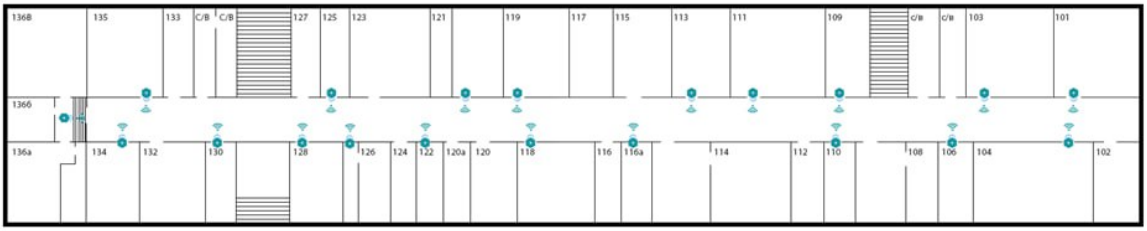

Figure 5: Beacon layout (author's development).

Initially, it was planned to use beacons to inform students about the characteristics of the classrooms and conduct cyber quests with applicants. That's why the beacons were installed in almost every audience. However, since the end of February 2022, the use of beacons as information stands has become irrelevant. The task of informing students and visitors about evacuation routes and finding shelters in the building has become much more urgent. When using beacons as information stands, their use turned into a small quest, the user had to install a browser with

corporate functions – Physic Web and allow this function interaction with cyber-physical systems (Figure 6). Which greatly increased the access time to beacons especially in the initial setting.

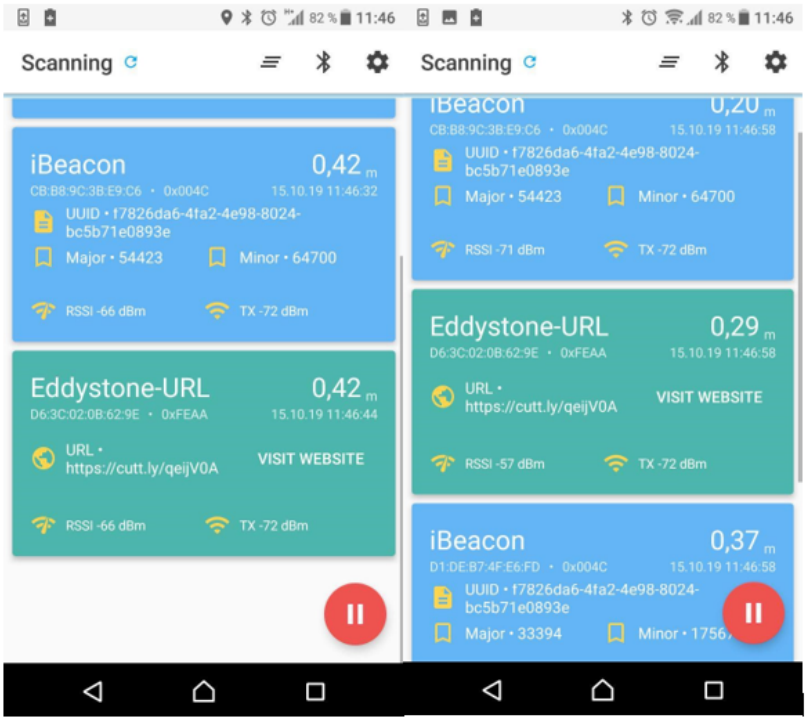

Figure 6: Browser with Physic Web technology (author's development).

When redesigning the layout of the beacons to be used for evacuation purposes, the authors had some questions:

1. Will the beacons be able to work and interact with smartphones without the internet?
2. If there is no electricity, will this circuit with beacons be operational?
3. Is a personal app necessary for this or will it be enough without the internet browser?

In experiments with different types of beacons browsers and smartphones, the following answers were obtained:

1. Autonomous Operation and Data Transmission: beacons, particularly those based on Bluetooth Low Energy (BLE) technology, can operate and interact with smartphones fully autonomously, without requiring an internet connection. The beacon's principle of operation involves continuously transmitting (broadcasting) radio signals containing a small volume of data. This data typically includes a unique identifier (e.g., UUID, Major, Minor) or a web address (URL). The beacon essentially functions as a "digital lighthouse". If Bluetooth is enabled on a smartphone, it continuously scans the airwaves for such signals. Upon detecting a signal from a beacon, it retrieves this unique identifier. All subsequent actions, such as localization and information display, occur locally on the smartphone itself. This process does not require an internet connection.
2. Resilience to Power Outages: in the majority of cases, the beacons will continue to operate because they are powered by their own integrated energy sources (batteries) and are thus independent of the building's centralized electrical grid. Since the beacons simply transmit a signal, their local operation does not depend on external power sources, servers, or the configuration of IT equipment. They will remain functional until their battery is depleted.
3. Application vs. Browser Limitations for Localization: built-in browser functions, such as Progressive Web Apps (PWA), allow caching web pages for offline access. However, for a

mapping application to successfully interact with beacons and accurately determine the user's location, it requires the ability to continuously scan for Bluetooth signals in the background. This functionality is native to the smartphone's operating system and is primarily accessible to specialized, dedicated mobile applications. A standard browser generally cannot access beacon data without an internet connection, unless the web page is designed with a complex architecture for specific offline data caching and usage.

A dedicated application, in contrast to a browser, can be configured for continuous background scanning for beacon signals. When the application receives a signal, it matches the beacon's identifier against data stored in its own local database (cache), which contains the building map and evacuation routes. It may also utilize other smartphone sensors, such as the accelerometer, for additional location refinement. This entire process occurs on the user's device, ensuring the system is fully autonomous and independent of external networks. If a beacon broadcasts an Eddystone URL, internet access would be required to open the link. Therefore, for autonomous operation, it is preferable to use beacons that only transmit a unique identifier (e.g., iBeacon or Eddystone UID). The dedicated application on the smartphone already "knows" what to do with this identifier, having all necessary information, including evacuation routes, pre-loaded into memory.

During the experiments conducted using beacons, the authors recorded the time required for evacuation from the furthest classroom, which is numbered 101 in Figure 7. The experiments were performed with two distinct groups of participants: those who were well-familiar with the building and those who were in the building for the first time.

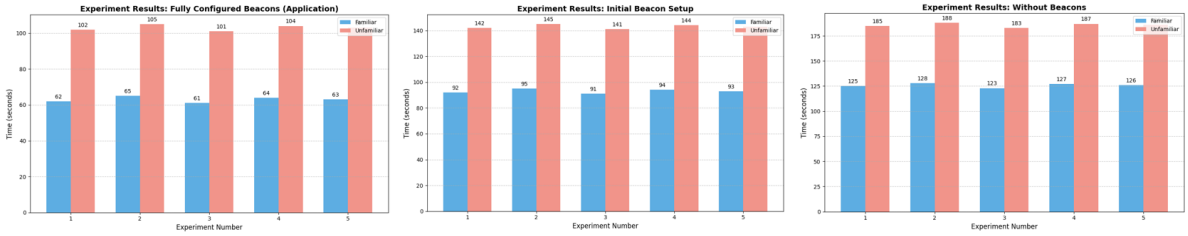

Figure 7: Experiment results (author's development).

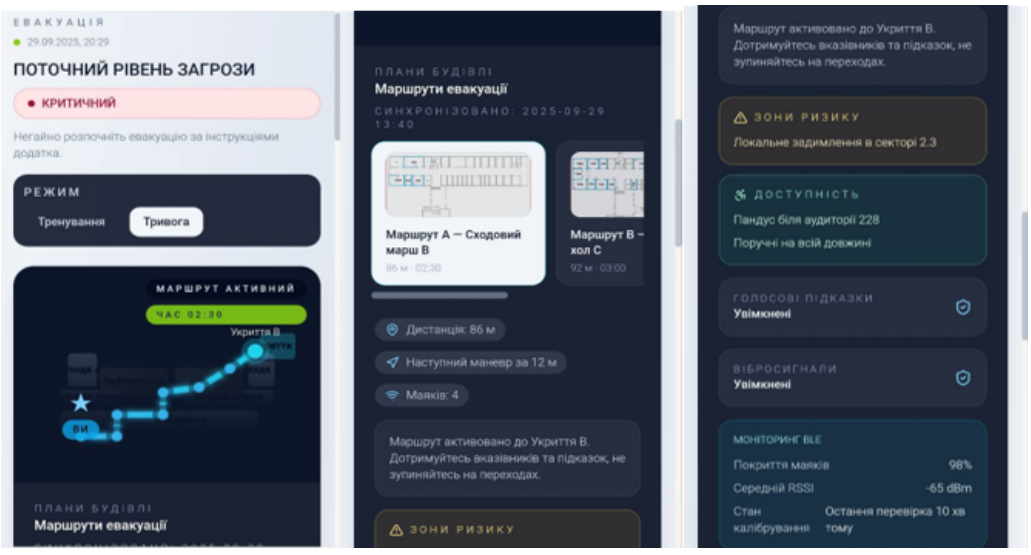

Figure 8: Mobile evacuation application interface (author's development).

As shown in Figure 7, the evacuation time significantly increases in both groups of individuals during the initial configuration of the application (browser) for utilizing the information broadcast by the beacons. The use of a pre-configured browser allows for a slight acceleration of the evacuation of individuals unfamiliar with the building layout or visiting it for the first time.

The traditional use of beacons for smartphones requires an Internet connection; otherwise, the browser cannot retrieve information from the beacon. To enable a beacon-based evacuation system operation in offline mode, it must be implemented via a dedicated native application. All essential information, including maps and routes, must be pre-cached in the smartphone's memory. In this architecture, beacons serve merely as triggers, with all logic and navigation processes executed locally on the user's device. A specialized application for building evacuation was developed by the authors (Figure 8). After installing the developed application for evacuation using beacons on smartphones of two groups of users, the experiment with evacuation was repeated. The time of evacuation is shown in Figure 9.

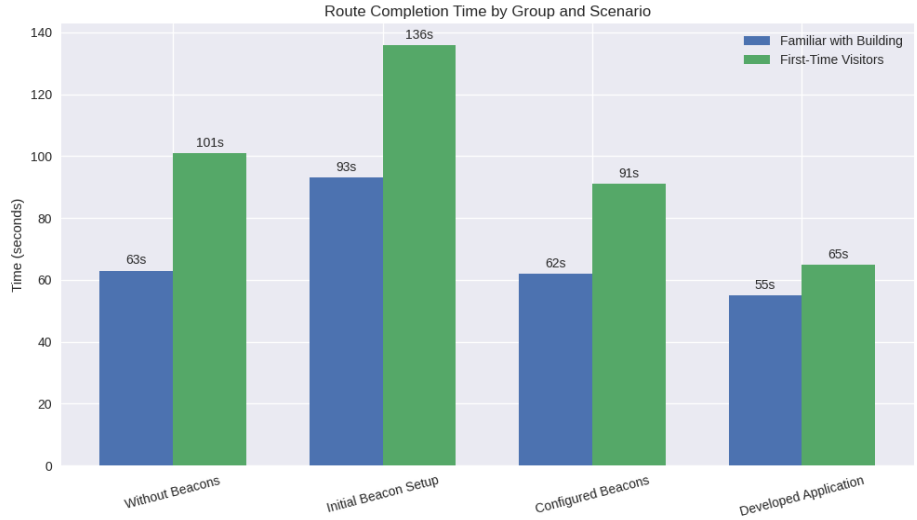

Figure 9: Graphs with time during evacuation using the developed application. (author's development).

As shown in Figure 9, the gain from using beacons and a specially developed application is about 8% for the group that knows the scheme of the building, which is insignificant. However, in a critical situation every second counts. For a group of people who do not know the building when using beacons and the application, the evacuation time is reduced by 30% and approaching the time of a group of people who know the schematics of the building. This greatly increases the chances of a successful evacuation. In fact, the use of beacons allows to instill confidence and knowledge of the building people for the first time in this building.

5. Discussions

The conducted research affirms that the foundational challenge in indoor positioning lies in navigating the trade-off between positioning accuracy and the total cost of ownership (TCO). While UWB technology offers superior, centimeter-level accuracy essential for critical industrial applications like Autonomous Guided Vehicles (AGV) and asset tracking, its high infrastructure cost and complex deployment limit its mass applicability. Conversely, BLE technology emerges as the optimal choice for mass-market deployment—such as in university campuses and retail—due to its low power consumption, cost-effectiveness, and near-universal compatibility with modern user devices. This dichotomy necessitates a hybrid deployment strategy as the most efficient path forward. Such a strategy strategically places high-accuracy UWB anchors only in mission-critical zones (e.g., laboratories, chemical storage), while relying on widespread, low-cost BLE beacons for general navigation and contextual alerting.

A key contribution of this work is demonstrating how Artificial Intelligence mitigates the fundamental technical weaknesses of these radio-frequency systems. Traditional positioning methods are severely compromised by multipath effects, Non-Line-of-Sight (NLoS) conditions, and device heterogeneity. However, AI models can be trained to recognize and compensate for signal

perturbations, such as “shadowing” caused by the human body, correcting RSSI values in real time. Furthermore, AI enables the creation of self-adapting models that eliminate the need for costly and labor-intensive manual recalibration a significant drawback of traditional fingerprinting methods by dynamically adjusting to changes in the environment.

Critical to the implementation of any beacon-based system is a robust cyber defense framework. The inherent vulnerability of many beacon protocols (such as the unencrypted transmission of identifiers) makes them susceptible to simple but devastating attacks, including spoofing, jamming, and cloning, which could entirely compromise the system's integrity during an emergency. The proposed defense strategy shifts the security paradigm from reactive to proactive, advocating for the mandatory use of end-to-end encryption, dynamic identifier changing (Secure Shuffling), and leveraging the Digital Twin concept. By modeling the physical and cyber state in a virtual environment, the Digital Twin allows for remote monitoring of device anomalies, real-time testing of countermeasures, and enhanced forensic analysis following an incident. The practical significance of this integrated approach was quantitatively validated in the emergency evacuation experiment. While users familiar with the building saw an acceleration of evacuation time by approximately 8%, the impact on individuals unfamiliar with the building was profound: the use of the beacon-assisted application reduced their evacuation time by 30%. This empirical result provides a strong validation of the system's value, transforming a simple navigation tool into a life-saving safety component, particularly for transient populations in large, complex facilities.

6. Conclusions

The research successfully achieved its objectives by analyzing the current state of mobile beacon infrastructure, classifying key technologies, detailing their vulnerabilities, and proposing an integrated cyber-physical defense model.

The comparative analysis (Table 1) clearly established the operational parameters of BLE, UWB, Wi-Fi RTT, and RFID, confirming that no single technology is optimal for all scenarios. The key finding is that the implementation of BLE-based positioning, secured by robust software and AI algorithms, is the most pragmatic solution for large-scale safety applications, such as emergency evacuation. The experimental data unequivocally demonstrate the life-saving potential of the developed system. The observed 30% reduction in evacuation time for people unfamiliar with the building, achieved through a dedicated, pre-configured application, validates the proposed methodology and underscores its ability to provide crucial guidance and stability during moments of panic. Even the seemingly small time savings for knowledgeable users (approximately 8%) can be critical in real-world air raids or other time-sensitive crises. The system thus instills both confidence and practical knowledge, effectively turning unfamiliar visitors into informed evacuees.

Future research should focus on further enhancing the system’s resilience by:

- Deepening the application of AI and Machine Learning for automated, real-time detection and prediction of sophisticated cyberattacks, transitioning from anomaly detection to predictive attack forecasting;
- Developing standardized protocols for the seamless integration of BLE positioning data with Digital Twin platforms for advanced real-time situational awareness and post-incident reconstruction;
- Investigating the system's resilience and operational performance in environments subjected to active Electronic Warfare (EW) countermeasures, building upon the initial concerns regarding GNSS reliability in contested areas.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] What is beacon technology? The uses of beacon technology, MOKOBlue. URL: https://www.mokoblue.com/en/beacon-technology-for-a-connected-world

[2] Beacon technology – how it works and how it can be used, MOKOSmart. URL: https://www.mokosmart.com/beacon-technology

[3] BLE beacon location tracking solutions, Dusun IoT. URL: https://www.dusuniot.com/blog/ble-beacon-location-tracking-for-asset-management

[4] M. Tomitsch, R. Schlögl, T. Grechenig, C. Wimmer, T. Költringer, Accessible real-world tagging through audio-tactile location markers, in: 5th Nordic Conference on Human–Computer Interaction, ACM, 2008. https://doi.org/10.1145/1463160.1463242

[5] 11 helpful ways beacons are changing education, TechGrid. URL: https://techgrid.com/blog/11-helpful-ways-beacons-are-changing-education

[6] M. Z. Karakuşak, H. Kivrak, S. Watson, M. K. Ozdemir, Cyber-WISE: A cyber-physical indoor positioning system and digital twin approach, Sensors 23 (2023) 9903. https://doi.org/10.3390/s23249903

[7] M. Vlasova, Indoor GPS | Alternatives to GPS inside building, Navigine (2023). URL: https://navigine.com/blog/why-is-gps-ineffective-inside-buildings

[8] Do Wi-Fi indoor positioning systems still make sense in 2025?, Mapsted Blog. URL: https://mapsted.com/blog/wifi-positioning-system-explained

[9] Beacon in education: Intelligent and digital development. URL: https://www.mokoblue.com/how-beacon-technology-can-be-applied-in-the-education-industry

[10] V. Pevnev, A. Plakhteev, M. Tsuranov, H. Zemlianko, K. Leichenko, Smart city technology: Conception and security issues, in: Integrated Computer Technologies in Mechanical Engineering 2021, Springer, 2022, 207–218. https://doi.org/10.1007/978-3-030-94259-5_19

[11] ISO/IEC 18305:2016 – introduction, NIST. URL: https://www.nist.gov/ctl/pscr/isoiec-18305-2016-introduction

[12] UWB vs Bluetooth: Which indoor positioning technology wins?, MOKOSmart. URL: https://www.mokosmart.com/uwb-vs-bluetooth-indoor-positioning-guide

[13] Exploring the role of Bluetooth in IoT device communication, MoldStud. URL: https://moldstud.com/articles/p-exploring-the-role-of-bluetooth-in-iot-device-communication-enhancing-connectivity-and-efficiency

[14] H. Wang, G. Ganesh, M. Zon, O. Ghosh, H. Siu, Q. Fang, BLE-based indoor positioning for aging-in-place, PLOS Digital Health 4 (2025) e0000774. https://doi.org/10.1371/journal.pdig.0000774

[15] UWB vs Wi-Fi RTT: Precision positioning showdown, RTLS Alliance. URL: https://www.rtlsalliance.com/resources/uwb-vs-wifi-rtt-precision-showdown

[16] C. S. Álvarez-Merino, H. Q. Luo-Chen, E. J. Khatib, R. Barco, Wi-Fi FTM, UWB and cellular fusion for indoor positioning, Sensors 21 (2021) 7020. https://doi.org/10.3390/s21217020

[17] A. Panyov, UWB technology (2025 guide), Navigine (2020). URL: https://navigine.com/blog/uwb-technology-features-examples-of-application

[18] C. Ma, B. Wu, S. Poslad, D. R. Selviah, Wi-Fi RTT ranging and positioning, IEEE Trans. Mob. Comput. 1 (2020). https://doi.org/10.1109/TMC.2020.3012563

[19] M. Orfanos, H. Perakis, V. Gikas, G. Retscher, T. Mpimis, I. Spyropoulou, V. Papathanasopoulou, Wi-Fi RTT for personal mobility, Sensors 23 (2023) 2829. https://doi.org/10.3390/s23052829

[20] H. Gomes, F. Navio, P. D. Gaspar, V. N. G. J. Soares, J. M. L. P. Caldeira, RFID traceability system in industry, Applied Sciences 13 (2023) 12943. https://doi.org/10.3390/app132312943

[21] L. Profetto, M. Gherardelli, E. Iadanza, RFID in healthcare: A review, Health and Technology (2022). https://doi.org/10.1007/s12553-022-00696-1

[22] C. Munoz-Ausecha, J. Ruiz-Rosero, G. Ramirez-Gonzalez, RFID applications and security, Computation 9 (2021) 69. https://doi.org/10.3390/computation9060069

[23] S. Naghdi, K. O'Keefe, Human obstacle mitigation in BLE trilateration, Sensors 20 (2020) 1350. https://doi.org/10.3390/s20051350
[24] J. Wisanmongkol, L. Klinkusoom, T. Sanpechuda, L.-O. Kovavisaruch, BLE multipath mitigation, in: ISCIT 2019, IEEE, 2019. https://doi.org/10.1109/ISCIT.2019.8905164
[25] How AI contributes to indoor geolocation performance, Pole Star. URL: https://www.polestar.eu/blog/use-of-artificial-intelligence-ai-in-indoor-geolocation-solutions
[26] S. Tiku, A. Mittal, S. Pasricha, CNN framework for indoor localization, in: Machine Learning for Indoor Localization and Navigation, 2023, 159–176. DOI: 10.1007/978-3-031-26712-3_7
[27] A. Famili, A. Stavrou, H. Wang, J.-M. Park, OPTILOD: Optimal beacon placement, Sensors 24 (2024) 1865. https://doi.org/10.3390/s24061865
[28] Detection of spoof attacks on location broadcasting beacons, Google Patents. URL: https://patents.google.com/patent/US20170026408A1/en
[29] A. C. Chan, R. M. Chung, Security and privacy of wireless beacon systems, arXiv (2021) abs/2107.05868.
[30] V. Pevnev, M. Tsuranov, H. Zemlianko, O. Amelina, Conceptual model of information security, in: Lecture Notes in Networks and Systems, 2021, 158–168. DOI: 10.1007/978-3-030-66717-7_14
[31] L. Xiao, X. Wan, C. Dai, X. Du, X. Chen, M. Guizani, Edge caching security via RL, IEEE Wireless Communications 25 (2018) 116–122. https://doi.org/10.1109/MWC.2018.1700291
[32] P. M. Sánchez Sánchez, J. M. Jorquera Valero, A. Huertas Celdrán, G. Bovet, M. Gil Pérez, G. M. Pérez, Hardware fingerprinting of SBCs, J. Netw. Comput. Appl. 212 (2023) 103579. https://doi.org/10.1016/j.jnca.2022.103579
[33] M. Mouzai, M. A. Riahla, A. Keziou, GPS spoofing detection using ML, Sensors 25 (2025) 4045. https://doi.org/10.3390/s25134045
[34] R. Singh, K. P. Sharma, L. K. Awasthi, ML ensemble for IoT security, Cluster Computing (2024). https://doi.org/10.1007/s10586-024-04519-y
[35] Z. Ayaz, BLE beacons for retail behavior analytics, J. Theor. Appl. Electron. Commer. Res. 20 (2025) 55. https://doi.org/10.3390/jtaer20020055
[36] J. H. Ziegeldorf, O. G. Morchon, K. Wehrle, Privacy in IoT, Security and Communication Networks 7 (2013) 2728–2742. https://doi.org/10.1002/sec.795
[37] Beacon security – protect your infrastructure. URL: https://kontakt.io/blog/beacon-security
[38] M. Rahaman, C.-Y. Lin, P. Pappachan, B. B. Gupta, C.-H. Hsu, Privacy-centric AI for smart farming, Sensors 24 (2024) 4157. https://doi.org/10.3390/s24134157
[39] M. I. Ibrahim, M. Y. Darus, DDoS analysis in smart home IoT, JOIV 8 (2024) 2104. https://doi.org/10.62527/joiv.8.4.2175
[40] What are the security challenges of 5G and IoT?, Fortinet Blog. URL: https://www.fortinet.com/blog/industry-trends/the-security-implications-for-5g-and-iot
[41] U. Tariq, I. Ahmed, A. K. Bashir, K. Shaukat, IoT cybersecurity review, Sensors 23 (2023) 4117. https://doi.org/10.3390/s23084117
[42] S. Holcer, J. Torres-Sospedra, M. Gould, I. Remolar, Privacy in indoor positioning, in: ICL-GNSS 2020, IEEE, 2020. https://doi.org/10.1109/ICL-GNSS49876.2020.9115496
[43] I. H. Putro, T. Ahmad, R. M. Ijtihadie, MQTT intrusion detection with ML, IEEE Open J. Commun. Soc. 1 (2025). https://doi.org/10.1109/OJCOMS.2025.3610132
[44] A. Mart, U. Zurutuza, R. Uribeetxeberria, M. Fern, J. Lizarraga, A. Serna, I. V, Beacon spoofing detection, in: ARES 2008, IEEE, 2008. https://doi.org/10.1109/ARES.2008.130
[45] V. Pevnev, A. Frolov, M. Tsuranov, H. Zemlianko, Data integrity in infocommunication systems, International Journal of Computing 21 (2022) 228–233. DOI: 10.47839/ijc.21.2.2591