RENA Service/Network Control Platform Architecture

Toru Kobayashi[†], *Tsukasa Okamoto, and Hideki Hayashi*

Abstract

The service/network control platform for RENA (resonant communication network architecture) is located between service applications and the core transmission network and plays a critical role in the implementation of the RENA concept. This article provides an overview of the architecture and highlights the position of the platform, the functions it provides, and the technologies used to implement those functions.

1. Importance of the platform

The service/network control platform provides the core functions needed to deploy networks that fully exploit the features and power of RENA (resonant communication network architecture): end-to-end real-time connectivity, QoS-awareness, and enhanced reliability and security [1] (QoS: quality of service). These core functions include shared capabilities for implementing networks on RENA and functions needed to connect multiple services to these networks. This approach substantially reduces the cost of developing and deploying new services and provides a robust network service platform to which users can freely interconnect multiple services to meet their needs.

2. Position of the platform

It lies between service applications (interactive end-to-end real-time communication, content delivery, and other services provided over RENA) and the core transmission network. By controlling lower layer transmission functions, it makes available to higher applications all the advanced features and capabilities of RENA—connectivity, quality control, security, and usability. In addition, it provides the basic functions needed to connect new services to RENA-based networks, thus facilitating the development and deployment of new services and business over RENA (Fig. 1). Its main functions are described in Table 1.

The basic functions needed to support reliable real-time connectivity matching the circumstances and intent of the people we want to contact are presence, discovery, location data management, and session control. The security management and network equipment control functions conceal the content of end-to-end transmissions, support differentiated services, and implement multilevel QoS control tailored to user needs by controlling home gateways in user networks and edge and core nodes in the core transmission network. The address management, customer ID management, authentication, and billing management functions are shared capabilities that significantly improve the usability of RENA services and are also necessary to connect new services to RENA.

This article highlights the most distinctive features of RENA: its real-time connectivity, security management, and network equipment control capabilities.

3. Features of the platform

3.1 Real-time connectivity

RENA was designed to accommodate a diverse range of users. It assumes they will employ different types of terminal equipment and different access networks, will want to send and receive different kinds

[†] NTT Information Sharing Platform Laboratories
Musashino-shi, 180-8585 Japan
E-mail: kobayashi.toru@lab.ntt.co.jp

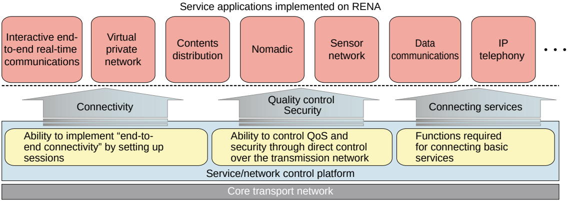
Service applications implemented on RENA
Interactive end-to-end real-time communications
Virtual private network
Contents distribution
Nomadic
Sensor network
Data communications
IP telephony
. . .
Connectivity
Quality control
Security
Connecting services
Ability to implement "end-to-end connectivity" by setting up sessions
Ability to control QoS and security through direct control over the transmission network
Functions required for connecting basic services
Service/network control platform
Core transport network

Fig. 1. Position of the service/network control platform.

Table 1. Functions provided by the service/network control platform.

Presence	Shows people you can contact, and the current status of people you want to contact.
Location data management	Keeps track of the locations of users and terminals to support mobile communications.
Session control	Establishes end-to-end connections including support for mobile communications. Establishes connections across heterogeneous networks where the access environments and terminals of senders and receivers are different.
Security management	Establishes connections across NATs/firewalls, sets up secure communication and signal path sessions, and protects the network against DDoS attacks.
Network equipment control	Provides network QoS control based on different services and user requests.
Address management	Manages the dispersal and conversion of addresses used by networks.
Customer ID management	Provides centralized management of customer data required by services.
Authentication	Provides user/terminal authentication to prevent unauthorized access, and connection to higher services through single sign-on authentication.
Billing management	Collects CDR data to collect service usage charges. Supports bundled billing and linked billing across multiple services.

DDoS: distributed denial of service, CDR: call detail record, NAT: network address translation

of media (voice, combined voice and video, text, etc.), will have different QoS and security requirements, will want to communicate from different kinds of locations under different network usage conditions, and so on. To provide a reliable connection in this kind of heterogeneous environment, the network must be capable of negotiation based on various kinds of information and be able to provide real-time connectivity based on differing combinations of circumstances at different times (Fig. 2). For example, if the person you want to contact is out of his/her office, only has a PDA (personal digital assistants), and can only be reached in a narrowband wireless LAN environment at a hotspot, then the network must be capable of setting up the communication by flexibly adapting to the access environment and the processing capabilities of the terminal. The service/network control platform thus supports end-to-end real-time communication by adapting to a particular set of heterogeneous network conditions and user requirements based on presence and other user management data, then directly controlling the access and core transmission networks to set up the communication.

3.2 Security management

Security management includes an arsenal of measures to prevent attempts to gain unauthorized access to the network, electronic eavesdropping, tampering with messages en route, distributed denial of service (DDoS) attacks [2], and other attempts to compromise the integrity of the network. There has been considerable anxiety about the vulnerability of IP-based end-to-end communications to forgery, tampering with data during delivery, and information leaks. As illustrated in Fig. 3, these problems have been addressed: the possibility of the forgery is prevented by setting up each session using secure signaling and protecting transmitted data from electronic eavesdropping by concealing the transmitted content (dynamic end-to-end secure session technology).

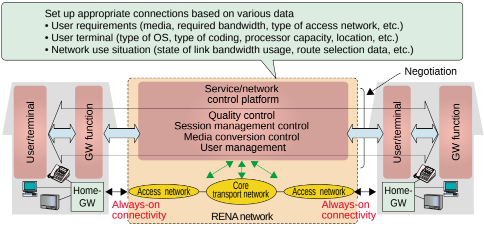
Set up appropriate connections based on various data
• User requirements (media, required bandwidth, type of access network, etc.)
• User terminal (type of OS, type of coding, processor capacity, location, etc.)
• Network use situation (state of link bandwidth usage, route selection data, etc.)
Negotiation
User/terminal
GW function
Service/network control platform
Quality control
Session management control
Media conversion control
User management
User/terminal
GW function
Home-GW
Access network
Core transport network
Access network
Home-GW
Always-on connectivity
RENA network
Always-on connectivity

Fig. 2. Real-time connectivity.

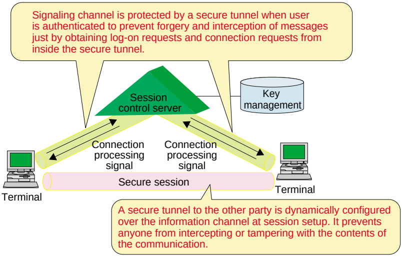
Signaling channel is protected by a secure tunnel when user is authenticated to prevent forgery and interception of messages just by obtaining log-on requests and connection requests from inside the secure tunnel.
Session control server
Key management
Connection processing signal
Connection processing signal
Terminal
Secure session
Terminal
A secure tunnel to the other party is dynamically configured over the information channel at session setup. It prevents anyone from intercepting or tampering with the contents of the communication.

Fig. 3. Dynamic end-to-end secure session technology.

We can prevent a malicious user from posing as a legitimate user by implementing the signaling channel between sending and receiving terminals and session control servers as a secure tunnel, and authenticating all parties to the communication within the secure tunnel. When sessions are set up in this way via a session control server, the end users need not send messages back and forth to one another directly to authenticate each other. Moreover, when a session is initially set up, the communication content is concealed by distributing an encryption key from the session control server and dynamically providing a secure tunnel that conceals the data sent to the other party.

Generally, an encryption key has to be exchanged between the parties to the private end-to-end communication in advance, which means that the message can only be concealed between designated locations or parties. One significant advantage of the session-based security management technique described here is that it can be used to conceal the content of communication sent to an unspecified large number of users.

3.3 Network equipment control

Most of the techniques that have been proposed for applying QoS control to transmission systems involve a scheme for guaranteeing bandwidth based on RSVP (resource reservation protocol) or MPLS (multiprotocol label switching). Implementing this kind of QoS control requires providing some means of instructing the transmission system equipment how to handle priority ID information and guarantee adequate resources.

The approach taken in RENA is to enable the service/network control platform to control QoS in units of sessions connected to the transport system. There are several ways that this could be implemented, but here we introduce the resource centralized management QoS control scheme illustrated in Fig. 4.

In this approach, information about all available resources on all network links is collected from the core transmission network and access networks in advance and centrally managed to keep track of the states of the network and routing information on a bandwidth management server. The session control server and bandwidth management server then work together to determine whether there are sufficient network resources to respond to each session connection request. The resource centralized management QoS control scheme thus involves enabling the service/network control platform to dynamically manage the state of network resource usage, and thereby provide rigorous end-to-end QoS guarantees.

The session control server and connected bandwidth management server are closely coupled servers implemented as part of the service/network control platform. Since QoS is achieved using the priority control function of the transport system, there is no need to implement advanced QoS capabilities in all the intermediate transport system equipment, which is advantageous in terms of holding down costs and allowing simpler deployment.

4. Architecture of the platform

As can be seen in Fig. 5, the service/network control platform has two interfaces: the network control interface with the core transmission network and the RENA application programming interface (RENA-API) with service applications implemented over RENA and higher application platforms.

The network control interface provides connectivity, quality control, and security functions to higher service applications, so this interface controls edge and core nodes in the core transmission network. The clear definitions of the interface between the service/network control platform and the core transmission network and of the allocation of functions between them allow these two basic elements to be improved and functionally upgraded independent of one another to enhance the network as a whole.

The RENA-API is designed to promote efficient development and deployment of service applications that take full advantage of RENA's powerful features, to facilitate interconnection between services, and to support the use of commercial service applications. It also supports higher application platforms to promote their development and the development of new platform businesses that add value and further exploit the features and capabilities of RENA. The platform configuration allows the core transmission network to be further migrated to broadband by implementing opti-

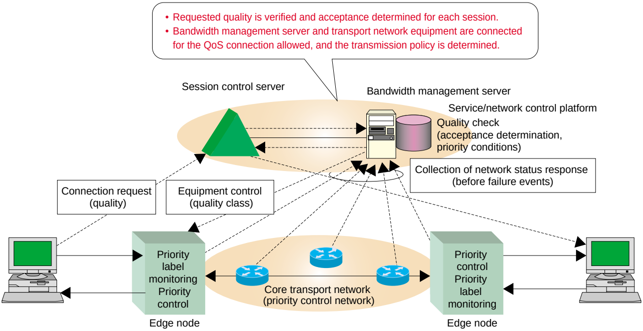
• Requested quality is verified and acceptance determined for each session.
• Bandwidth management server and transport network equipment are connected for the QoS connection allowed, and the transmission policy is determined.
Session control server
Bandwidth management server
Service/network control platform
Quality check (acceptance determination, priority conditions)
Collection of network status response (before failure events)
Connection request (quality)
Equipment control (quality class)
Priority label monitoring Priority control
Edge node
Core transport network (priority control network)
Priority control Priority label monitoring
Edge node

Fig. 4. Resource centralized management QoS control system.

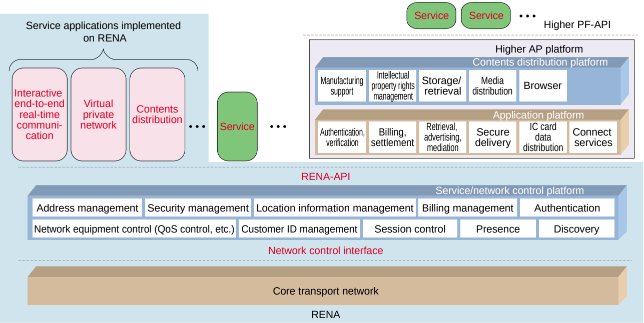

Fig. 5. Configuration of the service/network control platform.

cal switches in network nodes in the coming years without affecting the higher service applications or application platforms.

5. Conclusion

This article focused on the position of the service/network control platform in RENA and highlighted its main functions and architecture. Guided primarily by market needs, we will continue to incorporate enhanced functions in this platform in a phased approach including capabilities that support robust end-to-end connectivity, a range of multilevel QoS options, advanced security and privacy protection, carrier-grade scalability, fail-safe reliability, and other features.

Toru Kobayashi
Senior Research Engineer, Supervisor, Ubiquitous Computing Project, NTT Information Sharing Platform Laboratories.

He received the B.S. and M.S. degrees in mechanical engineering from Tohoku University, Sendai, Miyagi in 1985 and 1987, respectively. In 1987, he joined the Software Laboratories. Almost all of his experience is in R&D of software development environments including groupware tools and software development management. Since April 2003, he has been in charge of promoting the results of RENA development projects. He is a member of the Institute of Electronics, Information and Communication Engineers and the Japan Society of Information and Systems.

References

[1] N. Wada, "Vision for a New Optical Generation—Broadband Leading to the World of Resonant Communication," NTT Technical Review, Vol. 1, No. 1, pp. 6-17, 2003.

[2] Y. Yoshida and H. Takeuchi, "Applied Information Security Technologies," NTT REVIEW, Vol. 15, No. 1, pp. 15-20, 2003.

Tsukasa Okamoto
Senior Research Engineer, Supervisor, Information Service Sharing Service Network Innovation Project, NTT Service Integration Laboratories.

He received the B.E. and M.E. degrees from the University of Tokyo, Tokyo in 1987 and 1989, respectively. He joined NTT in 1989. From 1989 to 1996, he was engaged in research on ATM (Asynchronous Transfer Mode) network performance in the R&D division. From 1996 to 2001, he was with the operating company in NTT Group engaged in plant planning and investment. His research interests lie in the broad area of IP network technologies, with particular emphasis on the harmonization of economics, marketing science, and financial engineering with IP network technologies. In April 2003, he was made a "RENA Producer", charged with commercializing RENA network services.

Hideki Hayashi
Senior Research Engineer, Communication Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.S. and M.S. degrees in electrical and electronic engineering from Tokyo Institute of Technology, Tokyo in 1987 and 1989, respectively. Since joining the NTT Telecommunication Network Laboratories in 1989, he has been engaged in research and development of ATM network operation support systems and IP network elements operation support systems. In 2002, he joined the RENA development project in NTT Service Integration Laboratories.