International Journal of Future Generation Communication and Networking
Vol. 9, No. 11 (2016), pp. 337-344
http://dx.doi.org/10.14257/ijfgcn.2016.9.11.31

A High Security Architecture for LTE Core Network Server

[1] Gengxin Sun, [2]Sheng Bin and [1]Yixin Zhou

[1]*International College of Qingdao University, Qingdao, China*
[2]*Software Technical College of Qingdao University, Qingdao, China*
sungengxin@qdu.edu.cn

Abstract

With the expansion of wireless network technologies and the emergence of novel mobile applications, the 3rd Generation (3G) communication is moving to the 4th Generation (4G) communication. Comparing to preceding versions, one elementary difference is that 4G wireless networks will operate entirely on the TCP/IP, which would cause greater risks in terms of safety and reliability. In this paper, a new high security architecture for Long Term Evolution (LTE) core network server is proposed and designed. There are asynchronous array of simple processors and two physically isolated high-speed system buses in the security architecture, which ensure only one bus can be connected to array of processors at the same time. Experiment results show that the security architecture can effectively prevent external threats from accessing network resources.

Keywords: *4G communication, network security, long term evolution, security computer architecture.*

1. Introduction

Long Term Evolution (LTE) is the mobile network technology for the 4th Generation (4G) mobile communication. The standardization of the LTE protocol had become operational with the 3rd Generation Partnership Project (3GPP). LTE is a packet-based system containing less network elements, which improves capacity and coverage, and provides high performance in terms of high data rates and seamless integration with other existing wireless communication systems [1]. In addition to above features, one of the most important components is the novel all-IP core network architecture, known as the evolved packet system (EPS), is the evolved packet core (EPC), which is illustrated in Figure 1.

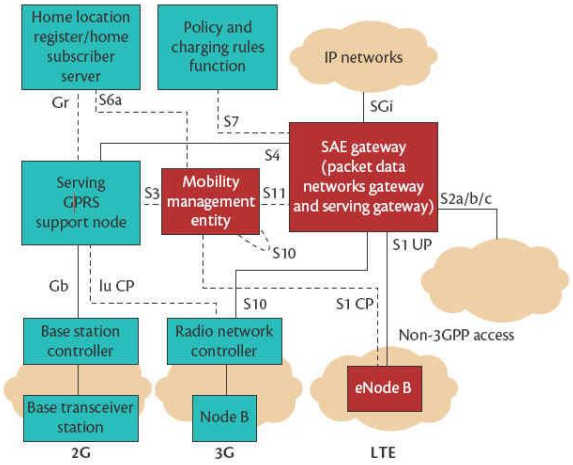

Figure 1. The Architecture of Evolved Packet System

ISSN: 2233-7857 IJFGCN

As the 4G evolution of LTE, EPS is the relevant aspect of the LTE main core network architecture—demands that security functions should be optimally and efficiently embedded into overall architecture. 4G essentially builds an open environment where various network operators and service providers share the core infrastructure. This openness of 4G poses much more security challenges as opposed to the traditional closed environment that has an inherent advantage of protection against security threats. It would just be a matter of time before 4G networks start to suffer the equivalent level of attacks experienced today by Internet. Hence, guaranteeing high level of security turns out to be one of the important requirements in the successful deployment of 4G networks.

Recent years, a lot of researches on the security of LTE networks have been proposed. Park [2] elaborated overview of the security threats on 4G networks. In the survey, the security architectures of IP Multimedia Subsystem and Next Generation Networks have been investigated and the weaknesses of the current security functionalities in the Worldwide Interoperability for the LTE systems are presented. It has pointed out that 4G systems will inherit all the security problems of underlying access networks and most of the IP-specific security vulnerabilities due to their heterogeneous and IP-based open architecture. Kolias [3] provided a comprehensive taxonomy of the malicious attacks and countermeasures in the LTE systems. In the survey, the qualitative characteristic of each type of the attacks has been evaluated in terms of both breadth and depth. Sankaran [4] provided the summary of LTE security functions and procedures. In the survey, the overall EPS architecture, EPS security threats and security requirements have been discussed. Seddigh [5] proposed security advances and challenges in the 4G wireless networks. The security architectures of LTE networks have been specified with concentration on the specific MAC layer security issues and possible vulnerabilities associating with the LTE systems. In addition, the LTE networks are also susceptible to DoS attacks, data integrity attacks, illegal use of user and mobile equipment, and location tracking at the MAC layer.

In this paper, the architecture of the LTE networks is presented firstly in Section II. In Section III, a high security architecture for server in the LTE network is proposed and designed. The existing solutions are compared to security architecture for LTE core network server with experiments in Section IV. Finally, the conclusion of the paper is presented in Section V.

2. LTE Network Architecture

As shown in Figure 2, the LTE network is comprised of the EPC and the E-UTRAN. The EPC is an all-IP and fully packet-switched backbone network in the LTE systems. The EPC consists of a Mobility Management Entity (MME) and a Serving Gateway (SGW), a Packet Data Network Gateway (PDN GW) together with Home Subscriber Server (HSS). When a User Equipment (UE) connects to the EPC, the MME represents the EPC to perform a mutual authentication with the UE. E-UTRAN includes the Evolved Universal Terrestrial Radio Access Network Base Stations, called eNodeBs (eNB), which communicates with UEs.

Compared with the 3G networks, some new functions and entities were introduced in the LTE networks. Firstly, a new type of base station, named HeNB, connects to the EPC over the Internet via a broadband backhaul. Secondly, the LTE system supports non-3GPP access networks such as wireless local area networks. For an untrusted non-3GPP access network, an UE needs to pass a trusted evolved packet data gateway connected to the EPC. Thirdly, a LTE system also supports a new type of data communications between entities, named as MTC, which can exchange and share data without any requirement on any form of human intervention.

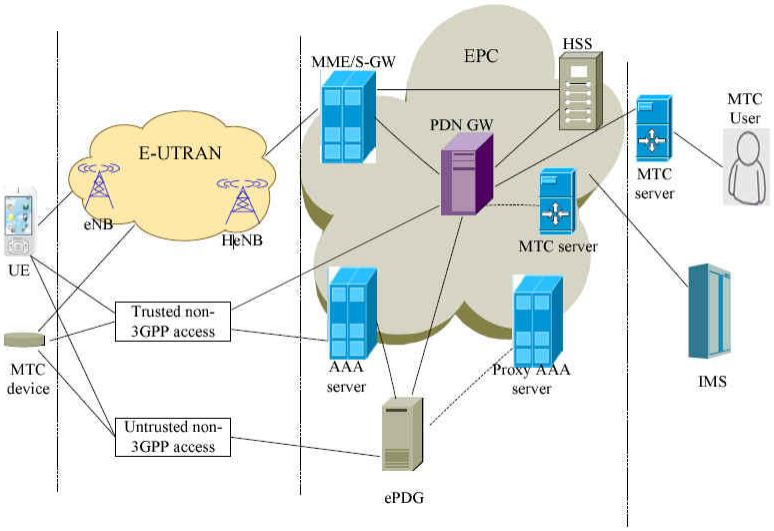

Figure 2. Network Architecture of LTE

There are two new entities existing in the MTC, the MTC user and the MTC server. The MTC server is connected to the LTE network to communicate with MTCDs. The MTC server may be an entity outside or inside an operator domain. When a MTC device connects to the LTE network, the MTC device can communicate with the MTC server and be controlled by the MTC servers. So the security of the servers is very important for the whole LTE network.

3. New High Security Computer Architecture for Server

A new high security architecture for server is proposed. The new computer architecture has a single asynchronous array of simple processors (AsAP) and two physically isolated high-speed system buses (local bus and network bus), ensure only one bus can be connected to AsAP at the same time via a Bus Bridge [6]. The new high security computer architecture is shown in Figure 3.

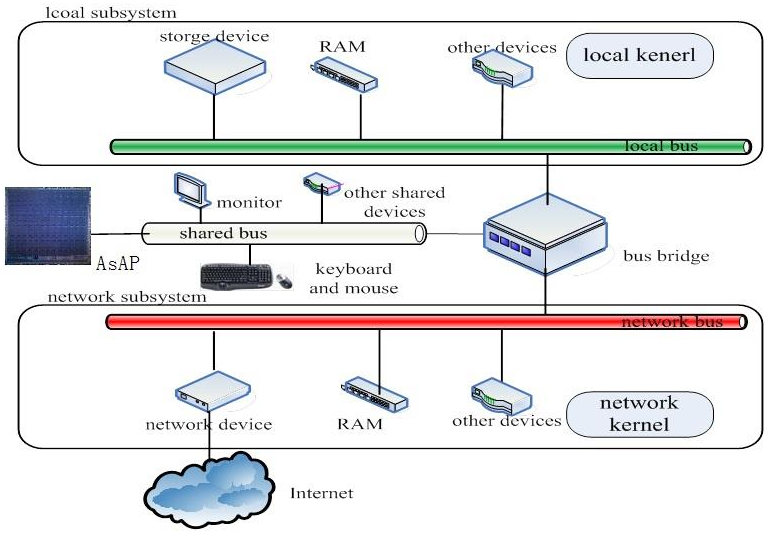

Figure 3. The New High Security Computer Architecture

In the new architecture, computer system is divided into tow sub-systems. All the network devices mounted on the network bus form into a network sub-system which

connects with other servers in the LTE network. All the storage devices mounted on the local bus form into a local sub-system which is isolated from the LTE network. So even if the network intruder suddenly gets the whole control of network bus in network sub-system, only the temporary information of the network sub-system is exposed, while the local sub-system is left intact. Thus, hardware-level isolation can effectively ensure the security of sensitive data in local sub-system.

3.1. Design of AsAP

AsAP architecture comprises a 2-D array of reduced complexity programmable processors with small memories interconnected by a reconfigurable mesh network. It was developed by researchers in the VLSI Computation Laboratory (VCL) at the University of California, Davis and achieves high performance and energy-efficiency, while using a relatively small circuit area [7].

AsAP processors are well suited for implementation in future fabrication technologies, the multi-processor architecture can efficiently make use of task-level parallelism in many complex DSP applications, and also efficiently computes many large tasks using fine-grained parallelism.

There are several novel key features of AsAP, they are:

- Chip multi-processor architecture designed to achieve high performance and low power for many communication applications.
- Small memories and a simple architecture in each processor to achieve high energy efficiency.
- Globally asynchronous locally synchronous clocking simplifies the clock design, greatly increases ease of scalability, and can be used to further reduce power dissipation.
- Inter-processor communication is performed by a nearest neighbor network to avoid long global wires and increase scalability to large arrays and in advanced fabrication technologies. Each processor can receive data from any two neighbors and send data to any combination of its four neighbors.

In the high security architecture, a chip containing 36 (6*6) programmable processors was adopted. The chip uses a synthesized standard cell technology and is fully functional. Block diagrams of a single AsAP processor is shown in Figure 4.

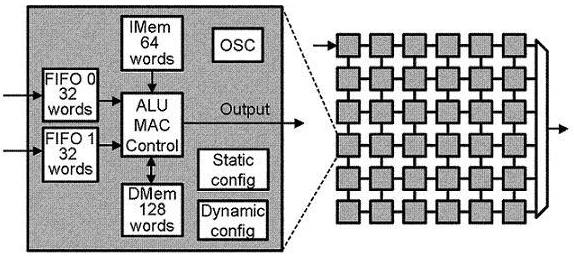

Figure 4. Block Diagrams of a Single AsAP Processor and the 6x6 AsAP Chip

3.2. Bus bridge

The function of the bus bridge is to connect the shared bus with one of the peripheral buses. The goal of the bus bridge is:

- The bus bridge should make sure that the shared bus can connect one of the peripheral buses in anytime;
- The bus bridge should make sure that only one of the peripheral buses is connected to the shared bus at the same time;
- When AsAP needs to connect the other peripheral bus, the bus bridge can cuts current connection and connects shared bus with the other peripheral bus.

Based on the functionality, the bus bridge is designed as Figure 5.

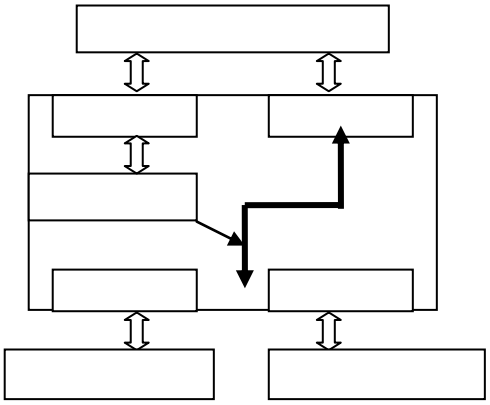

Figure 5.Structure of Bus Bridge

The bus bridge includes two slave ports (Control and S), two master ports (Ava0 and Ava1) and one state register.

The function of the Control port is to receive the instructions for the bus bridge from AsAP, or send the data of the state register to AsAP. The function of the S port is to receive/forward all Avalon signals from/to the shared bus. All these signals of the S port are bridged with their corresponding signals of the Ava0 or Ava1 port, which connects the peripheral bus with all Avalon bus signals, depending on the instruction type. Therefore, a path between the shared bus and the peripheral buses is built. A state register with five bits exists in the bus bridge. The lower four bits of the register store work modes; the higher one bit, called flag bit, stores the flag that helps describe which peripheral bus is connected to the shared bus through the bus bridge currently. If the flag bit is set as 0, all the signals of the S port connect with their corresponding signals of the Ava0 port. Therefore the shared bus connects peripheral bus 0, and the system works in area 0; otherwise the flag bit is set as 1 and the system works in area 1.

The data of state register shows as Table 1.

Table 1. Data of State Register

The lower 4 bit of state register	
value	***Work mode***
0000	Requirement for initialization
0001	Finish of initialization
0010	Maintain in current area
0011	Maintain in area 0
0100	Maintain in area 1
1111	System reset
others	reserved
The flag bit	
value	***Work area***
0	area 0
1	area 1
others	area 0

The implement of the bus bridge includes four modules:

- Write transfer

Avalon fundamental slave write transfer describes how ASAP writes state register through the Control port. Write transfer is completed in a single bus cycle. AsAP writes the work mode and work area according to Table 1.

For the write transfer of the bus bridge, ASAP passes signals *writedata*, *write_n* and *address* to the bus bridge through the shared bus. The signal *writedata* carry command code from ASAP; the signal *write_n* can enable the write operation, the shared bus set the signal *chipselect*, which selects the bus bridge, according to the signal address. Once the signals *write_n* and *chipselect* are both available, the bus bridge reads the lower five bits of the signal *writedata* and writes in the state register. The pseudo codes of write transfer are shown as following:

```
always @ (posedge clk)
begin
        if (!write_n && chipselect = = 1)
           the state register <= writedata[4:0] ;
end
```

- Read transfer

Avalon fundamental slave read transfer describes how AsAP reads state register through the Control port, Read transfer is completed in a single bus cycle. AsAP reads the work mode and work area according to Table 1.

In the read transfer of the bus bridge, the AsAP passes signals *read_n* and *address* to the bus bridge through the shared bus. The signal *read_n* can enable the read operation; the shared bus set the signal *chipselect*, which selects the bus bridge, according to the signal *address*. Once the signals *write_n* and *chipselect* are both available, the bus bridge sends data of the state register to the lower five bits of the signal *readdata*, which carry data to AsAP. The pseudo codes of read transfer are shown as following:

```
always @ (posedge clk)
begin
if (!read_n && chipselect == 1)
    readdata[31:0] <= {27'b0,the state register} ;
end
```

- Connection between S port and master ports

All the signals of the S port connect with their corresponding signals of the master ports, therefore the shared bus connects peripheral bus. For example, the S port gets a signal *writedata*, which has 32 bits, from the shared bus. Its corresponding signal in the Ava0 port is named *ava0_writedata*.

The flag bit hold the flag of the work area, if it's 0, the system works in area 0; otherwise the system works in area 1. The change of flag bit is one of trigger condition of always block for connecting the S port signals and master port signals. When the state of flag bit changes, the bus bridge automatically reconnects the S port and the master port.

- Reset

When the system is reset, the state register is set as 01111, which means the system work in area 0, and the work mode is "system reset".

4. Experiment Analysis

In this section, the security of the LTE core server is analyzed in terms of anonymity. In addition, capabilities of high security architecture against anonymous attack are compared with existing server.

Suppose that an adversary pretends to be a MME and sends an identity request message to some anonymous user of a particular zone. Upon receiving the identity

response, it will not be able to identify the user. This is because, the illegitimate MMEs don't have access to the patterns and keys. Furthermore, it is because of mutual authentication procedure between subscribers and HSS in LTE networks.

Figure 6 shows the difference of the security architecture server and the existing LTE core network server when the amount of simultaneous identification responses (SIR) received at the HSS increase.

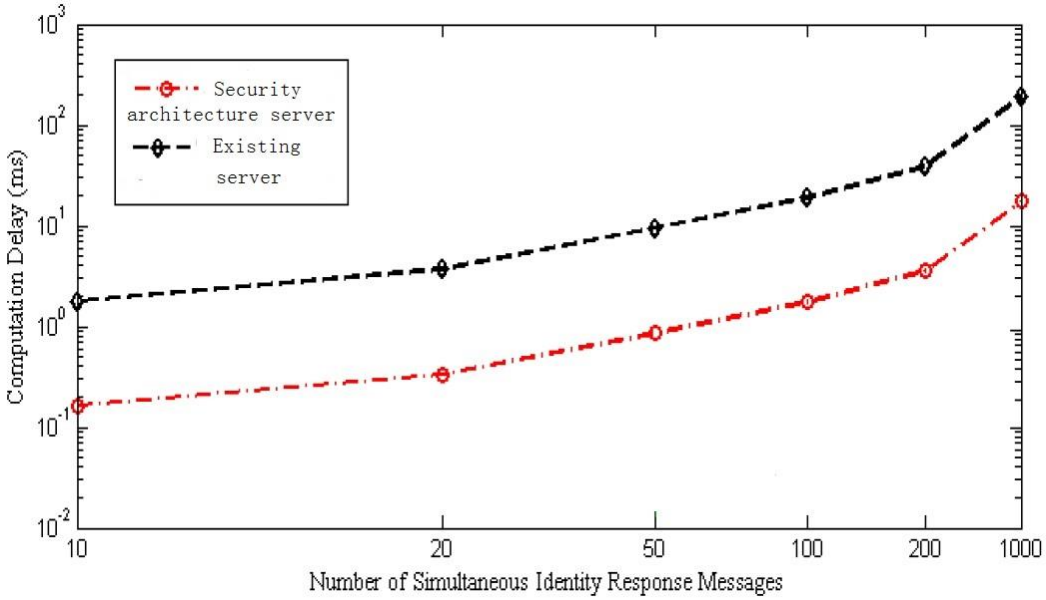

Figure 6. Identification Delay Comparison

The results indicate that, when the number of SIRs rises, the computation delay of the existing LTE core network server increases significantly in comparison with the security architecture server.

Then, we simulated three groups anonymous user attacks under different peak data rate and bandwidth, 10000 times in each group, the average number of server intrusion to the security architecture server and the existing LTE core network server are shown as Figure 7.

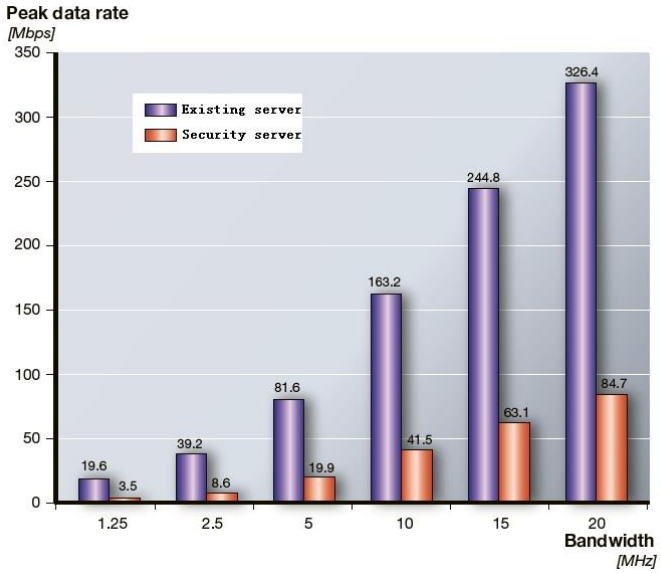

Figure 7. Intrusion Number Comparison

From the above experimental results, we can see clearly that communication efficiency and security of the security architecture server is higher than existing LTE core network server.

5. Conclusions

In order to prevent the network intrusions from LTE core servers from open environment in 4G communication network, a new high security computer architecture is proposed and designed in the paper. The architecture realized hardware-level physical isolation, so it can effectively ensure the security of sensitive data in LTE core servers. Experimental results also proved the effectiveness and security of the architecture.

References

[1] D. Astely, E. Dahlman, A. Furuskar, Y. Jading, M. Lindstrom and S.Parkvall, "LTE: The Evolution of Mobile Broadband", IEEE Commun. Mag., vol. 4, no. 47, **(2009)**.
[2] Y. Park and T. Park, "A Survey of Security Threats on 4G Networks", Proceedings of the IEEE Globecom Workshops, **(2007)**.
[3] C. Kolias, G. Kambourakis and S. Gritzalis, "Attacks and countermeasures on 802.16: Analysis and assessment", Communications Surveys & Tutorials, vol. 1, no. 15, **(2013)**.
[4] C. B. Sankaran, "Network Access Security in Next-generation 3GPP Systems: A Tutorial", IEEE Commun. Mag., vol. 2, no. 47, **(2009)**.
[5] N. Seddigh, B. Nandy, R. Makkar and J. F. Beaumont, "Security Advances and Challenges in 4G Wireless Networks", Proceedings of the 8th International Conference on Privacy Security and Trust, **(2010)**.
[6] W. Tiedong, S. Fengjing, S. Rencheng and H. Huang, "A hardware implement of bus bridge based on single CPU and dual bus architecture", Proceedings of International Symposium on Computer Science and Computational Technology, **(2008)**.
[7] B. Bevan and Y. Zhiyi, "Hardware and Applications of AsAP: An Asynchronous Array of Simple Processors", Proceedings of the IEEE HotChips Symposium on High-Performance Chips, **(2006)**.

Authors

Gengxin Sun, he received his Ph.D. degree in Computer Science from Qingdao University, China in 2013. He is currently an Associate Professor in the School of Computer Science and Engineering at Qingdao University. His main research interests include embedded system, operating system, complex networks, web information retrieval and data mining.

Sheng Bin, she received her Ph.D. degree in Computer Science from Shandong University of Science and Technology, China in 2009. She is currently a lecturer in the School of Software Technology at Qingdao University, China. Her main research interests include embedded system, operating system, complex networks, cloud computing and data mining.

Yixin Zhou, she received her Ph.D. degree in Computer Science from Qingdao University, China. She is currently an Associate Professor in the School of Computer Science and Engineering at Qingdao University. Her main research interests include complex networks, web information retrieval and data mining.

