Cases Study- PCP Deployment in Mobile Network

draft-chen-pcp-mobile-deployment-00.txt

IETF 83- Paris, Mar 2012

Gang Chen,   China Mobile

Zhen Cao,   China Mobile

Mohamed Boucadair,   France Telecom

Introductions

- Overviews
  - Provided concrete deployment modes and analysis in mobile network environment
  - Talked about specific demands to PCP technology
- Goals
  - Inform particular concerns from a mobile network aspect
  - Motivate new works in PCP WG
  - Generalize experiences regarding PCP practices

Motivations

- A PCP Study Item had proposed in 3GPP but failed...because NAT and Firewalls are not in scope (However, PLMNs involve already these functions)

- The current PCP base specification explicitly mentions the benefits to reduce battery consumption (see the introduction)

- We need a place to encourage devices with low battery resources to embed a PCP client (mobile terminal, advanced sensors, etc.)

Scenario

- Always-on Applications on Operator's Network

  - Instant Message (MSN, QQ, Fetion) and P2P application (BitTorrent exhibits this behavior during choke periods)

  - Those applications are producing small data of keepalive at a relatively constant rate to keep long-lived TCP connections

- Keepalives would let several nodes to keep track of all connections that pass through them

  - States on FW/NAT
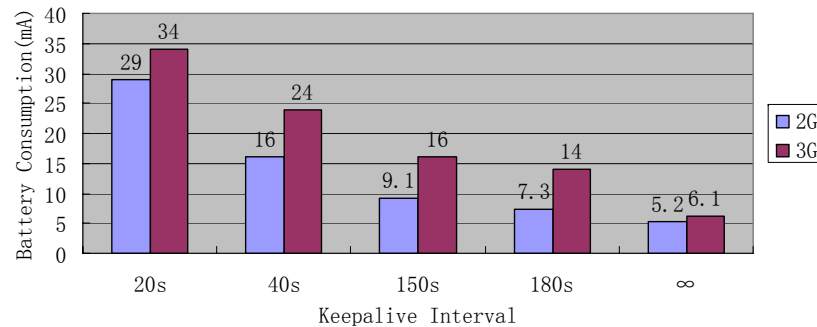
  - States on MGW

  - States on APPs servers

ME   eNB   MGW   Firewall   APP servers
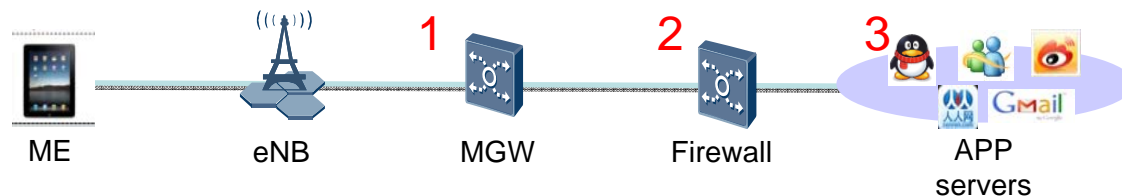
Problem Statements

- ## Radio Resource Consumption
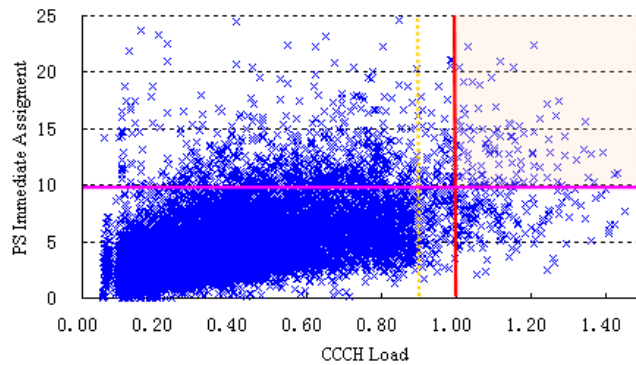
A dedicated air channel needs to be assigned to each keepalive message. It may cause congestion and calling failures due to radio resource depletions
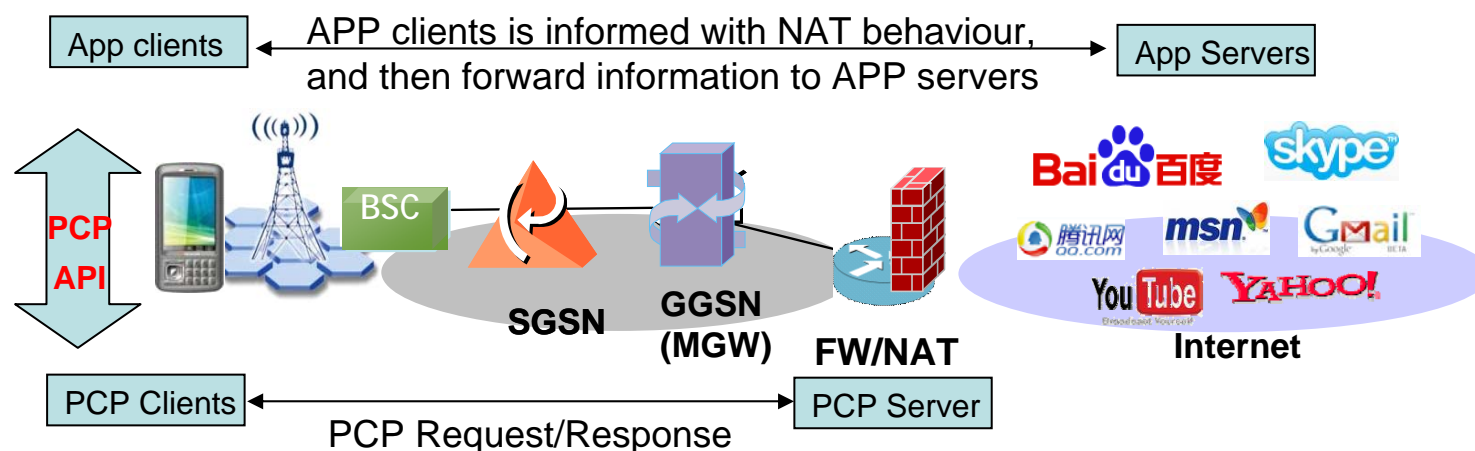
- ## Terminal Energy consumption

Battery consumption is reduced with decline of keepalive frequency

- ## Operational profits consumption
  - 16% instant signalling message would consume 50%~70% radio resource

Case1: PCP Clients located on UE

App clients → App Servers: APP clients is informed with NAT behaviour, and then forward information to APP servers

PCP Clients ↔ PCP Server: PCP Request/Response

- PCP API
  - The basic role is to provide applications with capabilities of triggering PCP requests and carrying PCP responds to apps
  - PCP API could eject an exception inform PCP server to delete related port binding, when application or PCP client is failed accidentally
- Authentication consideration
  - Provisioning of new credentials to mobile devices is a difficult tasks.
  - The integration with SIM authentication is one solution
  - Other way is to open authentication capability such as 3GPP GAA (Generic Authentication Architecture) defined in 3GPP 33.220

Case2: PCP Client located on MGW
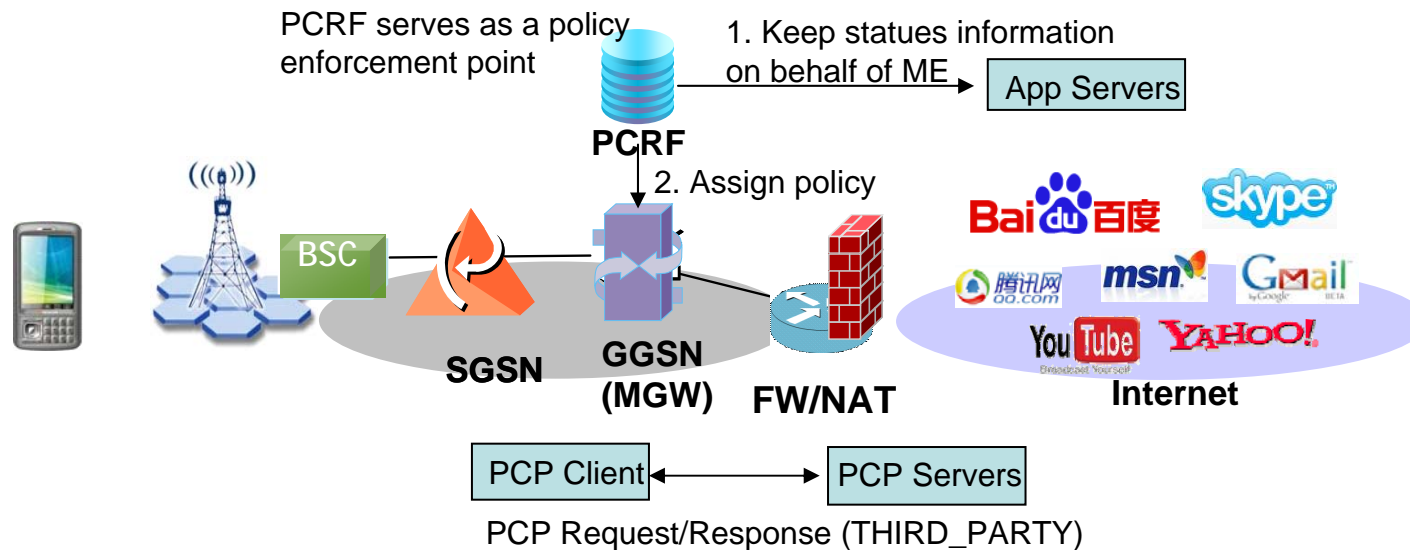
- **PCP Whitelist/Blacklist Design**
  - Whitelist priorities PCP requests sending from an operators trusted node, e.g. MGW, etc
  - Blacklist protect PCP server from overloaded PCP requests process and malicious attacks
- **PCP Policy Enforcements**
  - PCP requests could be labeled with different QoS tags (it might be implemented by adding one option).
  - PCP servers would take more fine-grained controls to occupy pre-determinative ports resources (both on quantity and hold-up time)

Next Steps

- Is it a valid input for WG?
- Adopted it as new work item?