Pave the Way to Future Smart Living Space - Cross-layer Enhanced AAA for 4G Core Network

Tin-Yu Wu, Chi-Yuan Chen, Kai-Di Chang and Diego Chung
Department of Electrical engineering, National Dong Hwa University, Taiwan R.O.C.
tyw@mail.ndhu.edu.tw

Han-Chieh Chao
College of Electrical Engineering & Computer Science, National Ilan University, Taiwan, R.O.C.
hcc@niu.edu.tw

Abstract

The 4th generation mobile communication system certainly will have a lot of improvement such as supporting higher multimedia loading, offering faster transmission rate, and the implementation of IP. The future service of the network will be definitely conveyed into an All-IP network. To allow people to better perform their daily living activities, improve the life quality, and enjoy entertainment and leisure activities, we proposed our system in this paper. This system is built upon a new technology of a 4G network, which includes the user authentication in heterogeneous network, the key generation, and data encryption that later merged together into a cross layer network for smart living space. This technology can develop a smart and convenient way of living.

1. Introduction

The rapid development of Internet and wireless network enables people to enjoy the commodity of wireless devices to transmit voice message, exchange data or gain access to multimedia services. These technologies were developed to modify human beings' life style. Nowadays, there are actually different kinds of technologies and functions for mobile node. The users face the problems with limited bandwidth, dispersible accounting and a great deal of interface. The 4th generation network is a solution to these problems, and it is expected to provide higher multimedia carrier loading ability and higher transmission rate. Furthermore, it adopts All-IP network structure.

The traditional 7 layered OSI network was implemented for years and each layer was designated some specific tasks. These layers are working together for the purpose of networking. The layered structure can diminish the complexity of the network structure, faster the implementation of new technology, and make the use of network more flexible. But this also brings some disadvantages, which refer to low efficiency in wireless and mobile network caused by high error rate, power consumption administration, QoS and new mobile networks.

Due to those issues, we proposed our system in this paper. This system is built upon a new technology of a 4G network, which includes the user authentication in heterogeneous network, the key generation, and data encryption that later merged together into a cross layer network for smart living space.

Section II introduces our motivation. Section III describes the analysis of system design. Section IV presents the results of the experiments. The conclusions are given in section V.

2. Motivation

2.1. The goal and function of the integration of 4G and WLAN network

Few years ago, 3GPP had analyzed thoroughly the possibility of the merge of WLAN and 3GPP. It proposed 6 steps to reach the goal, starting from the first and the easiest goal "accounting service" until the completion of convergence of all 6 mentioned stages. Each stage will include the works of the previous stage and we will give a brief description of each stage.

1) Common billing and service care:

To archive this goal, there is no additional requirement in both 3GPP and WLAN. This administrative issue provides users common billing information that will offer users with the charging information of both 3GPP and WLAN.

2) 3GPP System Based Access Control and Charging:

By using the original AAA mechanism in 3GPP system to unify both networks, users will not sense any differences while accessing to different networks. At this stage, users still cannot gain access to 3GPP services through WLAN. 3GPP has designed related standard of this stage. In AAA-server of 3GPP system incorporates the authentication of IEEE802.1x belonging to WLAN, by EAP-SIM authentication. At this moment, the technology has matured.

3) Access to 3GPP system PS Based Service:

Providing users access to services of 3GPP system through WLAN, such as IMS Based Services, location Based Service, Instant Messaging etc. Since 3GPP system is a private network, to enable its access through other network will need special attention in security issues. About this stage, 3GPP has also defined related standard but it is still in being developed.

4) Service Continuity:

Enable users to have seamless connection while switching from networks while roaming. During the handoff process, users might experience few moments of transmission interruption, but it is not necessary to connect to the network manually again. Some services might be stopped due to the lack of the services. To reach this goal, there are still many ongoing researches by many organizations. But, its related standard has not been defined by 3GPP yet.

5) Seamless Service:

Eliminate and minimize the tolerated data loss and disconnection of previous stages during roaming. To reach this goal, there are still many ongoing researches by many organizations. But, its related standard has not been defined by 3GPP yet.

6) Access to 3GPP Circuit Switch Services:

This final step will enable the users to have access to 3GPP Circuit Switch Services through WLAN. About this stage, its related standard has not been defined by 3GPP yet.

2.2. Cross-layer

Traditional 7-layer OSI structure of TCP/IP network has been used for years. However, using traditional TCP/IP might not be able to solve all problems but Cross-Layer is considered to be one of the possible solutions. Figure 1 refers to cross-layer coordination plane, and from the figure, we can know that instead of being built in a single network layer, the security also happens to the mobility.

We used to focus on handoff problems at IP level, but now our multi-layer point of view will be able to solve these troubles. Therefore, we proposed to build a 4G testbed which merge many other components such as Wi-Fi network, Core-network, user authentication in heterogeneous network, generation of key, encryption etc.

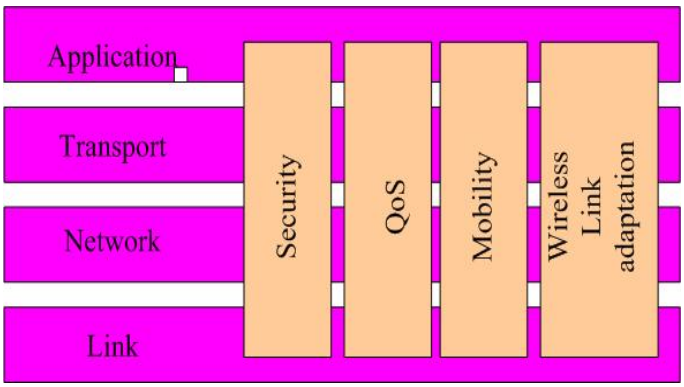

Figure 1. The cross-layer coordination plane

3. System design analysis

This system can be divided into several sections: 1) Combined authentication system of 4G network, WiFi and WiMAX. 2) AAA-Analyzer. 3) Cross layer encryption key generation. 4) Accounting in heterogeneous network. These sections will be elaborated in the following paragraphs.

3.1. Combined Authentication System of 4G, Wi-Fi and WiMAX

We followed the specification defined by 3GPP to design our system. This system is composed by 2 main components: RAN (Radio Access Network) and Core-Network. RAN includes RNC and Node B and The Core-Network includes SGSN (Serving GPRS Support Node), GGSN (Gateway GPRS Support Node), and HSS (Home Subscriber Server), which are shown in Figure 2.

At RAN, Node B works like the access point of wireless network, providing the ability for UE (User Equipment) to connect to core network through radio interface. Each RNC can work with single or multiple Node B to form a RNA. RAN is then constituted by these RNS.

At core network, SGSN is responsible for tasks such as connecting to core network with single or multiple RAN, access control, location management, routing management etc. GGSN is an interface that is responsible for connecting Core Network and outer network, and routing traveling packets. It is also responsible for mobility management.

HSS is a data center in charge of the operations of entire network. HLR is its main component and it functions to store users' identity location and registered services that are allowed to be used by users.

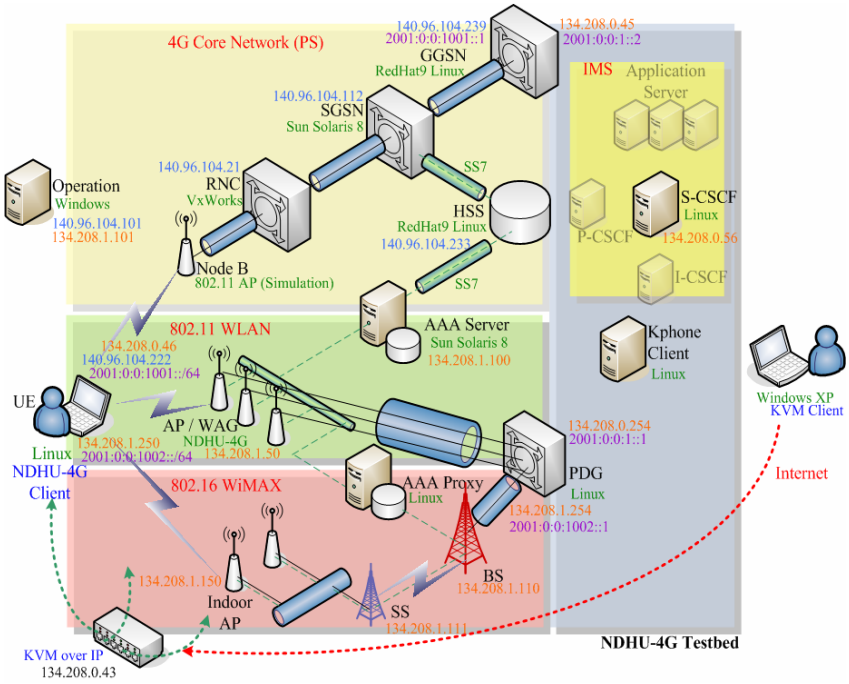

Figure 2. The cross-layer coordination plane

Since the radio of 3GPP cell phone adopts licensed band, it is required a legal license, so instead, we used 802.11g which belongs to ISM band to simulate the radio network through the broadcasting of UDP packets. Since the protocol stack of the simulation program executed in UE are based on 3GPP standard, all generated packets are identical to packets generated by real 3GPP cell phone. With this program, UE enable us to acquire the flow chart of packets generated through the process of data exchange between UE and the network.

Figure 3 and 4 shows the 4th generation mobile communication system based on WiMAX transmission topology. IEEE802.16 technology was developed in a smart living space to classify WiMAX standards. With the integration of heterogeneous network, UE can access to WLAN by acquiring authentication from AAA server with EAP-SIM method. During the authentication process, AAA server must acquire information related to SIM from HRL, so that can perform the later authentication procedure with UE. Beside, AAA server also gathers accounting information, which later will be provided as billing information.

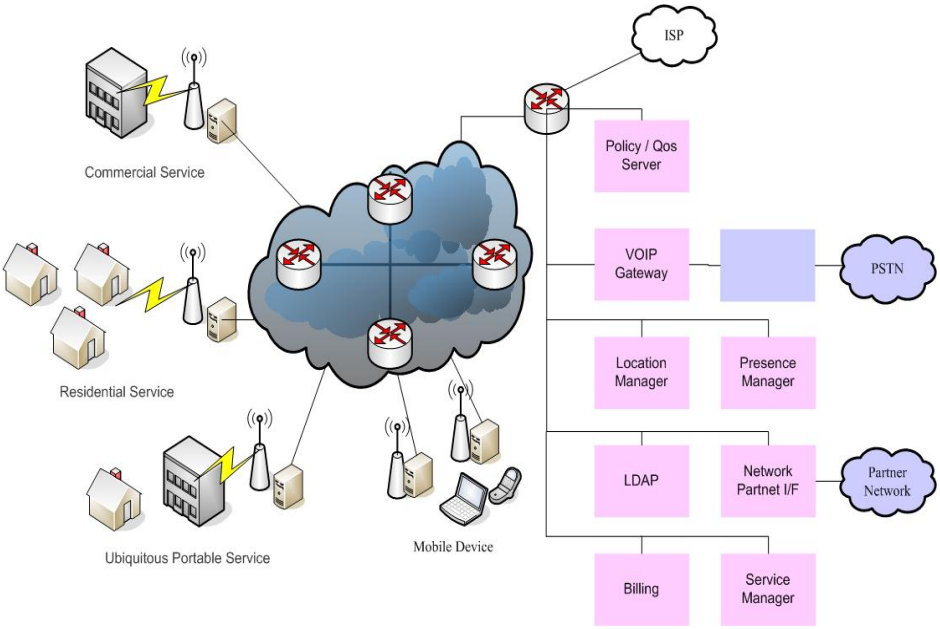

Figure 3. WiMAX Network Architecture

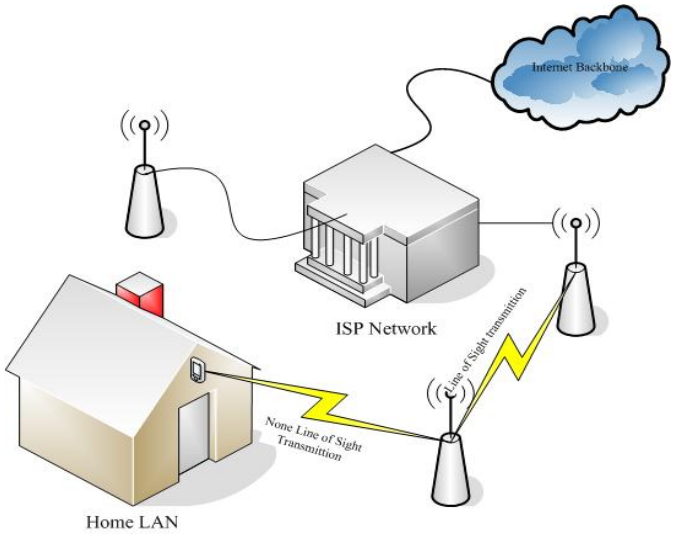

Figure 4. WiMAX is applied Home region environment

3.2. AAA Analyzer

What the future telecom services will provide will be more than a plain simple network. It should be a heterogeneous network and all kinds of authentication and accounting will be the challenges that they soon will encounter (Figure 5). AAA-Analyzer can solve these problems

and it's task is to analyze inter-domain or intra-domain procedures performed in single and heterogeneous network. With AAA-Analyzer, we can monitor and analyze the procedure of each packet, and then present it with an easy-understanding graphic. For example, such mechanism can also track the position of children to avoid getting lost or kidnapping.

3.3. Cross-layer encryption key generation system

By using AAA analyzer system, we can monitor all authentication procedures of UE and the key generated during cross layer authentication procedure. As shown in Figure 6, we will be able to store those data into cross-layer AAA server, and have a clear picture of how UE is connected, and charging it accordingly.

3.4. Heterogeneous network accounting system

Since we will have an environment of heterogeneous network in the future, users can select the best charging method that suits their needs, (to facilitate users to choose between charging methods). This system also includes a charging information system based on web service. Users can monitor the way how they use the network, and then can make decision about how they would like to be charged, providing users a flexible user-oriented charging system.

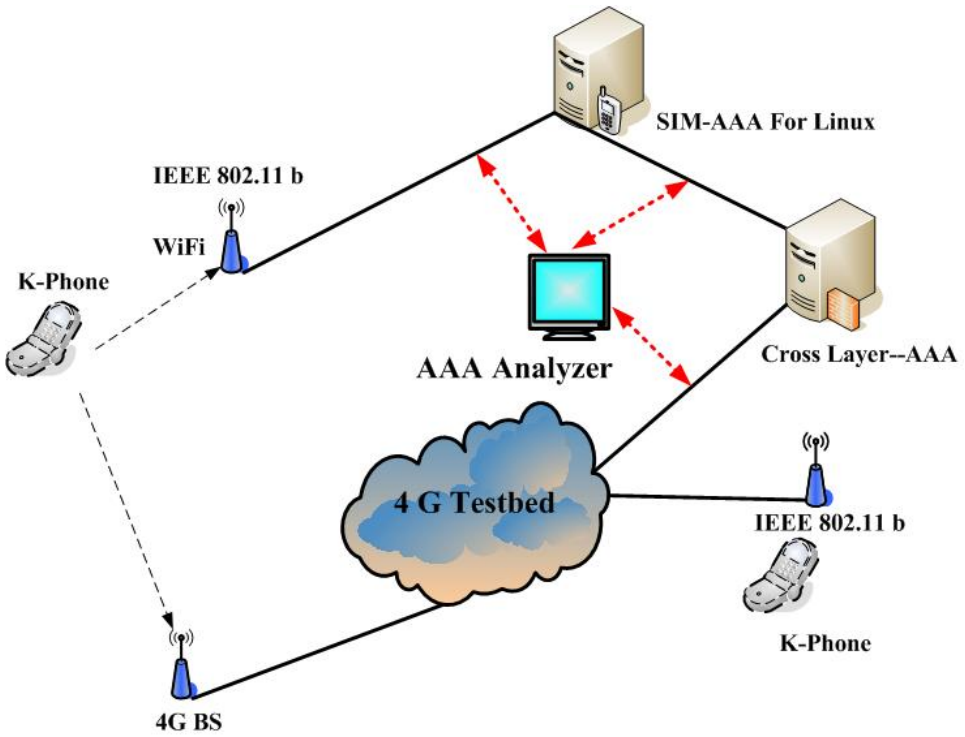

Figure 5. AAA-Analyzer system topology

4. Experiment results

Figure 7 shows the entire system proposed by our paper and Figure 8 shows the flow chart of packets interchange in the Core-Network. The UE we designed has the ability

to connect both Core-network and WLAN and has to exchange packets with Core-network in order to use the network resources.

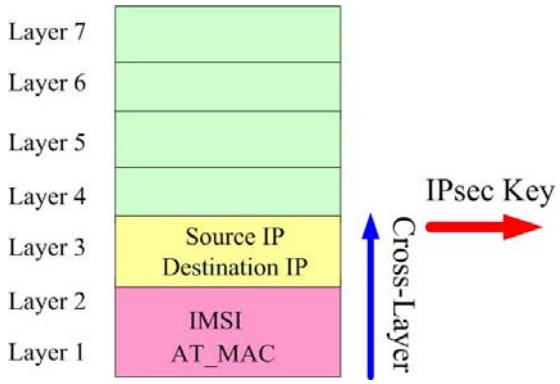

Figure 6. The Cross-layer IPsec Key

First, UE(a) will relay “Attach Request” toward SGSN(c) through RNC(b) to register and this packet contains identification information of UE. When SGSN received the request information, it will use this identification information to acknowledge 4G UE. When SGSN successfully completes the authentication procedures, it will also update UE location information through HLR(e). Finally, SGSN will send an “attach accept” message to UE, and this will be the completion of entire attachment procedure. When the attachment process is completed, UE will proceed to “PDP context activation” process by first sending an “activate PDP context request” to SGSN, requesting for the PDP address. When SGSN received “Activate PDP context request” message, it will then send “create PDP context request” to GGSN(d), and GGSN then establish PDP context for this UE, and send back “Create PDP context response” to SGSN. Once SGSN receives the response, it will establish a tunnel between SGSN and UE. After the process of attach and PDP context activation are both completed, UE will be able to access to the service of Core-network and resources of outer networks.

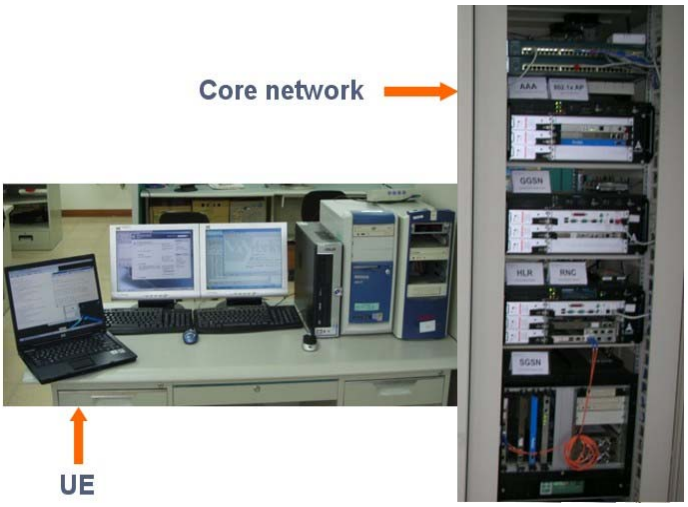

Figure 7. Test-bed system

The flow chart of wireless network is shown in Figure 9. The integrated 4G UE(f) can authenticate through access point(g) of 802.1x, routing information to AAA server, requesting for Access Request, automatically informing users information stored in SIM. When AAA server receives the request message, it will start negotiation for authentication method such as EAP-SIM, one of the supported authentication methods. When UE sends the needed authentication information back to AAA-Server, if AAA server doesn't have users information of this SIM card, it will request information from HLR(e), and once being acquired authentication information from HLR, it will verify if users to have authorization to use resources of WLAN. Then, UE will be able to access to the resources or services of outer network. Figure 10 shows the SIM based interface of UE connecting to 4G.

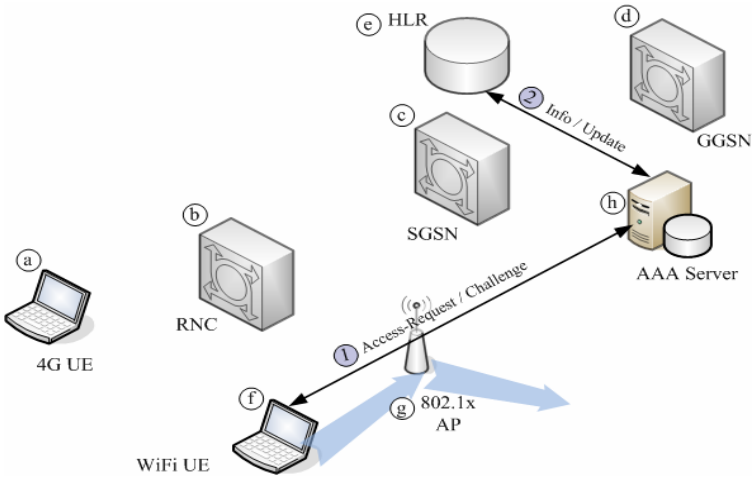

Figure 8. The operant steps of 4G-platform (I)

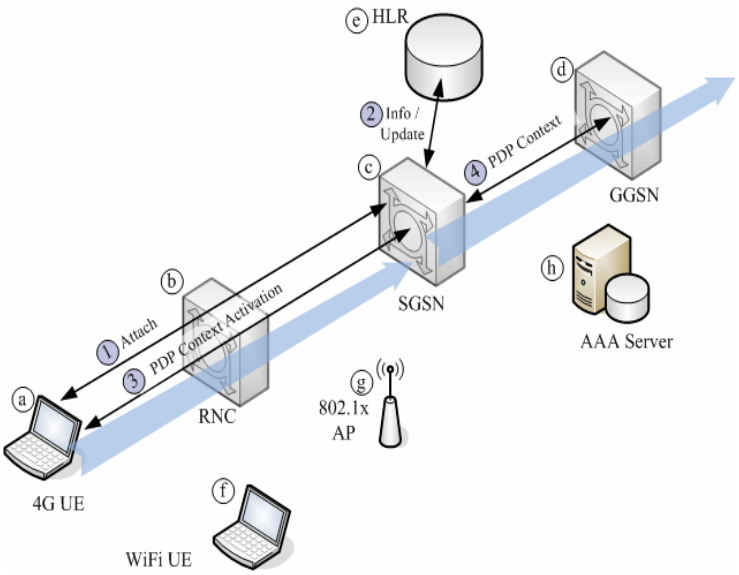

Figure 9. The operant steps of 4G-platform (II)

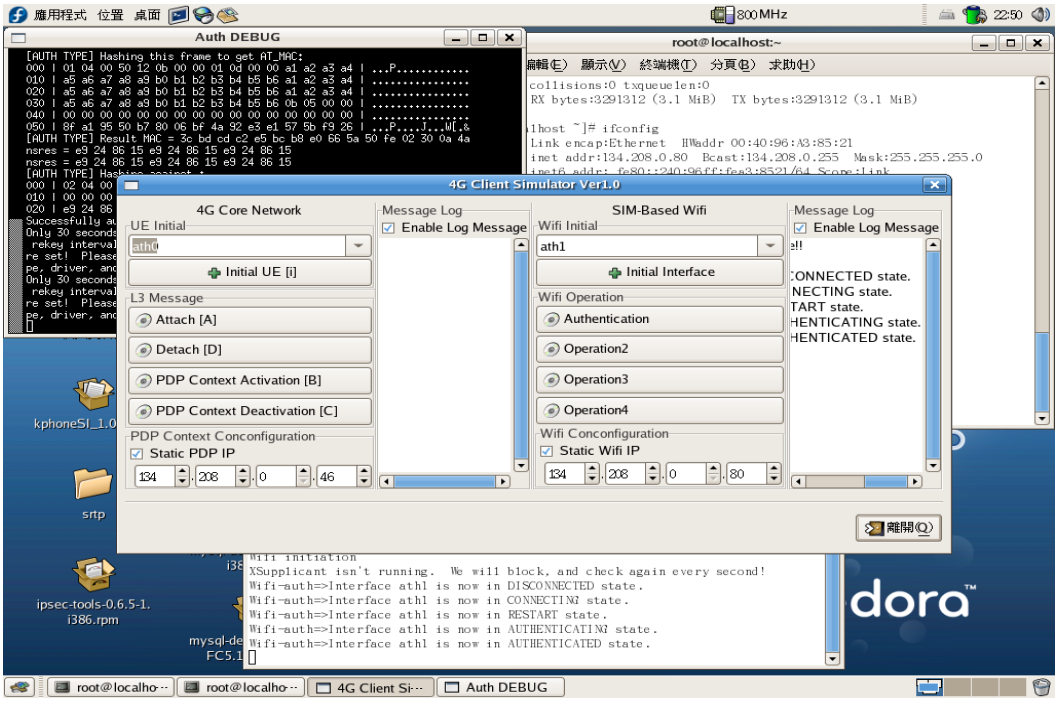

Figure 10. UE connect to interface of both 4G and SIM-Based.

AAA-analyzer provides heterogeneous network the abilities of accounting, monitoring and recording encrypted data for later decoding. This program is written in Perl, and when UE connects to 4G with SIM based interface, AAA-Analyzer then can capture the transmitted message, and present it with a graphic as shown in Figure 11.

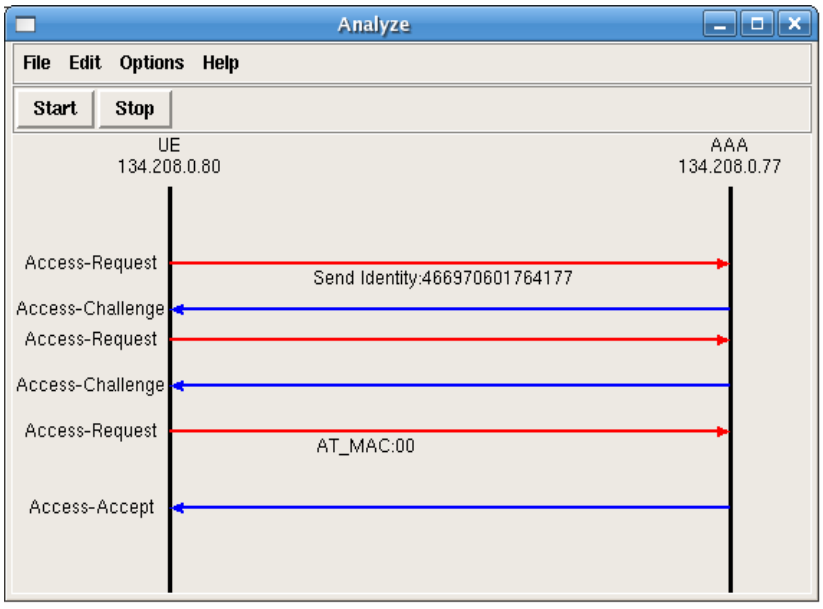

Figure 11. A variety of handshake signal of AAA-Analyzer

At last, the accounting and billing system was basically built on an application server. The way we develop PHP software to acquire the charging formation is based on the database of Radius server of HLR. Since the database of Radius server only registers its connection information of Core-network, the server does not offer data related to IB3G. Therefore, we set up a new database that contains columns of source_ip, dest_ip, packet_id, packet_size, and auth_accept, for purposes of registering IB3G connection information. By using information provided by this database and our charging system, users can check their connection details. This charging and billing system provided two charging methods for users: one is charged by time and another is charged by packets. We provide a web interface for users to check their connection details and choose the most appropriate charging method. We performed separately encrypted and un-encrypted test on our test platform, and as reference, we adopted the widely used jitter measurement to measure the voice quality. Figure 12 shows the normal condition, the jitter of an un-encrypted audio streaming. Figure 13 shows the jitter of an encrypted audio streaming. The black and green represents the jitter of half-duplex audio streaming.

Comparing the test results, we can find the jitter with bigger variation in encrypted test. Since we are using a notebook as UE to be the part of test platform, which has more computing power, as result, it only produced a few more jitter, a more detailed list of data will be presented in the following Table 1.

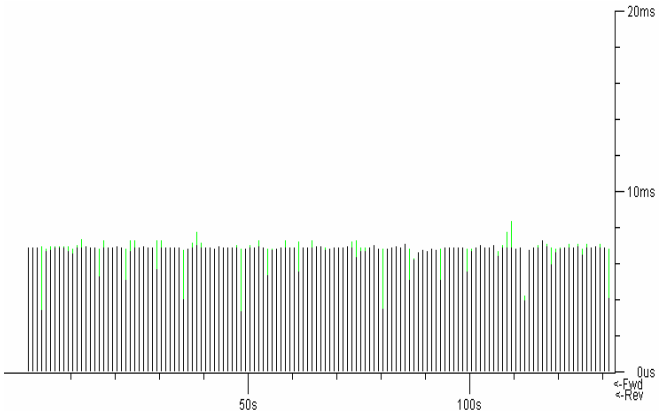

Figure 12. No Encrypted Voice Stream

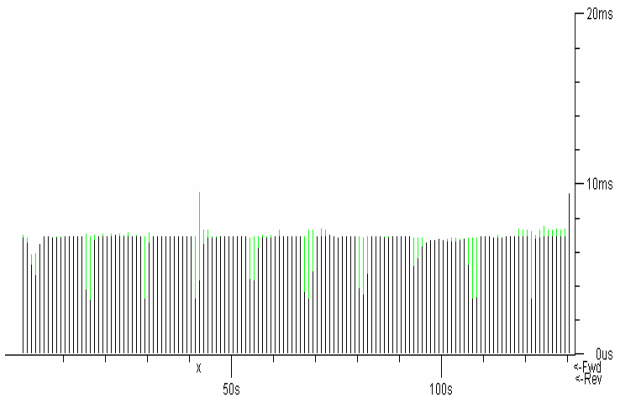

Figure 13. Encrypted Voice Stream

Table 1. Max and Mean Jitter

	Max Jitter (ms)	Mean Jitter (ms)
No Encrypted Voice Stream	7.75	6.19
Encrypted Voice Stream	9.38	6.30

5. Conclusion

The 4th generation mobile communication system certainly will have a lot of improvement such as supporting higher multimedia loading, offering faster transmission rate, and the implementation of IP. To allow people to better perform their daily living activities, improve the life quality, and enjoy entertainment and leisure activities, we proposed our system in this paper and we find many advantages: 1) Combined authentication in heterogeneous network, 2) assist operators to control the status of authentication, 3) generate Seeds with high performance and High security characteristic, and 4) billing according to duration or transmitted data. In the future, there will be still have many possibilities of development, such as adding 802.16 and 802.20 wireless communication technologies. No matter what standard will be applied, it will lead to a creative and convenient living style.

6. References

[1] S.S. Dixit, "Evolving to Seamless All-IP Wireless/Mobile Networks," IEEE Communications Magazine, Vol.39, No.12, pp.31-32, December 2001.

[2] S. Huusko, "Nokia All-IP System Design Principles," 3GPP all-IP Workshop, Nokia. (http://nokia.com)

[3] S. Wickware, "All IP in UMTS Networks- Benefits and Challenges," Nortel Networks, (http://www.nortel.com)

[4] K.E.E Raatikainen, "Middleware Solution for all IP Networks," Proceedings of the Second International Conference on 3G Mobile Communication Technologies, pp.335-340, 2001.

[5] H.C. Chao, Y.M. Chu, and M.T. Lin, "The Implication of the Next-Generation Wireless Network Design: Cellular Mobile IPv6," IEEE Transactions on Consumer Electronics, , Vol.46, No.3 , pp.656-663, 2000.

[6] T. Robles, A. Kadelka, H. Velayos, A. Lappetelainen, A. Kassler, L. Hui, D. Mandato, J. Ojala, and B. Wegmann, "QoS Support for an All IP System Beyond 3G," IEEE Communications Magazine, Vol.39, No.8 , pp.64-72, 2001.

[7] A.T. Campbell, J. Gomez, S. Kim, A.G. Valko, C.Y. Wan, Z.R. Turanyi, "Design, Implementation, and Evaluation of Cellular IP," IEEE Personal Communications, Vol.7, No.4, pp.42-49, Aug. 2000.

[8] W. Yurcik and D. Doss, "A Planning Framework Far Implementing Virtual Private Networks," IT Professional, Vol.3, No.3, pp.41-44, 2001.

[9] K. Segaric, P. Knezevic, and S. Dembitz, "Possible Problems and their Solutions with IPv6 Router Announcement," Proceedings of the International.

[10] 3GPP TS 24.228、3GPP TS 23.102、3GPP TS 23.002 v360、 3GPP TS 23.002 v480、3GPP TS 23.002 v5c0、3GPP TS 23.002 v690.

[11] http://mobile01.com/topicdetail.php?f=18&t=1752&PHPSESS ID=e82953549a5d71b0395f95556035df1e.

[12] 3G Americas, IMS Overview and Applications july, 2004.

[13] Vassilios Koukoulidis and Mehul Shah, The IP Multimedia Domain in Wireless Networks: Concepts, Architecture, Protocols and Applications 2004.

[14] 3GPP TR 22.934, "Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking".

[15] 3GPP TS 23.234, "3GPP system to Wireless Local Area Network (WLAN) interworking; System description".

[16] 3GPP TS 33.234, "3G Security; Wireless Local Area Network (WLAN) interworking security".

[17] H. Haverinen and J. Salowey, EAP SIM Authentication, Internet draft <draft-haverinen-pppext-eap-sim-11.txt>, Jun 2003.

[18] L. Blunk et al., Extensible Authentication Protocol (EAP), Internet draft <draft-ietf-pppext-rfc2284bis-03.txt>, May 2003.

Authors

Tin-Yu Wu

He is currently serving as the technician of the Network Division in the University Computer & IT Center at National Dong Hwa University (NDHU), Hualien, Taiwan, R.O.C. He received his MS degrees in Electrical Engineering from NDHU in 2000. His research interests focus on the next generation Internet protocol, mobile computing and wireless networks. He is now a PhD candidate in Department of Electrical Engineering, NDHU.

Chi-Yuan Chen

He is now a MS student in Department of Electrical Engineering, NDHU. His research interests focus on the network security, core network of communication system.

Kai-Di Chang

Acquired bachelor degree in 2006 from National Dong Hwa University. He will be attending National I-Lan university as master student,.

Jiun Haur Chung

Undergraduated from Medicine School of Buenos Aires University, entered electric engineering department of National Dong Hwa university at year 2003,will acquire master degree at year 2006.

,

Han-Chieh Chao

He is a Full Professor of the Department of Electronic Engineering, National Ilan Uni versity, I-Lan, Taiwan, R.O.C. His research interests include High Speed Networks, Wireless Networks and IPv6 based Networks and Applications. He received his MS and Ph.D. degrees in Electrical Engineering from Purdue University in 1989 and 199 3 respectively. Dr. Chao is also serving as an IPv6 Steering Committee member and Deputy Director of R&D division of the NICI Taiwan, Co-chair of the Technical Area fo r IPv6 Forum Taiwan.

INTENTIONAL BLANK