On the Potentials of Object Group Localization in the Internet of Things

Laura Galluccio, Giacomo Morabito, Sergio Palazzo
DIEEI - University of Catania (Italy), Email: {name.surname}@dieei.unict.it

***Abstract*—The incessant decrease in size, cost, and energy consumption of wireless devices is likely to boost the number of wireless devices dramatically. These will be deployed in several real world objects that we use in our daily life as envisioned by the Internet of Things (IoT) concept. Designing effective and efficient objects' location update and search mechanisms, is very important but is extremely difficult in the IoT scenarios. In fact, the number of mobile objects composing the IoT will be huge; this implies that signaling traffic generated for location update and discovery purposes can explode. Also, objects might currently be located where positioning solutions are not available or are not accurate enough to support most of the envisioned added value IoT applications. In this paper it is studied how object group mobility can be exploited to achieve accurate location update and search in the IoT, while reducing the signaling overhead. Object group mobility is a phenomenon that naturally emerges as usually moving objects are carried by a human or a vehicle together with several other objects. In this paper i) the concept of object group mobility is introduced and it is explained how and to which extent this can be used to reduce signaling overhead and improve accuracy in object location information; ii) the concept of collective-agent is introduced to further decrease signaling overhead in the IoT scenarios where object group mobility emerges, iii) an analytical framework is derived to assess the advantages of exploiting object group mobility in IoT scenarios.**

***Keywords*-Internet of Things (IoT), Mobility management;**

I. INTRODUCTION

The will for supporting added value applications, like domotics, supply and distribution chain monitoring and optimization, e-health, etc. is fostering the introduction of new communication paradigms where an indefinitely large number of *things* and/or real world *objects* can be addressed from everywhere with a unique addressing scheme and interact/cooperate with each others. The ITU paved the way to this new vision by defining a new communication paradigm, i.e., the *Internet of Things (IoT)*: "*A new dimension has been added to the world of information and communication technologies (ICTs): from anytime, anyplace connectivity for anyone, we will now have connectivity for anything*" [1]. This vision perfectly fits with the definition of the IoT given in the European Commission documents also, where IoT is referred to as "*Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental and users contexts*" [4]. Such a pervasive vision of the network of things gives an idea of the strong impact expected on everyday life and behavior of users. This is also recognized in the studies of the U.S. National intelligence Council about the IoT, which is enumerated among the six "Disruptive Civil Technologies" with high impact on the predominant positions of different countries [5]. Several heterogeneous communication technologies will converge into the IoT, such as RFID systems, wireless sensor and actor networks, personal and body area networks, etc., each using its own access solution. In this heterogeneous context, IPv6 will be the common language and, in this sense, recent efforts to integrate IEEE 802.15.4 networks or EPCGlobal RFID systems [3] in IPv6 networks will play a crucial role [13], [14], [16]. However, in the IoT several new research issues arise spanning all components of the systems as well as all layers of the protocol stack [7]. In this work we focus on object location update and search mechanisms which are key components of mobility management for mobile things in IoT scenarios. This is a very important problem as it is expected that hundreds of billions of mobile things will be networked and standard Mobile IPv6 [12] approach results not scalable as would involve the exchange of a paramount amount of signaling traffic – think that the exchange of binding update message requires the setup of an IPSec channel between the mobile node and its home agent. Also, many of the services conceived for IoT scenarios require accurate object location information which is usually not available. So appropriate solutions are needed to improve location information accuracy while reducing the signaling produced for mobility management purposes. To address the above aspects we exploit *object group mobility* (OGM), a phenomenon that naturally emerges as usually IoT objects are carried by a human or a vehicle together with several other objects. For example, goods produced by a supply chain are carried on trucks until they are delivered to a retail store or things in a bag are carried around as one single object until they are not put at their right place. Main contributions of this paper are i) a framework for object location update and search is introduced which is compliant with IPv6; ii) the concept of OGM is introduced and it is explained how this can be used to decrease signaling overhead and improve accuracy in object location information; iii) the concept of *collective-agent* is introduced to further decrease signaling overhead in the IoT scenarios where object group mobility emerges; iv) an analytical framework is derived to

The work of G. Morabito was partially supported by the European Commission in the framework of the FP7 CONVERGENCE project (contract n. FP7-257123).

978-1-4577-0351-5/11/$26.00 ©2011 IEEE

assess the advantages of exploiting OGM in IoT scenarios.

The rest of this paper is organized as follows. In Section II we describe the reference architecture. In Section III we introduce the OGM concept and how it can be used to achieve more accurate object localization and lower mobility management signaling. In Section IV we give a sketch of how procedures for mobility management in IoT scenarios could work. In Section V we derive an analytical framework for the evaluation of the advantages obtained by exploiting the OGM concept in the IoT. Some numerical examples are presented and discussed in Section VI. Finally in Section VII we draw our conclusions.

II. Reference Architecture

To date there is no universal agreement on a specific and detailed architecture for the IoT. Nevertheless, in order to introduce the notation which will be used in the rest of the paper, we provide a general reference architecture. This only takes the basic functional elements into account that even if named in different ways can be found in all existing proposals. We consider a network connecting several objects using different wireless interfaces: for example some of them can be wireless sensors or actuators and comply with IEEE 802.15.4, others can be PDAs with 3G/UMTS or IEEE 802.11 connections, others can be items labeled with RFID tags. Each object is described through some metadata which is called *Versatile Digital Item* (VDI) [8]. The problem we address is related to management of mobility for this multitude of devices which can coexist in the same area without knowing about each others because of the different wireless interfaces used. We focus our interest on a given area which can be divided in *ambiences* as shown in Figure 1. By definition an *ambience* is a limited space with homogeneous physical characteristics (temperature, humidity, luminosity, etc.) where objects (even, partially) sharing the same intents are located and can interact with each others to support added value services. Note that in the existing literature on smart computing ambiences have been defined and called in several different ways, like *contexts* or *rooms*, depending on the particular scenario [19], [17]. We denote the set of ambiences defined in the area of interest as $A = \{a_1, a_2, ..., a_M\}$, where a_i represents the i-th ambience. According to the IoT paradigm when several items are in the same ambience the behavior/characteristics of any of them should be modified due to the presence of the other objects. Unfortunately, devices which are usually deployed in the objects do not have enough computational power to support the expected level of awareness and thus, appropriate servers should be appositely deployed, as typically proposed in all architectural solutions for smart environments (e.g., [19], [17], [22], [11]). We call *context server* (CS) a server that supports the awareness of the proximity between objects in the same environment and assume that a CS can serve several ambiences. We assume that the area of interest is

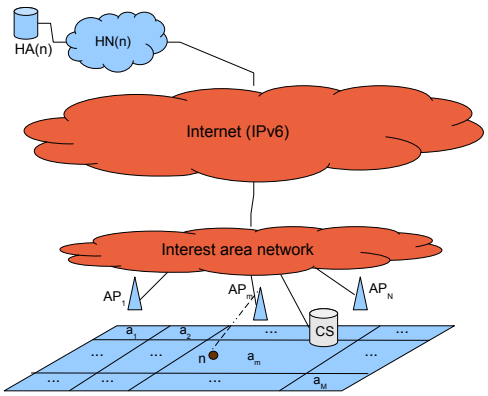

Figure 1. Reference architecture.

covered by an access network, which we refer to as *interest area network*[1], connected to the rest of the Internet. We also assume that communication with the objects is supported by a multitude of heterogenous *access points*. Indeed, it is most likely that different access technologies will be deployed in the same area of interest and therefore, access points in our architecture will represent WiFi or Bluetooth access points, IEEE 802.15.4 gateways, RFID readers, etc. Given an access point, AP, we call $\psi(AP)$ the access technology it uses. Obviously, the same access point can cover several ambiences. We denote the set of ambiences covered by the access point AP as $C(AP)$. Let n be a node of the IoT located in ambience X_n and equipped with a wireless interface of technology $\psi(n)$. Obviously, this node can only connect to access points supporting the same technology, i.e., n can connect with access point AP only if $\psi(n) = \psi(AP)$ and $X_n \in C(AP)$. As an example, in Figure 1, node n is placed in area a_m, i.e., $X_n = a_m$, and gets access through access point AP_m, given that $a_m \in C(AP_m)$ and $\psi(n) = \psi(AP_m)$. According to MIPv6, each node n belongs to a *home network* that we call $HN(n)$. The home network may be different from the network where the mobile node is currently attached. If this is the case, then the latter is referred to as *foreign network* and is denoted as $FN(n)$, whereas in the home network $HN(n)$ there will be a home agent $HA(n)$ which maintains updated information about node n position.

III. Group Mobility in the Internet of Things

Effective design of location update protocols should be based on the mobility characteristics of moving nodes. Accordingly, in the context of mobile networks a large research effort has been devoted to the design of appropriate

[1]In Figure 1 the context server is placed in the interest area network, however, it could be deployed anywhere in the network.

models capturing the mobility characteristics of individuals [15], [9]. While the mobility characteristics of moving *things* are unknown to date and must be studied so as to derive completely new models, it is an evidence suggested by our everyday experience that objects usually move in groups. We call such phenomenon *object group mobility* (OGM). Another evident feature of things' mobility is that groups of objects usually aggregate around a carrier (a person, a vehicle, a box, etc.). We denote this carrier as *group master* (GM). The things aggregated around the group master are denoted as *slaves*. It is obvious that slaves are always nodes of the IoT. We assume that also masters are nodes of the IoT; in fact, usually group masters carry at least one communication device that they take in any ambient they visit (e.g. usually a person carries a cell phone or a smart phone and a box has an RFID or an IEEE 802.15.4 device built in). Group mobility has been exploited in the past to improve energy efficiency or privacy of mobility management schemes in several wireless communication scenarios [10], [18]. Also, in the IoT we can exploit OGM to reduce the amount of traffic circulating in the network for mobility management purposes. To achieve this, the group master manages several addresses belonging to its home network, assigns them to its slaves, and register them in its home address. The slaves provide the above addresses to their home agents as their care-of address. In this way, when nodes in a group change their foreign addresses, no binding messages have to be exchanged between the slaves and their home address. Indeed, it is enough that the group master informs its home agent about the care-of addresses of all the nodes in its group. Note that according to such procedure the number of messages circulating in the network for mobility management purposes can be reduced significantly, as we will show in Section VI. In the IoT context, given that groups may be composed of nodes with different access technologies, such group mobility characteristic can be further exploited to achieve higher accuracy in the estimation of the position (i.e., the ambience) where nodes are located and, therefore, to support more effective and efficient added value services. For the sake of clarity, let us provide a simple example. Let n_0 and n_1 be two things/nodes belonging to the same group, with two different access technologies ψ_0 and ψ_1, respectively. Also suppose that node n_0 can communicate with an access point AP_0 covering the set of ambiences Φ_0, whereas node n_1 cannot communicate with any access point because it is located in an ambience not covered by any access point compliant with technology ψ_1. If we consider node n_1 individually, we do not have any information about its position. On the contrary, if we consider it as a part of a group together with n_0, we can conclude that most probably node n_1 will be located in one of the ambiences included in Φ_0. We can generalize this concept. Suppose now that nodes n_0 and n_1 access the network by means of access points AP_0 and AP_1 covering ambiences Φ_0 and Φ_1, respectively. If we look at n_0 and n_1 individually, then we know that n_0 will be placed in one of the ambiences included in Φ_0, whereas n_1 will be located in one of the ambiences in Φ_1. Differently, if we take into account that they are part of the same group, then we can deduce that both of them will be located in one of the ambiences contained in $\Phi_{0,1} = \Phi_0 \cap \Phi_1$. Thus, uncertainties on the positions of n_0 and n_1 are $\log_2 |\Phi_0|$ and $\log_2 |\Phi_1|$, respectively, as defined in [20], if we look at nodes individually; instead, uncertainty is equal to $\log_2 |\Phi_{0,1}|$ for the position of both nodes, if we look at them as belonging to the same group. Obviously, $|\Phi_{0,1}| \leq \min\{|\Phi_0|, |\Phi_1|\}$ and therefore, taking group mobility into account reduces uncertainty. Unfortunately, nodes belonging to the same group but using, in general, different technologies may be unable to communicate with each other for several reasons as we have already explained, and therefore, at a certain time, we may not have the certainty that nodes still belong to the same group. Indeed, considering nodes as a part of the same group whereas they have split can cause location errors and have dramatic effects on the application. In Section V-B we will analyze the tradeoff between the improvement in localization accuracy and the probability of making localization errors.

IV. Mobility Management procedures

In this section we introduce the basic operations required to exploit OGM, explaining how they fit in the context of mobile IPv6[2]. To this regards, we assume that the reader is familiar with mobile IPv6 operations.

Later, in Section V we will analyze their impact on performance in terms of location accuracy and resource utilization.

To understand OGM-aware mobility management procedures let us consider a group consisting of a group master and m slaves which we denote as $n_0, n_1, ..., n_m$, where we assume that n_0 is the master. Also, let $CoA(n)$ represent the current care-of address of node n.

The basic idea is that the group master n_0 assigns to each slave an address of its home network $HN(n_0)$. To this purpose each node which is likely to be a group master is reserved several IPv6 addresses. Let $LA(n_i)$, with $i > 0$, represent the address assigned by n_0 to node n_i. Each slave n_i will provide $LA(n_i)$ as its current care-of address to its home agent $HA(n_i)$; and will perform a binding to $HA(n_0)$ providing its current care-of address $CoA(n_i)$.

In this way, if a node – i.e., the so called "*correspondent node*" – sends a packet to a slave n_i, then the packet will reach the home network of n_i, $HN(n_i)$. Here the packet is captured by the home agent $HA(n_i)$ which will forward it to the care-of address it is aware of, $LA(n_i)$. In this way the packet will reach the home network of the group master

[2]The detailed description of the solutions based on the proposed approach is not provided for lack of space.

$HN(n_0)$ where the packet is captured by the group master home agent $HA(n_0)$ which will forward it to the actual current n_i care-of address, $CoA(n_i)$.

Observe that by using such scheme when a group moves and its nodes change their care-of addresses there is no need to inform the home addresses of the slaves; in fact, information must be updated only in the home agent of the group master.

Also observe that in several application scenarios (especially, in logistics) in the same group there might be a large number of nodes with the same home agent. For example, suppose that $\Omega = \{n_1, n_2, n_l\}$ is the set of slaves of the group with the same home agent $HA(n_1) = HA(n_2) = ... = HA(n_l)$. If this is the case, a *collective agent* is initialized in $HA(n_1)$ which is responsible for keeping updated information about all the nodes in Ω. Nodes in Ω will update $HA(n_1)$ about their location instead of the home agent of the group master $HA(n_0)$. We will show that collective agents are convenient when the number of nodes in Ω is higher than a given threshold n^* which we will calculate in Section V.

In the rest of this section we will briefly describe how the above approach can be realized.

When a node n leaves the radio coverage of access point AP_1 and enters the radio coverage of a new access point, say AP_2, it will get a new care-of address valid for the current foreign network. To this purpose, traditional stateless/stateful autoconfiguration procedures as defined in MIPv6 can be used.

Once the new CoA has been obtained, node n sends an update message to the context server (CS) communicating its IPv6 home address, its Home Agent address $HA(n)$, its MAC address, its access technology, $\psi(n)$, the set of addresses it has been reserved by its home network $HN(n)$ in case it is selected as group master and must assign addresses to its slaves, as we will explain in the following.

Note that this interaction between the node and the CS is necessary for supporting context aware services, independently of the mobility management procedures required to exploit OGM. Also observe that, using standard service discovery protocols such as UPnP [2], [6], a node entering the area of interest for the first time obtains information about the available CS.

Once the CS receives the above updated message, it must perform the following actions: i) Update group and location information ii) Evaluate more accurate location of nodes in the group. These actions will be described below.

Update group and location information: To perform group management the CS keeps track of the existing groups and of the movements of nodes within its area of interest.

If the node n sending the update message is part of an existing group, $\Gamma(n)$, the CS waits for a timeout and then checks that its new position is consistent with the positions of the other nodes in the group. More specifically, the policy which will be utilized is that slaves that have positions inconsistent with the group master are removed from the group. To this purpose both the home agent of the group master and the interested slave are informed. The latter will send a binding update to its home agent to provide it with its actual care-of address.

Also, the CS controls if it is possible to merge the group of n to other groups or to individual nodes. To this purpose, observe that the group of n, $\Gamma(n)$, and group Γ_1 can be merged in the following two cases:

- All nodes in Γ_1 with the same access technology of n have left the old access point of n, AP_1, and joined the new one, AP_2, in a recent epoch.
- In Γ_1 there are no nodes with access technology $\psi(n)$, however, the last h movements of all nodes of the two groups are consistent with each others[3].

Finally, location information must be updated. To this purpose, one of the nodes of the group $\Gamma(n)$ with access technology $\psi(n)$ is selected for sending a binding update to the home agent of the group master $HA(n_0)$. Observe that it is sufficient that the binding message contains information about the foreign subnet prefix of the new foreign network FN, which can be derived by the data contained in standard binding messages. Indeed, according to IPv6 stateless address autoconfiguration, foreign subnet prefix and MAC address are enough to calculate the care-of address of any node. Therefore, $HA(n_0)$ can reconstruct the new care-of addresses for all the nodes in the group $\Gamma(n)$ with access technology $\psi(n)$.

Finally, if a collective agent has been initialized for a set of nodes Ω containing n, then one of the nodes in Ω will be selected to inform $HA(n)$ that all the nodes in Ω have moved to another location.

The case in which n was not part of a group can be dealt with similarly. The obvious difference is that it is not necessary to perform controls on the state of $\Gamma(n)$ given that $\Gamma(n) = \{n\}$.

Evaluate location of nodes in the group: In order to achieve more accurate information about the ambience where a node is located, the CS defines for each node z in the group, i.e., $z \in \Gamma(n)$, the set $\Phi(z) = C(AP(z))$, where $AP(z)$ denotes the access point providing coverage to node z whereas $C(AP)$ represents the set of ambiences covered by access point AP. If nodes in $\Gamma(n)$ are in the same ambience, then it is obvious that they will be located in $[\cap_{z\in\Gamma(n)}\Phi(z)]$.

However, it is possible that some of the nodes have left the group $\Gamma(n)$ and, therefore, the above estimation of the position of the nodes may be not correct. Accordingly, CS estimates whether it is convenient to achieve higher accuracy

[3]Identification of the optimal value of h strongly depends on the specific application scenario. However, this is not a problem given that group merging will be performed by CS which is aware of the scenario.

at the risk of making a mistake in position estimation. To this purpose it uses the results of the analysis reported in Section V-B.

V. Analysis

In the following subsections we will derive an analytical framework for the evaluation of the impact of the use of OGM on the consumed network resources (Sections V-A) and the localization errors and inaccuracy (Sections V-B).

A. Impact on consumed network resources

In this section we evaluate the impact of exploiting object group mobility on the amount of consumed network resources. In fact, in Section III we have discussed how exploiting objects group mobility we can decrease the amount of signaling generated for location update purposes. Then, in Section IV we have observed that data traffic directed towards a slave node will pass through the HA of the group master before it is forwarded to the current foreign network, which causes longer delay besides increased resource consumption. Accordingly, we will first evaluate the reduction in the amount of network resources consumed for location update signaling and then we will calculate the increase in the network resources utilized to deliver a packet to a mobile node.

As in most literature (see [21], for example) we suppose that the time a node using communication technology ψ spends without the need for changing its CoA is distributed exponentially with average $\bar{T}_\psi$. Accordingly, new location update will be required with rate $\lambda_\psi^{(\mathrm{UP})} = 1/\bar{T}_\psi$.

Now suppose that at time t'' a group Γ_3 of nodes with the same access technology ψ moves out of the radio coverage of access point $AP_{(\mathrm{old})_\psi}$ and enters within the radio coverage of another access point $AP_{(\mathrm{new})_\psi}$. Due to such a movement, nodes will need a new care-of address. Note that the current group of nodes Γ_3 is different from what the system recognizes as such. In fact, information about the group was last updated at time t' when the nodes entered within the radio coverage of $AP_{(\mathrm{old})_\psi}$. We denote as Γ_1 the set on nodes with access technology ψ composing the group at time t' and as Γ_2 the subset of nodes in Γ_3 that were part of the group Γ_1 also at time t', i.e., $\Gamma_2 = \Gamma_3 \cap \Gamma_1$. Using traditional MIPv6 solutions each of the Γ_3 nodes will be required to take a new CoA and issue a binding message towards its home agent. Now let us define as Ω_1, Ω_2, and Ω_3 the subsets of nodes in Γ_1, Γ_2, and Γ_2, respectively, with the same home agent HA^*. Also let us define Λ_1, Λ_2, and Λ_3 as the remaining nodes in groups Γ_1, Γ_2, and Γ_3, respectively, that is $\Lambda_1 = \Gamma_1 - \Omega_1$, $\Lambda_2 = \Gamma_2 - \Omega_2$, and $\Lambda_3 = \Gamma_3 - \Omega_3$; Furthermore, for the sake of notation simplicity let Y_1, Y_2, and Y_3 be the random variables representing the number of nodes in the subsets Ω_1, Ω_2, and Ω_3, respectively; and Z_1, Z_2, and Z_2 be the random variables representing the number of nodes in the subsets Λ_1, Λ_2, and Λ_3, respectively.

Exploiting object group mobility we need one binding message for the group, one binding message for each of the nodes in $\Lambda_3 - \Lambda_2$ and a number V_{LU} of binding messages depending on the number Y_3 of nodes in the group at time t'' with the same home agent HA^*. In fact, if the current number of nodes with the same home agent Y_3 is lower than the threshold n^* – where value of n^* is given in the following[4] – then we will need a binding message for each of the $|\Omega_3 - \Omega_2|$ nodes with home agent HA^* that joined the group after time t' – to this regard, note that $(Y_3 - Y_2)$ is likely to be zero as composition of groups is not expected to change frequently. In the opposite case, we will need only one binding message sent to HA^* for all the nodes in Ω_3.

Accordingly, the value of V_{LU} is given by

$$V_{LU} = \begin{cases} Y_3 - Y_2 & \text{if } Y_3 < n^*. \\ 1 & \text{if } Y_3 \geq n^*. \end{cases} \tag{1}$$

It follows that the decrease in the consumption of network resources due to signaling generated for location updates purposes achieved by exploiting object group mobility is given by:

$$\Delta_{\mathrm{LU}} = \lambda_\psi^{(\mathrm{UP})} c^{(\mathrm{LU})} (Z_2 + Y_3 - 1 - V_{LU}) \tag{2}$$

where $\lambda_\psi^{(\mathrm{UP})}$ is the rate associated to the time spent by the group using technology ψ within the radio coverage of the same access point, and $c^{(\mathrm{LU})}$ represents the average amount of network resources consumed for each binding message.

The average value of Δ_{LU} is given by

$$\begin{aligned} &E\{\Delta_{\mathrm{LU}}\} = \lambda_\psi^{(\mathrm{UP})} c^{(\mathrm{LU})}. \\ &\cdot [E\{Z_2 - 1 + Y_2 | Y_3 < n^*\} \cdot p(Y_3 < n^*) + \\ &+ E\{Z_2 - 2 + Y_3 | Y_3 \geq n^*\} \cdot p(Y_3 \geq n^*)] \end{aligned} \tag{3}$$

If we assume that nodes with access technology ψ and home agent HA^* join the group according to an exponential process with rate λ_ψ^* and that each of these nodes leaves the group according to an exponential process with rate μ_ψ^*, then the probability distribution of Y_3 can be calculated as the steady state probability of a $M/M/\infty$ random process: $p(Y_3 = n) = \left(\rho_\psi^*\right)^n \cdot e^{-\rho_\psi^*}/n!$ where $\rho = \lambda_\psi^*/\mu_\psi^*$. Therefore, $p(Y_3 < n^*) = \sum_{n=0}^{n^*-1} \left(\rho_\psi^*\right)^n \cdot e^{-\rho_\psi^*}/n!$ and $p(Y_3 \geq n^*) = 1 - p(Y_3 < n^*)$.

Now we evaluate the first expected value in eq. (3). It is easy to show that

$$E\{Z_2 - 1 + Y_2 | Y_3 < n^*\} = E\{Z_2\} - 1 + E\{Y_2 | Y_3 < n^*\} \tag{4}$$

In order to calculate the average value of Z_2 we apply the theorem of the total probability, so that we can write

$$E\{Z_2\} = \sum_{n=0}^{\infty} E\{Z_2 | Z_1 = n\} p(Z_1 = n) \tag{5}$$

[4]Here we assume that there is only one subgroup of nodes with the same home agent, however, extension to the general case is straightforward.

If we assume that nodes with access technology ψ and home agent different from HA^* join the group with rate λ_ψ and that each of these nodes leaves the group with rate μ_ψ, then the probability distribution of Z_1 can be calculated as follows $p(Z_1 = n) = (\rho_\psi)^n \cdot e^{-\rho_\psi}/n!$ where $\rho_\psi = \lambda_\psi/\mu_\psi$; on the contrary Z_2 can be seen as the value at time t'' taken by a pure death random process that at time t' was in state Z_1. Accordingly, we can rewrite eq. (5) as follows:

$$E\{Z_2\} = \sum_{n=0}^{\infty} p(Z_1 = n) \cdot \cdot \int_0^{\infty} E\{Z_2 | Z_1 = n, t'' - t' = \tau\} f_{T_{\mathrm{UP}}}(\tau) d\tau \quad (6)$$

where $f_{T_{\mathrm{UP}}}(\tau)$ is the probability density function of the random variable T_{UP} representing the time spent by the group within the radio coverage of the same access point. If we assume that T_{UP} is distributed exponentially with average $1/\lambda_{\mathrm{UP}}$, then it is easy to show that the average value of the random variable Z_2 can be calculated as

$$E\{Z_2\} = \lambda_{\mathrm{UP}} \lambda_\psi / \left[\mu_\psi \left(\mu_\psi + \lambda_{\mathrm{UP}}\right)\right] \quad (7)$$

In eq. (4), we also need the average value of Y_2 given that $Y_3 < n^*$. To evaluate such term observe that

$$E\{Y_2 | Y_3 < n^*\} = = \frac{1}{p(Y_3 < n^*)} \sum_{n=0}^{n^*-1} p(Y_3 = n) \cdot E\{Y_2 | Y_3 = n\} \quad (8)$$

It can be shown that

$$E\{Y_2 | Y_3 = n\} = F_1(n, \lambda_{\mathrm{HO}}, \mu_\psi^*, \rho_\psi^*) + F_2(n, \lambda_{\mathrm{HO}}, \mu_\psi^*, \rho_\psi^*) \quad (9)$$

where $F_1(n, \lambda_{\mathrm{HO}}, \mu_\psi^*, \rho_\psi^*) = (n - \rho_\psi^*) \left(1 - e^{-\frac{\lambda_{\mathrm{HO}}}{\mu_\psi^*} \log(\frac{\rho_\psi^*}{\rho_\psi^* - n})}\right)$, $F_2(n, \lambda_{\mathrm{HO}}, \mu_\psi^*, \rho_\psi^*) = \frac{\lambda_{\mathrm{HO}} \rho_\psi^*}{\lambda_{\mathrm{HO}} + \mu_\psi^*} \left(1 - e^{-\frac{\lambda_{\mathrm{HO}} + \mu_\psi^*}{\mu_\psi^*} \log(\frac{\rho_\psi^*}{\rho_\psi^* - n})}\right)$, and λ_{HO} is the handover rate. The second expected value in eq. (3) can be easily calculated as:

$$E\{Y_3 + Z_2 - 2 | Y_3 \geq n^*\} = = \frac{1}{p(Y_3 \geq n^*)} \left[\rho_\psi^* - \sum_{n=0}^{n^*-1} \frac{(\rho_\psi^*)^n}{(n-1)!} e^{-\rho_\psi^*}\right] + E\{Z_2\} - 2 \quad (10)$$

where $E\{Z_2\}$ has been calculated in eq. (7).

However, as we already pointed out, use of OGM can cause an increase in the network resources consumed to deliver data to mobile nodes. In fact, packets sent by a correspondent node will pass through the home agent of the group master before they reach group slaves. Similarly to what we have discussed before, it can be shown that the average value of the difference between the amount of network resources consumed for data delivery when we exploit OGM and what is consumed using traditional mobility management scheme is

$$E\{\Delta_D\} = \lambda_D c_D \left[E\{Z_3\} + E\{V_D\}\right] \quad (11)$$

where:

- λ_D is the average rate at which packets that must be delivered to a mobile object are generated.
- c_D is the average increase in network resource consumption due to the fact that packets that must be delivered to a slave in the group will pass through the group master home agent HA_{GM}.
- V_D is a random variable defined as follows:

$$V_D = \begin{cases} Y_3 & \text{if } Y_3 < n^*. \\ 0 & \text{if } Y \geq n^*. \end{cases} \quad (12)$$

To solve eq. (11) it can be easily shown that $E\{Z_3\} = \rho_\psi$ and

$$E\{V_D\} = E\{Y_3 | Y_3 < n^*\} = \frac{e^{-\rho_\psi^*}}{p(Y_3 < n^*)} \sum_{k=0}^{n^*-1} \frac{(\rho_\psi^*)^k}{(k-1)!} \quad (13)$$

Finally, we want to evaluate the most appropriate value for n^*. To this purpose note that it becomes convenient to use a collective agent when the decrease in resource consumption achieved by using a collective agent is higher than the increase in resource consumption required to send a binding update to the home agent HA^*. This occurs when $\lambda_\psi^{\mathrm{UP}} c^{\mathrm{LU}} < Y_3 \lambda_D c_D$ and $n^* = \frac{1}{1 - (\lambda_D c_D / \lambda_\psi^{\mathrm{UP}} c^{\mathrm{LU}})}$.

B. Impact on localization accuracy and errors

In order to conveniently trade a decrease in uncertainty with the possibility of performing location errors we can define an appropriate cost function that weights the two competing terms for a certain node n_k:

$$c_{\mathrm{Tot}}^{(k)} = c_{\mathrm{Unc}}^{(k)} \cdot H(X_k) + c_{\mathrm{Err}}^{(k)} \cdot \Pr_k\{\mathrm{Error}\} \quad (14)$$

where:

- $c_{\mathrm{Unc}}^{(k)}$ is a term that weights the cost of location uncertainty for node n_k.
- $H(X_k)$ is the entropy (which is a measure of uncertainty [20]) of the random variable X_k representing the current ambience where node n_k is located.
- $c_{\mathrm{Err}}^{(k)}$ is a term that weights the cost of making an error when locating node n_k. Typically, this is higher than the weight of uncertainty, that is, $c_{\mathrm{Unc}}^{(k)} < c_{\mathrm{Err}}^{(k)}$.
- $\Pr\{\mathrm{Error}\}$ is the probability of doing an error in locating node n_k.

Observe, that if group mobility is not taken into account, the error probability is equal to zero whereas location uncertainty is $H(X_k) = \log_2 |\Phi_k|$, where Φ_k represents the set of ambiences where node n_k can be located. Note that if node n_k is reachable by one of the access points, say AP_k, then Φ_k includes the ambience X_k where node n_k is currently located; if node n_k is not reachable by any AP then Φ_k is the set of ambiences that is not covered by any access point of technology $\psi(n_k)$.

We start by evaluating the error probability $\Pr\{\mathrm{Error}\}$.

Suppose that a group Γ has been formed around the group master n_0, that is $\Gamma = \{n_0, n_1, ..., n_k\}$.

Here we are assuming that these $(k+1)$ nodes can exploit different communication technologies $\psi_i, \psi_z, \dots \psi_k$. Also let us suppose that t_0 is the last time instant when the existence of the group was verified. The probability of making an error at time t, with $t \geq t_0$, in the estimation of the position of n_k can be evaluated as the probability that the node has left the group in the time interval $]t_0, t]$. Let T_k be the random variable representing the duration of the time interval during which node n_k (which we suppose is a slave) is aggregated to its master n_0. We assume that T_k is exponentially distributed with rate $1/\mu_k$. Accordingly, the probability of error is

$$\Pr\{\text{Error}\} = \left(1 - \mu_k e^{-\mu_k (t-t_0)}\right) \left(\frac{|\Phi_k| - |\cap_{i=0}^{k} \Phi_i|}{|\Phi_k|}\right) \tag{15}$$

To explain eq. (15), note that exploiting the group mobility concept we guess that node n_k is located in one of the ambiences belonging to the intersection between all sets Φ_i, for $i \leq k$, i.e., we assume that $X_k \in \left(\cap_{i=0}^{k} \Phi_i\right)$. If node n_k is not part of the group anymore, then it is located in any of the ambiences included in Φ_k with equal probability. Accordingly, the probability that exploiting group mobility we incur in misleading localization is given by the probability that node n_k left the group, which is given by the first term of the product in the right hand side of eq. (15), multiplied by the probability that node n_k moved outside the intersection $\left(\cap_{i=0}^{k} \Phi_i\right)$, which is given by the second term of the product in the right hand side of eq. (15).

In order to evaluate the uncertainty on X_k considering that n_k was part of a group mastered by n_0 together with n_1 , n_2 , ..., n_{k-1}, let us define Φ_i the set of ambiences where the generic node n_i can be located.

Accordingly, we are interested in evaluating

$$\begin{aligned} &H\left(X_k | X_k \in \Phi_k, X_{k-1} \in \Phi_{k-1}, ..., X_0 \in \Phi_0\right) = \\ &= -\sum_{X_k \in \Phi_k} p\left(X_k = x_k | X_k \in \Phi_k, ..., X_0 \in \Phi_0\right) \cdot \\ &\cdot \log_2 p\left(X_k = x_k | X_k \in \Phi_k, ..., X_0 \in \Phi_0\right) \end{aligned} \tag{16}$$

The probabilities in eq. (16) can be calculated as follows:

$$\begin{aligned} &p\left(Xk = x_k | X_k \in \Phi_k, ..., X_0 \in \Phi_0\right) = \\ &= \begin{cases} 0 & \text{if } x_k \notin \Phi_k. \\ \frac{p(X_k = x_k, X_{k-1} \in \Phi_{k-1}, ..., X_0 \in \Phi_0)}{p(X_k \in \Phi_k, ..., X_0 \in \Phi_0)} & \text{if } x_k \in \Phi_k. \end{cases} \end{aligned} \tag{17}$$

In the above equation we need the probabilities $p\left(X_k = x_k, X_{k-1} \in \Phi_{k-1}, ..., X_0 \in \Phi_0\right)$ and $p\left(X_k \in \Phi_k, ..., X_0 \in \Phi_0\right)$. By applying the theorem of the total probability, we can calculate the first as follows:

$$\begin{aligned} &p\left(X_k = x_k, X_{k-1} \in \Phi_{k-1}, ..., X_0 \in \Phi_0\right) = \\ &= \sum_{x_0 \in \Phi_0} \cdot \sum_{x_1 \in \Phi_1} \cdots \\ &\cdot \sum_{x_{k-1} \in \Phi_{k-1}} p(X_k = x_k, X_{k-1} = x_{k-1}, ..., X_0 = x_0) \end{aligned} \tag{18}$$

If we refer the position of each node in the group to the position of the group master n_0, the probability in eq. (18) can be calculated as:

$$\begin{aligned} &p(X_k = x_k, X_{k-1} = x_{k-1}, ..., X_0 = x_0) = \\ &= p(X_k = x_k | X_0 = x_0) \dots p(X_1 = x_1 | X_0 = x_0) \cdot \\ &\cdot p(X_0 = x_0) \end{aligned} \tag{19}$$

By replacing eq. (19) in eq. (18) we obtain

$$\begin{aligned} &p\left(X_k = x_k, X_{k-1} \in \Phi_{k-1}, ..., X_0 \in \Phi_0\right) = \\ &= \sum_{x_0 \in \Phi_0} p(X_0 = x_0) \\ &p(X_k = x_k | X_0 = x_0) \sum_{x_1 \in \Phi_1} p(X_1 = x_1 | X_0 = x_0) \\ &\dots \sum_{x_{k-1} \in \Phi_{k-1}} p(X_{k-1} = x_{k-1} | X_0 = x_0) \end{aligned} \tag{20}$$

Observe that at time t the generic conditioned probability needed in eq. (20) can be calculated as follows:

$$\begin{aligned} &p(X_i = x_i | X_0 = x_0) = \\ &= \begin{cases} e^{-\mu_i \tau} + (1 - e^{-\mu_i \tau})/|\Phi_i| & \text{if } x_i = x_0. \\ (1 - e^{-\mu_i \tau})/|\Phi_i| & \text{if } x_i \neq x_0. \end{cases} \end{aligned} \tag{21}$$

where $\tau = (t - t_0)$.

Using eq. (21), it is easy to show that

$$\sum_{x_i \in \Phi_i} p(X_i = x_i | X_0 = x_0) = \begin{cases} 1 - e^{-\mu_i \tau} & \text{if } x_0 \notin \Phi_i \\ 1 & \text{if } x_0 \in \Phi_i \end{cases} \tag{22}$$

Accordingly, if we define the function $\phi_i(x, \Phi)$ as follows:

$$\phi_i(x, \Phi) = \begin{cases} 1 - e^{-\mu_i \tau} & \text{if } x \notin \Phi \\ 1 & \text{if } x \in \Phi \end{cases} \tag{23}$$

then, we can rewrite eq. (20) as

$$\begin{aligned} &p\left(X_k = x_k, X_{k-1} \in \Phi_{k-1}, ..., X_0 \in \Phi_0\right) = \\ &= \textstyle\sum_{x_0 \in \Phi_0} p(X_0 = x_0) p(X_k = x_k | X_0 = x_0) \phi_1(x_0, \Phi_1) \cdot \\ &\cdot \phi_2(x_0, \Phi_2) ... \phi_{k-1}(x_0, \Phi_{k-1}) \end{aligned} \tag{24}$$

The probability $p(X_0 = x_0)$ is, in general, independent of the specific value of x_0; therefore, we denote it as p_0 and can rewrite eq. (24) as

$$\begin{aligned} &p\left(X_k = x_k, X_{k-1} \in \Phi_{k-1}, ..., X_0 \in \Phi_0\right) = \\ &= p_0 \cdot \textstyle\sum_{x_0 \in \Psi_0} p(X_k = x_k | X_0 = x_0) \phi_1(x_0, \Phi_1) ... \dots \\ &\dots \phi_{k-1}(x_0, \Phi_{k-1}) \end{aligned} \tag{25}$$

Analogously, we can calculate the probability $p\left(X_k \in \Phi_k, ..., X_0 \in \Phi_0\right)$ as $\sum_{x_k \in \Phi_k} p\left(X_k = x_k, X_{k-1} \in \Phi_{k-1}, ..., X_0 \in \Phi_0\right)$.

VI. Numerical examples

In this section we use the analysis derived in Section V to evaluate the impact of exploiting OGM on the consumption of traffic resources (see Section VI-A) and on the accuracy of node localization (see Section VI-B).

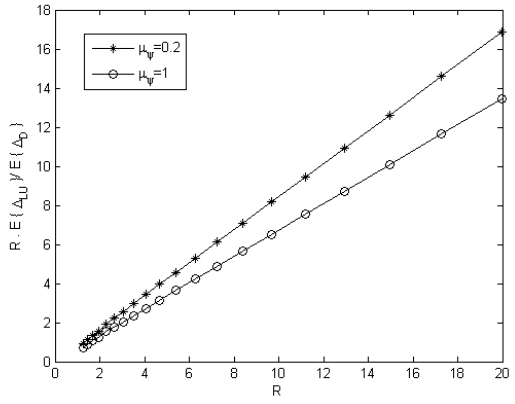

Figure 2. Ratio between $E\{\Delta_{\rm LU}\}$ and $E\{\Delta_{\rm D}\}$ versus the value of the ratio R for two different values of the rate with which nodes leave their group μ_ψ.

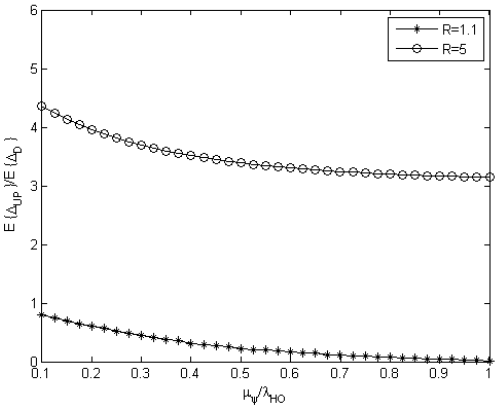

Figure 3. Ratio between $E\{\Delta_{\rm LU}\}$ and $E\{\Delta_{\rm D}\}$ versus the value of the rate with which nodes leave their group, μ_ψ/λ_{HO}, for two different values of the parameter R.

A. Network resource consumption

In this section we use the analysis developed in Section V-A to evaluate the impact of exploiting OGM on the amount of network resources consumed. To this aim, we focus on nodes applying technology ψ and define the parameter R as $R = \lambda_\psi^{(\rm UP)} \cdot c_\psi^{(\rm LU)}/(\lambda_D c_D)$. In Figure 2 we show the ratio between $E\{\Delta_{\rm LU}\}$ and $E\{\Delta_{\rm D}\}$ versus the parameter R for two different values of the parameter μ_ψ, that is $\mu_\psi = 0.2$ and 1 [hour^{-1}]. Other parameters were set as follows: $\rho_\psi = 10$, $\rho_\psi^* = 5$, $\lambda_{HO} = 2$ [hour^{-1}]. In Figure 2 we observe that the improvement in performance achieved exploiting OGM increases as the value of R increases. This result was expected. In fact, an increase in R involves a higher weight for the term taking into account the reduction in signaling produced for mobility management purposes, i.e., $E\{\Delta_{\rm LU}\}$ when compared to the increase in the amount of network resources consumption $E\{\Delta_{\rm D}\}$ due to the fact that packets are likely to pass through the home agent of the group master before they are delivered to slaves. Also by comparing the two curves obtained for the two different values of μ_ψ we note that the lower the value of μ_ψ the more convenient is to exploit OGM for mobility management purposes. This is also an expected result given that lower values of μ_ψ involve that nodes spend longer time within a group.

In Figure 3 we show the ratio between $E\{\Delta_{\rm LU}\}$ and $E\{\Delta_{\rm D}\}$ versus the value of the rate with which nodes leave their group, μ_ψ/λ_{HO}, for two different values of the parameter R.

B. Location accuracy

In this section we consider a group Γ of three nodes n_0, n_1, and n_2 applying three different access technologies: $\psi(n_0)$, $\psi(n_1)$, and $\psi(n_2)$. Let Φ_i represent the set of ambiances covered by the access point $AP(n_i)$, i.e., $\Phi_i = C(AP(n_i))$, and suppose that the rate with which nodes leave the group master is $\mu_1 = \mu_2 = \mu$. We distinguish three different cases as shown in the following:

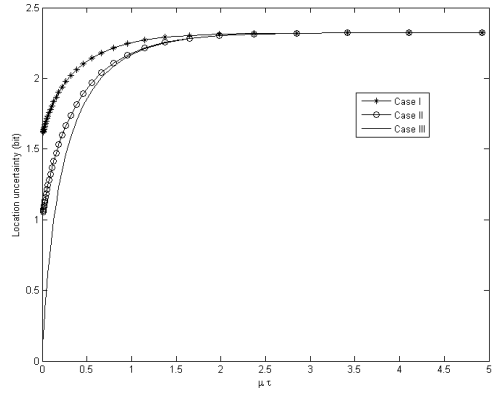

Figure 4. Uncertainty on the position of node n_2, given the location information available for the group, versus the product $\mu\tau$, in the three different cases.

- Case I: $\Phi_0 = \{0,1,2\}$, $\Phi_1 = \{0,1,2,3\}$, $\Phi_2 = \{0,1,2,3,4\}$, $\Phi_0 \cap \Phi_1 \cap \Phi_2 = \{0,1,2\}$
- Case II: $\Phi_0 = \{0,1\}$, $\Phi_1 = \{0,1,2,3\}$, $\Phi_2 = \{0,1,2,3,4\}$, $\Phi_0 \cap \Phi_1 \cap \Phi_2 = \{0,1\}$
- Case III: $\Phi_0 = \{0,1\}$, $\Phi_1 = \{0,2,3\}$, $\Phi_2 = \{0,1,2,3,4\}$, $\Phi_0 \cap \Phi_1 \cap \Phi_2 = \{0\}$

In Figure 4 we represent the uncertainty on the position of node n_2 provided that n_0, n_1, and n_2 are located in one of the ambiences in Φ_0, Φ_1, and Φ_2 versus the product between μ and τ, where τ represents the time elapsed since the last instant in which the state of group Γ was verified. In Figure 4 we plot three curves: one for each of the cases described. Observe that for all three curves we have that the uncertainty on the position of node n_2 increases as time goes by. This

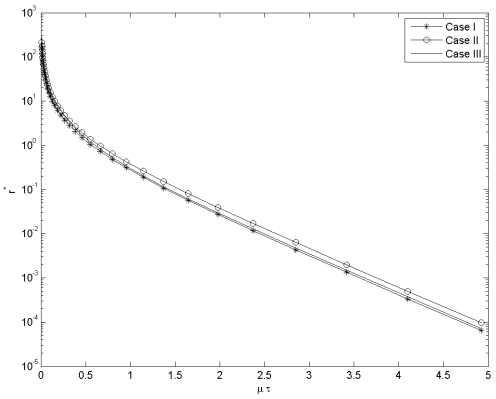

Figure 5. Critical value of the ratio $r^* = c^{(2)}_{\rm Err}/c^{(2)}_{\rm Unc}$ versus the product $\mu\tau$ for the three different cases.

is obvious because the probability that the node has split increases with τ. Also, in the same figure we observe that the uncertainty in Case II is lower than in Case I. This is an obvious result given that the intersection between Φ_0, Φ_1, and Φ_2 is smaller in Case II. The same reasoning can be repeated for Case III, in which we have modified Φ_1 when compared to Case II.

In Figure 5 we represent the values of the ratio $c^{(2)}_{\rm Err}/c^{(2)}_{\rm Unc}$ such that the total cost given in eq. (14) that we obtain exploiting OGM is equal to the total cost obtained with standard solutions. We call such critical value r^*. Obviously, the value of r^* depends on time as shown in Figure 5 where we represent r^* versus the product between μ and τ. Note that given the time interval τ elapsed since the instant when the group state was verified, and given the value of the ratio $c^{(2)}_{\rm Err}/c^{(2)}_{\rm Unc}$ for the specific application scenario we can evaluate if it is convenient to exploit information about the position of the other nodes in the group. Also in Figure 5 we plot three curves, one for each of the cases considered.

VII. Conclusions

In this paper we have studied how object group mobility (OGM) can be exploited to increase localization accuracy and reduce the consumption of network resources in IoT scenarios, while maintaining compatibility with mobile IPv6. We also derived an analytical framework for the evaluation of the impact of exploiting OGM on performance and used it to evaluate assess the improvements that can be obtained. Indeed, numerical results show that localization uncertainty can be decreased significantly and that network resource efficiency can be increased in several system settings.

References

[1] ITU Internet Reports. The Internet of Things (Ed. 2005). Nov. 2005.

[2] Universal Plug and Play. ISO/IEC 29341. Dec. 2008.

[3] EPC global website. http://www.epcglobalinc.org/

[4] INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems, in cooperation with the WG on RFID of the ETP EPOSS, "Internet of Things in 2020, Roadmap for the future" v. 1.1-27 May 2008.

[5] National Intelligence Council. Disruptive Civil Technologies-Six technologies with potential impacts on US Interests out to 2025. *Conference Report CR 2008-07*. Apr. 2008.

[6] Simple Service Discovery Protocol. IETF Internet Draft. Oct. 1999.

[7] L. Atzori et al. The Internet of Things: A survey. *Elsevier Computer Networks* Jun. 2010.

[8] N. Blefari Melazzi. CONVERGENCE: extending the media concept to include representations of Real World Objects. *20th TYWDC: The Internet of Things.* Sept.2009.

[9] A. Chaintreau et al. Impact of human mobility on the design of opportunistic forwarding algorithms. *IEEE Infocom*. Apr. 2006.

[10] L. Galluccio et al.. Spontaneous Group Management in Mobile Ad-Hoc Networks. *Wiley Wireless Networks*. Vol. 10, No. 4. Jun. 2004.

[11] A. Heil et al. The Internet of things-Context-based Device Federations. *IEEE HICSS* Jan. 2007.

[12] D. Johnson et al. Mobility support in IPv6. RFC, http://www.ietf.org/rfc/rfc3775.txt Jun. 2004.

[13] S. D. Lee et al. EPC vs. IPv6 Mapping mechanisms. *Int. Conf. on Advanced Communication Technology* Feb. 2007.

[14] Y. W. Ma et al. Mobile RFID Networking Mechanism Using Address Managment Agent. *NCM* Sep. 2008.

[15] A. Mei, J. Stefa. SWIM: A simple model to generate small mobile worlds. *IEEE Infocom.* Apr. 2009.

[16] G. Montenegro et al. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. *IETF RFC 4944*. Sep. 2007.

[17] Y. Oh et al. A Context management architecture for large-scale smart environments. *IEEE Comm. Magazine*. Mar. 2010.

[18] K. Sampigethaya et al. Caravan: Providing location privacy for Vanet. *ESCAR* Nov. 2005.

[19] H. Schulzrinne et al. Ubiquitous computing in Home Networks. *IEEE Comm. Magazine*. Nov. 2003.

[20] C. Shannon. Prediction and entropy of printed English. *The Bell System Technical Journal*. Vol. 30. Jan. 1951.

[21] W. Wang and I. F. Akyildiz. A new signaling protocol for Intersystem Roaming in Next Generation Wireless Systems. *IEEE JSAC* Vol. 19, No. 10. Oct. 2001.

[22] E. Welbourne et al. Building the Internet of Things Using RFID: The RFID Ecosystem Experience *IEEE Internet Computing*. May 2009.