

무선 컴퓨팅 환경에서의 IPsec 기반 iSCSI 스토리지 시스템의 설계 및 구현

A Design and Implement of IPsec-based iSCSI Storage system in wireless computing environment

정호원, 김대성, 오세웅*

동명정보대학교 정보대학원, 동의대학교 멀티미디어
어공학과*

Chung Ho-Won, Kim Dae-Sung, Oh Sei-Woong*

Graduate School of Information, Tongmyong
Univ. of Information Technology, School
Subject of Multimedia Engineering, Donggeui
University*

요약

현재 무선 네트워크 환경에서 많이 사용되고 있는 PDA의 스토리지 장치의 한계를 극복하기 위해 iSCSI를 이용한 원격 스토리지 시스템이 필요하며, 계속 급증하고 있는 무선 환경에서의 보안 문제를 해결하기 위해 IPsec 적용이 필요하다. 본 논문에서는 PDA 상에서 원격 스토리지 시스템을 사용하기 위한 iSCSI와 보안을 위한 IPsec를 각각 설계, 구현하고 실제 환경에서의 실험을 통해 성능을 알아본다.

Abstract

It need remote storage system using iSCSI to overcome a limit of PDA storage device used in currently wireless network environment, and IPsec to solve a security problem of wireless environment increasing continually. In this paper, it design and implement iSCSI to use a remote storage system on PDA, and IPsec for security. The experimental results in real environment show a system performance.

I. 서론

유선 네트워크를 이용한 인터넷이 보급되어 일반인에게 서비스된 이후로, 급속하게 발전한 지금의 정보통신 사회는 유선에서 무선으로의 혁명이 일어나고 있다. 기존 유선 네트워크에서의 서비스 등이 무선 인터넷 서비스를 통해 제공되기도 하고, 이와 더불어 휴대 전화, PDA 등의 모바일 기기의 발달로 모바일 기기의 사용이 크게 늘어나면서 모바일 기기에 대한 수요가 큰 폭으로 증가 되었다. 모바일 기기를 통한 원격제어, 전자지불 등이 가능하게 되었을 뿐 아니라, 최근 필수적으로 생각되고 있는 대용량 멀티미디어

서비스 지원도 가능하게 되었다. 그러나 현재 일반적으로 사용되고 있는 모바일 기기는 제한된 저장 공간으로 인하여 점차 증가하고 있는 소비자들의 다양한 서비스 요구를 만족시키기에는 많은 문제점을 가지고 있다. 이는 기존의 유선 환경에서 제공되는 서비스를 무선 환경에서 적용하고자 했을 때 제약 사항으로 작용할 뿐만 아니라 모바일 기기를 이용한 다양한 서비스의 제공에 걸림돌이 되고 있음을 의미한다. 특히 사용자들이 요구하는 멀티미디어 및 각종 어플리케이션에서 사용되는 데이터의 크기를 감안하면 모바일 기기의 저장 공간의 제한은 무엇보다 심각한

문제라고 할 수 있다. 이러한 문제를 극복하기 위해 서 필요한 기술이 원격 스토리지 서비스이다.

그리고 무선 환경에서 중요한 문제가 되고 있는 것이 보안이다. 무선 네트워크 환경이 데이터 중심으로 바뀌면서 기존 유선 네트워크에서 발생되고 있는 해킹 등의 보안 문제가 발생되고 있다.

본 논문에서는 무선 환경에서 보안이 제공되는 iSCSI(Internet Small Computer System Interface)와 IPSec(Internet Protocol Security)을 이용한 원격 스토리지 시스템을 구현하고 실제 환경에서의 실험을 통해 성능을 알아본다. 2장에서는 이 논문에서 구현한 IPSec 기반 iSCSI 스토리지 시스템의 기반이 되는 iSCSI와 IPSec 프로토콜에 대해 설명하고, 3장에서는 시스템에 대한 설계와 구현에 대해 설명하고, 4장에서는 구현된 시스템에 대한 성능 실험과 결과를 알아보고, 5장에서는 본 논문의 향후 연구 계획에 대해 기술한다.

II. 배경 지식

1. iSCSI



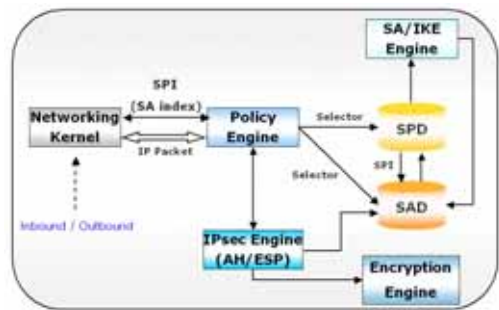
▶▶ 그림 1. iSCSI를 이용한 네트워크 구성도

iSCSI는 IETF(Internet Engineering Task Force)에서 표준화를 진행 중이며[1], 그림 1과 같이 기존의 TCP/IP 네트워크상에서 SCSI 프로토콜을 전송하기 위한 전송 프로토콜로서[2], 시스템 내부적으로 처리되는 블록(Block) 단위의 입출력을 네트워크를 통해 처리할 수 있도록 한다. 이러한 iSCSI 기

술은 기존의 네트워크 환경에 이미 존재하는 네트워크 인프라 구조, 관리 도구, 보안 등을 사용할 수 있고 거리의 제한이 없다는 이점이 있다.

2. IPSec

IPSec은 표준화 작업이 완성된 IP 계층의 인터넷 표준으로, 보안 협상과 그들의 암호화 키들을 관리하기 위한 IKE(Internet Key Exchange)와 데이터 무결성 및 데이터 인증 기능을 주로 수행하는 AH(Authentication Header), 데이터의 기밀성을 제공하는 것을 주요소로 하는ESP(Encapsulating Security Payload) 등으로 구성된다. IPSec은 시스템 상으로, 그림 2와 같이 크게 IP 주소를 바탕으로 보안 정책 수행을 담당하는 정책 엔진, SA(Security Association)/키 관리를 담당하는 IKE (Internet Key Exchange) 엔진, AH(Authentication Header) 및 ESP (Encapsulating Security Payload) 캡슐화 (Capsulation)를 담당하는 IPSec 엔진, 그리고 IPSec 및 IKE 엔진에 필요한 각종 암호 연산 라이브러리 및 API로 구성되는 암호 알고리즘 엔진으로 나눌 수 있다.



▶▶ 그림 2. IPSec 시스템 구성

IPsec 프로토콜은 일반적으로 호스트 간에 가상 터널(Tunnel)을 통해 보안을 제공하는 Tunnel 모드 (Mode) 또는 게이트웨이(Gateway) 간에 가상 터널을 통해 보안을 제공하는 Transport 모드로 동작하

게 된다.

III. 시스템 설계 및 구현

1. 전체 시스템 구성

무선 환경에서의 제한된 저장 공간을 극복하고 보안을 제공하기 위한 iSCSI 기반의 원격 스토리지 시스템 구조는 그림 3과 같이 iSCSI Initiator를 포함하고 있는 모바일 클라이언트(PDA)와 iSCSI Target을 포함하고 있는 서버로 구성된다.



▶▶ 그림 3. 전체 시스템 구성

모바일 클라이언트와 스토리지 서버 사이의 호스트 간 통신이 이루어질 경우 IPSec Transport 모드를 사용하게 되며, 모바일 클라이언트와 스토리지 서버 각각에 TCP/IP 스택과 NIC 드라이버 사이에 IPSec 모듈이 위치하여 IPSec 처리를 하게 된다.

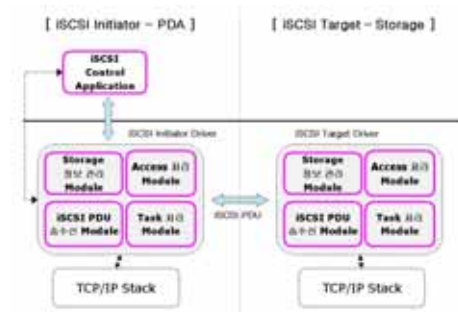
모바일 클라이언트 측의 iSCSI 계층은 시스템의 프로토콜 계층상 TCP/IP 계층과 SCSI 계층 사이에 존재하고 있으며, iSCSI Initiator와 Target이 IP 네트워크를 통해 주고 받는 SCSI 명령 또는 데이터들은 iSCSI 프로토콜에 의해 캡슐화되며, 캡슐화된 iSCSI 프로토콜은 다시 TCP/IP 프로토콜에 의해 캡슐화되어 IP 네트워크로 전달된다.

2. 시스템 세부 설계

2.1 스토리지 시스템을 위한 iSCSI 설계

그림 4와 같이 무선 환경에서의 모바일 클라이언트에는 스토리지 서비스를 받기 위해 iSCSI Initiator 드라이버와 드라이버 제어를 위한 iSCSI Control Application으로 구성되어 있으며, 스토리지 서비스를 제공해주는 스토리지 서버에는 iSCSI Target 드라이버로만 구성되어 있다.

iSCSI Control Application은 iSCSI Initiator에서만 실행되며, iSCSI Initiator에서 iSCSI Target으로의 로그인, 로그아웃 처리를 하거나 iSCSI Initiator와 Target 간의 동작에 필요한 파라미터를 설정하기 위해 사용된다.

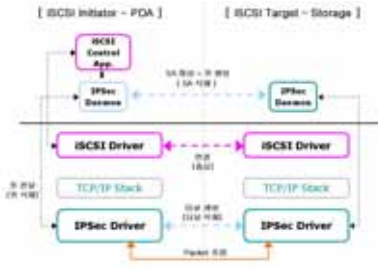


▶▶ 그림 4. iSCSI Initiator/Target 처리 모듈 설계

모바일 클라이언트와 스토리지 서버 각각에 존재하는 iSCSI Initiator와 Target 드라이버는 스토리지 정보 관리 모듈, 접근 처리 모듈, iSCSI PDU 송수신 처리 모듈, Task 처리 모듈 등 4개의 처리 모듈로 나누어진다.

2.2 IPSec 설계

IPSec을 포함하고 있는 시스템의 구조는 그림 5와 같다.



▶▶ 그림 5. IPsec이 포함된 시스템 구조

IPsec을 가지고 있는 시스템 간의 데이터 전송 시 네트워크 상의 패킷에 대한 IPsec 암호화, 복호화에 필요한 키 정보인 SA를 관리하는 IPsec 데몬은 양쪽 호스트 시스템에 모두 존재하며, 생성된 SA를 IPsec 드라이버로 전달하여 드라이버를 구동함으로써 네트워크 패킷에 대한 IPsec 처리를 가능하게 한다.

IPsec 드라이버는 TCP/IP 계층 아래에 존재하며 iSCSI 드라이버와는 별개로 동작하게 되어 있다. iSCSI 로그인, Full-Feature, 로그아웃의 모든 과정에서 iSCSI 드라이버에서 생성되는 모든 iSCSI PDU 들은 아래 계층에 있는 IPsec 드라이버를 통해 IPsec 프로토콜로 캡슐화되어 IP 네트워크로 전송된다.

3. 시스템 구현

본 논문에서 설계된 무선 네트워크 환경에서의 모바일 클라이언트, 스토리지 서버와 IPsec 게이트웨이는 리눅스 상에 구현하였으며, iSCSI Initiator, Target과 IPsec 모듈은 쉽게 적재할 수 있도록 드라이버 형태로 구현하였고, Target으로의 로그인, 로그아웃 등의 명령을 처리하는 iSCSI Control Application과 IPsec의 SA 정보를 관리하는 IPsec 데몬(Daemon)은 gcc 컴파일러를 이용하여 어플리케이션으로 구현하였다.

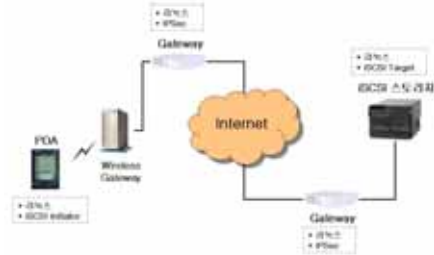
IV. 실험 및 결과

1. 실험 환경

iSCSI와 IPsec에 대한 성능을 측정하기 위한 실험

환경은 그림 6과 같다.

각 실험 환경에서의 성능 측정을 위해 벤치 마킹 프로그램인 Iozone를 사용하였으며[4], 설정된 실험 환경은 표 1과 같다. 스토리지 장치의 하드디스크는 36GByte, 10,000 rpm의 SCSI 디스크를 사용하였다.



▶▶ 그림 6. IPsec이 포함된 실험 환경

Iozone은 파일 시스템의 성능을 측정하는데 널리 사용되고 있는 벤치마킹 프로그램이다. Iozone은 일정한 크기 만큼의 임의의 파일을 생성한 후에, 그 파일에 여러가지 동작을 취하면서 성능을 측정하는 방법을 택하고 있고 블록 단위로 읽고 쓰기를 반복하여 측정을 하게 된다.

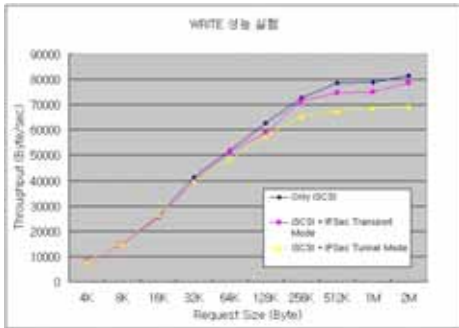
[표 1] 실험 환경

	스토리지 서버	PDA
OS	리눅스 9.0	리눅스 9.0
CPU	Pentium III	Intel Strong ARM
RAM	128 MB	64 MB
NIC	100 Mbps	802.11b (2Mbps)

2. IPsec 사용에 대한 성능 실험

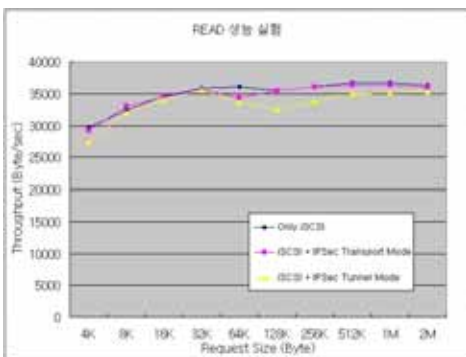
이 실험에서는 iSCSI만을 사용했을 경우, iSCSI와 IPsec을 함께 사용했을 경우에 대한 READ, WRITE 성능을 측정하였다.

실험은 PDA가 사용되는 무선 환경을 감안하여 4KByte에서 2MByte까지 데이터 크기를 변경시켜 가며 각각 WRITE 및 READ 수행에 대해 성능을 측정하였다.



▶▶ 그림 7. WRITE 성능 실험 결과

WRITE, READ 성능 실험 결과는 그림 7, 8과 같다. iSCSI만 사용했을 경우와 iSCSI, IPsec을 함께 사용했을 경우를 비교해보면 iSCSI만 사용했을 경우가 WRITE는 약 9%, READ는 약 2% 성능이 좋을 수 있다. 그리고 iSCSI, IPsec을 함께 사용했을 경우, Transport 모드가 Tunnel 모드에 비해 WRITE는 약 9%, READ는 약 2% 성능이 좋을 수 있는데, 이것은 Tunnel 모드시에 사용되는 IPsec 게이트웨이에서 처리하는 오버헤드(overhead)가 Transport 모드에서 처리하는 오버헤드보다 크기 때문이다.



▶▶ 그림 8. READ 성능 실험 결과

3. iSCSI PDU 크기 조절에 대한 성능 실험

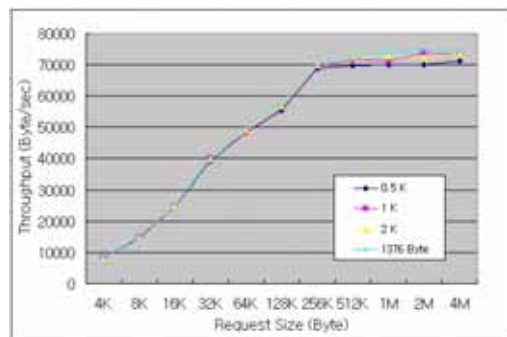
이 실험에서는 iSCSI와 IPsec을 함께 사용했을 경우에 iSCSI PDU 크기를 조절하면서 성능을 측정하

였다.

실험은 0.5K부터 2K까지의 크기와 IPsec을 사용했을 경우의 네트워크 MTU 최대 크기인 1378 Byte와 가장 근접한 1376 Byte 크기로 iSCSI PDU를 조절하면서 4KByte에서 4MByte까지 데이터 크기를 변경시켜가며 성능을 측정하였다.

실험 결과는 그림 9와 같이 iSCSI PDU 크기를 네트워크 MTU 크기와 같게 했을 경우가 다른 PDU 크기로 했을 경우보다 성능이 약간 좋은 것을 확인할 수 있다. 이것은 iSCSI 계층에서 PDU 크기만큼 데이터를 나누는 처리수, iSCSI 계층에서 TCP 계층으로 데이터를 복사하는 수, TCP 계층에서 MTU 크기만큼 데이터를 나누는 처리수에 따라 성능이 달라지기 때문이다.

PDU 크기를 0.5K와 1K로 할 경우를 보면 1376 Byte 크기로 하는 것에 비해 iSCSI 계층에서의 처리수와 iSCSI 계층에서 TCP 계층으로 데이터를 복사하는 수가 많기 때문에 성능이 좋지 않음을 알 수 있다. PDU 크기를 2K로 할 경우를 보면 1376 Byte 크기로 하는 것에 비해 iSCSI 계층에서의 처리수와 iSCSI 계층에서 TCP 계층으로 데이터를 복사하는 수가 약간 줄어들지만, TCP 계층에서 MTU 크기만큼 데이터를 나누는 처리수가 증가하기 때문에 성능이 좋지 않음을 알 수 있다. 그러므로 iSCSI 사용시 네트워크 MTU 크기에 맞춰서 PDU 크기를 조절하는 것이 성능에 좋다는 것을 알 수 있다.



▶▶ 그림 9. IPsec 사용시 PDU 조절에 대한

성능 실험 결과

V. 결론 및 향후 연구

본 논문에서는 무선 환경에서 모바일 기기에 적합한 원격 스토리지 시스템을 사용하기 위한 iSCSI와 보안을 적용하기 위해 사용한 IPSec을 설계, 구현하고 이에 대한 성능 실험을 하였다. 실험 결과 IPSec을 적용하지 않은 스토리지 시스템에서 보다 나은 성능을 보이는 것과 IPSec의 보안 모드 중 Transport 모드에서 더 나은 성능을 보이는 것, 그리고 iSCSI PDU 크기를 네트워크 MTU 크기와 같게 할 경우 성능이 좋다는 것을 알 수 있었다. 향후 연구로는 iSCSI를 이용한 원격 스토리지 시스템 사용시, 이동성이 갖는 모바일 환경에서의 IPSec 사용에 대한 연구와 IPSec 사용의 효율성을 위한 연구가 필요 하다.

■ 참고문헌 ■

- [1] Internet Engineering Task Force,
<http://www.ietf.org/html.charters/ips-charter.html>
- [2] Julian Sartran, iSCSI Draft 20,
<http://www.ietf.org/internet-drafts/draft-ietf-ips-iscsi-20.txt>
- [3] William D. Norcott, Iozone,
<http://www.iozone.org>