Towards Cellular IP Address Assignment in Wireless Heterogeneous Sensor Networks

Authors: Mazen G. Khair, Burak Kantarci, and Hussein. T. Mouftah
Presentation Outline

- Cellular IP
- Challenges
- Inter-domain and Intra-domain IP address assignment architecture
- IP address assignment scheme
- Uniform IP range assignment
- Blocking types
  - Block A: Real Blocking
  - Block B: Unjustified Acceptance
  - Block C: Unjustified Rejection
- Simulation settings
- Results
- Conclusion
Cellular IP

- Cellular IP specifies a protocol to enable routing the IP datagrams to moving mobile hosts in a local network.
- It provides local mobility and handoff support for frequently moving hosts,
  - i.e., mobile hosts can migrate inside a Cellular IP Network with little “disturbance” to active data flows.
- It is only intended for local area networks and metropolitan area networks.
- For mobility between different Cellular IP Networks, it works with Mobile IP
  - Out of the scope.
Cellular IP: How it works?

- Cellular IP can also be implemented on top of regular IP routers to allow smooth migration from existing installations.

- Idle mobile hosts
  - periodically generate short control packets, i.e., *paging-update packets (PUPs)*
  - *Send PUPs to* the nearest available base station.
  - PUPs are forwarded in the access network toward the gateway router (GW) on a hop-by-hop basis.
  - Nodes map mobile host identifiers to the port through which the PUP arrived.
Cellular IP
Challenges

- Both peers must go through a third party like Skype.
- There is no way to communicate with a cell or device behind the ISP firewall.
  - A Network Address Translation (NAT) router assigns private IP addresses to local users as a security measure.
- Adaptability to the varying traffic profile in time
  - Hard to handle by assigning a static IP pool to each intra-domain router
- Secure architecture in which only registered devices can communicate
  - This has been done for intra and inter-domain call admission
IP assignment architecture.
Security and Firewall

- Intra and Inter-domain IP-DNS provide security measures for the proposed architecture.
- Only registered IP devices can join the IP network.
- Only registered IP device numbers can initiate phone calls with other registered IP devices.
IP address assignment scheme

- Loop on all the IP addresses list to find the number of available IP addresses.
- Select a random number between 0 and number of available IP addresses
- Loop on the IP address list to locate the selected IP address.
IP address assignment scheme (Cont ‘d)

- Loop on the IP address list to find the number of available IP addresses.
  - Available number is 4
- Select a random number between 0 and 4
  - Let us assume 3
- Loop on the IP addresses list, to pick the IP address in the 3rd available position.

List of IP Addresses

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Uniform IP Address Range Assignment Method

- Divide the total number of available IP addresses on the number of network nodes
  - \(12/3 = 4\) IP addresses per node

- Based on the incoming request at a given node, loop on the IP address range specified for that source node.
  - Let us assume the request arrives on node 3 so the IP address range is \([9,12]\) for node-3.

- Apply the previous IP address scheme to select available IP address randomly from the IP range of node-3.
Threshold-based

- Each node broadcasts a message that has two lists:
  - List of available IP addresses and
  - List of released IP addresses

Threshold ($\tau_i$):

\[
\tau_i = \frac{\phi_i}{\zeta_i}
\]

- Upon the receipt of these two lists from all nodes that are eligible to advertise,
  - Each node $i$ updates its IP address list.
IP address update scheme

Released IP Addresses

<table>
<thead>
<tr>
<th>Node 3</th>
<th>Node 2</th>
<th>Node 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

List of IP Addresses

<table>
<thead>
<tr>
<th>Node 3</th>
<th>Node 2</th>
<th>Node 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

OR Operation

0 OR 0 = 0
0 OR 1 = 1
1 OR 0 = 1
1 OR 1 = 1

AND Operation

0 AND 0 = 0
0 AND 1 = 0
1 AND 0 = 0
1 AND 1 = 1
Blocking probability types

- **Real Blocking** ($\beta_i$)
  - The entire IP addresses are occupied.

- **Unjustified Acceptance** ($\phi_i$)
  - The status of the IP addresses is out of date
  - IP address status: Available
    - whereas it is occupied by another user.

- **Unjustified Rejection** ($\kappa_i$)
  - IP address status: Occupied
    - whereas it is available to be used but due to the out of date of the IP address status.
Simulation settings

- Downtown San Francisco network
  - $\sim 1\text{mi}^2$ with an estimated population of 15000 residents
  - Number of nodes ($N$) = 25

- Simulation Parameters
  - Service time 60s
  - Number of IP addresses is 400.
  - $\tau_i \in \{0.1\%, 0.2\%, 0.3\%\}$
Results

- Overall blocking probability

\[
\sum_{i} (\beta_i + \varphi_i + \chi_i) / N
\]
Resource Utilization

![Graph showing resource utilization vs. arrival rate (1/s)].

- Zero Threshold
- 0.5% Threshold
- 1% Threshold
- 1.5% Threshold
- IP Range
Blocking due to out of date routing info.

- **Unjustified acceptance**
  \[
  \sum_{i} \frac{\varphi_i}{N}
  \]

- **Unjustified rejection**
  \[
  \sum_{i} \frac{\chi_i}{N}
  \]

- More frequent updates lead to low unjustified acceptance
- More frequent updates lead to low unjustified rejection

\[\varphi \ll \chi\]
As the load gets heavier, low threshold values in threshold-based assignment lead to better enhancement in the blocking probability of the uniform IP Range assignment.

\[ \varepsilon = \frac{\beta_{IPRange}^k - \beta_{IPRange}^{\tau_k}}{\beta_{IPRange}} \]
Conclusion

- Dynamic management of IP addresses in IP networks has been proposed
- Only registered devices are admitted
  - Secure admission
- Each intra-domain wireless router advertises its IP address status table based on a threshold
  - Threshold ➔ Some per cent of call drop
- Adaptable to the changing traffic profile rather than assigning fixed IP ranges to the routers
  - Leads to close blocking probability to that of fixed IP range assignment as the load gets heavier
Thank you!

Questions?

- Dr. Mazen Khair
  - Email: mkhair@site.uottawa.ca

- Dr. Burak Kantarci
  - Email: kantarci@site.uottawa.ca

- Prof. Hussein Mouftah
  - Email: mouftah@site.uottawa.ca
IP address update scheme

Released IP Addresses

<table>
<thead>
<tr>
<th>Node 3</th>
<th>Node 2</th>
<th>Node 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

List of IP Addresses

<table>
<thead>
<tr>
<th>Node 3</th>
<th>Node 2</th>
<th>Node 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

OR Operation

\[
\text{A OR B}
\]

AND Operation

\[
\text{A AND B}
\]
IP assignment architecture.
IP assignment architecture.