CONEX WG
Internet-Draft
Intended status: Informational
Expires: January 10, 2013

D. Kutscher
F. Mir
R. Winter
NEC
S. Krishnan
Y. Zhang
Ericsson
CJ. Bernardos
UC3M

July 9, 2012

Mobile Communication Congestion Exposure Scenario
draft-ietf-conex-mobile-00

Abstract

This memo describes a mobile communications use case for congestion exposure (CONEX) with a particular focus on mobile communication networks such as 3GPP Evoled Packet System (EPS). The draft provides a brief overview of the architecture of these networks (both access and core networks), current QoS mechanisms and then discusses how congestion exposure concepts could be applied. Based on this, this memo suggests a set of requirements for CONEX mechanisms that particularly apply to mobile networks.

Table of Contents

1. Introduction

Mobile data traffic continues to grow rapidly. The challenge wireless operators face is to support more subscribers with higher bandwidth requirements. To meet the bandwidth demand, there is a need for new technologies that assist the operators in efficiently utilizing the available network resources. Two specific areas where such new technologies could be deemed useful are resource allocation and flow management. Analysis of widely available statistics for network traffic from cellular networks are available, reveals that most flows are short-lived and low-volume, but there a few large flows that constitute a large part of the overall traffic volume. Measurements have also shown that a small number of users is responsible for the majority of traffic in cellular networks. In view of such highly skewed user behavior and limited and expensive resources (Wireless Spectrum), resource allocation and usage accountability are two important issues for operators to solve in order to achieve a better and fair network resource utilization. CONEX, as described in [I-D.ietf-conex-concepts-uses], is a technology that can be used to do so.

The CONEX congestion exposure mechanism is intended as a general technology that could be applied as a key element of congestion management solutions in a variety of use cases. The IETF CONEX WG will however work on a specific use case, where the end hosts and the network that contains the destination end host are CONEX-enabled but other networks need not be.

A specific example of such a use case can be a mobile communication network such as a 3GPP Evolved Packet System (EPS) network, where UEs (User Equipment, i.e. mobile end hosts), servers and caches, the access network and possibly an operator's core network can be CONEX-enabled. I.e., hosts support the CONEX mechanisms, and the network provides policing/auditing functions at its edges.

This document provides a brief overview of the architecture of such networks (access and core networks), current QoS mechanisms and then discusses how congestion exposure concepts can benefit such networks and how they should be applied. Using this use case as a basis, a set of requirements for CONEX mechanisms are described.

2. Overview of 3GPP's Evolved Packet System (EPS)

This section provides an overview of 3GPP's "Evolved Packet System" (EPS [3GPP.36.300]) as a specific example of a mobile communication architecture in order to illustrate congestion exposure applicability in this memo. There are other mobile communication architectures.

The EPS architecture and its standardized interfaces are depicted in Figure 1. The EPS provides IP connectivity to user equipment (UE) (i.e., mobile nodes) and access to operator services, such as global Internet access and voice communications. The EPS comprises the radio access network called evolved UMTS Terrestrial Radio Access Network (E-UTRAN) and the core network called Evolved Packet Core (EPC). QoS is supported through an EPS bearer concept, providing hierarchical bindings within the network.

The evolved NodeB (eNB), the Long Term Evolution (LTE) base station, is part of the access network that provides radio resource management, header compression, security and connectivity to the core network through the S1 interface. In an LTE network, the control plane signaling traffic and the data traffic are handled separately. The eNBs transmit the control traffic and data traffic separately via two logically separate interfaces.

The Home Subscriber Server, HSS, is a database that contains user subscriptions and QoS profiles. The Mobility Management Entity, MME, is responsible for user authentication, bearer establishment and modification and maintenance of the UE context.

The Serving gateway, S-GW, is the mobility anchor and manages the user plane data tunnels during the inter-eNB handovers. It tunnels all user data packets and buffers downlink IP packets destined for UEs that happen to be in idle mode.

The Packet Data Network (PDN) Gateway, P-GW, is responsible for IP address allocation to the UE and is a tunnel endpoint for mobility protocols. It is also responsible for charging, packet filtering, and policy-based control of flows. It interconnects the mobile network to external IP networks, e.g. the Internet.

In this architecture, data packets are not sent directly on an IP network between the eNB and the gateways. Instead, every packet is tunneled over a tunneling protocol - the GPRS Tunneling Protocol (GTP [3GPP.29.060]) over UDP/IP. A GTP path is identified in each node with the IP address and a UDP port number on the eNB/gateways. The GTP protocol carries both the data traffic (GTP-U tunnels) and the control traffic (GTP-C tunnels [3GPP.29.274]). Alternativly Proxy Mobile IP (PMIPv6) is used on the S5 interface.

The above is very different from an end-to-end path on the Internet where the packet forwarding is performed at the IP level. Importantly, we observe that these tunneling protocols give the operator a large degree of flexibility to control the congestion mechanism incorporated with the GTP/PMIPv6 protocols.

```
                                                      +-------+
                             +-------+                | PCRF  |
                             |  HSS  |               /+-------+\
                             +-------+            Gx/           \Rx
                                 |                 /             \
                                 |                /               \
                                 |          +-------+    SGi  +-------+
                                 |          |  P-GW |=========|   AF  |
                                 |          +-------+         +-------+
   HPMN                          |              |
   ------------------------------|--------------|----------------------
   VPLMN                         |              |
                             +-------+          |
                             |  MME  |          |
                            /+-------+\         |S8
                    S1-MME /           \        |
                          /             \S11    |
                         /               \      |
                 +-----------+            \     |
   +----+ LTE-Uu |           |             \    |
   | UE |========|           |    S1-U      +-------+
   +----+        |  E-UTRAN  |==============| S-GW  |
                 |   (eNBs)  |              +-------+
                 |           |
                 +-----------+
```

Figure 1: EPS (non-roaming) architecture overview

3. CONEX Use Cases in the Mobile Communication Scenario

In general, quality of service and good network resource utilization are important requirements for mobile communication network operators. Radio access and backhaul networks are considered scarce resources, and bandwidth (and radio resource) demand is difficult to predict precisely due to user mobility, radio propagation effects etc. Hence today's architectures and protocols go to significant extent in order to provide network-controlled quality of service -- for instance by 3GPP's EPS bearer model that enables the network to allocate service data flows (SDFs) to certain EPS bearers with specific quality of service classes (which can be used for fine-granular per-application service differentiation).

In the following, we discuss ways how congestion exposure could be beneficial for supporting resource management in such mobile communication networks. [I-D.ietf-conex-concepts-uses] describes fundamental congestion exposure concepts and a set of use cases for applying congestion exposure mechanisms to realize different traffic

management functions, accounting etc. Here, we relate these CONEX use cases to the general mobile communication scenario in order to validate the use cases for this scenario.

3.1. CONEX as a Basis for Traffic Management

Traffic management is a very important function in mobile communication networks. Since wireless resources are considered scarce and since user mobility and shared bandwidth in the wireless access create certain dynamics with respect to available bandwidth, these resources are traditionally managed very tightly (admission control for bearer establishment etc.).

In EPS, the QoS requirements for different applications running on a UE are supported by a bearer concept which is managed by the network. Each bearer has an associated QoS Class identifier (QCI) and an Allocation and Retention Policy (ARP) that has been standardized for uniform traffic handling (across implementations). For the necessary QoS across the mobile network, an EPS bearer is maintained that crosses different interfaces in the network and maps to lower layer bearers for packet forwarding. A radio bearer transports traffic between a UE and eNB whereas S1 bearer transports traffic between the eNB and S-GW. Primarily LTE offers two types of bearer: Guaranteed Bit rate bearer for real time communication, e.g., Voice calls etc. and Non-Guaranteed bit rate, e.g., best effort traffic for web access etc. Packets mapped to the same EPS bearer receive the same bearer level packet forwarding treatment.

In the light of the significant increase of overall data volume in 3G networks, Deep-Packet-Inspection (DPI) is often considered a desirable function to have in the EPC -- on, for example, a PDN (Packet Data Network) gateway, and some operators do in fact deploy DPI today. 3GPP has a current work item on "Service Awareness and Privacy Policies" that is chartered to add DPI-related extensions to the PCC architecture [3GPP.23.203]. The (optional) DPI entity in the EPC is called "Traffic Detection Function" (TDF), and it performs application detection and reporting of detected application and its service data flow description to the Policy Control and Charging Rules Function (PCRF) for performing functions such as traffic blocking, redirection, policing for selected flows.

Congestion exposure can be employed to address these requirements for tight resource management in different ways:

1. It can enhance DPI by providing flow policy-based traffic management. At present, DPI-based resource management is often used to prioritize certain application classes with respect to others in overload situations, so that effectively more users can

be served on the network. In overload situations, operators use DPI to identify dispensable flows and make them yield to other flows (of different application classes) through policing. Such traffic management is thus based on static configuration and some estimation about the future per-flow bandwidth demand. With congestion exposure it would be possible to assess, in a more accurate and dynamic fashion, the congestion that certain flows are causing. This information can then be input to a policer that can optimize network utilization (better than a pure DPI-based approach can do).

2. It can reduce the need for DPI by allowing for a bulk packet traffic management system that does not have to consider flows' application classes and individual sessions. Instead traffic management would be based on the current cost (contribution to congestion) incurred by different flows and enable operators to apply policing/accounting depending on their preference. Such traffic management would be simpler and more robust (no real-time flow application type identification required, no static configuration of application classes) and perform better as decisions can be taken based on real-time actual cost contribution.

3. It can be used to more efectively trigger the offload of selected traffic to a non-3GPP network. Nowadays, it is common that users are equipped with dual mode mobile phones (e.g., integrating third/fourth generation cellular and WiFi radio devices) capable of attaching to available networks either sequentially or simultaneously. With this scenario in mind, 3GPP is currently looking at mechanisms to seamlessly and selectively switch over a single IP flow (e.g., user application) to a different radio access, while keeping all other ongoing connections untouched. The decision on when and which IP flows move is typically based on static configured rules, whereas the use of CONEX mechanisms could also factor in real-time congestion events in the decision.

In summary, it can be said that traffic management in 3GPP EPS and other mobile communication architectures in very important. Currently, more static approaches based on admission control and static QoS are in use, but recently, there has been a perceived need for more dynamic mechanisms such as DPI. Adding CONEX support might thus require slight changes the PCC architecture, depending on the scope and impact of a CONEX-based traffic management approach.

3.2. CONEX to Incentivize Scavenger Transports

As 3G and LTE networks are turning into universal access networks that are shared between mobile (smart) phone users, mobile users with

laptop PCs, home users with LTE access etc., it is likely that capacity-sharing among different users and application flows becomes more important in the mobile communication network as a fine-granular differentiation would be too costly.

Most of this traffic is likely to be classified as best-effort traffic, without differentiating (for example) periodic OS updates, application store downloads from web (browser)-based or other more real-time communication. Having said that, the general argument for scavenger transports apply. Especially when wireless and backhaul resources are scarce, incentivizing users to use less-than best effort transport for non-interactive background communication would improve the overall utility of the network. It can be argued that, if this would be done with a CONEX approach, it could be done in a more effective and cost-efficient way compared to the aforementioned DPI mechanisms.

This would work best if the network did not do any traffic class segregation below the IP layer, i.e., if all traffic would be in the same traffic class. In principle, this would be possible to implement with current specifications.

3.3. Accounting for Congestion Volume

3G and LTE networks provide extensive support for accounting and charging already, for example cf. the Policy Charging Control (PCC) architecture. In fact, most operators today account transmitted data volume on a very fine granular basis and either correlate monthly charging to the exact number of packets/bytes transmitted, or employ some form of flat rate (or flexible flat rate), often with a so-called fair-use policy. With such policies, users are typically limited to an administratively configured maximum bandwidth limit, after they have used their data contractual volume budget for the charging period.

Changing this data volume-based accounting to a congestion-based accounting would be possible in principle, especially since there already is an elaborate per-user accounting system available. Also, an operator-provided mobile communication network can be seen as a network domain within such congestion volume accounting would be possible, without requiring any support from the global Internet. Traffic normally leaves/enters the operator's network via well-defined egress/ingress points that would be ideal candidates for policing functions. Moreover, in most commercially operated networks, accounting is performed for both received and sent data, which would facilitate congestion volume accounting as well.

With respect to the current PCC framework, accounting for congestion

volume could be added as another feature to the "Usage Monitoring Control" capability that is currently based on data volume. This would not require any new interface (reference points) at all.

3.4. CONEX as a Form of Differential QoS

As mentioned above, 3GPP mobile communication networks provide an elaborate QoS architecture. In LTE, the idea is to map different traffic classes onto different logical channels (bearers) with individual QoS configuration.

It can be argued whether this approach is sufficient in a world where most traffic is on TCP port 80 and whether some more application control would be useful.

With CONEX, accurate downstream path information would be visible to ingress network operators, which can respond to incipient congestion in time. This can be equivalent to offering different levels of QoS, e.g. premium service with zero congestion response.

Again, CONEX could be used in two different ways:

1. as additional information to assist network functions to impose different QoS for different application sessions; and

2. as a tool to let applications decide on their response to congestion notification, while incentivizing them to react (in general) appropriately, e.g., by enforcing overall limits for congestion contribution or by accounting and charging for such congestion contribution.

3.5. Partial vs. Full Deployment

In general CONEX lends itself to partial deployment as the mechanism does not require all routers and hosts to support congestion exposure. Moreover, assuming a policing infrastructure has been put in place, it is not required to modify all hosts. Since CONEX is about senders exposing congestion contribution to the network, senders need to be made CONEX-aware (assuming a congestion notification mechanisms such as ECN is in place).

[I-D.briscoe-conex-initial-deploy] provides specific examples of how CONEX deployment can be initiated, focusing unilaterial deployment by single networks, i.e., by partial deployment.

In mobile communication networks that would for example allow early partial CONEX deployment in the downlink direction only, i.e., servers, gateways and caches would support CONEX but UEs (mobile

hosts) would not.

When moving towards full deployment in a specific operator's network, different ways for introducing CONEX support on UEs are feasible. Since mobile communication networks are multi-vendor networks, standardizing CONEX support on UEs (e.g., in 3GPP specifications) appears useful. Still, not all UEs would have to support CONEX, and operators would be free to choose their policing approach in such deployment scenarios. Leveraging existing PCC architectures, 3GPP network operators could for example decide policing/accounting approaches per UE -- i.e., apply fixed volume caps for non-CONEX UEs and more flexible schemes for CONEX-enabled UEs.

Moreover, it should be noted that network support for CONEX is a feature that some operators may implement to deploy if they wish, but it is not required that all operators (or all other networks) do so.

Depending on the extent of CONEX support, specific aspects such as roaming have to be taken into account. I.e., what happens when a user is roaming in a CONEX-enabled network, but their UE is not CONEX-enabled and vice versa. Although these may not be fundamental problems, they need to be considered. For supporting mobility in general, it can be required to shift users' policing state during hand-over. There is existing work in [raghavan2007] on distributed rate limiting and in [nec.euronf-2011] on specific optimizations for congestion exposure and policing in mobility scenarios.

Another aspect to consider is the addition of Selected IP Traffic Offload (SIPTO) and Local Breakout (LIPA), also see [3GPP.23.829], i.e., the idea that some traffic (e.g., high-volume Internet traffic) is actually not passed through the EPC but is offloaded at a "break-out point" closer to (or in) the access network. On the other hand, CONEX can also enable more dynamic decisions on what traffic to actually offload by considering congestion exposure in bulk traffic aggregates -- thus making traffic offload more effective.

3.6. Summary

In summary, the 3GPP EPS is a system architecture that can benefit from congestion exposure in multiple ways, as we have shown by this brief description of CONEX use cases in this environment. Dynamic traffic and congestion management is an acknowledged important requirement for the EPS, also illustrated by the current DPI-related work for EPS.

Moreover, we believe that networks such as an EPS mobile communication network would be quite amenable for deploying CONEX as a mechanism, since they represent clearly defined and well separated

operational domains, in which local CONEX deployment would be possible. Aside from roaming (which needs to be considered for a specific solution), such a deployment is fully under the control of a single operator, which can enable operator-local enhancement without the need for major changes to the architecture.

In 3GPP EPS, interfaces between all elements of the architecture are subject to standardization, including UE interfaces and eNodeB interfaces, so that a more general approach, involving more than one single operator's network, can be feasible as well.

4. CONEX in the EPS

The CONEX mechanism is still work in progress in the IETF working group. Still, we would like to discuss a few options for how such a mechanism (and possibly additional policing functions) could eventually be deployed in 3GPP's EPS. Note that this description of options is not intended as a complete set of possible approaches -- it is merely intended for discussing a few options. More details will be provided in a future revision of this document.

4.1. Possible Deployment Scenarios

There are different possible ways how CONEX functions on hosts and network elements can be used. For example, CONEX could be used for a limited part of the network only -- e.g., for the access network -- congestion exposure and sender adaptation could involve the mobile nodes or not, or, finally, the CONEX feedback loop could extend beyond a single operator's domain or not.

We present three different deployment scenarios for congestion exposure in the figures below:

1. In Figure 2 CONEX is supported by servers for sending data (here: web servers in the Internet and caches in an operator's network) but not by UEs (neither for receiving nor sending). An operator who chooses to run a policing function on the network ingress (e.g., on the P-GW) can still benefit from congestion exposure without requiring any change on UEs.

2. CONEX is universally employed between operators (as depicted in Figure 3), with an end-to-end CONEX feedback loop. Here, operators could still employ local policies, congestion accounting schemes etc., and they could use information about congestion contribution for determining interconnection agreements.

3. Isolated CONEX domains as depicted in Figure 4, CONEX is solely applied locally, in the operator network, and there is no end-to-end congestion exposure. This could be the case when CONEX is only implemented in a few networks, or when operators decide to not expose ECN and account for congestion for inter-domain traffic. Independent of the actual scenario, it is likely that there will be border gateways (as in today's deployments) that are associated with policing and accounting functions.

```
                                  +------------+
                                  | Web server |
                                  | w/ CONEX   |
                                  +------------+
                                            |
                                            |
                                            |
                         -----------------------
                         |                  |  |
                         |     Internet     |  |
                         |                  |  |
                         -----------------------
                                            |
   -------------------------------------------|--------
   |                                        |        |
   |                                    +-----------+ |
   |                                    | Web cache | |
   |                                    | w/ CONEX  | |
   |                                    +-----------+ |
   |                                        |        |
   |  +----+     +-------+     +-------+     +-------+ |
   |  | UE |=====|  eNB  |=====|  S-GW |=====|  P-GW | |
   |  +----+     +-------+     +-------+     +-------+ |
   |                                                 |
   |              Operator A                         |
   ---------------------------------------------------
```

Figure 2: CONEX support on servers and caches

```
-----------------------------------------------------
|  +----+     +-------+     +-------+     +-------+ |
|  | UE |=====|  eNB  |=====|  S-GW |=====|  P-GW | |
|  +----+     +-------+     +-------+     +-------+ |
|                                           |       |
|              Operator A                   |       |
-------------------------------------------|---------
                                           |
                         -----------------------
                         |                     |
                         |     Internet        |
                         |                     |
                         -----------------------
                                           |
-------------------------------------------|---------
|  +----+     +-------+     +-------+     +-------+ |
|  | UE |=====|  eNB  |=====|  S-GW |=====|  P-GW | |
|  +----+     +-------+     +-------+     +-------+ |
|                                                   |
|              Operator B                           |
-----------------------------------------------------
```

Figure 3: CONEX deployment across operator domains

```
    -----------------------------------------------------
    |   |---            CONEX path            ---|      |
    |   v                                        v      |
    |  +----+     +--------+     +--------+     +--------+ |
    |  | UE |=====|  eNB   |=====|  S-GW |=====|  P-GW | |
    |  +----+     +--------+     +--------+     +--------+ |
    |                                           |       |
    |              Operator A                   |       |
    --------------------------------------------|--------
                                                |
                         -----------------------
                         |                     |
                         |     Internet        |
                         |                     |
                         -----------------------
                                                |
    --------------------------------------------|--------
    |  +----+     +--------+     +--------+     +--------+ |
    |  | UE |=====|  eNB   |=====|  S-GW |=====|  P-GW | |
    |  +----+     +--------+     +--------+     +--------+ |
    |                                                   |
    |              Operator B                           |
    -----------------------------------------------------
```

Figure 4: CONEX deployment in a single operator domain

We consider all three scenarios to be relevant and believe that all of them are within the scope of the CONEX WG charter. A more detailed description will be provided in a future version of this document.

4.2. Implementing CONEX Functions in the EPS

We expect a CONEX solution to consist of different functions that should be considered when implementing congestion exposure in 3GPP's EPS. [I-D.ietf-conex-abstract-mech] is describing the following congestion exposure components:

- o Modified senders that send congestion exposure information in response to congestion feedback).
- o Receivers that generate congestion feedback (leveraging existing behavior or requiring new functions).
- o Audit functions that audit CONEX signals against actual congestion, e.g., by monitoring flows or aggregate of flows.

o Policy devices that monitor congestion exposure information and act on the flows according to the operator's policy.

Two aspects are important to consider: 1) how the CONEX protocol mechanisms would be implemented and what modifications to existing networks would be required and 2) where CONEX functional entities would be placed best (to allow for a non-invasive addition). We discuss these two aspects in the following sections.

4.2.1. CONEX Protocol Mechanisms

As described in [I-D.briscoe-conex-initial-deploy], the most important step in introducing CONEX (initially) is adding the congestion exposure functionality to senders. For an initial deployment, no further modification to senders and receivers would be required. Specifically, there is no fundamental dependency on ECN, i.e., CONEX can be introduced without requiring ECN to be implemented.

Congestion exposure information for IPv6 [I-D.ietf-conex-destopt] is contained in a destination option header field, which requires minimal changes at senders and nodes that want to assess path congestion -- and that does not affect non-CONEX nodes in a network.

In 3GPP networks, IP tunneling is used intensively, i.e., using either IP-in-GTP-U or PMIPv6 (i.e., IP-in-IP) tunnels. In general, the CONEX destination option of encapsulated packets should be made available for network nodes on the tunnel path, i.e., a tunnel ingress should copy the CONEX destination option field to the outer header.

For an effective and efficient capacity sharing, we envisage the deployment of ECN in conjunction with CONEX so that ECN-enabled receivers and senders get more accurate and more timely information about their flows congestion contribution. ECN is already partially introduced into 3GPP networks: Section 11.6 in [3GPP.36.300] specifies the usage of ECN for congestion notification on the radio link (between eNB and UE), and [3GPP.26.114] specifies how this can be leveraged for voice codec adaptation. A complete, end-to-end support of ECN would require specification of tunneling behaviour, which should be based on [RFC6040] (for IP-in-IP tunnels) and on [I-D.briscoe-tsvwg-ecn-encap-guidelines]. Specifically, a specification for tunneling ECN in GTP-U will be needed.

4.2.2. CONEX Functions in the Mobile Network

In the following, we discuss some possible placement strategies for CONEX functional entities (addressing both policing and auditing

functions) in the EPS and for possible optimizations for both the uplink and the downlink.

In general, CONEX information (exposed congestion) is declared by a sender and remains unchanged on the path, hence reading CONEX information (e.g., by policing functions) is placement-agnostic. Auditing CONEX normally requires assessing declared congestion contribution and current actual congestion. If the latter is, for example, done using ECN, such a function would best be placed at the end of the path.

In order to provide a comprehensive CONEX-based capacity management framework for EPS, it would be advantageous to consider user contribution to congestion for both the radio access and the core network. For a non-invasive introduction of CONEX, it can be beneficial to combine CONEX functions with existing logical EPS entities. For example, potential places for CONEX policing and auditing functions would then be eNBs, S-GWs or the P-GWs. Operator deployments may of course still provide additional intermediary CONEX-enabled IP network elements.

For a more specific discussion it will be beneficial to distinguish downlink and uplink traffic directions (also see [nec.globecom2010] for a more detailed discussion). In today's networks and usage models, downlink traffic is dominating (also reflected by the asymmetric capacity provided by the LTE radio interface). That does however not imply that uplink congestion is not an issue, since the asymmetric maximum bandwidth configuration can create a smaller bottleneck for uplink traffic -- and there are of course backhaul links, gateways etc. that could be overloaded as well.

For managing downlink traffic -- e.g., in scenarios such as the one depicted in Figure 2, operators can have different requirements for policing traffic. Although policing is in principle location-agnostic, it is important to consider requirements related to the EPS architecture (Figure 1) such as tunneling between P-GWs and eNBs. Policing can require access to subscriber information (e.g., congestion contribution quota) or user-specific accounting, which suggests that the CONEX function could be co-located with the P-GW that already has an interface towards the PCRF.

Still, policing can serve different purposes. For example, if the objective is to police bulk traffic induced by peer networks, additional monitoring functions can be placed directly at corresponding ingress points to monitor traffic and possible drive out-of-band functions such as triggering border contract penalties.

The auditing function which should be placed at the end of the path

(at least after/at the last bottleneck) would likely be placed best on the eNB (wireless base station).

For the uplink direction, there are naturally different options for designing monitoring and policy enforcement functions. A likely approach can be to monitor congestion exposure on central gateway nodes (such as P-GWs) that provide the required interfaces to the PCRF, but to perform policing actions in the access network, i.e., in eNBs, e.g., to police traffic at the ingress, before it reaches concentration points in the core network.

Such a setup would enable all the CONEX use cases described in Section 3, without requiring significant changes to the EPS architecture, while enabling operators to re-use existing infrastructure, specifically wireless base stations, PCRF and HSS systems.

For CONEX functions on elements such as the S-GWs and P-GWs, it is important to consider mobility and tunneling protocol requirements. LTE provides two alternative approaches: Proxy-Mobile-IPv6 (PMIPv6, [3GPP.23.402]) and GPRS Tunneling Protocol (GTP). For the propagation of congestion information (responses) tunneling considerations are therefore very important.

In general, policing will be done based on per-user (per subscriber) information such as congestion quota, current quota usage etc. and network operator policies, e.g., specifying how to react to persistent congestion contribution etc. In the EPS, per-user information is normally part of the user profile (stored in the HSS) that would be accessed by PCC entities such as the PCRF for dynamic updates, enforcement etc.

A more detailed description of the different approaches and their respective advantages will be provided in a future revision of this document.

5. Summary

We have shown how congestion exposure can be useful for efficient resource management in mobile communication networks. The premise for this discussion was the observation that data communication, specifically best-effort bulk data transmission, is becoming a commodity service whereas resources are obviously still limited -- which calls for efficient, scalable, yet effective capacity sharing in such networks.

CONEX can be a mechanism that enables such capacity sharing, while

allowing operators to apply these mechanisms in different ways, e.g., for implementing different use cases as described in Section 3. It is important to note that CONEX is fundamentally a mechanism that can be applied in different ways -- to realize different operators policies.

We have described a few possibilities for adding CONEX as a mechanism to 3GPP LTE-based networks and have shown how this could be done incrementally (starting with partial deployment). It is quite feasible that such partial deployments be done on a per-operator-domain basis, without requiring changes to standard 3GPP interfaces. For a network-wide deployment, e.g., with congestion exposure between operators, more considerations might be needed.

We have also identified a few implications/requirements that should be taken into consideration when enabling congestion exposure in such networks:

Performance: In mobile communication networks -- with more expensive resources and more stringent QoS requirements -- the feasibility of applying CONEX as well as its performance and deployment scenarios need to be examined closer. For instance, a mobile communication network may encounter longer delay and higher loss rates, which can impose specific requirements on the timeliness and accuracy of congestion exposure information.

Mobility: One of the unique characteristics in cellular network is the presence of user mobility compared to wired networks. As the user location changes, the same device can be connected to the network via different base stations (eNodeBs) or even go through switching gateways. Thus, the CONEX scheme must to be able to carry latest congestion information per user/flow across multiple network nodes in real time.

Multi-access: In cellular network, multiple access technologies can co-exist. In such cases, a user can use multiple access technologies for multiple applications or even a single application simultaneously. If the congestion policies are set based on each user, then CONEX should have the capability to enable information exchange across multiple access domains.

Tunneling: Both 3G and LTE networks make extensive usage of tunneling. The CONEX mechanism should be designed in a way to support usage with different tunneling protocols such as PMIPv6 and GTP. For ECN-based congestion notification, [RFC6040] specifies how the ECN field of the IP header should be constructed on entry and exit from IP-in-IP tunnels, and [I-D.briscoe-tsvwg-ecn-encap-guidelines] provides guidelines for

adding congestion notification to protocols that encapsulate IP.

Roaming: Independent of the specific architecture, mobile communication networks typically differentiate between non-roaming and roaming scenarios. Roaming scenarios are typically more demanding regarding implementing operator policies, charging etc. It can be expected that this would also hold for deploying CONEX. A more detailed analysis of this problem will be provided in a future revision of this document.

It is important to note that CONEX is intended to be used as a supplement and not a replacement to the existing QoS mechanisms in mobile networks. For example, CONEX deployed in 3GPP mobile networks can provide useful input to the existing 3GPP PCC mechanisms by supplying more dynamic network information to supplement the fairly static information used by the PCC. This would enable the mobile network to make better policy control decisions than is possible with only static information.

6. IANA Considerations

No IANA considerations.

7. Security Considerations

Security considerations for applying CONEX to EPS include, but are not limited to, the security considerations that apply to the CONEX protocols.

8. Informative References

[3GPP.23.203]
3GPP, "Policy and charging control architecture", 3GPP TS 23.203 10.7.0, June 2012.

[3GPP.23.402]
3GPP, "Architecture enhancements for non-3GPP accesses", 3GPP TS 23.402 10.7.0, March 2012.

[3GPP.23.829]
3GPP, "Local IP Access and Selected IP Traffic Offload (LIPA-SIPTO)", 3GPP TR 23.829 10.0.1, October 2011.

[3GPP.26.114]
3GPP, "IP Multimedia Subsystem (IMS); Multimedia

telephony; Media handling and interaction", 3GPP TS 26.114 10.4.0, June 2012.

[3GPP.29.060]
3GPP, "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface", 3GPP TS 29.060 3.19.0, March 2004.

[3GPP.29.274]
3GPP, "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3", 3GPP TS 29.274 10.7.0, June 2012.

[3GPP.36.300]
3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2", 3GPP TS 36.300 10.8.0, July 2012.

[I-D.briscoe-conex-initial-deploy]
Briscoe, B., "Initial Congestion Exposure (ConEx) Deployment Examples", draft-briscoe-conex-initial-deploy-02 (work in progress), March 2012.

[I-D.briscoe-tsvwg-ecn-encap-guidelines]
Briscoe, B., "Guidelines for Adding Congestion Notification to Protocols that Encapsulate IP", draft-briscoe-tsvwg-ecn-encap-guidelines-00 (work in progress), March 2011.

[I-D.ietf-conex-abstract-mech]
Mathis, M. and B. Briscoe, "Congestion Exposure (ConEx) Concepts and Abstract Mechanism", draft-ietf-conex-abstract-mech-04 (work in progress), March 2012.

[I-D.ietf-conex-concepts-uses]
Briscoe, B., Woundy, R., and A. Cooper, "ConEx Concepts and Use Cases", draft-ietf-conex-concepts-uses-04 (work in progress), March 2012.

[I-D.ietf-conex-destopt]
Krishnan, S., Kuehlewind, M., and C. Ucendo, "IPv6 Destination Option for Conex", draft-ietf-conex-destopt-02 (work in progress), March 2012.

[RFC6040] Briscoe, B., "Tunnelling of Explicit Congestion Notification", RFC 6040, November 2010.

[nec.euronf-2011] Mir, Kutscher, and Brunner, "Congestion Exposure in Mobility Scenarios", in proceedings of 7th EURO-NF CONFERENCE ON NEXT GENERATION INTERNET, June 2011.

[nec.globecom2010] Kutscher, Lundqvist, and Mir, "Congestion Exposure in Mobile Wireless Communications", in proceedings of IEEE GLOBECOM 2010, December 2010.

[raghavan2007] Raghavan, Vishwanath, Ramabhadran, Yocum, and Snoeren, "Cloud Control with Distributed Rate Limiting", in proceedings of ACM SIGCOMM 2007, 2007.

DOI: http://doi.acm.org/10.1145/1282427.1282419

Appendix A. Acknowledgments

We would like to thank Bob Briscoe and Ingemar Johansson for their support in shaping the overall idea and in improving the draft by providing constructive comments.

Authors' Addresses

Dirk Kutscher
NEC
Kurfuersten-Anlage 36
Heidelberg,
Germany

Phone:
Email: kutscher@neclab.eu

Faisal Ghias Mir
NEC
Kurfuersten-Anlage 36
Heidelberg,
Germany

Phone:
Email: faisal.mir@neclab.eu

Rolf Winter
NEC
Kurfuersten-Anlage 36
Heidelberg,
Germany

Phone:
Email: winter@neclab.eu

Suresh Krishnan
Ericsson
8400 Blvd Decarie
Town of Mount Royal, Quebec
Canada

Phone:
Email: suresh.krishnan@ericsson.com

Ying Zhang
Ericsson
200 Holger Way
San Jose, CA 95134
USA

Phone:
Email: ying.zhang@ericsson.com

Carlos J. Bernardos
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid 28911
Spain

Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI: http://www.it.uc3m.es/cjbc/