Policies to Enable Serving Untrusted Services on Alternative (non-3GPP) and Untrusted Access Networks in EPS

Author: Rebecca Copeland, Core Viewpoint Ltd, Kenilworth, Warwickshire, United Kingdom
Co-Author: Noel Crespi, Institut Telecom, Telecom SudParis, Evry, France

Abstract: The popularity of mobile Internet is driving the Mobile world towards untrusted services while increasing Mobile Data volumes encourage adoption of untrusted access network for delivery of MNO services. This paper examines the emerging methods of utilizing untrusted access and facilitating untrusted third party services on either trusted or non-trusted access networks via existing and extended EPS facilities. These methods and policies should be better organized in an effort to manage a multi-access and open service environment, with heterogeneous access technologies and collaboration across business borders. This paper proposes enhancements to managing untrusted access, selection of best available access network and delivering sponsored services utilizing MNO's policies and authentication.

Keywords*: ANDSF, WiFi, WLAN, Untrusted access, non-3GPP, Policy, PCRF, ABC (Always Best Connected), QoS, LTE, EPC, EPS, PMIP,*

I. INTRODUCTION

A. Background

The demand for service ubiquity and Mobile Internet is growing rapidly and has become the selling focus for Mobile Phones – not Voice, which is now taken for granted. This forces Telcos to re-examine their portfolios and consider supporting alternative technologies. They need to facilitate service delivery from untrusted and unknown sources, over both trusted and untrusted access networks.

The challenge for the MNOs is to exploit the extra spectrum capacity and add value to such untrusted services, using their assets, in particular the EPS facilities. MNOs (Mobile Network Operators) as well as Service Providers (SP) and Content Providers (CP) are seeking ways to monetize Internet services. MNOs need to exploit their capability to authenticate, validate credit, ensure privacy and security, vary the level of service quality and fine-tune charges. Applying these facilities to Internet services could open further opportunities and serve users with better choice.

B. Untrusted Access is set to grow

WiFi has recently re-gained popularity as an offloading solution to relieve 3G congestion caused by the Data services explosion. But now Telcos perceive such non-native access networks as opportunities for permanent augmentation of their ability to serve services.

Alternative access networks also include WiMax, which is making inroads in non-urban territories. Other in-building access networks, such as Femtocells, may be under the operator's control in subscribers' homes, but are not as ubiquitous and as low cost as WiFi. In Ref [8], the analyst's report predicts that WiFi volumes will grow at 25%-50% in 2011, much faster than 3G. It expects WiFi to become the default medium for video traffic, which generates far larger volumes of packets than Voice.

Many homes have subscribers of rival MNOs under a single roof, sharing a home WiFi access network, where any of the MNOs could utilize the added capacity.

C. Scope for Policies for Untrusted Service

In 'taming' the untrusted access, MNOs compete with OTT (Over-The-Top) players who take advantage of any Mobile Broadband. Therefore, it is important to enhance delivery of such services and justify their monetization.

The design of EPS (Evolved Packet System) separates the core functions from the LTE (Long Term Evolution) access, thus enabling using the same functions, especially session admission, authorization and policy, for alternative access networks as well. This multi-access environment with unknown 3rd party services increases complexity many folds. To simplify it, the selection of access network should be automated under selected policies, and optimized for quality and for lowest costs.

D. The paper contents

This paper describes several mechanisms already available for MNOs to manage untrusted access and untrusted services, and highlights how they can be extended to help MNOs leveraging their facilities and improve service delivery.

In **part II**, **untrusted access** types are discussed, with provision of authorization and heightened security.

In **part III the process of discovery** and selection of access networks is described, including what policies are required and how this process can be optimized.

In **part IV authorizing untrusted services** and the sponsoring models are examined.

In **Part V** the technologies for these three areas are analyzed and further scope for improvement is proposed.

II. UNTRUSTED ACCESS

A. Multi-Access Requirements

Smartphones have reshaped users' expectations for open access to Internet services and made them aware of access options, currently mostly 3G and WiFi. Untrusted access networks that are compatible with the handsets could be used by users without the MNO's help, if the handset is not barred from doing so. However, such services could be improved with better security, enhanced ubiquity and greater privacy.

Attaching to alternative trusted and untrusted access becomes easier in EPS, which is designed for multi-access. This can:

- Enable MNO packet services to run over untrusted access,
- Enhance non-MNO services by using core facilities.

B. Types of Untrusted Access Networks

What is a trusted or not trusted network is not a function of the compatibility of network or the type of technology, but is governed by the availability of information, adequate security and most of all – pre-determined commercial relationships.

Access networks may be trusted but not compatible, i.e. using different interfaces. For example, WCDMA based access networks are not compatible with 3GPP (3rd Generation Partnership Project) devices, but may belong to a trusted MNO. Conversely, access network may be compatible but not trusted, e.g. Home WiFi that is independent of the MNO. In each case, access attachment procedures, authentication methods and security protocols are different.

3GPP standards distinguish between 3GPP compliant and non-3GPP networks, e.g. WLAN, WiMax or 3GPP2. Non-3GPP networks can still be trusted, even 'native' (same MNO), or they can be untrusted, where there is no relationship.

In the case of other MNO's hotspots, WiMax or Enterprise WLAN, there may be a trust relationship that enables authorizing services via the mechanism of 3GPP AAA Proxy, as described in Ref. [12] chapter 10.

In particular, there is great potential in exploiting the unmanaged WiFi access via home gateways in private homes and public establishments (e.g. hotels and cafes). Currently this is left entirely to the OTT players who gain advantage by using this free resource. MNOs need to develop tools that allow them to exploit this opportunity and add value through their own facilities.

C. Heterogenous Access via IETF Protocols

Advanced Internet Data services have stimulated the evolution of protocols that handle data flows differently. Multimedia services may demand multiple IP connections simultaneously, so the access technology must cater for multi-connection. Multiple parallel streams can also be very useful to shorten handover between one WiFi access network to another, similar to handover between mobile cells. Several IETF (internet Engineering Task Force) drafts (Ref. [13]) specify Multi-Path TCP (MP-TCP) method, examining the consequences of multiple addresses, APIs and security threats.

Unlike handover between mobile cells, in Multi-path TCP over WiFi, the application is handed over to another IP connection that is often provided by entirely different entity. This still needs a discovery process and a decision to trust the new network. Any change to charging must be captured in order to reimburse the participating parties.

The IETF protocols are intended to provide a common way of reaching mobile handsets, independently of the mobile core network.These protocols, such as PMIPv6 (Proxy Mobile IPv6), DSMIPv6 (Dual Stack Mobile IPv6) and MIPv4 (Mobile IPv4), employ different mechanisms of managing service data flows.

In GTP (GPRS Tunneling Protocol), which is used by 3GPP GPRS/UMTS, the IP flows are grouped into 'bearers' with common QoS (Quality or Service) parameters. Since these IETF Mobile IP (MIP) protocols are not bearer based, they require Policy and QoS information to be transmitted on separate signaling connections, not via the same path of the session signaling, therefore require separate interfaces.

D. EPS Interworking with IETF MIP and Multi-Path

In order for EPS to inter-operate with both 3GPP and IETF MIP (Mobile IP) methods and facilitate handover when necessary, the BBERF (Bearer Binding and Event Reporting Function) has been defined as a separate function.

The BBERF performs the bearer binding, i.e. it links QoS PCC (Policy & Charging Control) rules to a bearer within the access network for each session, as described in Ref [1]. The BBERF resides within the S-GW (Serving Gateway) in the 3GPP compliant EPC (Evolved Packet Core), but it is found in access gateways in IETF-protocols based networks, i.e. the BBERF could be in an untrusted access network node.

Where the BBERF exists in the access nodes, it performs the binding of data flows into bearers, and the EPS can use PMIP (Proxy Mobile IP) interfaces (S5/S8) that differentiate multiple Packet Data links to the same access point. If the BBERF is not present, only interfaces that support parallel flows to the *same* access point (S2a/S2b) can be used by the Serving Gateway (Ref [4]).

E. Security for non-3GPP Access Connections via EPS

The authentication methods of most untrusted access network are not considered to be sufficient for MNO services. Much higher level of authentication is used for EPS, which is governed by mandatory EAP (Extensible Authentication Protocol) and AKA (Authentication & Key Agreement), using IKEv2 (Internet Key Exchange) (see Ref [6]).

To resolve this, the HSS/HLR capability of vicarious authentication for existing 3G/4G subscribers can be used (Ref [12] chapter 5) for non-3GPP access users. This means that the users' identification is processed through the Mobile subscription, as long as the user can identify safely the mobile account. The association with the WiFi network may be temporary (e.g. hotels or WiFi cafes), which could be treated as 'limited service' in roaming.

Where WiFi is not free, enabling payments transfer with automatic agreements could be processed via transactional services, which are yet to be standardized.

F. Routing Path and Special Gateways

Untrusted access also requires higher level of protection for the transmitted data, including encryption and tunneling which are not necessary in trusted connections. To accommodate untrusted access connections, the User Equipment (UE) connects via an ePDG (evolved Packet Data Gateway), not a regular PDN GW (Packet Data Network Gateway). Routing via the ePDG is decided at the point of session admission according to the level of trust given to the access network.

The ePDG supports protocols that are used by untrusted networks (e.g. IETF MIP) and is secured according to the Security Parameters Index as defined IETF in Ref [7], enabling the creation of Security Associations for IP tunnels directly from the UE to the ePDG. However, such tunneling is not always necessary, e.g. when using DSMIPv6, which is deemed to be sufficiently secure. Therefore, the UE needs to know not only the trust relationship, but also the protocol to be used and the routing (via ePDG) decision.

G. *Alternative Access Authentication and Trust Status*

Users need to obtain authentication from the untrusted access network first, and then obtain authorization from the MNO, so that MNO services can be delivered over the untrusted network. If the UE reaches an AAA server that can act as a 3GPP-AAA proxy, it can provide a 'trusted' authentication via the Home network (see Ref. [10]). In the case of roaming, the untrusted access is authenticating via the Visited Network's existing 3GPP AAA proxy that relays the authentication request to the Home network's 3GPP AAA server.

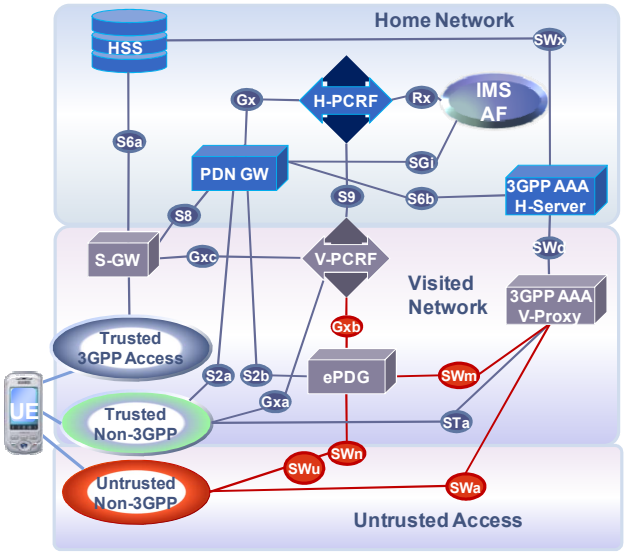

Figure 1: Untrusted Access in Roaming

As shown in *Figure 1,* for untrusted access, there is a special mutual authentication process between the UE and the ePDG over the SWu interface that establishes IPsec tunnel with security associations, using MOBIKE (Ref. [14]). This enables security for multiple streams in multi-homing mode.

In roaming scenarios policies from the Home network PCRF (Policy and Charging Rules Function) can be conveyed to the untrusted access via the Home-PCRF to Visited-PCRF interface (see *Figure 1*). These policies are enforced by the ePDG for the untrusted network, regardless of the location of the ePDG – in the Home Network or the Visited Network, thus providing consistent experience.

III. Access Network Discovery & Selection (ANDSF)

A. *ANDSF Principles*

3GPP Release 10 (Ref [3]) defines standards for *Intersystem Mobility Policy* to allow universal connectivity. In such an environment, the terminal needs to discover what access networks are available and select the best option. To do that, the UE must establish which type of trust relationship applies to the available access networks and select the correct attachment procedure and protocols.

The ANDSF Discovery function not only finds what is available but also assists in choosing the best partner (i.e. lowest charges, best QoS, best experience) via prioritization indicators. The selection may be adjusted if ANDSF indicates presence of a higher priority access network, or the UE's re-positioning triggers a re-evaluation of the ANDSF conditions.

ANDSF is an optional function. If only local access authentication is possible, the terminal uses pre-configured policy and information. ANDSF can reside within the local network, but it is easier to manage when it is operated from the core, independently of the access. In the latter case, the UE registers to the core network and receives an indicator of trust level in the AT_TRUST_IND attribute (Ref. [3]).

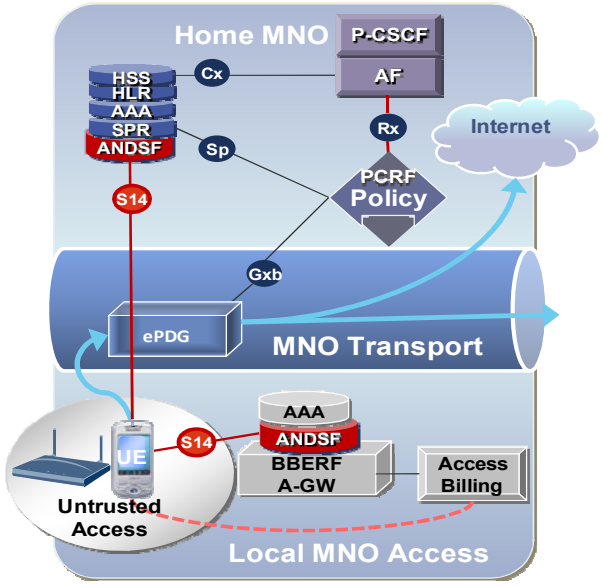

Figure 2: Untrusted Access Admission

Figure 2 shows the ANDSF architecture. The untrusted Access network can link to ANDSF via the S14 interface, either in the local MNO access node or in the core.

The S14 interface includes *Discovery Information* (lists of prioritized available networks within range), Inter-System *Mobility Policy* (rules for selection of one active access network), and *Routing Policy* (rules of access selection for potentially multiple simultaneous IP connections).

Mobility and routing policies for the user are determined in the ANDSF database, which can reside in a separate database local to the performing node (see *Figure 2*) or in the central

User Data Repository (UDR), together with HLR (Home Location Register), HSS (Home Subscriber Server), AAA (for non-3GPP services), and SPR (Subscriber Profile Repository for Policy data).

B. *ANDSF Policies*

As in the PCC architecture, the *Intersystem Mobility Policy* contains several rules, but only one can be in force at any one time. When several rules may apply, the rule to be activated is selected by preset order of priority. A rule is built of several conditions and resulting actions. The conditions are based on dynamic factors, such as location and time of day, and static factors, such as technology capability of the handset.

Same structure applies for ANDSF policies. The ANDSF condition analysis will indicate which access network is preferred or which one is restricted.

IV. AUTHORISING UNTRUSTED SERVICES

A. *Untrusted or Unknown 3rd Parties*

OTT players deliver untrusted Internet services over either trusted or untrusted access networks. MNOs can detect such services via DPI (deep Packet Inspection) and adjust the network policies accordingly. However, a better strategy is to embrace the trend and enable content and service delivery even when there is no direct relationship. An untrusted service can still benefit from certain MNO's facilities, whether running on the native access or an untrusted one.

In the past two years, major MNOs (Vodafone, AT&T, Telefonica) launched their own app stores to dispense untrusted apps. These app stores have become a vehicle of connecting MNOs to numerous untrusted 3rd parties for the delivery of untrusted services. The app stores take on the task of verifying the source Service Providers (SP) or Content Providers (CP), evaluating their services and determining the service packages and user prices. Since users pay the app store (not the MNO), they established commercial relationships with them, and validate users' service requests on behalf of the SP/CP. The app stores act as intermediary agents towards the MNO, obtaining permission to consume network resources, for a wholesale fee. Therefore, the app store model represents a good example of sponsored untrusted services.

B. *The Sposored Service Model*

To simplify the support for such service sponsoring agents, some standards are specified (Ref [2]) to allow for the three-way relationship to work, passing information between the sponsoring agent, the network carrier and the SP/CP.

The Sponsor must be able to authenticate the user in order to accept requests and collect payments. The Sponsor pays the MNO for network usage on behalf of authorized users, even when these users are also MNO subscribers.

Based on the commercial agreement with the user, the Sponsor determines what the user is entitled to, and initiates a service request via the AF (Application Function). The MNO recognizes the Sponsor and accepts requests for authenticated subscribers. Service level and QoS parameters are determined by the MNO's PCRF (the Policy Server), based on received data, and the PCRF conveys the policy rules to the enforcing network nodes that control the service data flows.

In this model, users' rights for the sponsored service are determined not by the MNO subscription, but by the user agreement with the Sponsor for the particular service.

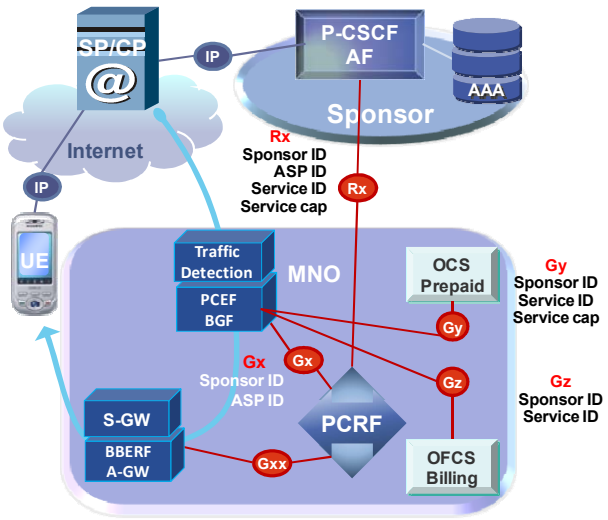

Figure 3: Sponsor intermediary between MNO and ASP

Figure 3 shows the SP/CP receiving a request from the user over an Internet connection. The SP/CP requests authorization of the service from the Sponsor over an IP link which is not standardized and may be application specific. The Sponsor retrieves user details from its own database and requests the service from the MNO. The MNO authorizes the network resources and makes the connection.

The MNO's PDN gateways in the PCEF (Policy & Charging Enforcement Function) produce charging records on the Off-line Charging system via the Gz interface. Usually, these charging records are reconciled against the Sponsor's wholesale charges and not accrued to the user's own billing, since the user may have paid the Sponsor for the service, and the MNO is recompensed by the Sponsor.

C. *Authenticating users for Untrusted Services*

Where users access their own choice of services over the open Internet, there is no validation of the service provider as the genuine party. The SP/CP identifies users by HTTP Digest authentication, which is regarded as the lowest level of authentication. Improvements can be made in both cases.

In the Sponsored Service model, users are authenticated by the MNO for network delivery with higher level of security that is a normal feature for Mobile number authentication via SIM cards. The MNO identifies the Sponsor as a trusted partner, and the Sponsor vouches for the SP/CP as a bona fide destination. Hence, the Sponsored Service provides higher level of authentication and service assurance, confirming the validity of the SP/CP and the users' identity.

D. Service Authorization

Authorizing the service involves not only setting up QoS parameters, but also limitations and caps, for example maximum duration. The session parameters may have been already agreed between the SP/CP and the Sponsor. When the user requests the service, the Sponsor needs to request these parameters from the MNO. These parameters may be different from the usual (not sponsored) service level that is normally provided to the user under the MNO subscription.

E. Untrusted Application Detection and Barring

Unauthorized services run over internet browsing as 'best effort', with no PCRF policies, however, the PCRF can exercise gate control according to detected applications that the operator wants to limit or throttle (See Ref [1]). The Application Detection and Control (ADC) rule can be dynamic (real time) or static (pre-configured).

The detection of the application is performed in the service Detection Traffic Function which is located on the PCEF nodes or as standalone node. This is one of the functions in DPI, and the control is based on sets of policies and rules.

The policy may be set to recognize the particular service and bar the packets from passing the gate, or set upper limits on the throughput of packets. Another policy may be to redirect the traffic via special gateways, e.g. the ePDG that provides better security for untrusted services.

V. Analysis and Future Scope

The various mechanisms described above are dealing with aspects of service admission via untrusted networks, the discovery, selection and handover of such access types and the authorization and policy control of untrusted services on any type of access. These emerging methods and protocols are yet to be proven in practice. They require more direct focus, experimenting and rigorous testing. Further extensions of these methods are detailed below.

A. Enhancements for Untrusted Access

The number of permutations that now exist in selecting access networks may lead to the usage of the PCRF as the final arbiter. For example, it could decide on the choice of:

- GTP (3GPP tunneling) or PMIP (Proxy Mobile IP),
- Home routing or Local routing for service data flows,
- IPv6, IPv4 or Dual Stack (DSMIPv6),
- Home IP mobility or local mobility for access selection.

Dealing with untrusted access networks means that session policies need to be synchronized across business entities. This should be performed by the PCRF that is able to negotiate with PCRFs in other networks via the S9 interface (*Figure 1*).

The PCRF is the core node that can communicate with the BBERF in untrusted access network as well as the transport nodes in the PCEF. Therefore, it can transfer vital information, such as events and triggers that occur either in the access or in the transport pipe. This can be used to detect service events outside the native network that change the session policy, even for non-native access networks.

This PCRF capability enables it to coordinate between an untrusted access node and the MNO's network. It can exchange information between nodes in different networks that otherwise have no means of doing so. The PCRF can ensure that they receive consistent policy rules and operate in the same manner. It can also guide handover between heterogeneous access networks, informing them of changed routing decisions and new parameters (Ref [5]).

B. Enhancements for ANDSF

Although ANDSF specification (3GPP Release 10) is new, the interest in it is high and developers are already adopting it. ANDSF compatible products are already commercially available. For example WeFi Inc. (www.wefi.com) has launched an ANDSF compliant product in March 2011.

ANDSF rules may be simple to begin with, but could become more intricate with special circumstances and numerous optional protocols and interfaces. In addition, policies should be consistent across any access network, therefore should reside in the core rather than in any particular access node. For all these reasons, the Policy Server is best placed to define such rules and resolve any conflict. The PCRF is also suitable because it is already linked to the OCS (Online Charging System), and could enable Telcos to apply usage caps, credit control and prepay services to untrusted access networks.

ANDSF is a step towards ABC (Always Best Connected) to be applied to access selection. ABC is conceived as an automatic facility that determines the lowest cost connection and best QoS. Compared with ANDSF, the ABC selection of a transport network is not visible to users and is performed on behalf of the operator. While access can be manually selected, the transport selection is always automatic. Hence ANDSF is optional, while ABC is not.

In addition, the quality of the connection, which is dynamically measured, could also be a factor in the selection of the access network. This is currently proposed for the ABC solution (see Ref [11]) but could also be specified for ANDSF. The MNO network may be aware of congestion status of alternative access networks through monitoring the link or via probes. This information need not be divulged to users but could be used to guide them to choose the best access.

Other ideas to enhance the ANDSF procedure further include:

- The manual selection of an alternative access network is usually based on cost considerations, but ignores other factors that should affect user choices, e.g. security, quality of experience, current congestion status and privacy. When presented with multiple choices, users could be guided by ANDSF recommendations.
- Access selection could be automated in a similar way that is proposed for 'Always Best Connected'. Using the MP-TCP methods and MOBIKE, ANDSF can support automatic mobility between untrusted access networks.
- Digital privacy could become a strong motivation of users to choose Telcos to deliver services rather than direct link to unknown parties via the open Internet, as predicted in Ref [8]. It is proposed that Privacy rules, e.g. preventing

users' behaviour to be recorded, could be added to user service profiles and used as another selection criteria.

C. *Enhancements for Untrusted 3rd Party Services*

The Sponsored Service model introduces some MNO capabilities into the delivery of untrusted or unknown services via an intermediary. Dealing with only few sponsoring agents who aggregate services from numerous SPs and CPs makes it easier for MNOs to offer more network facilities:

- Sponsors could use the MNO's authentication capabilities for identifying users.
- The MNO can help the Sponsor if the user owns several terminals which are included on the MNO unified user profile, e.g. tablet devices as well as phones. The identities can be linked together in an implicit registration, enabling the SP to accept multiple identities that are under the same user account and appearing to be a single number.
- The MNO can extend policy-based services to sponsored services. Such services can include avoiding bill shock when roaming, Gold service, off-peak service and so on.
- Different strategies for service delivery can be applied to the sponsored services. For example, the delivering network may offer reduced QoS level instead of rejection.
- The ability to apply charging policies for untrusted services & 3rd parties can assist the Sponsor to manage costs. This can be achieved by defining charging rules per Sponsor per SP/CP and require a sponsor indicator.
- Sponsors could also apply separate PCC rules - per Sponsor, not user. This may be used for sponsors' promotions and discounts, or to zero-rate certain service flows and exclude them from the normal user's usage, e.g. for the purpose of capping.
- Both MNOs and Sponsors would benefit from the ability to recognize traffic volumes per sponsor. This will enable recording historical usage and can be used when negotiating wholesale fees. This requires identification of the sponsored service flows (i.e. including a Sponsor ID indicator) to record them per sponsor (not per user).
- Since the traffic detection function only reports on the destination (the SP), the MNO may need to identify the Sponsor identity to recognize heavy traffic generated by a particular Sponsor.

D. *Testbed for Untrusted Network Policy*

The behaviour of untrusted access networks is particularly difficult to predict. However, many aspects can be examined or replicated in the safe environment of a testbed, where multiple WiFi modems and various access gateways can be plugged in, representing a multi-access environment.

Equally hard to predict is how various conditions and rules may interact, especially when the complexity of multi-access with heterogeneous technologies is increased. Therefore, the testbed should enable testing elaborate set of policies, instead of skipping this area altogether, as is often the practice,

VI. SUMMARY

In this paper a number of mechanisms are brought together to support the MNO's opportunities in extending their portfolios to untrusted access and untrusted services. They include handling different methods of connecting IP streams (PMIP, MP-TCP), discovery and selection of heterogeneous access networks via ANDSF and delivery of untrusted services via the Sponsored Service model.

The paper proposes extending these techniques. Notably, ANDSF can be used more like ABC, to automate selection of best access on behalf of the user and provide better guidance for manual selection, based on internal knowledge of the access network performance.

Also proposed is the use of the PCRF to synchronize between untrusted networks and the MNO transport network, to detect events in non-native access and support handover between them. This role can be expanded further to manage some of the trickiest decisions associated with handling untrusted multiple access networks and authorizing untrusted services.

The sponsored service model can be extended further with sponsor based policies, if sponsor ID is added to the sponsored service request information. MNO's could also augment the user authentication by the Sponsor through the MNO's details of the user's multiple terminals.

Finally, untrusted access and untrusted services should receive higher focus and rigorous testing, especially in modeling complex policies rules for untrusted networks and services.

REFERENCES

[1] 3GPP TS 23.203 Policy and Charging Architecture Rel 11

[2] 3GPP TR 23.813 Study on Policy solutions and Enhancements Rel 10

[3] 3GPP TS 23.402 Architecture Enhancements for non-3GPP accesses Release 10

[4] J J Pastor Balbas, Stefan Rommer & John Stenfelt, "Policy and Charging Control in the evolved Packet System", IEEE Communications Magazine, Volume 47 Issue 2, February 2009

[5] 3GPP TS 23.002 Network Architecture Release 10

[6] Rolf Blom et al, "Security in the Evolved Packet System", Ericsson Review, Feb 2010

[7] IETF RFC 4301Security Architecture for the Internet Protocol

[8] Deloitte "Technology, Media & Telecommunications prediction 2011"

[9] 3GPP TS 24.312 Access Network Discovery and Selection Function (ANDSF) Management Object (MO), Release 10

[10] 3GPP TS 24.302 Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks

[11] Jens Schumacher et al, "Providing an User Centric Always Best Connection", PERIMETER project.

[12] Rebecca Coepland "Converging NGN Wireline and Mobile 3G Networks with IMS", ISBN no. 97808493-9250-4, Informa CRC

[13] IETF drafts for MP TCP: draft-ietf-mptcp-multiaddressed-03.txt, draft-ietf-mptcp-congestion-03.txt; draft-ietf-mptcp-api-01.txt; http://www.rfc-editor.org/rfc/rfc6182.txt

[14] IETF RFC 4555, "IKEv2 Mobility and Multihoming Protocol (MOBIKE)"