This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2009 proceedings.

An Energy-Aware Autonomic Architecture for Localization in Ubiquitous Networks

Mathieu Bouet, Shahab Gashti, Guy Pujolle
University Pierre and Marie Curie (UPMC), LIP6, Paris, France
{Mathieu.Bouet; Shahab.Gashti; Guy.Pujolle}@lip6.fr

***Abstract*—One of the main challenges in ubiquitous networks is localization. Many positioning methods have been proposed in the literature since this data is critical for numerous protocols and services. Choosing the right localization algorithm for a specific environment is a hard task. However, it is even more complex when several radio access technologies are available in evolving environments. This paper presents a framework based on autonomic networking concepts to achieve localization in ubiquitous networks. This approach uses ambient intelligence to provide flexibility, accuracy, and energy savings.**

***Index Terms*—Autonomic networking, localization, ubiquitous networks, Universal Plug and Play (UPnP).**

I. Introduction

Future ubiquitous and pervasive networks aim to provide spontaneous emergent services and globally available services and resources in a network. Location in such networks is a key and often a critical data for many algorithms and protocols. Furthermore, services based on context-awareness generally rely on this type of information [1].

Localization in wireless networks has been studied for a long time now and many solutions have been proposed in the literature. However, in ubiquitous networks, the different available and overlapping wireless networks and the numerous localization methods generate complexity in term of choice. Thus, the integration of heterogeneous networks to support a localization service poses many challenges such as radio access technology selection, positioning technique selection, available infrastructure, and energy consumption. Such a service has to be able to automatically adapt in real-time to changing environments to provide flexibility, reliability and accuracy.

This paper proposes the first global framework for localization in ubiquitous networks. Our proposal is oriented towards accurate location estimation but also towards energy consumption since networks are generally not built for this unique service. We use some *autonomic networking concepts* [2] to develop our framework, providing self-optimization and self-configuration in order to adapt to changing environments. This is notably done by managing devices with *Universal Plug and Play (UPnP)* and by precisely defining the different entities of the architecture to achieve this purpose. The radio technologies considered are Radio Frequency IDentification (RFID), Ultra-WideBand (UWB), and IEEE 802.11. They are widely used and will be key components of ubiquitous networks. Furthermore, they have different interesting properties for localization. We also outline arising challenges such as *security, knowledge acquisition, and ambient-intelligent algorithm selection*.

The rest of the paper is organized as follows. Section 2 describes localization principles through the different radio technologies. Section 3 introduces the UPnP services. Section 4 presents the energy-aware autonomic framework for localization. Section 5 instances a scenario. Finally, Section 6 outlines challenges and perspective and Section 7 ends the paper with the conclusion and the future work.

II. Localization Techniques

Radio propagation is subject to numerous problems such as interference, severe multipath, rare line-of-sight (LOS), absorption and reflection [3]. Since signal cannot be measured very precisely, several localization algorithms have been proposed in recent years. They can be classified into three families: distance estimation, scene analysis, and proximity.

Algorithms based on distance estimation use properties of triangles to estimate the target location. The triangulation approach consists in measuring the angle of incidence (or Angle Of Arrival - AOA) of at least two reference points. The estimated position corresponds to the intersection of the lines defined by the angles. On the contrary, the lateration approach estimates the position of the target by evaluating its distance from at least three reference points. The range measurement techniques use Received Signal Strength (RSS), Time Of Arrival (TOA), Time Difference Of Arrival (TDOA), or Received Signal Phase (RSP) since the attenuation, the time of flight and the inter-delay of signals have well-known characteristics depending on the distance between the emitter and the receiver. These techniques can lead to large error measurements in harsh environments. Moreover, they can require on-site calibration and specific equipment such as directional antennas or very precise clocks.

Scenes analysis approaches are composed of two distinctive

978-1-4244-2948-6/09/$25.00 ©2009 IEEE

steps. First, information concerning the environment (fingerprints) is collected. Then, the location of the target is estimated by matching online measurements with the appropriate set of fingerprints. Generally, RSS-based fingerprinting is used. The three main fingerprinting-based techniques are: k-nearest-neighbors (kNN) also known as radio map, probabilistic methods, and constraints-based methods.

The last type of localization technique is based on proximity. This approach relies on dense deployment of antennas. When the target enters into the radio range of a single antenna, its location is assumed to be the same that this receiver. When more than one antenna detects the target, the target is assumed to be collocated with the one that receives the strongest signal. This approach is very basic and easy to implement. However, its accuracy is on the order of the size of the cells.

Each radio technology has its own advantages and disadvantages. RFID is a short range identification technology. RFID tags are very small, very cheap but also computationally limited. Due to these characteristics, RFID systems provide by default accurate proximity localization and limited positioning errors in dense deployments [4]. Infrastructure-based localization approaches, that is which belong to scene analysis family, are privileged with this technology. UWB uses a large portion of the radio spectrum to communicate at low-energy and high bandwidth. This radio technology has a high spatial resolution and the ability to easily resolve multipath components [5]. Thus, more classical techniques, for example lateration with RSS or TOA measurements, can be used. Finally, IEEE 802.11 is widely spread and has been studied for a long time [6]. Its longer range and its early adoption make this radio technology incontrovertible for localization in wireless networks.

In this paper, we only consider non-self-positioning methods, that is the methods where localization estimation is performed by a centralized entity, generally a server. This approach is more secured, more adapted to RFIDs and most of all is relevant for localization systems where the calculated locations are utilized by other services. However, self-positioning methods could be next included into our proposition by defining how the stations securely send their locations to the server.

III. UPnP Low Power Solution

In our global localization framework we propose to use an extension of Universal Plug and Play (UPnP) [7] allowing device and energy management.

UPnP allows automatic networking management. Its main goal is to simplify the installation and the administration of network devices and services enabling them to control and to be controlled, to discover and to be discovered.

UPnP leverages existing standards such as the TCP/IP stack together with Web technologies, especially HTTP and XML. UPnP is platform independent and runs over any physical network technology. In addition, the UPnP architecture offers pervasive peer-to-peer network connectivity since it does not require a central server.

An UPnP Network is composed of UPnP Devices, UPnP Services and UPnP Control Points. An UPnP Device may provide different set of services as well as embedded devices. An UPnP Service exposes the device functionalities, represents a set of actions to which the services respond, and consists of state variables. Finally, an UPnP Control Point can discover and control the UPnP services and devices, invoke actions, and subscribe to receive event messages when service's state variables change.

Initially, UPnP like a lot of network protocols forces devices to stay fully powered-up, even if they are inactive. This is a real problem for mobile devices where battery lifetime is a limited resource. UPnP Forum has thus recently standardized the UPnP Low Power architecture [8] in order to enable power management in UPnP devices. The UPnP Low Power architecture allows UPnP devices implementing power saving mode to enter and remain in a low-power sleep state and thus to conserve energy while still being discoverable. In this solution, an UPnP Low Power Aware Control Point can wake up a device from a sleep state or request the device to go into a low power state. In addition, devices can go to sleep/wake up state autonomously by using internal timers or on receiving a message on behalf of the control point.

The UPnP Low Power solution is particularly interesting for an implementation on wireless Access Points (APs) in order to dynamically control, monitor, and configure them. In this case, a Controller, i.e. UPnP control point, would be able to manage UPnP Low Power Access Point Devices. It would be able to manipulate and change, when necessary, several parameters such as security level, SSID, radio channel, antenna gain and direction, and power state. It could also easily retrieve data such as identities of users or transmitted packet rate. Most of all, in an energy-oriented approach, such a Controller would be able to wake up or put into a sleep mode APs in order to optimize the life-time of the network when events occur and thus to reduce energy consumption.

IV. The Proposed Energy-aware Localization Framework

Many localization methods have been proposed in the

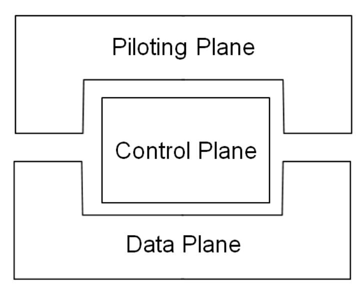

Fig. 1. Autonomic networking architecture.

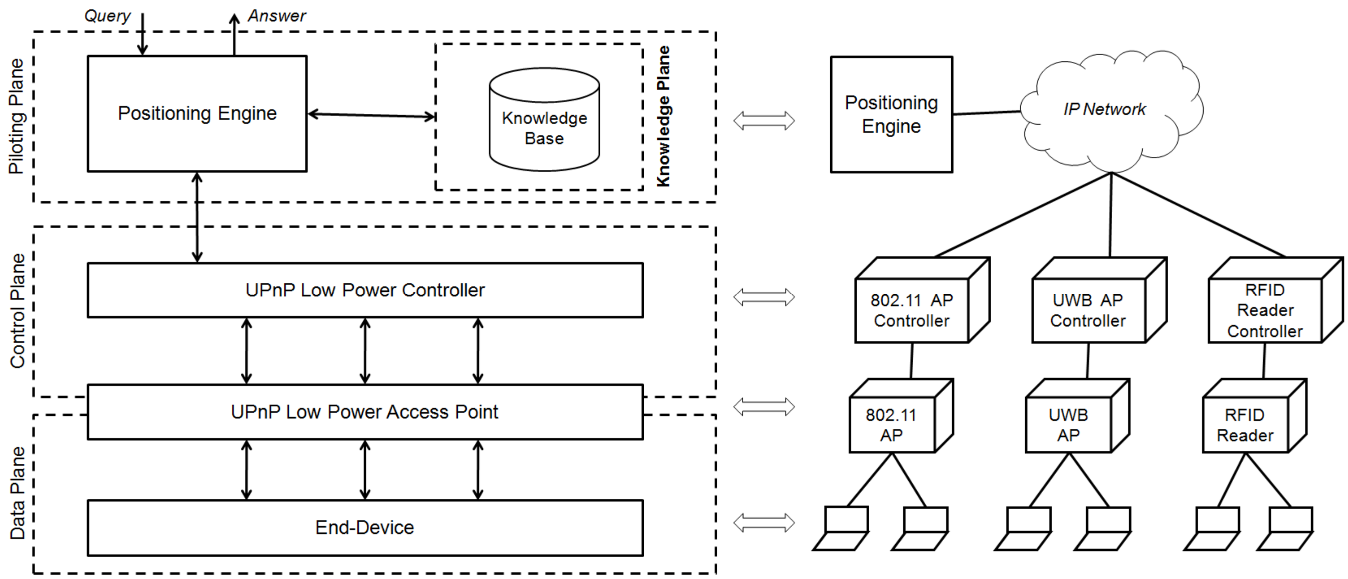

Fig. 2. The proposed energy-aware localization framework.

literature. With multiple available radio access technologies, choosing an appropriate positioning technique and applying it are very complex tasks in ubiquitous networks. We propose to address this issue using autonomic concepts. Indeed, autonomic communication is the vision of next-generation networking, which will be a self-behaving system with properties such as self-healing, self-protection, self-configuration, and self-optimization [2], [9]. We define three planes for real-time autonomic networking: the Piloting Plane, the Control Plane, and the Data Plane (Fig. 1). Each plane provides specific and interdependent functionalities which are described in details in the following subsections and in Fig. 2. The global localization service will thus be able to automatically adapt to changes in environment, select the relevant localization algorithm, and manage devices in order to maximize accuracy and minimize energy consumption.

In the rest of the paper, we consider that a device, for example a laptop, can have more than one radio access interface. If it is not the target to localize, it will be viewed by the system as one AP for each technology and will thus be controlled by different controllers. Consequently, the networks are composed of static and mobile APs and each controller is in charge of a particular network, in our case RFID, UWB, and IEEE 802.11.

A. *Date Plane*

The Data Plane concerns the basic data necessary for the localization process (Fig. 2). These can be RSS measurements, time-of-flight, or angle of incidence. In our framework, this plane includes the devices that are going to be localized and the different APs. The required measurements are realized by these last entities.

B. *Control Plane*

The Control Plane is situated between the Data Plane and the Piloting Plane. This abstract layer is in charge of controlling Data Plane's entities in order to retrieve the necessary data (Fig. 2).

In our framework, this plane includes two different types of devices: controllers and APs. The controllers manage, configure, and control several APs. For example, they can change the parameters of the APs, that is SSID, radio channel, transmission powers, and security algorithms. We propose to use UPnP Low Power solution to perform the control of the APs by the controllers. Its main advantage is to allow devices implementing power saving modes to conserve energy. This way, APs can go to sleep-wake states autonomously or upon receiving a control message on behalf of its control point. Measurement actions for the APs are also invoked by the control point.

C. *Piloting Plane*

The Piloting Plane is in charge of choosing, adapting and configuring in real-time the algorithms and services depending on context changes (Fig. 2).

To properly fulfill this function, an additional abstract sub-plane, the Knowledge Plane, is defined within this plane. It provides a global view of all information concerning the network. The information is built with data gathered from the network and is periodically updated. The goal of the Knowledge Plane is to feed with appropriate knowledge the Piloting Plane and more specifically its meta-control algorithms in order to adapt and choose the best control algorithms to optimally achieve the objectives of the system. In our case, the necessary information is typically the location of the APs in the network, their capabilities, their power state, the available locations of the end-devices and their different network interface cards.

The core of the Piloting Plane interacts with the Knowledge Plane in order to retrieve the information that it requires to take the best decision for the different control algorithms. In our framework, the entity in charge of this decision is called the Positioning Engine. It obtains, if possible, from the Knowledge Plane the list of the APs that were near the last position of the end-device which is going to be localized or try to iteratively limit the area where it might be located. This list enriched by other information such as the capabilities of the APs can be considered as a Situated View [9]. The Positioning Engine contains several localization algorithms. The decision consists in choosing the most accurate positioning technique depending on the local network topology and on available radio technology, since RFID, UWB, and IEEE 802.11 technologies provide short-range, medium-range, and long-range communications respectively. The selected algorithm will require a certain type of data to perform the localization. These data, which can be RSS, TDOA, AOA measurements, will be retrieved by the selected APs. Consequently, the Positioning Engine has to activate them through the Control Plane and indicate the identity of the targeted end-device and the nature of the measurements. APs can be in sleep mode or in low power state in order to save energy and hence have to be woken up. Once the data is collected, the Positioning Engine applies the algorithm and estimates the location of the target. The localization process can be reiterated by the Positioning Engine if the estimated location is not satisfactory.

V. Scenario

The proposed framework is intended to enable precise and energy efficient indoor positioning in ubiquitous networks. We illustrate its mechanisms with a scenario depicted in Fig. 3. Initially, the Positioning Engine, which offers an interface as a localization service for other applications, receives a query: what is the location of user *X*? To localize this user, the Positioning Engine needs some knowledge concerning the environment. Thus it requests to the Knowledge Plane information such as the last known location of the target, its available interfaces, a list of all APs that can potentially communicate with it, their capabilities, their locations, their power states. The Knowledge Plane, which is in charge of collecting data and building fresh information provides such knowledge and sends it to the Positioning Engine. Then, the Positioning Engine chooses an appropriate localization algorithm and sends a request to the right Controller in order to retrieve the required data, that is to say RSS, TDOA, AOA or other measurements. The Controller wakes up the selected APs if necessary using UPnP low power and asks them to perform the requested measurements relative to the target. When it is done, the Controller collects these measurements and forwards them to the Positioning Engine. This one executes the chosen

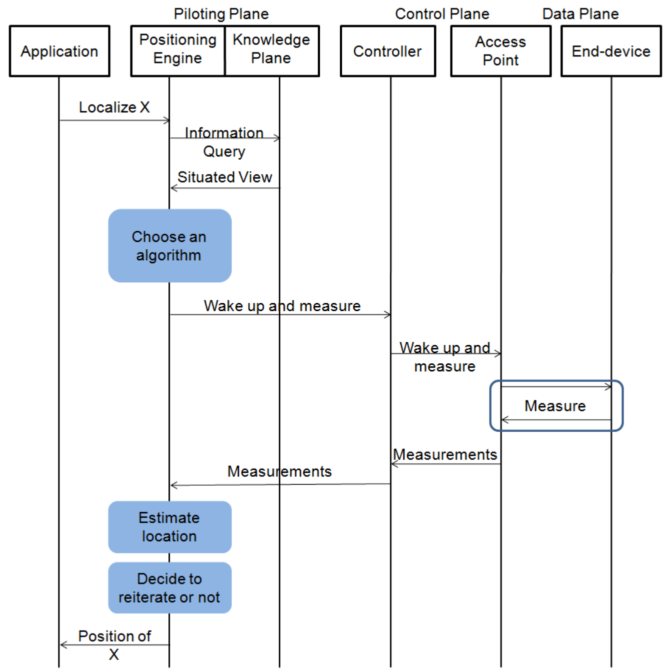

Fig. 3. Scenario: localization of user X.

localization algorithm in order to have an estimated location of the target. At this point, it decides whether to reiterate the process with another approach if the result is not satisfactory or to answer the localization query with the estimated location.

VI. Challenges and Perspectives

Some challenges arise from our framework. The methods and algorithms included in the Data and Control Planes have been studied for a long time. On the contrary, the intelligent modules of the Piloting Plane manipulate new concepts.

The first challenge concerns the selection of the localization algorithm. As explained in Section II, a great variety of them exists. The techniques go from simple lateration with RSS measurements to more sophisticated approaches that require the deployment of reference nodes. Moreover, the diverse radio frequencies used by RFID, UWB, and IEEE 802.11 have very different properties such as read range, absorption by metal or water, propagation in dense environments, or synchronization. For example, UWB enables precise clocks and thus offers very accurate results with TDOA. A first global approach to deal with all this complexity and make the best choice among all available localization techniques is of course to consider both the radio access technologies of the target and the infrastructure around it. If the target has only one interface, the choice will be considerably reduced. In the same way, if the target can communicate with a very limited quantity of APs, simple techniques depending on the characteristics of the radio frequency or another interface will have to be privileged. Choosing the appropriate localization algorithm is an opened problem.

The second challenge concerns the Knowledge Plane. This abstract entity is in charge of providing information related to the network and more generally related to the environment. The main difficulty is to build such knowledge from basic data. Indeed, the required data has to be identified but also the update frequency of the information has to be studied in order to keep data freshness. Another important issue concerns the structure of the plane. It can be centralized or distributed [10]. In the latter, the knowledge is shared by several nodes. They have to know which data they need and where to get them. They also need to synchronize their knowledge so as to keep consistency and to have a way to provide their knowledge to the Positioning Engine when asked. In our framework, a possible approach would be to retrieve the power state of the APs, which is identified as a necessary data, from the Controllers in order to feed the Knowledge Plane. In the same way, the Positioning Engine could feed it with the estimated locations.

Another challenging issue is security. Very few localization algorithms have been developed considering security. In a centralized architecture, the attackers can only try to impersonate the target. This can be overcome by introducing cryptography in order to authenticate users. In a decentralized architecture, threats increase. An attacker can, in addition, act as an AP and inject false data in the system. For example, it can claim that the target is within its communication range and report falsified signal measurements in order to degrade the accuracy of the positioning. Besides, compromised users and APs can have a large impact on the Knowledge Plane by diffusing false data in the network leading to wrong information and consequently to inappropriate decision and calculation. The global security of the architecture has to be addressed in future work.

VII. CONCLUSION

We proposed a framework to enable localization in ubiquitous networks. Our approach uses autonomic networking concepts to provide flexibility, accuracy and energy-savings. We first presented positioning principles in wireless networks and the UPnP Low Power solution, which is used to manage devices. Then, we explained autonomic networking and described our framework. The Positioning Engine included into the Piloting Plane retrieves information from the Knowledge Plane in order to select the more relevant localization algorithm. Then, it communicates with the controllers, which are in charge of the management of the APs, so as to get required data relative to the target node. These data are injected into the algorithm to compute the location. Several challenges have arisen from our framework and will be part of future work. They concern the selection of the appropriate positioning technique, the conception of the Knowledge Plane, and security.

REFERENCES

[1] A. Cangialosi, J.E. Monaly, and S.C. Yang, "Leveraging RFID in hospitals: Patient life cycle and mobility perspectives," IEEE Communications Magazine, 45(9):18–23, September 2007.

[2] International Business Machines, "An architectural blueprint for autonomic computing," IBM, April 2003.

[3] T.Rappaport, "Wireless Communications: Principles and Practice", Prentice Hall PTR, Upper Saddle River, NJ, USA, 2001.

[4] R. Want, "An introduction to RFID technology," IEEE Pervasive Computing, 5(1):25–33, January-March 2006.

[5] A. Hatami and K. Pahlavan, "Performance Comparison of RSS and TOA Indoor Geolocation Based on UWB Measurement of Channel Characteristics," IEEE PIMRC, pp. 1-6, September 2006.

[6] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of Wireless Indoor Positioning Techniques and Systems," IEEE Transactions on Systems, Man, and Cybernetics, vol.37, no.6, pp.1067-1080, November 2007.

[7] "Universal Plug and Play (UPnP) Forum," http://www.upnp.org.

[8] UPnP Design Complete, "UPnP Low Power Architecture V1.0," UPnP Forum, August 2007.

[9] G. Pujolle, "An Autonomic-oriented Architecture for the Internet of Things," IEEE JVA'06, pp. 163-168, October 2006.

[10] D. F. Macedo, A. L. dos Santos, G. Pujolle, and J. M. Nogueira, "Optimizing Wireless Ad Hoc Communication Resources with a Knowledge Plane," IFIP MWCN, pp. 86-90, November 2007.