Implementation of Cellular IP and Its Performance Analysis

Sujoy Halsana
Department:-M-Tech In C.S.E,W.B.U.T,Narula Institute Of Technology.

Abstract: *In the current Cellular IP architecture, only one gateway serves the entire CIP network. So, the gateway is single point of failure for all the mobile hosts who rely on it to be connected to the Internet. Cellular IP requires that a mobile host be using exactly one gateway to the Internet backbone with Mobile IP at a time. When multiply gateways are used in a cellular IP network, the optimal design for the multiple domains is needed. The cellular IP protocol provides better performance for hand-off than other protocol using micro-mobility. A set of base station cluster together on the same cellular IP network. This kind of domain base network is superior to mobile IP in support of routing optimization and QoS. Experiment were conduct to explore load our protocol and survey the packet loss. This result so that the load of control packet is negligible for cellular IP and the number of lost packet can be successfully reduced. This thesis developed to design cellular IP architecture and fault detection mechanism and recover the protocol of cellular IP.*

Keywords; *Protocol Overview, Network Model, Routing, Handoff, Paging, Security, Implement Cellular IP Network Model, Protocol Details,* Simulation Results, *Conclusions.*

I. Introduction

Recent initiative to add mobility to the Internet mostly focus on the issue of address translation [2] through the introduction of location directories and address translation agents .In these protocols (e.g., Mobile IP [1]), packets addressed to a mobile host are delivered using regular IP routing to a temporary address assigned to the mobile host at its actual point of attachment. This approach results in simple and scalable schemes that offer global mobility support. It is not appropriate, however, for fast mobility and smooth handoff because after each migration a local address must be obtained and communicated to a possibly distant location directory or home agent (HA). Cellular mobile telephony systems are founded on totally different concepts. Instead of aiming at global mobility support, cellular systems are optimized to provide fast and smooth handoff in a restricted geographical area. In the area of coverage mobile users have wireless access to the mobility unaware global telephony network. A scalable forwarding protocol interconnects distinct cellular networks to support roaming between them .Restricting the cellular coverage to a limited geographical area limits the potential number of connected users. This makes it feasible to maintain per mobile states which we believe is key to delivering fast handoff support to mobile hosts. Having per-mobile location information allows the cellular system to support location independent addressing avoiding the need to change addresses during each intra-network migration. Even in limited geographical areas, however, the number of users can grow to a point where using fast lookup techniques for per user data bases is no longer viable. In addition, mobility management requires mobile hosts to send registration information after migration. The resulting signaling overhead has significant impact on the performance of the wireless access network. To overcome this problem, cellular telephony systems require mobiles to register every migration only when they are engaged in "active" calls. In contrast, "idle" mobile hosts send registration messages less frequently and as a result can roam in large areas without loading the network and the mobility management system. The location of idle mobile hosts is only approximately known to the network at any one time. To establish a call to an idle mobile, the mobile host must be searched for in a limited set of cells. This feature called *passive connectivity* allows the cellular network to accommodate a very large number of users at any instance without overloading the network with large volumes of mobility management signaling information and messaging. Cellular networks offer a number of desirable features which if applied correctly could enhance the performance of future wireless IP networks without loosing any of important flexibility, scalability and robustness properties that characterize IP networks..In this paper, we present an analysis of *Cellular IP* [3] [4], a new mobile host protocol that is optimized to provide access to a Mobile IP enabled Internet in support of fast moving wireless hosts. Cellular IP incorporates a number of important cellular principles but remains firmly based on IP design principles. Because of its IP based design and the feature of passive connectivity, Cellular IP can scale from pico to metropolitan area installations. The Cellular IP distributed location management and routing algorithms loan themselves to a simple, efficient and low cost implementation for host mobility requiring no new packet formats, encapsulation or address space allocation beyond what is already present in IP.. In Section , I represent an overview of the Cellular IP protocol and design Cellular IP network using multiple gateway . I analyze the protocol which is implemented as extensions to the NS simulator. In particular i discuss the handoff performance and cost of mobility Management, location update cost, packet delivery cost.

Protocol Overview-

As the name suggests Cellular IP inherits cellular principles for mobility management such as passive connectivity, paging and fast handoff control but implements them around the IP paradigm. Cellular IP access networks require minimal configuration (e.g. similar to switched Ethernet LANs) thereby easing the deployment and management of wireless access networks. An important concept in Cellular IP design is simplicity and the minimal use of explicit signaling enabling low cost implementation of the protocol.

II. Network Model

The universal component of Cellular IP access networks is the base station which serves as a wireless access point and router of IP packets while performing all mobility related functions. Base stations are built on regular IP forwarding engine with the exception that IP routing is replaced by Cellular IP routing and location management. Cellular IP access networks are connected to the Internet via gateway routers. Mobile hosts attached to an access network use the IP address of the gateway as their Mobile IP care-of address. Figure 1 illustrates the path taken by packets addressed to a mobile host. Assuming Mobile IPv4 [5] and no route optimization [6], packets first will be routed to the host's home agent and then tunneled to the gateway. The gateway "detunnels" packets and forwards them toward a base station. Inside a Cellular IP network, mobile hosts are identified by their home address and data packets are routed without tunneling or address conversion. The Cellular IP routing protocol ensures that packets are delivered to the host's actual location. Packets transmitted by mobile hosts are first routed toward the gateway and from there on to the Internet. In Cellular IP, location management and handoff support are integrated with routing. To minimize control messaging, regular data packets transmitted by mobile hosts are used to refresh host location information. Uplink packets are routed from a mobile host to the gateway on a hop-by-hop basis. The path taken by these packets is cached by all intermediate base stations. To route downlink packets addressed to a mobile host the path used by recently transmitted packets from the mobile host is reversed. When the mobile host has no data to transmit then it sends small, special IP packets toward the gateway to maintain its downlink routing state. Paging is used to route packets to idle mobile hosts in a Cellular IP access network.

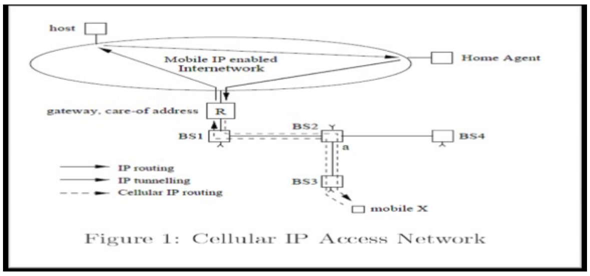

Figure 1: Cellular IP Access Network

III. Routing-

The Cellular IP gateway periodically broadcasts a beacon packet that is flooded in the access network. Base stations record the neighbor they last received this beacon from and use it to route packets toward the gateway. All packets transmitted by mobile hosts regardless of their destination address are routed toward the gateway using these routes .As these packets pass each node on route to the gateway their route information is recorded as follows. Each base station maintains a routing cache. In the situation illustrated in Figure 1 data packets are transmitted by a mobile host with source IP address X and reach base station BS2 via BS3. In the routing cache of BS2 this is indicated by a mapping (X,BS3). This soft-state mapping remains valid for a system specific time called route-timeout. Data packets are used to maintain and refresh mappings. As long as mobile host X is regularly sending data packets then base stations along the path between the mobile's actual point of attachment and the gateway will maintain valid routing cache mappings forming a soft-state path between the mobile host and gateway node. Packets addressed to the mobile host X are routed on a hop-by-hop basis using this established routing cache. A mobile host may sometimes wish to maintain its routing cache mappings even though it is not regularly transmitting data packets. A typical example of this is when a mobile host receives a UDP stream of packets on the downlink but has no data to transmit on the uplink. To keep its routing cache mappings valid mobile hosts transmit route-update packets on the uplink at regular intervals called route-update time. These packets are special ICMP packets addressed to the gateway. Route-update packets update routing cache mappings as is the case with normal data packets. However ,route-update messages do not leave the Cellular IP access network.

Handoff-

Cellular IP supports two types of handoff scheme. Cellular IP hard handoff is based on simple approach that trades off some packet loss in exchange for minimizing handoff signaling rather than trying to guarantee zero packet loss. Cellular IP semisoft handoff exploits the notion that some mobile hosts can simultaneously receive packets from the new and old base stations during handoff. Semisoft handoff minimizes packet loss providing improved TCP and UDP performance over hard handoff.

Hard Handoff-

Mobile hosts listen to beacons transmitted by base stations and initiate handoff based on signal strength measurements. To perform a handoff a mobile host tunes its radio to a new base station and sends a route-update packet. The route-update message creates routing cache mappings on route toward the gateway configuring the downlink route cache to point toward the new base station. Handoff latency is the time that elapses between handoff initiation and the arrival of the first packet along the new route. In the case of hard handoff this duration is equal to the round-trip time between the mobile host and the cross-over base station as illustrated in Figure 2. I define the cross-over base station as the common branch node between the old and new base stations, an example of which is illustrated in the figure. In the worst case the cross-over point is the gateway. During this interval, downlink packets may be lost. Mappings associated with the old base station are not cleared when handoff is initiated. Rather, mappings between the cross-over node and the old base station timeout and are removed. No packets are transmitted along the old path once the route-update message has created anew mapping at the cross-over base station that points toward the new base station.

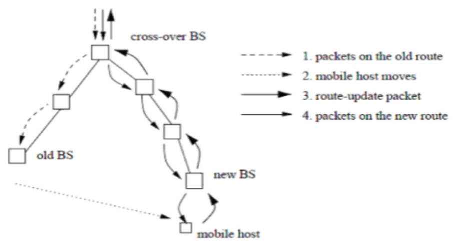

Figure 2: Cellular IP Handoff

Although packets may get lost during a hard handoff, the time taken to redirect packets to the new point of attachment is shorter than that of Mobile IP. This is due to the fact that only a local node has to be notified rather than a possibly distant home agent in the case of Mobile IP. There are several ways to reduce packet loss during handoff. One approach relies on interaction between the old and new base stations [11] during handoff. In this case the new base station notifies the old base station of the pending handoff. Packets that arrive at the old base station after notification of handoff are forwarded to the new base station and onto the mobile host. In contrast, packets that arrive at the old base station before notification is complete will be lost. If the notification time (i.e., the round-trip time between the new and the old base stations) is not smaller than handoff duration(i.e., the round-trip time between the new and cross-over base stations) then this approach does not significantly improve handoff. An additional cost of these schemes is that communications, signaling and information state exchange required between base stations for this approach to work. To preserve the simplicity of hard handoff, Cellular IP employs a different approach to counter the problem of packet loss.

Semisoft Handoff-

After hard handoff, the path to the old base station remains in place until the soft-state cache map-pings time out. We leverage this feature to support a new handoff service called semisoft handoff that improves handoff performance while maintaining the lightweight nature of the “listening” to the old base station.

The purpose of the semisoft packet is to establish new routing cache mappings between the cross-over base station and the new base station. During this route establishment phase the mobile host is still “connected” to the old base station. After a semisoft delay, the mobile host performs a regular handoff. The semisoft delay can be an arbitrary value that is proportional to the mobile to gateway round-trip delay. This delay ensures that by the time the mobile host finally tunes its radio to the new base station, its downlink packets are being delivered through both the old and new base stations. I observe that downlink packets consume twice the amount of resources during this period. However, this period represents a short duration when one considers the complete semisoft handoff process.

While the semisoft packet ensures that mobile hosts continue to receive packets immediately after handoff, it does not however, assure smooth handoff between base stations. Depending on the network topology and traffic conditions, the time to transmit packets from the cross-over point to the old and new base stations may differ and the packet streams transmitted through the two base stations will typically be unsynchronized. If the new base station is “behind” the old one, the mobile host will receive duplicate packets, which does not disrupt many applications. For example, TCP will not be forced into slow start due to the arrival of duplicate acknowledgments. If the new base station is “ahead” then packets will be missing from the stream received by at the mobile host. The second architectural component of semisoft handoff resolves this issue of the new base station getting ahead. The solution to this problem is based on the observation that perfect synchronization of packet streams is unnecessary. This condition can be eliminated by temporarily introducing a constant delay along the new path between the cross-over base station and the new base station using a simple “delay device” mechanism. The device needs to provide sufficient enough a delay to compensate, with high probability, for the time difference between the two streams traveling on the old and new paths. Optimally, the device delay should be located at the cross-over base station. The cross-over base station is aware that a semisoft handoff is in progress from the fact that a semisoft packet arrives from a mobile host that has mapping to another interface. Mappings created at cross-over points by the reception of semisoft packets include a flag to indicate that downlink packets must pass through a delay device before being forwarded for transmission along the new path. After handoff is complete, the mobile host sends a data or route-update packet along the new path. These packets have the impact of clearing the flag causing all packets in the delay device to be forwarded to the mobile host. Base stations only need a small pool of delay buffers to resolve this issue. Packets that cannot sustain additional delay can be forwarded without passing through the delay device. This differentiation can be made on a per packet basis, using e.g., differentiated service or transport (e.g., TCP, UDP or RTP).

Paging-

Typically, fixed hosts connected to the Internet (e.g., desktop computers) remain on-line for extended periods of time even though most of the time they do not communicate. Being “always connected” in this manner results in being reachable around the clock with instant access to Internet resources. Mobile subscribers connected to the wireless Internet will expect similar service. However, in the case of mobile hosts maintaining location information in support of being continuously reachable would require frequent location updates which would consume precious bandwidth and battery power. Cellular systems employ the notion of passive connectivity to reduce the power consumption of idle mobile hosts. Base stations are geographically grouped into paging areas. When there is no call ongoing, mobile hosts only need to report their position to the network if they move between paging areas. This makes location update and handoff support for idle hosts unnecessary. When an incoming call is detected at the gateway a paging message is transmitted to the mobile host's current paging area to establish the call. The mobile node informs the infrastructure of its location as a result of the paging process and transition to active mode to take the call. While the definition of an idle mobile device is well understood in the context of cellular systems ,which are connection oriented in nature, its meaning in IP-based mobile networks is unclear. Cellular IP defines an idle mobile host as one that has not transmitted packets for a system specific time active-state-timeout. Due to lack of updates, the soft-state routing cache mappings of idle mobile hosts will time out in a fully distributed manner. In order to remain “reachable” mobile hosts transmit paging-update packets at regular intervals defined by a paging-update-time. A paging-update packet is an ICMP packet, which is addressed to the gateway and is distinguished from route-update packets by its type parameter value. Mobile hosts send paging-update packets to base stations that have better signal quality. As in the case of data and route-update packets, paging-update packets are routed toward the gateway on a hop-by-hop basis. Base stations may optionally maintain paging cache. Paging cache has the same format and operation as routing cache with the following exceptions. Paging cache mappings have a longer timeout period called paging-timeout hence a longer interval exists between consecutive paging-update packets. In addition, any packet sent by mobile hosts including route-update packets can update paging cache. However, paging-update packets cannot update routing cache. This results in idle mobile hosts having mappings in the paging cache but not in the routing cache. In contrast, active mobile hosts will have mappings in both routing and paging cache. Packets addressed to a mobile host are normally routed by routing cache mappings. Paging occurs when a packet is addressed to an idle mobile host and the gateway or base stations find no valid routing cache mapping for the destination. If the base station has no paging cache, it will forward the packet to all of its interfaces except the one the packet came through. Cellular IP has no explicit paging control message. Rather, the first data packet that arrives at the gateway forms an implicit “paging message" that is forwarded in the access network. Paging cache is used to avoid broadcast search procedures. Base stations that have paging cache will only forward a paging packet if the destination has a valid paging cache mapping. In this case the paging message is only forwarded to the mapped interface. If there is no paging cache in an access network then the first packet addressed to an idle mobile will be broadcast, increasing the load on the access network.

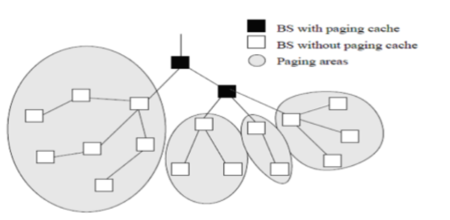

Figure 3: Paging Areas

The network operator can limit paging load in exchange for memory and processing cost by using paging cache in the access network. By placing paging cache in base stations, paging areas can be defined as required. An operator can construct paging areas and determine what nodes in the access network should support paging cache and which should not. For example, paging cache could be located at the gateway only or at the majority of the base stations in the access network. The construction of paging areas (i.e., the number of base stations that comprise a paging area) and the distribution of paging cache within paging area (i.e., which nodes do and do not have paging cache) is a configuration issue some examples of which are illustrated in Figure 3.In the case of Cellular IP a paging area identifier is broadcast as part of beacon messages. Idle mobile hosts will only transmit paging-update packets when they move between paging areas. An idle mobile host that receives a paging packet transition from idle to active state and immediately transmits a route-update packet towards the gateway. This ensures that routing cache mappings are quickly established limiting any further paging in the location area.

Security-

Cellular IP has been designed to support seamless and secure handoff. Mobile systems are open to a number of security problems that do not exist in their stationary counterparts. In a fixed network, the prefix of a subnet is usually configured manually and the location of the prefix is communicated between routers that have either some form of inherent trust model or use a secure protocol. This makes it hard to impersonate someone. Mobile hosts, on the other hand, must update their location while moving. These location messages make impersonation possible unless properly secured. Wireless access networks compound these security problems because packets can be snooped over the air interface. Cellular IP faces impersonation and snooping attacks because it is wireless and mobile.

Cellular IP addresses these security issues. First, only authenticated packets can establish or change cache mappings in a Cellular IP access network. By authenticating paging and routing update control messages malicious users are prevented from capturing traffic destined for mobile hosts. In Cellular IP access networks only control packets are authenticated. In this case, data packets are not to be authenticated which would be costly in terms of transport performance. Control messages establish and change existing mappings. In contrast, data packets can only refresh existing mappings. Active mobile hosts transmit route-update packets during handoff to create a new chain of soft-state cache mappings that point to the new point of attachment.

In case of Cellular IP seamless handoff is of primary importance. Therefore session keys used by mobile hosts to perform authentication must be promptly available at the new base station during handoff. Timeliness of the authentication process is critical in the case of micro-mobility due to the requirement of fast handoff control. In contrast, global mobility solutions may have broader requirements such as user identification, bilateral billing and service provisioning agreements. These boarder requirements out weight the need to support fast handoff control where the scalability of the global Authentication, Authorization and Account (AAA) [7] system is of more importance than seamless handoff. One can envision, however, micro-mobility protocols that build on global AAA preferences by offering enhanced services (e.g., fast session key management) to aid seamless handoff.

During handoff, the new base station could hypothetically acquire a session key by contacting the old base station, the cross-over base station or some central key management server. In Cellular IP fast session key management operates as follows. Rather than defining new signaling, a special session key is used in Cellular IP access networks. Base stations can independently calculate session keys. This eliminates the need for signaling in support of session key management, which would inevitably add additional delay to the handoff process. The session key is a secure hash, which combines:

1. the IP address of a mobile host (IPMH);
2. a random value (RMH) assigned to a mobile host when it first registers with an access network; and
3. a network secret (Knetwork) known by all base stations within an access network.

The session key is calculated using an MD5 hash function:

Ksession = MD5(IPMH; RMH;Knetwork)

A session key is first calculated and transmitted to a mobile host when it first contacts the Cellular IP network during global mobility authentication and authorization. The random value RMH is assigned to the mobile host at this point. Control packets carry this random value (RMH) together with their authentication information. A timestamp is used for replay protection. The session key is used to perform authentication. Base stations can quickly calculate the session key by combining the IP address and the random value found in the control packet with the "network secret". Base stations can validate the authentication easily with the session key. The base stations perform the validation process without any further communication or pre-distributed subscription databases. This results in fast and secure handoff. To enhance security, the network key could be periodically replaced thereby triggering session key changes making brute force attacks more difficult.

IV. Implement Cellular IP Network Model-

Mobile IP allows a mobile node to change its location without need to restart its applications or terminate any on going communication. It represents a simple and scalable global mobility solution but lacks the support for fast handoff control and paging found in cellular telephone networks. In contrast, 2Gand 3G cellular systems offer seamless mobility management but built on complex and costly connection-oriented networking infrastructure. As a solution to these issues, the concept of cellular IP and later cellular IPv6 were proposed to provide seamless mobility support in a limited geographical area. The specification of Cellular IP has been drafted by the IETF in [5][6], on which this paper is based. Significant research in the field of cellular IP has been published over the last several years. The works mainly deal with the design, implementation and analysis of cellular IP protocols, including routing, handoff, and paging performance with a single gateway [8]-[9].
Cellular IP requires that a mobile host be using exactly one gateway to the Internet backbone with Mobile IP at a time [5]. It is recognized that if the size (or the number of nodes) of a domain network is large, its gateway potentially becomes a bottleneck of the system performance as all the IP packets from mobile hosts in the domain to the Internet, or vice versa, must go through the gateway. Thus, a cellular IP network may be equipped with multiple gateways to reduce the size of each domain. However, when the size of a domain network is small, the frequency of location update for the home registration with a mobile host will be increased, since the mobile host will have higher probability to move out of the small domain. As a result, it becomes a practical issue to find out the optimal size of the cellular IP domain, where the system, including the gateway, can achieve the best performance. In this paper an analytical model is presented for the performance analysis of a cellular IP network with multiple gateways. Based on this model, an optimal system design can be theoretically found in terms of the network size ,traffic load, user population, user mobility and routing algorithm for IP packets in a domain. Consequently, an algorithm is proposed for breaking a large cellular IP domain into two small domains ,which can be easily used for the system selection in practice. Finally, some numerical results will be demonstrated for a number of typical cases presented in the algorithm.

Architecture-

Network are composed several domain network attaches to internet through multiple gateway. For example in Fig.4 the domain network connects to internet via gateway1 and gateway2 .packets can be forwarded by one of them . These gateway periodically broadcast their "gateway broadcast packet " to the domain. All nodes in the domain are aware of routing paths to all gateways from these control packets. In fig 3.1 routing path will be established after "gateway broadcast packet " are received .the rough blank line is the routing path for gateway 1 and dash line for gateway 2.Both of them loop-free trees . All nodes can packets to each gateway following the paths.

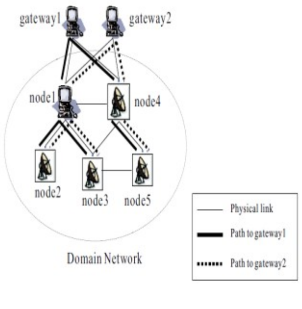

Figure 4:Routing path for multiple gateways.

Furthermore ,because the “gateway broadcast packet ” is sent periodically ,another available routing paths will be fount the failure of links occurs or node crash.

After an MN enters the cellular IP network ,it will select one gateway as its foreign agent for registration. After the selection ,the MN adds the IP address of the gateway to its routing updates packets and sends the packet to the gateway periodically. Like the cellular IP ,node receiving the packet cache the position of the MN and selected gateway information .Therefore the nodes can be forward packets for the MN based on cache information . For instance in Fig 4.1 node received the “gateway broadcast packet ” and routing packets ,all caches were established after MN1 sends packets to its base station node2 .Node2 lookups its cache and forward packets to node1.Similarly node 1 forward packets to gateway1.When packets arrive at gateway1, it forwards the packets to internet .With regard to Down-link, packets are forwarded in reverse path.

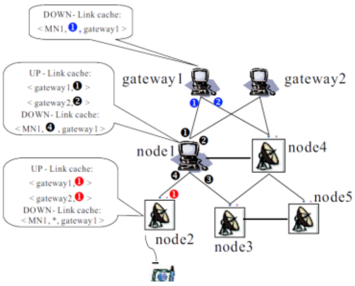

Figure 4.1:Routing cache for mobile node.

Routing Algorithm-

The cellular IP node must have enough information for forwarding packets for MNs. There are three processing for obtaining the routing in formation .First the node cache the information about MNs through routing-update or paging-update packets. They could forward packets to MNs according to these cache. Second nodes have to know the routing path to cache the gateway .These path were established with the help of “gateway broadcast packet ” .Last, the MN select one serviced gateway and periodically updates its location with the gateway .Therefore the node must know which gateway the packet are routed to .In other words, node have to know the selected gateway of the MN. These information could be retrieved from the update packets. The algorithm of sending packets to gateway is shown in Algorithm 1.

Algorithm 1: UP-Link algorithm for cellular IP node

```
Variables:
        RC(mn):Routing cache for mobile node,mn;
        PC(mn):paging cache for mobile node,mn;
        Rt(mn):The lifetime of the mobile node ,mn,in RC;
        Pt(mn):The lifetime of mobile node ,mn, in PC;
        SA     : The source address of the arrived packet;
        GA(mn): The gateway selected by mobile node,mn;
        UP(ga): The up-port for gateway ,ga;

While the packet is arrived…..
Begin :
    Set rc=0;
If(the type of packet is routing-update packet) then
   If(!(find RC(SA)))then
       Add RC(SA);
    Else
      Reset Rt(SA);
  End if
Set rc=1;
  End if
   If (the type of packet-update packet) or (rc) then
     If(there is paging cache) then
       If(!(find PC(SA))) then
 Add PC(SA);
Else
```

```
Reset Pt(SA);
End if
  End if
    Cache GA(SA);
End if
Forward this packet to the interface : UP(GA(SA));
End
```

Mobile Node-

When MNs enter a new cellular IP network , they will select a gateway for registration .There are two matrices for gateway selection . One of them is the nearest .The gateway with the minimum hop to MNs will be selected .Another one is the lower load. The gateway with the minimum number of visited MNs currently will be registered. These information of matrices can be obtain from beacon packet sent by cellular IP base station .After selecting the gateway for registration , the MN adds the IP address of the selected gateway to update packets for routing packets.

Gateway and base station-

For propagating the existence of gateway , the gateway has to broadcast the “gateway broadcast packet” in to its domain network. In every “gateway broadcast packet” ,there is one field for gateway selection . As mentioned above, this field record one type of gateway selection matrices. If storing the hop counter ,every cellular IP node will be increase the hop counter before forwarding this control packet. In lower load ,the gateway stores the number of visited MNs to this field and then propagates this control packet.

Every base station cellular IP attaches visited MNs through wireless interface. These base station propagates the existence of all available gateways to MNs and determine the availability of all gateways. For propagation the existence of all gateways, the base station will reach the information of all gateways from “gateway broadcast packet” and adds these information to beacon packet. The beacon packet is periodically sent to MNs by base station. While receiving “gateway broadcast packet” , the base station also start a timer(normally three times of gateway broadcast timer) for the gateway. After the timer expired , the base station will consider that the gateway is failed and removes the in formation of the failed the gateway from beacon packet. Therefore, MNs can be aware of the existence of the packet.

V. Protocol Details-

Redundancy-

Basing on the feature of cellular IP , the redundancy procedure is easy to achieve in this protocol. In cellular IP the MNs periodically sends the routing-update packet to its service gateway for maintaining its routing path. While this gateway is failed, another gateway will replaced. Because the gateway substituted for the fault one deliveries a “gateway broadcast packet” to its domain network instead, all nodes will change the routing path to that new gateway. For example fig 3 gateway 1 and gateway 2 maintain their routing path independently. After gateway 2 fail , gateway 1 replaces gateway 2 and maintain both routing paths, shown in fig 4. Therefore all packets including update packets will be redirected to the gateway substituted for the fault one. Then this new gateway obtains the information of MNs after receiving updates packets. In the redundancy procedure of HARP , all registration packets have to send to other gateways and wait for reply packets. This will increase the time latency of registration. The procedure of redundancy is easy to implement in cellular IP. MNs just add its information to updates packets and gateways retrieve the information of MNs from these packets. Therefore , there is no waiting time in the redundancy procedure of cellular IP.

Failure Detection-

There are three failure detecting packet in our protocol. They are routing-update , “ping” and “ping-ack” packets.

- Routing-update packet: Expect the source address is the IP address of the gateway , this packet is the routing-update packet sent by MN in cellular IP. Similar to the MN in cellular IP ,every gateway , select one serviced gateway and periodically sends routing-update packet to that gateway. Regarding the cellular IP nodes, they cache the information of the gateway similarly gateway detecting gateway. In addition to caching , it has to detect the failure according to the time out of the cache of the gateway.
- Ping packet: For detecting the type of the failure , the detecting gateway sends “ping” packet to the indeterminate gateway. This packet is sent by the detecting gateway while its detect the time out of one cache of gateway.
- Ping-ack packet: while a gateway receives one “ping” packet , it replies “ping-ack” packet back to the sender.

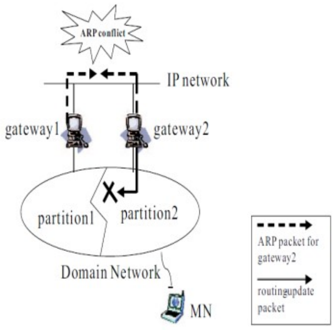

Figure 4.2:IP conflict without using “Ping”.

For detecting the failure and reducing the load of IP network, the routing-update packet routs through cellular IP network. Because all gateways periodically delivery routing-update packets, other in the same domain network can detect the failure. However , this procedure can not determine which the failure happens. The failure could result from the gateway or from the domain network partition.

When the network partition is occurred , route-update packets can not arrive at the detecting gateway which is located in the different network partition. Then the detecting gateway determines that the gateway is failed and it takeovers the gateway using ARP function. Therefore ,the conflict is happened after replacement. For example in Fig .4 gateway1 is the detecting gateway of gateway2. While the network partition is happened ,gateway1 replaces gateway2 starting ARP function. But the gateway2 is alive. This situation will result in the IP conflict. Therefore , the network partition have to be consider.

This procedure of detection can be improve by detecting both the routing-update packet and “ping” packet. This process is for further detection. Otherwise ,there is no reply from the indeterminate gateway, it determines that the gateway is failed and start the procedure of taking over.

Take over-

The failure of gateway

While one gateway detects the failure of another gateway ,it replaces the faulty one by one ARP packets and broadcasting the “gateway broadcast packet” to the domain network. In Internet ,the gateway substitutes for the faulty one has to intercept the packet sent to the fail gateway. In cellular IP ,while one gateway is failed , the gateway substitutes for this faulty one adds the IP address of the fail gateway to its “gateway broadcast packet”. Then it sends this control packet to its domain network immediately. Nodes will established a new routing path after receiving the control packet. Therefore ,nodes can redirect packets including the update packet to the new gateway. And MNs can be serviced by the new one. Gateway 1 and gateway 2 detect each other. While gateway 2 is failed , the gateway 1 will add the IP address of gateway 2 to its “gateway broadcast packet”. Then it sends this control packet to the domain. After receiving this “gateway broadcast packet” , nodes setup their new routing path shown in Fig 4.3. Therefore ,gateway 1 can forward all packets for MNs.

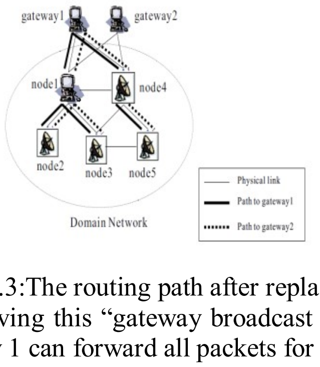

Figure 4.3:The routing path after replacement

Domain network partition

If the domain network partition is occurred , the MN and its registered gateway in different partition can not be connect with each other. Therefore ,the packet lost was happened.

For reducing the packet lost, MNs can communicate with its register gateway through other gateway located in the partition of MNs. While the detecting the gateway inspects the network partition if occurred, it replaces the gateway located in other partition for the broadcasting the “gateway broadcast packet”. After nodes receives this control packet , they establish new routing path and forward update packets to the new gateway. In addition to caching the information of MNs, the new gate way inspects the update packet after receiving it.

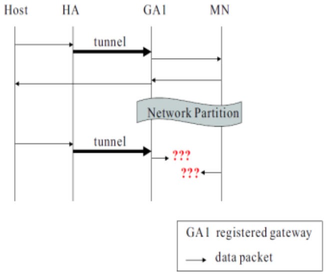

Figure 4.4:The problem on network partition

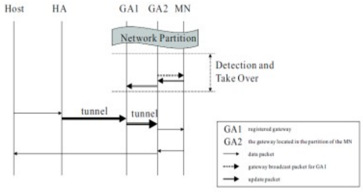

Figure 4.5:The procedure of take over at network partition

If the destination of the packet is the gateway located other partition , the new gateway forwards the update packet to that gateway through Internet. Similar to cellular IP , the registered gateway retrieves the information of the MN and cache these data after receiving the update packet. Therefore ,registered gateway can locate the MN. Furthermore , the registered gateway adds the IP address of the new gateway to its partition-gateway list for tunneling. Otherwise ,packets will be discarded.

While packets sent to MNs arrive at the domain , the registered gateway lookups its cache. If the address of the searching result is found in the partition-gateway list. The registered gateway will know the location of MN in different partition network, then tunneling [10,11] the packet to that gateway which serves MNs in the partition. It is the similar to cellular IP that gateway de-tunnels the packet and searches its cache to find the location of the MN, then forward the packet. The details are shown in Fig 4.5. Both GA1 and GA2 detect with each other. The registered gateway of MN is GA1. After the network partition happened, MN and GA2 in the same partition network. And GA1 is in different partition. While GA2 detects the network partition, it adds the IP address to its “gateway broadcast packet” and sends this packet to domain network. Therefore , the update packet of MN can be forwarded to GA2.GA2 forwards the update packet to GA1 after processing the update packet. While GA1 receives this update packet, it knows the location of MN. Consequently , GA1 can tunnel packets to GA2 for MN. GA2 de-tunnels and forwards to MN. Besides , both the failure detection and take over algorithms shown in Algorithm 2.

Algorithm 2. Failure detection and take over algorithm

```
Variables:
Rt(mn): The lifetime of the mobile node ,mn, in RC;
ARP(ga): The ARP control packets for gateway ,ga;
GBP(ga): The “gateway broadcast packet” for the gateway, ga;
Rt(ga)escapes….
Begin:
Send “ping” packet to the gateway,ga;
Wait for reply…
If(Ping_{time-out} escapes) then
  Send ARP(ga);
  Send GBP(ga);
```

```
Return;
  End if
 Send GBP(ga);
end
```

VI. Simulation Results-

From different points of view, simulation cases are carried out to illustrate the benefits of cellular IP protocol and the performance of this routing system.

Simulation Tool – Network Simulator

Network Simulator [NS2] is a simulation tool developed by UC Berkeley, and is widely used in the field of network technology research. As an open source simulation tool, many extensions targeted at various network technologies, for instance, support for mobile networks, have been added since its creation. The simulator is written in C++, and uses OTcl as a command and configuration interface. NS2 uses two languages to provide two different simulation requirements. The scenario generation and parameter configuration are carried out by OTcl code, and the detailed simulation of protocols is carried out by C++ code. Additionally, NS2 provides a method to combine these two languages.

Experiment-

We used NS2 (Network Simulator) to simulate our policy-based routing module. Since, at present, there is a multiple gateway support in cellular IP, and we wish to investigate is the routing path which could not be influenced by the mobility of nodes, we decided to use the basic ‘node’ instead of mobile nodes, although our module is designed for a mobile network. The simulation topology is described ,all the nodes in this topology are basic nodes defined in NS2. Shown Fig.5 where we design the network path .

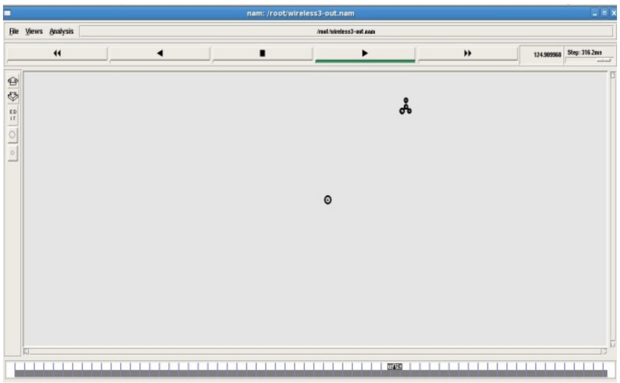

Figure .5

In Fig.5.1 we discover the multiple gateway and configure between Foreign Agent and Home Agent.

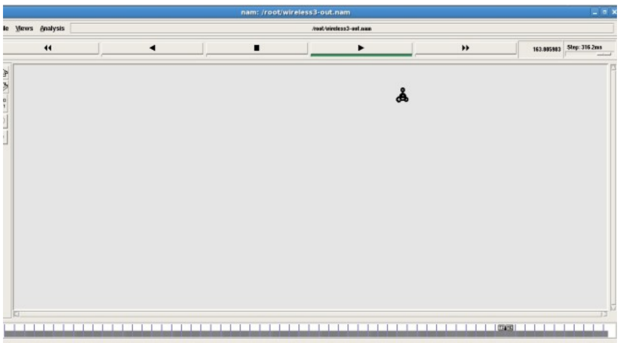

Figure 5.1

The experiment compares our proposal, name multiple gateways with failure detection protocol, cellular IP and multiple gateway protocol. In simulation with data traffics there were mobile node receiving different corresponding nodes. Every CN transmitted a 1280 bytes data/seconds 0.01ms. While connection were established mobile nodes enter active state, and send a route update packets for downlink routing. Therefore the no. of control packets was more than that without data traffics.

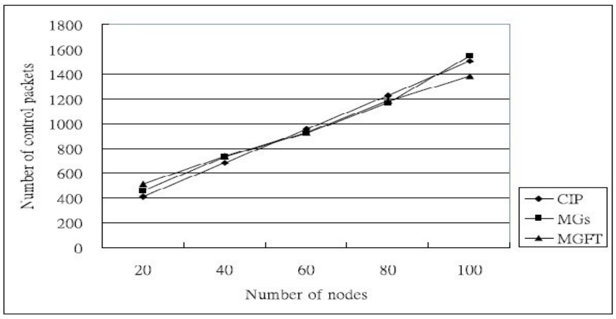

Figure 6:The average number of control packet without data traffic.

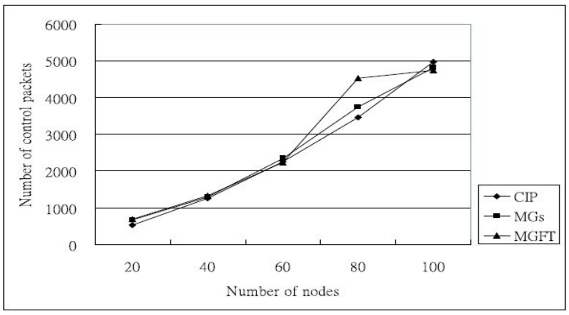

Figure 6.1: The average number of control packet with the data traffics.

VII. Conclusions-

The paper proposed a light weight extension to the cellular IP architecture to allow the multiple gateway in the cellular IP network. The mobile host initiated the gateway switchover when the serving the gate way goes down. The gateway selection algorithm uses the current snapshot of gateway state and uniformly distributed the serving gateway to the mobile host. The architecture is implemented using CIMS .

References

[1] P. Bhagwat, C. Perkins, S. Tripathi, "Network Layer Mobility: an Architecture and Survey", IEEE Personal Communications Magazine, Vol. 3, No. 3, pp. 54-64, June 1996.

[2] Andr_as G. Valk_o, "Cellular IP: A New Approach to Internet Host Mobility", ACM Computer Communication Review, January 1999.

[3] "WaveLAN Air Interface," Data Manual, AT&T Corporation, Doc. No. 407-0024785 Rev. 2(draft), July 11, 1995.

[4] M. Mouly, M-B. Pautet, "The GSM System for Mobile communications," published by the authors, ISBN 2-9507190-0-7, 1992.

[5] C. Perkins, editor, "IP Mobility Support", Internet RFC 2002, October 1996.

[6] S. Blake, D. Black, M. Carlson, E. Davis, Z. Wang, W. Weiss, "An Architecture for Di erentiated Services", Internet RFC 2475, December 1998.

[7] A. T. Campbell, Gomez, J., Kim, S., Turnyi, Z., Wan, C-Y, and A, Valko, "Design, Implementation and Evaluation of Cellular IP", IEEE Personal Communications, June/July 2000.

[8] Andrew T. Campbell, Jaview Gomez, Sanghyo Kim, and Chieh-Yih Wan, "Comparison of IP Micromobility Protocols", IEEE Wireless Communications, February 2002.

[9] Zach D. Shelby, Petri Mahonen, Dionisios Gatzounas, Alessandro Inzerilli, and Ville Typpo, "Cellular IP route Optimization", <draft-shelby-ciprouteoptimizationn-00.txt".

[10] A. Valko, "Cellular IP – new approach of Internet host mobility", ACM Computer Communication Reviews, January, 1999.

[11] "WaveLAN Air Interface," Data Manual, AT&T Corporation, Doc. No. 407-0024785 Rev. 2(draft), July 11, 1995.

[12] M. Mouly, M-B. Pautet, "The GSM System for Mobile Communications", published by the authors, ISBN 2-9507190-0-7, 1992.

[13] E. Gustafsson, A. Jonsson, C. Perkins, \Mobile IP Regional Tunnel Management," Internet Draft,draft-ietf-mobileip-reg-tunnel-01.txt,Internet Draft, August 1999, Work in Progress.

[14] The Network Simulator - ns-2, http://www.isi.edu/nsnam/ns/.