Stefano M. Faccin
Rajeev Koodli
Franck Le
Jari T. Malinen
Rene Purnadi

Dormant Mode Handover Support in Mobile Networks

<draft-koodli-paging-01.txt>

Status of This Memo

Abstract

This document defines an IP paging concept that supports IP dormancy for hosts and Mobile Nodes. The concept specifies a generic model that can be applied to several mobility mechanisms (including Mobile IPv6, Localized Mobility Managament) and is independent of the layer-2 access technology and paging capabilities. The model allows for optimizations of the benefits of layer-2 paging when present, while minimizing the impact on layer-2 paging.

Table of Contents

1. Introduction

The problem of Dormant Mode Host Alerting, otherwise known as IP Paging, is well-defined and described in [2]. It is generally accepted that an IP Paging solution would offer many advantages including, power saving when it is not available in certain Layer 2 technologies (and enhancing it in those that already offer it), reduced IP layer signaling during dormant mode movements, and offering location tracking across heterogeneous access technologies, among others. While these advantages are compelling, the solution itself has to meet certain requirements. Specifically, it is identified that an IP Paging proposal has to address the requirements set forth in RFC 3154. In this document, we propose a mechanism for IP Paging that provides the following advantages.

1. is independent of any mobility management protocol

2. can be adopted with several mobility management protocols while not only allowing to enjoy the benefit of DMHA in terms of both power saving and reduced signaling message exchange, but actually optimizing both

3. allows to optimize the interaction between IP paging and L2 paging mechanisms when present

4. minimizes impact on L2 paging and link layer technologies

5. provides improvements in terms of power saving and minimization of mobility signaling with respect to the presence of L2 paging only

6. supports both implicit and explicit IP dormancy

7. allows support of different access technologies in the same IP paging area

8. supports dynamic IP paging area

Our proposal addresses the requirements set forth in RFC 3154. This is outlined in Section 8.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", "OPTIONAL", and "silently ignore" in this document are to be interpreted as described in RFC 2119.

3. Protocol Overview

We coalesce the functional entities identified in RFC 3154, namely the Dormant Mobility Agent, the Tracking Agent, and the Paging Agent, into a single logical entity which we call the ``Paging Function'' or ``PF''. There are several advantages to such a coalescing of different functional elements. First, it provides a single, trusted channel of paging-related communication between a MN and the network. For all paging purposes, the MN communicates with a single logical entity and secures its communication using an appropriate security association it shares with that entity. Second, since the MN deals with a single logical entity, the problem of discovering different functionalities is alleviated. Depending on where the PF is realized, the MN deals with its Access Router or visited domain Mobility Agent only. Third, since the MN deals with a single logical entity, the number of separate messages necessary to communicate with different elements, potentially over an expensive air interface, can be reduced by aggregating them together. For instance, a single message can establish the necessary paging state at DMA, TA and the PA. It has to be noted that the PF is a logical funtion and for a given MN in a given moment there is only one PF. PF is, however, in no way a centralized function

The PF may be realized in different ways in practice. We provide some examples in Section 7. Note that since the IP dormancy of a MN has to be checked before the packet can be delivered to a MN, all the incoming packets traverse the PF. When an IP packet arrives at a PF, where the MN has last established its presence, the PF has to determine how to forward the packet. We propose two ways by which the PF acertains that the MN to which the packet is addressed to has undergone dormant mode handover. First, prior to undergoing the dormant mode handover, the MN performs an explicit registration with the PF. Second, we allow for an implicit registration, in which the network may initiate IP Paging when it discovers that a MN is no longer reachable. The details of these registration procedures are presented in Section 4.

Once the PF determines the need for IP Paging, it initiates a paging message addressed to an IP Paging Area (IP-PA). We identify each IP-PA by an IP multicast group, whose members are typically all the access routers to which a MN could be ``dormantly connected''. We propose sending IP Paging messages over the access network, which is typically connected with a higher-speed network compared to the access link bandwidth, and make use of Layer 2 paging as much as possible over the air interface. This ensures preserving spectrum where it is considered important and allows usage of enhanced IP messages over a higher-speed access network. Each IP-PA could span multiple subnets and each subnet could represent a disparate access

technology. An IP Paging message sent to the IP-PA multicast group contains a unique paging identity that is known both to the latest PF and the MN. This paging identity serves two purposes. It acts as input to a function that creates a Layer 2 identity to page once an IP Paging message is received over the access network. Where Layer 2 paging is not available, the unique paging identity is used to send an IP Paging message over the access link. The description of this unique paging identity and the IP Paging message sent over the acces network itself is described in Section 5.

One or more of the ARs perform paging (either L2 or IP layer) in response to the arrival of an IP Paging message over the access network. In response to this access link paging message, the MN wakes up and responds to the access link paging message. The MN may then proceed to perform IP layer registrations, such as a Binding Updates. The access link paging messages must be secure and allow for mutual authentication of the network and the MN. These messages and the corresponding operations (in the form of a state machine) are described in Section 4. In the subsequent section, we describe the relation between the IP paging and Layer 2 paging.

It is clearly identified that the IP paging mechanism must address the security considerations. These are elaborated in Section 6. We discuss the realization of the PF entity in an AR or a Mobility Agent in Section 7. Finally, we describe some important enahncements to the basic IP Paging protocol in Section A.

4. IP Paging Model

4.1. Mobile Node IP Paging States

The MN IP paging states model the MN behavior in terms of MN activity and reachability at IP level. The following states are defined.

- MN de-registered: MN is not reachable, has no IP address allocated and is not able to send or receive any packets to the network (e.g. terminal is powered off).

- MN Registered-Active: MN has performed the registration to access the network, has a valid IP address, and is capable of sending and receiving packets without need for additional signaling.

- MN Registered-IP Dormant: Location tracking is at the IP-PA level, i.e., routing information is available to route packets to the "paging area" or, better, to the node acting as PF. While IP dormant, MN wakes up only to perform appropriate operations (e.g.

listen for paging, signal when entering a new IP-PA, etc.). In order to forward packets to the MN the network needs to page the terminal at the IP level (IP paging).

When the terminal is not a mobile node but any generic host, we define the following states.

- Active Host: the host is connected to the network, has a valid IP address is capable of sending and receiving packets without need for additional signaling.

- IP Dormant Host: the host is reachable only at the IP-PA level, i.e., routing information are available to route packets to the "paging area" or, better, to the node acting as PF. While IP dormant, the host wakes up only to perform appropriate operations (e.g. listen for paging, paging area updates needed when entering a new IP-PA, etc.). In order to forward packets to the host, the network needs to page the host at the IP level(IP paging).

4.2. IP Paging Illustration

We illustrate the concepts using Figure 1.

At time t0 packets destined for the MN arrive at the PF. At t1, the PF realizes that the MN is IP dormant. At t2 the PF sends ``IP Paging Request'' message to all ARs within the IP-PA where the MN is located. At t3 the Access Router either sends a L3 paging request (e.g., a router advertisement with paging extension) or it converts the IP Paging Request message into an appropriate L2 paging message and forwards the request to the MN. When L2 paging is used, the L3 paging id is mapped to a L2 paging id. At the assigned time slot (t4) or the paging channel, the MN wakes up and listens to the page. The MN then responds to the paging message with a ``Paging Response'' message to its AR. The MN (either subsequently or together with the Paging Response message) performs the IP mobility (neighbor discovery and binding updates) procedures. At t5, the MN or its new AR requests PF to forward the buffered packets and delete the state of dormancy of the MN.

The PF determines that the MN is dormant based on explicit ``Paging Registration'' message that the MN sends before entering IP-dormant state. The PF may also determine, implicitly, that the MN is IP-dormant based on a MN-specific timer that expires in the event of traffic inactivity. When a MN wakes up in response to paging, the PF performs ``Paging De-registration'' in order to update or remove state related to MN's dormancy.

The IP Paging Request message is resent if it is not acknowledged. The acknowledgements, i.e., the Paging Response message could arrive from any of the ARs or directly from the MN. The re-transmissions are done up to a configurable number of times.

```
              |
              | (t0) incoming packet
              V
           +----+
           |    |
           | PF | (t1) PF realizes that MN is dormant
           |    |
           +----+
            (  |
           /   |<-(t2)``IP Paging Request''to all ARs within IP-PA.
          |<-(t5)MN (or AR on its behalf)
          |    | requests PF to forward packets.
+---------|---------------------------+
|     +---|----+--------+--------+    |
|     |   |    |        |        |    |
|     |   |    |        |        |    |
|     V   |    V        V        V    |
|  +----+ | +----+   +----+   +----+  |
|  | AR | | | AR |   | AR |   | AR |  |
|  +----+ \ +----+   +----+   +----+  |
|     |    \  |^        |        |    |
|     |     \ ||        |        |<- (t3) L3/L2 Paging Request to all MN
|     V      \V|        V        V  in each AR
|             +----+                  |
|             | MN | (t4)MN wakes-up and replies with ``Paging Response''
|             +----+  MN performs IP mobility
|                     to connect to AR and CN
| IP paging area                      |
+-------------------------------------+
```

Figure 1: IP Paging Illustration

4.3. Advertising Paging Area Information

The MN determines the identity of the IP Paging Area (IP-PA) it currently is in based on the IP-PA Identity that is advertised. Together with the IP-PA Identity, other IP-PA information, such as the IP-PA profile that indicates characteristics of that paging area,

could be broadcast as well. The IP-PA Identity and profile information are advertised by Paging Functions to all the Access Routers in the IP-PA by multicasting them to the ARs. On receipt of this information, each AR in the IP-PA needs to advertise the same information to the MNs in its subnet. This is done using extensions to Router Advertisements.

The multicast address for IP Paging Area Advertisements is the same used by the PF to send IP Paging Requests in its IP-PA.

4.4. PF Discovery

The MN needs to know the identity of the serving PF (or the previous serving PF) to send the different Paging messages such as Paging Area Update, IP Paging Registration in the case of explicit dormancy, etc. In the implicit dormancy case, the MN still needs to know the identity of the serving PF: e.g., when it moves to an area served by a new PF, the MN needs to provide the new PF with the identity of the previous PF so that IP paging state in the previous PF can be released and information required at the new PF (e.g. local paging session key) can be retrieved. As described in the following corresponding sections, many mechanisms exist for the MN to discover the PF identity.

The PF discovery can be done in several ways. The PF address can be sent over router advertisements. Or the MN can send a Paging Function Discovery Request to a pre-defined well-known anycast address. And then, one of the Paging Functions, serving the area the MN is currently located, would reply in a Paging Function Discovery Reply, providing its identity. Once it discovers the PF, the MN then perform all the required procedures with the selected PF.

4.5. Paging Area Update

When the MN realizes that it has moved to a different IP-PA, the MN initiate a paging area update procedure. The paging area update will inform the the PF the current IP-PA so that paging can be efficiently directed to the correct IP-PA. The Paging Area Update message is typically sent when a MN learns of a new paging area from paging area advertisements. In the implicit dormancy case, the MN still needs to know the identity of the serving PF: e.g., when it moves to an area served by a new PF, the MN needs to provide the new PF with the identity of the previous PF so that IP paging state in the previous PF can be released and information required at the new PF (e.g. local paging session key) can be retrieved.

4.6. Detecting IP Dormant MN

The PF declares that a MN is IP dormant upon receiving an explicit message to requet IP dormancy from the MN (explicit dormancy).The message requires to carry information such as the indication that MN wishes to go IP dormant, authentication data to verify the source of request, the Paging Area identity, etc. On the other hand, if the the lack of traffic activity timer expires (implicit dormancy), the PF determines that the MN is dormant again.

4.7. Paging Deregistration

Paging deregistration is required in the following cases.

- when MN goes out of coverage (automatic deregistration): the state in the PF must be released, and this will also save unecessary paging. This can be e.g based on a timer with an expiration time longer than the timer for IP dormancy.

- when MN power off: the state in the PF must be released, and this will also save unecessary paging upon receiving signal from the MN

- when the MN becomes active, the paging state in the PF must be released.

- when the MN handovers to a new PF, the paging state in the old PF must be released.

In the latter two cases, the Paging Response message or the Paging Area Update message to the new PF, results in releasing the paging state. For instance, when the MN is attached to a new PF, the latter sends a message to the old PF to release the state.

5. IP Paging Identity

To ensure that IP paging in an IP-PA can trigger L2 paging so that the appropriate identity can be used at L2 to page the MN (i.e. the identity at L2 that the MN is expecting to be paged with), an L3 IP paging identity is proposed for the MN. The identity is generated according to a well-know mechanism and based on a well-known set of inputs. This guarantees all MNs and networks know how to compute it. This also allows for the identity to be auto-configurable. This L3 IP paging identity needs to be unique only within an IP-PA. This allows for a shorter identifier.

The assumption is that when the MN is registered to the network, both the MN and the network (in particular the PF) know the L3 IP Paging Identity that will be used for paging while MN is within the IP-PA. A mapping algorithm is defined for each link layer technology (if needed) to convert the L3 IP Paging Identity into a L2 temporary identity that can be used to page the MN at L2. When MN is IP dormant and enters an area of coverage of a specific link layer technology, it will map the L3 IP Paging Identity to a L2 identity. When an IP Paging message is received by an AR, it is pushed to the AP where the L3 IP Paging Identity is mapped by the AP to a L2 paging identity according to the link layer technology. The L2 identity is then used to page the MN.

5.1. The network configures L3 IP Paging Identity

The PF generates a temporary L3 IP paging identity that is valid for an IP-PA. If the IP-PA consists of multiple access technologies, the L3 IP Paging Identity will have the length equal to the shortest length of the L2 paging identity in a particular technology. Therefore, for that particular technology that has the shortest length L2 paging identity, the L2 paging identity is equal to the L3 paging identity. For the other access technology, the L2 paging identity is the expansion of the L3 IP paging identity. To cover the case of the distibuted PF, each L3 IP paging identity consists of PF unique part and MN unique part. This scheme allows the uniqueness of the L3 paging identity in an IP-PA and uniqueness of L2 paging identity in each access technology.

Let's assume that the IP-PA consists of access technology A that requires 32 bits L2 paging identity, access technology B that requires 128 bits paging identity and access technology C that requires 20 bits L2 paging identity. The PF will generate a 20 bits temporary L3 IP paging identity for the MN. When the MN uses access technology C, it uses the temporary L3 IP paging identity as its L2 paging identity. If the MN acquires access technology A, the MN will expand the 20 bits temporary L3 IP paging identity into 32 bits L2 paging identity, retaining the uniqueness of the temporary L3 paging identity. In case of distributed PF, the uniqueness of the temporary L3 IP Paging identity can be defended by assigning the first `n' bits unique to the PF and the remaining of the bits unique to the MN.

In addition to computing the L2 Paging Identity, both the MN and the access point also use the L3 IP Paging identity to calculate the time slot/paging channel to be monitored.

5.2. The L3 IP Paging Identity via autoconfiguration

Each AR broadcasts PA identifier (PA-Id) that consists of AR specific part and paging area specific part. Upon receiving this PA-Id, the MN uses a hash function `F1' to its own identifier (e.g., its NAI, its permanent IP Address, etc.) and generates L3 IP Paging Id that consists of the AR specific part that is received from PA-Id and the result of `F1' toward its own identifier. The length of the L3 IP Paging Id is maximum equal to the L2 paging id in that particular access technology.

When the MN sends a paging area update, the newly calculated L3 IP Paging Id, together with old L3 IP Paging Id and old PF, are included in the paging area update request message. If the newly calculated L3 IP Paging Id is valid, an SUCCESS indication is sent by the PF to the MN through paging area update response message. If it is not valid, the PF calculates a new L3 IP paging Id that consists of the AR specific part and MN specific part, and sends it to the MN via the paging area update response. From the L3 IP Paging Id, the MN uses another function `F2' to calculate the L2 Paging Id and function `F3' to calculate the time slot/paging channel to monitor. The access point also uses the L3 IP Paging Id to calculate the L2 paging Id (using F2 function) and the time slot/paging channel (using F3 function).

5.3. L2 identity for paging

IP Paging must trigger L2 paging for technologies that have it. L2 paging is based on temporary identifiers specific to the L2 technology. Even if the L2 temporary identifier is known at the location where MN went IP dormant, the identifier cannot be used for paging in the points of attachment under other ARs since the identifier may be already in use. In addition, if several link layer technologies are supported in same IP-PA, IP paging cannot use the L2 paging identity of one technology to page in the others.

Link-layer technology needs to know what time-slot/paging channel to use to page the MN. The correct time-slot/paging channel is known at location where MN went IP dormant, but not necessarily at the point of attachment where the MN actually is located. How do the points of attachment select the appropriate time-slot/paging channel to page? The time slot/paging channel is decided based on the L3 paging identity. For instance, in the current cellular systems, the time slot/paging channel is obtained using a hash function to the IMSI.

6. IP Paging and L2 paging

When L2 paging is present:

- L3 paging triggers L2 paging for delivery of L3 paging request message

- when IP dormant, MN can avoid L2 mobility procedure while stays within the same IP-PA

7. Security Model for IP Paging

IP paging protocol MUST have a strong security mechanism to prevent all the threats identified and described in [4] that may affect the IP paging protocol performance. Without an adequate security scheme, IP paging may not provide all the identified benefits but results in opposite effects, namely, increased signaling load due to IP paging, congested network, reduced battery life and even breakdown in communication for the MN.

The different paging messages SHOULD be authenticated.

7.1. Authentication of Paging Request messages

The Paging Request messages SHOULD be authenticated. Otherwise, an intruder may send fake Paging Request messages to the dormant MN. The MN will unnecessarily wake up and this may prevent that MN from switching to dormant mode. As a result, the MN may quickly run out of battery, hence become inaccessible. In wireless networks, the MN will also try to set up the radio connection and this may result in the waste of radio resources, which are already rare and expensive.

Many methods are possible to authenticate the Paging Request messages: The MN and the network (specifically the PF) can set up a Paging session key `K'. The mechanism to compute and distribute this key is out of the scope of this document. Then the network can use this key to authenticate the Paging Request message.

Paging Request authentication may be performed between the PF and the MN or between the AR and the MN. If performed in AR, the PF may store this paging session key and distribute it to the different Access routers of the paged area in the paging message; or the access router may retrieve it from a Key Storage Center. If performed by the AR, the paging requet between the PF and the AR can be authenticated with keys that are not user specific but established between PF And arS in the IP-PA (method is out of the scope of this document)

Anti Replay protection may be provided using timestamps, however, time stamp based protocols require the involved nodes to have time clocks and for those time clocks to be both synchronized and secured. We propose the following mechanism to provide authentication of Paging Request message. See Figure 2.

1. When an incoming packet destined to a dormant MN arrives at the PF, the latter pages different access routers of the Paging Area by sending a Paging Request multicast message.

2. The Paging message may contain the session key shared between the MN and the network; or a receiving AR may retrieve it from a Key Storage Center.

3. The Access router generates a random number R, and creates a sequence number N1. This sequence number is user and router specific and must only increase in value.

   The Access Router computes a Token based at least on R, N1, K and a common algorithm shared with the MN: Token (N1, R, K).

   The access router encrypts N1 using K, K[N1], and sends the Token (N1, R, K), the random number, R, and the encrypted N1 to the MN for network authentication.

4. On receipt of the IP paging request, the MN

   - deciphers N1 using K (K[N1), and verifies its validity: N1 must always increase in value; this will ensure the freshness of the message

   - verifies the token: the MN can thus make sure the IP Paging Request is coming from the valid network

```
                 |
                 | 1)incoming packet
                 V
              +-----+
              |     |
              | PF  | PF realizes that MN is dormant
              |     | K
              +-----+
                |
                | 2)Page to all AR within the IP paging area
                |
   +------------|----------------------+
   |     +------+ -------+--------+     |
   |     |      |        |        |     |
   |     |(K)   |(K)     |(K)     |(K)  |
   |     V      V        V        V     |
   |  +-----+   +-----+   +-----+   +-----+ |
   |  | AR |    | AR |    | AR |    | AR | |
   |  +-----+   +-----+   +-----+   +-----+ |
   |     |        |^       |        |   |
   |     |        ||       |        | 3) L3 paging broadcast to
   |     |        ||       |        | all MN in each AR
   |     |        ||       |        |  Token (N1, R, K)
   |     |        ||       |        |  R, K[N1]
   |     V        V|       V        V   |
   |            +-----+                 |
   |            | MN | 4) MN deciphers N1
   |            +-----+    verifies Token|
   |                       keeps N1 for future
   +------------------------------------+
        IP paging area
```

Figure 2: Securing the Paging Request

If the authentication data is computed by the PF, anti replay attacks may also be provided by sequence numbers shared between the MN and the PF. But these sequence numbers must be synchronized. As an example, every time MN changes PF, the sequence number could be re-initiated.

7.2. Authentication of Paging Response

The Paging Response message SHOULD be authenticated: this will provide user authentication for network access and will ensure the validity of the user before forwarding the incoming packets.

Authentication of the Paging Response is based on a local session paging key K shared between the network and the MN. The mechanism to compute this key is out of the scope of this document. Based on this key, the local challenge, the MN computes a token whose validity is verified by the PF.

In order to expedite the network access authentication, the PF may supply the key to all the ARs in the paging area. The MN, when it performs neighbor discovery procedures to connect to the new AR, may supply a token using the key and a challenge specific to the AR. Since the AR would have already received the session key K, it can perform local authentication without having to approach a AAA server, for example. See [idle-mode-ct] for details.

1. in the Paging Request message, the PF (or the AR) generates and includes a Local Challenge.

2. the MN takes this Local Challenge, the local session paging key K and eventually some other information to compute some authentication data to be included in the Paging Response

3. the PF (or the AR) verifies the validity of the Paging Response. If the AR verifies the Paging Response, it sends a corresponding Paging Response message to the PF.

7.3. Authentication of Paging Area Update

Paging Area Update SHOULD be authenticated. This will limit the possible damages of Bogus Paging Information identified and described in [4].

When MN sends a Paging Area Update, the paging information SHOULD be authenticated. This authentication can be based on a local session paging key shared between the MN and the PF. The PF can be either the current one or a new one. The MN will e.g., compute a token based on the Paging information, the session key and other relevant information. If the PF is the current one, the PF will already have the session key and can verify the token. If the PF is a new one, the new PF can forward the token to the previous PF to have it verified. The MN then sets up a new session key with the new PF.

As another alternative, the new PF may get the session key either from the previous PF or from a Key Storage Center, and then perform authentication of the paging messages.

Anti replay attacks may be provided using:

```
                 |
                 | 1)incoming packet
                 V
              +----+
              |    |
              | PF | PF realizes that MN is dormant
              |    | K
              +----+
                |
                | 2)Page to all AR within the IP paging area
                |
   +------------|-----------------------+
   |     +------+ -------+--------+     |
   |     |      |        |        |     |
   |     |(K)   |(K)     |(K)     |(K)  |
   |     V      V        V        V     |
   |  +----+   +----+   +----+   +----+ |
   |  | AR |   | AR |   | AR |   | AR | |
   |  +----+   +----+   +----+   +----+ |
   |     |        |^       |        |   |
   |     |        ||       |        | 3) L3 paging broadcast to
   |     |        ||       |        | all MN in each AR
   |     |        ||       |        |  Local Challenge
   |     |        ||       |        |   |
   |     V        V| 4) Paging Response |
   |           +----+  authentication data
   |           | MN |  (LC, K)         |
   |           +----+                  |
   |                                    |
   +------------------------------------+
        IP paging area
```

Figure 3: Securing the Paging Response

- timestamps, but time stamp based protocols require the involved nodes to have time clocks and for those time clocks to be both synchronized and secured.

- sequence numbers but these sequence numbers must be synchronized. As an example, every time MN changes PF, the sequence number could be re-initiated.

- random numbers generated by the authenticating PF: the MN first send a Paging Area Update and the authentication PF will, in response, provide this random number. The MN will resend the

Paging Are Update containing authentication data computed from the Paging information, and the random number. This method therefore requires additional messages.

7.4. Filtering

Filtering MAY be applied to reduce the potential DoS Amplification damages identified and described in [4] and will allow detection of Bogus CN.

Filtering can be applied on the source or on the types of the packets:

- The MN specifies sources of packets for which it should woken up. Packets from sources not authorized will not generate paging request when they reach Paging Function.

- The MN can also specify the type of packets it should be woken up for.

The MN can send the filtering information to the network at IP Paging Area Update; and MN can update them at paging response or at any time. The network may also have some pre-defined filtering rules of its own.

Filtering allows a flexible handling of incoming packets. Based on the filtering information, the packets can be:

- discarded: packets are discarded and MN will not receive them

- buffered: packets are buffered up to maximum size of per-MN FIFO buffer and provided to the MN only when the MN becomes active. Buffer overflow can be handled by storing only the recent packets or according to other criteria (e.g. "priority")

- grouped:packets are buffered until a certain amount. When that amount is reached, MN is paged and the packets delivered, or

- processed based on other rules.

Efficiency of filtering is strongly related to the ability to verify the type or source of packets: A bogus CN can, e.g., send packets using fake source addresses. So there needs to be a mechanism to "verify" the source. The MN may be able to establish a Security Association with CN for which it wishes to be woken up (e.g., a SIP server) and provide filtering function with security parameters so that it can verify source authenticity for packet from CNs.

Filtering assumes that MN knows in advance what CN will initiate a Mobile Terminated communication. This may be acceptable in some specific environments. MN knows in advance what Mobile Terminated services will take place (e.g. SIP calls from a Call Control Function it has previously registered with, IMPP from server it has previously provided presence information to, e-mail server it has previously "registered" with, etc.); but this may not always be applicable and more particularly for push services to the MN from unknown sources.

8. Application of IP Paging Model to Different Scenarios

The IP paging model can be applied to several different scenarios, whether IP mobility is present or not. In case IP mobility mechanisms are present, the IP paging model can be applied to different scenarios. Scenarios for Mobile IPv4 are not described in this section, but the IP paging model can be applied to Mobile IPv4 as well.

Figure 4 represents the scenario where Mobile IPv6 is adopted in the network. In such a case, the PF can be either in the Access Router (AR) or it can be a node in the network not related to mobility. More than one PFs for a given IP-PA can be used. For a given MN connected to a given AR in a given IP-PA and goes dormant in the IP-PA, only one entity acts as the PF for the MN. Other dormant MNs in the IP-PA may be served by different PFs

```
              +-----------------------------+
             /                               \
            /                                 \
   +----+  +          IP Network               +
   | PF |------->                              |
   +----+  |                                   |
      |    +                                   +
      |     \                                 /
      |      \                               /
      |       +-----------------------------+
      |
      |---------+-------+-----------+-------+-------+
      |         |       |           |       |       |
      |   IP Paging Area|           |IP Paging Area |
   +--|---------|-------|---+  +----|-------|-------|---+
   | +V---+  +--V-+  +--V-+ |  | +--V-+  +--V-+  +--V-+ |
   | | AR |  | AR |  | AR | |  | | AR |  | AR |  | AR | |
   | +----+  +----+  +----+ |  | +----+  +----+  +----+ |
   +------------------------+  +------------------------+
```

Figure 4: MIPv6 scenario.

Figure 5 represents the scenario where Mobile IPv6 Regional Registration is adopted in the network. In such a case, the PF can be either in the Access Router (AR), in one of the Crossover Routers, in the GMA or it can be a node in the network not related to mobility (e.g. in case of implicit dormancy). In the Figure, CR is a Cross-over Router. Similarly, more than one PFs for a given IP-PA can be used. For a given MN connected to a given AR in a given IP-PA and goes dormant in that IP-PA, only one entity acts as the PF for the MN. Other dormant MNs in the IP-PA may be served by different PFs

```
      +------------------>+----+
      |       +-----------|GMA |------------+
      |      /            +----+             \
      |     /    +----+              +----+   \ IP
   +----+  +     | CR |              | CR |    + Network
   | PF |------->+----+              +----+    |
   +----+  |  +----+  +----+    +----+  +----+ |
      |    +  | CR |  | CR |    | CR |  | CR | +
      |     \ +----+  +----+    +----+  +----+/
      |      \                               /
      |       +-----------------------------+
      |
      |---------+-------+-----------+-------+-------+
      |         |       |           |       |       |
      |   IP Paging Area|           |IP Paging Area |
   +--|---------|-------|---+  +----|-------|-------|---+
   | +V---+  +--V-+  +--V-+ |  | +--V-+  +--V-+  +--V-+ |
   | | AR |  | AR |  | AR | |  | | AR |  | AR |  | AR | |
   | +----+  +----+  +----+ |  | +----+  +----+  +----+ |
   +------------------------+  +------------------------+
```

Figure 5: MIPv6 Regional Registration.

Figure 6 represents the scenario where Hierarchical Mobile IPv6 is adopted in the network. In such a case, the PF can be either in the Access Router (AR), in the MAP, or it can be a node in the network not related to mobility.

In scenarios where PF is distributed to the ARs, each AR acts as a PF for a given MN in a given moment. The simplest approach to implement a distributed PF is by defining as PF for a given MN the latest AR where the MN is connected before the MN becomes IP dormant (explicitly or implicitly). As shown in Figure 7, the PF forwards IP paging messages to all ARs within the IP-PA. Each AR will forward the IP paging to all the MNs connected to the AR with the appropriate interactions between IP Paging and L2 paging, when L2 paging is present.

```
   +------------------>+----+
   |       +-----------|MAP |------------+
   |      /            +----+             \
   |     /                                 \
+----+  +         IP Network                +
| PF |------->                              |
+----+  |                                   |
   |    +                                   +
   |     \                                 /
   |      \                               /
   |       +-----------------------------+
   |
   |---------+-------+-----------+-------+-------+
   |         |       |           |       |       |
   |   IP Paging Area|           |IP Paging Area |
+--|---------|-------|---+  +----|-------|-------|---+
| +V---+  +--V-+  +--V-+ |  | +--V-+  +--V-+  +--V-+ |
| | AR |  | AR |  | AR | |  | | AR |  | AR |  | AR | |
| +----+  +----+  +----+ |  | +----+  +----+  +----+ |
+------------------------+  +------------------------+
```

Figure 6: HMIPv6 Scenario.

In hierarchical IP mobility solutions such as MIPv6RR, the PF can be located in any of the mobile agents. In particular, the PF can be distributed to the ARs, to the CRs or implemented in the GMA. If PF is in the GMA, the CR and AR do not maintain any state for a MN when MN is IP dormant. MIPv6RR is used, as currently specified, only when MN is not IP dormant. If the PF is in a CR, IP-PA covers all ARs "below" CR and or even larger area. "Above" the CR, all mobility-aware routers (CRs and GMA) maintain the state for the MN (normal MIPv6RR). If the PF is in the AR, the scenario is the same as the MIPv6 or flat LMM. Similar to the PF in a CR, all mobility-aware routers (CRs and GMA) maintain the state for the MN.

The optimal location of the PF depends on relation with IP mobility and LMM and may depend on type of the terminal and the user.

9. Comparing Against the Requirements

The proposed paging concept is compared to the draft-ietf-seamoby-paging- requirements-01.txt

```
                  |t4:incoming packet routed
                  |last point of attachment(AR2)
                  |
       +----------|------------------------+  +----------------------+
       |          |   IP-PA 1              |  |       IP-PA 2        |
       |   _____  V t5:IP paging to all ARs in|IP-PA1                |
       |  /     \  /    \      \      \    |  |                      |
       | +----+  +----+  +----+  +----+  +----+ |  | +----+  +----+  +----+ |
       | |AR1|  |AR2|  |AR3|  |AR4|  |AR5| |  | |AR6|  |AR7|  |AR8| |
       | +----+  +----+  +----+  +----+  +----+ |  | +----+  +----+  +----+ |
       +------------------------------------+  +----------------------+
          |       |      |
          |       |      |
          |       |     t3:moves to AR3, no L3 mobility procedure
          |      t1:moves with L3 mobility procedure (active handoff)
    t0:MN point  t2:goes dormant, AR2 becomes PF
   of attachment
      is AR1
```

Figure 7: IP paging applied to the distributed PF scenario.

9.1. Impact on Power Consumption

The IP paging protocol MUST minimize impact on the Host's dormant mode operation, in order to minimize excessive power drain.

The proposed paging concept utlilizes IP-PA (IP Paging Area) where the MN does not have to wake up and execute L3 procedure while inside an IP-PA to make the MN wakes up less frequently.

It allows further optimizations in terms of power saving and reduced signaling message exchange when adopted in conjunction with IP mobility mechanisms.

It also allows to optimize the interaction between IP paging and L2 paging mechanisms when present. As an example, with the proposed model an IP dormant MN does not need to perform any L2 mobility signaling when moving within the same IP paging area

9.2. Scalability

The IP paging protocol MUST be scalable to millions of Hosts. Distributing and allowing flexible location of the paging function in

flat or hierarchical mobility scenarios as well in non-mobile networks in the proposed paging concept provides scalability

9.3. Control of Broadcast/Multicast/Anycast

The protocol SHOULD provide a filter mechanism to allow a Host prior to entering dormant mode to filter which broadcast/multicast/anycast packets active a page. This prevents the Host from awakening out of dormant mode for all broadcast/multicast/anycast traffic.

The paging function is capable of filtering the paging message (based on explicit information provided by the MN)

9.4. Efficient Signaling for Inactive Mode

The IP paging protocol SHOULD provide a mechanism for the Tracking Agent to determine whether the Host is in inactive mode, to avoid paging when a host is completely unreachable.

The proposed paging concept introduces explicit and implicit dormancy. In the explicit dormancy, the MN explicitly sends a message to the tracking agent (as one of the functions in the PF) to indicate that it is going to be dormant. In the implicit dormancy, the PF assumes the MN is dormant after the lack of activity from the MN goes beyond a certain threshold (e.g. a timer).

9.5. No Routers

Since the basic issues involved in handling mobile routers are not well understood and since mobile routers have not exhibited a requirement for paging, the IP paging protocol MAY NOT support routers. However, the IP paging protocol MAY support a router acting as a Host.

The proposed paging concept does not have mobile routers.

9.6. Multiple Dormant Mode

Recognizing that there are multiple possible dormant modes on the Host, the IP paging protocol MUST work with different implementations of dormant mode on the Host.

The solution does not presently describe different dormancy modes however, using the ability of a MN to provide information to the PF

regarding its requirements for the dormancy either during the paging area update or explicit IP paging registration, such scenarios can be easily supported.

9.7. Independence of Mobility Protocol

Recognizing that IETF may support multiple mobility protocols in the future and that paging may be of value to hosts that do not support a mobility protocol, the IP paging protocol MUST be designed so there is no dependence on the underlying mobility protocol or on any mobility protocol at all. The protocol SHOULD specify and provide support for a mobility protocol, if the Host supports one.

The proposed paging concept does not depend on any existing mobility protocol to function. On the other hand, it can enhance existing mobility protocols. For instance, when the MN responds to a Paging Request message to its AR, it can include Binding Update as encapsulation in the Paging Response message. The Paging Response message can also include a request for transfer of network contexts from the MN's previous AR. Furthermore, our support for securing paging messages can be used for expedited network access authentication.

9.8. Support for Existing Mobility Protocols

The IP paging protocol MUST specify the binding to the existing IP mobility protocols, namely mobile IPv4 [2] and mobile IPv6 [3]. The IP paging protocol SHOULD make use of existing registration support.

The proposed paging concept works with Mobile IP. The PF can be co-located in any Mobility Agent, including the Foreign Agent. The Paging Registration message can be constructed as an extension to the Registration Request or a Binding Update message.

Furthermore, when the PF is realized in a Mobility Agent, the expiration of lifetime field in the binding cache can serve as a trigger for determining the implicit dormancy of the MN. For example, when PF is realized in a GMA, the GMA's regional binding cache can provide the input for determining the implicit dormancy of the MN.

9.9. Dormant Mode Termination

Upon receipt of a page (either with or without an accompanying L3 packet), the Host MUST execute the steps in its mobility protocol to re-establish a routable L3 link with the Internet.

When the MN wakes up, either due to entering a new IP-PA, the need to send IP packets or as a response to a page, the MN executes the steps in the mobility protocol and re-establishese a routable L3 link with the Internet. For instance, when the MN receives a router advertisement with paging extension as an L3 Paging Request message, one of the things the MN does is to formulate a new CoA and it could include the Binding Update in the Paging Response message as encapsulation.

9.10. Network Update

Recognizing that locating a dormant mode mobile requires the network to have a rough idea of where the Host is located, the IP paging protocol SHOULD provide the network a way for the Paging Agent to inform a dormant mode Host what paging area it is in and the IP paging protocol SHOULD provide a means whereby the Host can inform the Target Agent when it changes paging area. The IP paging protocol MAY additionally provide a way for the Host to inform the Tracking Agent what paging area it is in at some indeterminate point prior to entering dormant mode.

The proposed paging concept has the L3 procedure to update the paging function and all mobility agent 'above' the paging function when the MN changes the IP-PA.

9.11. Efficient Utilization of L2

Recognizing that many existing wireless link protocols support paging at L2 and that these protocols are often intimately tied into the Host's dormant mode support, the IP paging protocol SHOULD provide support to efficiently utilize an L2 paging protocol if available.

The proposed concept has been developed in order to work with all the currently known L2 paging mechanisms in the different link layer technologies. The concept allows access-independent L3 paging and optimized interworking with L2 paging . As an example, with the proposed model an IP dormant MN does not need to perform any L2 mobility signaling when moving within the same IP paging area. The concept minimizes impact on L2 paging and link layer technologies by allowing for IP paging signaling and advertisement of IP paging information through optimizations at L2 Moreover, it provides improvements in terms of power saving and minimization of mobility signaling with respect to the presence of L2 paging only.

9.12. Orthogonality of Paging Area Subnets

The IP paging protocol MUST allow an arbitrary mapping between subnets and paging areas.

The proposed paging concept does not associate the paging area and subnets. The proposed paging concept allows an IP-PA to have multiple subnet and each AR is allowed to belong to different types of IP-PA

9.13. Future L3 Paging Support

Recognizing that future dormant mode and wireless link protocols may be designed that more efficiently utilize IP, the IP paging protocol SHOULD NOT require L2 support for paging.

The concept does not require L2 support for paging and, thanks to the introduction of the IP paging Identity allow for future L3 paging only.

9.14. Robustness Against Failure of Network Elements

The IP paging protocol MUST be designed to be robust with respect to failure of network elements involved in the protocol. The self-healing characteristics SHOULD NOT be any worse than existing routing protocols.

The distributed and flexible location of paging function contributes to the robustness against failure of network elements.

9.15. Reliability of Packet Delivery

The IP paging protocol MUST be designed so that packet delivery is reliable to a high degree of probability. This does not necessarily mean that a reliable transport protocol is required.

The paging request will be resent if a response is not received after PAGE_RESPONSE_RX_TIME expires on the access network. The re-transmission are performed for at most PAGE_RQST_RE_TX number of times. When L2 Paging is initiated on the access link as a result of receiving an IP Paging request, we rely on the underlying L2 protocol to reliably page the MN.

9.16. Robustness Against Message Loss

The IP paging protocol MUST be designed to be robust with respect to loss of messages.

The paging message will be resent if it is not acknowledged. The reduction of the number of message during the IP dormant state naturally reduce the possibility of message lost

9.17. Flexibility of Administration

The IP paging protocol SHOULD provide a way to flexibly auto-configure Paging Agents to reduce the amount of administration necessary in maintaining a wireless network with paging.

The proposed paging concept can configure the paging function to be located in any mobility agent (another access router in the flat LMM or in any access router, any cross-over router or the GMA in the hierarchical MIPv6RR). Moreover, dynamic IP Paging Areas are supported, where the size and scope of the areas can be modified dynamically.

9.18. Flexibility of Paging Area Design

The IP paging protocol MUST be flexible in the support of different types of paging areas. Examples are fixed paging areas, where a fixed set of bases stations belong to the paging area for all Hosts, and customized paging areas, where the set of base stations is customized for each Host.

The proposed paging concept is flexible enough to accommodate the concept of hierarchical overlapping paging area and the paging area with multiple access technologies. Moreover, dynamic IP Paging Areas are supported, where the size and scope of the areas can be modified dynamically.

9.19. Availability of Security Support

The IP paging protocol MUST have available authentication and encryption functionality at least equivalent to that provided by IPSEC.

The proposed IP paging security solutions support authentication and encryption functionality, equivalent to that provided by IPsec

9.20. Authentication of Paging Location Registration

The IP paging protocol MUST provide mutually authenticated paging location registration to insulate against replay attacks and to avoid the danger of malicious nodes registering for paging.

The proposed paging concept provides mutual authenticated paging location registration (both Paging area update and Paging Area Response are authenticated) with anti replay attacks so the network can make sure the user is valid and the user can also make sure he is communication with the valid network

9.21. Authentication of Paging Area Information

The IP paging protocol MUST provide a mechanism for authenticating paging area information distributed by the Paging Agent.

Authentication of PAU and PAR prevent possible attacks from bogus paging area information. If the Paging Area information are incorrect, the PAR will tell the MN. In such case, PAR and PAU may still be sent unnecessarily over the access link. Authentication of the advertised paging area information would avoid that but there may be some issues with anti replay attacks if time stamps are not valid.

9.22. Authentication of Paging Messages

The IP paging protocol MUST provide a mechanism for authenticating L3 paging messages sent by the Paging Agent to dormant mode Hosts. The protocol MUST support the use of L2 security mechanisms so implementations that take advantage of L2 paging can also be secured.

L3 Paging messages sent by the Agent (IP Paging Request, Paging Area Response, etc.) are authenticated; and if L2 security is present, it will enhance the security level and make it even more difficult for an intruder to perform the desired type of attacks

9.23. Paging Volume

The IP paging protocol SHOULD be able to handle large numbers of paging requests without denying access to any legitimate Host nor degrading its performance.

The proposed paging concept can handle a large number of paging request without denying access to any legitimate Host nor degrading its performance. The limiting factor may be the L2 (wireless link)

10. References

[1] N. Asokan, Patrik Flykt, C. Perkins, and Thomas Eklund. AAA for ipv6 Network Access (work in progress). Internet Draft, Internet Engineering Task Force, March 2000.

[2] J. Kempf. Dormant mode host alerting (ip paging) problem statement. Request for Comments (Informational) 3132, Internet Engineering Task Force, June 2001.

[3] O. Levkowetz and et al. Problem description: Reasons for doing context transfers between nodes in an ip access network (work in progress). Internet Draft, Internet Engineering Task Force, February 2001.

[4] P. Mutaf, "IP Paging Security Requirements", Internet draft, Internet Engineering Task Force, May 2001

11. Authors' Addresses

Stefano M. Faccin
Mobile Networks Lab
Nokia Research Center
6000 Connection Drive
Irving, Texas 75039
USA
Phone: +1 972 894-4994
EMail: stefano.faccin@nokia.com
Fax: +1 972 894-4589

Rajeev Koodli
Communications Systems Lab
Nokia Research Center
313 Fairchild Drive
Mountain View, California 94043
USA
Phone: +1-650 625-2359
EMail: rajeev.koodli@nokia.com
Fax: +1 650 625-2502

Franck Le
Mobile Networks Lab
Nokia Research Center
6000 Connection Drive
Irving, Texas 75039
USA
Phone: +1 972 374-1256
EMail: franck.le@nokia.com
Fax: +1 972 894-4589

Jari T. Malinen
Communications Systems Lab
Nokia Research Center
313 Fairchild Drive
Mountain View, California 94043
USA
Phone: +1-650 625-2355
EMail: jmalinen@iprg.nokia.com
Fax: +1 650 625-2502

Rene Purnadi
Mobile Networks Lab
Nokia Research Center
6000 Connection Drive
Irving, Texas 75039
USA
Phone: +1 972 894-4897
EMail: rene.purnadi@nokia.com
Fax: +1 972 894-4589

12. Appendix A - Hierarchical Overlapping Paging Area Support

Functional model for overlapping PAs gives no indication on implementation or allocation of PFs to any specific node. According to different implementation options, PFs can be located all in the same node(i.e. same node acts as PF for more than one PA and more than one type of PA). No relation between PAs at different levels

Different mobile nodes/users have different traffic patterns and mobility patterns, e.g., some MNs generate very low traffic and stay dormant for long time (e.g. basic voice terminals that generate/receive few calls a day), others are very heavy on traffic (e.g. data MNs may be always on and receive/send data almost continuously). Based on the different behaviours, the relation between mobility procedures and IP Paging is different. For low traffic MN would make sense to use large IP-PA since, even if the MN moves a lot inside the IP-PA, the traffic patterns indicates that the MN will have to wake up and perform IP mobility procedure not very often. Although in this case IP paging will require multicast of paging messages to a larger area, there is however a large saving in terms of the IP mobility signalling in the network and on the radio link otherwise needed to keep track of the MN point of attachment.

For always-on terminals that are always in an IP session (i.e. they go dormant very rarely and only for very limited periods of time), it would make sense to consider small IP-PA or even rely only on L2 paging only when available. If the MN moves often, IP mobility procedures will be performed quite often but, when the MN needs to wake-up for incoming packets, paging has less impact in terms of latency in delivering the packets and in terms of signalling needed for paging.

This concept allows several types of IP-PA defined in the system, each type corresponds to a specific set of terminal capabilities/user

```
   +-----+    +-----+    +-----+         +-----+    +-----+    +-----+
   |     |    |     |    |     |         |     |    |     |    |     |
   | PF1 |    | PF4 |    | PF2 |         | PF6 |    | PF5 |    | PF3 |
   |     |    |     |    |     |         |     |    |     |    |     |
   +-----+    +-----+    +-----+         +-----+    +-----+    +-----+
       \         |          |                  |           |         /
   +----\ -------|----------|-----------------|-----------|--------/---+
   |     \        \         | IP-PA 1 Type 3            /        /    |
   |+-----\ -------\ --------\ ----+  +-----------------/--------/---+ |
   ||      \ IP-PA 1 Type 2   \    |  |        IP-PA 2 Type 2   /    | |
   || +-----\ ------- ---+ +---\ -------------+ +--------------/---+ | |
   || |  IP-PA1 Type 1   | |  IP-PA 2 Type 1  | |  IP-PA 3 Type 1  | | |
   || | +--+  +--+  +--+ | | +--+  +--+  +--+ | | +--+  +--+  +--+ | | |
   || | |AR|  |AR|  |AR| | | |AR|  |AR|  |AR| | | |AR|  |AR|  |AR| | | |
   || | +--+  +--+  +--+ | | +--+  +--+  +--+ | | +--+  +--+  +--+ | | |
   || +-----------------+ +-----------------+ +-----------------+ | |
   |+----------------------------+  +----------------------------+ |
   +---------------------------------------------------------------------+

                       |->|                    |->|                |-->
                        1                      1                   1
                                 |->|                               |-->
                                  2                                  2
                                                                      |-->
                                                                        3
   1 = MN "care for" PA Type1, perform "PA Update" in this cases
   2 = MN "care for" PA Type2, perform "PA Update" in this cases
   3 = MN "care for" PA Type3, perform "PA Update" in this case
```

Figure 8: Hierarchical Overlapping Paging Area

requirements/services being used by the user. For examples, IP-PA type 3 is for MNs with low traffic and long period of dormancy, IP-PA type 1 is for MNs with very brief periods of dormancy and almost continuous traffic. The choice of the PA Type most appropriate for the MN can be done in several ways:

The visited domain where the MN is roaming determines it based on the user profile and terminal capabilities, and indicates it to the MN. In such case, the MN may be indicated one or more PA types, and decision of which one to use at a certain point in time is based on MN status: if MN is inactive (no active sessions at all) MN can choose the PA Type that minimizes the need for mobility procedures; if MN is in active sessions for services that require continuous or frequent exchange of data (e.g. real-time multimedia services), MN choose the PA Type that allows the most precise tracking of the MN.

Or the MN itself makes the selection based on user preferences, user profile, services currently used, etc. Other cases are possible

Each access router "broadcasts" the IP-PA identifier(s) for the IP-PA(s) it belongs to. Each Access Router may belong to one or more IP- PAs, but one AR belongs to only one IP-PA of a specific type. E.g. if the AR belongs to three IP-PAs, it will broadcast three different IP-PA identifiers

The IP-PA identifier(s) must be broadcasted by the AR in such a way that the MNs can easily determine what types of IP-PA are supported and their identifiers. Several solutions are available. Also IP-PA types need to be standardized to guarantee inter-operation at roaming. The number of types of paging areas in a given network can be dynamic, i.e. it does not need to be mandated by the standards. E.g. this means that, if the standard defines 10 types of IP-PAs, a given network may adopt only 2