Introduction

Goal:
• To investigate a new nature-inspired distributed computing technique.
• The selected nature field is Neuroscience. Specifically, how neurons recover from injury in the peripheral nervous system and the supportive cells that work as helpers for neurons to build connections and find paths.
• Design and implementation of a general purpose middleware for P2P applications that require a high degree of anonymity between peers.

Theoretical background:
Neurons create connections between them called Synapses. Those synapses are protected by myelin, which at the same time contains a variety of supportive cells that protects the connection and communication. If the synapse is broken (injury), Schwann cells will work to help the injured neuron to re-build the broken connection. These Schwann cells have a Neuron Growth Factor (NGF) which attracts a neuron's axon towards its destination.

Diagram of a presynaptic and postsynaptic neuron joined by a synapse, which shows what happens at the axon terminal and dentritic spine level.

In terms of P2P systems, we have special interest in systems that provide anonymity, which as a side effect also improves security and freedom of speech.
• Freenet: distributed data store system with strong anonymity which benefits directly freedom of speech. It protects both authors and readers when data is publicized, replicated or retrieved.
• Anonymous Remailers: it strips out the sender's identification marks from all email messages it receives, replace them with new identification marks and forwards, or “re-mail” them to the intended recipient.
• Pseudonymous Remailers: It replace the sender's real identity from emails with a pseudonym that is known only by the server to handle replies, and forwards, or “re-mail” them to the intended recipient.

Design

A general purpose middleware for P2P applications that require a high degree of anonymity between peers.
• Main purpose: Anonymity, which has side effects such as privacy and freedom of speech.

Mapping of Neuroscience into P2P applications

<table>
<thead>
<tr>
<th>Concept</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presynaptic Neuron Peer</td>
<td>A peer that originates a message.</td>
</tr>
<tr>
<td>Postsynaptic Neuron Peer</td>
<td>A peer that receives a message.</td>
</tr>
<tr>
<td>Schwann Peer</td>
<td>Any peer that forwards messages.</td>
</tr>
<tr>
<td>NGF to build routes</td>
<td>The value peers use to decide on the route for a message.</td>
</tr>
<tr>
<td>Synapse connection</td>
<td>The path once a message is delivered from the presynaptic to the postsynaptic peer.</td>
</tr>
</tbody>
</table>

• Forwarding messages:
  • Every Peer acts as a Schwann Peer which has a certain amount of NGF. Its job is to forward or deliver messages.
  • Routes are created through the highest NGF at each hop.
  • When a Schwann Peer forwards a packet it consumes some of its own NGF.
  • No information that could trace back the sender is kept at any point.
  • The presynaptic peer decides how many hops the message has to do before it is delivered. Anonymity is assured with high values of this indirection.

Evaluation

• Anonymity: no simple way to trace back to the originator of a message; the identity of the sender is protected.
• Routing: efficient in terms of providing anonymity, as it depends on the NGF value, which changes constantly giving high churn to the network.
• Simplicity: simple concept that yields the desired results.
• Portability and Re-usability: the prototype built specifically for portability and re-usability, desirable characteristics of any SON implementation.
• Nature-Inspired concepts were successfully applied to design a distributed system that has a positive social contribution if used correctly.
• Typical network attacks such as eavesdropping, data modification, identity spoofing, man-in-the-middle and replay are not covered.

Conclusion

The Neuroscience concept of Schwann cells that act as helpers for neurons to build connections between them has been successfully applied to P2P systems, which supports the provision of a general middleware to send anonymous messages.

Future work: provide a distributed solution for managing the information and to provide encryption and secure channels to send information.