INTERNET-DRAFT
<draft-valko-cellularip-01.txt>
Expires Apr. 2000

A. Campbell
J. Gomez
C-Y. Wan
Columbia University
Z. Turanyi
A. Valko
Ericsson

October 1999

Cellular IP

Status of this Memo

Abstract

This document specifies a protocol that allows routing IP datagrams to a mobile host. The protocol is intended to provide local mobility and handoff support. It can interwork with Mobile IP [1] to provide wide area mobility support. Four fundamental design principles of the protocol are: (1) location information is stored in distributed data bases (2) location information referring to a mobile host is created and updated by regular IP datagrams originated by the said mobile host (3) location information is stored as soft state (4) location management for idle mobile hosts is separated from location management of hosts that are actively transmitting or receiving data.

Table of Contents

0. What's Changed

The following major improvements have been made to the protocol since the previous version of this document:

- Security support for Cellular IP has been added.
- Paging Areas have been introduced. As long as an idle mobile host is moving inside a Paging Area, it is not necessary to transmit any

control packets.
- Semi-soft handoff has been introduced to improve handoff performance.
- Each node maintains only one valid Route Cache mapping and only one valid Paging Cache mapping for each mobile host. There is an exception to this in the case of semisoft handoff.

In addition, the following minor changes have been made:

- Cache mappings can not be created or modified (but still can be refreshed) by data packets.
- Paging-update packets remove Route Cache entries.
- An optional paging-teardown packet has been introduced that explicitly removes Paging Cache mappings.
- The Base Station's beacon signal has been extended to include Paging Area ID.
- The example algorithm in Appendix A. has been extended to distribute Network ID, Gateway IP address and Paging Area IDs.
- Control packet format has been changed to ICMP.
- Control packets must contain timestamp and authentication information.
- Cache mappings now contain timestamp information of the update packet that created the mapping.
- Cache mappings also contain the MAC address of the downlink Cellular IP node to allow multiple Cellular IP nodes to reside a shared medium. The notion of Uplink and Downlink I/Fs has been replaced by Uplink and Downlink neighbors.

1. Introduction

Hosts connecting to the Internet via wireless interface are likely to change their point of access frequently. A mechanism is required that ensures that packets addressed to moving hosts are successfully delivered with high probability. A change of access point during active data transmission or reception is called a handoff. During or immediately after a handoff, packet losses may occur due to delayed propagation of new location information. These losses should be minimized in order to avoid a degradation of service quality as handoffs become more frequent.

This memo specifies Cellular IP, a protocol that provides mobility and handoff support for frequently moving hosts. It is intended to be used on a local level, for instance in a campus or metropolitan area network. Cellular IP can interwork with Mobile IP [1] to support wide area mobility, that is, mobility between Cellular IP Networks.

1.1. Applicability

Cellular IP is applicable to networks ranging in size from LANs to metropolitan area networks. To provide global mobility support, Mobile IP [1] should be used above Cellular IP.

Cellular IP is designed to support frequently migrating, rarely moving or static hosts as well.

Cellular IP assumes that a random access L2 protocol covers the air interface.

1.2. New Architectural Entities

Cellular IP Node
A Cellular IP Network consists of interconnected Cellular IP nodes. The role of nodes is twofold. They route IP packets inside the Cellular IP Network and communicate with mobile hosts via wireless interface. Referring to the latter role, a Cellular IP node that has a wireless interface is also called a Base Station.

Cellular IP Base Station
See Cellular IP node.

Cellular IP Gateway
A Cellular IP node that is connected to a regular IP network by at least one of its interfaces.

Cellular IP Mobile Host
A mobile host that implements the Cellular IP protocol.

1.3. Terminology

Active Mobile Host
A mobile host is in active state if it is transmitting or receiving IP packets. (Exact definition is given in section 3.8.)

Active-state-timeout
The time a Cellular IP mobile host remains in active state without receiving IP packets.

Cellular IP Network Identifier
A unique identifier assigned to Cellular IP Networks.

Control packet
Paging-update, paging-teardown and route-update packet.

Data packet
An IP packet that is not a control packet.

Downlink
Directed to a mobile host.

Downlink neighbor
All neighbors of a Cellular IP node except its Uplink neighbor are referred to as Downlink neighbors.

Idle Mobile Host
A mobile host is in idle state if it has not recently

transmitted or received IP packets. (Exact definition is given in section 3.8.)

Internet
A Cellular IP Network provides access to a regular IP network.

This IP network in this memo is referred to as "Internet", but it can also be a corporate intranet, for example.

Neighbor
One Cellular IP node is said to be the neighbor of another if they are connected directly. Neighbors are identified in a Cellular IP node by interface and MAC address.

Paging Area
A set of Base Stations. Idle mobile hosts moving within a Paging Area do not need to transmit control packets to update their position. (Exact definition is given in section 2.1.)

Paging Cache
A cache maintained by some Cellular IP nodes, used to route packets to mobile hosts.

Paging-timeout
Validity time of mappings in Paging Caches.

Paging-update packet
A control packet transmitted by Cellular IP mobile hosts in order to update Paging Cache.

Paging-update-time
Time between consecutive paging-update packets.

Paging-teardown packet
A control packet transmitted by Cellular IP mobile hosts in order to explicitly disconnect from the Cellular IP Network.

Route-timeout
Validity time of mappings in Route Cache.

Route-update packet
A control packet transmitted by Cellular IP mobile hosts in order to update Route Cache.

Route-update-time
Time between consecutive route-update packets.

Route Cache
A cache maintained by all Cellular IP nodes, used to route packets to mobile hosts.

Update packet
Paging-update and route-update packet.

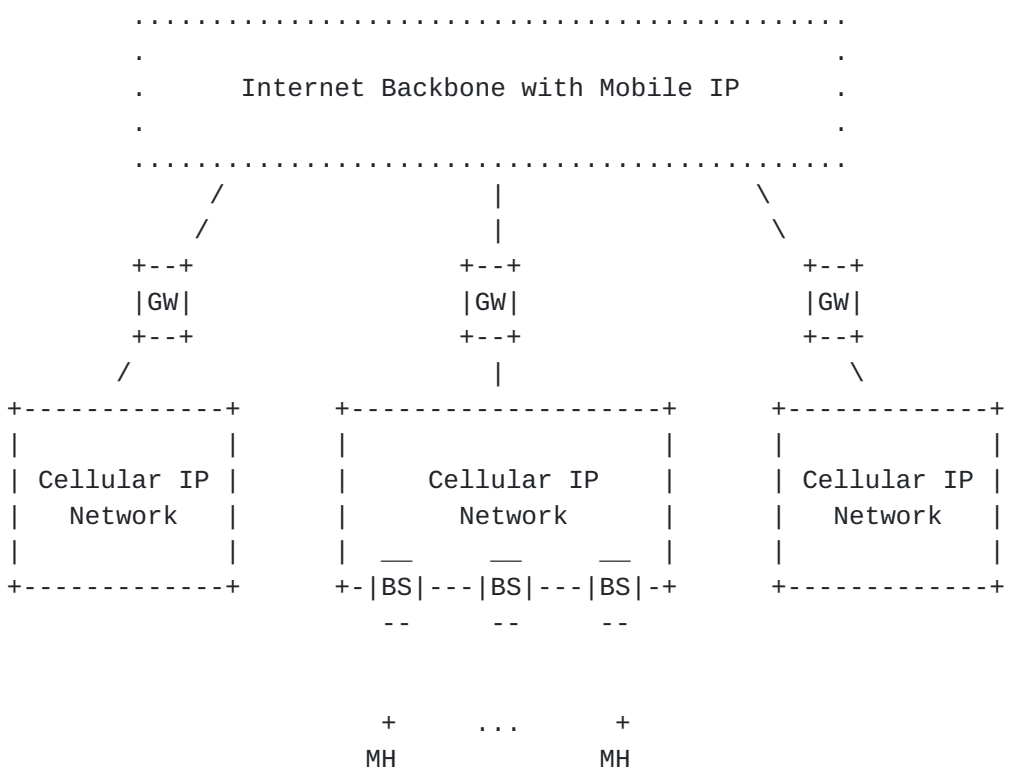
Uplink

Originated by a mobile host.

Uplink neighbor
The neighbor of a Cellular IP node which is the next hop on the shortest path towards the Gateway.

1.4. Protocol Overview

The figure shown below presents a schematic view of multiple Cellular IP Networks providing access to the Internet.



In what follows, we present an overview of the operation of Cellular IP, followed by a figure illustrating the functional entities that comprise Cellular IP.

Base Stations periodically emit beacon signals. Mobile hosts use these beacon signals to locate the nearest Base Station. 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 neighbor from which the packet arrived to the node.

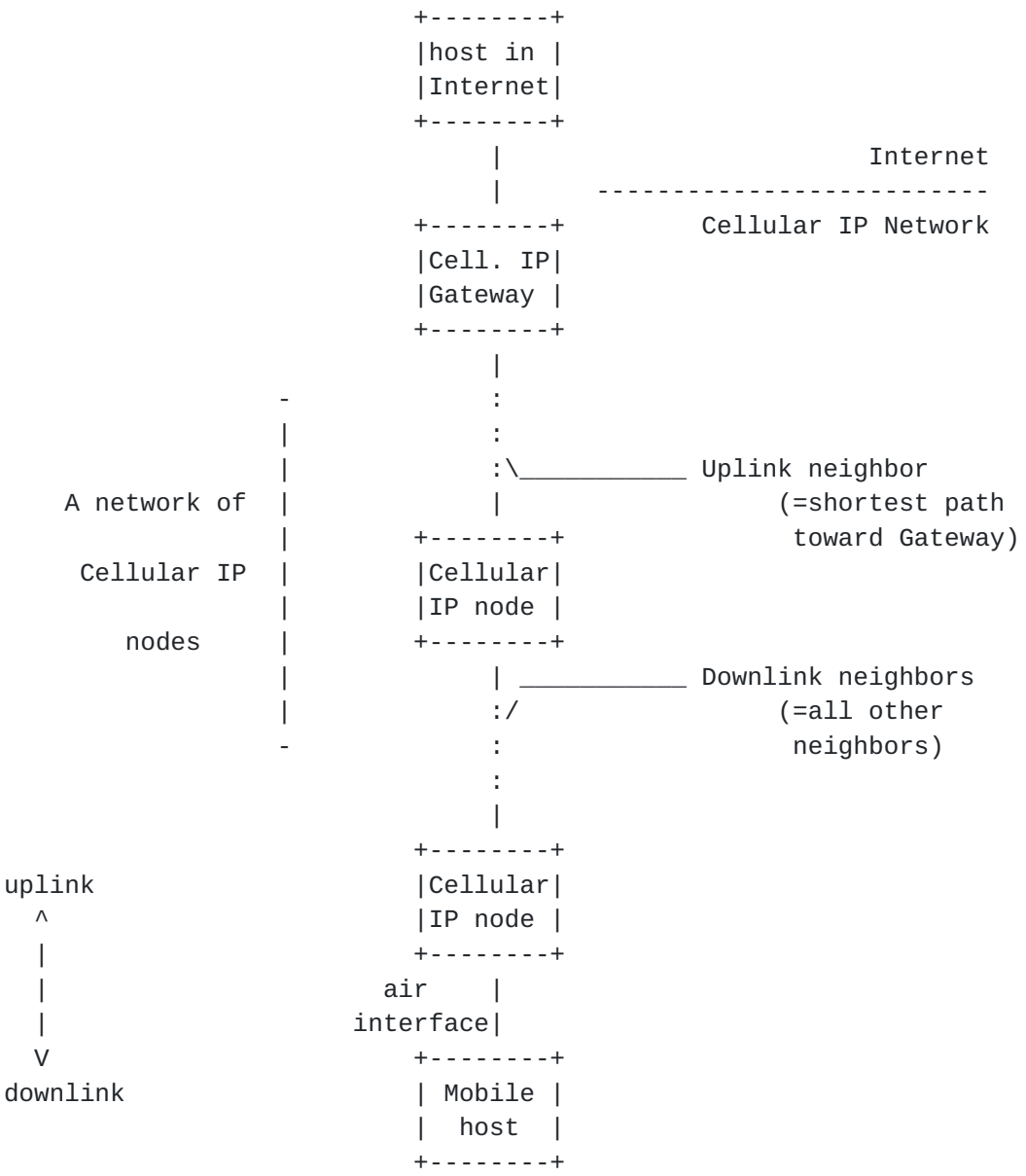
The chain of cached mappings referring to a single mobile host constitutes a reverse path for downlink packets addressed to the same mobile host. As the mobile host migrates, the chain always points to

its current location because its uplink packets create new and change old mappings.

IP packets addressed to a mobile host are routed by the chain of cached mappings referring to the said mobile host.

To prevent its mappings from timing out, a mobile host can periodically transmit control packets. Control packets are ICMP 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 timeout value than Route Caches and are not necessarily maintained in every node.



1.5. Location Management and Routing

Cellular IP uses two parallel cache systems to store the information related to the location of mobile hosts. The two systems basically operate in the same way. This section is intended to clarify why we use two distinct caches.

When a mobile host is in active state, the network must follow its

movement from Base Station to Base Station to be able to deliver packets without searching for the mobile host. As a consequence active mobile hosts must notify the network about each handoff. For idle mobile hosts exact location tracking is less important, instead mimizing communication to save battery is of higher priority. By deploying two caches, the granularity of location tracking can be different for idle and active mobile hosts.

Separating the location tracking for idle and active mobile hosts also has a performance benefit. Supposing there is just one set of cache, for each downlink packet the entire cache must be searched to find the destination mobile host. It is expected, however, that only a portion of the hosts will be in active state at any given time and that most of the packets are destined for active mobile hosts. Thus by separating the caches for active and idle mobile hosts only a smaller cache needs to be searched for most of the packets. This results in faster lookups and better scalability.

2. Cellular IP Functions

2.1. Location Management

Cellular IP allows idle mobile hosts to roam large geographic areas without the need to transmit location update packets at cell borders. The network operator can group the cells into Paging Areas, each comprising an arbitrary number of (typically adjacent) cells. Each Paging Area has an identifier that is unique in the given Cellular IP Network. Each Base Station transmits its Paging Area Identifier in its periodic beacon signals, thus enabling mobile hosts to notice when they move into a new Paging Area.

An idle mobile host that moves into a new Paging Area must transmit a paging-update packet. Paging-update packets are routed from the Base Station to the Gateway using hop-by-hop routing. Selected nodes of the Cellular IP network are equipped with Paging Cache. These nodes monitor passing paging-update packets and update Paging Cache mappings to point toward the new Paging Area. Paging-update packets reach the Gateway and are discarded there to isolate Cellular IP specific operations from the Internet.

When the mobile host moves within a Paging Area, it transmits a paging-update packet only when the system specific time, paging-update-time expires. Outdated mappings of Paging Caches are cleared if no update arrives before paging-timeout expires.

When an IP packet arrives at a Cellular IP node, addressed to a mobile host for which no up-to-date Route Cache mapping is available, the Paging Cache is used to route the packet. This is called

"implicit paging". If the node has no Paging Cache, it forwards the packet to all Downlink neighbors. A node that has Paging Cache but has no mapping in it for the destination mobile host discards the packet.

On the path from the gateway to the mobile host there may be Cellular

IP nodes with and without Paging Cache mixed. After the paging packet leaves the last node which has a Paging Cache it is effectively broadcast downlink by all nodes it passes. The set of cells that are reached by the paging packet forms a Paging Area. The number, size and population of Paging Areas in a Cellular IP network are determined by the topology of the network and the placement of Paging Caches. If a Base Station has a Paging Cache itself then it is alone in its Paging Area. If there are no Paging Caches in a Cellular IP Network, then the whole network is one Paging Area and paging becomes broadcasting.

When the mobile host receives the paging packet, it moves to active state and creates its Route Cache mappings by sending a route-update packet. Further IP packets addressed to the same host will be routed by Route Caches as long as the mobile host keeps the Route Caches updated.

2.2. 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 neighbors of the Cellular IP node. Packets 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 two, we summarize the operation of Paging Caches and Route Caches in the following table. For the reasons of separating the two functions, see section 1.7.

	Paging Caches	Route Caches
refreshed by	all uplink packets (data, paging-update, route-update)	data and route-update packets
updated by	all update packets (paging-update, route-update)	route-update packets
updated when	moving to a new Paging Area, or after paging-update-time	moving to a new cell, or after route-update-time
scope	both idle and active MHs	active mobile hosts
purpose	route downlink packets if	route downlink

The mobile host may keep receiving data packets without sending data for possibly long durations. To keep its Route Cache mappings up to

date 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 borders. 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 update packets and refreshed by all upplink packets including data packets as well.

2.3. Handoff

Handoff is initiated by the mobile host. As an active host approaches a new Base Station, it transmits a route-update packet and redirects its packets from the old to the new Base Station. The route-update packet will configure Route Caches along the way from the new Base Station to the Gateway. (The paths leading to the old and new Base Stations may overlap. In nodes where the two paths coincide, the route-update packet simply refreshes the old mapping and the handoff remains unnoticed.)

An idle mobile host, moving to a new Base Station, transmits a paging-update packet only if the new Base Station is in a new Paging Area. During handoffs between Base Stations within the same Paging Area idle mobile hosts may remain silent, as paging is performed within the entire Paging Area.

2.4. 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 Stations' 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 a 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 packets 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. After successful authentication to the Cellular IP network the mobile host can send a Mobile IP registration message to its home agent, specifying the Gateway's IP address as 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 timeout. Alternatively, as a performance optimization the host may send a paging-teardown packet to clear Cache mappings from both Route and Paging Caches.

2.5. 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. The details of the authentication mechanism can be found in section 3.5.

Data security issues are not discussed in this document. We note that any further authentication or encryption can be performed in addition to control packet authentication built into Cellular IP.

3. Protocol Details

3.1. Protocol Parameters

The following parameters shall be set by network management. The values listed here are for information only. Note that most of the time an active mobile host will transmit data packets and route-update packets will need to be sent less frequently than 1 in every second.

Name	Meaning	Typical Value
route-update-time	Maximal inter-arrival time of packets updating the Route Cache	1 sec
route-timeout	Validity of Route Cache mappings	3 sec
paging-update-time	Maximal inter-arrival time of packets updating the Paging Cache	1 min
paging-timeout	Validity of Paging Cache mappings	3 min
active-state-timeout	Time the mobile host	5 sec

remains in active state
without receiving data

3.2. Beacon Signal Structure

Cellular IP Base Stations must periodically transmit beacon signals to allow for mobile hosts to identify an available Base Station. Information elements carried by the beacon signal are:

- Layer2 parameters related to the Base Station;
- the Cellular IP Network Identifier;
- the IP address of the Gateway;
- the ID of the Paging Area.

All parameters can be configured by network management. As an alternative, in Appendix A we present an example algorithm for automatically distributing the Cellular IP Network Identifier, the IP address of the Gateway and the Paging Area IDs to Base Stations.

3.3. Packet Formats

3.3.1. Data packet

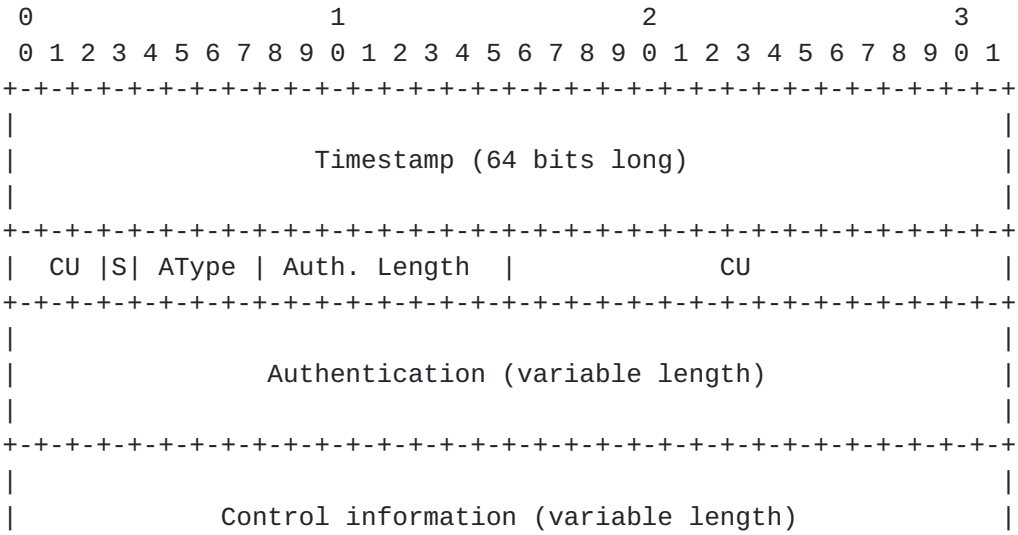
Cellular IP forwards regular IP packets without modification, segmentation, encapsulation or tunneling.

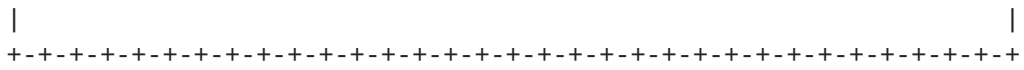
3.3.2. Route-update packet

A route-update packet is an ICMP packet of which

- the source address is the IP address of the sending mobile host;
- the destination address is the Gateway; and
- the type is Cellular IP Control Packet and the code is Route-update.

The payload of the route-update packet carries authentication and control information in the following format:





Timestamp Contains a timestamp used to determine the order in which update packets are sent. The timestamp

field is formatted as specified by the Network Time Protocol [2]. The low-order 32 bits of the NTP format represent fractional seconds, and those bits which are not available from a time source should be generated from a good source of randomness. Mobile hosts must ensure that the 64 bit value of timestamps is strictly increasing in consecutive control packets.

CU — Currently Unused. Must be set to 0.

S flag — Set to 1 to indicate semi-soft handoff. Default value is 0. Any Cellular IP node that does not support semi-soft handoffs may ignore this bit. (See section 4.1.)

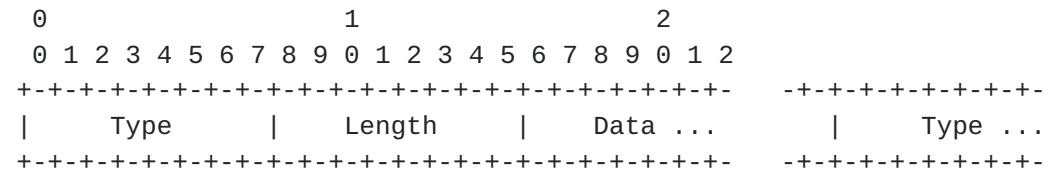
AType — Denotes the authentication method used. The default authentication method is described in [4]. All authentication methods must utilize the timestamp field.

Auth. Length — Denotes the length of the authentication information in bytes.

Authentication — Contains the authentication information.

Alternatively the Authentication Header [3] could also be used for authenticating control packets. This issue is for further study.

Control information is encoded in the following Type-Length-Value format:



Type — Indicates the particular type of control information.

Length — Indicates the length (in bytes) of the following data field within. The length does not include the Type and Length bytes.

Data — This field may be zero or more bytes in length. The meaning, format and length of the data field is determined by the Type and Length fields.

Currently the following type of control information is defined

(details are for further study):

Registration request
Used when a mobile host enters the Cellular IP Network.

3.3.3. Paging-update packet

A paging-update packet is an ICMP packet of which

- the source address is the IP address of the sending mobile host;
- the destination address is the Gateway; and
- the type is Cellular IP Control Packet and the code is Paging-update.

The payload of the paging-update packet carries authentication and control information in the same format as the route-update packet. The S flag must be 0 for paging-update packets.

3.3.4. Paging-teardown packet

A paging-teardown packet is a ICMP packet of which

- the source address is the IP address of the sending mobile host;
- the destination address is the Gateway; and
- the type is Cellular IP Control Packet and the code is Paging-teardown.

The payload of the paging-teardown packet carries authentication and control information in the same format as the route-update packet. The S flag must be 0 for paging-teardown packets.

3.4. Addressing

Cellular IP requires no address space allocation beyond what is present in IP. Mobile hosts are identified by their home IP addresses.

3.5. Security

Each Cellular IP Network has a secret network 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, however. Upon initial registration the Gateway must authenticate and possibly authorize the mobile host. This initial authentication and authorization 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 by an MD5 Hash similarly as in [4]:

PID := MD5(network key, IP address of MH)

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 (and optionally to encrypt) IP packets over the air interface. Authentication is performed by creating a short hash from the (PID, timestamp, packet content) triple that is placed into the transmitted packets. The validity of

each packet can be easily checked by any Base Station even immediately after a handoff and without prior communication with the mobile host or with the old Base Station.

In addition to authenticating control packets, PID can optionally also be used to provide security for data packets transmitted over the wireless link. To this avail, any known shared secret based security mechanism can be used where PID serve as the shared secret.

3.6. Cellular IP Routing

Cellular IP nodes need only to implement the algorithm described in this section. They do not need regular IP routing capability. This section describes the routing algorithm in Cellular IP nodes other than the Gateway. The extra functions required only in the Cellular IP Gateway are described in section 3.7.

3.6.1 Topology

In uplink direction (toward the Gateway), packets are routed in the Cellular IP Network on a hop-by-hop basis. The neighbor to which a node will forward a packet toward the Gateway is referred to as the node's Uplink neighbor. The Uplink neighbor at each node may be designated by network management. Alternatively, a simplified shortest path algorithm can select Uplink neighbors instead of manual configuration. (A regular shortest path algorithm is also applicable but is more complex than required since it determines routes to all nodes in the network.) A simple algorithm that configures Uplink neighbors and automatically reconfigures them if necessary after a topology change is described in Appendix A.

A node's neighbors other than the Uplink neighbor are called Downlink neighbors.

3.6.2 Uplink Routing

A packet arriving to the node from one of the Downlink neighbors is assumed to be coming from a mobile host. The packet is first used to update the node's Route and Paging Caches and is then forwarded to the node's Uplink neighbor.

To update the Caches, the node reads the packet type, port number and the source IP address. Paging-update packets update the Paging Cache only. Route-update packets update both Route and Paging Caches. Data packets only refresh the soft state of both caches, but do not change it. Both types of caches consist of

{ IP-address, interface, MAC address, expiration time, timestamp }

5-tuples, called mappings. The IP address is the address of the mobile host the mapping corresponds to. The interface and the MAC address denote the Downlink neighbor toward the mobile host. The timestamp field contains the timestamp of the control packet that has

established the mapping.

When a data packet arrives from a Downlink neighbor, the Route Cache entry of the source IP address is searched first. If the data packet is coming from the same neighbor as indicated by the cache entry then it is sent from the direction where the mobile host was last seen. In that case the mapping is only refreshed: the expiration time is set to the current time + route-timeout. If the node has Paging Cache, then the expiration time of the mapping in the Paging Cache is set to current time + paging-timeout as well. Then the packet is forwarded uplink.

If the data packet arrived from a different neighbor than that is in its mapping or no mapping exists for the IP address, then the packet is dropped.

When an update packet arrives from a Downlink neighbor then the authentication is validated first. Packets with invalid authentication must be dropped and the event should be logged as a potential tampering attempt. For valid packets the node creates the following 5-tuple:

```
{ the newly arrived packet's source IP address,
  the interface through which it arrived,
  the source MAC address of the arrived packet,
  current time + route-timeout,
  the timestamp in the arrived update packet }
```

This mapping is used to update Route Cache, if the incoming packet is a route-update packet. If a valid mapping for the source IP address already exists, then it is replaced by the new 5-tuple, if the timestamp is newer, otherwise the packet is dropped. If no mapping exists for the source IP address then the mapping is added to the Route Cache. The Paging Cache is updated in the same way, but using paging-timeout instead of route-timeout. If the node has no Paging Cache then only the Route Cache is updated. If the incoming packet is a paging-update, then only the Paging Cache is updated (if any).

If the packet is a paging-teardown packet and the authentication information is valid, then mappings of the mobile host with timestamp earlier than the timestamp of the packet are removed from both the Route and the Paging Cache.

After cache modifications the control packet is forwarded to the Uplink neighbor.

3.6.3 Downlink Routing

A packet arriving to a Cellular IP node from the Uplink neighbor is

assumed to be addressed to a mobile host. The node first checks if the destination IP address has a valid mapping in the Route Cache. If such a mapping exists, the packet is forwarded to the Downlink neighbor found in the mapping.

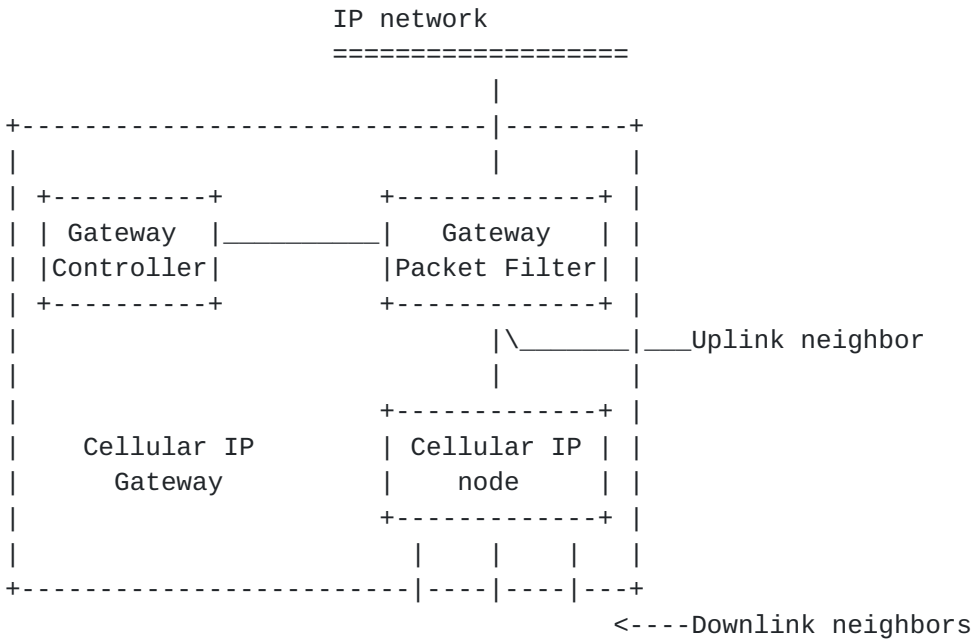
If the Route Cache contains no mapping for the destination IP address and the node has no Paging Cache, then the packet is broadcast on all interfaces of the node except the interface of the Uplink neighbor.

If the node has Paging Cache and there is a mapping for the destination IP address, then the packet is forwarded to the neighbor found in that mapping.

If the node has Paging Cache, but there is no mapping for the destination IP address, then the packet is dropped.

3.7. Cellular IP Gateway

The following figure is a schematic view of a Cellular IP Gateway. The Gateway can logically be divided into three building blocks: a regular Cellular IP node, a Gateway Packet Filter and a Gateway Controller.



Uplink packets update the Route and/or Paging Caches in the Cellular IP node block and are forwarded towards the Gateway filter. The Gateway filter reads the destination IP address. If this is the Gateway's address, the packet is forwarded to the Gateway controller. Most of these packets are control packets with empty control information field and are immediately dropped. If the packet carries control information, for instance a registration request, it is interpreted and processed by the Gateway controller.

If the destination address is not the Gateway's, the packet is forwarded to the Internet. (This means that a packet sent from a

mobile host to another mobile host in the same Cellular IP Network goes through the destination Home Agent. However, this is not the case if route optimization is used. To operate efficiently even without Mobile IP route optimization, the Gateway Packet Filter can also check if the destination address of an uplink packet has a valid mapping in any of the Gateway's caches. If a mapping is found, the

packet is "turned back" and is treated as a downlink packet.)

Packets arriving from the Internet (using Mobile IP) to mobile hosts in the Cellular IP Network are decapsulated and forwarded to the Cellular IP node block. Arriving packets not using Mobile IP are assumed to be sent to mobile hosts of which this Cellular IP Network is the home network. If no foregin registration shows that the mobile host is away, these packets are forwarded to the Cellular IP node block unchanged.

The Gateway's Cellular IP node block treats these packets as determined by the Cellular IP Routing algorithm (section 3.5) according to the mappings in Route and Paging Cache. Though in Cellular IP nodes it is optional to have Paging Cache, it is recommended that the Gateway's Cellular IP node have one. This esnures that packets addressed to hosts currently not connected to the Cellular IP Network do not enter the network and do not load it in vain but are immediately discarded in the Gateway when neither Route, nor Paging Cache mapping is found for the destination address. (It may be advantageous to also generate an ICMP message in this case and send it back to the packet's source address.)

3.8. Cellular IP Mobile Host

While connected to a Cellular IP Network, a mobile host must be in one of two states: 'active' or 'idle'. The host moves from idle to active state when it receives or wishes to send any IP packet. If it does not receive or send more IP packets, it remains in active state for a time equal to active-state-timeout. Any IP packet received in active state restarts the active state timer. When the timer elapses, the host returns to idle state.

When the host moves from idle to active state, it must transmit a route-update packet. At the same time, a timer is initiated from a value equal to route-update-time. If the timer expires without any data packet being transmitted from the host, again a route-update packet is transmitted and the timer is re-initiated. Any IP packet transmitted before the timer expires, resets the timer to route-update-time. This ensures that while the mobile host is in active state, the largest interval between two transmitted packets is never longer than route-update-time. The mechanism also ensures that if data packets are transmitted with sufficient frequency, no route-update packets will be generated, which will probably be typical.

If the host is in active state, it must immediately transmit a route-update packet whenever it connects to a new base station. This typically happens at migration, but is also the case after a wireless channel black-out or when the host enters the Cellular IP Network. A

packet transmitted this way also resets the route-update packet timer.

In idle state, the mobile host must transmit paging-update packets periodically, at intervals of paging-update-time. Similarly to the route-update packet timer, the paging-update timer is reset if a data

packet is transmitted.

If the host is in idle state, it must send a paging-update packet when it connects to a new Base Station with different Paging Area ID form the previous. When connecting a new Base Station whose Paging Area ID is equal to the Paging Area ID of the previous Base Station, the mobile host may remain silent.

The mobile host must ensure that the 64 bit value of timestamps is strictly increasing in consecutive control packets.

4. Extensions to Cellular IP

4.1. Semi-soft Handoff

When a mobile host switches to a new Base Station it sends a route-update packet to make the chain of cache bindings to point to the new Base Station. Packets that are traveling on the old path will be delivered to the old Base Station and will be lost. Although this loss may be small it can potentially degrade TCP throughput. This kind of handoff, when the mobile switches all at once to the new Base Station is called "hard" handoff. For performance details of hard handoff in a Cellular IP network see [5].

To improve the performance of loss sensitive applications, another type of handoff may be introduced, called "semi-soft" handoff. During semi-soft handoff a mobile host may be in contact with either of the old and new Base Stations and receive packets from them. Packets intended to the mobile host are sent to both Base Stations, so when the mobile host eventually moves to the new location it can continue to receive packets without interruption.

To initiate semi-soft handoff, the moving mobile host transmits a route-update packet to the new Base Station and continues to listen to the old one. The S flag is set in this route-update packet to indicate semi-soft handoff. Semi-soft route-update packets create new mappings in the Route and Paging Cache similarly to regular route-update packets. When the semi-soft route-update packet reaches the cross-over node where the old and new path meet (note that the cross-over node already has a mapping for the mobile host), the new mapping is added to the cache instead of replacing the old one. Packets sent to the mobile host are transmitted to both Downlink neighbors. When the mobile host eventually makes the move then the packets will already be underway to the new Base Station and the handoff can be performed with minimal packet loss. After migration the mobile host sends a route-update packet to the new Base Station with the S bit cleared. This route-update packet will remove all mappings in Route Cache except for the ones pointing to the new Base

Station. The semi-soft handoff is then complete.

If the path to the new Base Station is longer than to the old Base Station or it takes non negligible time to switch to the new Base Station, then some packets may not reach the mobile host. To overcome the problem, packets sent to the new Base Station can be

delayed during the semi-soft handoff. This way a few packets may be delivered twice to the mobile host, but in many cases this results in better performance than a few packets lost. Introduction of packet delay can be best performed in the Cellular IP node that has multiple mappings for the mobile host as a result of a semi-soft route-update packet. Packets that belong to flows that require low delay but can tolerate occasional losses should not be delayed. For performance details of semi-soft handoff in a Cellular IP network see [5].

4.2. Multiple Gateway Networks

Cellular IP requires that a mobile host be using exactly one Gateway at a time. This requirement comes from the fact that the Gateway serves as the mobile host's Foreign Agent and it relays its packets both up and downlink. It is also required to make uplink routing unambiguous. The Cellular IP Network can have multiple Gateways as long as a single host still uses just one Gateway at any time. (The host can change Gateway, involving a Mobile IP location updating.) In a Network with multiple Gateways, nodes must be able to determine which Gateway a given mobile host is using. Assignment of Gateways can, for instance, be based on geographical partitioning of the network, or on partitioning the mobile hosts' address space. This issue is for further study.

4.3. Charging

Cellular IP Network providers can charge Cellular IP Mobile users for connectivity or for transmitted data or both. Charging information is best collected in the Gateway. The Gateway receives all control packets and can determine the time a mobile host was connected to the network. It can also measure through traffic in both directions.

5. Security Considerations

A Cellular IP Network is a single administrative domain. It is connected to the Internet through a Gateway that may eventually also serve as a firewall. Hence security issues only need to be considered at the wireless interface.

The security of a Cellular IP system will be determined by the wireless link. Security issues relating to wireless links are not specific to Cellular IP, and are out of the scope of Cellular IP, even though they must be dealt with in practical Cellular IP implementations.

A security problem specific to Cellular IP is the security of the control packets, which can be solved by the authentication mechanism described in section 3.5.

6. Intellectual Property Right Notice

This is to affirm that Telefonaktiebolaget LM Ericsson and its subsidiaries, in accordance with corporate policy, will offer patent licensing for submissions rightfully made by its employees which are

adopted or recommended as a standard by your organization as follows:

If part(s) of a submission by Ericsson employees is (are) included in a standard and Ericsson has patents and/or patent application(s) that are essential to implementation of such included part(s) in said standard, Ericsson is prepared to grant - on the basis of reciprocity (grantback) - a license on such included part(s) on reasonable, non-discriminatory terms and conditions.

Ericsson has filed patent applications that might possibly become essential to the implementation of this contribution.

References

[1] "IP Mobility Support," C. Perkins, ed., IETF RFC 2002, October 1996.

[2] "Network Time Protocol (Version 3): Specification, Implementation and Analysis," D. Mills, IETF RFC 1305, March 1992.

[3] "IP Authentication Header," R. Atkinson, IETF RFC 1826, August 1995.

[4] "IP Authentication using Keyed MD5," P. Metzger, W. Simpson, IETF RFC 1828, August 1995.

[5] "Cellular IP Performance," J. Gomez, A. T. Cambell, S. Kim, Z. Turanyi, A. Valko, C-Y Wan, Work in Progress, <draft-gomez-cellularip-performance-00>, October 1999.

Authors' Addresses

Andrew T. Campbell, Javier Gomez, Chieh-Yih Wan
Department of Electrical Engineering, Columbia University
Rm. 801 Schapiro Research Building
530 W. 120th Street, New York, N.Y. 10027
phone: (212) 854 3109
fax : (212) 316 9068
email: {campbell,javierg,wan}@comet.columbia.edu

Zoltan R. Turanyi, Andras G. Valko
Ericsson Traffic Analysis and Network Performance Laboratory
H-1300 Bp.3.P.O.Box 197, Hungary
phone: +36 1 437 7774
fax : +36 1 437 7219
email: {zoltan.turanyi,andras.valko}@eth.ericsson.se

Appendix A. Uplink Neighbor Selection

This algorithm selects the Uplink neighbor of all nodes of a Cellular IP Network and reconfigures them if necessary after a change of topology. An Uplink neighbor is identified by the interface through which it is accessible from the node and its corresponding MAC address. The algorithm also distributes the Cellular IP Network

Identifier, the IP address of the Gateway and the Paging Area IDs to the Base Stations.

The Gateway periodically creates a control packet called a "Gateway broadcast packet". The Gateway broadcast packet contains

- the Cellular IP Network Identifier;
- the IP address of the Gateway;
- a sequence number increased each time by the Gateway; and
- a Paging Area ID field initially set to the ID of the Gateway.

The Gateway broadcasts the packet on all of its interfaces except those connected to the Internet. A Cellular IP node receiving a Gateway broadcast packet follows the steps below.

1) It drops the packet if the sequence number is lower or equal to the sequence number of one of the previously received Gateway broadcast packets. In this case no further processing is needed.
2) It stores the sequence number of the Gateway broadcast packet for later comparison.
3) It stores the Cellular IP Network Identifier and the IP address of the Gateway.
3) It stores the interface through which the packet arrived together with source MAC address of the packet (if any) to identify the Uplink neighbor. All other interface/MAC address combinations will dentote Downlink neighbors.
4) If the node has a Paging Cache, it overwrites the value of the Paging Area ID field in the packet by its own ID.
5) The value of the (possibly overwritten) Paging Area ID field is stored as the Paging Area ID of the node. This value will be used in beacon signals if the node is a Base Station.
6) It stores the Cellular IP Network Identifier and the IP address of the Gateway. These values will be used in beacon signals if the node is a Base Station.
7) After a short random delay, the node broadcasts the packet through all of its interfaces, except the air interface(s) and the interface of the Uplink neighbor.