Internet-Draft   X. Chen

Expires: August 2007   Orange PCS Ltd

                                                                        J. Rinne

Nokia

                                                                        J. Wiljakka

Nokia

                                                                    January 2007

Problem Statement for MIPv6 Interactions with GPRS/UMTS Packet Filtering
draft-chen-mip6-gprs-07.txt

Status of this Memo

   Abstract

      This document provides an analysis of certain inter-working problems
      between IPv6 nodes running Mobile IPv6, at least one of which is
      connected to a Third Generation Partnership Project (3GPP)
      specified General Packet Radio Service/Universal Mobile Tele-
      communications System (GPRS/UMTS) network. The inter-working
problems

are caused by some specific packet filtering operations at the edge
of the GPRS/UMTS network which are applied to control access to the
GPRS/UMTS services and network resources. However, we believe that
other scenarios may exist in which similar packet filtering
operations may be applied and that similar problems would arise in
these more general scenarios.

The GPRS Gateway Support Node (GGSN) checks the source address or
the destination address in the basic IPv6 header of incoming or
outgoing IP datagrams against a set of packet filtering information
established during the GPRS/UMTS session set-up. The packet
filtering
information remains stable during the sessions and independent of
Mobile IP. When MIPv6 is activated by either end of the IPv6 mobile
nodes, the packet filtering will fail to perform properly and
subsequently block the traffic due to the mismatch between the
packet
filters and the current source address or destination address in the
basic IPv6 header of the IP datagrams to and from the IPv6 mobile
nodes.

Table of Contents

1. Introduction

Mobile IPv6 [1] allows a mobile node to maintain its IP connectivity regardless of its network attachment point. Packets sent to the mobile node may still use its home address, or the care-of address of the mobile node as the destination address. The mobile node may continue to communicate with its existing communication peers (stationary or mobile) by using its topologically correct IP addresses. An important and highly desirable feature of mobile IP based mobility is that the control is transparent to transport and higher-layer protocols and applications, i.e. the higher layer protocols and applications function as if the mobile node is "stationary".

Packet filtering in GPRS/UMTS [2] is used for differentiating GPRS/UMTS connections and Quality of Service (QoS), and protecting the network resources and services against Theft of Service attacks. It is achieved by checking the header information of the incoming and outgoing IP datagrams against a set of packet filtering information. The packet filtering information is defined or authorised by the application layer entities during the set-up of the GPRS/UMTS and IP Multimedia Subsystem sessions operating independently of Mobile IP. This pre-defined packet filtering information is used by the GGSN to check the header of incoming or outgoing IP datagrams so as to select the appropriate GPRS/UMTS sessions with QoS or control the access to network resources and IMS services based on the operator defined local policies. For example, the Service Based Local Policy control (SBLP) [5][6] in UMTS IP Multimedia Subsystems (IMS)[4] enables the GGSN to check the destination address for outgoing IP datagrams according to policy information authorised by the Policy Decision Function during the IMS session establishment.

When Mobile IPv6 is activated, an IPv6 node sends IP datagrams using Care-of Address as either the destination address or source address while its home address is carried in the extension headers. The change of source address or destination address in the basic IPv6 header from the mobile node's home address to its care-of address or from one care-of address to another during a session leads to a mismatch with the header information such as the source address or destination address in the set of parameters for packet filtering information and, as a result, the discard of incoming or outgoing IP datagrams by the GGSN.

In the following sections, the basic packet filtering operations in

GPRS/UMTS are described and followed by the analysis of the failure
of those operations when Mobile IPv6 is activated.

1.1 Scope of this Document

This document provides information about the potential problems for
mobile terminals to use Mobile IPv6 when at least one of them
is connected to the GPRS/UMTS networks. It analyses the scenarios
when Mobile IPv6 is applied and how the problems occur.

Similar problems may also exist in CDMA2000 as defined by 3GPP2
and other Internet technologies such as firewalls. But the
discussions in this document are intended to apply to 3GPP compliant
GPRS/UMTS networks.

1.2 Abbreviations

3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project Two
GGSN	Gateway GPRS Support Node (default router for 3GPP User Equipment)
GPRS	General Packet Radio Service
IMS	IP Multimedia (Core Network) Subsystem, 3GPP Release 5 IPv6-only part of the network
NSIS	Next Steps In Signalling
PDP	Packet Data Protocol
RSVP	Resource Reservation Protocol
SIP	Session Initiation Protocol
SBLP	Service Based Local Policy
TFT	Traffic Flow Template
UE	User Equipment, for example a UMTS mobile handset
UMTS	Universal Mobile Telecommunications System

2. Terminology

  GPRS services those services provided or accessed by the GPRS/UMTS
           networks. They can be a single media service with one
           traffic flow or a multimedia service with several
           traffic flows.

  IMS Services   those services provided by the IP Multimedia (Core
           Network) Subsystems (IMS). They are distinguished
           from the general GPRS Services as defined above in
           that the latter are not provided by the IMS.

3. Packet Filtering in 3GPP Networks

     The following sections list some packet filtering operations in
GPRS/

UMTS. It is not intended to exhaust all the possible application
scenarios for packet filtering operations in 3G networks such as
those used by firewalls.

3.1 Mobile Terminal Defined Packet Filtering for GPRS Services

The GPRS Services are defined to be those services that are not run
on the IP Multimedia Subsystem (IMS) [4]. IMS is defined by 3GPP to
provide SIP Based IP multimedia services. To support GPRS services
with more than one traffic flow with differentiated QoS, GPRS/UMTS
networks support multiple simultaneous sessions as typically
represented by multiple secondary PDP (Packet Data Protocol)
Contexts[2] in association with one Primary PDP Context for each of
its IP address. Each GPRS/UMTS session may be assigned specific QoS
with the necessary network resources (including radio resources).
An
incoming IP datagram from the external public data network such as
Internet will be checked by the GGSN, to decide if there is an
existing GPRS/UMTS session to deliver the datagram through the
network to the mobile terminal.   The basic IPv6 header as well as
some higher layer information such as the ports is checked against a
Traffic Flow Template (TFT) [3] that contains the packet filtering
information such as the IPv4/IPv6 Source Addresses, Protocol
Identifier, Source/Destination Ports, etc.

The TFT is generated by the mobile node and recorded by the GGSN
upon
a successful establishment of a GPRS/UMTS session for the mobile
node. The TFT only applies when secondary PDP contexts are
activated
in which case only one PDP context among both the primary PDP
context
and secondary PDP context(s) is allowed not to have a TFT associated
with it.

The GGSN will use at least one of those packet filter parameters
defined in the TFT, primarily the Source Address, to check if an
appropriate GPRS/UMTS session has been set up for incoming traffic.
The GGSN searches for a GPRS/UMTS session with the TFT that
contains
the parameter values matching those carried in the datagram. For
example, the Source IP Address field of each existing TFT will be
compared with the source address carried in the basic IPv6 header of
an IPv6 datagram. If no matching TFT is found, the datagram may be
discarded.

3.2 Mobile Terminal Defined Packet Filtering for IMS Services

For a UE running IMS Services, the GGSN ignores any UE supplied TFT.
The filters in that TFT are not installed in the packet processing
table at the GGSN. The packet filtering for IMS services is based
on the Service Based Local Policy as discussed in the next section.

3.3 Network Service Defined Packet Filtering for IMS Services

      In IMS, Service Based Local Policy (SBLP) [5][6] is enforced by the
      GGSN to authorise and control the access to the IMS services and
the
      GPRS/UMTS network resources based on operator defined local
policies.
      The SBLP can be applied to both the traffic leaving the GPRS/UMTS

networks (uplink) and the traffic entering the GPRS/UMTS network
(downlink).

An IMS service request, a GPRS/UMTS session set-up request and the
subsequent data packets originated by the mobile terminal will be
checked by the GGSN against a set of policy control information
parameters such as Destination Address, Destination Port Number,
Transport Protocol ID, etc. The policy control information is issued
as an authorisation from the IMS application layer (the IMS/Policy
Decision Function -PDF). An IP datagram carrying an IMS service
request or user data will be blocked by the GGSN if mismatch is
found
between the authorised policy information and those carried by the
IP
datagram. For example, an IMS service request or a VoIP packet will
be blocked by the GGSN if the destination address carried by the IP
datagram does not match that authorised by the Policy Decision
Function. This is designed for protecting GPRS/UMTS and IMS against
ToS attacks.

4. Problem statement

The problem is stated in terms of an IPv6 node, A, communicating
with a second IPv6 node, B. B is connected to the GPRS/UMTS network.
The Internet or IP networks are between A's local network and B's
GPRS/UMTS network.

We consider in turn the cases in which the GPRS node, B, is acting
either as a Correspondent Node or as a Mobile Node. For each case,
we consider sub-cases related to terminal defined filters
(i.e. TFTs) and network defined filters (i.e. SBLP).

Further, for each sub-case, we further consider the use of Home
Agent
tunnelling and Route Optimisation by the Mobile Node.

4.1 GPRS node, B, acting as Correspondent Node

This is the case where A is a Mobile Node that is having multimedia
sessions with a Correspondent Node, B. B is connected to a GPRS/UMTS
network. The sessions are set up when A is connected to its home
network link.

4.1.1 Mobile Terminal defined Packet Filtering for GPRS Services

Upon a successful establishment of multimedia sessions between A and
B, each session is associated with a TFT packet filter(s) defined
by

B which have A's home address as the source address for IP
datagrams
           sent from A to B. The GGSN uses these packet filters to decide which
           PDP Context to use to deliver an incoming IP datagram to B.

4.1.1.1 Home Agent Tunnelling

The IP datagrams sent from A to B use the (reverse) tunnel from A's
current CoA to its HA. IP datagrams exit the tunnel at A's home
agent
and transmit to B using A's home address as the source address.
Upon
arriving at the GGSN, the IP datagrams' source address matches the
IPv6 source address (A's home address) recorded in one of the TFT
filters and, if other filtering parameters are matched as well, the
IP datagrams will be delivered to B through the PDP Context
corresponding to the TFT. No specific issues are identified for this
case.

4.1.1.2 Route Optimisation

When A moves away from its home network link and connects to a
foreign network link and attempts the Mobile IPv6 binding update
procedures, it starts sending IP datagrams to B directly using its
CoA address as the Source Address and carrying its Home Address in
the Home Address destination option extension header.

When such an IP datagram sent from A arrives at the GGSN, it does
not
match the TFT packet filters containing A's home address as the
IPv6
source address. As result, two possible decisions can be made by the
GGSN; If there happens to be a different PDP Context with a TFT
which
does match A's CoA or a PDP Context without an associated TFT, the
GGSN will decide to use it to deliver the IP datagram to B. But in
this case it may not receive the correct Quality of Service
treatment. Additionally, the PDP Context with the Quality of Service
appropriate for delivering the IP datagram is left unused.

Figure 1 shows an example of two GPRS sessions that are
distinguished
by GGSN using TFT packet filters, TFT1 and TFT2,respectively.

```
                                       TFT      +--------+
                                      Packet  /           \  CN
       MN                             Filter / TFT1->Sess.1 \+--+
      +-+   +---------+   +--------+   +----+/----->----------|B |
      |A|->-| Foreign |->-|Internet|->-|GGSN| ----->----------|  |
      | |   | Network |   +--------+   +----+\  TFT2->Sess.2  +--+
      +-+   +---------+       |              \           /
                             |               \         /
                             |                +----------+
```

```
                           |
          /\               |
          ||               |
          ||               |
    +---------+            |
    | Home    |------------+
    | Network |
    +---------+
```
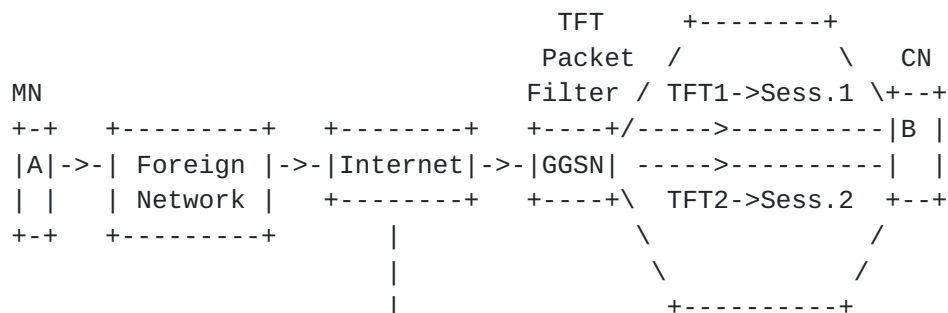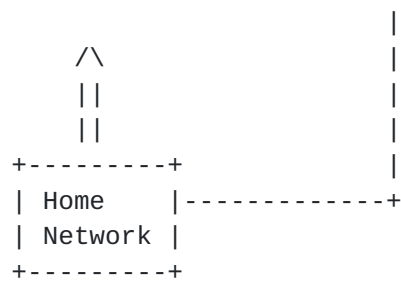
Figure 1. Route Optimization with TFT-based Packet Filtering in GGSN

Alternatively the GGSN will discard the IP datagram if all sessions have TFTs and none of them match the incoming packet.

The first IP datagram sent out by A will carry the Care-of Test Init message of the Return Routability Procedure. If this message is dropped, then Route Optimisation will not complete, and IP datagrams from A to B will continue to be routed via the Home Agent instead (see Section 4.1.1.1).

If, instead, this message is delivered to B by the GGSN, the Return Routability procedure may complete and subsequent datagrams will be routed in the same way as the Care-of Test Init. The session with optimised route from A to B will therefore continue.

The major problem is then that the IP datagrams will not receive the correct Quality of Service treatment. Since UMTS Quality of Service can involve small constant bit-rate bandwidth reservations, this can cause a complete loss of service, if the incorrect QoS treatment involves a path with too low a bandwidth or no bandwidth guarantee at all.

In addition, extra complexity or even difficulties will be incurred in the system with respect to PDP Contexts and network resources, especially, the radio resources, that remain unused but are being paid for by the user.

4.1.2 Network Service defined Packet Filtering for IMS Services

4.1.2.1 Home Agent tunnelling

We have not identified any issues with this case, for the same reason as discussed in Section 4.1.1.1.

4.1.2.2 Route Optimisation

When IMS multimedia sessions are set up between A and B, the SBLP Policy Control authorises IP datagrams to be sent from B to A's home address using assigned GPRS/UMTS network resources and the associated QoS. When A moves away from its home network link and connects to foreign network link, Mobile IPv6 Route Optimisation may be used to allow B to continue sending IP datagrams to A by using A's CoA.

Upon arrival at the GGSN, they will not match the SBLP filter for the session which is authorised only for destination equal to A's home address. SBLP filters are associated with the particular UMTS QoS reservation (PDP Context) for the session. If B continues to use

this QoS reservation for these packets, the GGSN will drop them as
they do not match the filter.

Figure 2 shows an example of SBLP packet filtering for IP datagrams
sent from B through IMS sessions, 1 and 2, to A.

```
                                   +----------+
                                   |   SBLP   |
                                   | Control  |
                                   | Function |
                                   +----------+
                                        |      +----------+
                                        |     /            \    CN
MN                                      |    / IMS Sess. 1  \ +--+
+-+   +---------+   +--------+   +----+/-----<----------  |B |
|A|---| Foreign |---|Internet|---|GGSN| -----<----------  |  |
| |   | Network |   +--------+   +----+\  IMS Sess. 2   /+--+
+-+   +---------+        |             \              /
                        |              \            /
                        |               +----------+
                        |
 /\                     |
  ||                    |
  ||                    |
     +--------+         |
     |  Home  |--------+
     | Network|
     +--------+
```

Figure 2. Route Optimization with SBLP-based Packet Filtering in
GGSN

In practice, as discussed in Section 4.1.1.2, the Return Routability
procedure requires that there is a route for the Care-of Test Init
message from A to B. A route from B to A for the Care-of Test itself
is also required.

The means by which outgoing MIP control packets are allocated to QoS
reservation on the PDP Context by the UE are undefined in 3GPP, but
we note that such a message would not pass the SBLP filters (as
described above).

If the message is routed (i.e. on a different QoS reservation), then
Route Optimisation can be established with the consequences as
described above.

Similar considerations to those of Section 4.1.1.2 apply to IP
datagrams sent from A to B.

4.2 GPRS node, B, acting as Mobile Node

This is the case where the GPRS node, B, is acting as MIPv6 Mobile
Node and has a live session such as VoIP with a Correspondent Node,
A. The MN, B, connects to the GPRS network after leaving either a
GPRS network or non-GPRS network. Therefore, the current GPRS
network
is NOT taken to be B's home network but a foreign network.

4.2.1 Mobile Terminal defined Packet Filtering for GPRS Services

4.2.1.1 Home Agent Tunnelling

When B moves away from its home network link and connects to GPRS
network link, a PDP Context is set up and associated with a TFT
filter containing A's address as the Source Address for IP datagrams
sent from A to B.

Figure 3 shows an example of two PDP Contexts representing two GPRS
sessions, 1 and 2, that are distinguished by GGSN using TFT
filters,
TFT1 and TFT2, for incoming IP datagrams to be delivered to B.

```
                                        TFT      +--------+
                                       Packet  /          \
                                       Filter /            \ MN
                                       +------+ TFT1-Sess.1+---+
                                *****|        |---->-------|   |
                                +-->--| GGSN |             | B |
                                |*****|        |---->-------|   |
        CN     +-------+        |       +------+ TFT2-Sess.2+---+
       +---+   | Local |    +--------+ |          \   GPRS   /
       | A |->-|Network|->-|Internet|==            \ Network /
       +---+   |   A   |    +--------+ |              +--------+
               +-------+               |
                                       |           +------+
                                       |           | Home |         /\
                                       |...********|+----+|         ||
                                       +-------<---|| HA ||         ||
                                        ...********|+----+|
                                                   | Net- |
                                                   | work |
                                                   +------+
```
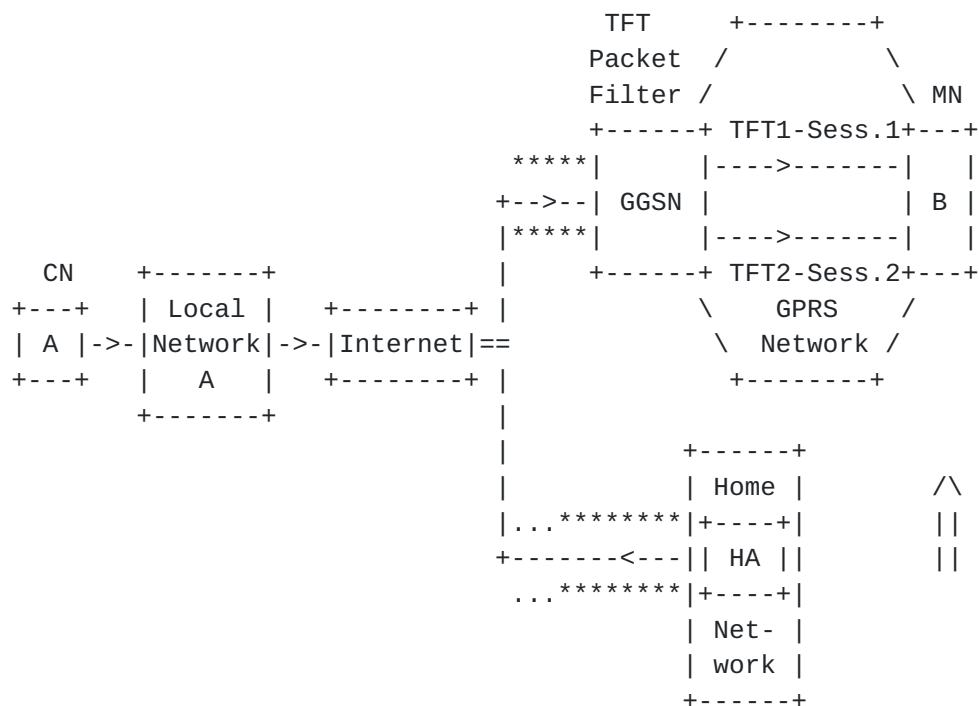
Figure 3. HA Tunnelling with TFT-based Packet Filtering in GGSN

The IP datagrams sent from A to B may use Home Agent Tunnelling from
B's Home Agent to its current CoA. The IP datagrams tunnelled from
B's Home Agent to B's CoA have the Home Agent address as the source
address in the outer header, while the TFT filter associated with
the
existing session has A's address as the Source Address. When the IP
datagrams arrive at the GGSN, the source address in the outer header
does not match the Source Address in the TFT template associated
with
the session. As a result, the IP datagrams may be discarded by the
GGSN or provided with incorrect QoS treatment.

4.2.1.2 Route Optimisation

For the Return Routability Procedure to complete, there needs to be
a route from HA to B to deliver the Home Test messages. If no
matching TFT is found by the GGSN for the tunnelled Home Test
Messages and the GGSN chooses to drop the message, the Return
Routability procedure will fail and, as a result, the Route
Optimisation will not take place.

If tunnelled packets are routed at all from the Home Agent to B,
then
the Return Routability procedure can complete successfully.

Packets from A are then sent directly to B's Care-of Address. These
will be correctly filtered by the TFTs and then delivered through
the
corresponding PDP Context to B.

4.2.2 Network Service defined packet filtering for IMS Services

4.2.2.1 Home Agent Tunnelling

When B moves away from its home network link and connects to a GPRS
network, it requests and acquires an IMS session with terminal A
with
authorised SBLP information containing A's address as the
Destination
Address for IP datagrams sent from B to A.

When Home Agent Tunnelling operation mode is used, B uses a
(reverse) tunnel from its CoA to its Home Agent to send IP datagrams
to A. In the reverse tunnel, the IP datagrams tunnelled from B
carry
its Home Agent address as the destination.

Figure 4 shows an example of two IMS sessions, each of which is
associated with a SBLP filter, SBLP1 and SBLP2, for IP datagrams to

be sent to the authorised destination, i.e. A's address.

When the IP datagrams in an IP-in-IP tunnel arrive at the GGSN, GGSN
will find no authorised SBLP matching the destination indicated by
the outer header of the tunnelled IP datagrams, and it will block
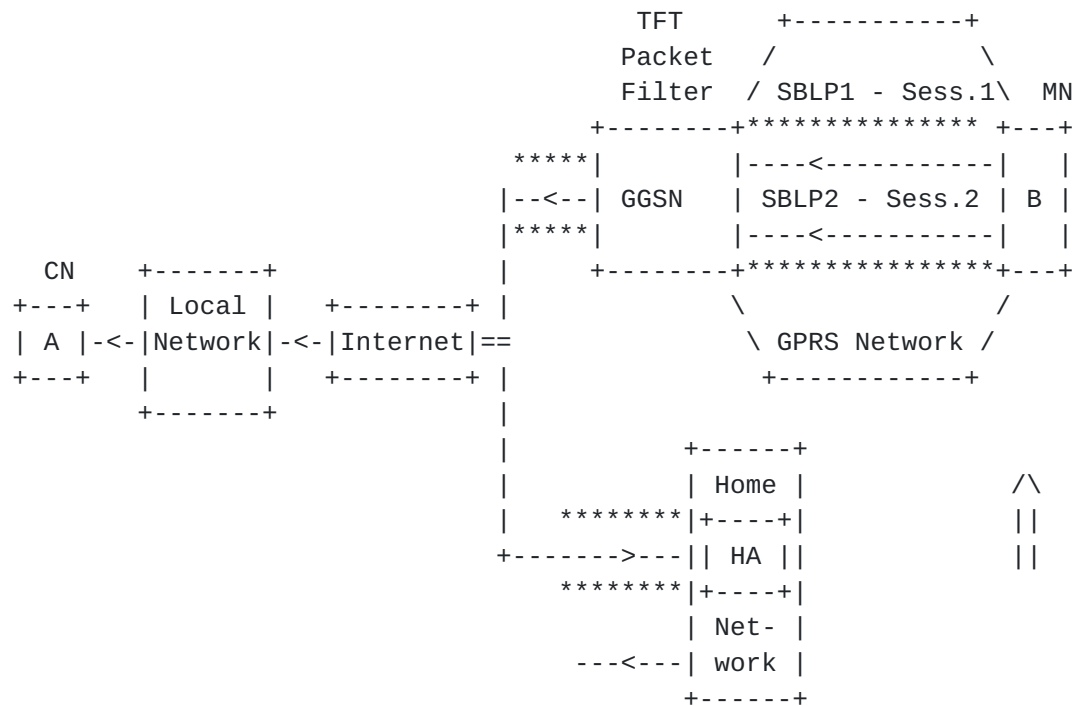and drop them.

```
                                       TFT        +-----------+
                                      Packet   /               \
                                      Filter  / SBLP1 - Sess.1\  MN
                                   +--------+*************** +---+
                               *****|         |----<-----------|   |
                               |--<--| GGSN    | SBLP2 - Sess.2 | B |
                               |*****|         |----<-----------|   |
       CN      +-------+        |     +--------+***************+---+
      +---+    | Local |  +--------+ |          \                 /
      | A |-<-|Network|-<-|Internet|== \ GPRS Network /
      +---+    |       |  +--------+ |          +------------+
            +-------+                |
                                     |     +------+
                                     |     | Home |            /\
                                     |   ********|+----+|          ||
                               +------->---|| HA ||          ||
                                     ********|+----+|
                                           | Net- |
                                       ---<---| work |
                                             +------+
```

            Figure 4. HA Tunnelling with SBLP-based Packet Filtering in GGSN

        4.2.2.2 Route Optimisation

           When Route Optimisation is used, IP datagrams from A to B (and B to
           A) use B's Care-of Address as destination (resp. source) and
           therefore will not match any of the established SBLP filters. This
           is because the pre-established SBLP filters authorise IP datagrams
           sent to B's Home Address to enter the GPRS/UMTS network. These will
           be either blocked or carried with inappropriate QoS treatment.

           The Figure 5 shows an example of filtering IP datagrams
           sent from A directly to B using route optimisation passing an SBLP
           filter SBLP1 or SBLP2. Both authorise the use of IMS sessions and
           associated network resources to deliver IP datagrams to B's home
           address.

           Depending on the policy applied to packets which do not match the
           SBLP filters, the Return Routability procedure may not complete.
This
           is because the SBLP filters, SBLP1 and SBLP2, authorise IP datagrams
           sent to B's Home Address for accessing GPRS network resources and
           IMS services. The 'Care of Test' message in response to the 'Care
of
           Test Init' message from B uses B's Care-of Address as the
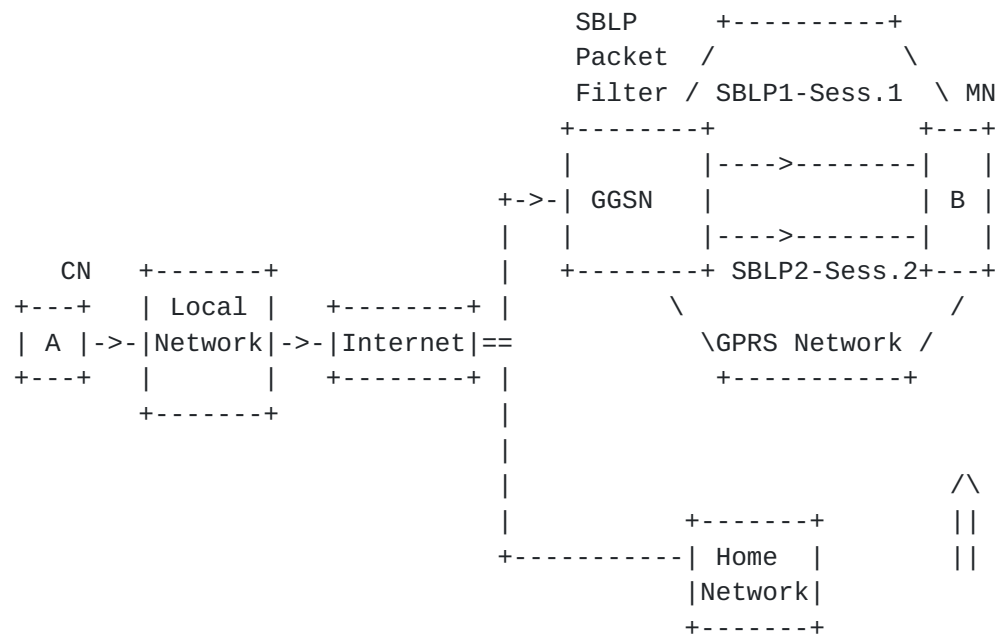   destination address.

```
                                          SBLP      +----------+
                                          Packet  /            \
                                          Filter / SBLP1-Sess.1 \ MN
                                         +--------+              +---+
                                         |        |---->--------|   |
                                     +->-| GGSN   |             | B |
                                     |   |        |---->--------|   |
              CN     +-------+       |   +--------+ SBLP2-Sess.2+---+
          +---+    | Local |    +--------+ |           \              /
          | A |->-|Network|->-|Internet|==          \GPRS Network /
          +---+    |       |    +--------+ |            +----------+
               +-------+              |
                                      |
                                      |                        /\
                                      |         +-------+       ||
                                      +-----------| Home  |       ||
                                                  |Network|
                                                  +-------+
```

       Figure 5. Route Optimization with SBLP-based Packet Filtering in GGSN

   4.3 Summary

       GPRS Services will be disrupted when a GPRS mobile terminal
       have multiple secondary PDP Contexts to communicate with a
       mobile node which changes its network attachment point and starts
       using Mobile IPv6 route optimisation. This will also happen
       when the GPRS mobile terminal that is having more than one GPRS
       session with a mobile node leaves its home network, enters GPRS
       network and starts using mobile IPv6 home agent tunnelling or
       route optimisation.

       IMS services will be disrupted when a mobile node that is having
       an IMS session with a GPRS mobile terminal changes its network
       attachment point and starts using mobile IPv6 route optimisation.
       This will also happen when the GPRS mobile terminal that is having
       an IMS session with a mobile node leaves its home network, enters
       the GPRS/UMTS network and starts using mobile IPv6 home agent
       tunnelling or route optimisation.

    5. Problem generalisation

       Although the description above is presented in terms of GPRS-
specific
       mechanisms for installing packet filters in the network. More
general
       situations may exist in which such filters are installed. This may

give rise to similar problems [9].

In the analysis above, we classify the filters as mobile terminal defined and network service defined. This represents the source of the information within the filters.

An example of a 'terminal defined' filter in the network is a filter installed as a result of RSVP (or in future NSIS protocols). Such filters determine the QoS treatment that will be applied to packets according to the user's request and are therefore very similar to Traffic Flow Templates.

An example of a 'network service defined ' filter would be one installed through policy mechanisms. In this case it is in order to apply appropriate network policy that packets filtered.

6. Security Considerations

6.1 User security considerations

No user security issues have been identified.

6.2 Network security considerations

In the case of network service defined filters (e.g. Service Based Local Policy), the purpose of the filters is to ensure that appropriate network policy for controlling access to network resources and services is applied to the packets.

The problems described in this paper do not themselves represent security issues for the network (for example users circumventing the network's policy). Indeed, the problems arise largely because the policies cause packets to be dropped, or treated according to a different policy which explicitly allows those packets to pass.

However, care must be taken in considering solutions to these problems which cause modification of the network's policies. Such modification will necessarily be caused by the mobility event at one or other user. These events can easily be faked by users.

For example, IP address spoofing could be used to convince the network that a user has moved when in fact they have not. Collaborating users could convince the network that a user has moved, when in fact the new address belongs to a different host.

7. Acknowledgements

The authors would like to thank Paul Reynolds, Ric Bailey, Ronan Le Bras, Graham Fisher, Stuart Shutt, Steve Blythe and Rob Allan for

their constant and valuable support for the work.

References

Normative:

[1]   Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in
      IPv6", RFC3775, June 2003.

[2]   3GPP, "3rd Generation Partnership Project; Technical
      Specification Group Services and System Aspects; General Packet
      Radio Services (GPRS); Service Description; Stage 2", 3GPP TS
      23.060.

[3]   3GPP, "3rd Generation Partnership Project; Technical
      Specification Group Core Network; Mobile Radio Interface Layer
      3 Specifications; Core Network Protocols - Stage 3", 3GPP TS
      23.008.

[4]   3GPP, "3rd Generation Partnership Project; Technical
      Specification Group Services and System Aspects; IP Multimedia
      Subsystem (IMS); Stage 2", 3GPP TS 23.228.

[5]   3GPP, "3rd Generation Partnership Project; Technical
      Specification Group Services and System Aspects; End-to-end
      Quality of Service; Concept and Architecture", 3GPP TS 23.207.

[6]   3GPP, "3rd Generation Partnership Project; Technical
      Specification Group Core Network; Policy Control over Go
      Interface", 3GPP TS 29.207.

[7] Bradner, S.:IETF Rights in Contributions, RFC3667, February 2004

[8] Bradner, S.: Intellectual Property Rights in IETF Technology,
    RFC 3668, February 2004.

[9] Le, F. et al.: Mobile IPv6 and Firewalls: Problem Statement,
    RFC4487 May 2006.

Authors' Addresses

    Xiaobao Chen
    Orange PCS Ltd.
    Keypoint
    St. James Court, Almondsbury Park
    Bradley Stoke
    Bristol BS32 4QJ
    UK

    Phone: +44 7989 477679
    Email: xiaobao.chen@orange-ftgroup.com

    Janne Rinne
    Nokia
    Visiokatu 3
    Tampere, FIN-33720
    Finland

    Phone: +358 7180 40995
    Email: janne.rinne@nokia.com

    Juha Wiljakka
    Nokia
    Visiokatu 3
    Tampere, FIN-33720
    Finland

    Phone: +358 7180 48372
    Email: juha.wiljakka@nokia.com

Intellectual Property Statement

    The IETF takes no position regarding the validity or scope of any
    intellectual property or other rights that might be claimed to
    pertain to the implementation or use of the technology described in
    this document or the extent to which any license under such rights
    might or might not be available; neither does it represent that it
    has made any effort to identify any such rights. Information on the
    IETF's procedures with respect to rights in standards-track and
    standards-related documentation can be found in BCP-11. Copies of
    claims of rights made available for publication and any assurances
of
    licenses to be made available, or the result of an attempt made to
    obtain a general license or permission for the use of such
    proprietary rights by implementers or users of this specification
can
    be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any
copyrights, patents or patent applications, or other proprietary
rights which may cover technology that may be required to practice
this standard. Please address the information to the IETF Executive
Director.

Full Copyright Statement

Acknowledgement