On IoT Localization Architectures Comparison and Privacy Concerns in the Healthcare Sector

Antonio Scarfò(✉)

Department of Information of Computer Science, University of Salerno, 84084 Fisciano, Italy
ascarfo@unisa.it

Abstract. Nowadays, localization is one of the most interesting and used application in IoT domain. It promises to gain more and more relevance, especially in the healthcare market, thanks to the optimization of the operations that localization-aware applications allow to achieve. The paper presented has the aim to provide a high-level review of some significant use cases of localization applications in the healthcare industry and highlight their peculiarities in a framework of evaluation. That helps to select the most suitable localization architecture, given the requirements of a use case. Among the parameters that are part of the framework of evaluation, the paper gives special relevance to the privacy concerns, that are tightly related to the IoT-based applications in the sector of healthcare. The work is introduced by a brief description of the IoT topics, the guiding question, and the main elements which are taken into consideration to evaluate the cases selected. These elements define the main criterion to select the cases in the literature. A brief description of the cases selected is reported. And the final part of the review consists of a very concise comparison of the cases, leveraging the key elements of evaluation framework defined.

Keywords: IoT · Localization · Privacy · Comparison · WiFi · BLE · RFID · Indoor · Healthcare · 802.15.4

1 Introduction

The availability of new technologies in IoT sector opens the doors to new use cases aimed to optimize operations through a pervasive interaction among sensors and the real word. In the healthcare sectors, for instance, the continuous and the real time monitoring of patients allow to save lives, improve treatments fulfillments, and optimize the logistic. Emerging use cases require new communication technologies that can connect a multitude of smart things from the world of "perception", randomly, in mobility fashion, and with low power consumption. This is especially true for localization aware applications where the mobility is mandatory and, often, low energy consumption is also a basic requirement. The localization aware applications are getting a more and more relevant role in the IoT sector. A report of Market&Market shows that applications based on GPRS will record a 12.9% CAGR of market growth from 2016 to 2023. Specifically,

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2022
O. Gervasi et al. (Eds.): ICCSA 2022 Workshops, LNCS 13380, pp. 401–418, 2022.
https://doi.org/10.1007/978-3-031-10542-5_28

m-Heath market is forecasted to record a CAGR of 30% from 2021 to 2030 by Global Market Insight Institute. This impressive growth of localization application is related with the benefits that is possible to achieve in terms of processes optimization, according to [1]. This sector will leverage more and more localization features as well as IoT healthcare technologies will evolve and will be adopted. This comes really clear in the current pandemic period, where monitoring people form remote and trace them is key to contain the infection and monitor the status of the patients. This paper analyzes four cases of localization aware application based on different methods, to highlining differences, peculiarities, and provide a guide to select the most suitable architecture against the use case requirements, giving a special relevance to the privacy concerns related with.

Localization requires multidiscipline contributes and involve the complete IoT stack, including devices, communication protocols, algorithms and computational resources, data collection and analytics. To provide the background useful to create the framework of reference of relevant parameters, following are summarized the most common methodologies and methods used to localize a target [2].

- Proximity vs Localization: proximity returns the distance between the target and another object whereas localization provides coordinates of the target in a reference system (anchors). Proximity could be a part of a localization system.
- Devices-free vs devices-based localization, device-based localization uses devices as a target whereas in device-free targets that are not equipped with a device.
- Architecture models: in anchor-based the architecture leverages a well-known reference system. In anchor-free, the architecture does not leverage a well-known reference system.
- Methodology of calculation:
  - range-based uses target-sensor geometrical distance calculation.
  - range-free uses indirect methods based on hop count between anchors and targets.
- Range-based required hardware and is not simple to deploy whereas range-free do not needs of special hardware and it is cost efficient but less accurate.

Among the localization techniques, following a summary of the most used.

- Time based, based on signal propagation information
  - ToA or ToF, Time of Arrival or of Flight, is based on time of propagation of the signal and time stamps, it requires tightly synchronization among anchors-targets.
  - DToA, Difference of Time of Arrival, is based on Difference of Time of Arrival of the signal at anchors, it limits the need of synchronization at transmitters.
  - RToF, Return Time of Flight, is an evaluation of distance between two targets based on round-trip time of the signal, it requires a moderate synchronization.

- Angle Based, based on trigonometrical evaluation.
  - AoA, Angle of Arrival, uses array of antennas to evaluate the angle of arrival, it leverages the difference of time of arrival on adjacent antennas.
  - PoA, Phase of Arrival, based on phase difference of the signal received in adjacent antennas of an array, it could be used to estimate distances or improve accuracy of RSSI, ToF, TDoA.
- Signal energy based.
  - RSSI, Received Signal Strength Indicator, based on signal power received.
- Other elements
  - CSI, Channel State Information, enrich RSSI with information about subchannel amplitude and phase information (CIR + CFR), it improves accuracy.
  - Fingerprinting, mathematical algorithms to compare real time RSSI/CSI information with an offline measurement data set. Often used with AI algorithms.
  - Likelihood function, this is an estimator statistical function, it depends on condition changing and have tradeoff with accuracy vs granularity of samples.
  - Artificial Neural Network (Multi-Layer Perceptron), mostly used to train RSSI.
  - K-Nearest Neighbors, used to obtain k-nearest matches with known location in the RSSI online measures.
  - Support Vector Machine, a method to gain classification and regression, used for ML and statistical analysis with high accuracy, can be used for localization on RSSI online/offline measures.
  - Dead Reckoning, try to predict the position of targets using information like historical information, accelerometers and so on.
  - Hybrid methods, a combination of methods to increase accuracy and robustness.

The picture Fig. 1 reports pro and cons of the most used localization techniques.

Technique	Advantages	Disadvantages
RSSI	Easy to implement, cost efficient, can be used with a number of technologies	Prone to multipath fading and environmental noise, lower localization accuracy, can require fingerprinting
CSI	More robust to multipath and indoor noise,	It is not easily available on off-the-shelf NICs
AoA	Can provide high localization accuracy, does not require any fingerprinting	Might require directional antennas and complex hardware, requires comparatively complex algorithms and performance deteriorates with increase in distance between the transmitter and receiver
ToF	Provides high localization accuracy, does not require any fingerprinting	Requires time synchronization between the transmitters and receivers, might require time stamps and multiple antennas at the transmitter and receiver. Line of Sight is mandatory for accurate performance.
TDoA	Does not require any fingerprinting, does not require clock synchronization among the device and RN	Requires clock synchronization among the RNs, might require time stamps, requires larger bandwidth
RToF	Does not require any fingerprinting, can provide high localization accuracy	Requires clock synchronization, processing delay can affect performance in short ranger measurements
PoA	Can be used in conjunction with RSS, ToA, TDoA to improve the overall localization accuracy	Degraded performance in the absence of line of sight
Fingerprinting	Fairly easy to use	New fingerprints are required even when there is a minor variation in the space

Fig. 1. Advantages and Disadvantages of Different Localization Techniques [2]

Localization techniques are tightly related to wireless communication protocols, to complete the background, a summary of the most used wireless protocols and localization methodologies are reported. The Table II of [2] reports the most important telecommunication protocols and their characteristics in terms of throughput, coverage, scalability, energy consumption. The Table I of [10] shows the relations among telecommunication protocols and localization techniques, including some key parameters like accuracy, scalability, costs.

2 Previous Works and Methodology

Researching in engines like IEEE, Research Gate, Direct Science, does not return relevant papers about comparison among real cases based on heterogeneous methods to localize things/people in healthcare sector. Whereas it is possible to find several works about localization methods and localization performance improvement, and comparison among them. This is, likely, due to the complexity to compare heterogeneous architectures. The keywords used to search previous works were: IoT, Localization, Indoor, Case, Healthcare.

The methodology adopted to select and compare real use cases about localization in healthcare domain is explained in the following points:

- Create a framework of evaluation. A set of parameters, that are relevant for the most common use cases, is created to compare the cases selected.
- Select the cases. To be as relevant as possible, the cases selected from literature leverage different methods and methodologies to localize targets. All of them include applied tests in real or nearly real world.
- Analysis. The cases selected were analyzed trying to esteem the parameters that are part of the framework of evaluation. When the parameters are not deducible from the analysis of the cases, their esteem has been completed using data from the literature.
- Comparison. A comparison was carried out from the cases analysis according to the framework of evaluation. This comparison can be used as a guide to select the most suitable architecture of localization, given the requirements of a use case.

The methodology is designed to be the easily appliable and open to be extended including more cases or parameters.

3 Evaluation Parameters and Cases Selection

The parameters selected are the most common for the use cases of localization: Range of coverage, Latency, Accuracy, Power consumption/Energy Efficiency, Scalability, Costs, Privacy. Given a solution, these parameters define its scope of the applications.

Given the framework of evaluation, it is the moment of select the cases. The purpose of the review is comparing applied cases of localization in healthcare industry, to respond the question: “What is the most suitable method to fulfill a given use case of localization in healthcare applications domain?”. The research was carried out to find heterogeneous cases.

The first criterion was restricting the set of articles to select as following:

- Restricting the research to IEEE Explorer engine
- Restricting the research to IEEE journals
- Restricting the research to the last 10 years of publication.

Then, the key words used were: indoor, localize/localization, healthcare. Fifty-five articles emerged and, in that basket, five experimentations were selected, which leverage different localization methodologies.

4 Privacy Perspectives

Localization applications in healthcare domain often have the final aim to trace patients and transmit data related to his vitals. That entails serious issues of privacy and security. Indeed, according to GDPR regulation [11, 22], data related to health status are specifically defined as sensitive because of the compromission of this information could have significant impact on the rights of the patients. The personal health data are among the most priced in the dark web due to the high level or returns that is possible earn from them. Fundamentally, according to [12, 21], the risks related to the privacy are: illegitimate access to data and diffusion, unwanted data changing, data cancellation. Risk management models take in consideration the process of collect, transmit, memorize, and use data. Each process could be object of privacy risks coming from both humans and not humans. The model of risk analysis in Fig. 2, from [12], is taken in consideration in the following part of the document.

Risks	Impacts on data subjects	Main risk sources	Main threats	Existing or planned measures	Severity	Likelihood
Illegitimate access to personal data						
Unwanted change of data						
Disappearance of data						

Fig. 2. Risk analysis model [12]

All cases taken in consideration relay on wireless telecommunication protocols that are used also to localize targets through many methods, where devices that equip the target are used to collect and transmit data. Protocols and devices are exposed to several privacy risks, according to the model of Fig. 3, is possible to categorize in:

- Edge attacks, that are the attacks to the devices in the perception layer.
- Network attacks, that are the attacks to the elements devoted to collect and transmit the information coming from perception layer.

Often, in the domain of the analysis, devices are limited in resources of computation to save energy, this could entail limitations in apply complex algorithms for authentication and encryption. On the other hand, general purpose devices, like smartphones, are more exposed to be attacked due to both the commercial operation systems and the presence of many and not always secure applications.

The Fig. 4, [14, 18] summarizes the attacks that can threat the edge and the network layers of an IoT infrastructure. Finally, the Fig. 5 reports the correlation between threats and risks of a IoT infrastructure, according to the risk model aforementioned, which is used to evaluate the cases selected.

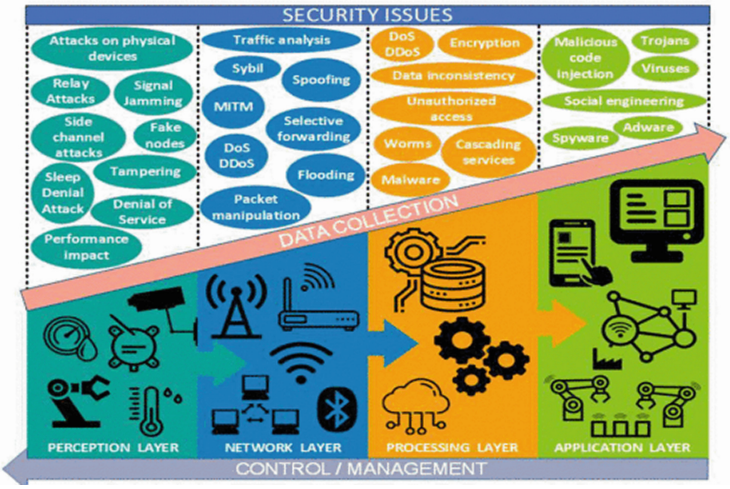

Fig. 3. Layers and typologies of attacks [17]

EDGE ATTACKS	PRIVACY IMPACTS
Hardware Trojan	Leak personal data, data manipulation
Node replication	Unreal data generation, inpersonification, access to security parameters
Denial of Service (DoS) attacks	Block of services
Sleep deprivation	
Battery draining	
Outage attacks	
Physical attack	Leak security parameters, device cloning, unreal data
Malicious node	Possibile entry point for an excalation phase
Side channel attack	Leak of information even about security parameters
Eavesdropping	Leak of data related to the sensors and also security parameters
Tag Counterfeiting	Unreal data transmission
Tag cloning	Unreal data trasmission of an device associated person
Tag Tracking	Leak of data related to the sensor localization
Tag Inventorying	Sensitive data leakage

NETWORK ATTACKS	PRIVACY IMPACTS
Side channel attacks	Access to security parameters
Collision attacks:	Service blocking (eg sensor battery drain)
Fragmentation attacks	Service issues
Routing attacks	
Hello Flood	Service issues
Gray Hole	Service issues
Sybil attack	Unreal data transmission
Worm Hole	Lack of information
Selective forwarding	Service issues
Eavesdropping	Observation of data related to the sensors and also security parameters
Inject malicious packets	Unreal data transmission
Dos attacks	Service issues, service blocking
Desynchronized attack	N - usually result in service preformance issues or service break
Spoofing	Unreal data transmission
Sinkhole	Service issues, preparation for other attacks
Man in the middle attack	Observation of sensitive data, unreal data trasmission

Fig. 4. Edge attacks and privacy impacts - networks attacks and privacy impacts

Finally, looking at the whole architecture, the most likely targets of the attackers are the points where data are stored and visualized. Access to the data storage open the doors to gain the access to all data available. The magnitude of the impact of an attack to a datastore is certainly higher than an attack to the edge or to the network of the

architecture. Attack the edge and the network of the architecture can result in trace a person, corrupt/leak some data, denial a little piece of the service, but, also, access to the infrastructure and moving gradually to the datastore in datacenter, in cloud or in the edge. The focus of the analysis is limited to the edge and to the network because of the cases do not report the processing and application layers architectures.

Risks	Main risk sources	Main Threats	Risks	Main risk sources	Main Threats
Illegitimate acces to personal data	Non Human	Hardware Trojan	Unwanted change of data	Non Human	Hardware Trojan
	Non Human	Node replication		Non Human	Node replication
	Human	Physical Attack		Human	Physical Attack
	Non Human	Eavesdropping		Non Human	Eavesdropping
	Human & Non Human	Tag cloning		Human & Non Human	Tag Counterfeiting
	Non Human	Tag Tracking		Non Human	Sybil attack
	Human & Non Human	Tag Inventorying		Non Human	Inject malicious packets
	Non Human	Network Eavesdropping		Non Human	Spoofing
	Non Human	Network Side channel attacks		Non Human	Man in the middle attack
	Non Human	Network Sinkhole	Risks	Main risk sources	Main Threats
	Non Human	Network Worm Hole	Disappearance of data	Non Human	Hardware Trojan
	Non Human	Man in the middle attack		Non Human	Tag Counterfeiting
				Non Human	Network Worm Hole

Fig. 5. Risk analysis for IoT privacy

To protect edge and network layers what is fundamental to protect security and privacy are [18]:

- Strong authentication methods.
- Strong encryption other methods.
- Robust key/certificate management system.
- Decouple device ID and people identity.
- Hardening Operating System of the employed devices.

The methodology used to evaluate the privacy aspects of the cases selected is based on risk qualitative analysis according to the risk model aforementioned.

5 A Brief Description of the Cases Selected

In this section are described four use cases about localization in healthcare industry, taken from the literature. The cases are based on different architectures and use different methods of localization.

5.1 Case 1. "An IoT-Aware Architecture for Smart Healthcare Systems"

The purpose of this case, descripted in [3], is to create a solution able to provide insights about patients and environmental conditions in a healthcare budling, within a robust, optimized, and low power HMS (Health Management System). Key goals:

- Tracking the patients' paths to allow a fast first aid in case of emergencies.

- Collecting vitals samples in time and space, to provide insights for decisions support.

The authors chose to use a hybrid solution, 802.15.4 and RFID, with the aim to reduce energy consumption as much as possible. The architecture is composed by:

- Host Terminal (HT), the mobile devices for patients, supporting both RFID Tag and 802.15.4 radios, with sensors for vitals and a battery to enable RFID-BAP (battery-assisted passive). The battery is used to send alarms via 802.15.4 in wakeup mode.
- Low Power Router Reader (LPRR), devices equipped with an RFID reader, an 802.15.4 transceiver, and some environmental sensors. LPRRs act as anchors localizing the HTs and collecting data. LPRR are scattered in the budling with the appropriate density to detects patient in rooms. LPRR upload data in WSN fashion.
- IoT Smart Gateway, a server that receive and elaborate locally data from LPRRs.
- A central server that memorizes data and provide post elaboration/http interface to the users.

The architecture is shown in Fig. 1-Fig. 2-Fig. 3 of [3]. The system uses a CoAP protocol, which use http interface to provide insights to the doctors. The HT, usually passive, can generate alarms, proactively, in the case that vitals/movements are anormal. The Table I of [3] shows the comparison of power consumption among protocols used, to give the idea how the dual radio approach at HT (with 802.15.4 sleeping most of the time except for emergencies) could improve power consumption if compared with a full 802.15.4 based architecture. The result of experimentation points out a wakeup range of 11 mt in RFID, 13 mt of coverage in fully passive mode, 22 mt of coverage in BAP mode. It is very interesting that BAP mode recorded 0.025 mA of current consumption, which is three order of magnitude less than 802.15.4, with the same range of coverage when devices are set up for indoor operation (22 mt). Finally, the architecture provides quite real time insightful information, asking for three orders of magnitude less of energy than a WSN architecture, assuring comparable range of coverage as shown in Fig. 6 and Table III of [3]. The scalability of the model is related to the scalability, in terms of people-things/mt^2, of RFID and of 802.15.4. Accuracy is not discussed because the aim of the work is tracking with approximation. The devices used are not directly available on the market but easily makable.

Privacy consideration. In this case, the utilization of ah-hoc target, could reduce the security vulnerabilities compared to commercial targets. Like all systems aimed to save energy, RFID is subject to several kind of attacks due to the lack of resources of computation. These systems, even if is more secure if compared with the past generation of tags, has several weaknesses [16]. Main risks coming from the possibility to compromise the tag, eavesdropping and rouge scanning attacks. That could result in privacy risks for data transmitted, for data authenticity and data observation. Anyway, the short range of the RFID technology reduce the possibility to attack the devices, the attacker should be very near to the target.

802.15.4 is a protocol that shows issues in term of security, the most important are Denial of Services attacks, attacks aimed to decrypt frames and reply attack [15]. The needs to save energy is a limitation to use all security features of the protocol.

Given the sensitivity of the data transmitted and the weakness of the protocol used, the architecture proposed left doubt about the privacy robustness. To improve the privacy, several counter measures are needed. Mostly, the personal information of the patients must be separated and anonymized by the data transmitted from the edge.

5.2 Case 2. "A Novel Architecture Using iBeacons for Localization and Tracking of People Within Healthcare Environment"

The purpose of the case, descripted in [4], is tracking patients and devices in a hospital, and provide insights related to the patient caring and the asset management.

The architecture is based on BLE iBeacon and RSSI technique to localize targets. To improve the accuracy of the centroid - RSSI a smoothing filter and an improved Least Square Estimation are used. The authors have chosen BLE because it is a very widespread technology, accurate and energy efficient. They discarded WiFi and RFID. Like reported by [8, 9], WiFi would require many APs to achieve accuracy of some meters, whereas RFID is accurate but requires dense infrastructure due the short range achievable. The architecture, reported in Fig. 3 of [4], involves some anchors in fixed and well-known positions, determined in previous works to achieve the optimal signal coverage. The practical maximum distance between the anchor and devices is claimed to be under 10 m. The mobile device should be a wearable, but a smartphone was used for the tests. It collects anchors RSSI signals along the path. This information is integrated with other parameters, accelerometer and gyroscopes information, to improve the accuracy and add on real time insights about patient conditions.

A phase of positioning and calibrating is needed (fingerprinting), then the data are collected by the application and sent to server via 4G/WiFi. A server elaborates information sent by smartphone to provide position. The server acts also as beacon manager, but it is not explained in which way it manages the bacons in term of communication protocols. In the experimentation, the beacons are four vertices of a parallelogram of 20 mt^2, there were 12 people, 16 computers, 32 chairs and tables, 2 WiFi routers. The devices were at 1.2 mt of height. The results, reported by Fig. 5 of [4], show that the system can achieve 37 cm of maximum error and 12.5 cm of average error. RSSI accuracy is really improved by LSE method.

Some words related to our metrics: the architecture presents a good cost given the commercial devices used, the coverage is quite limited and rely on BLE capabilities. The improved LSE returns good results, but nothing is said about the latency related to post elaboration. The energy consumption of BLE is one of the best technologies on the market.

Privacy consideration. This case leverage two wireless technologies BLE and WiFi/4G, this entails to expose the architecture to the weakness of both protocols. The architecture leverage on ad-hoc targets and, generally, reduce the privacy risks compared to a localization method based on smartphone application. Contiki is an operative system that is prone to several CVEs, mostly related to DDoS attacks. BLE [13] is a system that has been really improved in the recent past with the integration features to address parity, authentication, and encryption schemes, reducing the threats in security and privacy. Given that the target exchanges only distance information with anchors, (aggregation and elaboration are performed by the central architecture) the risks related the privacy

at edge and at network are low as well as the impact resulting. 4G protocol has some weakness in terms of security and privacy, it can receive sinkholes attacks via DNS and redirect packets. What is more critical is that the target device is a smartphone, that has a more extended attack surface compared to ad-hoc target devices. On the other hands, a smartphone has more capacity of computation and memory to adopt strong authentication and encryption algorithms. That, anyway, requires more energy. Further, WiFi Router [17], even using WPA3, allows the attackers to perform side-channel attacks, downgrade attacks, passphrase brute-force attacks and even DoS attacks.

5.3 Case 3. "Indoor Localization Using 802.11 WiFi and IoT Edge Nodes"

The purpose of the case, descripted in [5], is to create a system that provides localization of patients and medical staff in real time. The accuracy requested is at room level. The system, called LoCATE, is based on WiFi, with APs already deployed at the site, and Edge Nodes that are ad-hoc devices. The Authors chose ad-hoc devices instead of smartphone because of, often, healthcare's organization do not have smartphone policies. The idea to experiment a framework that provides localization services based on 802.11 via RSSI, which is notoriously one of the less accurate methods of localization, takes in primary consideration costs of the infrastructure. In fact, WiFi infrastructures are in place in almost all healthcare organizations. The Edge Nodes are built on a Raspberry Pi Zero with USB WiFi dongles, powered via a rechargeable lithium battery pack which grants 6/8 h of autonomy. Edge nodes operates in monitor mode (beaconing) when they scan for AP, and in upload mode when they communicate to a central serve a considerable change of position. The experimentation was done at James Madison University where a survey of 1/2/4 min for channel hopping took place to find most of the APs (4 min allows to discover all AP) from four different spots. The Fig. 1 of [5]. shows the architecture. The software took one minute to scan and elaborate signals, which results in a near real time localization. A trimming could improve the accuracy, but it is not impacting so much if compared with the average error recorded.

The results, reported in Table 1 of [5], show that coherent measurements are achievable, even if, some incongruent values are also present. The authors relate that incongruence with the presence of barriers. Anyway, errors could reach 60% against the expected distance. The AP that recorded the worst measures are the ones which have obstacles interposed with the spot.

To give a reference regarding Wifi localization based on RSSI, the [7] claims to achieve a mean of error of 3.7 mt and using a denser solution of APs per square meters achieves 1.5 mt mean of error (18AP per 100 mt^2). The proposed model is very rough in terms of accuracy and in terms of variance of the measures. The time required to discover the APs could be an insurmountable limitation that restricts drastically the scope of the application to some static scenarios. The architecture is largely available, often already in place and not complex. There is not information about scalability.

Privacy consideration. In this case, the authors given some indication about how to manage security and privacy concerns, recognizing the sensitiveness of the data managed. The authors take in consideration the risks related to the data transmission and the attacks like spoofing or side-channel. They want to avoid the tracking of the devices and the

patients path reconstruction. To reduce these risks, they employ an AES-128-GCM for authentication and encryption and 802.1x to authenticate the devices.

Anyway, the analysis seems to be uncomplete, indeed the device based in Raspberry Pi is prone to some attacks that could result in unauthorize access and in denial of service [19]. Further, as already mentioned in the previous case, WiFi has several security concerns still.

5.4 Case 4: "DeFi: Robust Training-Free Device-Free Wireless Localization with WiFi"

The purpose of the case, descripted in [6], is to create an architecture based on commercial WiFi devices to provide localization information both devices-free and training-free. Devices-free method of localization is very suitable for healthcare industry because carrying on devices or wearable sensors could be inconvenient for elder and children. The methodology proposed to implement devices-free model leverage the distortion and the fluctuation of transmitted signals to establish the location of the target. Usually, that is achieved via both mathematical methods and machine learning algorithms. These methodologies use time consuming and labor-intensive offline learning activities, which are prone to environmental changes. The approach proposed, called DeFi, is aimed to avoid learning activities, estimating the target location by refining the angle-of-arrival (AoA) of the signal reflected by the target, using just out of shelf APs. To achieve that object is basic to identify the reflection paths of the signal from the transmitter to the receivers. To do that, it is needed to have N antennas to discriminate N-1 reflection paths and, empirically, eight antennas are required in almost of all real cases. Given that commercial APs hardly are equipped with eight antennas, CSI (available on new models of APs) have a key role because it provides the phase shift information from the subchannel, and this allows to simulate more antennas. Even ten time more than the physical antennas installed. In this way it is possible estimate both AoA and the related ToF. The Fig. 1 and Fig. 2 of [6], shows the geometry of the AoA method and the paths of the signal. The implementation consists in three steps.

- Calibration, a phase of calibration is required to eliminate random phase across sub-channels, drift by Sampling Time Offset. Commercial AP are imperfect in hardware and loosely synchronized in the transmitter - receiver pairs.
- Estimation of AoA via the MUSIC algorithms to extract key signal parameters.
- A joint AoA and ToF estimations to refine the evaluation.

Given the three steps above, the phases to estimate AoA are following summarized:

- Identify and eliminate static paths (background). Using the high correlation of samples of static paths is possible eliminating background.
- Separate out the target reflection path from the motion path via a likelihood criterion. To identify direct reflection path, a target reflection paths refinement is needed. It is possible assuming that direct path is the shortest one and has the minimum ToF. Also, direct reflection path produces the smaller variation of AoA compared to other paths. By a likelihood criterion, the reflection paths are separated out from the motion

paths, and it is possible leverage the informative AoA estimation of the target direct reflection path to estimate the target location.

- Make the evaluation of AoA reliable, even in challenging conditions, via a particles filter. Due to the complex signal propagation characteristics, it is possible that large errors in the AoA estimations are recorded, that leads to poor target location estimation. The Particles Filter is a Bayesian filter which estimates the posterior probability distribution function (Fig. 6).

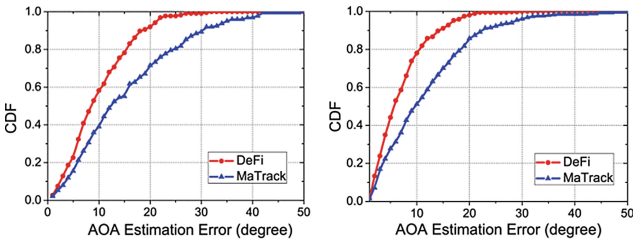

Fig. 6. AoA methods estimation of error in CDF in laboratory (a) and lobby (b) [6]

The model depicted is extended to all receivers and the target position is estimated thought the intersection of the probability distribution function of each receiver.

In the experimentation were involved a lobby (36 mt^2) and a laboratory (48 mt^2) with chairs, desks, and computers. One mini pc, equipped with an AP, operated as transmitters and four APs were used as receivers. Transmitter sent packets every 1 ms on channel 132 of the 5 GHz spectrum, and the receivers provide CSI information that are elaborated by a server. The server applies all concepts above descripted and perform a triangulation. Also, the impact of receivers was evaluated increasing from two (that is the desiderata) to four, it returns a reduction of median localization error of 13%. Finally, the number of particles impacts as well, 100 particles needed to get the saturation in localization error. In conclusion, in the lobby, the system returns a mean error of 0.47 mt with a variance of 0.07 mt. Figure 6 of [6] shows the cumulative distribution functions of the localization errors that results from tests in laboratory (a) and lobby (b).

The experimentation is well arranged and complete in the analysis of parameters. Anyway, no information is given about complexity of calculation and its latency, scalability, and range of coverage to face a real environment with many people. Concerning costs, the devices used are out of shelf but an high density is required in the test. The power consumption is practically zero given the lack of devices. Further works should analyze multi targets in a noisier environment.

Privacy consideration. In this case there are not issues related to edge of the networks. Indeed, there are not devices to be identified and traced and there are not sensitive data to be transmitted. Consequently, the approach does not require authentication and encryption. Even if the attackers could track a target, leverage the weakness of WiFi, them should discover the link between the path of the target and the people related with. Also, tracking a target is not so simple because the location of the target is obtained

by a complex analysis of many signals coming from all the receivers. The architecture is prone to all the weakness of WiFi and to risks related with. Giving the opportunity to the attacker to reduce the performance and denial the service, manipulate the signal and corrupt data. As mentioned, almost all anchors should be compromised localize the target.

6 Comparison

The final part of the survey is aimed to compare the cases selected. To make the reading easy, the Fig. 7 reports a synthesis of the analysis done with some notes related to the framework of reference defined. The scale of evaluation is created on the base of the measures reported by cases, normalized in a scale of 0–10. For the KPIs not included in the description of the cases, we take in account the estimation reported in the Table I of [10] and in the the Table II of [2].

Following a brief description of the parameters of evaluation of their meaning.

Case			
	Object	***Method***	***Note***
1	Patient/assets tracing, vitals recording, emergency alerts with localization	Hybrid: 802.15.4 + RFID • Devices based (ad hoc) • Proximity • No post elaboration • RFID scalability • RFID coverage (11mt) • Costs in average • Power consumption the best • Accuracy less than the avg (mt) • Latency no reported	To use when is required: high energy efficiency, accuracy in meters, coverage in meters, average market costs and no latency.
2	Patients/assets localization, localization for emergency alerts	BLE iBeacons, Out of Shelf beacon • Device based (Smartphone) • RSSI device-anchors distance • Post elaboration LSE+Smoothing filter • BLE scalability • BLE coverage (mt) • Costs in average • Power consumption better than avg • Accuracy the best (cm) • Latency not reported but existing	To use when is required: high accuracy (in cm), good energy efficiency, average market costs, coverage of meters is acceptable, dense infrastructure is acceptable, latency is not required in very real time.
3	Localization of patients and medical staff in real time	802.11 OFS • Devices based (ad hoc Raspberry) • RSSI • Post Elaboration No • WiFi scalability • WiFi Coverage the best (x100mt) • Costs better than the avg • Power consumption less of the average • Accuracy the worst (mt) • Latency 1 min	To use when is required: large coverage, high scalability, low costs, accuracy is acceptable in tens of meters, power consumption is not a problem, one minute of latency
4	Localization of patients	802.11 OFS • Devices free • RSSI • Post Elaboration No • Scalability to be investigated more • Coverage less than the avg • Costs the worst due the infrastructure • Power consumption the best • Accuracy better than the avg (cm) • Latency not reported but likely impacting	To use when is required: zero power consumption, zero cost of devices, accuracy in tens of meters, coverage acceptable in ten of meters, cost of infrastructure above the average.

Fig. 7. Summary of the cases analysis

- Range of coverage – reported by the cases, it means how many infrastructural devices are used by square meters. The lower the better.
- Latency – not reported by cases, it means how match time is needed to have the localization once it has been measured. The case 3 asks minutes to prepare the measure because of the multi-hopping action to discover all reachable APs Even if, in a real case, it could be a too long time to consider the solution applicable, it does not impact on latency, indeed once the multi-hopping is completed the localization is available in real time The case 4 could require of a consistent post elaboration time. The case 2 asks for some post elaboration, less than the case 4 and more than the case 1 and 3. The case 3 takes 1 min to export the position of the target. To take in consideration this scenario a score of 10 is given to the case with no post elaboration, zero to the case 4, 5 to the case 2. The lower the better.
- Accuracy – reported by each case, it means the average error to localize the target. The lower the better.
- Power consumption/Energy Efficiency – not reported by all cases, it means how much energy is needed to feed mobile devices. It is complex to compare the cases because of the measurements are not directly comparable. The [23] reports a comparison among WiFi, BLE and 802.15.4. Assuming that most of the time the device target is in sleeping, then it is in beaconing mode and sometimes it transmits/receives data mode. BLE is the most energy efficient technology, 802.15.4 absorbs about 145% more electricity than BLE, and, finally, WiFi requires five time more of energy compared to BLE. The power consumption of the case 4, device-free, is esteemed almost zero. The authors of the case 1 claim to achieve three orders of magnitude less than 802.15.4 using RFID in BAP mode. The lower the better.
- Scalability - not reported by cases. Scalability means how many targets are sustainable for square meters. About the case 4, it is very hard to talk about scalability, [20] shows that it is possible to manage multi-target scenarios with 80% of error about present entities. On the other hand, it is possible estimate how many targets WiFi and BLE can manage but, at the same time, these technologies are prone to interferences and obstacles, so even in these cases is not too easy esteem in term of number of target detectable/error measured. More research is required to have a precise evaluation, so, we assume this parameter according to [10]. The higher the better.
- Costs – this is related to the costs of the solutions. To esteem the cost of architecture selected, are taken in consideration both the costs of the targets and the cost of the infrastructure used for the implementation. To normalize the cost of the infrastructure, it is normalized by per square meters. The lower the better.
- Privacy – the privacy evaluation is threated apart. A qualitative evaluation is provided on the base of the security risks related to both edge and network, the likelihood of the attacks and the consequences of the attacks.

To make the comparison as more readable as possible, all metrics are reported in the higher the better fashion even if the metrics are naturally evaluable as the lower the better, these are converted in complement of ten.

The Fig. 8 shows the comparison among the cases selected by the means of a radar.

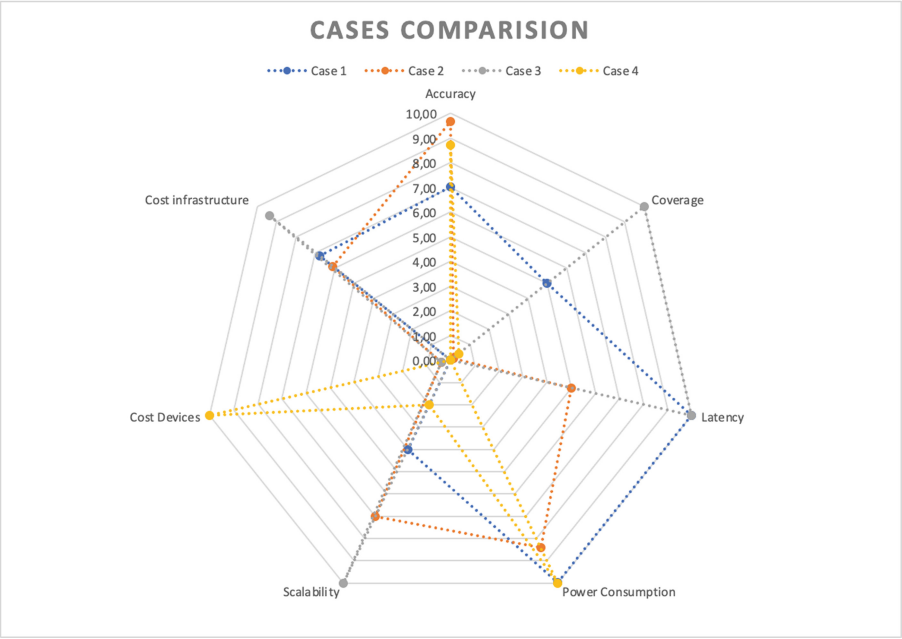

Fig. 8. Cases comparison by radar graph

The case 1 has the best compromise. This is a solution suitable for case where accuracy is acceptable in meters and the power consumption is key. The cost of the devices, generally, is affordable, even if it is poor compared with the other cases. The case 2 is excellent for accuracy and power consumption. The limited coverage does not affect the costs of the infrastructure. Latency and scalability are around the average and devices are generally affordable. The case 3 is clearly suitable for use cases that require low cost, high coverage but accuracy and power consumption should be not a key factor. The case 4 provide the very intriguing opportunity to localize people in devices-less fashion. This is a real step forward in terms of power consumption and easiness of adoption. The solution works very well in term of accuracy and, of course, in term of power consumption and cost of devices. The cost of infrastructure is poor compared to the other cases because a high density of APs is required, but WiFi device could be found already in place in many network infrastructures. Anyway, that solution needs of a complex post elaboration phase that is not evaluated in the case neither in term of costs nor of latency. To complete the evaluation, it should be investigated the scalability of the system, in other words, how the solution behaves in a multitarget scenario. In the end, the case 2 seems to be the most balanced solution because of do not has important weaknesses.

Consideration on privacy. From the privacy perspective we can split the risks in two categories, risk from network and risk form edge both reported by Fig. 4. About the edge, the case 1 is the most exposed because of the weakness of both the RFID protocol and the tag. Also, a successful attack to the RFID tag results immediately in accessing

to the vital data of the patients and tracking the path of the target. The case 2 leverage a smartphone device, that has weakness related to the operative system and to the Apps installed. The case 3 leverage a Raspberry target that is prone to unauthorized accesses to the device and to denial of service. The case 4 do not use any target device. The attacks to the network can target both the anchors and the target devices. In the second case, the attacks can be risky for the privacy in terms of data exfiltration, device tracking, denial of the service, data manipulation. Attacking the anchors hardly affect the privacy. Indeed, to collect data about a target entail the corruption a significative number of anchors. Instead, attacks to the anchors, and to edge as well, can result very impactful as a first step to access centralized data. Among the protocol used, the WiFi results exposed to attacks also because of its wide range of coverage that allow the attackers to avoid being near the target. The protocol could be prone to device tracking, brute-force, side-channel, denial of service and so on. BLE is prone to several attacks, but recent developments have improved its security, especially regarding to the tracking of the device, but it remains prone to eavesdropping and man in the middle attacks. 802.15.4 is prone to denial of service, frame decrypt and reply to attacks. The case 4, that does not use target devices, is less prone to privacy risks because of it does not transmit data at all, even tracking the target entail a complex attack to the infrastructure. Finally, WiFi seems to be the protocol most exposed to be attacked and risky for the privacy as well as RFID is the weakest device prone to consequences about privacy.

7 Conclusions and Future Works

Even if the comparison among the four cases selected is not simple to yield, by the mean of a framework of key parameters it emerges clear when the solutions investigated are suitable. In this moment in time, BLE based architecture seems to be the most balanced even in terms or privacy risks. WiFi based architecture is excellent for coverage, costs, and latency but is weak for accuracy, power consumption and privacy. RFID based architecture is something in the middle, excellent for power consumption and latency, weak for privacy and in the middle for the other parameters. Device free architectures are very promising from the perspective of energy consumption and accuracy, but some elements require of further investigation, the impact of a complex post elaboration phase effort for latency and costs, and accuracy in multi-targets scenarios. The most real risks in term of privacy are related to device tracking, data observation/corruption and limitation of service. Risks that coming from the attacks to devices are more likely and impact on a single target. The attacks to the networks could involve many targets and are mostly oriented to denial of services. A most critical and likely scenario is when attackers use edge and network to escalate towards the datacenter.

The analysis of the cases selected leaves some point of further investigation to provide a more complete scenario. It is possible split the improvement in two typologies:

- Vertical improvement: further investigation about the parameters that are not clearly threated by the case. For instance, the behavior of the architecture in terms of scalability and latency in a multi-target environment as well as the costs/time required by post elaboration computations. It is also possible to provide a set of suggestions to improve the cases analysis is another important domain of further studies.

- Horizontal improvement: extend the framework with more parameters and extend the number of cases analyzed, adding solutions tested in actual environments that employ other and different architecture to localize targets.

This approach improves the analysis done and provide the opportunity to extend the scope of the analysis and its applicability in terms of use case requirements.

References

1. Mckinsey Digital: Unlocking the potential of the Internet of Things, 1 June 2015|Report. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world. Accessed 15 May 2022
2. Zafari, F., Gkelias, A., Leung, K.K.: A survey of indoor localization systems and technologies. IEEE Commun. Surv. Tutor. **21**(3), 2568–2599 (2019). https://doi.org/10.1109/COMST.2019.2911558
3. Catarinucci, L., et al.: An IoT-aware architecture for smart healthcare systems. IEEE Internet Things J. **2**(6), 515–526 (2015). https://doi.org/10.1109/JIOT.2015.2417684
4. Nguyen, Q.H., Johnson, P., Nguyen, T.T., Randles, M.: A novel architecture using iBeacons for localization and tracking of people within healthcare environment. In: Global IoT Summit (GIoTS), pp. 1–6 (2019). https://doi.org/10.1109/GIOTS.2019.8766368
5. Salman, A., El-Tawab, S., Yorio, Z., Hilal, A.: Indoor localization using 802.11 WiFi and IoT edge nodes. In: IEEE Global Conference on Internet of Things (GCIoT), pp. 1–5 (2018). https://doi.org/10.1109/GCIoT.2018.8620162
6. Zhang, L., Gao, Q., Ma, X., Wang, J., Yang, T., Wang, H.: DeFi: robust training-free device-free wireless localization with WiFi. IEEE Trans. Veh. Technol. **67**(9), 8822–8831 (2018). https://doi.org/10.1109/TVT.2018.2850842
7. Zhang, L., Wang, H.: 3D-WiFi: 3D localization with commodity WiFi. IEEE Sens. J. **19**(13), 5141–5152 (2019). https://doi.org/10.1109/JSEN.2019.2900511
8. Mainetti, L., Patrono, L., Sergi, I.: A survey on indoor positioning systems. In: 22nd International Conference on Software Telecommunications and Computer Networks (SoftCOM) (2014)
9. Van Haute, T., et al.: Performance analysis of multiple Indoor Positioning Systems in a healthcare environment. Int. J. Health Geogr. **15**(1), 13–15 (2016)
10. Stojanovic, D., Stojanovic, N.: Indoor localization and tracking: methods, technologies and research challenges. Facta Universitatis Ser. Autom. Control Robot. **13**, 57–72 (2014)
11. Homepage page Regulation EU. https://www.privacy-regulation.eu/. Accessed 14 May 2022
12. Homepage CNIL PIA. https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf. Accessed 14 May 2022
13. Cäsar, M., Pawelke, T., Steffan, J., Terhorst, G.: A survey on Bluetooth Low Energy security and privacy. In Computer Networks **205**, 108712 (2022). https://doi.org/10.1016/j.comnet.2021.108712. ISSN 1389-1286
14. Ahmadi, P., Islam, K., Maco, T., Katam, M.: Survey on internet of things security issues and applications. In: International Conference on Computational Science and Computational Intelligence (CSCI), pp. 925–934 (2018). https://doi.org/10.1109/CSCI46756.2018.00182
15. Reziouk, A., Laurent, E., Demay, J.: Practical security overview of IEEE 802.15.4. In: International Conference on Engineering & MIS (ICEMIS), pp. 1–9 (2016). https://doi.org/10.1109/ICEMIS.2016.7745382

16. Garcia-Alfaro, J., Herrera-Joancomartí, J., Melià-Seguí, J.: Security and privacy concerns about the RFID layer of EPC Gen2 networks. In: Navarro-Arribas, G., Torra, V. (eds.) Advanced Research in Data Privacy. SCI, vol. 567, pp. 303–324. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-09885-2_17
17. Zahariev, P., Hristov, G., Kinaneva, D., Chaisricharoen, R., Georgiev, G., Stoilov, P.: A review on the main characteristics and security vulnerabilities of the wireless communication technologies in the Industry 4.0 domain. In: Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON), pp. 514–517 (2022). https://doi.org/10.1109/ECTIDAMTNCON53731.2022.9720331
18. Abdul-Ghani, H.A., Konstantas, D.: A comprehensive study of security and privacy guidelines, threats, and countermeasures. J. Sens. Actuator Netw. **8**, 22 (2019). https://doi.org/10.3390/jsan8020022
19. Sainz Raso, J., Martin, S., Diaz, G., Castro, M.: Security vulnerabilities in Raspberry Pi–analysis of the system weaknesses. IEEE Consum. Electron. Mag. **8**, 47–52. https://doi.org/10.1109/MCE.2019.2941347
20. Seifeldin, M., Saeed, A., Kosba, A.E., El-Keyi, A., Youssef, M.: Nuzzer: a large-scale device-free passive localization system for wireless environments. IEEE Trans. Mob. Comput. **12**(7), 1321–1334 (2013). https://doi.org/10.1109/TMC.2012.106
21. Di Martino, B., Mastroianni, M., Campaiola, M., Morelli, G., Sparaco, E.: Semantic techniques for validation of GDPR compliance of business processes. In: Barolli, L., Hussain, F.K., Ikeda, M. (eds.) CISIS 2019. AISC, vol. 993, pp. 847–855. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-22354-0_78
22. Campanile, L., Cantiello, P., Iacono, M., Marulli, F., Mastroianni, M.: Risk analysis of a GDPR-compliant deletion technique for consortium blockchains based on pseudonymization. In: Gervasi, O., et al. (eds.) ICCSA 2021. LNCS, vol. 12956, pp. 3–14. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-87010-2_1
23. Kazeem, O., Akintade, O., Kehinde, L.: Comparative study of communication interfaces for sensors and actuators in the cloud of internet of things. Int. J. Internet Things **6**, 9–13 (2017). https://doi.org/10.5923/j.ijit.20170601.02