Security Models for Heterogeneous Networking

Glenford Mapp, Mahdi Aiash and Aboubaker Lasebae
School of Engineering and Information Sciences
Middlesex University, Hendon, London NW4 4BT
Email: g.mapp, m.aiash, a.lasebae@mdx.ac.uk,

Raphael.Phan
Electronic and Electrical Engineering,
Loughborough University,
Loughborough, UK
Email: r.phan@lboro.ac.uk

***Abstract*—Security for Next Generation Networks (NGNs) is an attractive topic for many research groups. The Y-Comm security group believes that a new security approach is needed to address the security challenges in 4G networks. This paper sheds light on our approach of providing security for the Y-Comm architecture as an example of 4G communication frameworks. Our approach proposes a four-layer security integrated module to protect data and three targeted security models to protect different network entities, thus providing security in different situations without affecting the dynamics of the 4G networks.**

***Index Terms*—Heterogeneous Networks, Security Models, Integrated Security Module, Y-Comm Framework**

I. Introduction to Y-Comm

Future communication systems must provide ubiquitous connectivity where users are always connected from anywhere and at any time. The need for continuous connection is being met by the development and deployment of a number of wireless technologies including 3G/HSPDA, WLAN, with 802.11n being the latest network that is being deployed, WiMax and satellite communications.

However, the widespread deployment of wireless networks will have a significant impact on the evolution of the Internet. These developments mean that soon, it will not be possible to think of the Internet as a single unified infrastructure [1]. It would be better to view the Internet as comprising a fast core network with slower peripheral networks attached around the core. The core network will consist of a super-fast backbone using optical switches and fast access networks which use ATM and MPLS. Most of these peripheral networks will make use of wireless technologies described above.

Y-Comm is an architecture for heterogeneous networking [2], [3]. The architecture consists of two frameworks.

The Peripheral Framework deals with issues in peripheral networks while the Core Framework deals with issues in the core network. The Y-Comm architecture is shown in Figure 1. In this architecture, the Peripheral Framework and the Core Framework are brought together to represent a future telecommunications environment which supports heterogeneous devices, disparate networking technologies, network operators and service providers. One of the key goals of the Y-Comm architecture is to address security in a more comprehensive way compared with other networking paradigms because Y-Comm closely integrates security with the communications architecture.

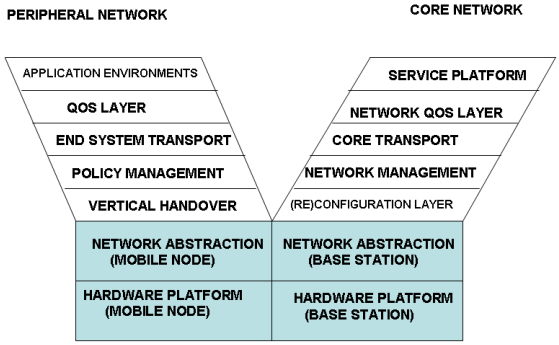

Fig. 1: The Y-Comm Framework

II. Y-Comm Security Framework

Y-Comm employs a multi-layer security model which must be applied to both the Peripheral and Core Framework simultaneously to provide total security. The security layers must work together across both frameworks in order to be fully integrated with the new architecture. The important point to note is that the need to support heterogeneous networking with open architectures means that security should not only protect data but entities

as well. The highest layer of security is at layer seven and is called Service and Application Security or SAS. In the Peripheral Framework, SAS defines the AAAC functions at the end-device and is used to authenticate users and applications. SAS in the Core Framework provides AAAC functions for services on the Service Platform in the core network.

The next security layer is called QoS-Based Security or QBS and is concerned with QoS issues and the changing QoS demands of the mobile environment as users move around [4], [5]. In addition, in order to meet their service-level agreements, servers may choose to replicate services closer to the current position of the mobile. So it is necessary to ensure that core endpoints and peripheral networks are not overloaded. The QBS layer also attempts to block QoS related attacks, such as Denial-of-Service (DoS) attacks on networks and servers.

The next security layer is at layer five, and is called Network Transport Security or NTS. In the Peripheral Framework, NTS is concerned with access to and from end-devices and the visibility of these devices and services on the Internet. In the Core Framework, NTS is used to set up secure connections through the core network. So NTS in the Core Framework involves setting up secure tunnels between core endpoints using mechanisms such as IPsec to ensure that moving data across the core network is done in a secure manner.

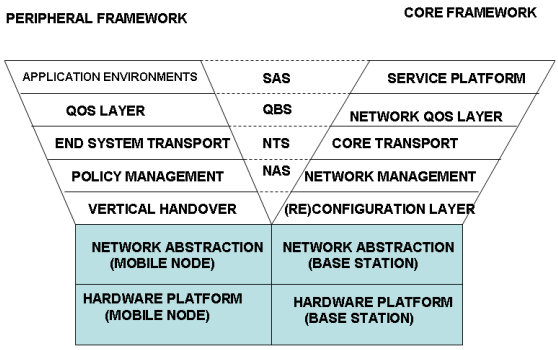

Fig. 2: The Complete Y-Comm Architecture

Finally, the fourth and last level of security is defined at layer four but can also encompass layers three and two. It is called Network Architecture Security or NAS. In the Peripheral Framework, it attempts to address security issues involved in using particular networking technologies and the security threats that occur from using a given wireless technology. So when a mobile device wishes to use any given network, NAS is invoked to ensure that the user is authorized to do so. NAS also ensures that the local LAN environment is as secure as possible. In the Core Framework, NAS is used to secure access to the programmable infrastructure. NAS in this context determines which switchlets, routelets or base-station resources may be used by the network management system. The full Y-Comm architecture including its security layers is shown in Figure 2. Since the security framework is integrated with the Core and Peripheral Frameworks within Y-Comm, these security functions being part of the communications architecture can be used to much greater effect than previous methods.

A. Security Models in Y-Comm

The security layers described above are concerned with the management of secure data transport and the authentication of mobile devices and services. However, because Y-Comm is an open architecture, it is also necessary to protect entities such as users, servers and network infrastructure. Y-Comm is therefore able to offer three distinct network security models [6]. The first model is called the Connection Security model, the second security model is called the Ring-Based Security model and the third security model is called the Vertical Handover Security model.

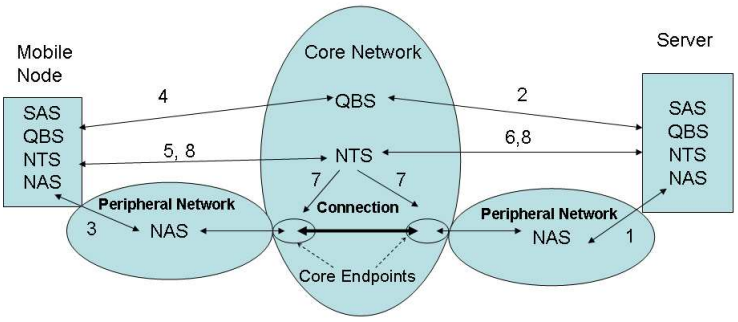

Fig. 3: The Connection Security Model

B. The Connection Security Model

In this model, the different security layers work together to establish a connection between a mobile node (MN) and a service being hosted at another site. The main idea is that end-users must use the security layers to connect to each other and this allows the system to setup, maintain and monitor the connection. The Connection

Security model is highlighted in Figure 3. We can show how the security framework is used by looking at the interaction involved in setting up a connection. This is shown as a series of steps.

- Step 1: The server is started. The NAS module in the server talks to the NAS module on the Local LAN to get access to its wireless infrastructure.
- Step 2: The QBS security module on the server informs the QBS module in the core network about its Service Level Agreement which contains the QoS associated with a connection to this service.
- Step 3: The mobile node is started. The NAS module in the mobile node contacts the NAS module in the peripheral networks to gain access to the wireless infrastructure.
- Step 4: When the mobile node wants to use the service, the QBS Module in the mobile node contacts the QBS module in the core network and asks for a connection with a given quality of service to be made to the Server. The QBS module returns two core endpoints which must be used to set up the connection.
- Step 5: The NTS module on the mobile node contacts the NTS module in the core network and says that it would like a connection to the server, using the core endpoints, the QoS and security parameters.
- Step 6: The NTS module in the core network contacts the NTS module on the server to signal an incoming call. At this point, the server can also check the security details of the client as well as the security of the connection.
- Step 7: If the server accepts the request, then the NTS module in the core network joins the two core endpoints.
- Step 8: It then signals to both the client and server that a connection has been established.

C. Ring-Based Security Model

Ring-Based security is an extension of Off-by-Default, an idea introduced by Ballani, et al. [7]. See Figure 4. The Ring-Based concept does not allow servers to be directly accessible over a WAN such as the Internet without initially interacting with the network infrastructure. This is done by using the concept of scope where a server acts only within a given scope.

There are 3 scopes:

- Local: Only processes on the same machine are allowed to use a local server. This is enforced by the SAS layer on the local machine.

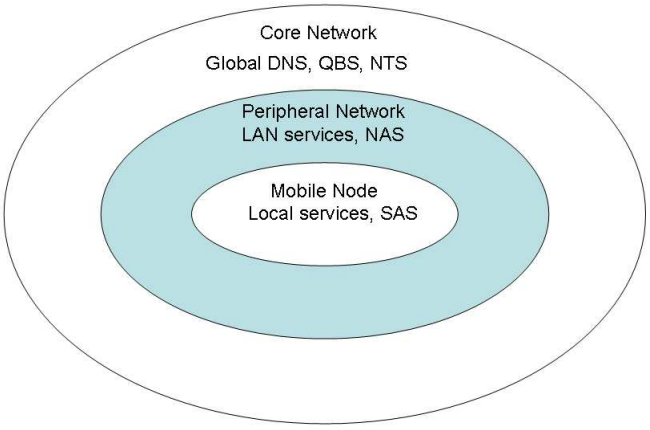

Fig. 4: The Ring-Based Security Model

- LAN: Only processes on the same network are allowed to access these servers. This is enforced by the NAS layer of the peripheral network. These servers must register with a Local DNS and are made available to mobile devices when users are cleared to use the peripheral network.
- Global: Global Servers are accessible from any point via the core network using Global Services. This therefore involves the Core NTS and QBS layers. In addition, servers must register with the Global DNS which is also managed by the core network to allow WAN access.

D. Vertical Handover Security Model

Vertical handover mechanisms [8] involve the acquisition and the release of network resources as the mobile nodes moves around. In current cellular networks, handover is controlled by the network to which the mobile is attached. However, handover mechanisms such as Mobile IPv6 (MIPv6) [9] and Fast Mobile IPv6 (FMIPv6) [10] use client-based handover. Y-Comm also uses client-based handover to support heterogeneous networking [11]. In such circumstances, it is necessary to ensure that mobile nodes do not try to abuse network resources. This is the purpose of the Vertical Handover Security model.

As shown in Figure 5, in addition to the Authentication, Authorization, Auditing and Cost (AAAC) servers, new entities are involved in the Vertical Handover Security Model (VHSM); the QoS Brokers (QoSB) which monitor the network performance and QoS-related issues; they accomplish this using admission control and auditing mechanisms. This model is given by the steps below:

- Step 1: The QBS layer of the MN asks the QBS of the QoSB about potential target networks for handover with required QoS and security level.
- Step 2: The request is passed to the QBS layer of the Core endpoint.
- Step 3: If this information has not been already in the Core-End point, the QoS Brokers of all the available networks are probed by the core endpoint. At the end of this first stage, the MN has a clear idea of the QoS and security suits available at all potential networks in the vicinity and could decide on the target network for future handover.
- Step 4: The NAS layer of the MN initiates a Re-authentication process to lunch the security mechanisms in the target network.
- Step 5: Through its NAS layer, the currently serving AAA server (CAAA) forwards the re- authentication request along with core information that are used to derive a fresh set of the security parameters for the new network to the NAS layer of a Central Authority (CA) in the Core endpoint.
- Step 6: If the target network is located in the core-endpoint, CAs NAS layer passes the core information to the target network to derive the security materials and achieves the triple A tasks.

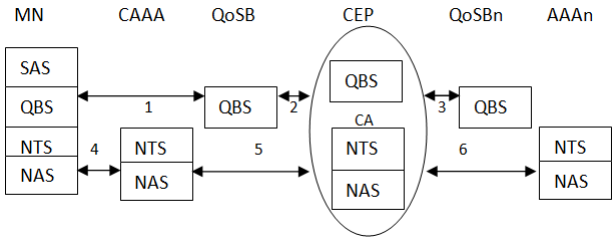

Fig. 5: The Vertical Handover Security Model

The MN will check whether it has the same security parameters the AAA of the target network has generated using core information. In case of a match this means that the new network is authentic.

Moreover, we presume certain trust relationships between the AAA servers, different trust relationship models might be implemented such as parent-child model where the top level Authority in the Core-endpoint issues certificates for all the AAAC servers working in its zone. Alternatively, current Authentication and Key Agreement protocols such as EAP as defined in RFC 5247 [12], might be used to set up a lower-layer secure association among AAA servers.

III. Concluding Remarks

We have showed how the new communications architecture for heterogeneous networking called Y-Comm can have a multi-layer security framework. The integration of the various layers into the security framework as well as the fact that the model itself is closely integrated with the overall architecture make it possible to design new security solutions. We believe that the security models introduced using the Y-Comm architecture supersede a lot of security techniques being used today, including firewalls and Network Address Translation (NAS), leading to a more secure but also a more efficient network infrastructure.

References

[1] J. H. Saltzer, D. Reed, and D. D. Clark, "End-to-end arguments in system design," in *ACM Transactions in Computing Systems*, 1984, pp. 277–288.

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

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

[4] A. Duda and C. Sreenan, "Challenges for Quality of Service in Next-Generation Mobile Networks," in *Proceedings of IT &T Annual Conference*, October 2003.

[5] C. Irvine and T. Levin, "Quality of Security Service," in *Proceedings of the New Security Paradigms Workshop*, September 2000.

[6] M. Aiash, G. Mapp, A. Lasebae, and R. Phan, "Providing Security in 4G Sysytems: Unveiling the Challenges," in *Proceedings of the Sixth Advanced International Conference in Telecommunications, (AICT 2010), Barcelona, Spain*, May 2010.

[7] H. Ballani, Y. Cathwathe, S. Ratnasamy, T. Roscoe, and S. Shenker, "Off by Default," in *Proceedings of the Fourth Workshop on Hot Topics in Networking (HotNets-II)*, November 2005.

[8] J. McNair and F. Zhu, "Vertical Handoffs in Fourth-Generation Multinetwork Environments," in *IEEE Wireless Communications*, vol. 11, 2004.

[9] D. Johnson, C. Perkins, and J. Arkko, *RFC 3775 - Mobility Support in IPv6*, IETF, June 2004.

[10] R. Koodli, *RFC 4068 - Fast Handovers for Mobile IPv6*, IETF, July 2005.

[11] G. Mapp, F. Shaikh, M. Aiash, R. Vanni, M. Augusto, and E. Moreira, "Exploring Efficient Imperative Handover Mechanisms for Heterogeneous Networks," in *Proceedings of the International Symposium of Emerging Ubiquitous and Persuasive Systems, Indianapolis, USA*, August 2009.

[12] B. Aboba, D. Simon, and P. Eronen, *RFC 5247 - Extensible Authentication Protocol (EAP) Key Management Framework*, IETF, August 2008.