2016 30th International Conference on Advanced Information Networking and Applications Workshops

WiFACT – Wireless Fingerprinting Automated Continuous Training

Walter Balzano, Aniello Murano, Fabio Vitale
Dipartimento di Ingegneria Elettrica e Tecnologie dell'Informazione
Università degli Studi di Napoli Federico II
Email: {walter.balzano, aniello.murano}@unina.it
fvitale86@gmail.com

***Abstract*—The increasing importance in ubiquitous computing and context-dependent information has led in the last years to a growing interest in location-based applications and services. A considerable market demand concentrates on indoor localization tasks. In this setting, *WiFi fingerprinting* is currently one of the most popular and widespread techniques as it provides reasonable positioning accuracy while being able to exploit, at the same time, existing wireless infrastructures.**

WiFi-fingerprinting systems mainly operate though two distinct phases: one initial, named *training*, in which signals are collected and one subsequent, named *usage*, in which the recorded data are used to localize users.

While the usage phase is fast and effective, the training phase is time consuming. Moreover, to maintain a localization accuracy, the training needs to be repeated anytime the network structure changes. The latter may occur, for example, if an access point goes off-line or it is (re)moved.

In this paper, we propose a novel framework that allows for an automatic and continuous training in WiFi-fingerprinting systems, which is based on an opportune deployment of a WSN (*Wireless Sensor Network*). Precisely, the solution we propose allows for an efficient real-time updating of the database collecting the signals, without any human intervention.

Keywords: WiFi fingerprinting, indoor localization.

I. Introduction

Indoor localization is an important field of research that aims to provide accurate location-contextual information to the users [1, 2, 3, 4, 5, 6, 7, 8]. In recent years, the popularity of mobile and pervasive computing has further stimulated the research in this field. Many solutions have been introduced to provide room-level location-based services such as locating a person or a computer in a house.

In outdoor environments, localization is possible with GPS systems. These kind of systems, however, may present problems indoor where satellites are not visible, so methods to achieve reliable positioning are still under research.

In the last years several localization techniques have been proposed, some leveraging on WiFi and GSM cells, some based on body-mounted sensor systems like accelerometers and gyroscopes to detect user movement [9]. Also, hybrid solutions have been exploited by making use of ad-hoc systems able to process location dependent information combining data from sensors (accelerometer, compass, gyroscope) and heterogeneous receivers (GPS, WiFi, RFID, bluetooth beacons like iBeacon, and the like) [10, 11, 12, 13].

Nowadays, widespread solutions mainly exploit range-based WSN solutions for indoor user positioning [5], to estimate the position of the user relative to a set of fixed sensors, whose position is known a priori. One of the most popular and powerful solution in this setting consists of *WiFi-fingerprinting based systems* [14], which provides reasonable position accuracy while exploiting existing wireless infrastructures. Unlike other radio navigation techniques, fingerprinting is not geometrical, i.e. the position calculation does not rely on angles or distances but it's only based on existing wireless RSSs (*Received Signal Strength*).

The way WiFi fingerprinting based systems work is simple and efficient. In each place the set of all access point BSSIDs (MAC addresses of the wireless transmitters) and their RSS forms a unique *fingerprint*. All the fingerprints in the interesting area generate a database which is called *RadioMap*, which is then used to localize the users.

In this paper, we present *WiFACT*, a module that allows for an automatic and continuous training phase, enhancing any WiFi-fingerprinting based-location system over time. Any variation, either environmental or network-related (addition, moving or failure of any access point), triggers a database update, allowing clients to rely on a more accurate and recent RadioMap.

II. Related work

Indoor localization systems are receiving a lot of attention in the industry. The recent popularity of mobile and pervasive computing has further stimulated the research in this field. We report some lines of research that are related to the WiFi-fingerprinting approach we consider.

SMARTPOS [15] is an indoor positioning system that uses the combination of a (deterministic) WiFi fingerprinting and a digital compass. It can be deployed standalone on a mobile phone and considers the user's orientation to use only a part of the fingerprint database. During the training phase, for each position the system needs four different fingerprints, which are then used according the the user position in space.

In *"A system for LEASE: Location Estimation Assisted by Stationary Emitters for IndoorRF Wireless networks"* [16] the authors have developed an algorithm to generate a

978-1-5090-2461-2/16 $31.00 © 2016 IEEE
DOI 10.1109/WAINA.2016.137

radio model using *sniffer* and *transmitters* modules. These modules are carefully deployed in the interesting area and are used to analyze wireless signals behavior and interpolate data for every point of the map, generating a dynamic RadioMap but relying on the existing signal communication infrastructure.

SurroundSense (mobile phone localization via ambience fingerprinting) [17] is a mobile phone based system that explores logical localization via ambience fingerprinting. Precisely, this approach uses any data available to a mobile device, such as ambience sounds, lighting and, of course, available WiFi networks.

Fingerprinting systems are also used to localize users outdoor, allowing reduced battery consumption while still granting a good accuracy. It is possible to use GSM cells (lower accuracy, with error up to 2km) or WiFi networks available in the neighborhood.

Inevitably, every system that makes use of additional sensors, besides those related to the WiFi networks, needs to pay an extra battery consumption. As these systems are designed to work on mobile devices like smartphones, it is important to keep the energy consumption as low as possible.

ZiLoc: energy efficient WiFi-fingerprinting based localization with low-power radio [18] uses an interesting approach to reduce energy consumption, replacing normal 802.11 networks with IEEE 802.15-4 networks (*ZigBee* receivers and transmitters) which use little energy, allowing to build an extremely efficient localization system. However, offline training phase is more complex requiring access point recognition via *beacon phases* and comparison of values via *nearest neighbor* method. Precision is similar while battery consumption is reduced up to 66%.

OUTLINE

The rest of this paper is organized as follows. In Section III we introduce WiFi-fingerprinting based systems. In Section IV, we introduce the layout of the developed WiFACT module. In Section V, we report a case of study in order to show how WiFACT works. Finally in Section VI we report some conclusion and future work directions.

III. WIFI-FINGERPRINTING BASED SYSTEMS

In this section we briefly recall the main aspects of WiFi-fingerprinting systems used in indoor localization. We refer to [14] for more details.

WiFi-fingerprinting systems exploit available wireless networks in a designated area to offer positioning and location-based services. In some specific locations, the set of all the access points detected, together with their own signal strengths, form a unique fingerprint that can be saved in a database for subsequent pattern matching.

Most WiFi-fingerprinting systems have two distinct phases: *training* and *usage*. In the training phase, several fingerprints in the area of interest are recorded and associated with their location in a database, which is called *RadioMap* (see Table I). In the usage phase, the client sends detected RSSs to a localization server, which applies a pattern matching algorithm against the RadioMap to estimate user location. The training phase is normally manual. An operator physically covers the area identifying places in order to build the database. Also, he has to recalibrate the entire area in case the locations of any access point previously recorded changes. If the area to be covered is large, this operation can be time-consuming. Moreover, the quality of the RadioMap largely depends on the amount of spots analyzed by the operator.

Location	**BSSID**	**RSS**
A	f0:7d:68:fb:4d:3f	-40dBm
A	00:0f:3d:0a:40:ea	-74dBm
A	9c:d6:43:2f:07:3c	-65dBm
B	f0:7d:68:fb:4d:3f	-72dBm
B	00:0f:3d:0a:40:ea	-56dBm

Table I: RadioMap with two different fingerprints.

There are several available algorithms to find an accurate position from a low-definition RadioMap. Basically, it's possible to find the *closest match* via the formula

$$\min_{i=1\to m}\left|\sqrt{\sum_{i=1}^{m}\left[SS_{RM}(i,j)-SS_{UM}(i)\right]^{2}}\right| \quad j=1\to n \quad (1)$$

where $SS_{RM}(i,j)$ is the signal strength of the i-th access point in the j-th fingerprint in the RadioMap and $SS_{UM}(i)$ is the signal strength of the access point i as it is seen by the user. The RadioMap point j which has the minimum norm is considered to be the most probable location [19].

If the RadioMap holds many fingerprint locations, a simple algorithm like the one above grants sufficient accuracy whilst maintaining low algorithmic complexity. However if the RadioMap is *sparse* it is possible to approximate a user position via interpolation between different fingerprints.

Consider data reported in Table I, in particular regarding location A. The three records represent three different access points transmitting. Over time, these RSSs will change, due to interferences, network modifications and environmental changes, but the fingerprints stored in the RadioMap will only get updated after a new training phase. Until then, the system will not be able to properly localize users in the interesting area.

A. Fingerprinting systems quality evaluation method

Fingerprinting systems can be evaluated over three main characteristics:

- **density** or **definition** – depends on the number of fingerprints recorded in different places. A higher def-

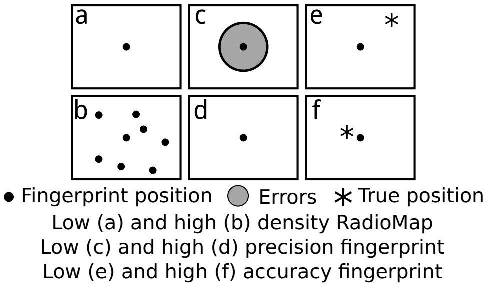
a
c
e
b
d
f
● Fingerprint position
Errors
∗ True position
Low (a) and high (b) density RadioMap
Low (c) and high (d) precision fingerprint
Low (e) and high (f) accuracy fingerprint

Figure 1: RadioMap and fingerprints quality evaluation.

inition allows better approximation of the true user position over the time (Figure 1, (a) and (b));

- **precision** – depends on the number of samples recorded in a single place, which are then filtered to reduce noise (figure 1, (c) and (d));
- **accuracy** – depends on the distance between the position where the fingerprint has been recorded and the position selected on the map: if the fingerprint is well placed during the training phase, the system has higher accuracy (figure 1, (e) and (f)).

In optimal conditions, WiFi fingerprinting systems achieve a precision up to 1-3m which, however, degrades over time due to interferences, obstacles and changes in weather conditions like humidity, pressure and temperature [18].

IV. WiFACT LAYOUT

We now introduce the WiFACT system we have developed, along with its main characteristics.

The WiFACT system is composed of a user-segment used for localization, with a network of WiFi receivers connected via a WSN, which are used for real-time tracking of the network status.

A. WSN segment

In this section, we describe the modules, the nodes and the network topology of the WSN segment.

For the WSN we build modules using a XBee transmitter (which is based on ZigBee protocol) (see IV-B) connected and managed by a Arduino microcontroller.

There are 3 kinds of nodes in the network:

- **coordinator**: it is the most important kind of node in the network and there is exactly one of such a node for each network. It assigns network addresses to every other node and guarantees that the network is working;
- **router**: the most common kind of node in a WSN, is able to send and receive informations from other nodes as well as reroute data received to other nodes;
- **end device**: it is the simplest kind of node in the network and is able to receive and send information, but not to route data to other nodes. This kind of node can only connect to routers or coordinators nodes.

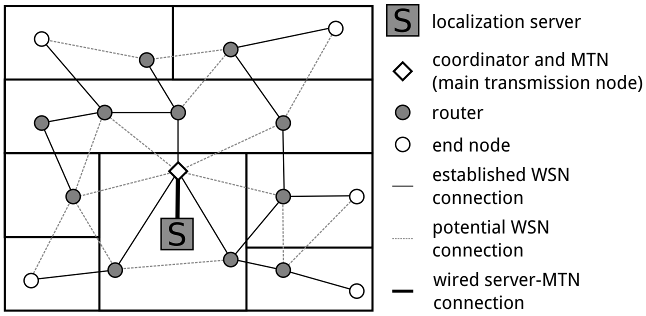
S
S localization server
coordinator and MTN (main transmission node)
router
end node
established WSN connection
potential WSN connection
wired server-MTN connection

Figure 2: Example of WSN structure.

Network structures can be very simple. It is possible to have networks consisting of just two nodes connected, such as the coordinator connected with an end device. In general, however the network structure can be very complex. For example we can have the following topologies:

- **star**: a coordinator node is in the center of a group of end devices. In this case, every message of the system goes through the coordinator. This is a quite simple network structure and is useful to cover small areas;
- **cluster tree**: a coordinator node is connected to all the routers, and every router can be connected to one or more end devices. Routers are not interconnected. This topology is used to cover small-to-medium areas;
- **mesh**: the coordinator and the routers are interconnected. Routers can be connected in cascade and the network can be very large. This topology is very flexible and can be used in any situation, but it is truly useful in big areas.

B. ZigBee networks and XBee modules

ZigBee is a set of network protocols [20], based on IEEE 802.15.4 protocol, that use small and low-powered digital antennas to implement simple WPAN (*wireless personal area network*) networks. The ZigBee protocol is normally used to implement WSNs due to its low power consumption and low cost per-module.

Using the ZigBee protocol offers several advantages over IEEE 802.15.4 underlying protocol:

- **routing**: defines how the messages move through the network to get to the main node;
- **ad hoc network creation**: the whole structure is automatically built without human intervention;
- **self-healing mesh**: if any node is missing the network auto-reconfigures to replace damaged connections and to restore functionality.

XBee is a brand name for modules that implements the ZigBee protocol. XBee modules are very small (less than 1 inch wide) and cheap, and are available in two form-factors, *Through-Hole* with a rigid antenna and *Surface Mount* with wired soft antenna.

Fingerprint in p_0 at t_0	**BSSID**	**RSS**
	f0:7d:68:fb:4d:3f	-40dBm
	00:0f:3d:0a:40:ea	-74dBm
	9c:d6:43:2f:07:3c	-65dBm
Fingerprint in p_0 at t_1	**BSSID**	**RSS**
	f0:7d:68:fb:4d:3f	-38dBm
	00:0f:3d:0a:40:ea	-74dBm
	9c:d6:43:2f:07:3c	-55dBm

Table II: Differences found at times t_0 and t_1 in a discovered fingerprint, with respect to a fixed location.

Algorithm 1 New RadioMap calculation.

```
Input: RadioMap, wifiNetwork, wifactWsn
Output: RadioMap
for sensor in wifactWsn do
    for [bssid, rss] in sensor do
        oldRss $\leftarrow$ RadioMap.search(sensor, bssid)
        if oldRss $-$ newRss $<$ threshold then
            newRss $\leftarrow$ interpolate(oldRss, rss)
        else
            // difference is big, replacing old data
            newRss $\leftarrow$ rss
        end if
        RadioMap.save(sensor, bssid, newRss)
    end for
end for
return RadioMap
```

C. Training segment with the WiFACT network

The implementation of the training segment comes in two distinct phases: a *distribution* one (with the WSN configuration) and a *tracking* one, in which the network is used to find informations on the available WiFi networks.

1) Distribution and configuration phase: Distribution and configuration phase is very important to obtain higher precision and reliability.

- **network topology** must be identified in relation to the surface to cover (star, cluster tree, mesh);
- **network coordinator** should be as close to the center as possible. Normally it's directly connected to the database server (Figure 2);
- **modules** are then distributed in the area, linking every identifier with a physical position (room, coordinates on area map).

If any module needs to be moved, its position or identifying name must be updated.

During the distribution phase it is very important to take care of every node position. Every module must be able to connect to at least another module in the WSN. As the networks generated by XBee transmitters are redundant, reachability of more than one other node is desirable as it enhances reliability of the network against failures.

2) Tracking phase: During the tracking phase, every sensor sends detected wireless data through the WSN with its identifier. These data are gathered in the *main transmission node* which relays them to the server. The server filters data to reduce jitter and errors and replaces and integrates the previous data in a more accurate and updated RadioMap.

This structure allows to rapidly detect network structure changes (like a failure or a wireless transmitter that has been moved or replaced) and enviromental changes which can alter RSSs (like air humidity and pressure variations).

D. Advantages of an overlying infrastructure

WiFACT uses an overlying infrastructure to gather data from the access points. While having slighter higher deployment cost (even if modules are very cheap), such approach has several advantages:

- **network-agnostic**: the WiFACT modules only needs to use the underlying wireless network protocol in tracking components, as intercommunication between modules is always done via IEEE 802.15.4 protocol. Modules need no network-related configuration, and tracking components can be added or replaced if needed to follow underlying network protocol modifications;
- **automatic quality improvement**: provided they use the same wireless protocol, WiFACT uses any AP available, and is able to use APs which are not part of the underlying network infrastructure, allowing better accuracy;
- **reliability**: being independent from the underlying network, in case of a failure WiFACT keeps functioning and reflects the new network status in a matter of seconds;
- **energetic independency**: modules may be deployed in places where there is no electricity available. WiFACT modules can be battery-operated and can last for several months as they use very little power.

E. Dynamic network extension

Since the WSN network configuration is automatic, it is possible to add new modules to the existing network with little effort. It allows, for example, to extend the localization training to new rooms, or to change network density locally to obtain different levels of precision in each zone.

F. User segment

The proposed system is just an upgrade to the classic training phase, which is present in any fingerprinting-based system. The training phase is normally a manual and time-consuming operation, which must be repeated often to guarantee system reliability. The developed module can be adapted to any previous localization algorithm, improving accuracy through more precise and updated data.

The user segment can be composed of simple mobile devices, equipped with WiFi receiver, and an application that allows to:

1) passively read data on available networks;
2) request the RSSs-based position to the servers;
3) receive and display user position from the server.

V. Testing and system evaluation

For testing purposes, we have built an Android application to gather raw wireless data every 2 seconds, simulating a WSN behavior via WiFi. The test devices have recorded data for 45 minutes and sent them to a database server. The two modules, simulated via a LG Nexus 4 (S_1 in figure 4) and a ASUS Nexus 7 (S_2 in figure 4), running Android 5.1, have been placed in distant spots, so they are able to record different fingerprints.

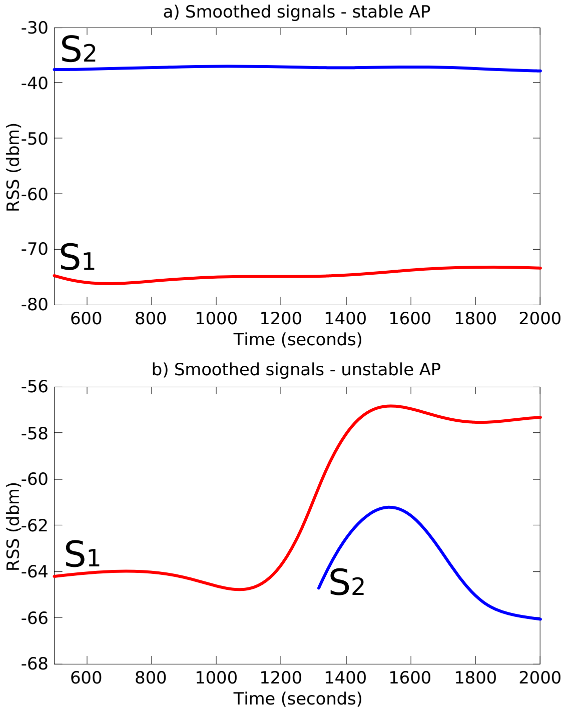

Figure 3: Examples of network signal graph.

Data was smoothed using *Tikhonov regularization* in GNU Octave with a regularization parameter (lambda) of 0.1 and a smoothing derivative of 3. These values allow an accurate definition of the true behavior of the network signals, drastically reducing spikes and allowing greater accuracy in the test system.

In Figure 3a data show that a *stable* access point (B in figure 4), which is always in the same position, has little variations over the time in RSS for both modules.

After 20 minutes, one access point has been moved from A_1 to A_2. It is possible to see this network structure changes in Figure 3b. This shows that the system is able to detect network changes and adapt to them. As soon as the device is moved, the two trackers update their respective fingerprints to match the new network structure, allowing for a better accuracy.

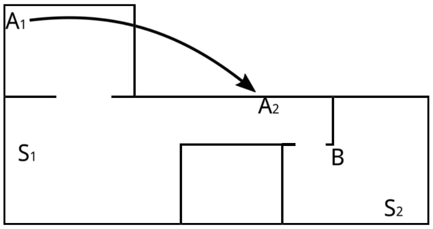

Figure 4: Test area map.

To prove the validity of the model, we have conducted several experiments with a tracking device over a fixed spot. We have evaluated the localization error with and without the WiFACT system, moving and disabling different APs. In figure 5 we report the location information as detected by the tracking device regarding three different experimental scenarios we have evaluated. In t_0, in all three examples, we got the base position with an average error of $1m$ with 5APs visible from the fixed spot. However, after the variation of the APs conditions and without WiFACT WSN being online (at t_1), we found a positioning error of up to $10m$ (10% of the original precision). After enabling the WSN, the error rapidly reduced over the next 3 minutes, back to $\sim 1m$ (t_2 through t_6), showing that the system is in fact able to integrate data to calculate a reliable fingerprint in a small timeframe. Subsequent incremental fingerprint calculations, moreover, further improved the fingerprint quality over time, reducing the error up to $0.6m$ over 30 minutes after WSN enabling. One can see that, in all cases, the tracking device will locate correctly back the fixed spot (as it was in t_0).

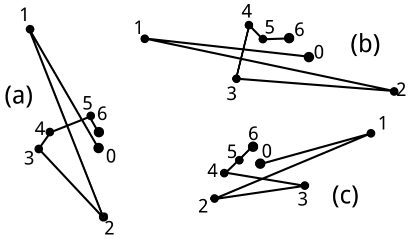

Figure 5: Accuracy evaluation results.

We also conducted several robustness tests to verify the model quality. We tried disabling one or more APs, moving more than one AP at a time, and dynamically adding and removing APs and obstacles without any prior WSN configuration. In all case studies the positioning errors has been corrected by the WiFACT WSN in less than 5 minutes.

VI. Conclusions and Future Work

In this paper we have introduced the project WiFACT, which is a module developed to improve fingerprinting-based localization systems, through the implementation of a WSN of components able to detect a wireless network in the neighborhood and communicate gathered data to a central server.

Regarding the fingerprint evaluation method defined in paragraph III-A, we have managed to achieve:

- **higher precision**: continuous training that allows to have several measurements for each place, enabling higher precision per fingerprint;
- potentially **higher accuracy**: due to the initial distribution phase that enables better fingerprint positionings according to building plans;
- **higher density**: the WiFACT components are very cheap so it is possible to distribute a high-count WSN in order to obtain higher RadioMap density. Moreover, it is possible to use different densities in different places to achieve different fingerprinting accuracy levels.

While the initial distribution phase is more complex than a normal training phase, WiFACT allows to improve the system efficiency over the time and guarantee a correct behavior of the localization system in case of any network-structure change or environmental alteration, without any manual human intervention. As said in paragraph IV-D, having an overlying infrastructure grants several advantages, such as the ability to gather data from any available AP in the area, being network-agnostic, and being more reliable as it is independent from any APs/network failure. The only downside of having another network is the deployment cost, which is however very small as the modules are very cheap and require very little mantainance and setup efforts.

Future works include implementing a system that allows for automatic modules distribution to further reduce human interaction and improve module positioning accuracy, which in turn can improve location accuracy system-wide. Moreover, while the WiFACT WSN network is redundant (via self-healing mesh described in paragraph IV-B), the Main Transmission Node is the only one that is cable connected to the server, so in case of a module failure the whole network would stop working without any warning. An implementation of a simple and automatic reliability system on the MTN is currently under research.

Acknowledgments

This research was partially supported by MYOPENGOV Research project, Grant for industrial research and experimental development for the realization of innovation Campus (POR Campania, Italy region 2007/2013 - CUP B17I12000070007).

References

[1] Z. Yang, C. Wu, and Y. Liu, "Locating in fingerprint space: wireless indoor localization with little human intervention," in *18th MobiCom*. ACM, 2012.

[2] G.-y. Jin, X.-y. Lu, and M.-S. Park, "An indoor localization mechanism using active rfid tag," in *SUTC 2006*, vol. 1. IEEE, 2006, pp. 4–pp.

[3] K. Chintalapudi, A. Padmanabha Iyer, and V. N. Padmanabhan, "Indoor localization without the pain," in *16th MobiCom*. ACM, 2010, pp. 173–184.

[4] P. Krishnamurthy, "Wifi location fingerprinting," *Advanced Location-Based Technologies and Services*, p. 55, 2013.

[5] P. Baronti, P. Pillai, V. W. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and zigbee standards," *Computer communications*, vol. 30, no. 7, pp. 1655–1695, 2007.

[6] L. T. Nguyen and J. Zhang, "Wi-fi fingerprinting through active learning using smartphones," in *UbiComp*. ACM, 2013, pp. 969–976.

[7] D. A. Tran and P. Truong, "Total variation regularization for training of indoor location fingerprints," in *2nd MiSeNet*. ACM, 2013, pp. 27–32.

[8] A. Eleryan, M. Elsabagh, and M. Youssef, "Synthetic generation of radio maps for device-free passive localization," in *GLOBECOM*. IEEE, 2011, pp. 1–5.

[9] O. Woodman and R. Harle, "Pedestrian localisation for indoor environments," in *10th UbiComp*. ACM, 2008.

[10] T.-K. Dao, H.-L. Nguyen, T.-T. Pham, E. Castelli, V.-T. Nguyen, and D.-V. Nguyen, "User localization in complex environments by multimodal combination of gps, wifi, rfid, and pedometer technologies," *The Scientific World Journal*, vol. 2014, 2014.

[11] F. Amato, A. Mazzeo, V. Moscato, and A. Picariello, "Exploiting cloud technologies and context information for recommending touristic paths," *Studies in Computational Intelligence*, vol. 511, pp. 281–287, 2014.

[12] F. Amato, A. Chianese, V. Moscato, A. Picariello, and G. Sperli, "Snops: A smart environment for cultural heritage applications," 2012, pp. 49–56.

[13] F. Amato, A. Mazzeo, V. Moscato, and A. Picariello, "A system for semantic retrieval and long-term preservation of multimedia documents in the e-government domain," *International Journal of Web and Grid Services*, vol. 5, no. 4, pp. 323–338, 2009.

[14] Y. Chen and H. Kobayashi, "Signal strength based indoor geolocation," in *ICC*. IEEE, 2002, pp. 436–439.

[15] M. Kessel and M. Werner, "Smartpos: Accurate and precise indoor positioning on mobile phones," in *MOBILITY*, 2011.

[16] P. Krishnan, A. Krishnakumar, W.-H. Ju, C. Mallows, and S. Gamt, "A system for lease: Location estimation assisted by stationary emitters for indoor rf wireless networks," in *INFOCOM 2004*, vol. 2. IEEE, 2004, pp. 1001–1011.

[17] M. Azizyan, I. Constandache, and R. Roy Choudhury, "Surroundsense: mobile phone localization via ambience fingerprinting," in *15th MobiCom*. ACM, 2009, pp. 261–272.

[18] J. Niu, B. Lu, L. Cheng, Y. Gu, and L. Shu, "Ziloc: Energy efficient wifi fingerprint-based localization with low-power radio," in *WCNC*. IEEE, 2013, pp. 4558–4563.

[19] E. Mok and G. Retscher, "Location determination using wifi-fingerprinting versus wifi-trilateration," *Journal of Location Based Services*, vol. 1, no. 2, pp. 145–159, 2007.

[20] S. Lin, J. Liu, and Y. Fang, "Zigbee based wireless sensor networks and its applications in industrial," in *TCAL*. IEEE, 2007, pp. 1979–1983.