모바일 기기를 위한 안전한 유비쿼터스 스토리지 시스템

태유슈* · 이은유* · 이훈재** · 임효택**

A Secure Ubiquitous Storage System for Mobile Devices

Yu-Shu They* · Ern Yu Lee* · Hoon Jae Lee** · Hyo Taek Lim**

요 약

최근 유비쿼터스 기술의 급속한 성장으로 모바일 컴퓨팅 분야에서의 스토리지 용량에 대한 요구가 증가하였다. 가상 스토리지 프로토콜인 iSCSI(Internet Small Computer Interface)는 이러한 문제를 효율적으로 해결하기 위한 방안이 될 수 있다. 그러나, 이 프로토콜의 불안전한 특성은 스토리지 시스템을 불안하고 외부에 노출되게 할 우려가 있다. 따라서, 본 논문에서는 모바일 기기를 위한 안전하고도 가벼운 iSCSI 기반의 가상 스토리지 스킴을 설계하고 제안하고자 한다. 성능평가를 통해 제안된 알고리즘은 기존의 IPsec보다 100% 읽기/쓰기 성능개선을 보여주고 있다.

ABSTRACT

The rapid growth of ubiquitous technology has increased the demand of storage capacity in mobile computing. iSCSI (Internet Small Computer Interface), a virtual storage protocol would be one of the possible solutions to resolve this problem. However, the insecure nature of this protocol makes it vulnerable to malicious attacks. In this paper, we aims to design and propose a new secure lightweight iSCSI-based virtual storage scheme for mobile devices. Suitable security mechanisms are considered in the design of our proposed solution in order to overcome existing security problems in iSCSI. Relevant experiments are carried out and the results revealed that the efficiency of proposed algorithm in which it introduces over 100% Read/Write performance improvement compared with the IPsec approach.

키워드

Security, Virtual Storage, iSCSI, Cryptography, Mobile Computing, Ubiquitous

Ⅰ. Introduction

With the advancement of wireless and mobile technologies in recent decades, information is more likely to be accessed ubiquitously. This phenomenon causes an enormous increase in the demand of mobile data storage. Various approaches are proposed to enhance the storage capability and data accessibility of mobile devices.

The adoption of iSCSI (Internet Small Computer System Interface) protocol in mobile devices in order to expand the storage capability is no longer a new idea [1]. iSCSI is a network storage protocol which is developed by Internet Engineering Task Force (IETF). It allows SCSI commands and hard disk data to be transported over TCP/IP network and hence makes the access of hard disk via Internet become possible [2].

* 동서대학교 디자인&IT 전문대학원
** 동서대학교 컴퓨터공학과

접수일자 : 2007. 11. 20

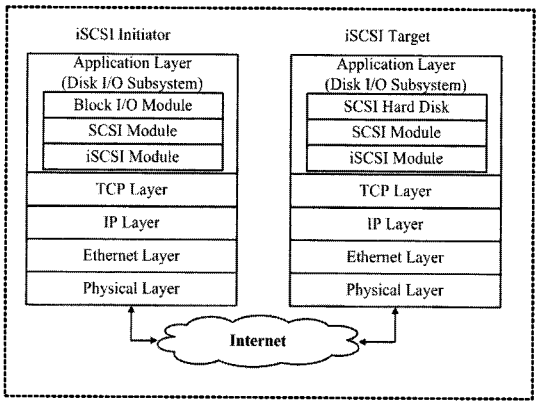

그림 1. iSCSI 프로토콜 모델
Fig. 1 iSCSI protocol Model

Figure 1 shows the protocol model for iSCSI. The model consists of an initiator (iSCSI Client) and a target (iSCSI Server). When a block I/O request is issued from at the initiator side, appropriate SCSI Command Descriptor Block (CDB) will be generated from the SCSI Module. The CDB is then encapsulated together with the subsequent hard disk data to form a single Protocol Data Unit (PDU), which is the basic transaction unit in iSCSI protocol. The PDU is then and transported over the network to the target by the iSCSI module. Similarly, the iSCSI module at the target side will decapsulate and reassembles iSCSI packet into CDB and passes it to the SCSI module. The response is generated and replied with the same encapsulation model.

With the exploitation of the widely available TCP/IP standard, iSCSI is able to provide a low-cost, long distance, high speed, reliable and simple network storage scheme for mobile devices. However, iSCSI protocol itself is vulnerable to malicious attacks. Transporting the sensitive commands and data without proper protection might lead to the compromise of the whole storage system. The insecure nature of the iSCSI protocol causes it not likely to be considered in an open network environment unless external security mechanisms are enforced.

This paper contributes toward the design, implementation, and evaluation of a new secure lightweight iSCSI-based virtual storage scheme for mobile devices. It turns out that existing security protocols such as Internet Protocol Security (IPsec) have proved to be a major hindrance to the overall throughput. In the storage industry where performance is the key consideration, such performance degradation is obviously unacceptable.

In an effort to provide robust, standard-based, interoperable secure storage solutions for mobile device, a security module which is suitable for mobile devices was proposed. Given that mobile devices have limited resources, a lightweight variation of the Secure Remote Password based on Elliptic Curve Cryptography (EC-SRP) was chosen for in-band initiator-target authentication protection [3]. One of the greatest advantages of using elliptic curves to implement Secure Remote Password is that it poses the potential in providing equivalent security to the existing public key schemes but with shorter key lengths. After that, the entire iSCSI PDU will be encrypted using the session key produced by the authentication process and a message authentication code is generated from the resulting cipher text. Encrypt-then-MAC was proven by Mihir Bellare and Chanathip Namprempre to be the most secure and favorable choice to facilitate authenticated encryption scheme [4]. It is claimed to be secured against chosen plain text and cipher text attack while data integrity is guaranteed. To identify the significance of the proposed framework, we have implemented our proposed scheme and conducted an experiment to study its performance. Surprisingly, there is only a minor degradation of the overall performance which has shines the path for us to further our research in this area.

The rest of this paper is organized as follows: Section 2 discusses several related work. Section 3 describes the design of our proposal in detail. Section 4 reveals the implementation and performance evaluation with micro benchmark along and the analysis for both IPsec approach and our proposed scheme before we summarize the paper and describe our future work in section 5.

Ⅱ. Related Work

In [5], in-band authentication between the initiator and target at iSCSI connection level is recommended in conjunction with packet protection mechanism to create a

secure communication channel between iSCSI initiator and target. Challenge Handshake Authentication Protocol (CHAP) or Secure Remote Password (SRP) is proposed with the purpose of providing endpoints mutual authentication during the in-band initiator-target authentication phase in [6].

In the RFC specification of iSCSI protocol [7], Internet Protocol Security (IPsec), a standardized network layer security framework is recommended to provide end-to-end data confidentiality and authentication protection. IPsec consists of 2 types of message architecture: Authentication Header [8] which guarantees data authentication as well as data integrity and Encapsulating Security Payload (ESP) [9] which provides data confidentiality and integrity. Additionally, Internet Key Exchange protocol (IKE) can be used in conjunction with IPSec to promote robust authentication and encryption of IP packets [10].

The iSCSI authentication methods that described above do not provide per-packet security protection. It relies on the IPsec protocol to provide per-packet data confidentiality, integrity and authentication services. Also, these authentication methods do not perform well in mobile devices with limited computational resource. The same situation also happened on IPsec. Furthermore, the IP address of a mobile device usually changes frequently [11]. This limitation can be served as an impediment to mobility of mobile devices. In view of various limitation exhibited by IPsec, we aim to find a practical solution that is more lightweight and offers higher performance.

III. Secure Ubiquitous Storage System

The design of our secure virtual storage scheme aims to provide a iSCSI-based lightweight secure storage access method for mobile devices which fulfill major security goals included user authentication, data confidentiality, packet authenticity, and message integrity. In other words, the storage system should be able to avoid from unauthorized access, message interception and packet modification.

To prevent the iSCSI storage system to be accessed from unauthorized parties, a secure initiator-target authentication procedure has to be carried out before an iSCSI session is created. We propose to use EC-SRP as our authentication and session key-agreement protocol for in-band initiator-target authentication. EC-SRP protocol is a Secure Remote Password (SRP) protocol which uses Elliptic Curve method for its secret key and public key derivation. The security of the EC-SRP protocol is depends on the intractability of the Elliptic Curve analogue of discrete logarithm, which is a well-known and extensively studied computationally hard problem [12]. The length of secret key is a major factor that will affects the performance and security level of a cryptosystem. EC-SRP is proven to be able to offer higher throughput achieve equivalent level of security compared to other algorithms by using shorter secret key [13]. A 256-bit session key is generated at the end of the EC-SRP authentication and key agreement process. This session key is then used to encrypt and decrypt data in the subsequent secure iSCSI transactions.

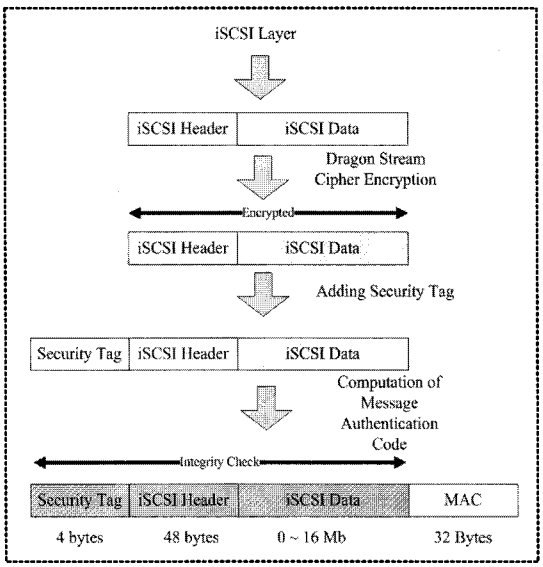

그림 2. 암호화된 iSCSI PDU 포맷
Fig. 2 Encapsulation of Encrypted iSCSI PDU

In the protection of iSCSI messages, a fast word based symmetric stream cipher algorithm, Dragon is used for the data encryption. The design of Dragon was motivated by ECRYPT stream cipher project (eStream), a long term

project to evaluate and identify new stream cipher that is suitable for widespread adoption. Dragon has successfully entered the 3rd phase of evaluation in the eSTREAM project. It is proven to be secure form various currently known cryptanalytic attacks. The structure of Dragon consists of a large non-linear feedback shift register (NLFSR), a state update function (F function) and a 64-bit memory state. 64 bits of keystream are generated in a single iteration of the algorithm. Dragon is a high-speed, low memory consumption algorithm. It is able to produce a throughput of gigabits per second with just about 4 kilobytes of memory in software implementation. In addition, the high performance and efficiency in rekeying indicates that it is very suitable for mobile and wireless communication environment which requires frequent rekeying. The detailed design and evaluation of Dragon can be found in [14].

To ensure the integrity of the encrypted iSCSI messages, HMAC-SHA256 [15], which is a hash function based message authentication code algorithm are adopted in our scheme. This message authentication code algorithm uses SHA256 [16] as its hashing mechanism. The SHA256 is the 2nd generation of the Secure Hash Algorithm (SHA). It has longer digests than SHA and thus provides 256-bit of security against collision attack. Up to now, SHA256 is secure enough to withstand all known hash attacks. It suits perfectly in conjunction with HMAC algorithm to provide a highly secure message authentication code.

Figure 2 shows an iSCSI PDU is encrypted by Dragon stream cipher using the session key. The cipher text is the computation result of the XOR operation between keystream and the iSCSI PDU. As the cipher text does not reveal any information about the length of the original iSCSI PDU, which is required by the receiver side for the decryption purpose; we introduce a security tag which carries 4 bytes of original iSCSI PDU length to be integrated with the encrypted iSCSI PDU. The computation of message authentication code is then performed on the concatenation of security tag and the cipher text base on the HMAC-SHA256 algorithm. The resulting message authentication code will be appended to the end of the cipher text to construct a secure iSCSI PDU which is safe to be transmitted over TCP/IP network

Once the secure iSCSI PDU arrives at the receiver side, integrity and authenticity check is carried out by comparing the recomputed and received message authentication code. The received PDU will be discarded if both recomputed and received message authentication code does not match each other. In the case of the received PDU passes the message authentication code check, the cipher text from the secure iSCSI PDU will be decrypted. Lastly, the decrypted iSCSI PDU is digested by the original iSCSI module to complete the relevant iSCSI tasks.

In this session, a protection scheme with the features of authentication, key-agreement, data encryption and integrity

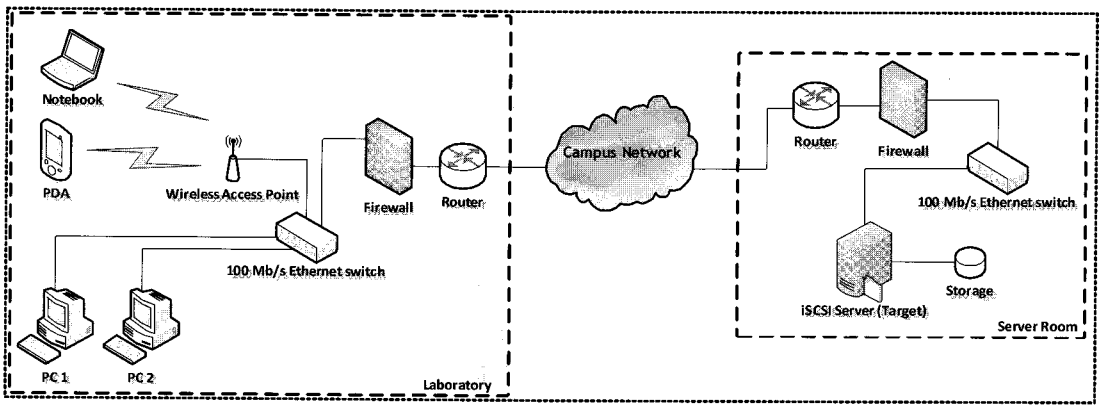

그림 3. 테스트베드 환경
Fig. 3 Testbed Environment

check for iSCSI is discussed. The lightweight nature of the proposed algorithms makes our scheme more appropriate to be considered in a mobile device with limited resources. The implementation and performance analysis is discussed in the next session

Ⅳ. Implementation and Performance Evaluation

We have successfully implemented our prototype based on the UNH-iSCSI [17], an open source iSCSI development project maintained by InterOperability Laboratory from University of New Hampsphire. We implanted our codes into both initiator and target modules to change the native iSCSI implementation into our proposed scheme. The modified software modules are installed in both initiator and server machines in order to conduct our experiment.

Figure 3 depicts our testbed environment. The iSCSI target server is an Intel Premier Provider 2001 equipped with dual 1 GHz of Intel Pentium III (Coppermine), 512MB RAM and a 20GB IBM DDYS-T18350M hard disk. The server machine is running on Fedora Core 1 (kernel version 2.4.22-1.2115.nptlsmp) along with our modified iSCSI target implementation. It is located in a server room and connected directly to the campus network by a 100 MB/s Ethernet switch via Intel Corporation 82557/8/9 [Ethernet Pro 100] network interface card.

On the other side, the iSCSI initiator module is installed in Zaurus SL-6000, a Linux (kernel version 2.4.18-rm7-pxa3-embedix) based PDA manufactured by Sharp. It runs with an Intel PXA255 400MHz XScale processor, 64MB SDRAM and built-in with 802.11b WiFi module.

To quantitatively evaluate the performance of the iSCSI

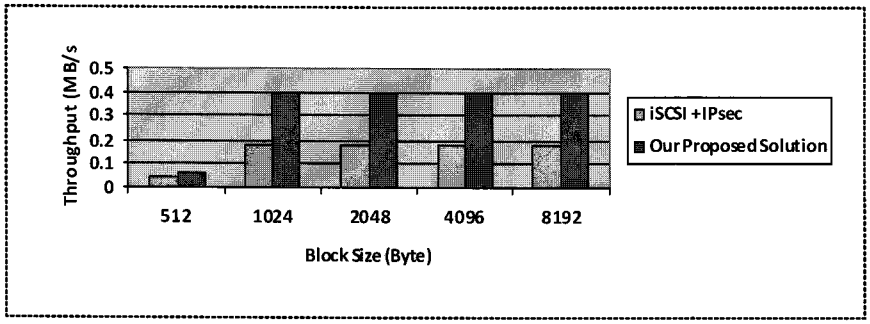

그림 4. IPsec 기능을 가진 iSCSI와 제안된 방법의 Write throughput 비교
Fig. 4 Write throughput comparison between iSCSI with IPsec (AH and ESP) and our proposed solution (Dragon and HMAC-SHA256)

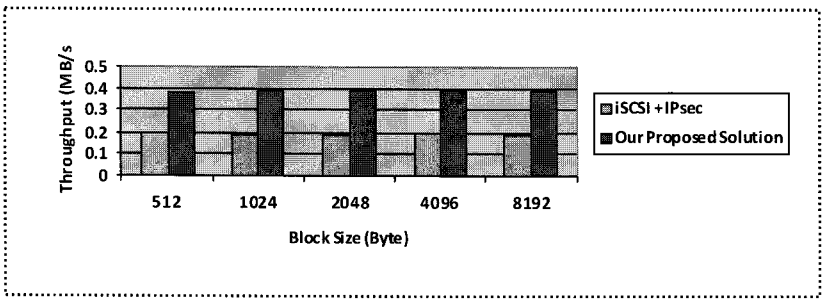

그림 5. IPsec 기능을 가진 iSCSI와 제안된 방법의 Read throughput 비교
Fig. 5 Read throughput comparison between iSCSI with IPsec (AH and ESP) and our proposed solution (Dragon and HMAC-SHA256)

storage system with and without security in a real environment, we used a portable, robust and fully threaded file system tool called Tiobench [18]. Tiobench is configured to read or write multiple numbers of times on varying block sizes ranging from 512 bytes to 8KB. In our experiment, 256MB file size which is 4 times greater than the total memory of PDA is chosen as to minimize the local caching effects. Figure 4 and 5 show the average write and read throughput various scheme respectively.

According to Figure 4, we can see that the performance of iSCSI with IPsec performs badly in the experiments. It lacks behind our proposed scheme by approximately 50% throughput reduction. We are aware that in the case of the block size is equals to 512 bytes, the writing throughput dropped dramatically. This is because small block size may cause low utilization of disk transfer capability and almost all access needs to perform a seek operation which results a low throughput. From Figure 5, we can observe that. average read performance of our proposed scheme achieves around 105% of improvements over IPsec in all the tested block size.

표 1. Write 성능 비율
Table. 1 Write Performance Ratio

Block Size	iSCSI + IPsec	Our Proposed Solution	Ratio (%)
512	0.0484	0.0636	**131%**
1024	0.1809	0.4010	**222%**
2048	0.1822	0.4033	**221%**
4096	0.1809	0.4030	**223%**
8192	0.1810	0.4040	**223%**

Table 1 and Table 2 show the write and read performance throughput ratio between iSCSI with IPsec and our proposed scheme. Other than 512 bytes, the performances of the rest of the block size as stated in both tables are able to achieve the ratio of over 200%.

Table 3 depicts the result obtained from a latency test. As shown in the table, our proposed scheme introduced a lower latency in both read and write operations. We also noticed that IPsec does not perform well when the block size increasing. This shows that our proposed scheme has higher performance than IPsec when larger block size is being used

표 2. Read 성능 비율
Table. 2 Read Performance Ratio

Block Size	iSCSI + IPsec	Our Proposed Solution	Ratio (%)
512	0.1936	0.3766	195%
1024	0.1914	0.3930	205%
2048	0.1917	0.3913	204%
4096	0.1945	0.3916	201%
8192	0.1922	0.3956	206%

표3. 평균 지연시간 비교
Table. 3 Comparison of Average Latency

Block Size	Average Latency		Latency Difference (ms)
	iSCSI + IPsec	Our Proposed Solution	
512	0.5215	0.3825	0.1390
1024	0.1905	0.0900	0.1005
2048	0.3390	0.1780	0.1610
4096	0.6970	0.3475	0.3495
8192	1.3515	0.6900	0.6615

V. Conclusions

In this paper, we presented a lightweight and secure iSCSI-based virtual storage scheme for mobile devices. We have implemented a prototype based on our design to evaluated the performance of our proposed scheme. Obtained experiment results shown that our proposed scheme is far more superior than IPsec based approach in term of performance in which it achieved over 100% increasement in both Read and Write operation. The results revealed that our proposed scheme is suitable to be adopted by the mobile devices due to its high performance, and lightweight characteristic. In the near future, we would like to evaluate the CPU utilization and the performance of our approach in a multiple clients environment.

References

[1] Hyotaek Lim, Saebom Choi.: Design and Implementation of iSCSI-based Virtual Storage System for Mobile Health Care, HEALTHCOM 2005, Jun. 2005, PP 37-42

[2] J. Satran, K. Meth, C. Sapuntzakis, M. Chadalapaka, E. Zeidner.: Internet Small Computer Systems Interface (iSCSI), Request For Comments 3720, April 2004.

[3] T. Wu: The Secure Remote Password Protocol, Proceedings of the Internet Society Symposium on Network and Distributed System Security, NDSS 98, San Diego, California. March 1998, PP. 97-111
[4] M. Bellare and C. Namprempre.: Authenticated encryption: Relations among notions and analysis of the generic composition paradigm, Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, Lecture Notes In Computer Science, Vol. 1976, pp. 531- 545.
[5] B. Aboba, J. Tseng, J. Walker, V. Rangan, and F. Travostino.: Securing Block Storage Protocols over IP, Request For Comments 3723, April 2004.
[6] S. Kent and R. Atkinson.: Security Architecture for the Internet Protocol, Request For Comments 2401, November 1998.
[7] Shuang-Yi Tang, Ying-Ping Lu, David H.C Du.: Performance Study of Software-Based iSCSI Security, Proceedings of the First InternationalIEEE Security in Storage Workshop, December 11, 2002
[8] S. Kent and R. Atkinson.: IP Authentication Header, Request For Comments 2402, November 1998.
[9] S. Kent and R. Atkinson and.: IP Encapsulating Security Payload (ESP), Request For Comments 2406, November 1998.
[10] D. Harkins and D. Carrel.: The Internet Key Exchange (IKE), Request For Comments 2409, November 1998.
[11] Jail Arkko and Pekka Nikander.: Limitations of IPsec Policy Mechanisms, In Security Protocols, Eleventh International Workshop, Cambridge, UK, April 2003.
[12] IEEE Standard 1363.2 Study Group. Password-Based Public-Key Cryptography, http://grouper.ieee.org/groups/1363/passwdPK
[13] K. Lauter, "The advantages of Elliptic Curve Cryptography For Wireless Security", IEEE Wireless Communications, vol. 11, no. 1, Feb 2004, PP. 62-67
[14] K. Chen, M. Henricksen, W. Millan, J. Fuller, L. Simpson, E. Dawson, H. Lee, and S. Moon.: Dragon: A fast word based stream cipher, ECRYPT Stream Cipher Project Report 2005/2006.
[15] H. Krawczyk, M. Bellare and R. Canetti.: HMAC: Keyed-Hashing for Message Authentication, Internet Engineering Task Force, Request For Comments 2104, 1997.
[16] National Institute of Standards and Technology, FIPS-180-2: Secure Hash Standard (SHS), August 2002.
[17] UNH-iSCSI project, http://unh-iscsi.sourceforge.net/
[18] Threaded I/O Tester, http://sourceforge.net/projects/tiobench/

저자소개

태 유 슈 (They Yu Shu)

2002년 Multimedia University (이학사)
2006년~현재 동서대학교 디자인&IT 전문대학원 석사과정

※관심분야 : IP Storage Network, Storage Security ,IPv6, Mobile Application

이 은 유(Lee Ern Yu)

2001년 Multimedia University (이학사)
2006년~현재 동서대학교 디자인&IT 전문대학원 석사과정

※관심분야: Computer Security and Cryptography, Storage Security ,Network Security

이 훈 재 (Hoon Jae Lee)

1985년 2월 경북대학교 전자공학과 졸업 (학사)
1987년 2월 경북대학교 전자공학과 졸업 (석사)
1998년 2월 경북대학교 전자공학과 졸업(박사)
1987년2월~1998년1월 국방과학 연구소 선임연구원
1998년3월~2002년2월 경운대학교 조교수
2002년3월~현재 동서대학교 컴퓨터정보공학부 부교수
※관심분야 : 암호이론, 네트워크보안, 부채널공격

임 효 택 (Hyo Taek Lim)

1988년 홍익대학교 전자계산학과 졸업 (이학사)
1992년 포항공과 대학원 전자계산학과 졸업(공학석사)
1997년 연세 대학교 컴퓨터과학과 졸업(공학박사)
1988년~1994년 한국전자통신연구소 연구원
2000년~2002년 Univ. of Minnesota(미) 컴퓨터공학과 연구교수
1994년~현재 동서대학교 컴퓨터공학과 부교수
※관심분야 : Computer Network, Protocol Engineering, Storage Networking, IPv6, Mobile Application