4

A Location Privacy Aware Network Planning Algorithm for Micromobility Protocols

László Bokor, Vilmos Simon, Sándor Imre
Budapest University of Technology and Economics, Department of Telecommunications, Mobile Communication and Computing Laboratory – Mobile Innovation Centre
Magyar Tudosok krt. 2, H-1117, Budapest Hungary
{goodzi | svilmos | imre}@mcl.hu

1. Introduction

Telecommunication systems both are converging into a complex and synergistic union of wired and wireless technologies, where protocols and terminals will provide integrated services on a universal IP-based infrastructure (Huber, 2004). The Internet itself is evolving towards a more pervasive and ubiquitous architecture in which users are expected to be able to apply different technologies enabling accessibility anytime and anywhere. Not only wireless networks are evolving toward heterogeneous, convergent, broadband, all-IP mobile communication architectures but also end terminals are becoming more and more versatile and powerful devices. Contemporary mobile phones are implementing extremely large scale of functions from making voice and video calls through sharing multimedia and providing Internet connection till exploiting the advantages of geographic positioning solutions — e.g., Global Positioning System (El-Rabbany, 2006) or IP address-based methods (Connolly, Sachenko, & Markowsky, 2003) — in order to use navigational applications and Location Based Services. However mobile terminals' location data possess important service-enabler potentials, in the wrong hands it can be used to build up private and intimate profile of the mobile user. Such a profile can be set up from accurate location information of a user in real time using GPS, network and cell based tracking or even exploiting knowledge of actual IP addresses. There is a strong motivation for creating and maintaining such profiles but the access of this sensitive data must be supervised, controlled and regulated by authorities or even by the operators themselves to ensure privacy protection of mobile users. As mobility becomes one of the most unique characteristics of future's convergent architectures, more attention to the above privacy issues must be given. A whole bunch of new challenges are emerging, but not only solutions to efficiently manage mobile users in the widest range of different application scenarios are needed. More care has to be taken on the privacy issues, even at the earliest phases of design: at the network planning level.
When discussing network planning in next generation, IP based wireless networks, at least two main types of mobility should be considered. On one hand the case when a mobile terminal moves across different administrative domains or geographical regions and thus

changes its actual IP address has to be taken into account (i.e. macromobility). On the other hand, roaming across multiple subnets within a single domain resulting in more frequent address changes also need to be managed (i.e. micromobility). The aim of the latter case is to provide fast, seamless, and local handoff control in areas where mobile nodes change their point of attachment to the network so often that the general macromobility scheme originates significant overhead in terms of packet delay, packet loss, and excrescent signalling (Reinbold & Bonaventure, 2003). Next generation micro-cell based heterogeneous wireless networks are quite sensitive to the above Quality of Service (QoS) factors which implies the spreading of micromobility protocols — e.g., (Valko, 1999), (Bokor, Nováczki, & Imre, A Complete HIP based Framework for Secure Micromobility, 2007), (Soliman, Castelluccia, Malki, & Bellier, 2005) — and the need of advanced network planning algorithms to support real-life deployment issues.

One of the issues of deploying micromobility protocols in next generation mobile environments is the optimal design of micromobility domains. Inside a domain the given micromobility protocol deals with mobility management but at each domain boundary crossing, mobile nodes must register their new locations through signalling messages of the used macromobility protocol in order to update the global address management database for their global reachability. In this way the system is able to maintain the current domain of each user, but this will produce a registration cost in the network. Therefore the question arises, what size (in means of consisting subnets) the micromobility domain should be for reducing the cost of paging, maintaining routing tables and registration signalling. Existing network planning algorithms are focusing on minimizing the signalling costs (Bhattacharjee, Saha, & Mukherjee, 1999), (Pack, Nam, & Choi, 2004), (Loa, Kuo, Lam, & Lic, 2004). In our earlier works we also gave solutions for optimized domain forming, which are capable of reducing the signalling overhead caused by the subnet boundary crossing (Simon & Imre, A Simulated Annealing Based Location Area Optimization in Next Generation Mobile Networks, 2007), (Simon, Bokor, & Imre, A Hierarchical Network Design Solution for Mobile IPv6, 2009). In these studies two main factors were considered. On one hand if we join more and more subnets (i.e., wireless points of attachment with their relevant coverage area) into one micromobility domain, then the number of inter-domain movements will be smaller, so the number of macromobility location update messages sent to the upper levels will decrease. But in the case of big number of subnets belonging to a domain, more possible mobile nodes can join into one micromobility domain (increasing the possibility of routing table explosion), and an incoming call will cause lot of paging messages. On the other hand if we decrease the number of subnets, then we do not need to send so much paging messages (hereby we will load less links and the processing time will decrease too) and the scalability problem can be solved as well, but then the number of domain changes will increase. Therefore the overall problem in micromobility domain planning comes from the trade-off between the paging cost and the registration cost, considering the scalability issues as well.

However, an important factor is left out from all the existing algorithms: the potential of micromobility protocols to efficiently support location privacy has never taken into consideration in any domain planning algorithms available in the literature. The privacy supporting potential of micromobility management lies in the fact that subnet border crossings inside a micromobility domain will remain hidden from the outside world, thus reducing signalling overhead and hiding location information easily exposable by IP

address changes of handovers. Only in cases of inter-domain handovers, the location is updated and revealed to outside of the domain; not on each subnet handover.
This chapter will guide the reader through the evolution steps of network planning algorithms designed to optimally form domain structures for (micro)mobility protocols by introducing all the important methods and schemes. The chapter will also discuss the main privacy issues of next generation mobile and wireless telecommunication systems, focusing on the protection of location information of mobile users in an all-IP world. The importance of location privacy protection in future mobile networks will be emphasized by proposing a novel, uniquely developed and evaluated, simulated annealing based micromobility domain optimization approach, which introduces privacy awareness in network planning methodologies.
The remainder of the chapter is organized as follows. Section 2 presents the background and the related work; Section 3 introduces our novel, simulated annealing-based and location privacy aware network planning algorithm, while in Section 4 the evaluation of the described scheme is detailed. Finally, we conclude the chapter in Section 5 and sketch the scope of future research.

2. Background

As communication architectures evolve, the complex set of user requirements will also align to the changing environmental characteristics. The concept of global reachability fuelled with the advanced mobility schemes and the "anytime, anywhere" paradigm has already started entering the everyday life of people, as real-time multimedia-driven services gain more and more popularity. This is the reason that the requirements for security and privacy in the global Internet era differs a lot from the ones of a decade ago. Despite the fact that the problem space of trust, security and privacy addresses the whole spectrum of computer and communication sciences, this chapter focuses only on a subset of these issues, namely the location privacy questions defined by locators (i.e., IP addresses) in the network layer.

2.1 Location privacy in nutshell

Generally speaking, privacy is procreated as an appropriate combination of anonymity, pseudonymity and unlinkability. Anonymity means that an individual communicating on the network can not be identified by third party entities belonging to a definite group or without some a priori knowledge. The concept of pseudonymity is more permissive compared to anonymity in the means of that it provides protection on the individual's identity but not on linking the actions to the used pseudonym identifier (i.e., supplies no linkability protection). Emanated from this, unlinkability is the feature which prevents traceable bonds between actions of individuals and their identity or pseudonym identifiers. Location privacy is a bit more specific privacy case and its significant influence on the evolution of communication systems in the pervasive computing era was firstly described by (Beresford & Stajano, 2003). Here the authors defined location privacy as the ability to prevent others from learning one's actual or past location. Assuming an all-IP world and global mobility, location privacy concerns the relation between the identifier of a communicating node and its actual or past topological location (Haddad W. , Nordmark, Dupont, Bagnulo, & Patil, 2006), (Koodli, 2007). In the current Internet architecture (which also plays as the basis for all-IP mobile and wireless communication systems), an IP address

not only identifies a node (or an interface) on the network but also serves as the essential element for routing packets through the Internet topology. Accordingly, when an IP packet is sent from one Internet node to another, both sender and receiver entities reveal their topological location (i.e., their IP addresses) in the network, which can then easily be translated to a quite accurate estimation of the peers' current geographical location (Lakhina, Byers, Crovella, & Matta, 2003), (Freedman, Vutukuru, Feamster, & Balakrishnan, 2005), (Gueye, Ziviani, Crovella, & Fdida, 2006), (Baden, 2008) (Eriksson, Barford, Sommersy, & Nowak, 2010), and thus making third parties able to track mobiles' real-life movements or posing other threats to users (Haddad W. , et al., 2006).

In order to protect location privacy in next generation networks, several ideas, schemes and protocols have already been proposed in the literature. These location privacy preserving methods apply various approaches — like policy negotiation and control (Snekkenes, 2001), (Langheinrich, 2002), path confusion (Hoh & Gruteser, 2005), anonymization (Cornelius, Kapadia, Kotz, Peebles, Shin, & Triandopoulos, 2008), change of pseudonyms and mix-zones (Beresford & Stajano, 2003) — which could be deployed either centrally on trusted third-party entities or on end-user terminals to prevent bogus nodes from easily learning past or current locations of communicating hosts. Also various protocol extensions are available implementing protective measures for mobile users' location privacy by advancing existing mobility management protocols and mechanisms. RFC 5726 (Qiu, Zhao, & Koodli, 2010) introduces efficient and secure techniques for Mobile IPv6 nodes (Johnson, Perkins, & Arkko, 2004) to protect their location privacy. For the promising Host Identity Protocol (Moskowitz, Nikander, Jokela, & Henderson, 2008) the HIP Location Privacy Framework was proposed (Matos, Santos, Sargento, Aguiar, Girao, & Liebsch, 2006) where authors cover only part of the location privacy problem space, as some exceptions are allowed on correspondents or trustworthy nodes. A complete HIP location privacy solution was proposed by (Maekawa & Okabe, 2009) where authors decouple identifiers for mobility from identifiers for end-to-end communications and construct an extensional mobility management protocol of BLIND (Ylitalo & Nikander, BLIND: A Complete Identity Protection Framework for End-Points, 2006). Similarly, Stealth-LIN6 (Ichikawa, Banno, & Teraoka, 2006) was proposed for LIN6 (Kunishi, Ishiyama, Uehara, Esaki, & Teraoka, 2000) in order to achieve anonymity of node's identity in the IP layer by dynamic generation of addresses for every single transmission and also to provide anonymity of users' location by introducing special proxy entities in the network.

A further and special kind of protocol extensions providing location privacy in mobile environments is formed by the micromobility solutions which are developed to complement the base macromobility protocols with localized mobility management.

2.2 Micromobility protocols: providers of simple location privacy

Over the past decade a number of micromobility protocols have been proposed, designed and implemented in order to extend the base macromobility protocols like Mobile IPv6 (Johnson, Perkins, & Arkko, 2004) or Host Identity Protocol (Moskowitz, Nikander, Jokela, & Henderson, 2008). The research on such solutions has generated significant interest in industry and academia, aiming to improve global mobility management mechanisms.

One of the most known micromobility solutions is the Cellular IP protocol (Valko, 1999) that introduces a Gateway Router dealing with local mobility management while also supporting a number of handoff techniques and paging. To minimize control messaging,

regular data packets transmitted by mobile hosts are also used to refresh host location information inside the domain. A similar approach is the handoff-aware wireless access Internet infrastructure or HAWAII (Ramjee, Porta, Thuel, Varadhan, & Wang, 1999), which is a separate routing protocol to handle micro-mobility. In TeleMIP (Das, Misra, Agrawal, & Das, 2000) a mobility agent is used to reduce the location update traffic, leading to a new architecture. Terminal Independent Mobility for IP (Grilo, Estrela, & Nunes, 2001) combines some advantages from Cellular IP and HAWAII, where terminals with legacy IP stacks have the same degree of mobility as terminals with mobility-aware IP stacks. Nevertheless, it still uses Mobile IP for macro-mobility scenarios. Auto-Update Micromobility (Sharma & Ananda, 2004) exploits the hierarchical nature of IPv6 addressing and uses specialized mechanisms for handover control, while µHIP (Bokor, Nováczki, & Imre, A Complete HIP based Framework for Secure Micromobility, 2007) integrates micro-mobility management functionalities into the Host Identity layer by introducing a local rendezvous server into the architecture and uses macromobility capabilities of HIP for global mobility. Multicast-based Micromobility (Helmy, Jaseemuddin, & Bhaskara, 2004) is a local mobility management method where a visiting node gets multicast address to use while moving inside a domain, and intra-domain handover is realised using multicast join/prune mechanisms. Anycast-based Micromobility (Bokor, Dudás, Szabó, & Imre, 2005) is similar to M&M: a mobile node obtains a unique anycast care-of address, forms a virtual anycast group, and lets the underlying anycast routing protocol to handle the intra-domain movements. Hierarchical Mobile IPv6 (Soliman, Castelluccia, Malki, & Bellier, 2005) is also a well-known and significant micromobility solution to reduce the number of signalling messages to the home network and to reduce the handover latency. The basic idea of this approach is to use domains organized in a hierarchical architecture with a mobility agent on the top of the domain hierarchy. The deployment of such agents will reduce the signalling load over the air interface produced by Mobile IPv6, by limiting the amount of Mobile IPv6 signalling outside the locally managed domain. A novel, network-based paradigm for micromobility management is called Proxy Mobile IPv6 (Gundavelli, Leung, Devarapalli, Chowdhury, & Patil, 2008), that is based on the concept that the network provides always the same home prefix to the MN independently of its point of attachment to the domain. Special anchor and gateway entities are responsible in the network for tracking the movements of the mobiles and initiating the required mobility signalling on behalf of them.

As the above examples show and (Reinbold & Bonaventure, 2003) express, micromobility protocols denote mobility signalling between the mobile node and an intermediate node (real or virtual) that is located in the local operator network, and at the same time hide inside locators from the outside world. The routing path that goes via the intermediate node offers location privacy for end hosts because it obliterates the actual location of the host while it roams within a micromobility domain: mobiles can benefit from local mobility, which hides the regional movement from the peer nodes, optimizes the signalling between end terminals, therefore reduces the handoff related latency and increases location privacy (Ylitalo, Melen, Nikander, & Torvinen, 2004). This behaviour is similar to the operation of privacy proxies (Reed, Syverson, & Goldschlag, 1998). Note, that such usage necessitates that the intermediate node/proxy is trusted to keep the mobile's real locator (i.e., inside domain address) secret.

In this article we focus on these micromobility proposals, more precisely on how to design and form micromobility domains for extending location privacy protection capabilities of micromobility protocols.

2.3 Optimization of micromobility domains

The problem is that none of the existing micromobility protocols addresses the realization of the domain structure in detail; none provides clear guidance or instructions for network design. It is not clear and usually hard to determine the size of a micromobility area (i.e., locally administrated domain). Several important questions arise: how to group wireless points of attachments with their relevant coverage (like cells in cellular networks) into different micromobility domains, what kind of principles must be used to configure the hierarchical levels if the protocol makes them able to be applied (like in case of HMIPv6), and in which hierarchical level is advisable to implement special functions like mobility anchors or gateways. The traffic load and mobility of mobile nodes may vary, therefore a fixed structure lacks of flexibility.

The key issues here are on which level of hierarchy to deploy the anchor/gateway functionalities, and how to group wireless point of access nodes (access routers) and the coverage areas they implement, actually how many cells should be beneath an anchor or gateway node within a single domain. An obvious solution is to group those cells and access nodes into one domain, which has a high rate of handovers among each others. In that way the number of cell and access router changes for the mobile hosts will be decreased. But joining too much cell and access router into one domain would degrade the overall performance since it will generate a high traffic load on anchor/gateway nodes, which results in a high cost of packet delivery (Casteluccia, 2000). Contrarily a small number of cells inside a micromobility domain will lead to a huge amount of location updates to the home network. Based on these assumptions, (He, Funato, & Kawahara, 2003) proposed a dynamic micromobility domain construction scheme which is able to dynamically compose each micromobility domain according to the aggregated traffic information of the network. The related questions are very similar to the Location Area (LA) planning problem where cells must be grouped into location areas in an optimal way (Markoulidakis, Lyberopoulos, Tsirkas, & Sykas, 1995), (Tabbane, 1997), (Rubin & Choi, 1997), as in micromobility domain planning we also need to search for a trade-off compromise between the location update and the packet delivery cost.

One of the most known LA planning schemes is the solution called Traffic-Based Static Location Area Design – TB-LAD (Cayirci & Akyildiz, 2003), that groups cell pairs with higher inter-cell mobile traffic into the same LA. In this algorithm a list of neighbours is created for each cell, in a decreasing order by the inter-cell traffic. The neighbour with the highest inter-cell traffic will be selected from the list and included in the same LA with this cell. In the next step the algorithm finds neighbours with the highest traffic from the neighbour lists of the cells that are included for the current LA and includes them into the current LA. This is terminated, when there are no more neighbours that can be included or the maximum number of cells is reached for the current LA. After this loop the algorithm starts the forming of the next LA in the same way. However, in case of the Location Area Forming Algorithm - LAFA (Simon & Imre, 2009), LAs are not formed one after the other, but simultaneously, always including the actual cell-pair to an already existing LA or creating a new one, enabling to build the LA structure in a distributed way. Based on the

experiments of LAFA, the duet of the Greedy LA Forming Algorithm (GREAL) and the Simulated Annealing Based Location Area Forming Algorithm (SABLAF) was proposed by (Simon & Imre, A Simulated Annealing Based Location Area Optimization in Next Generation Mobile Networks, 2007). In this scheme GREAL is adopted to form a basic partition of cells into LAs in a greedy way without any additional assumptions for cell contraction, and then SABLAF is applied for getting the final partition. Authors of (Prajapati, Agravat, & Hasan, 2010) also proposed a similar simulated annealing based LA planning method giving a heuristic and near-optimal solution for LA planning in tolerable run-times. There is also a specific Location Area planning algorithm for GEO Mobile Satellite Systems: by the way of extensive comparison of the cost of location management using different types of location area designs, an appropriate scheme was separated by the authors satisfying the special requirements of GEO satellite systems (Qian, Guang-xia, Jing, Yi-qun, & Ming, 2010).

A dominant part of current Location Area and micromobility domain planning algorithms is not able to handle network structures with hierarchical levels. Despite the fact that there are existing proposals for that deficiency (Simon, Bokor, & Imre, A Hierarchical Network Design Solution for Mobile IPv6, 2009), (Pack, Choi, & Nam, 2006), in this work we still stick to the "flat nature" of the original idea. However this study does not consider hierarchical structures, our contribution is still applicable in those cases.

It is important to emphasise that while there exists quite a broad literature on location area and micromobility domain forming, it leaves a substantial and a-priori question unexplored: how to integrate location privacy requirements into the algorithms. To the best of our knowledge, at the time of the writing this is the first study about location privacy aware micromobility domain planning.

3. A location privacy aware network planning algorithm

3.1 Motivation

As we introduced above, an open question of any micromobility proposal and domain/LA forming algorithm is the optimal design of the domains, aiming to minimize the signalling costs while to maximize the domains' location privacy protection capabilities at the same time. At each domain boundary crossing, mobile hosts reveal and register their new locations through signalling mechanisms of the applied macromobility protocol (e.g., Mobile IPv6) in order to update the global location management database (i.e., the Home Agent in case of MIPv6) and their actual peer nodes. In this way the network is able to maintain the current location of each user, but this will produce a registration cost in the network and will go hand in hand with the disclosure of the actual location to potential bogus nodes. Therefore the question arises: what size the micromobility domain should be for reducing the cost of paging and registration signalling, and increasing built-in location privacy. On one hand if we join more and more cells into one domain, then the number of inter-domain handovers will be smaller, so the number of macromobility location update messages sent to the upper levels will decrease. Also the domain's potential to hide inside movements of mobile terminals from the outside network will become more powerful and effective. But in the case when big number of cells belong to a single domain, more possible mobile nodes can join into one micromobility area (such increasing also the possibility of routing table explosion), and an incoming call will cause tremendous paging overhead. On

the other hand if we decrease the number of cells, then we do not need to send so much paging messages (hereby we will load less links and the processing time will decrease, too) and the scalability problem can be solved as well, but then the number of subnet changes will increase and the location privacy of mobile nodes moving between different domains gets more vulnerable. Therefore the overall problem in location privacy aware micromobility domain planning comes from the trade-off between the paging cost and the registration cost, considering the location privacy issues as well.
In order to deal with this, we qualify the paging cost as a constraint; therefore the registration cost is left alone in the objective function. Hence we define and formulate a problem in which the final goal is the determination of optimum number of cells per a domain for which the registration cost is minimum, with the paging cost limitation as an inequality constraint function. Based on this cost structure we propose a domain optimization algorithm that contains two phases: first a greedy grouping is adopted which forms a basic partition of cells or any kind of point of access nodes into micromobility domains by also using a rate weighting technique to cover location privacy issues of micromobility, and then a simulated annealing based algorithm is applied for getting the final and near-optimal partition within tolerable run time. This novel network planning solution is a natural extension of our former, simulated annealing based domain optimization methods (Bokor, Simon, Dudás, & Imre, 2007), (Simon & Imre, A Simulated Annealing Based Location Area Optimization in Next Generation Mobile Networks, 2007). We designed and implemented a realistic mobile environment simulator in order to generate the algorithm input metrics (cell boundaries crossing and incoming session statistics, location privacy model parameters, etc.,), and to execute and study the algorithms with and without location privacy awareness for extensive comparison and performance analysis.

3.2 Cost structures

The goal of employing micromobility is to keep the boundary crossing between different coverage areas (e.g., cells) inside a well defined local domain (i.e., hidden from the upper levels), therefore an administrative message for the global registration of the new location of the mobile host will not be generated during intra-domain handovers, and also location privacy is provided for hosts moving inside the domain. Hence for the purpose to make calculations about the movement of mobile nodes among the domains and such temporarily loosing their location privacy protection, a simple and well known choice is the fluid flow model. The fluid flow model characterizes the aggregate mobility of the mobile nodes in a given region (for example micromobility domain) as a flow of liquid. The model assumes that hosts are moving with an average speed v, and their direction of movement is uniformly distributed in the region. Hence the rate of outflow from that region can be described by (Kumar, Umesh, & Jha, 2000)

$$R_{out} = \frac{v \cdot \rho \cdot P}{\pi} \tag{1}$$

where v is the average speed of the mobile nodes (MN), ρ is the density of mobiles in the region and P is the perimeter of the given region. This model is very simple and

convenient to analyze and to use for the definition of the registration cost function. We can define easily the density of the mobile nodes in a domain:

$$\rho = \frac{K}{N_k \cdot S} \tag{2}$$

where K is the number of mobile hosts in the k th domain, N_k is the number of cells in the k th domain, and S is the area of a cell.
Every time when a mobile node crosses a cell boundary which is micromobility domain boundary also, a global registration process is initiated, and a special update message is sent to the upper level. This signalling cause the registration cost and that the location information of the mobile node can be revealed to third parties and communication peers. From this point of view the intra-domain boundary crossing is negligible, and this handoff cost should be not considered in the registration cost. Similarly to (Bokor, Simon, Dudás, & Imre, 2007), we need to determine the number of cells located on the boundary of the k th micromobility domain, like a subset of N_k, and the proportion of the cell perimeter which contributes to the k th domain perimeter. Using this, the perimeter of the k th domain:

$$P_k = N_p \cdot \nu_p\left(N_k\right) \tag{3}$$

where N_p is the number of boundary cells in the k th domain, and ν_p is the average proportion of the boundary cell perimeter in the k th domain perimeter in the function of N_k. The number of the boundary cells can be approximated according to (Simon & Imre, A Domain Forming Algorithm for Next Generation, IP Based Mobile Networks, 2004):

$$N_p = \kappa \cdot \sqrt{N_k} \tag{4}$$

The average proportion of the cell perimeter which will be the part of the domain perimeter too can be expressed with an empirical relation (Bhattacharjee, Saha, & Mukherjee, 1999):

$$\nu_p\left(N_k\right) \approx \nu \cdot \left(a + b \cdot {N_k}^{\eta - 1}\right) \tag{5}$$

where ν is the perimeter of a cell and $a = 0.3333$, $b = 0.309$, $\eta = 0.574965$. Substituting the values of N_p and $\nu_p\left(N_k\right)$ in (3), the expression for the perimeter of the k th domain becomes:

$$P_k = \kappa \cdot \sqrt{N_k} \cdot \nu \cdot \left(a + b \cdot {N_k}^{\eta - 1}\right) \tag{6}$$

Therefore the number of crossing the k th micromobility domain boundary can be given by substituting the values of ρ and P_k in the outflow rate of the fluid flow model:

$$R_{out} = \left(\frac{v \cdot \frac{K}{N_k \cdot S} \cdot \kappa \cdot \sqrt{N_k} \cdot \nu \cdot \left(0.333 + 0.309 \cdot N_k^{-0.425}\right)}{\pi} \right) \tag{7}$$

As we mentioned earlier a registration process is initiated when the mobile node crosses a cell boundary which is also a domain boundary, hence the total registration cost will be:

$$C_{\mathrm{Re}g_k} = B_{LU} \cdot R_{out} \tag{8}$$

$$C_{\mathrm{Re}g_k} = B_{LU\cdot} \cdot v \cdot K \cdot \kappa \cdot \nu \cdot \left(\frac{0.333 \cdot N_k^{-0.5} + 0.309 \cdot N_k^{-0.925}}{\pi \cdot S} \right) \tag{9}$$

where B_{LU} is the cost required for transmitting a global location update message. The final goal is the determination of optimum number of cells per a micromobility domain for which the registration cost is minimum and the domains' location privacy protection potential is maximum, with the paging cost as an inequality constraint function.

To have a feasible micromobility support, the network capacities assigned for paging should not be exceeded; therefore we need to define a paging constraint per micromobility domains. The limited network capabilities of locating the exact location of a stand-by mobile node in case of an incoming session will cause a limit on the peak session arrival rate; therefore we need to define an upper paging cost constraint for every domain. The paging cost for the k th domain should not exceed the paging cost constraint (the paging cost for the k th micromobility domain will be the sum of C_{P_i} over the N_k cells):

$$C_{P_k} = \sum_{i=1}^{N_k} C_{P_i} = \sum_{i=1}^{N_k} B_P \cdot N_k \cdot \lambda_i < C_k \tag{10}$$

$$C_{P_k} = B_P \cdot N_k \cdot \sum_{i=1}^{N_k} \lambda_i < C_k \tag{11}$$

where B_P is the cost required for transmitting a paging message and λ is the number of incoming sessions terminated to a mobile node. If we assume that the mobile hosts have the same average number of terminated sessions for all cells in the k th domain ($\lambda_i = \lambda$), the paging cost reduces to

$$C_{P_k} = B_P \cdot N_k \cdot K \cdot \lambda < C_k \tag{12}$$

3.3 Cost optimization

The problem is to find the optimum number of cells per a micromobility domain for which the registration cost is minimum and the paging constraint (C_k must not be exceeded) is satisfied. If we know that the session arrivals (λ) follow a Poisson process and the function

of the registration cost (9) is a monotonically decreasing function, the paging constraint can be expressed in the following way:

$$P(C_{P_k} < C_k) < 1 - e^{-\gamma} \tag{13}$$

where $\gamma = (10,100)$, depending on the accuracy of the paging constraint. The monotonically decreasing attribute of the registration cost function and the nature and modality of location privacy provision inside micromobility domains will mean, that we need to find the highest value of the N_k for which the (13) will be still satisfied.
Substituting the expression of the paging cost in (13):

$$P(B_P \cdot N_k \cdot K \cdot \lambda < C_k) < 1 - e^{-\gamma} \tag{14}$$

Furthermore if we know that the λ probability variable follows a Poisson process, then the maximum value of N_k can be easily calculated ($N_{\max}$):

$$P(\lambda < \frac{C_k}{B_P \cdot N_k \cdot K}) = 1 - e^{-\gamma} \tag{15}$$

Substituting the calculated value of N_k in (9) will give us the minimum of the registration cost. We will use this calculated N_k as an input for our location privacy aware micromobility domain forming algorithm.

3.3 The algorithm

The optimal partitioning of cells into micromobility domains is proofed to be an NP-complete problem (Cayirci & Akyildiz, 2003). Since the time required solving this problem increases exponentially with the size of the problem space, no algorithm exists that provides the optimal result within acceptable run times. Therefore, special techniques offering near-optimal solutions in reasonable amount of time are needed. A suitable approach is the use of heuristic approximation that runs in polynomial-time for finding the optimum or near-optimum cell configuration.
Simulated annealing is considered as an effective approximation scheme fitting to this specific application and also to various problems in general. Simulated annealing is a random-search method that exploits the analogy between the way in which metals cool and freeze into their minimum-energy crystal structure (the so called annealing process) and the search for a minimum in a general space (Laarhoven & Aarts, 1987). By this analogy, each step of a simulated annealing-based heuristic algorithm replaces the current solution by a "neighbouring" solution from the solution space, randomly chosen with a probability depending on the difference between the corresponding function values and on a global parameter called the Temperature, which is gradually decreased during the run. The technique grants the basis of a whole family of optimization schemes for combinatorial and

other mathematical challenges and also for dealing with highly nonlinear problems. This motivated us to use simulated annealing in order to find a near-optimal solution in our cell partitioning problem without searching the entire solution space.

As we described, the registration cost is proportional to the number of handovers among different domains (q), therefore the registration cost can be minimized by designing the domains such that the cells belonging to one domain have the lowest boundary crossing rates among each other. However, if location privacy is to be taken into consideration, the crossing rates also must contain location privacy specific information from both user and the network side. This is achieved by introducing a simple location privacy policy model and a special rate weighting technique.

In the location privacy policy model we applied, a combination of cells' static location privacy significance and mobile nodes' location privacy profile creating dynamic demands in the network is used to provide boundary conditions for location privacy aware domain planning.

From the mobile network operators' perspective we can separate coverage areas considered to be more sensitive to location privacy than others. In order to capture the difference in this sensitivity, we introduce the *static location privacy significance level of the cells*. This attribute defines what level (in scale of 1-5) of location privacy protection is required at a given cell in the design phase, such allowing for network designers to take maximally into consideration the operator's location privacy requirements and needs.

Mobile node's location privacy profile for different location types is defined to describe what level (in scale of 1-5) of location privacy protection is required for a mobile user at a given type of location. We specified four types of location for cells (micro-cell at home, workplace, hospital or hotel), and mobile nodes –when entering a certain type of cell– can announce their required level of location privacy protection for that cell type. These dynamic demands are cumulated during the cell operation. The average of the cumulated demands will be compared with the static location privacy significance level of the issued cell at every announcement, and the bigger value – named as the cell's *overall location privacy factor* – will take over the role of the cell's static significance level. In this simple way not only operators' requirements, but also the dynamic demands of mobile users can be respected during the location privacy aware network design.

Our special *rate weighting technique* is used to integrate the effects of the cells' static location privacy significance and mobile nodes dynamic demands into the boundary crossing rates between neighbouring cells. According to the mathematical representation we use (where the cells are the nodes of a graph, and the cell border crossing directions are represented by the graph edges) weights can be defined to the edges of this graph based on the cell border crossing (i.e., handover) rates of every direction (i.e., rates of entering or leaving a cell are summarized and assigned to the corresponding edge as its weight). These rates are weighted with the overall location privacy factor of the destination cell, as the *weighted rate* is generated by the sum of product of every incoming and outgoing rate and their appropriate destination cell's overall location privacy factor, respectively:

$$WRate_{[k][l]} = Rate_{[k][l]} \cdot OverallLocPFact_{[l]} + Rate_{[l][k]} \cdot OverallLocPFact_{[k]} \quad (16)$$

where $WRate_{[k][l]}$ is the weighted rate of edge between cells (graph nodes) k and l, the notation of $Rate_{[k][l]}$ stands for the cell border crossing rate from cell k to l, and the $OverallLocPFact_{[l]}$ is the overall location privacy factor of cell l.

Based on the above, our location privacy aware micromobility domain planning algorithm will start with a greedy phase that will provide the basic domain partition as an input (i.e., initial solution) of the simulated annealing. In the beginning of this greedy phase, we choose the cell pair with the biggest weighted rate in our cell structure ($q_{\max}$). If there is more than one biggest rate, then we choose one of them randomly and include the two cells belonging to that handover rate into the $Domain_1$ set of cells. In the next step, we search for the second biggest weighted rate (if there are more than one, we choose it in the same way as in the first step) among the cell pairs for which is true, that one of them belongs to the $Domain_1$ set of cells. We must check if inequality

$$N_k < N_{\max} \tag{17}$$

satisfied, where $N_{\max}$ is the maximum value of N_k calculated from (15), namely the maximum possible number of cells in a single micromobility domain which will give us the minimum of the registration cost and the maximum size of the location privacy protective micromobility domain. If the inequality is satisfied, the cell can be included into the $Domain_1$ set of cells. If the inequality is not satisfied, the cell can not be included into this set in order to prevent exceeding the paging cost constraint (12). In this way we can join the most important cells according to the location privacy policy model which are also in the same dominant moving directions (highways, footpaths, etc.,). Therefore the number of handovers among domains can be decreased while the location privacy is also considered in the created structure.

After the processing of all cell pairs in the above sequential and greedy way, a system of domains will be created, which is likely not the optimal solution. However, this will be only a basic domain partition which will serve as an input to the simulated annealing based domain forming scheme.

The simulated annealing procedure starts with this basic partition or initial solution s_0. A neighbour to this solution s_1 is then generated as the next solution, and the change in the registration cost $\Delta C_{Reg}(s_0, s_1)$ is evaluated. If a reduction in the cost is found, the current solution is replaced by the generated neighbour, otherwise we decide with a certain probability set to $e^{\left(-\frac{\Delta C_{Reg}}{T}\right)}$ (usually called the acceptance function) whether remains or becomes the current solution, where T is the control parameter (i.e., the temperature in the simulation annealing terminology). The algorithm is started with a relatively high value of T, to have a better chance to avoid being prematurely trapped in a local minimum. The cooling schedule consists of three parameters, used like an input to the algorithm: the initial temperature (T), step of decrement ($decr$), and the stopping rule of the algorithm. The stopping rule is the maximal iteration step number or maximum number of steps when ΔC_{Reg} do not changes. Another important input parameter is the calculated maximum

number of cells in a micromobility domain ($N_{\max}$). The performance of our algorithm depends heavily on the cooling schedule and the initial partition, which should be carefully investigated and optimized to have the best results. The detailed flowchart of the whole algorithm is depicted on Fig. 1.

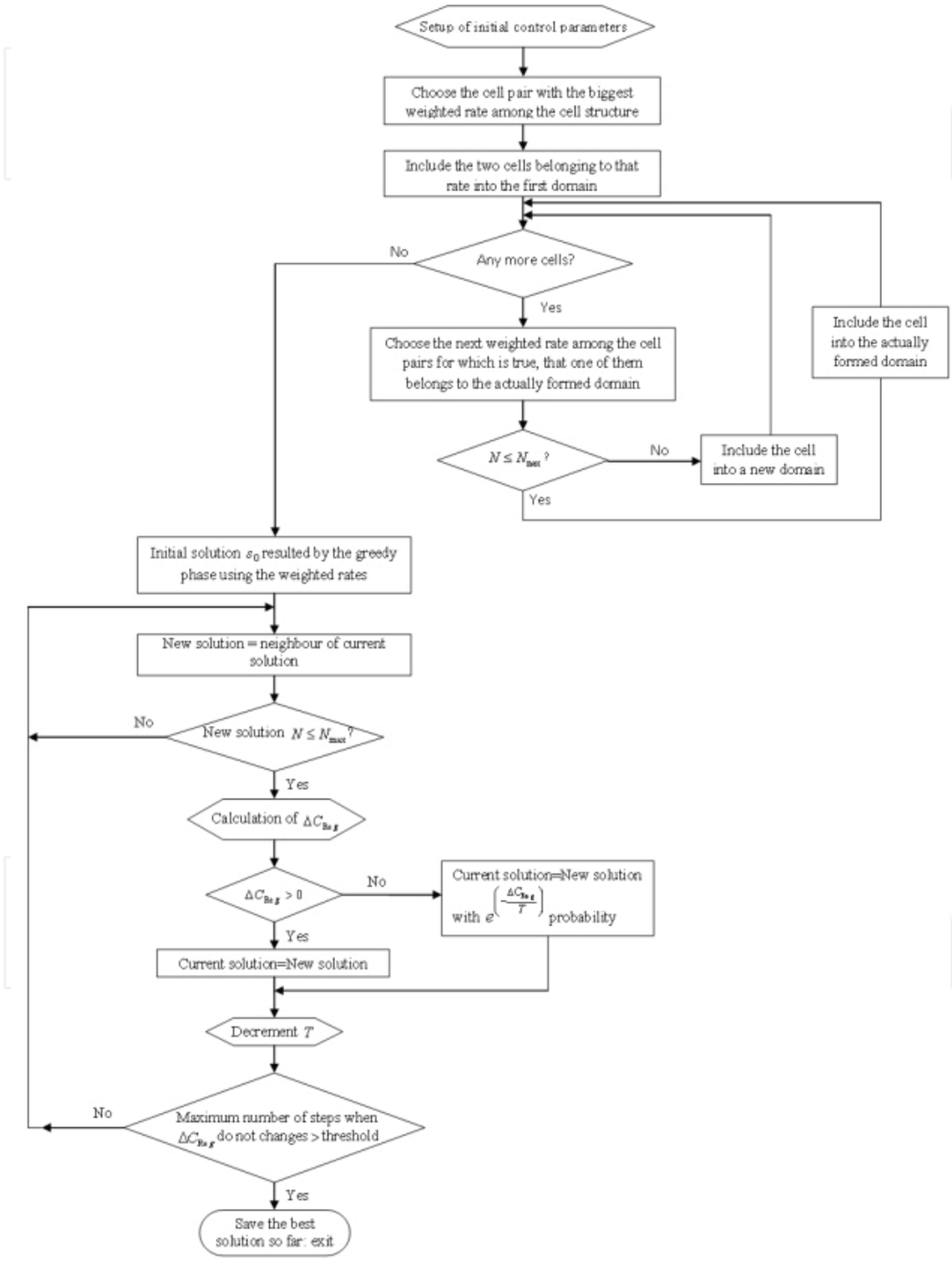


Fig. 1. The detailed flowchart of our proposed location privacy aware domain planning algorithm

4. Evaluation

4.1 The simulation framework

In order to evaluate our algorithm and analyse its performance in real-life scenarios, we designed and implemented a realistic, Java-based mobile environment simulator, which serves a two-fold purpose. On one hand it will generate a realistic cell boundary crossing and incoming call database in a mobile system given by the user with cell, mobile node and movement path placing. It also calculates both the handover rate and the location privacy-weighted rate for each cell pair, defined on the border of these cells. The incoming session statistic can be also generated for every cell; therefore the paging cost and the registration cost can be calculated in the same time for every domain. On the other hand the simulator uses the above produced data as an input for the widest scale of LA and domain planning algorithms, and forms LAs and micromobility domains by running the implemented mathematical functions, e.g., our novel simulation annealing-based, location privacy aware micromobility domain planning algorithm.

As Fig. 2 shows, an arbitrary and customizable road grid can be given and then covered by cells of various access technologies (e.g., WiFi, GSM, UMTS) using the simulator's graphical user interface. The static location privacy significance level of the cells can also be set from 1 to 5 during the cell placement as well as the location type (micro-cell at home, workplace, hospital or hotel). Then the user of the simulator can place communicating mobile nodes firstly by choosing between MNs of different velocities, setting the incoming call arrival parameter (call intensity) and the location privacy profile for different location types to every mobile node.

This way different types of mobility environments with different location privacy characteristics can be designed (rural environment with highways without strict location privacy requirements or a densely populated urban environment with roads and carriageways and the widest scale of location privacy sensitive areas like military facilities, government buildings, etc.,), together with the grids of cells configured and adapted to these environments. The different mobile terminals will move on the defined road grid, continuously choosing randomly a destination point on the road, similarly as in real life. Since typical mobile users are on the move aiming to manage a specific duty or reach a particular destination (e.g., heading to a hotel, a workplace, a hospital, etc.,) and they usually want to arrive in the shortest possible time, therefore the Dijkstra algorithm is used in our simulation framework in order to find the shortest path for mobile hosts towards their selected destination. For every mobile node an incoming call arrival parameter is defined and when an incoming call hits the node, the simulator designates it to the cell where the node is in that moment. When a mobile host changes a cell, the simulator registers that a handover (i.e., cell boundary crossing) happened between the respective cell-pair. When a simulation run ends, the simulator sums the cell boundary crossings and incoming call distribution for every cell in the simulated network, and also calculates the normal and the location privacy-weighted rates for the LA and micromobility domain planning algorithms. The results (road structure, cell structure, call numbers and cell matrix, mobile data) can be saved and opened to easily provide inputs for the Java implementation of our algorithms.

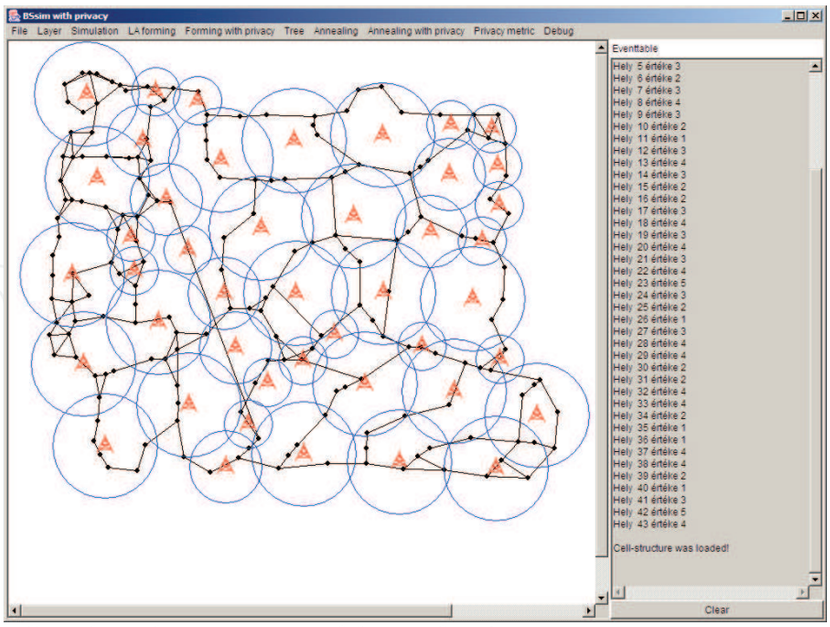


Fig. 2. Initial cell and road structure used for evaluation

Our goal with this mobility simulator was to provide a flexible tool which is able to give the possibility to evaluate Location Area partitioning and micromobility domain planning algorithms for the widest scale of network types, by freely choosing the road grid, communicating mobile hosts and cell structure and characteristics. During our measurements we used our former, simulated annealing based domain optimization method (Bokor, Simon, Dudás, & Imre, 2007) as a basis to compare with the location privacy aware algorithm variant, and also developed a special location privacy metric in the simulator for this comparison.

4.2 Location privacy metric

In order to evaluate the potential and effectiveness of location privacy preserving methods in terms of assessing, quantifying or measuring the abstract concept of location privacy, several metrics are introduced and examined in the literature. (Diaz, Seys, Claessens, & Preneel, 2002) present an information theoretic model that allows to measure the degree of anonymity provided by schemes for anonymous connections. Authors of (Serjantov & Danezis, 2003) introduce an information theoretic measure of anonymity that considers the probabilities of users sending and receiving the messages and also show how to calculate this measure for a message in a standard mix-based anonymity system. The main advantage of this proposal is its capability of not only comparing the effectiveness of different systems, but also evaluating the strength of different attacks. The study of (Shokri, Freudiger, Jadliwala, & Hubaux, 2009) first presents a formal model, which provides an efficient representation of the network users, the bogus entities, the location privacy preserving solutions and the resulting location privacy of users. By using this model, authors provide formal representations of four location privacy metrics among the most relevant categories (uncertainty-based metrics, “clustering error”-based metrics, traceability-based metrics, K-anonymity metrics), and also develop a novel metric for measuring location privacy (called

the distortion-based metric), which estimates location privacy as the expected distortion in the reconstructed users' trajectories by an attacker.
Based on the literature we can say that perfect and ideal location privacy metric would capture the exact amount of information that bogus nodes may have about mobile users' actual positions or trajectories. It also means that an ideal location privacy metric should be able to quantify the incapacity of a particular bogus node in localizing or tracking mobile users. Existing location privacy metrics do not utterly capture these attributes of location privacy, often are too specific to particular protocol or scheme, and many times are not able to perfectly represent issues of location privacy because several were not originally designed for mobile networks. Moreover, to the best of our knowledge none of the published location privacy metrics is supposed to help domain or location area planning purposes and none of them focuses on the location privacy peculiarities of micromobility protocols.
It is out of scope of this paper to answer all the above questions and problems and to give a general solution for quantifying location privacy. Our goal, by defining a simple location privacy metric in this section, is to express, that how effectively a given micromobility domain structure takes static location privacy significance of cells and the incoming dynamic location privacy demands of users into account during operation (i.e., how effective could be the protection of users' location privacy while keeping paging and registration costs on a bearable level). In order to achieve this we quantify the inability of non inside-domain attackers in tracking mobile users by computing a weighted number of inter-domain changes of mobile nodes in the network. This is implemented by an extension to our mobility simulator.
During the simulation we track and save movements (i.e., whole paths) of mobile users and also save cell boundary crossings. After running a domain forming algorithm and such creating a domain structure from cells, these savings will help us to localize and count inter-domain changes for every mobile terminal. For every inter-domain handover of a mobile node and for the previous and the next cells of such handovers we sum the value of the cells' static location privacy significance and the squared value of the level of the mobile node's location privacy profile set for the issued location types. We perform the above calculation for every mobile node, and the sum of these values will stand for the location privacy metric of a network containing several micromobility domains. This metric is able to numerically present the location privacy capabilities of a complete network's certain micromobility domain structure: the less the value of the metric is, the higher protection of location privacy will mobile users inherit from micromobility.

4.3 Results

We have tested our novel location privacy aware micromobility domain planning algorithm in a randomly structured complex architecture consisting of 43 cells, 32 mobile nodes and a compound road grid, depicted in Fig. 2. Using this environment we compared our location privacy aware network design scheme with its ancestor which is also a simulated annealing based micromobility domain forming algorithm but without any trace of location privacy awareness (Bokor, Simon, Dudás, & Imre, 2007), (Simon & Imre, A Simulated Annealing Based Location Area Optimization in Next Generation Mobile Networks, 2007).
As an initialization of our experiments we ran the mobility simulator on the example network of Fig. 2 for many thousands of handovers in order to produce all the required realistic input data (e.g., the boundary crossing and incoming session database) for the two

solutions we compared and analysed. After that we executed the two algorithms under evaluation (both with parameters $N_{\max} = 7$, $T = 100$, and $decr = 2$) on the produced input data and cell structure in order to render the two domain configuration. Fig. 3 shows the generated micromobility domain structure when the location privacy requirement was not taken into consideration (scenario A), while Fig. 4 presents the result after running our location privacy aware micromobility domain planning algorithm (scenario B).

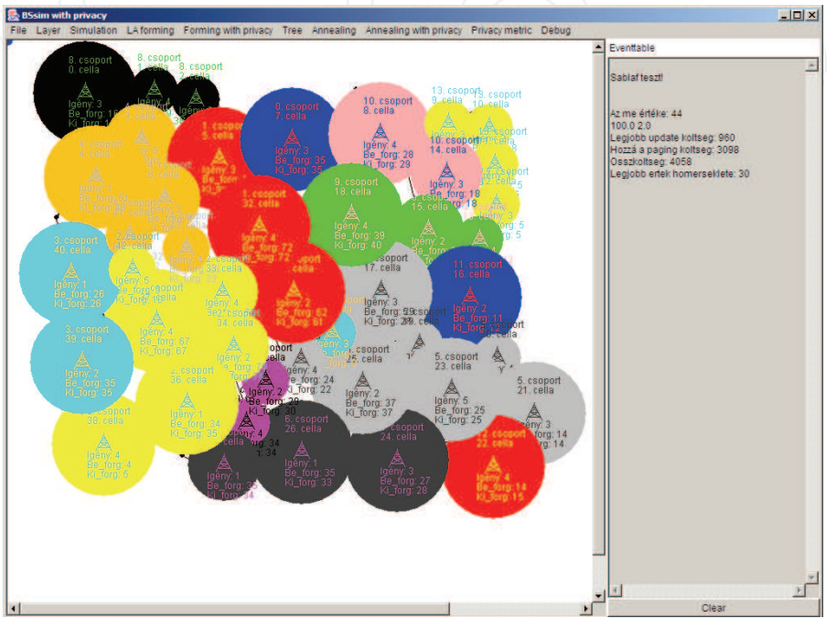


Fig. 3. Micromobility domain structure without taking location privacy into account

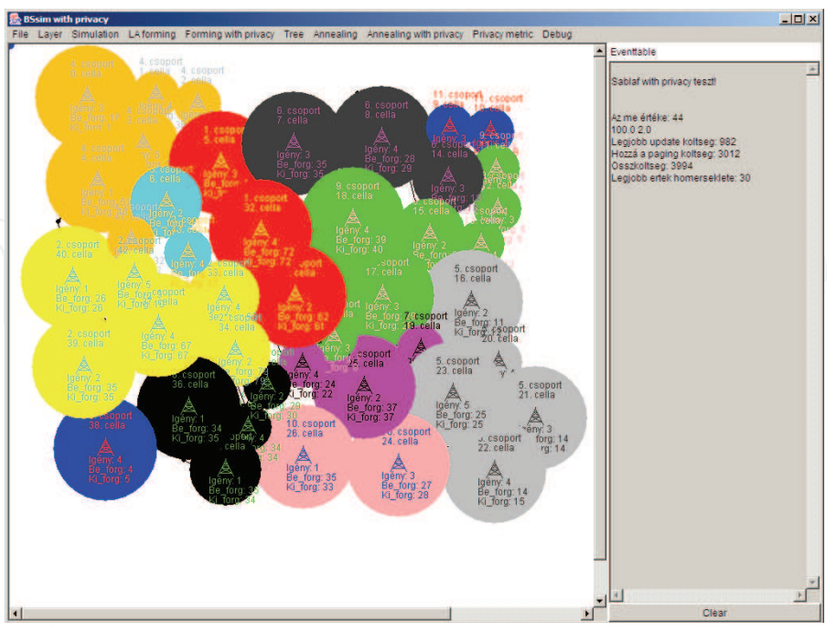


Fig. 4. Micromobility domain structure formed with our location privacy aware design algorithm

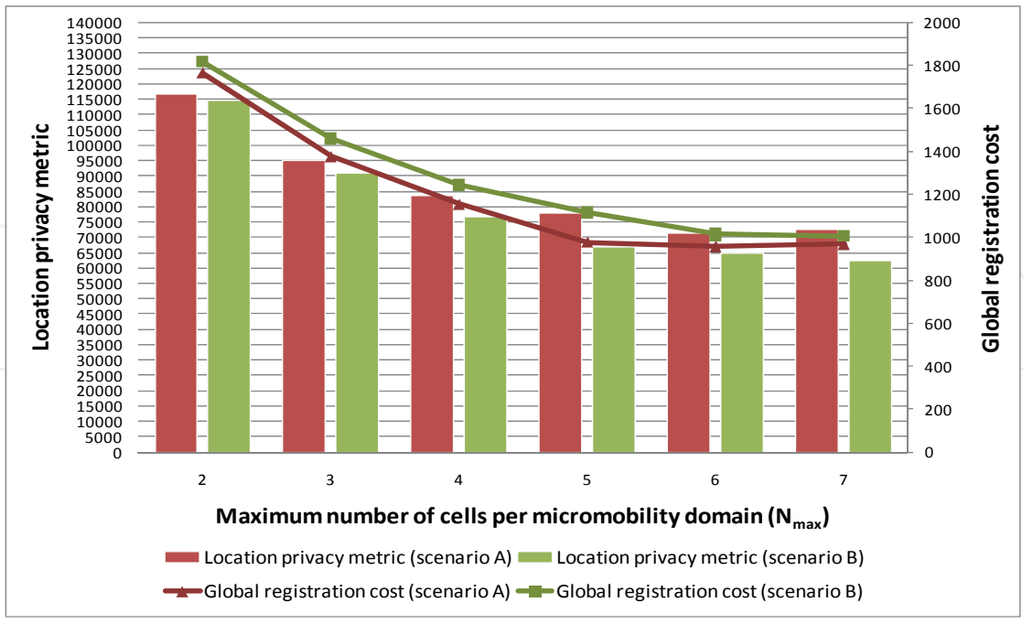


Fig. 5. Comparison of the two scenarios based on location privacy metric and global registration cost

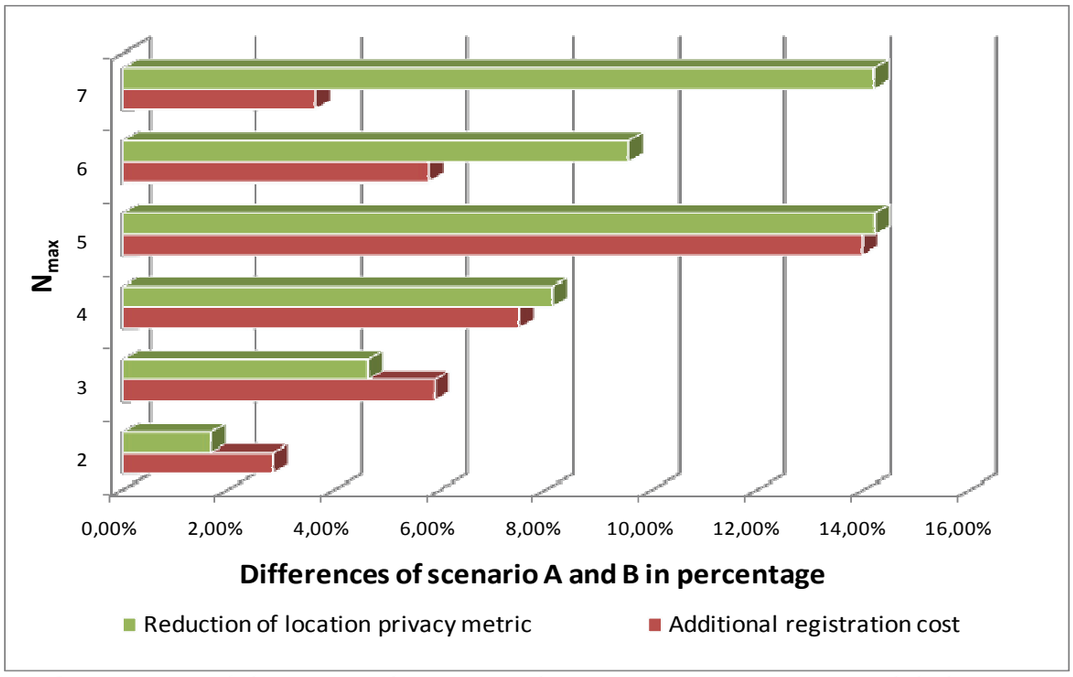


Fig. 6. Comparison of the gain and cost ratio: location privacy metric vs. global registration cost

We examined how the registration cost and the location privacy metric changes by increasing the maximum number of cells in one micromobility domain for each scenario. This way we could check whether the registration cost function is correct, whether it reaches the minimum value when a domain consists of the calculated (15) maximum number of cells

($N_{\max}$), and how our extended domain forming scheme performs. As Fig. 5 denotes, our simulated annealing based location privacy aware micromobility domain planning algorithm finds a much better solution in means of location privacy support for every value of $N_{\max}$ compared to the original scheme which does not care with privacy issues. However, we have to pay the prize of this benefit: the registration cost is slightly higher in scenario B than in scenario A for every domain sizes. This effect is depicted on Fig. 6 which compares the revenue of location privacy support and the accompanied registration cost increment. Fig. 6 shows that our location privacy aware solution responds well to the increasing value of $N_{\max}$, and sees more gain in location privacy metric than loss in registration cost for values $N_{\max} \geq 4$.

We can summarize, that our novel algorithm gives much better results than its ancestor when the maximum number of cells is higher ($N_{\max} \geq 6$), decreasing the location privacy metric of the network almost for 15% more effective than the former solution, at the expense only of an approximate 4% growth of the global registration cost.

5. Conclusion and future work

In order to design a mobile network that provides location privacy for mobile users in micromobility environments by exploiting inherent properties of micromobility protocols, optimized domain planning is needed, considering the strict constraints like paging service capacity of the network. In this Chapter, we proposed a simulated annealing based location privacy aware micromobility domain planning algorithm for a near-uniform network usage, defining the global registration cost function with the help of the fluid flow model together with a paging constraint. The presented algorithm is a two-step domain forming solution, which consists of a greedy phase that gives the basic cell partitions, and a simulated annealing phase which gives a near-optimal domain structure in acceptable runtime. Aiming to evaluate the performance of our novel method, a simple quantifier for the location privacy ability of micromobility structures was defined and a mobile environment simulator was implemented in Java. Using the input data produced by such a realistic simulation environment, different micromobility planning algorithms were executed. Based on this comprehensive toolset we evaluated our location privacy aware algorithm by examining the global registration cost and the location privacy metric of the network in the function of the maximal number of cells per a micromobility domain. As a result of our evaluation efforts we can say that our algorithm proved its power by significantly reducing the location privacy metric of the network at the expense only of an approximate 4% growth of the global registration cost.

As a part of our future work we plan to extend our algorithms and simulation environment with advanced and more sophisticated location privacy metrics in order to broaden the evaluation of our schemes. We also plan to integrate the concept of location privacy aware network planning into researches relating to personal paging area design.

6. Acknowledgement

This work was made in the frame of Mobile Innovation Centre's 'MEVICO.HU' project, supported by the National Office for Research and Technology (EUREKA_Hu_08-1-2009-0043). The authors also would like to express their appreciation to Krisztián Kovács for his essential work on this research and also to Gábor Gulyás and Iván Székely for raising interest in location privacy studies.

7. References

Baden, R. (2008). IP Geolocation in Metropolitan Area Networks. *Master's Degree Scholarly Paper* . University of Maryland, College Park.

Beresford, A., & Stajano, F. (2003). Location privacy in pervasive computing. *IEEE Pervasive Computing* , 46–55.

Bhattacharjee, P. S., Saha, D., & Mukherjee, A. (1999). Heuristics for assignment of cells to switches in a PCSN. *Proc. IEEE Int. Conf. Personal Comm.*, (pp. 331-334). Jaipur, India.

Bokor, L., Dudás, I., Szabó, S., & Imre, S. (2005). Anycast-based Micromobility: A New Solution for Micromobility Management in IPv6. *in Proceedings of MoMM'05*, (pp. 68-75). Malaysia, Kuala Lumpur.

Bokor, L., Nováczki, S., & Imre, S. (2007). A Complete HIP based Framework for Secure Micromobility. *5th @WAS International Conference on Advances in Mobile Computing and Multimedia*, (pp. 111-122). Jakarta, Indonesia.

Bokor, L., Simon, V., Dudás, I., & Imre, S. (2007). Anycast Subnet Optimization for Efficient IPv6 Mobility Management. *IEEE GIIS'07*, (pp. 187-190). Marrakesh.

Casteluccia, C. (2000). Extending Mobile IP with Adaptive Individual Paging: A Performance Analysis. *Proc. IEEE Symp. Computer and Comm.*, (pp. 113-118).

Cayirci, E., & Akyildiz, I. (2003). Optimal Location Area Design to Minimize Registration Signalling Traffic in Wireless Systems. *IEEE Transactions on Mobile Computing , 2* (1).

Connolly, G., Sachenko, A., & Markowsky, G. (2003). Distributed traceroute approach to geographically locating IP devices. *Second IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, (pp. 128 – 131).

Cornelius, C., Kapadia, A., Kotz, D., Peebles, D., Shin, M., & Triandopoulos, N. (2008). Anonysense: privacy-aware people-centric sensing. *International Conference On Mobile Systems, Applications And Services*, (pp. 211-224).

Das, S., Misra, A., Agrawal, P., & Das, S. K. (2000). TeleMIP: telecommunications-enhanced mobile IP architecture for fast intradomain mobility. *IEEE Pers. Commun.* , 50-58.

Diaz, C., Seys, S., Claessens, J., & Preneel, a. B. (2002). Towards measuring anonymity. San Francisco: PET'02.

El-Rabbany, A. (2006). *Introduction to GPS: The Global Positioning System* (2 ed.). Artech House Publishers.

Eriksson, B., Barford, P., Sommersy, J., & Nowak, R. (2010). A Learning-based Approach for IP Geolocation. In *Lecture Notes in Computer Science* (Vol. 6032/2010, pp. 171-180). Berlin / Heidelberg: Springer.

Freedman, M. J., Vutukuru, M., Feamster, N., & Balakrishnan, H. (2005). Geographic Locality of IP Prefixes. *Internet Measurement Conference (IMC)*. Berkeley, CA.

Grilo, A., Estrela, P., & Nunes, M. (2001). Terminal Independent Mobility for IP (TIMIP). *IEEE Communications Magazine* , 34-41.

Gueye, B., Ziviani, A., Crovella, M., & Fdida, S. (2006). Constraint-based geolocation of internet hosts. *IEEE/ACM Transactions on Networking , 14* (6), 1219-1232.

Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., & Patil, B. (2008, August). Proxy Mobile IPv6. *IETF RFC 5213* .

Haddad, W., Nordmark, E., Dupont, F., Bagnulo, M., & Patil, B. (2006, June 26). Privacy for Mobile and Multihomed Nodes: MoMiPriv Problem Statement. *IETF Internet Draft* .

Haddad, W., Nordmark, E., Dupont, F., Bagnulo, M., Park, S. S., Patil, B., et al. (2006, June 26). Anonymous Identifiers (ALIEN): Privacy Threat Model for Mobile and Multi-Homed Nodes. *IETF Internet Draft* .

He, X., Funato, D., & Kawahara, T. (2003). A dynamic micromobility domain construction scheme. *Personal, Indoor and Mobile Radio Communications (PIMRC'03)*, *3*, pp. 2495 - 2499.

Helmy, A. A.-G., Jaseemuddin, M., & Bhaskara, G. (2004). Multicast-based mobility: a novel architecture for efficient micromobility. *IEEE Journal on Selected Areas in Communications , 22* (4).

Hoh, B., & Gruteser, M. (2005). Protecting Location Privacy Through Path Confusion. *First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, (pp. 194 - 205).

Huber, J. (2004). Mobile next-generation networks. *IEEE Multimedia , 11* (1), 72-83.

Ichikawa, T., Banno, A., & Teraoka, F. (2006). Stealth-Lin6: Anonymizing IPv6 mobility communication. *IPSJ SIG Technical Reports , 2006 (26)* , 55–60. Japan.

Johnson, D., Perkins, C., & Arkko, J. (2004, June). Mobility Support in IPv6. *IETF RFC 3775* .

Koodli, R. (2007, May). IP Address Location Privacy and Mobile IPv6: Problem Statement. *IETF RFC 4882* .

Kumar, A., Umesh, M. N., & Jha, R. (2000). Mobility modeling of rush hour traffic for location area design in cellular networks. *3rd ACM Int. Workshop Wireless Mobile Multimedia*, (pp. 48-54). Boston, MA.

Kunishi, M., Ishiyama, M., Uehara, K., Esaki, H., & Teraoka, F. (2000). LIN6: A New Approach to Mobility Support in IPv6. *International Symposium on Wireless Personal Multimedia Communication, 455.*

Laarhoven, P. v., & Aarts, E. (1987). *Simulated Annealing: Theory and Applications.* Springer.

Lakhina, A., Byers, J., Crovella, M., & Matta, I. (2003, August). On the Geographic Location of Internet. *IEEE Journal on Selected Areas in Communications* .

Langheinrich, M. (2002). A Privacy Awareness System for Ubiquitous Computing Environments. In G. Borriello, & L. E. Holmquist (Eds.), *Lecture Notes in Computer Science* (Vol. 2498, pp. 237–245). Springer.

Loa, S.-W., Kuo, T.-W., Lam, K.-Y., & Lic, G.-H. (2004). Efficient location area planning for cellular networks with hierarchical location databases. *Computer Networks , 45* (6), 715-730.

Maekawa, K., & Okabe, Y. (2009). An Enhanced Location Privacy Framework with Mobility Using Host Identity Protocol. *Ninth Annual International Symposium on Applications and the Internet (SAINT'09)*, (pp. 23-29).

Markoulidakis, J., Lyberopoulos, G., Tsirkas, D., & Sykas, E. (1995). Evaluation of location area planning scenarios in future mobile telecommunication systems. *Wireless Networks , 1*, 17 - 29.

Matos, A., Santos, J., Sargento, S., Aguiar, R., Girao, J., & Liebsch, M. (2006). HIP Location Privacy Framework. *1st ACM/IEEE international workshop on Mobility in the evolving internet architecture* (pp. 57–62). New York, USA: ACM Press.

Moskowitz, R., Nikander, P., Jokela, P., & Henderson, T. (2008, April). Host Identity Protocol. *IETF RFC 5201* .

Pack, S., Choi, Y., & Nam, M. (2006). Design and Analysis of Optimal Multi-Level Hierarchical Mobile IPv6 Networks. *Wireless Personal Communications , 36*, 95–112.

Pack, S., Nam, M., & Choi, Y. (2004). A Study On Optimal Hierarchy in Multi-Level Hierarchical Mobile IPv6 Networks. *IEEE Globecom*, (pp. 1290-1294).

Prajapati, N. B., Agravat, R. R., & Hasan, M. I. (2010, March). Simulated Annealing for Location Area Planning in Cellular networks. *International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC)* , 1-7.

Qian, G., Guang-xia, L., Jing, L., Yi-qun, X., & Ming, Z. (2010). Location Area Design for GEO Mobile Satellite System. *Second International Conference on Computer Engineering and Applications (ICCEA)*, (pp. 525 - 529). Bali Island, Indonesia.

Qiu, Y., Zhao, F., & Koodli, R. (2010, February). Mobile IPv6 Location Privacy Solutions. *IETF RFC 5726* .

Ramjee, R., Porta, T. L., Thuel, S., Varadhan, K., & Wang, S. (1999). HAWAII: A Domain-Based Approach for Supporting Mobility in Wide-area Wireless Networks. *IEEE Int. Conf. Network Protocols.*

Reed, M., Syverson, P., & Goldschlag, D. (1998). Anonymous Connections and Onion Routing. *IEEE Journal on Selected Areas in Communication Special Issue on Copyright and Privacy Protection , 16*, 482–494.

Reinbold, P., & Bonaventure, O. (2003). IP Micro-Mobility Protocols. *IEEE Communications Surveys & Tutorials* , 40-57.

Rubin, I., & Choi, C. (1997). Impact of the Location Area Structure on the Performance of Signalling Channels in Wireless Cellular Networks. *IEEE Commun. Mag. , 35* (2).

Serjantov, A., & Danezis, G. (2003). Towards an Information Theoretic Metric for Anonymity. In *Privacy Enhancing Technologies* (Vol. 2482/2003, pp. 259-263). Berlin / Heidelberg: Springer.

Sharma, A., & Ananda, A. L. (2004). A Protocol for Micromobility Management in Next Generation IPv6 Networks. *2nd international workshop on Mobility management & Wireless Access Protocols*, (pp. 72-78).

Shokri, R., Freudiger, J., Jadliwala, M., & Hubaux, J.-P. (2009). A Distortion-Based Metric for Location Privacy. *8th ACM workshop on Privacy in the electronic society*, (pp. 21-30). Chicago, Illinois, USA .

Simon, V., & Imre, S. (2004). A Domain Forming Algorithm for Next Generation, IP Based Mobile Networks. *SOFTCOM'02*, (pp. 289-292). Split, Dubrovnik (Croatia), Venice (Italy).

Simon, V., & Imre, S. (2007). A Simulated Annealing Based Location Area Optimization in Next Generation Mobile Networks. *Journal of Mobile Information Systems , 3* (3/4), 221-232.

Simon, V., & Imre, S. (2009). Location Area Design Algorithms for Minimizing Signalling Costs in Mobile Networks. In D. Taniar (Ed.), *Mobile Computing: Concepts, Methodologies, Tools, and Applications* (pp. 682-695).

Simon, V., Bokor, L., & Imre, S. (2009). A Hierarchical Network Design Solution for Mobile IPv6. *Journal of Mobile Multimedia (JMM) , 5* (4), 317-332.

Snekkenes, E. (2001). Concepts for Personal Location Privacy Policies. *3rd ACM Conference on Electronic Commerce* (pp. 48–57). ACM Press.

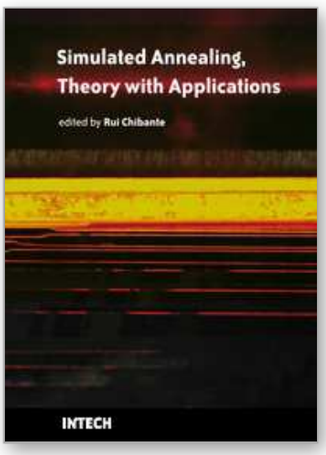
Soliman, H., Castelluccia, C., Malki, K. E., & Bellier, L. (2005, August). Hierarchical Mobile IPv6 Mobility Management (HMIPv6). *IETF RFC 4140* .

Tabbane, S. (1997). Location Management Methods for Third Generation Mobile Systems. *IEEE Commun. Mag. , 35* (8).

Valko, A. (1999). Cellular IP: A New Approach to Internet Host Mobility. *ACM SIGCOMM Comp. Commun. Rev. , 29* (1), 50-65.

Ylitalo, J., & Nikander, P. (2006). BLIND: A Complete Identity Protection Framework for End-Points. In *Lecture Notes in Computer Science* (Vol. 3957, pp. 163–176). Springer Berlin / Heidelberg.

Ylitalo, J., Melen, J., Nikander, P., & Torvinen, V. (2004). Re-thinking Security in IP based Micro-Mobility. *Proc. of the 7th International Conference on Information Security Conference (ISC'04)*, (pp. 318-329). Palo Alto, CA, USA.



Simulated Annealing, Theory with Applications
Edited by Rui Chibante

ISBN 978-953-307-134-3
Hard cover, 292 pages
Publisher Sciyo
Published online 18, August, 2010
Published in print edition August, 2010

The book contains 15 chapters presenting recent contributions of top researchers working with Simulated Annealing (SA). Although it represents a small sample of the research activity on SA, the book will certainly serve as a valuable tool for researchers interested in getting involved in this multidisciplinary field. In fact, one of the salient features is that the book is highly multidisciplinary in terms of application areas since it assembles experts from the fields of Biology, Telecommunications, Geology, Electronics and Medicine.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen