Quality of Service and Security as Frameworks toward Next-Generation Wireless Networks

ZORAN BOJKOVIĆ, BOJAN BAKMAZ
Faculty of transport and traffic engineering
University of Belgrade
Vojvode Stepe 305, Belgrade
SERBIA AND MONTENEGRO

Abstract: This article aims to analyze quality of service (QoS) and security as frameworks toward next-generation wireless networks. QoS, security and mobility can be viewed as three different indispensable aspects in 4G networks. However all are related to networks nodes involving the controlling or the processing if IP packets for end-to-end flows between a mobile node (MN) and its corresponding node (CN). The goal is to present network mobility issues and requirements in the context from beyond 3G (B3G) toward 4G networks. Finally, as an example soft handover of streamed multimedia in 4G networks is invoked in order to enable the MN to control the handover. Also it is shown that there is no modification to the existing architectures of wireless network, where this handover is used.

Key-Words: quality of service, security, fourth generation (4G) network, handover, next-generation wireless networks

1 Introduction

Many quality of service (QoS) guarantees in multimedia systems is an end-to-end issue, that is from application to application. A key observation is that for applications relying on flows, it is essential that quality of service be configurable, predictable and maintainable system-wide, including the end system devices, communication subsystem and networks. Furthermore, it is also important that all end-to-end elements of distributed systems architecture work in unison to achieve the desired application-level behavior [1]. To date, most of the developments in the area of QoS support have occurred in the context of individual architecture components. Much less progress has been made in addressing the issue of an overall QoS architecture for multimedia communications. However, considerable progress has been made in the separate areas of distributed systems platforms, operating systems, transport systems, and multimedia networking support for quality of service. In end systems, most of the progress has been made in the areas of scheduling, flow synchronization and transport support [2]. In networks, research has focused on providing suitable traffic models and resource reservation protocols [3]. Many current network architectures, however, address QoS from a provider's point of view and analyze network performance failing to address comprehensively the quality needs of applications.

On the other side, new devices and software have made it possible for consumer worldwide to create, manipulate, share, and enjoy media more efficiently in digital forms. The successful development and adoption of media security management technology involve issues within and beyond technology arena. Regardless of how we describe multimedia, security is a very critical part of networking today [4]. Also, it is a very complex and broad topic which is important to recognize the significance of security for future and current users and implementors of multimedia networks. Security is a critical technology in conventional and emerging networks and their applications and services today. Networks are being used in a wide range of computing environments, ranging from distributed embedded systems and system area networks to private enterprise networks and the Internet. Their widespread use has been triggered by the significant development in high-speed transmission systems with low bit error rates at low cost. However, their increasing use in application areas requires the provision of several properties at the network or application layers which are typically considered security properties: privacy of

communication, authentication of parties in an application, high availability of network links and services, among several others. Protection of the network is an important security issue for multimedia service providers, as is the ability to offer customers value added security services as needed or desired. Service or network providers planning for implementation of security mechanisms need to consider: the nature of the security threat, strength of security needed, location of security solutions, cost of available mechanisms, speed and practicality of mechanisms, interoperability.

People want to have continuous high quality services and, at the same time, are unaware of how they will get it and where they are going next. Hence, they need a functioning mobile infrastructure capable of handling high amounts of data. Current mobile standards can be used to transfer data at very limited speed (second generation 2G networks). The next generation, 3G, will offer better data transfer capabilities but its speed is still insufficient for many desired applications like videoconferencing. The next generation, 4G, the fourth generation, will offer data transfer at fully acceptable rate [5]. However, since the 4G will need to use higher frequencies, it also provides much smaller coverage area per a base station. In particular, this means that while users could enjoy continuous videoconferencing, a more complicated infrastructure of service providers has to be set up. Some effort has been done to elaborate on the 4G technical solutions. The 4G networks need a completely different business model and trust relationships compared to the 2G networks.

Starting from beyond 3G toward 4G networks we will analyze the importance of three main parameters: QoS, security and mobility. In the second part, one solution for handover is presented.

2 From Beyond 3G toward 4G

The step to be taken in order to arrive to the goal of 4G is called beyond 3G (B3G). In other words B3G is also known as heterogeneous systems and networks together while 4G is a new air interface. Path to beyond 3G and 4G is shown in Figure 1, where transmission speed in Mbit/s is shown in dependency of cellular environment. By IMT we mean International Mobile Telecommunication.

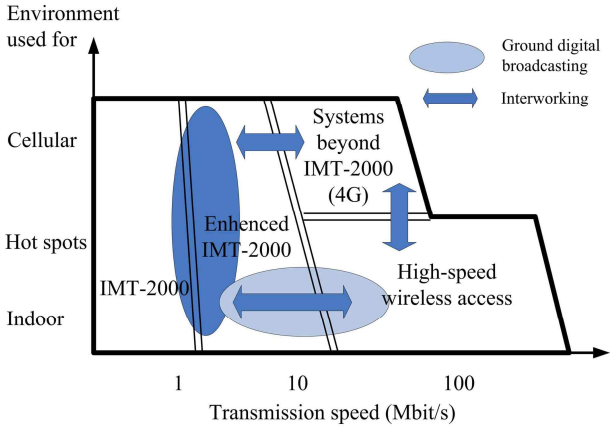

Figure 1. Step to B3G and 4G

Within the rapid development wireless communication networks, it is expected that fourth generation mobile systems will be launched within decades. 4G mobile systems focus on seamlessly integrating the existing wireless technologies including GSM, wireless LAN and Bluetooth. This contrasts with 3G, which merely focuses on developing new standards and hardware. 4G systems will support comprehensive and personalized services, providing stable system performance and quality service.

Different research programs have their own visions on 4G features and implementations. Some key features, mainly from the users point of view of 4G networks, are stated in follows:

- High usability: anytime, anywhere and with any technology,
- Support for multimedia services at low transmission cost,
- Personalization,
- Integrated services.

First, 4G networks are all-IP based heterogeneous networks that allow users to use any system at any time anywhere. Users carrying an integrated terminal can use a wide range of applications provided by multiple wireless networks. Second, 4G systems provide not only telecommunications services, but also data and multimedia services. To support multimedia services high data rate services with good system reliability will be provided. At the same time, a low per-bit transmission cost will be maintained. Third, personalized service will be provided by this new generation network. It is expected that when 4G services are launched, users in widely different

locations, occupations and economic classes will use the services. In order to meet the demands of these diverse users, service providers should design personal and customized services for them. Finally, 4G systems also provide facilities for integrated services. Users can use multiple services from any service provider at the same time. To migrate current systems to 4G with the features mentioned above, we have to face a number of challenges.

Fourth generation (4G) wireless communication systems will be made up of different radio networks providing access to an Internet Protocol version 6 (IPv6) based network layer. In densely populated area, 3G will augment ubiquitous 2,5G networks by providing higher bit rate access. In hotspots and in corporate campuses, Wireless LANs will complement these systems. Multimedia is expected to be a main application of 4G networks. However, multimedia streams can be sensitive to packet loss, which in turn can result in video artifact. Such packet loss can often occur when there is an interruption to a connection when a user is moving between networks that are autonomous.

3 QoS in 4G Networks

Quality of service (QoS) mechanisms, including resource reservation (signaling), admission control and traffic control, allow multimedia applications to get certain quality guarantee e.g., on bandwidth and delay for its packets delivery. Providing QoS guaranties in 4G networks is a non trivial issue where both QoS signaling across different networks and service differentiation between mobile flows will have to be addressed. On the other hand, before providing network access and allocating resources for a mobile node (MN), the network needs to authenticate the mobile nodes (or mobile users) credential. Further more, a security association needs to be established between the mobile node and the network to ensure data integrity and encryption.

IP network element (such as a router) comprises of numerous functional components like mobility, QoS, and for authentication, authorization, and accounting (AAA). We identify these components into two planes: the control plane and data plane functionalities, as shown in Figure 2. The control plane performs control related actions such as AAA, Mobile IP (MIP) registration. QoS signaling, installation (maintenance of traffic selectors and security associations, etc.). The data plane is responsible for data traffic behaviors (classification, scheduling, and forwarding) for end-to-end traffic flows. Some components located in the control plane interact through installing and maintaining certain control states for data plane, with data plane components in some network elements such as access routers (ARs), IntServ nodes or DiffServ edge routers. However, not all control plane components need to exist in all network elements. Also, not all network elements are involved with data plane functionalities.

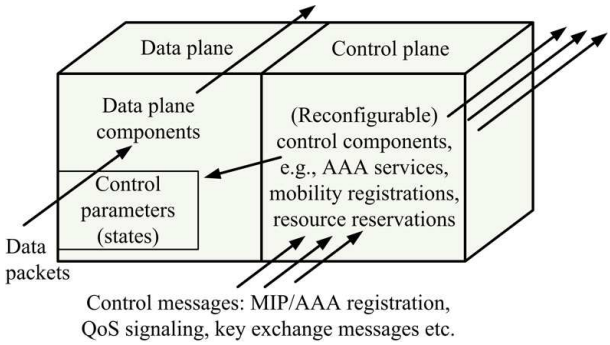

Figure 2. Control plane and data plane

QoS provisioning comprises data plane (mainly traffic control) and control plane (mainly admission control and QoS signaling) functions. We can identify the fundamental difference of QoS provisioning in all-IP 4G mobile networks from a traditional, wired or wireless IP networks. Where-as its resource control mechanisms can be similar to that of traditional networks, changing a location during the life time of a data flow introduces changed data path thus requiring identifying the new path and installing new resource control parameters and data plane. The control plane is mainly involved with path decoupled, end-to-end way of mobility registrations, while data plane concerns mobility-enabled routing for data flows into and from an MN while it moves between different locations. The data plane behavior is achieved by installing changing certain binding caches upon certain control plane information exchange.

Security in wireless networks mainly involves authentication, confidentiality, integrity, and authorization for the access of network connectivity and QoS resources for the mobile nodes flow. Firstly, the mobile node (MN) needs to prove authorization and authenticate itself while roaming to a new provider's network. AAA protocols

provide a framework for such suffered especially for control plane functions and installing security policies in the mobile node (MN) such as encryption, decryption and filtering. Secondly, when QoS is concerned, QoS requires needs to be integrity protected, and moreover, before allocating QoS resources for a mobile nodes flow, authorization needs to be performed to avoid attacks.

4 Security in 4G Networks

The heterogeneity of wireless networks complicates the security issue. Dynamic reconfigurable, adaptive, and light-weight security mechanisms should be developed. Modification in existing security schemes may be applicable to heterogeneous systems.

As IP will be a common layer, it makes it easier for a network manager to manage the security at IP layer. As IP will be a common layer to all technologies, it is obvious to check security issues at the IP layer. IP Security (IPSec) has already been defined by Internet Engineering Task Force (IETF) and implemented by several vendors. Also, IPSec is an embedded feature of IPv6 and comes with additional protocols for key exchange. IPSec provides a framework to which additional features can be added to fulfill the needs of future generation communications. While looking at issues related to IPSec, we must also look at issues like mobility and network address translation (NAT). We must keep in mind that security should not be an add-on feature but it should be a part of the system from the very beginning. Security solution must provide the required security while being energy efficient, provide high goodput, low delay, provide security depending on flow, service and user, must be relatively easy to manage and scalable.

The basic idea of developing IPSec was to make something which is interoperable, of high quality in terms of security provision and use of cryptography. The idea was also to develop something at network layer which is transparent to applications if desired and is independent of link layer technology. IPSec should be algorithm independent although standard algorithms are defined. This allows closed communities to define their own algorithms. The services provided by IPSec are integrity, confidentiality, replay protection and partial protection from traffic analysis.

IPSec utilizes two protocols one of which can be used at a time or a combination can be used. These protocols are Authentication Header (AH) protocol and Encapsulated Security Payload (ESP) protocol. All provides authentication to the whole packet while ESP can either provide authentication or not. ESP uses encryption unlike AH. Besides the protocols IPSec also provides two modes, the transport mode and the tunnel mode. IPSec transport and tunnel modes are shown in Figure 3.

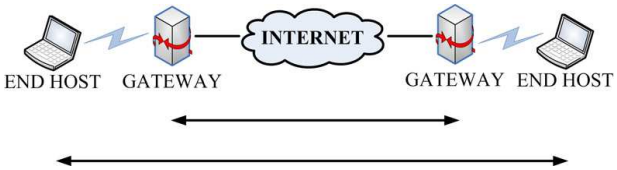

Figure 3. Transport and tunnel modes for IPSec

IPSec integrates with current Internet infrastructure without modification and is a required functionality for IPv6. Although IPSec is a secure solution, there are security issues related to IPSec like session stealing, encryption weakness and lock of access control.

Mobile IP allows mobility of devices in Internet by transparent routing of IP packets. Mobile IP elements are shown in Figure 4.

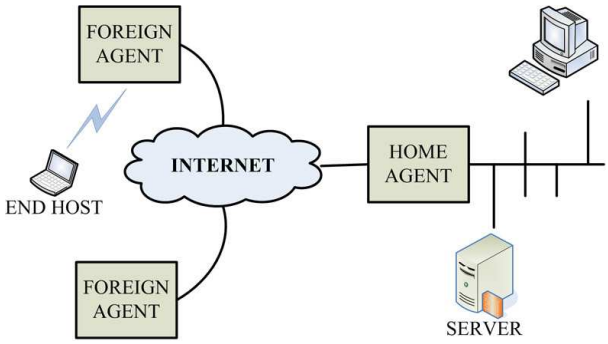

Figure 4. Mobile IP elements

Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is associated with a care of address which provides information about its current point of attachment to the Internet. The protocol provides for registering the care-of addressed with a home agent. The home agent

sends datagrams destined for the mobile node through a tunnel to the care of address. After arriving at the end of the tunnel, each datagram is then delivered to the mobile node. In practice, people are applying IPSec together with Mobile IP as a mobile and secure solution.

5 Handover

One can think of different kinds of handover, intra or inter domain handover and vertical or horizontal (intra) handover. In general, handover must be done at layer 1, 2 and 3 while keeping the session alive and fulfilling the Service Level Agreement (SLA) with the customer. Mobile IP can provide such handover but with delay which will not be acceptable to many customers especially when talking about realtime services.

Handover between heterogeneous networks, i.e., for example, vertical handover between wireless LAN (WLAN) and Universal Mobile Telecommunication System (UMTS) can be an issue. Also, one of the issues is that authentication is to be done when a dence handovers (this will be also the case with inter domain) and the need of the authentication will vary depending on the technology. Another issue is key management (again valid for inter domain) which will be difficult as the device moves from place to place. Of course, the issue of maintaining the SLA is very important. WLAN at present is not very secure, while UMTS is. It will be a big issue for the operator to accept handover from WLAN.

Mobile IP uses hard handover. Handovers are slow and packets can be lost during the handover procedure. Therefore, it is unsuitable for the handover of streamed multimedia. The mobility support provided in the handover of streamed multimedia. The mobility support provided in the Session Initiation Protocol (SIP) has been proposed for realtime communication. SIP is an application layer protocol for establishing and tearing down multimedia sessions. It can help provide personal mobility, terminal mobility and session mobility. SIP uses hard handover and “in-flight” packets can be lost during the handover period. So SIP does not provide seam less handover of streamed video in networks. Soft handover scheme shown in Figure 5 is appropriate to the needs of streamed multimedia. Here, UDP represent User Datagram Protocol. The system consists of a multimedia server that is connected to the Internet and a mobile node (MN) that is streaming a multimedia session from the multimedia server while roaming from wireless access network to wireless access network. The server has a handover agent that handles the soft handover. The MN has a handover agent. The server’s handover agent is located between the transport layer and the normal play out function of the server, while the MN’s handover agent is located between the transport layer and the normal decoding function.

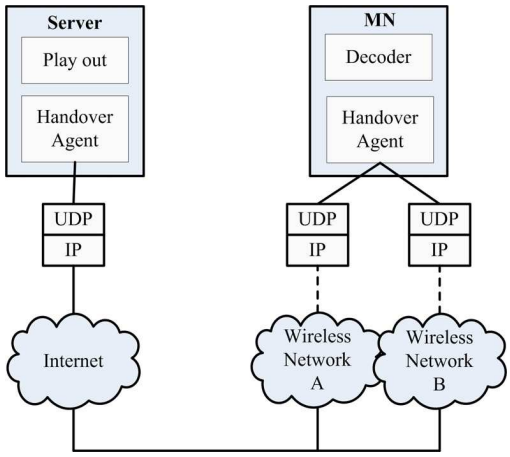

Figure 5. Architecture of the handover system

The MN has two radio interfaces, each with its own IP address. The MN is receiving the multimedia content from the server via one wireless network. The other radio interface is looking for another wireless network. When it discovers another wireless network, the MN sends a START_HANDOVER command to the server’s handover agent. After receiving this command, the server’s handover agent duplicates each multimedia packet it receives for this multimedia session from the play out part of the server, until it receives the END_ HANDOVER command from the MN. Soft handover protocol is represented in Figure 6.

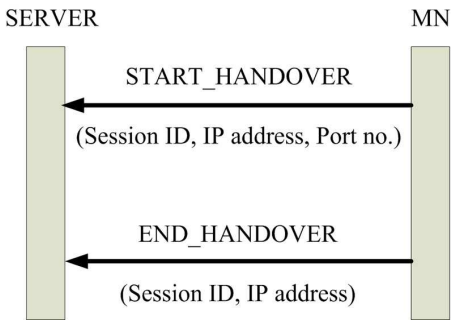

Figure 6. Soft handover protocol

START_HANDOVER command supplies a number of parameters to the server's handover agent: a session ID, an IP address and port number. The session ID pertains to the current multimedia streaming session in the MN, and is used by the server's handover agent to decide which packets to duplicate. The IP address and port number refer to the IP address and port number that will be used by the MN's radio interface in the wireless network just discovered. The server's handover agent uses these values with the duplicated packets when it inserts them into the UDP transport layer. Therefore the MN receives two streams from the server during the handover period, one through each wireless network, enabling the MN's handover agent perform a soft handover. The MN's handover agent decides which packets to pass on to the decoder, the original packets or the duplicate packets.

6 Concluding remarks

The goal of the frameworks described is to facilitate operations over wireless networks, where an operator does not necessarily run all the networks and multiple service providers may contribute to the overall system, differentiating themselves by the added value they bring to end users. IP level network mobility is an important element in future B3G systems, addressing real user cases being experimented on today by the research community. Today IPSec and MobileIP can be used for current purpose where the traffic is mostly non-realtime. For future systems one must solve the security problem based on study the requirements of various services being envisaged for B3G and 4G as well as propose solutions which fulfill the security requirements and resolve the threats. The most important is developing optimized solutions to enable seamless mobility for mobile networks and mobile nodes.

References:

[1] K. R. Rao, Z. S. Bojković, D. A. Milovanović, *Introduction to multimedia communications: applications, middleware, networking*, Wiley, 2005.

[2] K. R. Rao, Z. S. Bojković, D. A. Milovanović, *Multimedia communication systems*, Prentice-Hall, PTR, 2002.

[3] K. R. Rao, Z. S. Bojković, *Packet video communications over ATM networks*, Prentice-Hall, PTR, 2000.

[4] M. Wu, N. Memon, T. Ebrahimi, I. Cox, Multimedia security and rights management, *EURASIP Newsletter*, Vol.15, No.4, December 2004, pp. 91-94.

[5] S. Y. Hui and K. H. Yeung, Challenges in the Migration to 4G Mobile Systems, *IEEE Communications Magazine*, Vol.41, No.12, December 2003, pp. 54-59.

[6] O. Benali, K. El-Khazen, D. Garrec, M. Guiraudou, G. Martinez, A framework for an evolutionary path toward 4G by means of cooperation of networks, *IEEE Communications Magazine*, Vol. 42, No.5, May 2004, pp. 82-89.