Mobility Management, Quality of Service, and Security in the Design of Next Generation Wireless Network

Deeya S Nursimloo *(deeya@crg.uct.ac.za)*, *Student Member*, *IEEE* and H Anthony Chan, *SrMember*, *IEEE* *(h.a.chan@ieee.org)*

Department of Electrical Engineering, University of Cape Town, Private Bag, Rondebosch 7701, South Africa

***Abstract*—The next generation wireless network needs to provide seamless roaming among various access technologies in a heterogeneous environment. In allowing users to access any system at anytime and anywhere, the performance of mobility-enabled protocols is important. While Mobile IPv6 is generally used to support macro-mobility, integrating Mobile IPv6 with Session Initiation Protocol (SIP) to support IP traffic will lead to improved mobility performance. Advanced resource management techniques will ensure Quality of Service (QoS) during real-time mobility within the Next Generation Network (NGN) platform. The techniques may use a QoS Manager to allow end-to-end coordination and adaptation of Quality of Service. The function of the QoS Manager also includes dynamic allocation of resources during handover.**

Heterogeneous networks raise many challenges in security. A security entity can be configured within the QoS Manager to allow authentication and to maintain trust relationships in order to minimize threats during system handover. The next generation network needs to meet the above requirements of mobility, QoS, and security.

***Index Terms* —Mobility, NGN, QoS, Security, Wireless.**

I. Introduction

As Wireless communication evolves towards providing high-speed real-time and non-real-time multimedia services, it is desired to enable the end-user to access the network at anytime and anywhere. In order to provide ubiquity, different networks using different radio technologies will have to be integrated within the next generation wireless network environment to allow the user to be connected to a network that best suits one's needs. The handover (handoff) from one network to another in this heterogeneous environment will appear to the users as a smooth handover within a homogeneous network.

A preliminary design of 4G Wireless network was presented in [1]. The design considerations of mobility management, QoS, and security in the next generation wireless network are discussed here.

The next generation wireless networks are expected to include different access networks, which will need to provide the services of mobility management, QoS, and security as detailed in Section II. In the design considerations of mobility management, the IP-based protocols are compared for enabling seamless mobility across different access technologies as well as within the same network (Section III). The QoS functions, such as resource management, may be coordinated by a QoS manager (Section IV). In the heterogeneous network environment, additional security issues are encountered and have to be considered in conjunction with the QoS requirements during handover (Section V).

II. Access Networks and Services

A variety of wireless access networks are expected to coexist within the next generation wireless network environment to allow the user to connect to the best wireless system that will provide the suitable services to the user [2]. Fig. 1 illustrates the various types of wireless networks that can be included in the next generation wireless network environment.

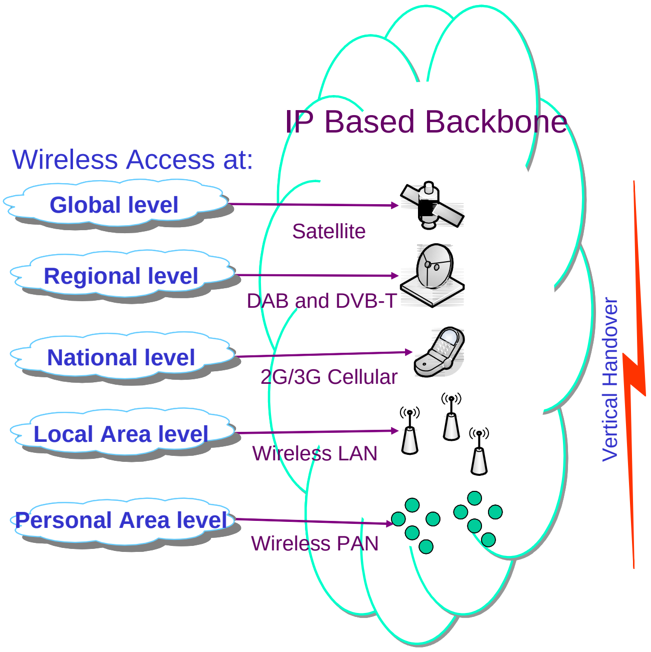

Fig. 1. Different levels of mobility in the wireless system.

At the global network level, satellite systems and High Altitude Platform provide broadband global access.

Networks at the regional level will include systems such as Digital Audio Broadcasting (DAB) and Digital Video Broadcasting-Terrestrial (DVB-T). The networks at this level have to ensure full coverage for global roaming to

Manuscript received July 21, 2005. This work is supported in part by Telkom, Siemens, and National Research Council, South Africa under the Broadband Communication Center of Excellence program.

enhance broadband services.

Networks at the national level consist of cellular networks such as 2G, GPRS, and 3G Wireless. At this level, the system will provide nationwide coverage of network services with a high degree of mobility. These systems have high capacity and support data rates up to 2 Mbps in 3G Wireless.

Networks at the Local area level, which can also be called the “Hotspot” level, include IEEE 802.11(a, b, g, n) WirelessLAN and HIPERLAN link. These technologies support individual user links and are best suited for high data-rate applications. WirelessLAN is also flexible to support adaptive modulation schemes and asymmetric data services [3]. These systems typically work on a distance range of the order of 100 meters, which is shorter than that of those systems described above.

Personal area level networks will include technologies such as Bluetooth. These technologies allow the user to interact with different equipments, e.g., laptops, printers, and refrigerators within an office or home environment. Ad hoc wireless services may be implemented for accessing these different technologies.

Access networks also include fixed access network such as ADSL and coaxial systems, which do not fall under the wireless system.

The essential services of the network at any level, irrespective of the access technologies, include mobility management, Quality of Service, and security. A conceptual layer model specifying these required services is shown in Fig. 2.

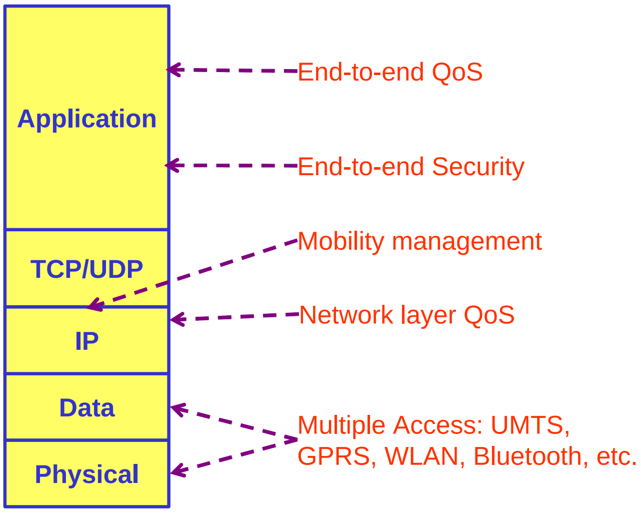

Fig. 2. Different Services are handled at layers above the network access layers.

III. Mobility Management

Mobility management consists of location management and handover management [4].

Location management continuously monitors the location of the mobile terminal and provides input to a database of system locations.

Handover Management ensures the mobile terminal maintains a continuous connection as it moves from one wireless point of access to another.

In the next generation wireless network system, the different access technologies of the network will be connected to an IPv6 core network and to the Internet [5]. Therefore IP-based protocols are needed to enable mobility. We will consider these protocols under the two types of mobility mechanism: macro-mobility and micro-mobility. As shown in Fig. 3, macro-mobility refers to mobile nodes moving between two networks. Micro-mobility refers to mobile nodes moving within a network. In addition, vertical handover involves mobile nodes moving between access points of different network types, while horizontal handover involves mobile nodes moving between access points of the same network type [6].

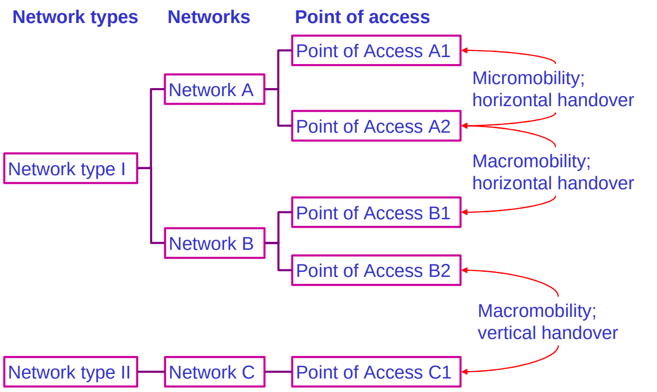

Fig. 3. Handover in Next Generation Network

A. *Macro-mobility*

Macro-mobility technology allows the mobile node to move to networks which may be of the same network type or of different network type. The relevant protocols considered here are Mobile IPv6 and Session Initialization Protocol (SIP). The characteristics of these protocols are compared in Table I.

TABLE I
Comparison of The Macro-Mobility Protocols MIPv6 and SIP.

	MIPv6	SIP
OSI Layer	Layer 3	Layer 3
Paging	On Request	✗
Signaling	✓	✓
Triangular Routing	✗	✗
Intra-Mobility Tunneling	——	——
Host	HA	SIP
Handover	Fast	——

Mobile IPv6 allows IPv6 nodes to move across different networks, which may be heterogeneous [6]. It also offers route optimization, which allows a mobile node to directly send packets to an IPv6-compatible correspondent node (CN). Route optimization therefore reduces transmission delay and achieves better network performance required for real-time applications such as Voice over IP.

While Mobile IPv6 is generally used to enable macro-mobility whereas SIP is generally used in signaling, integrating these protocols to support IP traffic will lead to improved mobility performance [7].

B. *Micro-mobility*

Micro-mobility technology enables a mobile node to move within a network domain with minimal handover disruptions. Micro-mobility protocols handle handover signaling and forward packets within the domain [8].

Some IP-based micro-mobility protocols are Handover Aware Wireless Access Internet Infrastructure (HAWAII), Cellular IP, Hierarchical Mobile IP (HMIP), and Intra Domain Mobility Protocol (IDMP). Table II compares these protocols in terms of paging, signaling, routing, intra-mobility tunneling, and handover.

There are two types of micro-mobility handover routing schemes: tunnel-based scheme and route-based scheme. Tunnel-based routing scheme enables scalability of the network. However route-based scheme is more robust against signaling load. Yet, route-based scheme causes more propagation delays than tunnel-based scheme.

TABLE II.
COMPARISON OF DIFFERENT MICRO-MOBILITY PROTOCOLS.

	HAWAII	Cellular IP	HMIP	IDMP
OSI Layer	Layer 3	Layer 3	Layer 3.5	Layer 3
Paging	✓	✓	✓	On Request
Signaling	✓	✓	✓	✓
Triangular Routing	✓	✓	✓	✓
IntraMobility Tuneling	✗	✗	✓	✓
Host	CoA	HA	CoA	LCoA
Handover	Routing-based	Routing-based	Tunnel-based	Tunnel-based
	Forward/ Non-Forward scheme	Semi soft/Hard	Hard	Fast

HMIP or Cellular IP is generally used to handle micro-mobility. An analysis to compare the characteristics of different micro-mobility protocols has been given in [8]. A summarized comparison is provided in Table II, which suggests that HMIP is best suited for micro-mobility management. In addition, the advantage of HMIP is in its use of hierarchies in the network structure to reduce routing delays [9].

Fig. 4 illustrates the interworking of the protocols within the next generation wireless network environment. In this architectural design, a Mobility Anchor Point (MAP) is configured within the access router in each network domain. When a mobile node moves within a domain, MAP will be notified about the change of address through a binding update. The MAP therefore offers the Home Agent (HA) transparency to such a change of address. Therefore the amount of required signaling is reduced.

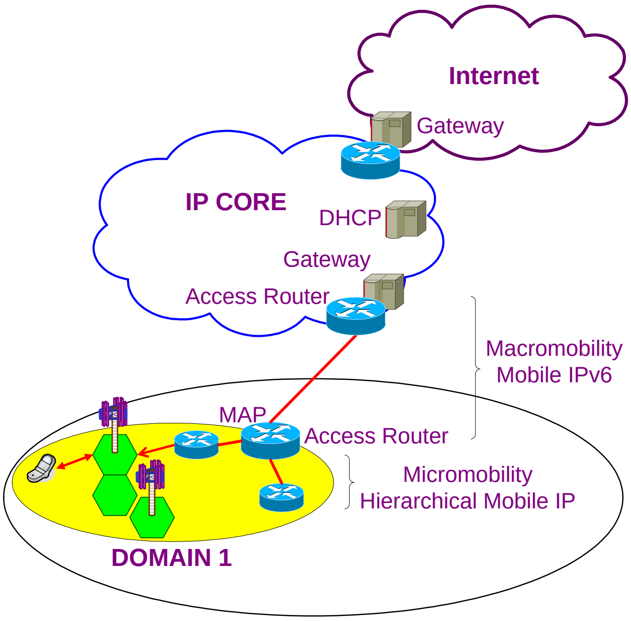

Fig. 4. Interworking of protocols.

IV. QUALITY OF SERVICE

Quality of Service requires a set of technologies that allow network administrators to manage the network to avoid network congestion and manage real-time multimedia traffic. Since the next generation wireless network will be composed of multiple types of services, the network needs to monitor the usage per service and per user. In addition, the network also needs to provide these services while users are moving either within a network or from one network to another.

For the integration and interworking of multiple protocols, research and development is needed in the following areas: signaling, Quality of Service, security and Authentication, Authorization, Auditing, and Charging (AAAC) [10]. The support of QoS especially during handover is a key challenge for this future heterogeneous network. The traffic may have different delays and different fault-tolerance levels. In addition, the channel conditions may often vary in the wireless environment. Yet under all these circumstances, Quality of Service disruptions must be avoided.

The next generation wireless network will accommodate different QoS requirements based on the user applications (Section IV-A). The network resources need to be controlled and allocated appropriately (Section IV-B) to meet the QoS requirements. Such resource allocation needs to be consistent with the policies of the networks (Section IV-C).

A. *Multiple QoS Framework*

In general, applications can receive better service through reservation type QoS scheme but the utilization of network resources will be more efficient through priority type QoS scheme. Therefore a combination of Integrated Services (IntServ) and Differentiated Services (DiffServ) can be used in the network to coordinate Quality of Service along the data flow.

IntServ specifies the characteristics of data flow and the requested service from the network. It uses Resource Reservation Protocol (RSVP) to request the resources along a unidirectional data path. IntServ have three classes: path guaranteed services, controlled load services, and best effort services. These services are end-to-end but Intserv only works best for small scale networks [11].

In DiffServ, the aggregate control handling mechanism is as follows. The priorities of the packets are first identified. Those marked with the same priority are aggregated and then ordered into queue. DiffServ involves less processing and offers better scalability to large networks with even heavy traffic.

Approaches to combine IntServ and DiffServ include using IntServ near the sender and receiver ends in the access networks but using DiffServ in between. At the transition points, the parameters of IntServ and those of DiffServ will need to map to each other properly.

Packet loss may occur in a number of ways. The different recovery mechanisms take place in different layers under the layered network model, and may exchange information between different layers using a cross-layer approach [12].

The buffer at the receiver may overflow when the data transmission rate of the sender is too fast for the receiving side to handle. Flow control mechanisms at the end-to-end transport layer (TCP) are effective for such packet loss.

Packet loss may occur at the wireless link owing to poor RF conditions. Recovery mechanism may then take place in the physical layer or link layer. Packet loss may also occur at the router due to congestion in the network.

Packet loss not owing to congestion may be recovered using automatic resend request (ARQ) messages. Yet when packet loss in the network is owing to congestion, the ARQs from the many senders will only deteriorate the congestion, resulting in more packet loss. Therefore, the sender needs to cut down their transmission rate instead.

Explicit congestion notification (ECN) may be used to notify the sender about congestion. These notifications are achieved by marking the IP packets at the network layer.

A framework to integrate IntServ and DiffServ together with a cross-layer approach involving different layers to provide information, to control the traffic, and to recover the packets may achieve better Quality of Service. The implementation of these QoS functions may be coordinated through a QoS manager.

B. *Quality of Service Manager*

In order to meet the QoS requirements for different data flow, the network needs to manage its resources properly. Such functions may be supported by a QoS Manager whose functions are defined in Fig. 5. The QoS Manager allocates and controls network resources such as bandwidth through the QoS Reservation while also supporting various types of handovers. A seamless handover requires resource allocation before handover. Network policies will be incorporated to provide relevant information to match the service requirements and resources that need to be allocated to the mobile user.

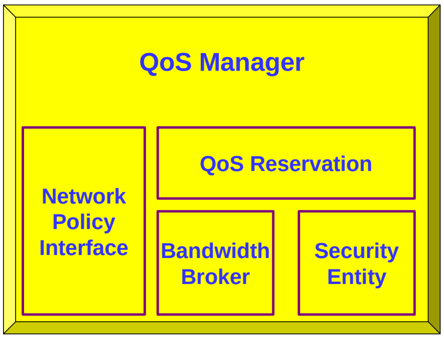

Fig. 5. Components within QoS Manager.

Fig. 6 shows the IP core network with a QoS manager while another QoS manager, known as a Domain QoS (DQoS) manager operates within each network domain. The DQoS manager in Domain 1, the QoS manager in the core, and the DQoS managers in neighboring domains will coordinate with each other to ensure end-to-end QoS resource reservation.

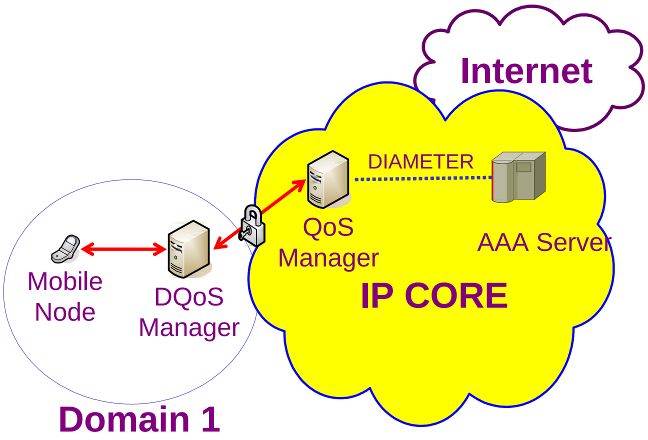

Fig. 6. QoS Negotiations.

A security entity is configured within the QoS manager to coordinate authentication of the user during handover. The security domain entity will support user authentication and data protection.

C. *Protocols to interact between QoS manager and AAA server*

In performing resource allocation functions, the QoS manager needs to interact with the Authentication, Authorization, and Accounting (AAA) server in order to be consistent with the policies of the networks.

The following protocols: Common Open Policy Service (COPS) [13] and DIAMETER Base [14] may be used to coordinate with the AAA server.

1) *COPS*

Common Open Policy Service (COPS) can be used to allow interaction between the QoS Manager and policy enforcement points (PEP) for coordination. This IETF standard protocol supports policy control in IP network. The COPS message system works on a request and response basis. Messages are exchanged between a policy decision point (PDP) in a policy server and policy enforcement points (PEPs) at the networks of the clients.

After the messages have been exchanged, COPS will convey the user information to the transport layer to ensure adequate network service.

2) DIAMETER BASE

The DIAMETER protocol can be used in conjunction with AAA server in the next generation wireless network system. This protocol is designed to transport AAA information between network access server and AAA server. DIAMETER can therefore relay information for authorization. It also has an extension to Mobile IPv6 to support mobility between domains.

The AAA server contains a database of user information which includes user authentication information, services the user is authorized to access, and information of the type of service the user has subscribed to.

D. End-to-end Quality of Service and its Negotiation Protocol

Quality-of-service violations as such frequent packet losses and delays in the mobile environment are undesirable, especially in real-time multimedia service. End-to-end QoS requires one to enforce and to incorporate QoS throughout all network layers of the multimedia systems. End-to-end QoS negotiation protocol may be used to support QoS at the application layer and to coordinate QoS from the network layer to the application layer [15].

In addition, bandwidth availability in the heterogeneous environment will differ significantly so that delay and packet losses may occur. Therefore applications will have to adapt to different network conditions to avoid these losses. The end-to-end QoS negotiation protocol may be used to provide QoS adaptation within resource management to set up a complete QoS framework.

V. Security

From a user's point of view, the network is expected to provide security functions such as privacy, confidentiality, and data integrity to protect the users' assets. Security is especially important here because the integrated heterogeneous system will allow the user to gain access from one network to another. The challenge to network operators and service providers in the next generation wireless environment is to provide new flexible security features to maintain consistent security link across the heterogeneous networks [16].

While the next generation wireless networks shares the security issues common to all networks, the additional challenges are those owing to mobility in a heterogeneous environment. The main features that will be required in integrating security within the new environment are listed in Figure 7 and are outlined below.

A. Attaching/Detaching security mechanism

Within the heterogeneous environment, mobility will involve mobile nodes attaching to and detaching from different networks while continuously preserving confidentiality and privacy (Section V-B), Network trust relationship is needed (based on the network service agreement among the network operators) to determine whether connections can be set up (Section V-C). In addition, authentication mechanism is needed to identify the users (Section V-D) and to ensure their accounting confidentiality (Section V-E).

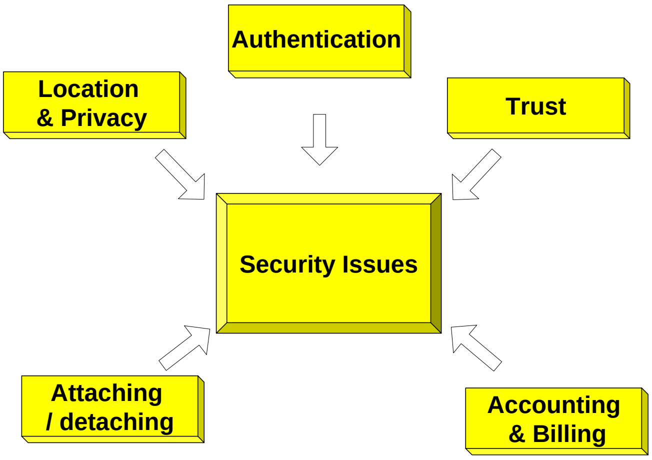

Fig. 7. The security issues in the heterogeneous mobile network.

B. User location and privacy

Location privacy of the user needs to be protected. Yet the IP addressing mechanism needs to tell the position of the mobile node so that the mobile operator knows to which neighboring network it has to correlate to. Therefore the next generation wireless network will need to ensure stronger levels of protection against eavesdropping and other illegal actions which are prone to happen in the heterogeneous mobile environment. New standards to address these issues are needed in future.

C. Trust

The new network that the user moves to must have established a trust relationship so as to enable the user to subscribe to it based on the agreements of the service providers. The trust mechanism in the security system takes place between the mobile operator and the user, and has to abide to the service level agreements between the operators of the networks involved.

D. Authentication

The new network also needs to authenticate the mobile node and the user. Authentication mechanisms will vary, depending on the heterogeneous devices used in the network. The "integrated" identity model in [17] associates a unique identifier to each user no matter what location one is in. The model will correlate this user identifier for end user authentication.

E. Accounting and Billing

Security in accounting and billing is important from the business perspective. There will be different operators allocated to different networks. A change of tariff can then occur during vertical handovers. Therefore security mechanisms have to be set-up to ensure accounting integrity and at the same time maintain user's confidentiality.

VI. Interworking Design

In the design of the next generation wireless network, the IP core and the different wireless networks need to interwork. Issues in mobility, QoS, and security in this heterogeneous network need to be addressed. Our architectural design is shown in Figure 8.

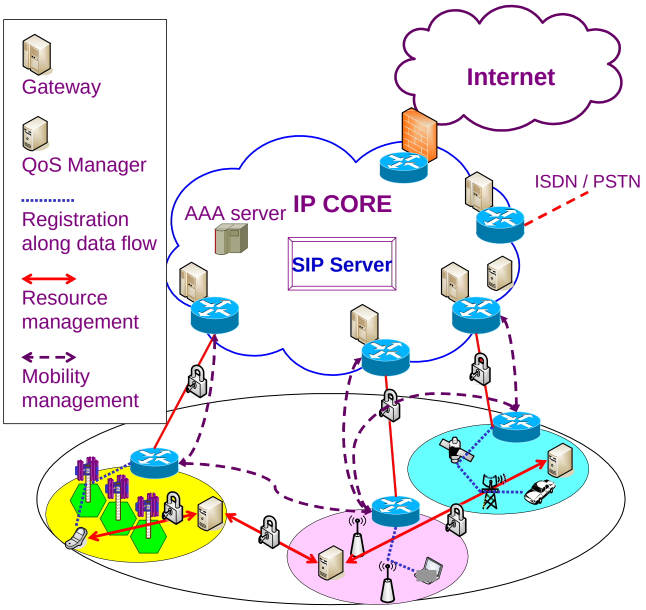

Fig. 8. Design of Next Generation Wireless Network.

A. *Integrating Mobile IPv6 and SIP*

With the emergence of all-Internet Protocol mobile networks, the approach here is to operate protocols at different layers together to support seamless roaming.

In the above architecture, Mobile IPv6 is the appropriate macro-mobility protocol to allow the mobile node to move between networks. On the other hand, Hierarchical Mobile IPv6 will handle micro-mobility. Session Initiation protocol can be applied at the application layer to manage multimedia applications by exchanging multimedia data through peer-to-peer connection.

Because the next generation wireless networks will converge to offer more real-time applications such as video conferencing across the heterogeneous environment, proper quality of data transmission at high data rates will have to be ensured in a seamless manner.

A multimedia data transfer is shown Figure 9. When a mobile node needs to handover (usually triggered at layer 2), it will use a SIP INVITE message to send the signaling request to the SIP proxy. This request will be forwarded to the SIP server (Step 1). In Mobile IPv6 a mobile node which is roaming will be assigned a Care-of-address (CoA) by its Home Agent. In integrating Mobile IPv6, SIP will have to detect the new location of the mobile node through the binding update obtained from Mobile IPv6 (Step 2). A request is sent from the QoS Manager at the IP core to the DQoS manager of the mobile node's domain to check whether sufficient resources such as bandwidth are available for the requested data flow. If there is a scarcity of local resources, the DQoS Manager will send the request to a neighboring DQoS Manager. Meanwhile the QoS Manager will use DIAMETER protocol to communicate with the AAA Server which will then perform authentication and authorization of the user. After (1) the resources have been established, (2) the SIP server has obtained the current location of the mobile node, and (3) the AAA Server has approved the user, an acknowledgment message is sent to the mobile node (Step 3). The connection is now set up so that multimedia data transfer will now take place.

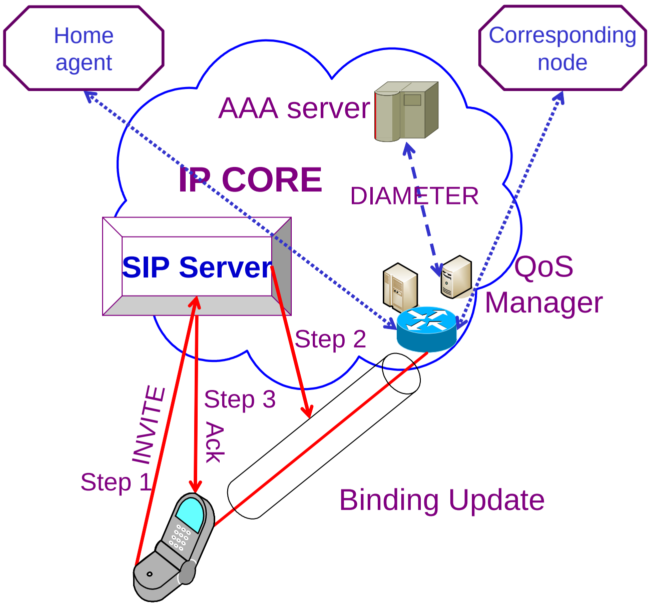

Fig. 9. The integration of Mobile IP and SIP.

The End-to-end QoS negotiation protocol can also be implemented within the SIP sever to provide adaptation of the multimedia traffic to varying network conditions in order to achieve consistency in multimedia flow.

B. *Implementing Quality of Service requirements through Quality of Service Manager*

QoS manager will use relevant information that has been set up by network operators to match the service requirements of the mobile user. During vertical handovers, the QoS manager must dynamically allocate resources. The Quality of Service manager must also adapt to different data rates without degrading Quality of Service such as visual quality when the mobile node is changing networks. In horizontal handovers, the Domain QoS manager will maintain Quality of Service in the intra domain environment.

C. *Ensuring Top-to-Bottom Security.*

It is necessary to bring protection and confidentiality within the domains for the users' applications. Security needs to be taken into account from the beginning of the architectural design, The security mechanisms have to be flexible so as to accommodate the heterogeneous environment. The QoS manager can be optimized to handle security issues by creating a security domain entity within the QoS Resource model. Within the security domain entity, it will provide authentication and protection as data flows through the domain and provide additional security services during handover.

VII. Conclusion

Next generation wireless network will present a new era of wireless communication. It presents design challenges in mobility management, QoS, and security. Yet it offers the opportunity of bringing in new designs for interworking existing technologies in a heterogeneous environment.

From the comparisons tabulated in section III, Mobile IPv6 is best suited for macro-mobility, while Hierarchical Mobile IP will handle micro-mobility. Improved mobility performance can also be achieved by integrating SIP and Mobile IPv6.

Nevertheless, the mobility protocols exhibit limitations. They cause increase in signaling loads and delays during handover, which will affect network performance. The QoS manager is used to maintain Quality of Service in the IP core network while DQoS will maintain QoS within domains. Dynamic allocation of resources during handover will also be accomplished by the QoS Manager.

Different security issues such as authentication are important for heterogeneous networks. A security entity can be configured within the QoS Manager to allow authentication and to maintain trust relationships in order to minimize threats during system handover.

References

[1] Deeya S. Nursimloo and H. Anthony Chan, "Design of a 4G wireless network with mobility management, quality of service, and security," *Proceedings of International Conference on Telecommunication*, Cape Town, 2005.

[2] Keiji Tachikawa, "A perspective on the evolution of mobile communications," *IEEE Communications Magazine*, October 2003.

[3] Sarah Disch and Robert Nicodemus, "3G or 4G: That is the Question,"Available:http://www.columbia.edu/itc/ee/eee6951/2002spring/Projects/CVN/report2.pdf .

[4] Prasan de Silva and Harsha Sirisena, "A mobility management Protocol for IP-based cellular networks," *IEEE Wireless Communication*, June 2002, No. 3, pp. 31-37.

[5] James Kempf and Jonathan Wood, "All IP wireless, all the time," Available at http://research.sun.com/features/4g_wireless/

[6] J. Manner, *et al.*, " Mobility-related terminology," IETF RFC 3753, June 2004.

[7] Deeya S. Nursimloo and H. Anthony Chan, "Integrating fast Mobile IPv6 and SIP in 4G network for real-time mobility," to be published in Proceedings of International Conference on Networks (MICC-ICON 2005), Kuala Lumpur, Malaysia, November 2005.

[8] A. T. Campbell, J. Gomez, S. Kim, and C. Y. Wan, "Comparison of IP micro-mobility protocols," *IEEE Wireless Communication*, Vol. 9, February 2002, pp. 72-82.

[9] Norbert Niebert, *et al.*, "Ambient networks: an architecture for communication networks beyond 3G," IEEE Wireless Communications, April 2004, Volume 11, No. 2, pp. 14-21.

[10] Victor Marques, *et al.*, "An IP-Based QoS Architecture for 4G Operators Scenario," *IEEE Wireless Communications*, June 2003, pp. 54–62.

[11] Jukka Manner, *et al.*, "Evolution of Mobility and QoS interaction," Available at http://www.ctr.kcl.ac.uk/publications/papers/manner_jctn_02.pdf , 2002.

[12] S. Shakkotai, *et al.*, "Cross-Layer design for wireless networks," IEEE Communications, October 2003, Volume 41, pp74-80.

[13] D. Durham, *et al.*, "The COPS (Common Open Policy Protocol)," IETF RFC 2748, January 2000.

[14] P. Calhoun, *et al.*, "Diameter Base Protocol," IETF RFC 3588, October 2004.

[15] Teodora Guenkova-Luy, "End–to-End Quality of Service Coordination for Mobile Multimedia Applications," *IEEE Communications Magazine*, June 2004, Volume 22, No 5, pp 74- 87.

[16] A. R. Prasad, *et al.*, "An Evolutionary Approach towards Ubiquitous Communications: A Security Perspective," *Proceedings of International Symposium on Applications and the Internet* (*SAINT*), Tokyo, Japan, 2004.

[17] Jeroen van Bemmel, Harold Teunissen, and Gerald Hoekstra, "Security aspects of 4G service," *Wireless World Research Forum*, 2002.

Biographies

Deeya S Nursimloo received her B.Sc in electrical engineering from the University of Cape Town in 2004. She is currently a postgraduate student in the same institution. Her current research interests include mobility management, QoS and architectural design of next-generation wireless network.

H. Anthony Chan (M'94–SM'95) received his PhD in physics at University of Maryland, College Park in 1982 and then continued post-doctorate research there in basic science.

After joining the former AT&T Bell Labs in 1986, his work moved to industry-oriented research in areas of interconnection, electronic packaging, reliability, and assembly in manufacturing, and then moved again to network management, network architecture and standards for both wireless and wire line networks. He designed the Wireless section of the year 2000 state-of-the-art Network Operation Center in AT&T. He was the AT&T delegate in several standards work groups under 3rd generation partnership program (3GPP). During 2001-2003, he was visiting Endowed Pinson Chair Professor in Networking at San Jose State University. In 2004, he joined University of Cape Town as professor in the Department of Electrical Engineering.

Prof. Chan is Administrative Vice President of the IEEE CPMT Society and has chaired or served numerous technical committees and conferences. He is a distinguished speaker of the IEEE CPMT Society and has been in the speaker list of the IEEE Reliability Society since 1997.