Cellular IP report

A Katouzian

Detecen, Germany

1.o Introduction

Cellular IP represents a new mobile host protocol that is optimised to provide access to a mobile IP enabled Internet in support of fast moving wireless hosts. It is firmly based on IP design principles allowing Cellular IP to scale from Pico to metropolitan area installation.
Cellular systems are optimised to provide fast and smooth handoffs within restricted geographical areas. A scalable forwarding protocol interconnects distinct cellular networks to support roaming between them.
Mobility management requires mobile hosts to send registration information after migration. Hence the resulting signalling overhead has significant impact on the performance of wireless access networks.

2.0 Applicability

Cellular IP is applicable to all networks ranging from LANs to metropolitan area networks. To provide global mobility support, mobile IP should be used above cellular IP.

3.0 Architectural components

Cellular IP Node
This is also known as base station. A cellular IP network consists of interconnected
Cellular IP nodes. The nodes route IP packets inside the cellular network and communicate with mobiles via wireless interface. The cellular IP node that has wireless interface is also called a Base Station.
Cellular IP Gateway
This is a cellular IP node that is connected to a regular IP network by at least one of its interfaces.
Cellular IP Mobile Host
A Cellular IP mobile host that implements the cellular IP protocol.

4.0 Protocol Overview

This section consist of routing, Handoffs and paging algorithms. Handoff is a change of access point during active data transmission or reception. During or immediately after handoff packet losses may occur due to delayed propagation of new information location.
Figure 1 shows a schematic of multiple cellular IP networks providing access to the internet.
Base stations periodically emit beacon signals. Mobile hosts use these beacon signals to locate the nearest Base stations. A mobile host can transmit a packet by relaying it to the nearest Base Station.
All IP packets transmitted by a mobile host are routed from the Base Station to the Gateway by hop-by-hop shortest path routing, regardless of the destination address.
Cellular IP nodes maintain route Cache. Packets transmitted by the mobile host create and update entries in each node's cache. An entry maps the mobile host's IP address to the neighbour from which the packet arrived to the node.
The chain of cached mappings referring to a single mobile host constitutes a reverse path for downlink packets addressed to the same mobile host. As the mobile host migrates, the chain always points to its current location because its uplink packets create new and change old mappings.
To prevent its mapping from time out, a mobile host can periodically transmit control packages. Control packets are ICMP (Internet Control Management Protocol) packets with specific authentication payloads. Mobile hosts that are not actively transmitting or receiving data but, want to be reachable for incoming packets, let their route Cache mappings time out, but, maintain Paging Cache mappings. IP packets addressed to these mobile hosts will be routed by Paging Caches. Paging Caches have a longer time out value than Route Cache and are not necessarily maintained in every node.

5.0 Routing

Packets transmitted by mobile hosts are routed to the Gateway using shortest path hop-by-hop routing. Cellular IP nodes monitor these passing data packets and use them to create and update Route Cache mappings. These map mobile host IP addresses to Downlink neighbours of the Cellular IP nodes. Packet addressed to the mobile host are routed along the reverse path, on a hop-by-hop basis, by these Route Cache Mappings.

The structure and basic operation of routing is similar to that of location management. To clarify the duality between the Paging Caches and Route caches we shall refer to the table 1.
The mobile host may keep receiving data packets without sending data for possibly long durations. To keep its Route Cache mappings up to data and to avoid repeated paging, mobile hosts in active state that have no data to send must send periodic route-update packets. Like uplink data packets, route-update packets update Route Caches and ensure that the hop-by-hop route from the gateway to the mobile host does not time out.

In addition, active mobile hosts must transmit a route-update packet when they cross cell border s. This is required because the Route Cache mappings associated with the new Base Station can only be created by authenticated route-update packets. Data packets are not required to carry authentication information and hence can refresh, but not modify Route Cache mappings.
For reliability and timeliness, Paging Caches also contain mobile hosts that are contained by Route Caches. For this reason, Paging Caches are updated by all uplink packets and refreshed by all uplink packets including data packets.

6.0 Handoffs

This is based on a simple approach to mobility, supports fast and simple handoffs at the price of potential packet loss. Hand off is initiated by mobile hosts. Hosts listen to the beacons transmitted by base stations and initiate handoff based on signal strength measurements. To perform a handoff a mobile host has to tune its radio to the new base station and send a route-update packet. This creates routing cache mappings on route to the gateway hence configuring the downlink route to the new base station. Handoff latency is the time that elapses between the handoff and the arrival of the first packet through the new route.
Hand off latency is the time that elapses between the handoff and the arrival of the first packet through the new route.
For hard handoffs the latency time is the sum of round trip time between the mobile host and the cross-over point, which is the gateway in the worst case, as downlink packets may be lost. The mappings associates with the old base station are not cleared at hand off, they timeout as the associated soft-state timers expire.
Before the mapping timeout, a period exists when both the old and new downlink routes are valid and packets are delivered through both Base Stations. This feature is used in cellular IP semisoft handoffs algorithms, that improves handoff performance. The semisoft handoff procedure has two components described below.
First, in order to reduce handoff latency, the routing cache mappings associated with the new base station must be created before the actual handoff takes place. When the mobile host initiates a hand off it sends a semisoft packet to the new base station and immediately returns listening to the old base station. Afterwards the host can perform a regular handoff. The semisoft delay can be an arbitrary value between the mobile gateway round trip time and the route timeout. The delay ensures that by the time the host tunes its radio to the new base station, its downlink packets are delivered through both the old and new base stations.
The semisoft packet ensures that the mobile host continues to receive packets immediately after handoff, it does not ,however, assure smooth handoff. Depending on the network topology and traffic conditions, the time to transmit packet to the old and new base stations will be different. This means the packets transmitted are not synchronised at the host mobile. If the new base station lags behind the old one, then the mobile host may receive dual packets. If the new base station gets a head in receiving packets, it would mean the packets will be deemed to be missing from the data stream observed at the receiving mobile host.
The second component is based on the observation that perfect synchronisation of the two streams is not necessary. To eliminate this one can introduce a constant delay sufficient to compensate, with high probability, the time difference between the two streams.
This is best achieved at the cross-over switch that understands a semisoft packet has arrived from a mobile host that has a mapping to another interface. The mapping created by the semisoft packet has a flag that states this downlink packet must pass a delay device before transmission. After handoff, the mobile host will send data or route-update packets along the new path clearing the flag and causing all packets in the delay device to be forwarded to the mobile host.

7.0 Paging

In cellular IP an idle mobile host is defined as one which has not received data packets for a system specific time active-state-timeout. The idle mobile hosts allow their respective soft-state routing cache mappings to time out. These hosts transmit paging-update packets at regular intervals defined by paging-update-time. This is an empty IP packet addressed to the gateway that is distinguished from a route-update packet by its IP type parameter. Paging updates are sent to the base station that offers best signal quality. The paging-update packets are routed on a hop-by-hop basis to gateway. Base stations may optionally maintain paging cache. A paging cache has the same format and operation as a routing cache except for two differences:

1. Paging cache mappings have a longer time out period called paging-timeout.
2. Paging cache mappings are updated by any packet sent by mobile hosts including paging update packets.

In contrast, routing cache mappings are updated by data and route-update packets sent by mobile hosts. Therefore, mobile hosts have mappings in paging caches but not routing caches. Paging occurs when a packet is addressed to an idle mobile host and the gateway or the base station find no valid routing cache mapping for the destination. If the destination has no paging cache, it will forward the packet to all its interfaces except for the one the packet came through. Paging cache is used to avoid broadcast search procedures found in cellular

systems. Base stations that have paging cache will only forward the paging packet if the destination has a valid paging cache mappings and only to the mapped interface. Without any paging cache the first packet addressed to an idle mobile host is broadcast in the access network. While the packet does not experience extra delay it does, however, load the access network. Using paging caches the operator can restrict the paging load in exchange for memory and processing cost. Idle mobile hosts that receive a packet move from idle to active state. [1,2]

8.0 Features

Cellular IP inherits cellular systems principles for mobility management, passive connectivity and handoff control, its design is based on IP paradigm. The universal component of a cellular IP network is the Base Station which serves as a wireless access point, but, at the same time routes IP packets and integrates cellular control functionality traditionally found in Mobile Switching Centres(MSC) and – base Station Controllers (BSC).The Base stations are built on regular IP forwarding engines, but, IP routing is replaced by Cellular IP routing and location management. The Cellular IP Network is connected to the Internet via a gateway router. Mobility between gateways (i.e. cellular IP networks) is managed by Mobile IP, however, mobility within access networks is handled by Cellular IP.

Mobile hosts attached to the network use the IP address of the gateway as their Mobile IP care-of-address. Figure 2 illustrates the path of the packets addressed to a mobile host. The packets will be first routed to the host's home agent and then tunnelled to the gateway. The gateway detunnels the packets and forwards them towards Base Stations. Inside the cellular Mobile IP the hosts are identified by their home addresses and data packets are routed without tunneling or address conversion. Cellular routing IP protocol ensures that packets are delivered to the host's actual location. Packets transmitted by mobile host's are first routed to the gateway and then from there on to the Internet.

In cellular IP, location management and handoffs support are integrated with routing. To minimise control messaging regular data packets transmitted by mobile hosts are used to establish host location information. Uplink packets are routed from mobile to the gateway on a hop-by-hop basis. The taken path is cached in base stations. When the mobile host has no data to send ,it then transmits empty IP packets to the gateway to maintain its downlink state. Those hosts, who have not received packets for a certain period of time allow their downlink soft-state routes timeout and be cleared from the routing cache. To route packets to the idle hosts paging is used.

9.0 Wide area Mobility

Wide area mobility occurs when the mobile host moves between Cellular IP networks. The mobile host can identify Cellular IP networks by the Cellular IP network identifier contained in the Base Station's beacon signals. The beacon signal also contains the IP address of the gateway. For security and charging purposes, authentication and other user-related information may need to be provided by the mobile host, when it first contacts the Cellular IP network. This information will be inserted in the payload of the first paging-update packet and may be repeated in a few following paging-update packet for reliability. Upon receiving the first paging-update packet, the Gateway performs admission control that may involve technical and charging decisions. The Gateway's response is sent to the mobile host in regular IP packet(s).

If the request was accepted, the response may also carry the required setting of protocol parameters. Once authentication is accomplished, the mobile host can send a Mobile IP registration message to its home agent, specifying the Gateway's IP address as a care of address. Alternatively, the gateway can register at the Home Agent on behalf of the mobile host.

The Mobile host may leave the service area at any time without prior notice. Mappings associated to the host will be cleared after the time out. Alternatively, as a performance optimisation the host may send a paging-teardown packet to clear the Cache Mappings from both Route and Paging Caches.

9.0 Security

Cellular IP control Packets (paging-update, route-update and paging teardown packets) carry mandatory authentication information. This prevents malicious mobile hosts from changing location information related to other mobile hosts using a spoofed source address.

Each cellular IP network has a key of arbitrary length known to all Cellular IP nodes. The network key is kept secret from mobile hosts and other nodes outside the Cellular IP Network. Upon initial registration the Gateway must authenticate and possibly authorise the mobile host. This initial authentication and authorisation can be based on any known symmetric or asymmetric method. After authentication the gateway concatenates the key of the network and the IP address of the mobile host and calculates the PID of the mobile host. Then it acquires the public key of the mobile host from a trusted party, encrypts the PID and sends it to the mobile host. This way the mobile host and the cellular IP network have a shared secret.

The PID remains the same during handoff and can be easily computed by each Base Station. The PID can be used to authenticate IP packets over the air interface. Authentication is performed by creating

a short hash from the PID, timestamp, Packet content that is placed into the transmitted packets. The validity of packets can be checked at the base stations after a handoff.
PID could also be used to provide security for Data packets transmitted over the wireless link. [1,2]

Conclusion

Cellular IP is a protocol that provides mobility and handoff support for frequently moving hosts. Cellular IP can interwork with mobile IP to support wide area mobility, that is, mobility between cellular IP networks.

References

1
http://comet.ctr.columbia.edu/cellularip/overview.html
2.
http://www.comet.columbia.edu/cellularip/draft-valko-cellularip-01.tex.txt