Abstract

This Internet Draft proposes a basic architectural model which allows users to exchange spatial location information.

<table>
<thead>
<tr>
<th>Internet Draft</th>
<th>Basic SLoP Architecture Proposal</th>
<th>July 15, 2000</th>
</tr>
</thead>
</table>

Abstract

<table>
<thead>
<tr>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
</tr>
<tr>
<td>1.1 Scope</td>
</tr>
<tr>
<td>1.2 Terminology</td>
</tr>
<tr>
<td>2 Architecture</td>
</tr>
<tr>
<td>2.2 Broker Architecture</td>
</tr>
<tr>
<td>2.3 Elements</td>
</tr>
<tr>
<td>2.4 Protocol Issues</td>
</tr>
<tr>
<td>3 Roaming among SLoP Servers</td>
</tr>
<tr>
<td>3.1 Roaming Architecture</td>
</tr>
<tr>
<td>3.2 Server Discovery</td>
</tr>
<tr>
<td>4 Security</td>
</tr>
</tbody>
</table>
1. Introduction

There are several on-going efforts defining architectures to allow devices to exchange location information. There are even several systems being put into service that make use of location information. The location may be obtained in many ways: by GPS; by triangulation; by configuration; etc.

In order to allow services based on spatial location information to inter-operate, a simple architecture supporting the transport of spatial location information needs to be developed. This architecture will impact any protocol(s) developed.

Certain requirements [SLOP-REQ] are assumed. Furthermore, it is assumed that targets follow an orderly naming system [TARGET] and a simple, text-based format for spatial information is also assumed [FORMAT].

1.1 Scope

This document strives to present basic considerations on developing an architecture to support location information services. This architecture should consider solutions being developed within other bodies, such as the WAP Forum and W3C. The architecture developed should support and inter-work with such other architectures rather than replace them. It does not set out to assign requirements for any architecture or applications.

How the spatial location information is obtained is outside of the scope of this document.

1.2 Terminology

Client: The entity which desired to learn the location of the target. One end of the protocol.

Server: Entity which supplies the location of the target to the client. One end of the protocol.

SLoP: Spatial Location Protocol

TAD: Target record Accessing ID

Target: The entity whose location is known by the server and desired by the client. The protocol does not specify how the server learns the location of the target.

TID: Target information ID

2 Architecture

2.1 Basic Architecture

The following diagram shows a basic functional architecture supporting spatial location services. This is not a complete architecture, but a basic reference for discussion. The actual physical realization of the functions is an implementation issue.
Note that the architecture is showing a one-sided exchange of spatial location information for simplicity. It is likely that exchanges may be bi-direction, and no restrictions on this are implied.

2.2 Broker Architecture

There may be scalability concerns with the SLoP architecture. To ensure scalability, a broker architecture is suggested. This architecture is provided below:

2.3 Elements

Client - the consumer/requestor of spatial location information.

Server - acts as a SLoP server for the target. It may support more than one target.
SLoP Broker - acts as a forwarder/transit element for several SLoP servers. The broker may either provide redirection services or simple message routing.

Target - device or entity whose location information is desired by the client. The target may change servers, especially if the target is mobile.

Policy Database - database where the target’s policy for granting access to it’s location. The database needs to be accessible by the server and, maybe, by the target or the owner of the target as well.

2.4 Protocol Issues

It is assumed that SLoP may use UDP, TCP or SCTP as transport. The client needs to be able to request certain elements of a format.

The server should be able to provide certain elements of a format based on authorization policy (ex: give my speed, but not my position). The server should be able to obfuscate a (numeric/coordinate) location based on authorization policy.

The protocol should extendable to support new location representations and information.

3 Roaming among SLoP Servers

Target roaming between location servers means the representation of a target changing from one location server to another.

3.1 Roaming Architecture

In the "Target Naming Scheme" [TARGET] document, two identifiers to name a target are proposed: (1) Target information ID (TID) and (2) Target record Accessing ID (TAD).

Using identifiers (TID and TAD) for a target can used for roaming purposes. Thus, the Target can change its current representing location server from one location server to another in an ingenious and easy manner.

After authentication between a target and a location server, the target’s TID is registered to the spatial location server. According to the target’s information registered, the location server immediately assigns a TAD to that "Target" for future client queries of the target’s spatial location. This process is described in Figure 3-1. This process requires the pertinent secure mechanism. The security aspect of the transactions will be covered by other document of the group.

If the Target is moving and turns under another server scope, a temporary TAD will be added to the same TID and to the original TAD. That transaction is depicted in Figure-1.b)
Figure 3.1: TID Registration and TAD assignment

```
+-----------+
| SLoP Server|
| (TID, TAD  |
| TADtemp)   |
+-----------+
  |
+-----------+ +-----------+
| Target TID| .............>| SLoP Server|
| +-----------+ | (TADtemp) |
| +-----------+     +-----------+
```

Figure 3.2: Temporary TAD assignment when roaming.

A target has a default TAD assigned by a server that serves as a default record accessing ID. In roaming situations, the visited location server becomes the current representing location server for the target. After mutually authenticated each other on the Target’s TID (or a subset of it) and the visited server ID, the visited server allocates a temporary TAD for the Target and informs its default location server of the target’s current temporary TAD.

The default location server of the target can then bind the two TADs (the default and the temporary).

When a client requests the location information of the Target via the default TAD to the default location server, the server replies with the temporary Target’s TAD. Then, the client can request the location information via the temporary TAD to the target’s visited location server.

To keep updated any new or recently assigned TAD within the scope of SLoP servers, a synchronization process is implemented in the group of SLOP elements serving in a common area.

3.2 Server Discovery

If a client does not know of an existing SLoP server, it must perform a server discovery process. Figure 3.3 shows a mechanism for doing this, based upon TAD values.

Figure 3.3: Server Discovery using directly TAD

```
+------++------------------++---++
| Client| (TAD, Auth)          | Home|
| +------++<........................>|
|       | (TADtemp, Auth)       | SLoP Server|
|       |                     | (TID, TAD  |
|       |                     | TADtemp)   |
```
The two possible mechanisms are defined below.

Sending the SLoP queries to a well-known multicast address which SLoP servers listen. There may be scalability problems with this approach, so it might be useful in closed networks.

The second approach is using a DHCP client for obtaining a DNS string pertaining to the local SLoP server. Afterward, the Client can construct the FQDN to resolve the SLoP address. This approach is feasible via a DHCP (6) option for obtaining a string that contains the SLoP server domain name.

The Client provides to the server basic information from the Target that it tries to locate. Then, the server checks if any of them match with the partial information received (Figure-3). If it finds a match, it will be retrieved to the Client for contacting the target’s home server. Otherwise, the server will return unknown Target or it will ask for additional information.

```
------- (Name=Jose ) ----------
|Client|  .....................|  Primary |    ,,,,,,,,,,,,,,,,,,,,
------- <......................|SLoP Server|....,TAD1=Pete,English ,
               | (TAD3,TAD7,Auth) | (TID,TAD | ,TAD2=Mari,French ,
               | TADtemp) | TADtemp) | ,TAD3=Jose,Portug ,
               |          |          | ,TAD7=Jose,Spanish ,
               |          |          | ,      :           ,
               |          |          | ,,,,,,,,,,,,,,,,,,,
------- (TAD7,Auth) > Visited |
(TAD7,Auth) | SLoP Server |
(TADtemp) |
```

Figure 3.3 Server Discovery with restricted information

4 Security

Any architecture developed for exchanging spatial location information introduces many complications to security. This document does not seek to list or set requirements for the security architecture, but rather discuss some issues.

4.1 Privacy Concerns

Spatial location information presents privacy concerns. It could be possible to track a user’s location if not designed correctly. It is a basic assumption that the user MUST be in control of his/her location information. The user MUST explicitly authorize access to his/her location information data.

4.2 Security Concerns
It should be noted that there may be local regulations which necessitate the access of location information data to third parties (for the purposes of emergency calls, etc.).

The communication between the various entities transporting location information data MUST be secure.

There must be an authorization method for allowing users to access location services and allowing those services from querying users based upon location information.

4.3 Security Methods

Three possible security methods are introduced below. The first method but relies on underlying security mechanisms, such as IP Security. The second method is hop-by-hop security. The third method involves secure proxies.

4.3.1 Underlying Security

When possible, IP Sec should be used.

4.3.2 Hop-By-Hop

When firewalls, NATs or proxies prevent end-to-end security, hop-by-hop security should be employed.

```
 Shared Secret 1     Shared Secret 2
+-------+           +-------+           +-------+
 |       |           |       |           |       |
 | SLoP1 +---------->+ SLoP2 +---------->+ SLoP3 |
 |       |           |       |           |       |
 +-------+           +-------+           +-------+
```

4.3.3 Secure Proxying

Secure proxying is needed in other protocols, and this should be studied for use with SLoP.

4.4 Policy Issues

It is suggest the a simple policy architecture is used. After authentication, users are granted a user class. This user class is then used to determine the rights to spatial location information, when compared against the target’s policy database.

The user class can be used to restrict (or grant access) to the following information:

- Accuracy
- Frequency
- Application Specific data

5 IANA Considerations
TBD
6 Issues for Further Study

Roaming Support
Broker support
Server Discovery
Authentication support

7 Acknowledgements

This draft has taken some elements from the following draft: <draft-nyckelgard-isl-arch-00.txt>. The author would like to thank

Funding for the RFC editor function is currently provided by the Internet Society.

8 Author’s Addresses

John Loughney
Nokia Research Center
PO Box 407
FIN-00045 Nokia Group
Finland
john.loughney@nokia.com

Jose Costa-Requena
Nokia Corporation
Office: Heikkilantie 7, FIN-00210 HELSINKI
Phone: +358 9 5116 2209
Fax: +358 9 5116 2010
Email: Jose.Costa-Requena@nokia.com

9 References


[TARGET] Tang, et al.; "Target Naming Scheme"; <draft-tang-spatial-target-00.txt>; July 2000; Work in Progress


Copyright Statement

Copyright (C) The Internet Society (2000). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it
or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing...