Aiash, Mahdi ORCID logoORCID: https://orcid.org/0000-0002-3984-6244, Mapp, Glenford E. ORCID logoORCID: https://orcid.org/0000-0002-0539-5852, Lasebae, Aboubaker ORCID logoORCID: https://orcid.org/0000-0003-2312-9694, Augusto, Mario, Vanni, Renata M. P. and Moreira, Edson (2011) A QoS framework for heterogeneous networking. In: Internation Conference on Wireless networks 2011 (ICWN'11), 6th - 8th July 2011, London. . [Conference or Workshop Item]

This version is available at: https://eprints.mdx.ac.uk/7795/

A QoS Framework for Heterogeneous Networking

Mahdi Aiash, Glenford Mapp, and Aboubaker Lasebae, *EIS, Middlesex University*
Mario Augusto, Renata Porto Vanni, and Edson Moreira, *ICMC, University of Sao Paulo*
Raphael Phan, *Electronic and Electrical Engineering School, Loughborough University*

Abstract—**In order for next generation networks to support effective handover procedures, there is a need for defining QoS signaling mechanisms that guarantee the provision of point- to-point as well as network level QoS. This paper proposes a QoS signaling mechanism to be implemented by the Y-Comm architecture as a potential 4G framework. The proposed mechanism requires certain level of cooperation among network elements; therefore, it proposes some functional modules/ interfaces to be run on different network entities. As showed in the paper, the proposed mechanism could be implemented in different scenarios such as initial registration and connection, and also in the case of handover.**

Index Terms—**Network Level of Agreement, Service Level of Agreement, Administrative domain, the Y-Comm framework**

I. Introduction

In multi-technology and multi- operator environment such as 4G networks, the mobile terminal (MT) should be able to access the service regardless of the access network technology. Consequently, huge cooperation among different operators is required to enhance user experience. To deal with QoS variation of the access networks and for an end- to- end provision of QoS, a novel architecture is needed to deal with network resources reservation as well as enabling an end- to- end QoS signaling.

The Y-Comm framework as introduced in [1][2] is a reference communication framework to support mobility in heterogeneous networks, this is referred to as Vertical Handover (VH). However, for the Y-Comm procedure to fully support (VH) in 4G systems [3], it has to consider the diversity of security and QoS among different networks. While the security issue has been tackled by the Y-Comm Integrated Security Module (ISM) [4][5], there is still a need for defining an approach for signaling and providing QoS over an heterogeneous environment such as in the 4G system.

The paper is laid out as following: Section 2 gives a brief introduction to the Y-Comm communication framework. Network architecture is viewed in Section 3 then, a detailed view of the network architecture; the used protocols and entities structure are given in Section 4. An attempt to map the functionalities of these entities to the Y-Comm layers is introduced in Section 5. While in Section 6, different practical implementation of the proposed framework such as Registration, Connection and inter/ intra administrative domain Handover are explained. A conclusion and further work is included in Section 7.

II. The Y-Comm Architecture

As shown in Fig 1, the Y-Comm architecture uses two frameworks. The first is the Peripheral framework which deals with operation on the mobile terminal. The second is the Core Framework and deals with functions in the core network to support different peripheral networks. Both frameworks share the two bottom layers: the Hardware Platform Layer (HPL) which classifies the wireless technologies based on their electro- magnetic spectrum. The Network Abstraction Layer (NAL) provides a common interface to control different wireless network.

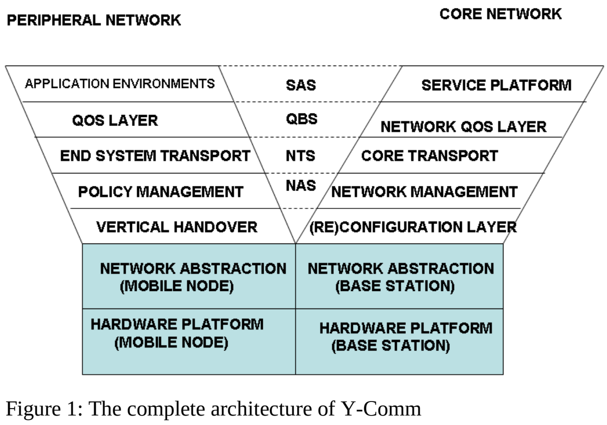

Figure 1: The complete architecture of Y-Comm

In addition to the previous two layers, the peripheral framework consists of the following layers: The Vertical Handover Layer (VHL) triggers the handover by acquiring network resources and signaling the handover, it also does context transfer and packet redirection after the handover [3]. The Policy Management Layer (PML): by considering different parameters such as user preference and network availability, this layer decides whether to perform a handover or not. The End Transport Layer (ETL) provides the functions of the Transport and Network layers of the TCP/IP module. The QoS Layer (QL) has two interfaces: the first interacts with the applications in the Application Environment Layer to specify their required QoS to the system. The second interface tries to guarantee and maintain network- level QoS over varying access networks. The Applications Environment Layer (AEL) defines the applications running on the Mobile terminal in the peripheral networks.

The Core framework consists of the following layers: The Reconfiguration Layer (REL) is responsible for reserving network resources to accommodate the handover. The Network Management Layer (NML) manages and controls the peripheral networks, attached to the core network; it also gathers information on these networks and launches it to the Policy Management Layer (PML) on the (MT). The Core Transport System (CTS) manages data movement in the core network. The Network QoS Layer (NQL) this layer is responsible for managing QoS and performing load balancing between the attached peripheral networks, this layer also monitors the utilization of network resources in terms of QoS. It is worth pointing out that, the functionalities of the NQL are provided on different entities which are distributed over the network. The Service Platform Layer (SPL) allows different service providers to install and run their services.

Fig 1 shows the security module which comprises four layers: The Network Architecture Security (NAS) defines the threats resulting on moving to a particular network. The Network Transport Security (NTS) is used by the end device to define its accessibility over the Internet. The QoS Based Security (QBS) deals with degrading of QoS due to security breaches. On one hand, it controls the access and utilization of network resources and services accordingly to the user contract; this contract comprises two agreements: the Network Level of Agreement (NLA) which specifies the access networks, the user could use along with their associated QoS, the Service Level of Agreement (SLA) defines the user's subscribed services with the required QoS. The Service And Application Security (SAS) deals with authenticating the user to use the terminal and the service.

Based on the Y-Comm architecture, we might view the future Internet as composed of a fast core network with attached slower peripheral networks via Core End-Points (CEPs) as shown in Fig 2.

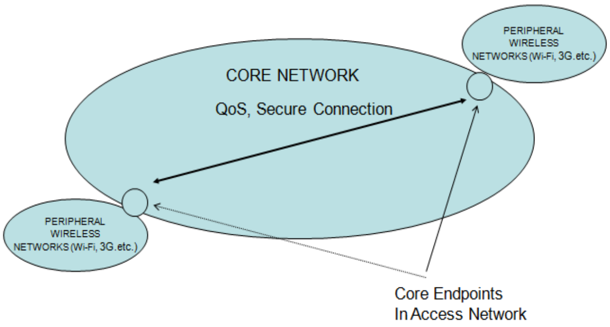
CORE NETWORK
QoS, Secure Connection
PERIPHERAL WIRELESS NETWORKS (Wi-Fi, 3G.etc.)
PERIPHERAL WIRELESS NETWORKS (Wi-Fi, 3G.etc.)
Core Endpoints
In Access Network

Figure 2: Future Internet structure

III. NETWORK ARCHITECTURE OVERVIEW

Fig 2 shows a very simplified view of the Internet structure. This section presents a more detailed view of the network. As shown in Fig 3, the Core End-Point (CEP) represents an Administrative domain(Ad-domain) [6][7], connected to one or more domains. Although, each domain is technology dependent, cooperation between domains is possible and is managed by the Core-end point

Similarly to [6][8], for scalable support of Security, QoS and handover in heterogeneous networks, different operating entities exist in the network such as Domain QoS Broker (DQoSB), Core QoS Broker (CQoSB) and A3C servers. These entities collaborate and function on both network and service management.

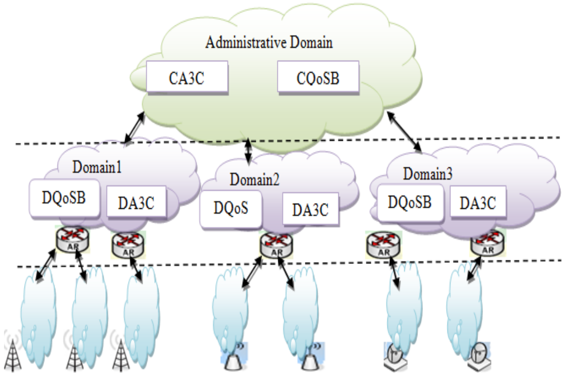

Figure 3: Network Hierarchal structure

A. Core A3C (CA3C)

The top level A3C server resides in the administrative domain and is responsible for service level management. It holds users' Service Level Agreements (SLA) which contains the subscribed services along with the associated QoS and Network Level Agreements (NLA) which contain the networks- the Operators-, the user can access with the corresponding QoS. The NLA is passed to the CQoSB for network level management.

B. Core QoS Broker (CQoSB)

It plays a major role in managing inter- Administrative domains functions as well as negotiating QoS parameters with other CQoSBs in the case of cross administrative domain connection. CQoSB initially extracts users' Network Level of Agreement (NLA) from the CA3C.

C. Domain A3C (DA3C)

The DA3C is responsible for handling users' service aspects [8]. Initially, it extracts users' profile information from the CA3C and uses this information for authorizing the users' requests to access services.

D. Domain QoS Broker (DQoSB)

It gets user's profile information from the CQoSB and manages the resources of the attached peripheral networks with respect to the user preference and network availability, it also makes a per-flow admission control decision. In order to support handover, DQoSB uses a Network Intelligent Interface Selection (NIIS) module [9][7] for load balancing and handover initiation between peripheral networks. There is an obvious resemblance between the QoSB and the Visitor Location Register (VLR) of the circuit switching systems [15].

E. Access Router (AR)

This is the link between the domain and the peripheral networks; it enforces the DQoSB's admission control decision.

F. Mobile Terminal (MT)

The MT user's device, used to access the network and request a service. To comply with the heterogeneity of 4G systems, the MT should be able to get the subscribed service using the best available access network. Therefore, for the integration of Handover and QoS, the MT contains mobility decision module called Intelligent Interface Selection (IIS) [7][9] and a QoS module called QoS Client (QoSC).

Optionally, some service providers- not shown in Fig 3- such as video on- demand providers might reside in the Core end-point or the Administrative domain; these providers have agreements with the network providers to guarantee the required QoS [8].

IV. Network Structure and Entities

This section starts by explaining the network elements structure; it then defines possible protocols for the connection between the elements.

A. Network entities structure

In our design, we separate the Service and Network management elements. However, for these elements to interact using the above protocols, they should contain certain interfaces as shown in the figures below.

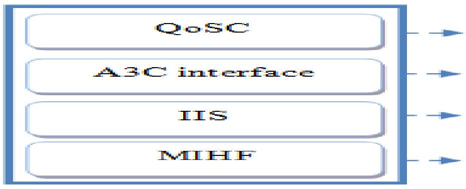

Figure 4: The Mobile terminal structure

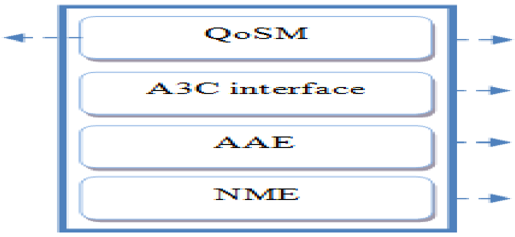

Figure 5: The Access Router structure

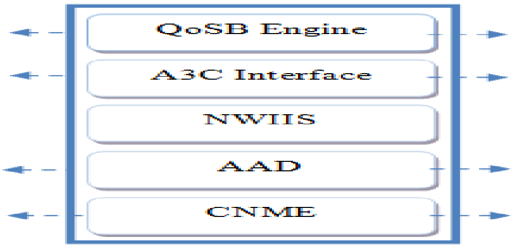

Figure 6: The Domain QoS Broker (DQoSB) structure

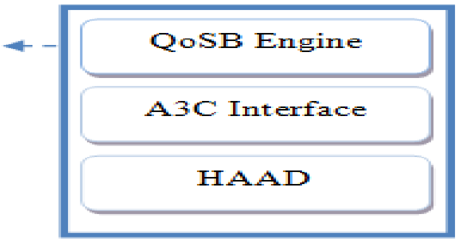

Figure 7: The Core QoS Broker (CQoSB) structure

1) *The Mobile Terminal (MT)* has four interfaces: QoS Client (QoSC) talks to the QoS Manager (QoSM) of the Access Router, A3C interface enables the client to send A3C Registration/ de- registration requests to the A3C server; the Intelligent Interface Selection (IIS) to choose the best network for a handover based on user preference and network availability, and Media Independent Handover Functions (MIHF) which is used to control the NICs of the Mobile terminal and perform handover based on the IIS module decision.

2) *The Access Router (AR):* comprises five modules: QoSM which has two interfaces one with the QoSC and the other with the QoSB engine of the DQoSB, A3C interface used to talk to the DA3C; Access Admission Enforcement (AAE) module enforces the decision of the Access Admission Decision module (AAD) in the DQoSB; Network Monitoring Entity (NME) module monitors the utilization of network resources and reports this to the Centralized NME (CNME) module of the DQoSB, the MIHF module enables the (AR) to manage different types of peripheral networks

3) *The Domain QoS Broker (DQoSB*): the DQoSB has five modules: the QoSB Engine which makes management decisions and has two interfaces: one with the QoSM of the (AR) and the other with the CQoSB in the administrative domain, A3C interface to talk to the DA3C server in the domain; NWIIS module to manage the ARs and support load balancing, Access Admission Decision (AAD) module acts as a proxy for the high level AAD (HAAD) in the Core endpoint, and provides the AAE with policy- related decisions; the CNME module, as proposed in [13] comprises two main sub-modules: a Merger sub-module which aggregates the traces from NMEs and provides a coherent view of the traffic status. Analysis engine does a screening for network resource utilization and informs other modules of any abnormalities.

4) *The Core QoS Broker (CQoSB)* comprises three modules: the QoS Engine manages inter-domain connection and provides end-2-end QoS across

administrative domains, the A3C interface is used for the interaction with the CA3C server.

B. *Network protocols*

In the proposed QoS framework, to convey QoS –related information, network entities have to interact using a common language. Three different types of protocols are needed for the network entities interactions.

For the connection between the AAE and AAD, there is a need for policy information and configuration exchange protocol such Common Open Policy Service (COPS) [10]. In our architecture, the access router (AR) acts as (AAE), the DQoSB acts as AAD and the CQoSB acts as a top level AAD. We used the concept of policy for a network level access control. However, for authorizing the service level request, we propose using an A3C such as DIAMETER [6][11] or RADIUS [14] protocols.

The A3C protocol with its basic structure [11] has no QoS- related functions. Therefore, an enhanced version of the protocol [12] introduces three QoS- context aware entities: **Resource Requesting Entity (RRE)** which triggers the authorization process, **Authorizing Entity (AE)**, an A3C server processes the access request and generates a permit/ deny decision to the **Network Element (NE)**. The (NE) is an intermediate router between the AE and the RRE and acts as a client to the AE. Additionally, the extension proposes four new messages which are used to request QoS-related resource authorization for a given flow and then to activate the reserved resources to accommodate the connection. In the proposed architecture, the authorization process is triggered by the MT, acting as a (RRE) entity. The access router (AR) corresponds to an (NE) and the DA3C acts as (AE). For the initial request, DA3C contacts the CA3C and gets the required information for authorizing the request; this information might be cashed for later requests.

Since the Mobile terminal (MT) deals with different types of access networks, it needs a common interface to hide these differences. The IEEE 802.21 protocol introduces the Media Independent Handover Functions (MIHF) module [9] to manage the resources in the peripheral networks regardless of their technologies.

V. THE NETWORK ARCHITECTURE IN THE CONTEXT OF Y-COMM

This section shows a possible mapping between the afore-explained modules and the Y-Comm layers. On one hand, while The CQoS module of the MT corresponds to the QoS layer in the peripheral framework, the QoSM, QoSB engines in the DQoSB and the CQoSB are mapped to the Network QoS Layer (NQL) of the core framework. On the other hand, the Access Admission- related modules: the AAE, AAD and the HAAD which provide access control in two different scenarios: controlling the access of the MT to a specific network based on the user's NLA. Also, they might be used by the end –point servers to specify the server's accessibility, since server's NAL defines its visibility i.e. locally, in the local network (LAN) or globally over the Internet. Such access control mechanisms might be provided as a part of the Y-Comm security module.

The IIS and NWIIS modules correspond to the Policy Management layer (PML) on the peripheral framework and the Network Management Layer (NML) of the core framework respectively. The functionality of the monitoring modules (NME, CNME) is provided through the QoS (QL) and Network QoS (NQL) layers as well as the security module. The MIHF module could be used in the Network Abstraction Layers (NAL) to deal with different access networks. The A3C interfaces mainly manages the interactions with the A3C severs and thus, is considered as a part of the security module.

VI. QOS SESSION SETUP

The proposed QoS framework deals with three distinct scenarios [8]: Initial Registration, Connection initiation and Handover. To provide QoS in each of these situations, both the service level entities – DA3C and CA3C- and the network level elements – AR, DQoSB and CQoSB- interact with each other using the COPS, DIAMETER and IEEE 802.21 protocols.

A. *Registration*

Initially, the user subscribes to a Network Level of Agreement (NLA) and Service level of Agreement (SLA), containing the user's access network and the subscribed services along with the associated QoS and security parameters, this information are shared between the MT and the CA3C in the administrative domain. The QoSB engine of the CQoSB gets a copy of the NLA. As shown in Fig 8, once the (MT) gets an IP address, it should be authenticated by the A3C server in order to access the network. After a successful authentication, the AAE of the AR asks the AAD of the DQoSB for a user- specific Access Decision (AD Req). Since it is the first interaction with this user, the DQoSB approaches the CQoSB- the HAAD module- for this information, the HAAD extracts user's profile from the QoSB Engine and passes the decision - via (AD Res) message- all the way back to the (AR) which configures the access policy according to the received profile and sends an acknowledgment message (Ack).

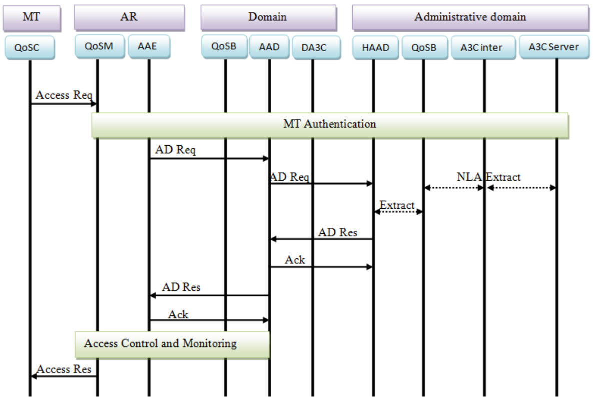

Figure 8: The Registration process

B. *Connection initiation*

In the case of a connection between the MT and a server (S), residing in the same Administrative Domain(Ad-Domain) but in a different domain- domain1 and domain2-, the MT initiates a connection request -with a required QoS denoted in the QoS Specification (QoS-Spec) field - to the server (S). If the request complies with the network access policy configured on the AR of the source domain, an Authorization Request (Auth-Req) to access the service with the QoS stated in the QoS-Spec is initiated towards the DA3C server. If the DA3C holds a copy of the user's profile, it responds with Authorization Response (Auth-Res) message; otherwise, it passes the request to the CA3C server which holds user's contract details. In the case of a successful authorization, the QoSM of the AR in the source domain forwards the access request to the QoSM of the AR in the destination domain. This triggers the same request authorization process as in the first domain. As shown in Fig 9, in the case of a successful authorization, resources in the destination domain are activated using Resources-Activation request/ response messages (Resc-Act. Req / Res), L2 resources are allocated IEEE 802.21 messages, and then an access response is sent back to the AR in the source network. Upon the recipient of a positive access response, resources in the source network are activated using (Resc-Act. Req/Res) messages, these activities in the source network were not shown in Fig 9.

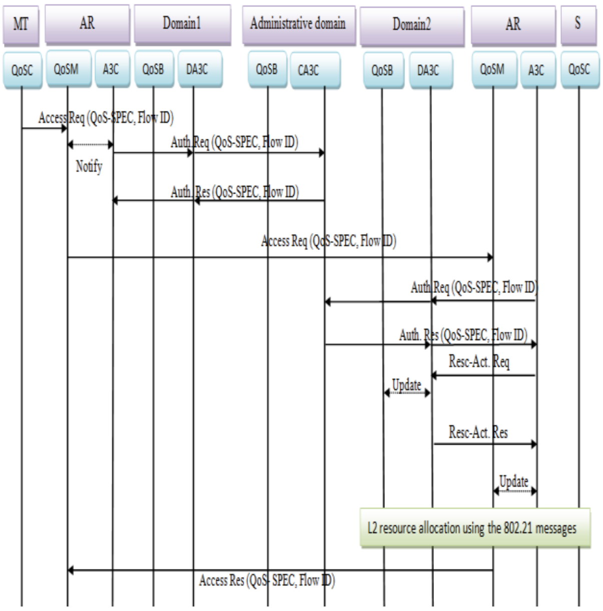
MT
AR
Domain1
Administrative domain
Domain2
AR
S
QoSC
QoSM
A3C
QoSB
DA3C
QoSB
CA3C
QoSB
DA3C
QoSM
A3C
QoSC
Access Req (QoS-SPEC, Flow ID)
Notify
Auth Req (QoS-SPEC, Flow ID)
Auth Res (QoS-SPEC, Flow ID)
Access Req (QoS-SPEC, Flow ID)
Auth Req (QoS-SPEC, Flow ID)
Auth. Res (QoS-SPEC, Flow ID)
Resc-Act. Req
Update
Resc-Act. Res
Update
L2 resource allocation using the 802.21 messages
Access Res (QoS- SPEC, Flow ID)

Figure 9: Connection initiation

C. *Handover*

This section explains QoS provision in the case of intra and inter-administrative domain handover. As shown in Figs 10 and 11, the MT gets QoS -related information about available networks, the IIS module of the MT decides on the target network and a Handover request containing the desired associated QoS is sent to the QoSM module of the AR which passes it all the way to the DQoSB2 via the Core end- point. The MT has to be authenticated; also the security keys should be launched in the target network before the handover really happens. To apply the right access control in the new network, the AAD module of the DQoSB2 approaches the HAAD of the core end- point to get the Admission Decision related to the user. After configuring the access policy in the target Access Router, it starts L2 resources reservation using IEEE802.21 messages. A successful handover response message is sent back to MT to trigger the actual handover.

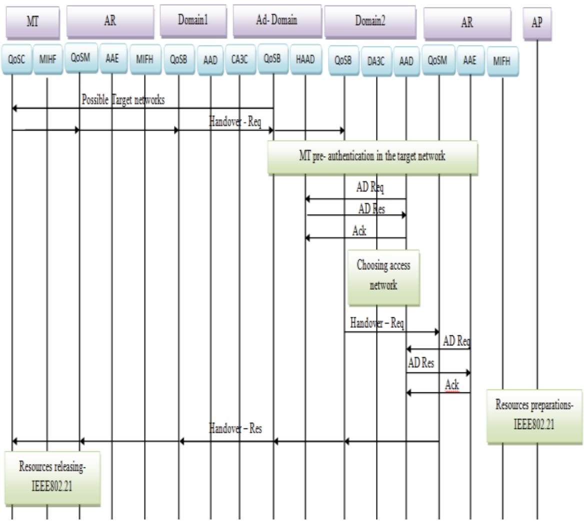

Figure 10, Intra-Administrative domain handover

In the case of an Inter- Administrative domain handover, the old Core-end point (CEP) provides the target CEP with the user's SLA and NLA; thus, the MT's related information becomes available in the target network. The remainder steps are very similar to the intra-administrative domain handover as shown in Fig 11.

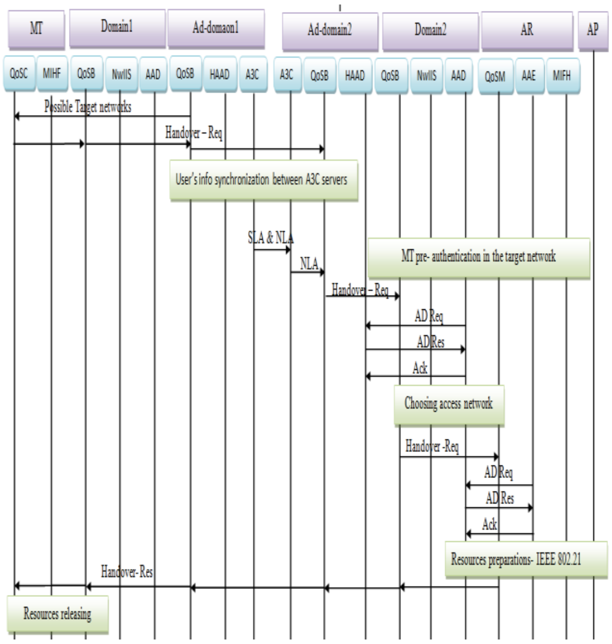

Figure11. Inter-Administrative domain handover

VII. Conclusion

Dynamics and heterogeneity are the main distinct features of 4G system, and they bring about huge challenges in terms of providing Security and QoS. Therefore, any successful communication system should be able to effectively tackle these two issues. With Y-Comm as a potential framework for 4G system, security aspect has been dealt with using an Integrated Security module. The proposed architecture in this paper might be considered as a potential QoS framework for Y-Comm; however, a further experimental and analytical study is needed to validate the performance of the proposed architecture, and this is next goal of our ongoing research.

References

[1] G . Mapp, F. Shaikh, D. Cottingham, J. Crowcroft, and J. Beliosian," Y-Comm: A Global Architecture for Heterogeneous Networking". (Invited Paper). 3rd Annual International Wireless Internet Conference (WICON 2007), October 2007.

[2] G. Mapp, D.N. Cottingham, F. Shaikh, P. Vidales, L. Patanapongpibul, J. Balioisian, and J. Crowcroft, "An Architectural Framework for Heterogeneous Networking". International Conference on Wireless Information Networks and Systems (WINSYS), pp. 5-10. August 2006

[3] G. Mapp, F. Shaikh, M. Aiash, R. Porto Vanni, M. Augusto and E, "Exploring Efficient Imperative Handover Mechanisms for Heterogeneous Wireless Networks", International Symposium on Emerging Ubiquitous and Pervasive Systems (EUPS-09) August 2009.

[4] M. Aiash, G. Mapp, A. Lasebae, amd R. Phan, " Providing Security in 4G Systems: Unveiling the Challenges". AICT 2010. Barcelona, Spain, 9-15 May 2010.

[5] G. Mapp, M. Aiash, A. Lasebae and R. Phan, " SECURITY MODELS FOR HETEROGENEOUS NETWORKING" . SECRYPT 2010, Athens, Greece, 26-28 July.

[6] M. Almeida, D. Corujo, S. Sargento, V. Jesus and R. Aguiar, "An End-to-End QoS Framework for 4G Mobile Heterogeneous Environments" , OpenNet Workshop, March 27-29, 2007, Diegem, Belgium

[7] S. Sargento, V. Jesus, F. Sousa, F. Mitrano, T. Strauf, J. Gozdecki, G. Lemos, M. Almeida, D. Corujo, "Context-Aware End-to-End QoS Architecture in Multi-technology, Multi-interface Environments" Proc. 16th IST Mobile & Wireless Communications Summit, Budapest, Hungary 1-5 July 2007.

[8] V. Margues, R,L. Aguiar, C. Garcia, J, I. Moreno, C. Beaujean, E. Melin and M. Liebsch, "An ip- based QoS architecture for 4G operator scenarios" IEEE Wirless Communications, Vol. 10, June 2003, pp. 54-62.

[9] Institute of Electrical and Electronics Engineers. IEEE 802.21/D8.0, Draft Standard for Local and Metropolitan Area Networks: Media Independent Handover Services, December 2007.

[10] D. Durham, Ed, J. Boyle, R. Cohen, S. Herzog, R. Rajan and A. Sastry, "The COPS (Common Open Policy Service) Protocol" RFC 2748.

[11] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, " Diameter Base Protocol" , RFC 3588.

[12] D. Sun, Ed, P. McCann, H. Tschofenig, T. Tsou, A. Doria and G. Zorn, Ed , "Diameter Quality-of-Service Application," RFC 5866.

[13] Y. Sheng, G. Chen, K. Tan, U. Deshpande, B. Vance, H. Yin, C. McDonald, T. Henderson, D. Kotz, A. Campbell, J. Wright, "MAP: A scalable monitoring system for dependable 802.11 wireless networks," IEEE Wireless Communications, Special Issue on Dependability Issues with Ubiquitous Wireless Access. 15(5):10-18, October 2008

[14] C. Rigney, S. Willens, A. Rubens, W. Simpson " Remote Authentication Dial In User Service," RFC 2865.

[15] P, Chandra, "Bulletproof wireless security : GSM, UMTS, 802.11 and ad hoc security," Newnes. Oxford, pp. 129-158, 2005.