A Proposal of the Security System for the next Generation Mobile Telecommunication System

Young-Ho Park* and Hoon-Jae Lee**

요 약 본 논문에서는 차세대 이동통신 시스템을 위한 새로운 보호시스템을 제안한다. 제안한 보호시스템은 3GPP의 네트워크 영역 보호에 기초하며 3GPP의 2계층인 RLC 계층에 비밀보장 및 무결성 서비스를 제공한다. 제안한 보호시스템은 3GPP 프로토콜의 변형없이 보호서비스를 제공할 수 있으며 전송부하가 작다는 장점들을 가진다. 보호 알고리즘과 보호모드는 3GPP의 3계층인 RRC 계층에서 제어된다.

Abstract This paper proposes a new security system for the next generation mobile telecommunication system. The system is based on the network domain security of the 3GPP. The system provides confidentiality and integrity services in the RLC layer, the second layer of 3GPP. Our system has merits in that it can provide security services without any modification to the 3GPP protocol and has low transmission overhead. Security algorithm and mode are controlled by the RRC layer, the third layer of 3GPP.

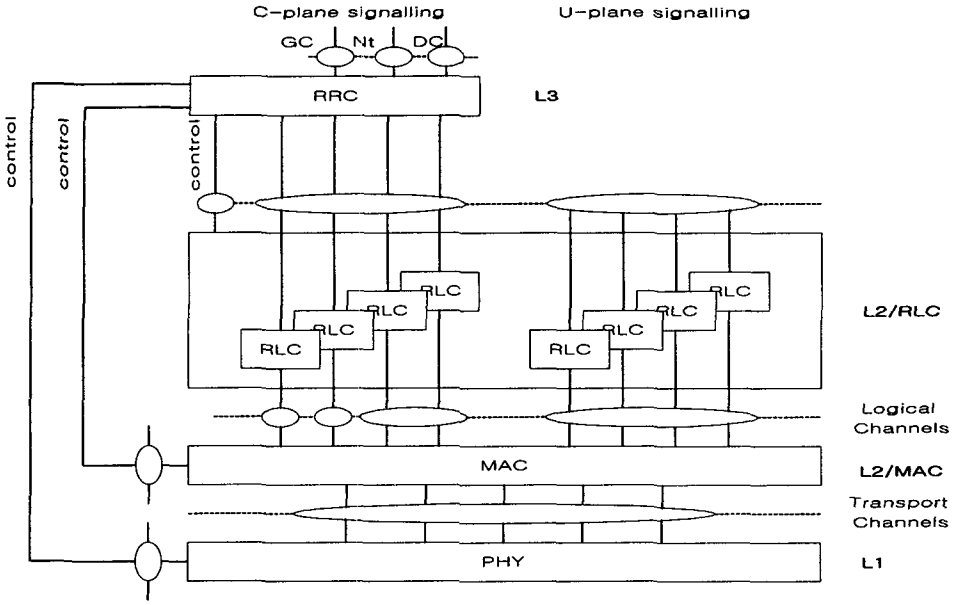
1. Introduction

Mobile communication systems are areas of rapid growth as the technology necessary to provide time and space independent services[1]. On the functional viewpoint, mobile communication systems are classified as the 1st generation(analog system), 2nd generation(digital system) and next generation(next-generation system). While current second generation systems ,such as IS-95 and GSM, are providing commercial service in the global areas, the next generation systems, such as IMT-2000 and UMTS, are in the standardization phase[2]. Mobile communication systems use wireless media as a transmission media, it's possible to provide communication convenience to users, but it has some drawbacks such as eavesdropping and difficulty of monitoring[3]. The illegal use of the transmitted information prevents the mobile communication systems from settling on the information society.

To develop a 3rd generation mobile telecommunication systems, a collaborative research project called "3GPP(3rd generation partnership project)" is accomplished by the ARIB, ETSI, T1, TTA and TTC from 1998. The studies by this project includes classification of radio access network, core network and terminal group[4], but study concerning security is in a relatively frail phase[5,6]. 3GPP defines security regions as network access security, network domain security, user domain security, application domain security, and visibility and configurability of security[7].

This paper proposes a new security system in the network domain for the next generation mobile telecommunication system. The security system provides confidentiality and integrity services in the RLC(radio link control)[8] layer, the second layer of 3GPP. This security system has merits in that it can

* 상주대학교 전자전기공학과 조교수
** 경운대학교 컴퓨터공학과 전임강사

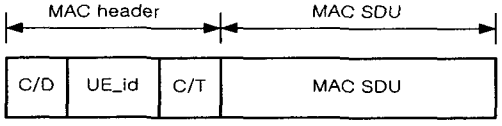


<Figure 1>. Radio interface protocol architecture in 3GPP.

provide security services without any modification to the 3GPP protocol and has low transmission overhead. Security algorithm and mode are controlled by the RRC(radio resource control) layer[9]. A merit that we can check security service on the telecommunication-node with security service offered between nodes is also added.

2. 3GPP Radio Interface Protocol Architecture

<Figure 1> shows the radio interface protocol architecture in 3GPP. It is classified by three layers. The physical layer offers information transfer services to MAC and higher layers. The MAC layer provides data transfer of MAC SDUs between peer MAC entities, reallocation of radio resources and MAC parameters, and reporting of measurement. The RLC layer provides connection establishment/release, data transfer, QoS setting, and notification of unrecoverable errors. RRC(radio resource control) layer handles the control plane signalling of layer 3 between UE(user equipment)s and UTRAN(UMTS terrestrial radio access network).



<Figure 2>. MAC data PDU.

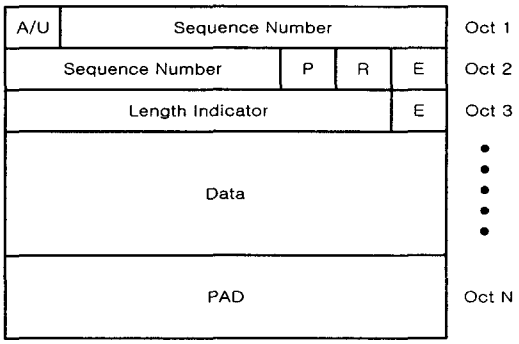
<Figure 2> shows the data PDU of MAC layer[10].

- The C/D field is a single-bit flag that provides identification of the logical channel class on FACH(forward link access channel) and RACH(random access channel) transport channels, i.e. whether it carries CCCH(common control channel) or dedicated logical channel information.

- The C/T field provides identification of the logical channel instance when multiple logical channels are carried on the same transport channel. The C/T field is used also to provide identification of the logical channel type on dedicated transport channels and on FACH and RACH when used for user data transmission. The size of the C/T field may be

variable.

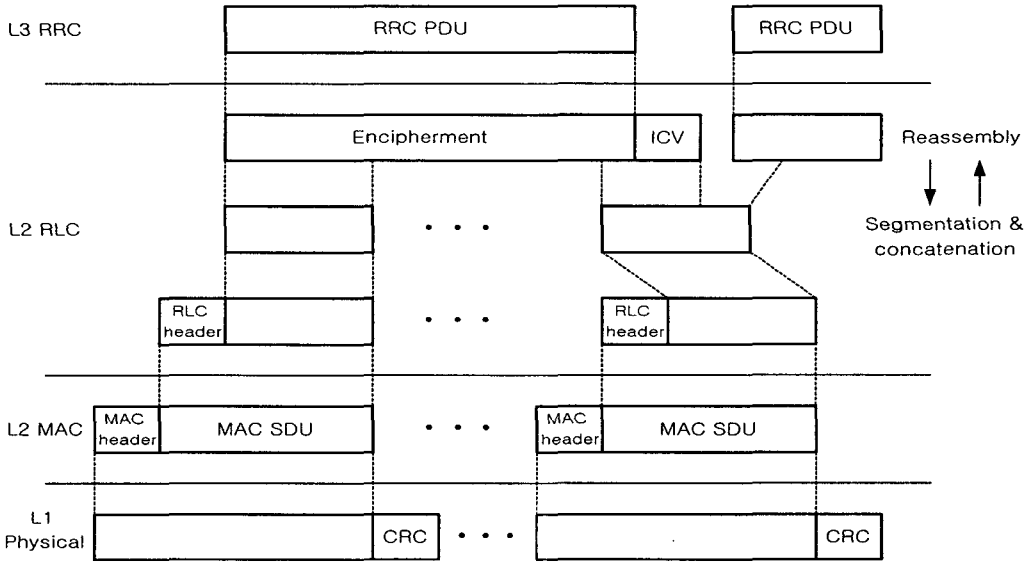
- The UE_Id field provides an identifier of the UE . The following types of UE_Id are currently defined: s-RNTI , this UE_Id is related to the serving RNC, c-RNTI, this UE_Id is related to the controlling RNC.



<Figure 3>. RLC data PDU.

<Figure 3> shows the data PDU of RLC layer.

- A/U bit is a single bit that indicates acknowledged mode data PDU or unacknowledged mode data PDU/control PDU. If it indicates acknowledged mode, the PDU is AMD PDU.
- SN(Sequence Number) field indicates the sequence number of the payload unit. In normal acknowledged-mode RLC-PDU header it is the sequence number of the first PU(payload unit) in the PDU. If the PU's are not in sequence, a sequence number is indicated separately for each PU in the extended header.
- Polling bit (P) is a single bit that is used to request a status report from the receiver RLC.
- Extension bit (E) is a single bit that indicates whether the next octet will be header information (LI) or data.
- Reserved (R) field is a single bit. This field is coded as zero and ignored by the receiver.
- Length Indicator (LI) field is 7 bits. This field is optional and is used if concatenation or padding takes place in RLC. It indicates the end of the last segment of a SDU. Especially 0000000 indicates that the previous RLC PDU is exactly filled with the last segment of a RLC SDU, and 1111111 indicates that the rest part of the RLC PDU is padding.



<Figure 4>. The proposed security model for the next generation mobile telecommunication system.

3. The Proposed Security System

3GPP defines security regions as network access security, network domain security, user domain security, application domain security, and visibility and configurability of security. This paper proposes a new security system for the network domain security. The network domain security needs entity authentication, data confidentiality, and data integrity services. Entity authentication service ensures that no malicious operational or maintenance commands can be injected into a network domain by intruder. Authentication service may be achieved either by an explicit or implicit entity authentication mechanism, which is performed each time data are exchanged between two network entities. Implicit authentication is realized by exchanging encrypted messages only, so that only an entity in possession of a certain shared key can make use of the data. Explicit authentication mechanisms can be achieved either by asymmetric(e.g. by using digital signatures) protocols or by symmetric (e.g. challenge-response) protocols. If these authentication data are eavesdropped in the network domain, serious fraud problems will arise. Therefore, confidentiality of sensitive data are critical here, e.g. authentication data or other subscriber data inside the network domain. The data integrity service ensures that operational and maintenance commands or user data exchanged between two network elements cannot be modified by an intruder without being detected.

<Table 1>. The comparison of security characteristics in each layer.

layer / characteristics	MAC	RLC	RRC
protection boundary	node-to-node	node-to-node	end-to-end
transmission load	large	small	small
protocol modification	needed	not needed	not needed
MAC PDU increased	yes	no	no
security unit	MAC PDU	RLC PDU	RRC PDU

Data confidentiality and data integrity service can be provided in the RLC layer. <Figure 4> shows the proposed security model for the next generation mobile telecommunication system. Data confidentiality service is provided in the RLC SDU before segmentation. The reserved bit of the RLC header represents whether data confidentiality service is provided or not. Data integrity service is provided in the RLC SDU after data confidentiality service is provided. ICV(integrity check value) field is used to check integrity of a transmitted data. It has a disadvantage of transmission overhead grows because ICV field is added to RLC or MAC(medium access control) PDUs when integrity service is provided to MAC layer or RLC layer after segmentation. When data confidentiality service is applied to MAC layer, there is no field that indicate whether data confidentiality service is applied or not. Therefore, as a shortcoming, protocol modification is required. On the other hand, when data confidentiality service is applied to RLC layer, protocol modification is not required because encryption can be represented by the use of the reserved bit located at RLC PDU header. Security algorithm and mode are controlled by RRC layer and decided when RRC connection is established.

4. Conclusion

This paper proposed a new security system for the network domain security of the 3GPP. The network domain security needs entity authentication, data confidentiality, and data integrity services. Authentication service may be achieved either by an explicit or implicit entity authentication mechanism, which is performed each time data are exchanged between two network entities. Data confidentiality and data integrity service are provided in the RLC layer. This security system has merits in that it can provide security services without any modification to the 3GPP protocol and has low transmission overhead.

References

[1] L.Hagen, M.Breugst, and T.Magedanz,"Impacts of Mobile Agent Technology on Mobile Communication System Evolution," IEEE Personal Communications, August 1998, pp.56-69

[2] L.N.Kriaras, A.W.Jarvis, V.E.Phillips, and D.J.Richards,"Third-Generation Mobile Network Architecture for the Universal Mobile Telecommunications System," Bell Labs Technical Journal, Summer 1997, pp.99-117

[3] A. Mehrotra and L.S. Golding, "Mobility and Security Management in the GSM System and Some Proposed Future Improvements," Proceeding of the IEEE, Vol.86, No.7, July 1998, pp.1480-1497

[4] 3G TS 25.301, 'Radio Interface Protocol Architecture', 3rd Generation Partnership Project(3GPP): Technical Specification Group(TGS) RAN: WG2, April 1999

[5] 3G TS 21.133, 'Security Treats and Requirements', 3rd Generation Partnership Project(3GPP): Technical Specification Group(TGS) SA: 3G Security, May 1999

[6] 3G TS 33.120, 'Security Principles and Objectives', 3rd Generation Partnership Project(3GPP): Technical Specification Group(TGS) SA: 3G Security, May 1999

[7] 3G TS 33.102, 'Security Architecture', 3rd Generation Partnership Project(3GPP): Technical Specification Group(TGS) SA: 3G Security, May 1999

[8] 3G TS 25.322, 'Description of the RLC Protocol', 3rd Generation Partnership Project(3GPP): Technical Specification Group(TGS) RAN: WG2, April 1999

[9] 3G TS 25.331, 'RRC Protocol Specification', 3rd Generation Partnership Project(3GPP): Technical Specification Group(TGS) RAN: WG2, April 1999

[10] 3G TS 25.321, 'MAC Protocol Specification', 3rd Generation Partnership Project(3GPP): Technical Specification Group(TGS) RAN: WG2, April 1999

박 영 호

1989년 경북대학교 공과대학 전자공학과 (공학사)
1991년 경북대학교 대학원 전자공학과 (공학석사)
1995년 경북대학교 대학원 전자공학과 (공학박사)
1996년 3월 - 현재 상주대학교 전자전기공학과 조교수
관심분야: 정보보호, 컴퓨터 네트워크

이 훈 재

1985년 경북대학교 공과대학 전자공학과 (공학사)
1987년 경북대학교 대학원 전자공학과(공학석사)
1998년 경북대학교 대학원 전자공학과(공학박사)
1987년 - 1998년 국방과학연구소 선임연구원
1998년 3월 - 현재 경운대학교 컴퓨터공학과 전임강사
관심분야: 정보보호, 디지털 통신