Lawful Interception for Mobile IP Networks - a Mobile Agent Approach

Andres Rojas and Philip Branch
{anrojas, pbranch}@swin.edu.au
Swinburne University of Technology, Melbourne, Australia
14th October 2004

Abstract
Mobility enabling architectures, such as Mobile IP, bring unique challenges to the act of Lawful Interception (LI). Inefficiencies in bandwidth and host resource usage result when the LI model used in telephony networks is applied to the Mobile IP architecture. A Mobile Agent based approach is proposed that has the potential to meet the unique challenges of the Mobile IP and LI combination.

Keywords:- lawful interception, mobile IP, mobile agent

1 Introduction
Lawful Interception (LI) is the process whereby a Law Enforcement Agency (LEA) is legally allowed to intercept a target’s communications for law enforcement purposes. The process is dependent upon the provision of a legal warrant to carry out the interception, and the technology being available to perform the interception.

The authors believe that IP architectures that enable user mobility (eg. Mobile IP) will provide a transparent form of every-day communications one day [1]. It is prudent to research LI in networks such as Mobile IP as these bring a different dimension to the problem of LI [2].

This paper firstly argues that the model used in mobile telephony networks for activating interceptions is not a suitable model to apply to Mobile IP based networks as it suffers from scalability problems such as inefficient use of bandwidth and computing resources.

Secondly, we propose a potentially more flexible and efficient solution based on the use of Mobile Agents (MA). An outline of the components used and operation of the proposed solution is presented. Relevant to LI are the issues of the movement model used, predictive or reactive, and their potential to miss a target’s traffic, potential bandwidth and host resource usage benefits, and security risks inherent with using MAs within the LI context.

The next section introduces the LI activation model used for mobile telephony. Section III describes the implications of applying this model to a Mobile IP based network using a simple simulation. Section IV and V describes the MA based approach and future research and, finally, in section VI we present concluding remarks.

2 Lawful Interception (LI) in Mobile Telephony

In this section we focus on a specific mobile telephony technology - GSM, and the LI solution employed. In a GSM system the mobile switching center (MSC) is where the switching of telephone calls takes place. MSCs are complex pieces of infrastructure and have been engineered to handle the requirements that come with supporting LI.

The LI solution for GSM uses a centralized controller residing at the operation and maintenance center and an interception component which resides at each MSC which performs the actual physical interception of a call.
Once the legal document that permits an interception is served to the network operator, information relevant to the interception is loaded into the central interception component. This includes the mobile number being intercepted, the authorised start and stop date, and which agency to send data to.

As the number of MSCs in the network tends to be small, the model used to activate interception is a simple round robin model. The central interception controller sends an activation message to each MSC in the network one by one. These are acknowledged by each MSC. De-activating an interception is handled in the same way.

### 3 Applying the Activation Model to Mobile IP

Mobile IP technology [3] promises to provide mobility services such that a node may maintain its active sessions whilst on the move. This notion of mobility is analogous to mobile telephony’s notion in that active calls are maintained whilst a mobile user moves.

To support a network that services the equivalent area as a mobile telephony system, the Mobile IP infrastructure is characterised by less capacity per piece of equipment, therefore more numerous in number. Consider a simple Mobile IP network which provides coverage for a small city. Only the wired part of the network is considered as it is assumed that LI is placed at the edge.

The network topology consists of a backbone of $n$ nodes each connected to the next backbone node. Each backbone node is connected to $n$ child nodes (point-point). These nodes (routers), conceptually, service the suburbs of the city. Each “suburban” node is connected to $n$ child nodes again (point-point). These nodes (routers) are conceptually the nodes that service the city at a street level, and where LI functionality resides. The node that represents the central interception controller is connected to each backbone node.

The central controller sends an activation message to the first leaf node, waits for the acknowledgment and continues with the second leaf node, third, and so on until the interception is activated on all leaf nodes. Results for different values of $n$ are presented in Table 1.

<table>
<thead>
<tr>
<th>$n$</th>
<th>No. of leaf nodes</th>
<th>Activation Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>125</td>
<td>7.51</td>
</tr>
<tr>
<td>6</td>
<td>216</td>
<td>12.98</td>
</tr>
<tr>
<td>7</td>
<td>343</td>
<td>20.62</td>
</tr>
<tr>
<td>8</td>
<td>512</td>
<td>30.78</td>
</tr>
<tr>
<td>9</td>
<td>729</td>
<td>43.82</td>
</tr>
<tr>
<td>10</td>
<td>1000</td>
<td>60.11</td>
</tr>
<tr>
<td>11</td>
<td>1331</td>
<td>80.01</td>
</tr>
<tr>
<td>12</td>
<td>1728</td>
<td>103.88</td>
</tr>
</tbody>
</table>

Table 1: Activation times, total number of leaf nodes for different values of $n$.

Consider the movement of a target individual throughout the coverage area, and the period of time a target is intercept-able. A total of 3794 lawful interceptions were active in Australia in the 2002-03 period with an average interception period of 44.2 days [4]. It is highly unlikely that a target individual will move through all areas that are covered within the interception period. This leads to the assertion that the activation model leads to wasted bandwidth and computational resources because all activated interceptions use node resources as interception typically involves the analysis of all packets on a subnet to match them to those sent/received by the target [2].

For a simple movement case, where a target moves from an outer suburb to an opposing outer suburb, even though activations have been sent to all leaf nodes, only a fraction of these nodes needed activation. A target’s movement throughout the intercept period will range between the above, and movement through all coverage areas (unlikely).

Also of note is that with $n=8$, the total activation time is approximately 30 seconds. This time is important because if the communication contained a vital piece of evidence within the first 30 seconds of the intercept period, this traffic might be missed.

A more efficient interception scheme for mobility networks with a large number of leaf nodes is necessary.

### 4 A Mobile Agent based Approach

The concept of a Mobile Agent (MA) was explored in the 1990s as a new paradigm for distributed systems - an
There are varying definitions of what exactly an MA is. The authors define an MA, along the lines of [5], within the context of LI, as being a self-contained software that moves within the network with code, state and the ability to decide when to move to a new location.

The components in an MA based LI system for mobility networks include a Central Interception Controller managing all interceptions for the network and deploying MAs for each target, and the Mobile Agent - which carries the logic to configure interception, and the logic to decide when to move to a new network. Also part of the system are MA platforms throughout the network - which provide visiting MAs necessary resources, such as CPU time and networking - and LI enabling resources throughout the network which can be programmed by visiting MAs to intercept a target’s communications.

The ability for an MA to decide where to move, is of critical importance. As much of a target’s traffic as possible must be intercepted and delivered to the lawful agency. This traffic is evidence in criminal proceedings.

Two methods of determining movement for an MA for LI are foreseen. Reactive movement is movement of the MA once the target individual has already moved. The MA uses indications produced by network infrastructure. For example, in a Mobile IP network that uses an AAA service to authenticate and authorise it’s users, the AAA servers can be used to provide indications to the MA on a target’s movement into another administration area.

Another method is predictive movement where the benefit lies in the MA’s ability to move to the predicted network to setup the interception of traffic before the target moves there. The work by [7], for example, is based on the hypothesis that movement can be categorised into a random part and a regular, pattern based part. They propose a set of prediction algorithms that are relatively simple which make them cheap in terms of processing power.

The tracking of a target with 100% certainty provided by a reactive approach is offset by the possibility that the MA does not react in time to capture all of the target’s traffic. Conversely, the challenge for the MA that uses a predictive approach is to predict the movement accurately so that, again, all of the target’s traffic is intercepted.

As an example of how the LI application of MA would work, consider the predictive case shown in Figure 1. The central interception controller deploys the MA. The MA attaches to the MA platform in “net-A”, where the target is located. It uses the services provided by the platform to configure the LI resource for interception of traffic. The MA will then, upon prediction, move to “network-B” and use the MA platform there to configure interception.

![Figure 1: An LI system for a Mobile IP network using MA - predictive approach.](image)

### 5 Future Work

For both approaches to movement, there is a tradeoff that involves the potential to miss the target’s traffic. This is important as the intercepted traffic is evidence that can be used in criminal proceedings. For the reactive approach, future research will investigate how significant the delay is between a target’s movement and the MA movement. For the predictive approach, future work will focus on the accuracy of prediction, and how to reduce the impact of an unpredicted move on interception. For instance, a fully predictive approach might be compared to a technique where the MA propagates to each adjacent coverage area. Future research will also extend the work by [7].

The challenge of security is a critical issue when considering MA applications in general [8, 6, 9]. [6] argues that the problem of the protection of an MA from a malicious MA platform is not solved (9 provides countermeasures). A rogue MA platform could identify who is being targeted, modify the MA, or make the target aware...
of the interception. Future research should focus on verifying the countermeasures presented in the literature. [6] also describes that the very definition of an MA is identical to that which defines a virus: they are both mobile code which act autonomously to achieve their defined purpose. [8] and [9] suggest signed code from trusted sources, and access control for MAs as possible answers. Future research should concentrate on investigating whether an MA that is constrained to migrate within one network only, and to migrate to specific types of hosts (MA platforms) can be trusted.

Future work will also investigate how much of a saving can be attained under different mobility models [10], and how this is affected by inaccurate predictions. Related to this is determining how much of a benefit the MA approach delivers with respect to host resources, and determining ways in which this can be measured.

6 Conclusion
Research into Lawful Interception in IP networks is in its infancy. LI systems based on sniffers are used by ISPs and governments to provide LI functionality in IP networks today. It is not known what LI solutions are needed for next generation networks such as mobile IP.

Applying the simple interception activation model used in mobile telephony to a mobile IP network with similar coverage results in scalability issues. Inefficient use of bandwidth and host resources result in all but the most pessimistic cases of movement.

An approach that leverages the fact that a target user is mobile is proposed - based on the use of Mobile Agents. The control of where to activate an interception is encapsulated within a MA that has the ability to move throughout the coverage area of the network autonomously. The decision by a MA to move to a new network can be either reactive or predictive.

Challenges to be studied further include: how much bandwidth and host resources are saved under different mobility models, how can the time lag between the target movement and the MA movement be minimized, and, how can the prediction algorithm be made more accurate, simpler to execute by the MA, and how can the effects of unpredicted movement be minimized.

Although the use of MA technology carries with it many security issues, the focus of this research within the LI context promises to solve the unique problems that exist with the mobile IP and LI combination.

References