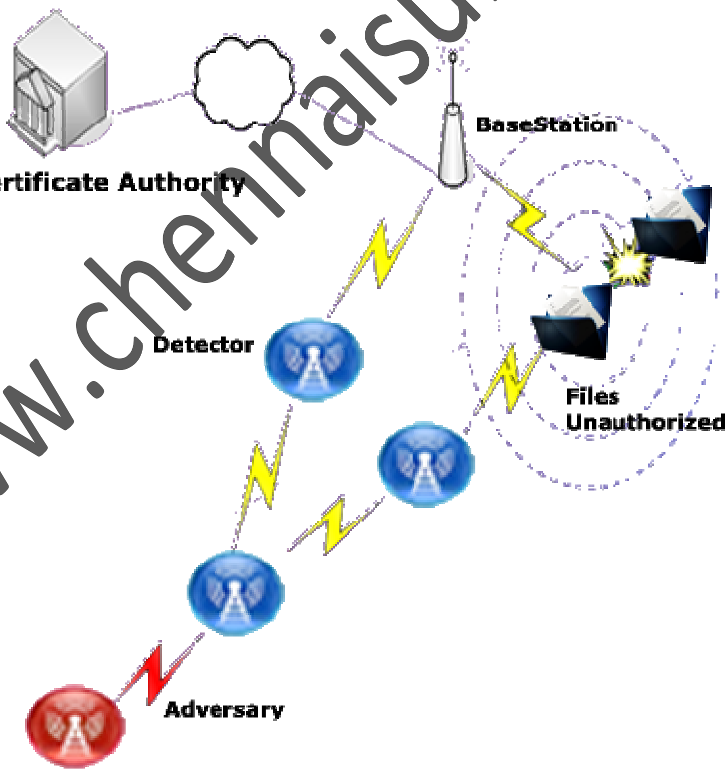
Non-Cooperative Location Privacy

Abstract:

In mobile networks, authentication is a required primitive for most security protocols. Unfortunately, an adversary can monitor pseudonyms used for authentication to track the location of mobile nodes. A frequently proposed solution to protect location privacy suggests that mobile nodes collectively change their pseudonyms in regions called mix zones. This approach is costly. Self-interested mobile nodes might thus decide not to cooperate and jeopardize the achievable location privacy. In this paper, we analyze non-cooperative behaviour of mobile nodes, where each node aims at maximizing its location privacy at a minimum cost. As in practice mobile nodes do not know their opponents' payoffs, we then consider static incomplete information. By means of numerical results, we predict behaviour of selfish mobile nodes. We then investigate dynamic games where nodes decide to change their pseudonym one after the other and show how this affects strategies at equilibrium.

Architecture:



Existing System:

In contrast with existing approaches, we consider rational mobile nodes that locally decide whether to change their pseudonyms. Although selfish behaviour can reduce the cost of location privacy, it can also jeopardize the welfare achieved with a location privacy scheme. We investigate whether the multiple pseudonym approach achieves location privacy in non-cooperative scenarios.

Disadvantages:

The drawback of this model is that nodes may have misaligned incentives (i.e., different privacy levels) and this can lead to failed attempts to achieve location privacy.

Proposed System:

We propose a user-centric location privacy model that captures the evolution of the location privacy level of mobile nodes over time and helps them determine when to change pseudonyms, which model the decisions of mobile nodes in a mix zone.

Advantages:

We analyze non-cooperative behaviour of mobile nodes by using this model, where each node aims at maximizing its location privacy at a minimum cost.

Algorithm:

Routing Algorithm:

The adversary A observes the set of n(T) nodes changing pseudonyms, where T is the time at which the pseudonym change occurs. A compares the set B of pseudonyms before the change with the set D of pseudonyms after the change and, based on the mobility of the nodes, predicts the most probable matching . Let pd|b = Pr(“Pseudonym d ∈ D corresponds to b ∈ B”), that is the probability that a new pseudonym d ∈ D corresponds to an old pseudonym b ∈ B. As is standard in the literature , the location privacy level of node i involved in a successful pseudonym change at time T is computed as the adversary’s uncertainty:

Modules:

1. **Location Privacy**
2. **User Centric Model**
3. **Pseudonym Change Module**

1) Location Privacy:

There are several techniques to mitigate the tracking of mobile nodes. We consider the use of multiple pseudonyms: over time, mobile nodes change the pseudonym to sign messages, thus reducing their long term link ability. To avoid spatial correlation of their location, mobile nodes in proximity coordinate pseudonym changes in regions called mix zones. We assume that as soon as a node changes pseudonym, the old pseudonym expires and is removed from the node’s memory. In other words, two nodes cannot use the same pseudonyms at the same time.

Mix zones can also conceal the trajectory of mobile nodes to protect against the spatial correlation of location traces, e.g., by using (i) silent/encrypted mix zones (ii) regions where the adversary has no coverage . Without loss of generality, we assume silent mix zones: mobile nodes turn off their transceivers and stop sending messages for a certain period of time. If at least two nodes change pseudonyms in a silent mix zone, a mixing of their whereabouts occurs and the mix zone becomes a confusion point for the adversary.

2) User Centric Model:

The entropy measures the location privacy achieved in specific mix zones at some point in time. However, location privacy needs of individuals vary depending on time and location. It is thus desirable to protect location privacy in a user-centric manner, such that each user can decide when and where to protect its location privacy. We consider a user-centric model of location privacy, where each mobile node locally monitors its location privacy over time. A network-wide metric could evaluate the network but might ignore that some nodes have a low location privacy level and are traceable for long distances.

As a user-centric approach captures the evolution of location pri- vacy of users over time, mobile nodes can evaluate the distance over which they are potentially tracked by an adversary (i.e., the distance-to-confusion) and can act upon it by deciding whether and when to change its pseudonym. With a user-centric model, mobile nodes can request a pseudonym change from other nodes in proximity if their local location privacy level is lower than a desired level.

3) Pseudonym Change Module:

We present the aspects of achieving location privacy with multiple pseudonyms in a rational environment. The key aspect is to consider costs and the potential location privacy gain when making a pseudonym change decision. Considering the cost of pseudonym and the available location privacy gain, the user-centric location privacy level might encourage selfish mobile nodes to change pseudonym and obtain a satisfactory location privacy level, as long as other nodes are also changing.

Nodes may also delay their decision in order to try to find the better conditions that maximize the effectiveness of pseudonym changes. Therefore, we investigate whether location privacy can emerge in a non-cooperative system despite the cost of changing pseudonym, differentiated privacy levels, and the need for coordination to achieve a confusion point.

Hardware Requirements:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

Software Requirements:

- Operating system : - Windows 8.
- Coding Language : C#.net
- Data Base : SQL Server 2008