Evaluation of the Location Privacy Aware Micromobility Domain Planning Scheme*

László Bokor† *Member IEEE,* Vilmos Simon† *Member IEEE,* Sándor Imre† *Member IEEE*

***Abstract*—Next generation telecommunication systems are converging into a synergistic union of wired and wireless technologies, where integrated services are provided on a universal IP-based infrastructure. The concept of global reachability fuelled with the advanced mobility schemes and the "anytime, anywhere" paradigm caused that the requirements for security and privacy in the global Internet era differs a lot from the ones of a decade ago. We focus on a subset of this complex problem space and consider location privacy issues defined by the information leakage of IP addresses during the movement of users. In our previous work we proposed a special domain planning algorithm to optimize location privacy supporting potential of certain mobility management mechanisms by increasing the level of concealment of address changes in the network. In this paper we extensively evaluate the scheme by applying well-known location privacy metrics from the literature and using them as objective measures for our original algorithm and its variants first introduced here. The conducted series of simulations verified the efficiency of the scheme and also confirmed the performance enhancements commenced by our improvements and modifications to the original algorithm.**

***Index Terms*—location privacy, privacy metrics, micromobility, simulation, domain planning algorithms, simulated annealing**

I. Introduction

The Internet is evolving towards a fully pervasive and ubiquitous architecture in which users are expected to be able to use remote resources anytime and anywhere. Besides the evolution of wireless networks toward heterogeneous all-IP mobile communication architectures, end-user terminals are also becoming more and more powerful devices implementing extremely large variety of functions from making voice and video calls through social networking and sharing multimedia till exploiting the advantages of geographic positioning solutions in order to use navigational applications and location based services. However mobile terminals' location data possess important service-enabler potential, in wrong hands it can be used to build up private and intimate profile of the mobile user and can pose serious threats to location privacy [1]. In the all-IP world of future mobile Internet, location privacy of users is even harder to protect as the most common parameters in every single packet – i.e., the source and destination IP addresses – can easily be translated to a quite accurate estimation of the peers' actual geographical location [2][3][4][5][6] thus making third parties able to track mobiles' real-life movements [7][8]. As mobility becomes one of the most unique characteristics of future's convergent architectures, more attention must be given to the above location privacy issues, even at the earliest phases of design: at the network planning level.

When discussing network planning in next generation all-IP heterogeneous wireless communication systems, at least one special factor should be considered. In such systems moving across multiple IP subnets (i.e., changing access nodes which provide IP connection with topologically different address spaces) will occur more likely, resulting in much frequent IP address changes compared to today's mainly homogeneous architectures, therefore raising a strong need of special mobility handling mechanisms. The most known solution for this is called micromobility management which aims to localize mobility events by grouping several IP subnets into domains, and provides fast, seamless, and local handoff control in areas where mobile nodes (MNs) change their point of attachment to the network so often that the general (i.e., macromobility) schemes originate significant overhead in terms of packet delay, packet loss, and excrescent signaling [9]. Frequent IP address changes further aggravate problems of location information leakage. However, micromobility also includes capabilities to support location privacy: localization of mobility events inside a micromobility domain can hide location information easily exposable by IP address changes of handovers [10]. Note that only in cases of inter-domain handovers the location is updated and revealed to outside of the domain; not on each access point change. Next generation, heterogeneous, pico- and femto-cell based mobile architectures [11] are even more sensitive to the above Quality of Service (QoS) and privacy issues which imply the spreading of micromobility protocols (e.g., [12][13][14][15]), and the need of advanced network planning algorithms to support real-life deployment of the micromobilty paradigm.

One of the open issues of deploying micromobility protocols in next generation mobile environments is the optimal design of micromobility domains. The main question is what size (in means of consisting subnets) a micromobility domain should be for reducing the cost of paging, maintaining routing tables and registration signaling. Existing network planning algorithms (e.g., [16][17][18][19][20][21]) are mainly focusing on the trade-off between the paging cost and the registration cost. In our earlier work [22] we considered

* This work is supported by the project TÁMOP-4.2.1/B-09/1/KMR-2010-0002, which is connected to the program of the "Development of quality-oriented and harmonized R+D+I strategy and functional model" at the Budapest University of Technology and Economics.

† Budapest University of Technology and Economics, Department of Telecommunications, Budapest, H-1117, Magyar tudósok körútja 2, Hungary. Corresponding author: László Bokor, E-mail: bokorl@hit.bme.hu

also the location privacy supporting potential of micromobility management and presented a simulated annealing based micromobility domain optimization approach, which – to the best of our knowledge – firstly introduced privacy awareness in network planning methodologies. However, the evaluation of this algorithm was only performed on one specific cell and road structure, and the comparison of simulation results was based on a proprietary quantifier for the location privacy ability of micromobility structures and not on widely and comprehensively accepted location privacy metrics available in the literature. This motivated us to broaden our evaluation efforts and provide an extensive and more complete simulation analysis of the location privacy aware micromobility domain planning scheme and also to use the novel results to further enhance the original algorithm.

The rest of the paper is organized as follows. Section 2 introduces the related work. Preliminaries are summarized in Section 3 by reviewing our prior work – the first delegate of the location privacy aware domain planning scheme called PA-SABLAF – and the definition of the location privacy metrics applied by us for evaluation purposes. Section 4 presents the way how these metrics were realized to be applicable in our scheme, while Section 5 shows the modifications and enhancements of PA-SABLAF eventuated by the applied metrics. The extensive evaluation based on the metrics and the enhanced algorithm versions is detailed in Section 6. Finally, we conclude the paper in Section 7 and sketch the scope of future research.

II. RELATED WORK

It is usually hard to design 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 into micromobility domains, what kind of principles must be used to configure the hierarchical levels if they are available, and in which hierarchical level is advisable to implement special functions (e.g., anchors or gateways). The traffic load and mobility of nodes may vary, therefore a fixed structure lacks of flexibility: design schemes are needed to comprise these network dynamics and to provide optimal or near-optimal solutions.

An obvious algorithm is to group those access nodes and their coverage areas (i.e., cells) into one domain, which has a high rate of handovers among each other. In that way the number of global location updates (registration messages) can be significantly decreased. But joining too much access nodes into one domain would degrade the overall performance since it will generate a high traffic load on anchor/gateway nodes, and result in higher cost of packet delivery and paging. Contrarily a small number of cells inside a micromobility domain will lead to a huge amount of location updates to the home network but will alleviate paging costs.

Based on these assumptions, He Xiaoning et al. [16] 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 [23][24]), 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 [25], that groups cell pairs with higher inter-cell mobile traffic into the same LA. In this algorithm a list of neighbors is created for each cell, and the neighbor 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 neighbors with the highest traffic from the neighbor 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 neighbors 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 [26], 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 [20]. 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.

Based on this algorithm, authors in [27] constructed a simulated annealing based anycast subnet forming algorithm (SABAS) aiming to use the idea of GREAL+SABLAF for micromobility domain planning. SABAS is a general method for optimal grouping of cells into micromobility domains. Authors show its efficiency by applying the method for a particular micromobility protocol based on IPv6 anycasting.

In [28] authors also propose 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 [29].

There are also Location Area and micromobility domain planning algorithms which are able to handle network structures with hierarchical levels [18][21] for assignment of an optimal tree structure to a given source of access router handover rates.

However there exists a quite broad literature on location area and micromobility domain planning, the substantial and a-priori question of how to integrate location privacy requirements into the algorithms is still almost completely unexplored. To the best of our knowledge, the only study about location privacy aware domain planning is our prior research [22], which extends SABLAF/SABAS with a simple location privacy policy model and a special rate weighting technique applied to integrate the effects of the cells' static location privacy significance and mobile nodes' dynamic privacy demands into the boundary crossing rates between neighboring cells. The algorithm is called PA-SABLAF (Privacy Aware SABLAF) and joins 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. This scheme allows network designers to maximally take into consideration pre-existing location privacy requirements and also the users' dynamic privacy demands in the design phase.

Aiming to provide more general results and to improve the original algorithm of [22], we applied some well-known location privacy metrics from the literature and started the work on more thorough simulation analysis of the location privacy aware micromobility domain planning scheme.

III. PRELIMINARIES

This section reviews our earlier work related to PA-SABLAF together with our originally applied, proprietary metric, then introduces the basics of two, widely accepted and more general metrics from the literature, both are used for evaluating PA-SABLAF in a more universal way and also to enhance our original algorithm.

A. Review of PA-SABLAF and the proprietary metric used for its preliminary evaluation

In the location privacy policy model we applied in [22], a combination of two substances is used to provide boundary conditions for location privacy aware domain planning. On one hand we introduced the *static location privacy significance level of the cells* (denoted by $SLP_{[k]}$ for cell k) which can separate coverage areas inside the operator's network considered to be more sensitive to location privacy than others. On the other hand we defined *user's location privacy profile for different location types* (denoted by $ULP_u^{lt[k]}$ for user u and location type lt of cell k) to describe what level of location privacy protection is required for a mobile user at a given type of location. The incoming dynamic demands are cumulated and the average will be compared with the static location privacy significance level of the issued cell at every announcement. The winner of this comparison – called 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.

In order to integrate the effects of the cells' overall location privacy factor into the boundary crossing rates between neighboring cells, a special rate weighting technique was created. In the mathematical representation we use, the cells are the nodes of a graph, the cell border crossing directions are represented by the graph edges and the weights are assigned to the edges based on the cell border crossing 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.

$$WR_{[k][l]} = CR_{[k][l]} \times OLPF_{[l]} + CR_{[l][k]} \times OLPF_{[k]} \quad (1)$$

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

Based on the above definition, PA-SABLAF will start with a GREAL-based greedy phase that will provide a basic domain partitioning as an input (i.e., initial solution) of the simulated annealing. At the beginning of this greedy phase, we choose the cell pair with the biggest weighted rate in our cell structure. If the biggest rate occurs multiple times, then we choose one of the instances randomly and include the two cells belonging to that handover rate into domain D_1 of cells. In the next step, we search for the second biggest weighted rate among the cell pairs for which is true, that one of them belongs to domain D_1. We must check whether inequality $N_k < N_{max}$ is satisfied, where N_k is the number of cells in the k^{th} domain and N_{max} stands for the maximum 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 set D_1. If the inequality is not satisfied, the cell can not be included into this set: a new domain with this cell is to be created in order to prevent exceeding the paging cost constraint [22]. 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.,).

After processing all the cell pairs in the above sequential and greedy way a likely sub-optimal domain structure will be created, which will serve as an input (i.e., initial solution or s_0 domain partitioning) for the simulated annealing part of the algorithm. Based on s_0 a neighbor solution s_1 is then generated as the next solution ($N_k < N_{max}$ must be satisfied by s_1 too), and the change in the registration cost $\Delta C_{Reg}(s_0, s_1)$ is calculated. If a reduction in the cost is achieved, the current solution is replaced by the generated neighbor; otherwise we evaluate the acceptance function $e^{(-\frac{\Delta C_{Reg}}{T})}$ to decide whether to retain or change the current solution (T is the temperature). The cooling schedule is based on three input parameters: initial temperature T, step of decrement ($decr$) for T, and the stopping rule which is the maximal iteration step number until ΔC_{Reg} does not change. The details and the complete flowchart of the whole PA-SABLAF can be found in [22].

In [22] we also performed simulations on PA-SABLAF and showed the potential of our method by comparing it with our previous domain planning algorithm called SABAS. A proprietary location privacy metric – denoted by $\boldsymbol{LP^{s}_{mic}}$ in this paper – was designed for this purpose to express how efficiently 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). We quantified 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 metric tracks and saves movements (i.e., whole paths) of mobile users and also saves cell boundary crossings in order to localize and count mobile nodes' inter-domain changes. For every inter-domain handover of a mobile node and for the previous and the next cells of such handovers the algorithm sums 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. The above calculation is performed for every mobile node, and the sum of these values will stand for the location privacy metric of the whole micromobility domain system.

$$\boldsymbol{LP^{s}_{mic}} = \\ = \sum_{u} \sum_{h \in IH_u} (ULP_u^{lt[k]})^2 + (ULP_u^{lt[l]})^2 + SLP_{[k]} + SLP_{[l]} \qquad (2)$$

where IH_u means the set of all inter-domain handover events of user u, and $h_{[k][l]} \in IH_u$ stands for a handover event with exit and entry cells of k and l respectively. Implicitly the smaller $\boldsymbol{LP^{s}_{mic}}$ values are the better.

However the above metric is able to numerically present the location privacy capabilities of a complete network's certain micromobility domain structure, it lacks in generality. That is why we started to evaluate our scheme using more general and widespread location privacy metrics. The metrics we have chosen for our efforts are introduced in the next two sections.

B. Uncertainty-based location privacy metric

This type of metric was originally proposed in [30] [31]. Authors in [30] present an information theoretic model that allows to measure the degree of anonymity provided by schemes for anonymous connections. Authors of [31] 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. Both proposals use the same metric model. The attacker's goal is to identify the initiator and/or the responder of a message travelling in the network. Each user in the system is assigned a probability for being the possible initiator/responder of a particular message, and the system's overall anonymity level is determined by the entropy of the random variable that is formed by the users' probabilities. In this way the metric captures the attacker's uncertainty (measured by the entropy) during the identification procedure.

This metric can be easily applied to comply also with location privacy measurement purposes: the location privacy of a given user in the system is calculated as the attacker's uncertainty during linking observed events (e.g., positions in trajectories) to users. Authors in [32] define a well-detailed system model which can be used to formalize the uncertainty-based location privacy metric as follows.

Consider a user $u \in U$ and an event $\hat{e}_i \in \hat{R}_u|_{obs}$ successfully observed by the attacker ($\hat{R}_u|_{obs}$ means all the user u events observed by the attacker). Also consider E^l as the set of edges of the probabilistic graph called the linkability graph (G^l) representing the linkability of observed events based on the attacker's knowledge. (Note, that the attacker's goal is to reassemble the user's actual set of events; hence it assigns probabilities to possible related events in order to reconstruct the user's trajectory.) Define $\pi^l(\hat{e}_i, \hat{e}_j)$ as the weight function of G^l for representing the probability with which the attacker believes that both $\hat{e}_i$ and $\hat{e}_j$ events are associated with the same user and $\hat{e}_i$ is an immediate predecessor of $\hat{e}_j$ in the user's observed set of events. Let a random variable X_i stand for the probability that another observed event $\hat{e}_j$ is the immediate successor of $\hat{e}_i$. According to the notations of [32] we have $Pr_A(X_i = j) = \pi^l(\hat{e}_i, \hat{e}_j)$ for any j such that $(\hat{e}_i, \hat{e}_j) \in E^l$ in G^l, where $Pr_A(s)$ means the probability with which the attacker considers a statement s to be true. The entropy of X_i can be calculated to measure the attacker's uncertainty when linking observed events to users and therefore can be used as objective location privacy metric for user u at the $tm(\hat{e}_i)$ time instance at which the event $\hat{e}_i$ occurred.

$$\boldsymbol{LP^{u}_{u}}\big(tm(\hat{e}_i)\big) = \mathbb{H}(X_i) \\ \mathbb{H}(X_i) = -\sum_{j} Pr_A(X_i = j) \times log_2\big(Pr_A(X_i = j)\big) \qquad (3)$$

Eq. (3) is the common form of the uncertainty-based metric which has been widely used to measure location privacy in different wireless scenarios. For example, authors of [33] applied this scheme in order to maximize the location privacy at each identifier update by users, in the presence of asynchronous identifier updates and predictability of movements of user terminals. In [34] this metric is used to analyze a novel location privacy enhancement protocol which obfuscates several types of privacy-compromising information revealed by mobile nodes, including sender identity, time of transmission, and signal strength. Our last example for application use-cases of the uncertainty-based metric is [35] where authors employ the scheme to measure the performance of their solution designed to enhance users' contradictory requirements on location privacy without diminishing communication QoS.

These examples show how varied application possibilities of the uncertainty-based location privacy metric are and why it is considered a widely accepted and adapted metric in the literature.

C. Traceability-based location privacy metric

This kind of metric captures the level to which the attacker can track a mobile user with high certainty. The attacker's uncertainty or confusion in the tracking procedure is measured by the uncertainty-based metric (e.g., using entropy). In [36] authors define a so called *mean time to confusion* metric to measure the degree of privacy as the time that an attacker could correctly follow a user's trace. Therefore the *mean time to confusion* is the mean tracking time between points where the attacker faced confusion (i.e., was not able to determine the next sample with sufficient certainty). Authors of [37] propose another variant of the traceability-based location privacy metric called the *mean distance to confusion*, which measures the mean distance over which tracking of a user may be possible by the attacker.

The above variants are defined as the time/travel distance until the uncertainty of the tracking grows above a pre-defined threshold. The formalization of the traceability-based location privacy metric is also done according to the system model defined in [32]. We call an event in the observed trace of a user ($\hat{e} \in \hat{R}_u|_{obs}$) as a confusion point if the attacker's uncertainty is above a given threshold: $\boldsymbol{LP_u^u}(tm(\hat{e})) > \mathbb{H}_{cf}$. It means that the *time to confusion / distance to confusion* is specified as the time/distance to travel before reaching a confusion point, during which the attacker's uncertainty remains below $\mathbb{H}_{cf}$. In this way the average value of *time/distance to confusion* represents a user's lack of location privacy.

Denote $\hat{R}_u|_{obs}^{cf}$ as the set of all confusion points (events) of user $u \in U$. Let C_u stand for the union set of the last observed event of user u and the user's confusion events. Let B_u denote the set of events that contain the first observed event from u and all the events which are not confusion points but are immediate successors of each confusion point in the observed trace of user u. Consequently, a traceable period can be defined as the time/travelled distance between an event in B_u and an event in C_u such that there is no other event in B_u in that period. Denote Z_u as the set of all these traceable periods for user u. Based on the above notation the location privacy metric of user u based on *mean time to confusion* ($\boldsymbol{LP_u^{\dot{t}}}$) and *mean distance to confusion* ($\boldsymbol{LP_u^{\ddot{t}}}$) can be defined as the mean tracking time/distance during which uncertainty stays below a confusion threshold and can be calculated as follows (note, that this metric is inversely proportional to *mean time to confusion* and *mean distance to confusion* values).

$$\boldsymbol{LP_u^{\dot{t}}} = \left(\frac{\sum_{(\hat{e}_i, \hat{e}_j \in Z_u)} |tm(\hat{e}_i) - tm(\hat{e}_j)|}{|Z_u|} \right)^{-1} \tag{4}$$

$$\boldsymbol{LP_u^{\ddot{t}}} = \left(\frac{\sum_{(\hat{e}_i, \hat{e}_j \in Z_u)} \| loc(\hat{e}_i) - loc(\hat{e}_j) \|}{|Z_u|} \right)^{-1} \tag{5}$$

where $tm(\hat{e}_i)$ and $loc(\hat{e}_i)$ stands for the time instance and the location at which the event $\hat{e}_i$ occurred, respectively.

This metric is also a well-known and widespread measure of location privacy. One of its main advantages is the fine-grained tuneability: if the threshold of $\mathbb{H}_{cf}$ is chosen high, tracking times increase but so may do the number of false positives (i.e., the attacker follows incorrect traces). A good example for the application of this metric is [38] where authors used the approach in a trace-based simulation of their anonymizer scheme camouflaging users' current location with various predicted paths.

Both the above introduced uncertainty- and traceability-based location privacy metrics are general, widespread and also effective in the means that they are able to quantify the incapacity of a particular attacker in localizing or tracking mobile users. That was our main motivation for choosing them as base approaches in our evaluation work.

IV. REALIZATION AND ADAPTATION OF THE METRICS

Since to the best of our knowledge no other location privacy aware domain planning algorithm exists even in these days, during our preliminary measurements we used our former, simulated annealing based domain optimization method called SABAS [27] as a basis to compare with the PA-SABLAF, and also developed a proprietary location privacy metric in the simulator for this comparison [22]. However, this earlier evaluation work was performed on one cell/road topology only, and the used metric was not general enough for comprehensive analysis. In order to eliminate the above shortcomings we extended the range of topologies/scenarios and adopted two of the most widespread and common location privacy metrics into our simulation environment: uncertainty- and traceability-based location privacy metrics.

A. Metric requirements and assumptions

The level of location privacy in a complete network (i.e., system of several micromobility domains) can be determined by how easily attackers can recognize trajectories (series of cells/access areas owning unique IP prefixes) of mobile users. Every single user in the mobile network passes cells of several domains during their respective paths.

In such architecture inside-domain movements are safe as localized mobility management obfuscates IP address changes of mobile users: valuable addressing information (i.e., location information data of IP communication) will not leak out the domain. However, domain changes will disclose IP address information to all correspondent nodes (CNs) of the mobile as macromobility mechanisms will also be executed besides the micromobility procedures. We assume that the attacker is in continuous communication with the observed mobile user (or at least the attacker is able to capture packets originating from the MN) and is located outside of the MN's domain. The obtainable address information is enough to identify the MN's actual domain but not sufficient to determine the particular cell or access area from where the mobile node communicates.

Due to the aforementioned characteristics of the micromobility management the attacker continuously communicating with the MN can be aware of the complete set of domains crossed during the MN's path, and this information can be used to specify the precise, cell-based trajectory of the observed entity (i.e., the solution which the attacker wants to obtain). Reconstruction of the whole trajectory gets harder if the built-in location privacy supporting capability of the micromobility domain system (i.e., the obfuscation of the observable information performed by the localized mobility management) becomes more effective. This is what a metric in our framework should measure.

As the attacker can observe only the set of domains the MN passes, it must apply statistical calculations to get the solution. An adequately large domain with sufficient number of inter-domain transitions is able to significantly increase the quantity of potential solutions and to enhance location privacy of users in a general way, independently of pre-defined or dynamic privacy parameters we applied in our earlier work. The metrics below serve as efficient tools in our efforts to enhance PA-SABLAF and create more comprehensive and universal algorithms.

B. Realization and adaptation of LP^u

Aiming to implement the uncertainty-based metric in our simulation framework and to adapt it for our evaluation purposes we slightly modified the $\boldsymbol{LP^u}$ scheme. In order to do this, we adapt the $\boldsymbol{LP^u}$ scheme to our framework and also extend it to be applicable for all the users in the micromobility system (as a sum of their entropies).

In a micromobility network the attacker relying on intercepted IP packets can only observe series of crossed domains along the MN's movements. This is because domains usually contain several cells with multiple possible transitions inside and outside of the particular domain. The exact place of a domain change (i.e., the two cells of that transition) can be determined with probability $\frac{1}{n}$ where n is the number of possible transitions between the two domains.

That is why we calculate $\boldsymbol{LP^u}$ in the following way. We split the trajectory of the MN into domain entry and exit points which are basically the observable events (locations) in our threat model and delimit unobservable path segments between them. As these inside-domain path segments are not traceable based on IP information and assuming that domains contain more than two cells at least, the attacker can only deduce the entry and exit points (so called "flashes"). We assume that transitions are not weighted and the transition probability is the same in every case. Considering $Pr_A(d)$ here as the probability of the attacker guessed right when reckoning the actual entry and exit points of crossing domain d, a user's $\boldsymbol{LP^u}$ for a particular domain inside the network can be produced by calculating the entropy of $Pr_A(d)$. (Note that $Pr_A(d)$ can be computed as the product of the probabilities of inlet- and outlet routes belonging to two consecutive "flashes".) By calculating this entropy for every domain of every user, and creating the sum of these entropies we get the overall entropy of a micromobility system denoted by $\boldsymbol{LP^u_{mic}}$ (as this metric is an entropy-like measure, the larger values denote the better location privacy support).

$$\boldsymbol{LP^u_{mic}} = -\sum_u \sum_j Pr_A(d_j) \times log_2\left(Pr_A(d_j)\right) \tag{6}$$

C. Realization and adaptation of LP^t

Due to the peculiar application scenario devised by our domain planning scheme, modifications in the original concept of the traceability-based metric ($\boldsymbol{LP^t}$) were required. During the realization and adaptation phase of this kind of location privacy measurement approach we recognized that according to our scheme and threat model the attacker is not able to track mobile users when they are moving inside a particular micromobility domain. It means that domains serve as confusion points, which also implies that *mean time to confusion* and *mean distance to confusion* approaches become vague: users spend their time mostly in confusion points and only inter-domain handovers ("flashes") are considered as inter-confusion point events which are negligible both in means of time and distance.

This motivated us to create two slightly modified traceability-based metrics called *mean time in confusion* and *mean distance in confusion*. These two metrics capture the level to which the attacker cannot track a mobile user with high certainty. The mobile user's safety during the IP information-based tracking procedure is measured by our modified $\boldsymbol{LP^t}$ metric versions. We define the *mean time in confusion* metric to measure the degree of privacy as the time that an attacker could not correctly follow a user's trace: the *mean time in confusion* is the mean tracking time between points where the attacker overcomes the confusion (i.e., becomes to be able to determine the next sample with sufficient certainty). Similarly, the *mean distance in confusion* measures the mean distance over which tracking of a user may not be possible by the attacker.

According to the already introduced formalization C_u stands for the union set of the last observed event of user u and the user's confusion events, B_u denotes the set of events that contain the first observed event from u and all the events which are not confusion points but are immediate successors of each confusion point in the observed trace of user u. Consequently, an untraceable period can be defined as the time/travelled distance between two or more consecutive events in C_u such that there is no other event in B_u in that period. Let Y_u stand for the set of all these untraceable periods for user u. Based on the above notation the location privacy metric of user u based on *mean time in confusion* ($\boldsymbol{LP^{\bar{t}}_u}$) and *mean distance in confusion* ($\boldsymbol{LP^{\bar{\bar{t}}}_u}$) can be defined as follows.

$$\boldsymbol{LP^{\bar{t}}_u} = \left(\frac{\sum_{(\hat{e}_i,\hat{e}_j \in Y_u)} \left| tm(\hat{e}_i) - tm(\hat{e}_j) \right|}{|Y_u|}\right)^{-1} \tag{7}$$

$$\boldsymbol{LP^{\bar{\bar{t}}}_u} = \left(\frac{\sum_{(\hat{e}_i,\hat{e}_j \in Y_u)} \left\| loc(\hat{e}_i) - loc(\hat{e}_j) \right\|}{|Y_u|}\right)^{-1} \tag{8}$$

where $tm(\hat{e}_i)$ and $loc(\hat{e}_i)$ stands for the time instance and the location at which the event $\hat{e}_i$ occurred, respectively.

Our simulation framework is not prepared for measuring the time duration between user events (i.e., handovers); the system fits only for marking locations (i.e., cells) and the distance between different locations in means of required transition numbers. Therefore we calculate the overall traceability-based location privacy metric of a micromobility system ($\boldsymbol{LP^{\bar{\bar{t}}}_{mic}}$) in our simulator as follows (the location privacy supporting capability is proportional with the *mean distance in confusion*, so here the exponent implies that the smaller values are the better).

$$\boldsymbol{LP^{\bar{\bar{t}}}_{mic}} = \sum_u \left(\frac{\sum_{(\hat{e}_i, \hat{e}_j \in Y_u)} \left\| loc(\hat{e}_i) - loc(\hat{e}_j) \right\|}{|Y_u|} \right)^{-1} \tag{9}$$

V. IMPROVING PA-SABLAF

The above applied metrics introduced more general, extensive and comprehensive aspects into the requirement set of our location privacy aware domain planning scheme, and therefore also eventuated modifications in the original PA-SABLAF algorithm. These modifications formed two novel PA-SABLAF versions, both trying to present more universal and pervasive solutions compared to their predecessor. In this Section these new PA-SABLAF variants are introduced.

A. PA^u-SABLAF

The main design choice for this algorithm was to eliminate the dependency of the operation from both the *static location privacy significance level of the cells* and the *mobile node's location privacy profile* (which equally can narrow the applicability of the model) and create a more general scheme based on the criteria of the widespread and universal uncertainty-based location privacy metric.

In order to do this we altered the greedy phase of the algorithm for increasing the uncertainty of the attacker during its tracking intentions by dismissing the privacy weighted boundary crossing rates ($WR_{[k][l]}$) and creating a novel weighting technique which raises the possible number of transitions at inter-domain movements.

For that reason the greedy phase of PA^u-SABLAF also considers the crossing rates of all the neighboring transitions besides the crossing rates of the actually examined transition. It means that during the contraction the greedy phase favors to choose cell pairs rendering big crossing rates and also showing big traffic through large number of edges between their neighbors. Since the maximum number of cells in a single micromobility domain is limited by N_{max}, we can always create a structure where cells with big transition rates will create domains and simultaneously their neighbors with reasonably significant number and volume of transitions will form neighboring domains such increasing the uncertainty of the attacker observing users' domain changes. According to this, PA^u-SABLAF will lead the traffic of cells with large transit demands away toward as many edges/edge series as possible. The calculation of the weighted rate based on the above considerations and used in the greedy phase of PA^u-SABLAF is as follows.

$$WR^u_{[k][l]} = CR_{[k][l]} + CR_{[l][k]} + TF_{[l]} \tag{10}$$

where $CR_{[k][l]}$ stands for the cell border crossing rate from cell k to l, and $TF_{[l]}$ is the transition factor of cell l (a cell still waiting to be grouped into a domain). We defined the transition factor as $TF_{[l]} = \sum_{m \in A_l} (CR_{[l][m]} + CR_{[m][l]})$ where A_l means the set of all neighbors of cell l. Besides this modified weighting and cell selection scheme the PA^u-SABLAF algorithm is the same as the method introduced in Section III/A.

B. PA^t-SABLAF

This algorithm variant also breaks with the rate weighting technique of the original PA-SABLAF and focuses on more general requirements characterized by the traceability-based location privacy metrics. Here the motivation is to create a micromobility domain structure where user traffic is mainly transacted and kept inside the domains. In case of PA^t-SABLAF we also approach this problem by modifying the applied weighting scheme of the greedy phase inside the original algorithm.

The traceability-based metric implies a single domain covering all the access areas (i.e., cells) as the optimal solution for the location privacy aware domain planning problem. Of course this is not an option: N_{max} is the maximum number of cells in a single micromobility domain in order to provide a strict burden for the paging (and such also maximizing the size of the location privacy protective micromobility domain). So we have to take the cost constraints into consideration and simultaneously create a domain structure in which mobile users likely will perform inside-domain movements.

This can be achieved by increasing the number of "deflector" edges inside the domains. We name an edge or a series of edges as "deflector" if it possesses significant crossing rate and/or it provides input and output for high crossing rates of other edges or series of edges from multiple directions. By inserting cell pairs with deflector edges into the micromobility domains we can enforce that frequent cell sequences of mobile users will likely consist a domain. Such a structure decreases inter-domain movements while fulfilling all the domain planning constraints and also enhances the privacy level of the micromobility scheme in an efficient manner. The calculation of the weighted rate based on the above introduced idea framed for the greedy phase of PA^t-SABLAF is as follows.

$$\begin{array}{ll} if & \\ & E_{[k][l]} \in D_\psi \\ then\,for & \\ & \forall E_{[i][j]} \in E_{[k][l]} \cup A_{[k][l]} \\ do & \\ & WR^t_{[i][j]} = CR_{[i][j]} + CR_{[i][j]} + DF \end{array} \tag{11}$$

where $E_{[k][l]}$ denotes the edge between cells k and l, D_ψ means the set of deflector edges containing edges with the upper ψ percent of all crossing rates in the network, $A_{[k][l]}$ is the set of neighbors of $E_{[k][l]}$, $CR_{[k][l]}$ stands for the cell border crossing rate from cell k to l, and DF is a constant called deflector factor used for rewarding certain edges with deflector properties. This basically means that deflector edges chosen with parameter ψ and their neighboring edges are rewarded with parameter DF.

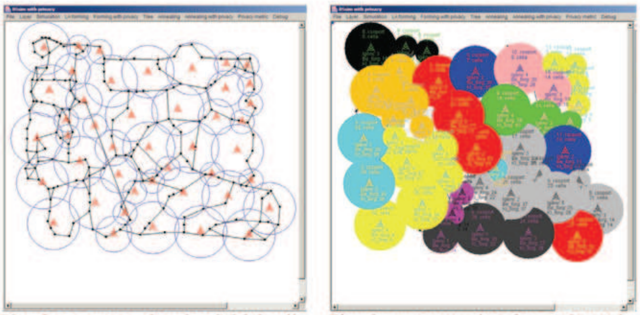
Besides the special weighting technique of (11) the PA^{t}-SABLAF algorithm is basically identical to our original scheme.

VI. Evaluation Results

We have evaluated our location privacy aware micromobility domain planning methods (PA-SABLAF, PA^{u}-SABLAF and PA^{t}-SABLAF) in four different scenarios formed by complex network architectures consisting of several cells, mobile nodes and various compound road grids (Fig. 2). Using this environment we compared our algorithms with their ancestor – the already introduced SABAS [27], which is also a simulated annealing based micromobility domain forming solution but without any trace of location privacy awareness.

A. Simulation framework

In order to evaluate PA-SABLAF together with its variants and analyze their performance in real-life scenarios, we designed and implemented a realistic, Java-based mobile environment simulator, which serves a two-fold purpose.



Simulator screen showing initial cell and road structure built in the GUI

Simulator screen showing a planned micromobility domain structure

Fig. 1. The simulation software in use

On one hand it generates a realistic cell boundary crossing and incoming call (i.e., initiation of IP session) database in a mobile system given by the user with cell, mobile node and movement path placing within the GUI. 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 location area and domain planning algorithms, and forms LAs and micromobility domains by running the implemented mathematical functions.

The simulation can be executed on an arbitrary and customizable road grid covered by cells of various access technologies (e.g., WiFi, GSM, UMTS) as shown in Fig. 1 (left). The static location privacy significance level of the cells can also be set in case of need as well as the location type. Mobile nodes (MN) can be placed into this highly customizable environment by firstly specifying MNs' velocities, setting the incoming session arrival parameter (IP session intensity) and the location privacy profile to every mobile node if needed.

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 applied mobility model here for MNs is the following. The different mobile terminals will move on the defined road grid by time-to-time choosing a random 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. The average speed of MN movements is defined by the velocity parameter of each mobile node.

For every mobile node an incoming session arrival parameter is defined and when a session initiation packet 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 session initiation 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. An example domain structure gathered at the end of the whole simulation process is depicted in Fig. 1 (right).

Our goal with this mobility simulator was to provide a flexible tool which is able to give the possibility to evaluate LA 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/characteristics.

B. Parameters and scenarios

The comparison was carried out with the help of two key performance indicators. On one hand we analyzed the schemes using the applicable privacy metrics ($\boldsymbol{LP^{s}_{mic}}$, $\boldsymbol{LP^{u}_{mic}}$, and $\boldsymbol{LP^{\bar{\bar{t}}}_{mic}}$, respectively) from the location privacy point of view. On the other hand we used the global registration cost to measure the efficiency of the algorithms from the signaling cost optimization perspective. Note, that besides the above we also considered the N_{max} as a constraint for the paging costs.

In order to provide an extensive and broad simulation analysis of the location privacy aware micromobility domain planning scheme represented by the three algorithm versions, we executed several simulation runs for all the three algorithm variants, for $N_{max} = [2..6]$ values, for every scenario, and depicted the total average of all the measurements for a particular domain planning solution in function of the N_{max}. Besides this, in case of the third variant (i.e., PA^{l}-SABLAF) we applied different ψ and DF value combinations ($\psi = 20\%, DF = 20,\ \ \psi = 40\%, DF = 15,\ \ \psi = 60\%, DF = 10$), and showed the average of these results in our analysis.

Four different scenarios were defined and created in our simulation framework by cell (i.e., wireless internet point of access), mobile node and movement path placing. These scenarios were designed to differ in their cell/access point structures, number of active mobile users, and style of interconnection (i.e., possible transition paths between cells) aiming to provide a reasonable scale and variety of initial input data for evaluation. Fig. 2 depicts these scenarios and the following enumeration details the most important scenario parameters and characteristics.

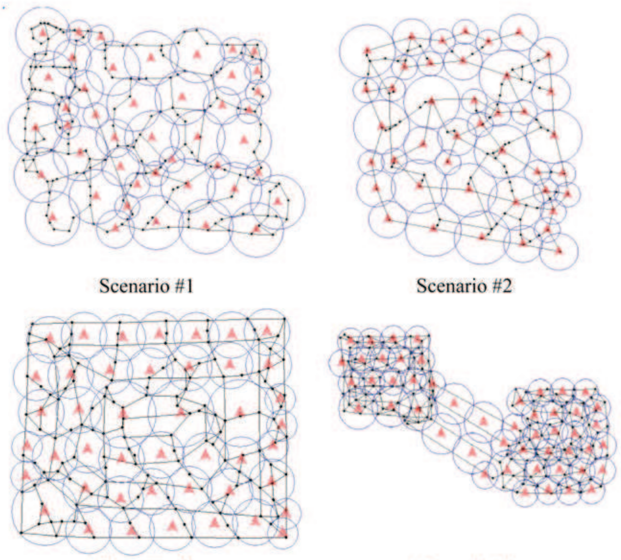


Fig. 2. Simulation scenarios used for evaluation

1) *Scenario #1* consists of 44 multiply interconnected cells and 33 mobile users. Both densely linked (urban-like) and rarely linked (rural-like) areas exist in this construction.
2) *Scenario #2* consists of 42 multiply interconnected cells and 33 mobile users. The average level of interconnection of cells is significantly lower than in Scenario #2, implicating smaller number of transition possibilities.
3) *Scenario #3* consists of 44 multiply interconnected cells and 25 mobile users. This scenario represents a structure where the possible number of inter-cell transitions is high.
4) *Scenario #4* consists of 50 multiply interconnected cells and 22 mobile users. This structure has two, densely linked cell groups, which is interconnected with only a limited set of cells and transition paths.

The simulation of the four scenarios was run till the completion of several thousands of handovers in order to generate substantial number of realistic cell boundary crossings, incoming call/session data and location privacy-weighted rates for each cell pair, also calculating the paging cost and the registration cost for every domain. The produced data will then be used as an input for our algorithms to be evaluated.

C. Results

As an initialization of our experiments we ran the mobility simulator on the scenarios of Fig. 2 and gathered all the required input data for our three location aware domain planning solutions (PA-SABLAF, PA^{u}-SABLAF, PA^{l}-SABLAF) and for the base algorithm of our evaluation (SABAS). After that we executed all the algorithms (with parameters $N_{max} = 6$, $T = 100$, and $decr = 2$) on the produced input data and cell structure in order to render the micromobility domain configuration.

On the rendered domain layout 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 algorithm and scenario. This way we could check how the domain forming methods perform in terms of location privacy support and signaling cost optimization, and also whether the registration cost function is correct (i.e., whether it reaches the minimum value when a domain consists N_{max} number of cells.)

Simulation results depicted on Fig. 3 and 4 show that PA-SABLAF finds a much better domain structure in means of the $\boldsymbol{LP^{s}_{mic}}$ metric for every value of N_{max} compared to the original SABLAF. However, we have to pay the prize of this benefit: the registration cost is slightly higher in most of the cases with a maximum of 4.8%. We have to emphasize, that the $N_{max} = 6$ case results in gain also regarding the registration cost, so here the algorithm managed to ameliorate both parameters of the trade-off.

Fig. 5 and 6 introduces that PA^{u}-SABLAF achieves the most significant relative gain in means of the location privacy metric and the registration cost increment: a more then 30% relative growth can be noticed for location privacy in the $N_{max} = 6$ case. Despite this promising result PA^{u}-SABLAF shows the most serious volume of additional registration costs after location privacy aware domain planning: even the smallest cost growth is 27%. However, this is compensated by the remarkable revenues of the $\boldsymbol{LP^{u}_{mic}}$ metric.

Results of PA^{l}-SABLAF evaluation is depicted in Fig. 7 and 8. This algorithm variant performs a moderate average gain (3.9%) in our scenarios and also shows negative relative gain in the $N_{max} = 4$ case. However, the algorithm enhances the privacy metric together with registration cost in all the other N_{max} cases which is not a negligible achievement.

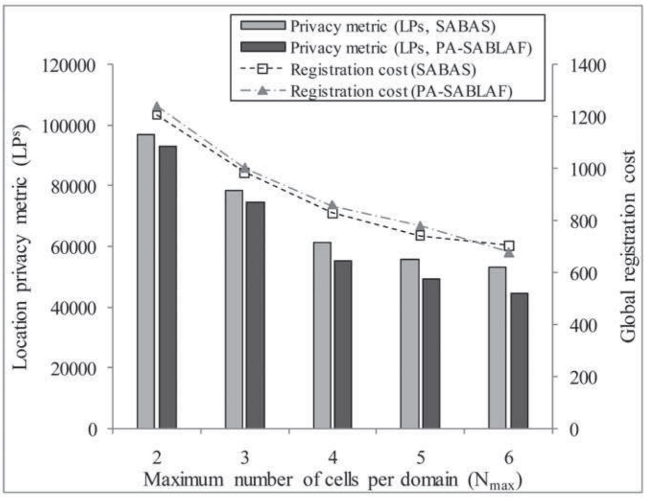


Fig. 3. PA-SABLAF vs. SABAS

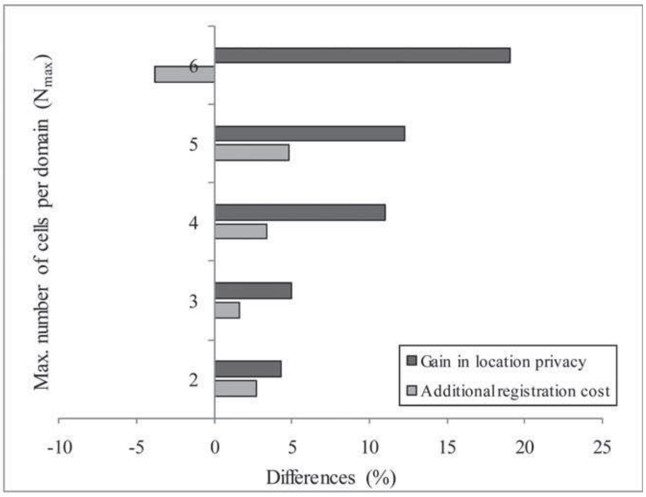


Fig. 4. Location privacy gain vs. cost increment: PA-SABLAF

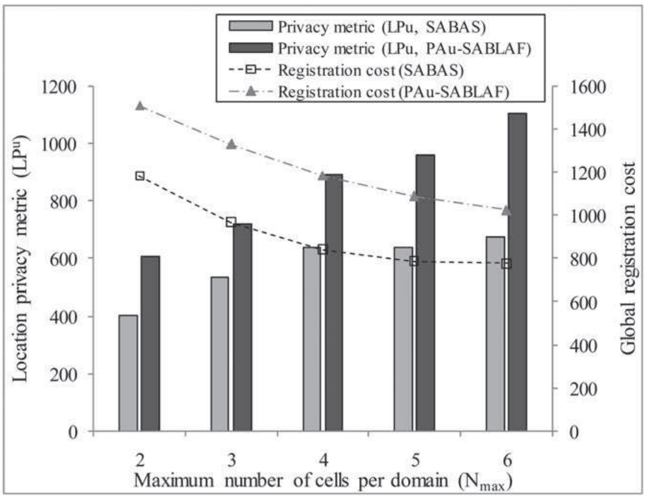


Fig. 5. PA^u-SABLAF vs. SABAS

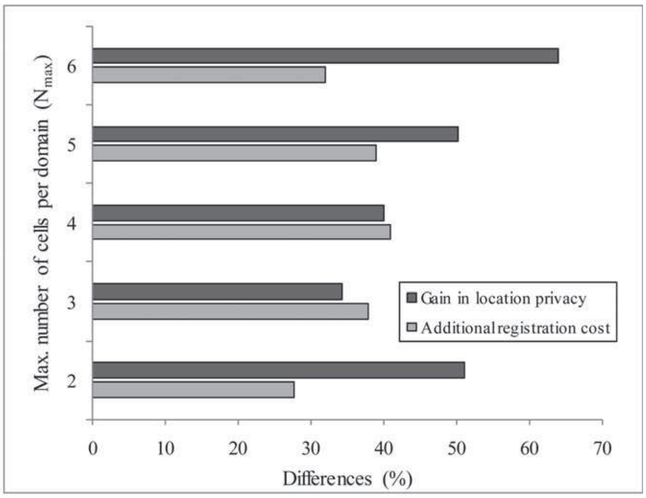


Fig. 6. Location privacy gain vs. cost increment: PA^u-SABLAF

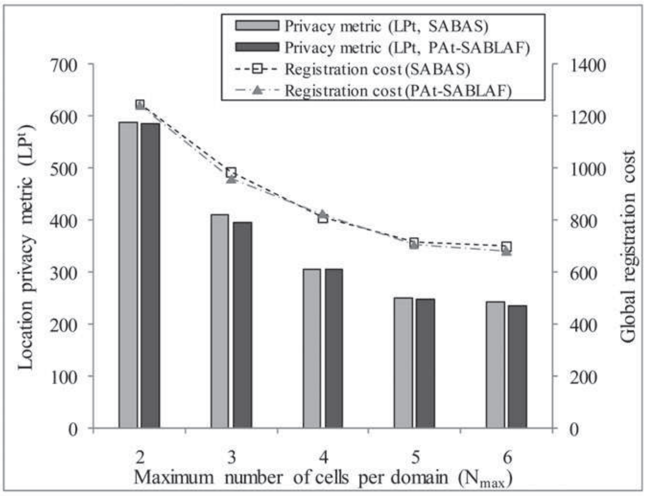


Fig. 7. PA^t-SABLAF vs. SABAS

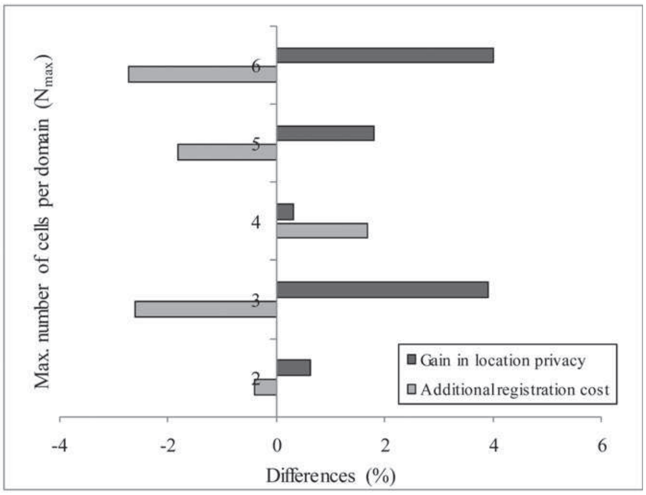


Fig. 8. Location privacy gain vs. cost increment: PA^t-SABLAF

VII. Conclusion

In order to create a mobile network architecture which provides location privacy for mobile users in micromobility environments by exploiting inherent properties of micromobility protocols, optimized domain planning is needed that also considers the strict constraints formed by paging and registration costs. This paper evaluates the location privacy aware micromobility domain planning scheme. The scheme is represented here by three algorithm variants (PA-SABLAF, PA^u-SABLAF and PA^t-SABLAF, the last two first presented in this paper), both of them based on 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. The algorithms differ in the operation of their greedy schemes, respectively optimized for a particular attribute of location privacy.

Aiming to evaluate the performance of the scheme, a mobile environment simulator was used and three different quantifiers for the location privacy ability of micromobility structures were applied ($\boldsymbol{LP^{s}_{mic}}$, $\boldsymbol{LP^{u}_{mic}}$, $\boldsymbol{LP^{\bar{\bar{t}}}_{mic}}$, the first being a proprietary metric from the earlier work of the authors, and the last two being adaptations of well-known and widespread measures of location privacy from the literature). Using the input data produced by a realistic simulation environment, the micromobility domain planning methods could be evaluated. Based on this comprehensive toolset we evaluated our location privacy aware algorithms 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 the scheme proved its power by significantly enhancing the location privacy of users in the network. The total average gain in location privacy for every run of all the three algorithm variants approached 20% at the expense only of a total average 8% growth of the global registration cost (meaning an average 12% relative gain), and there were also distinct cases when the scheme operated with more than 30% relative gain.

As the main part of our future work we plan to integrate our algorithms. It is obvious that PA^u-SABLAF and PA^t-SABLAF catch conflicting attributes of location privacy. In order to provide a more general and complete scheme, it is advisable to combine their features and integrate them in a complex solution. Even merging all three proposed algorithms could be efficient and achievable. We also plan to integrate the concept of location privacy aware network planning into researches relating to personal paging area design.

Acknowledgment

This study was supported by Mobile Innovation Centre Hungary. 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.

References

[1] A.R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, pp. 46–55, 2003.

[2] A. Lakhina, J. Byers, M. Crovella, and I. Matta, "On the Geographic Location of Internet," *IEEE Journal on Selected Areas in Communications*, August 2003.

[3] Michael J. Freedman, Mythili Vutukuru, Nick Feamster, and Hari Balakrishnan, "Geographic Locality of IP Prefixes," in *Internet Measurement Conference (IMC)*, Berkeley, CA, 2005.

[4] B. Gueye, A. Ziviani, M. Crovella, and S. Fdida, "Constraint-based geolocation of internet hosts," *IEEE/ACM Transactions on Networking*, vol. 14, no. 6, pp. 1219-1232, December 2006.

[5] Brian Eriksson, Paul Barford, Joel Sommersy, and Robert Nowak, "A Learning-based Approach for IP Geolocation," in *Lecture Notes in Computer Science*. Berlin / Heidelberg: Springer, 2010, vol. 6032/2010, pp. 171-180.

[6] Y. Wang, D. Burgener, M. Flores, A. Kuzmanovic, and C. Huang, "Towards Street-Level Client-Independent IP Geolocation," in *Proc. USENIX Symposium on Networked Systems Design and Implementation (NSDI'11)*, Boston, MA, 2011.

[7] W. Haddad et al., Anonymous Identifiers (ALIEN): Privacy Threat Model for Mobile and Multi-Homed Nodes, June 26, 2006.

[8] R. Koodli, IP Address Location Privacy and Mobile IPv6: Problem Statement, May 2007.

[9] P. Reinbold and O. Bonaventure, "IP Micro-Mobility Protocols," *IEEE Communications Surveys & Tutorials*, pp. 40-57, 2003.

[10] Jukka Ylitalo, Jan Melen, Pekka Nikander, and Vesa Torvinen, "Re-thinking Security in IP based Micro-Mobility," in *Proc. of the 7th International Conference on Information Security Conference (ISC'04)*, Palo Alto, CA, USA, 2004, pp. 318-329.

[11] FemtoForum. (2010, June) Femtocells – Natural Solution for Offload – a Femto Forum brief.

[12] A. Valko, "Cellular IP: A New Approach to Internet Host Mobility," *ACM SIGCOMM Comp. Commun. Rev.*, vol. 29, no. 1, pp. 50-65, January 1999.

[13] H. Soliman, C. Castelluccia, K. El Malki, and L. Bellier, Hierarchical Mobile IPv6 Mobility Management (HMIPv6), August 2005.

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

[15] A. A.-G. Helmy, M. Jaseemuddin, and G. Bhaskara, "Multicast-based mobility: a novel architecture for efficient micromobility," *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 4, May 2004.

[16] Xiaoning He, Daichi Funato, and Toshiro Kawahara, "A dynamic micromobility domain construction scheme," in *Personal, Indoor and Mobile Radio Communications (PIMRC'03)*, vol. 3, 2003, pp. 2495 - 2499.

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

[18] S. Pack, M. Nam, and Y. Choi, "A Study On Optimal Hierarchy in Multi-Level Hierarchical Mobile IPv6 Networks," in *IEEE Globecom*, 2004, pp. 1290-1294.

[19] Shi-Wu Loa, Tei-Wei Kuo, Kam-Yiu Lam, and Guo-Hui Lic, "Efficient location area planning for cellular networks with hierarchical location databases," *Computer Networks*, vol. 45, no. 6, pp. 715-730, August 2004.

[20] V. Simon and S. Imre, "A Simulated Annealing Based Location Area Optimization in Next Generation Mobile Networks," *Journal of Mobile Information Systems*, vol. 3, no. 3/4, pp. 221-232, 2007.

[21] V. Simon, L. Bokor, and S. Imre, "A Hierarchical Network Design Solution for Mobile IPv6," *Journal of Mobile Multimedia (JMM)*, vol. 5, no. 4, pp. 317-332, 2009.

[22] L. Bokor, V. Simon, and S. Imre, "A Location Privacy Aware Network Planning Algorithm for Micromobility Protocols," in *Simulated Annealing, Theory with Applications*.: Sciyo, 2010, pp. 75-98.

[23] J.G. Markoulidakis, G.L. Lyberopoulos, D.F. Tsirkas, and E.D. Sykas, "Evaluation of location area planning scenarios in future mobile telecommunication systems," *Wireless Networks*, vol. 1, pp. 17 - 29, 1995.

[24] S. Tabbane, "Location Management Methods for Third Generation Mobile Systems," *IEEE Commun. Mag.*, vol. 35, no. 8, 1997.

[25] E. Cayirci and I.F. Akyildiz, "Optimal Location Area Design to Minimize Registration Signalling Traffic in Wireless Systems," *IEEE Transactions on Mobile Computing*, vol. 2, no. 1, 2003.

[26] V. Simon and S. Imre, "Location Area Design Algorithms for Minimizing Signalling Costs in Mobile Networks," in *Mobile Computing: Concepts, Methodologies, Tools, and Applications*, David Taniar, Ed., 2009, pp. 682-695.

[27] László Bokor, Vilmos Simon, István Dudás, and Sándor Imre, "Anycast Subnet Optimization for Efficient IPv6 Mobility Management," in *IEEE GIIS'07*, Marrakesh, 2007, pp. 187-190.

[28] N. B. Prajapati, R. R. Agravat, and M. I. Hasan, "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)*, pp. 1-7, March 2010.

[29] Gao Qian, Li Guang-xia, Lv Jing, Xu Yi-qun, and Zhou Ming, "Location Area Design for GEO Mobile Satellite System," in *Second International Conference on Computer Engineering and Applications (ICCEA)*, Bali Island, Indonesia, 2010, pp. 525 - 529.

[30] Claudia Diaz, Stefaan Seys, Joris Claessens, and and Bart Preneel, "Towards measuring anonymity," in *PET'02*, San Francisco, 2002.

[31] Andrei Serjantov and George Danezis, "Towards an Information Theoretic Metric for Anonymity," in *Privacy Enhancing Technologies*. Berlin / Heidelberg: Springer, 2003, vol. 2482/2003, pp. 259-263.

[32] Reza Shokri, Julien Freudiger, Murtuza Jadliwala, and Jean-Pierre Hubaux, "A Distortion-Based Metric for Location Privacy," in *8th ACM workshop on Privacy in the electronic society*, Chicago, Illinois, USA , 2009, pp. 21-30.

[33] Li Mingyan, Sampigethaya Krishna, Huang Leping, and Poovendran Radha, "Swing & swap: user-centric approaches towards maximizing location privacy," in *Proceedings of the 5th ACM workshop on Privacy in electronic society (WPES '06)*, Alexandria, VA, USA., 2006.

[34] Jiang Tao, J., Wang Helen, and Hu Yih-Chun, "Preserving Location Privacy in Wireless LANs," in *ACM MobiSys'07*, vol. Proceedings of the 5th international conference on Mobile systems, applications and services, San Juan, Puerto Rico, USA., 2007.

[35] Huang Leping, Yamane Hiroshi, Matsuura Kanta, and Sezaki Kaoru, "Silent Cascade: Enhancing Location Privacy Without Communication QoS Degradation," in *Security in pervasive computing*, J.A. Clark et al., Ed. Berlin Heidelberg: Springer-Verlag, 2006, vol. Lecture Notes in Computer Science 3934/2006, pp. 165-180.

[36] Hoh Baik, Gruteser Marco, Xiong Hui, and Alrabady Ansaf, "Preserving privacy in gps traces via uncertainty-aware path cloaking," in *Proceedings of the 14th ACM conference on Computer and communications security (ACM CCS '07)*, Alexandria, Virginia, USA., 2007.

[37] Hoh Baik et al., "Virtual trip lines for distributed privacy-preserving traffic monitoring," in *Proceeding of the 6th international conference on Mobile systems, applications, and services (ACM MobiSys '08)*, Breckenridge, Colorado, USA., 2008, pp. 15-28.

[38] T., Meyerowitz Joseph and Roy, Choudhury Romit, "Realtime location privacy via mobility prediction: creating confusion at crossroads," in *Proceedings of the 10th workshop on Mobile Computing Systems and Applications (ACM HotMobile '09)*, Santa Cruz, CA, USA, 2009.

László Bokor graduated in 2004 with M.Sc. degree in computer engineering from the Budapest University of Technology and Economics (BME) at the Department of Telecommunications. In 2006 he got an M.Sc.+ degree in bank informatics from the same university's Faculty of Economic and Social Sciences. He is a Ph.D. candidate at BME, member of the IEEE, member of Multimedia Networks Laboratory and Mobile Innovation Centre of BME where he participates in researches of wireless protocols and works on advanced mobility management related projects (as FP6-IST PHOENIX and ANEMONE, EUREKA-Celtic BOSS, FP7-ICT OPTIMIX, EURESCOM P1857, EUREKA-Celtic MEVICO). His research interests include IPv6 mobility, next generation networks, mobile broadband networking architectures, network performance analyzing, and heterogeneous networks.

Vilmos Simon received his Ph.D. from Budapest University of Technology and Economics (BUTE) in 2009 and is currently a senior lecturer at the Department of Telecommunications. His research interests include self-organizing and adaptive networks, evolution of communication protocols, opportunistic and delay-tolerant networks, mobility management and energy efficiency in 3G and 4G mobile systems. He participated in several research projects including the EU ICST-FET FP6 BIONETS where he also acted as a WP leader. He published 30+ papers in international journals and conferences, and acts as a reviewer or organizer for numerous scientific conferences.

Sándor Imre was born in Budapest in 1969. He received the M.Sc. degree in Electronic Engineering from the Budapest University of Technology (BME) in 1993. Next he started his Ph. D. studies at BME and obtained dr. univ. degree in 1996, Ph.D. degree in 1999 and DSc degree in 2007. Currently he is carrying his teaching activities as Head of the Dept. of Telecommunications of BME. He was invited to join the Mobile Innovation Centre of BME as R&D director in 2005. His research interest includes mobile and wireless systems, quantum computing and communications. Especially he has contributions on different wireless access technologies, mobility protocols and reconfigurable systems.