CDMA 3G 환경에서 Wireless VPN의 설계/구현 방안에 관한 연구

김정태* · 이종필** · 신승중*** · 류대현***

*목원대학교 · **(주)시큐어넥서스 · ***한세대학교,

A SUDY on the Design and Implementation of Wireless VPN in CDMA 3G Surroundings

Jung-Tae Kim · Jong-pill Lee · Seung-jung Shin · Dae-hyun Ryu

Mokwon University, Xecurenexus Co., Hansei University,

E-mail : jtkim3050@mokwon.ac.kr/dhryu@hansei.ac.kr

요 약

본 논문에서는 CDMA 3G 환경에서의 Wireless VPN에 있어서의 문제점을 분석하고 설계/구현 방안을 제시하고자 한다. Wireless VPN의 최종 목표는 Wireline VPN과의 통합을 이루어서 진정한 Mobile VPN을 구현하는 것이지만 아직까지 Mobile IP 지원에 대한 국제 표준이 완전히 정비되지 않은 상태이고 또한 Mobile VPN에 대한 기술적 검증이 이루어진 적이 없기 때문에 본 논문에서는 Wireless VPN에 초점을 맞추도록 한다.

Key words

Security, Wireless VPN, CDMA, 3G, IPsec

I. 서 론

최근들어 무선 네트웍에서 유선 VPN으로 이루어진 기업망(Wireline VPN)에 접속하도록 하는 기술들과 각종 모바일 VPN 단말기에 대한 요구가 급증하고 있다. 하지만 국내의 경우 무선 네트웍에서 전송되는 데이터의 보안에 대한 기술력이 미흡하고 무선 단말기와 유선 호스트 사이의 종단간(end-to-end) 보안이 이루어지지 않아서 기존의 Wireline VPN과의 연동에 있어서 많은 문제점을 갖고 있었다.[1,2]

본 논문에서는 CDMA 3G 환경에서의 Wireless VPN에 있어서의 요구사항과 문제점을 분석하고 설계/구현 방안을 제시하고자 한다. Wireless VPN의 최종 목표는 Wireline VPN과의 통합을 이루어서 진정한 Mobile VPN을 구현하는 것이지만 아직까지 Mobile IP 지원에 대한 국제 표준이 완전히 정비되지 않은 상태이고 또한 Mobile VPN에 대한 기술적 검증이 이루어진 적이 없기 때문에 본 논문에서는 Wireless VPN(무선 VPN)에 초점을 맞추도록 한다.

II. Wireless VPN의 기술적 요구사항과 문제점

먼저 Wireline VPN(유선 VPN) 제품에 대한 시장에서의 요구사항을 살펴보면 크게 다음과 같다.

A. 고속 암복호화 속도 요구
- 3DES 등의 연산량이 많은 고급 암호화 알고리즘 사용시 Wire Speed에 근접하는 속도를 요구함
- Gigabit 이상의 대역폭을 수용할 수 있는 장비 요구가 점차 확대됨.

B. 다수의 동시 사용자 접속 허용
- 1만명 이상의 사용자 접속을 1대의 VPN Gateway로 수용
- 터널의 안정성과 회선 속도 유지

C. 네트웍 무정지를 위한 고가용성(HA) 확보

D. 방화벽 제품과 원활한 연동 기능
- Checkpoint 등의 유명 방화벽과 안정적인 연동

E. 동일 프로토콜을 사용하는 타사제품과의 호환성 확보
- IPSec 기반의 제품간 상호연동(Interoperation) 기능 요구

F. 다양한 네트웍 접속환경 지원(LAN-to-LAN, Remote Access)

G. 다수의 무선 단말기와 현존하는 운영체제를 최대한 지원

A에서 G까지의 7가지 조건 중에서 A와 B 항목은 Wireless VPN이 반드시 갖추어야 하는 필수 조건에 해당한다. 그리고 VPN 제품 공급업체 측면에서는 C, D 항목이 매우 중요하다.

현재 Wireless VPN 제품을 준비하거나 아니면 이미 제품을 내놓은 업체들이 현실적으로 가장 어렵게 고민하는 문제는 바로 G 항목이다. 현존하는 무선 단말기의 경우, 휴대폰, PDA, 노트북, 포켓 PC, 스마트폰 등이 있고 운영체제로는Palm OS, Windows CE, Embedded Linux 등이 대표적이다. 그리고 무선 데이터 통신 기술로는 CDMA, GSM, CDPD 등이 있다. G 항목이 문제시 되는 것은 바로 이와 같이 수많은 단말기와 통신 기술, 그리고 운영체제가 난립 하기 때문에 시장을 리드할 수 있는 사실상의 표준(defacto standard)가 없다는 것이다.

특히 Palm OS(시장 점유율이 가장 높고OS의 사이즈가 작고 PIMS와 같은 기본 기능에 강하지만 멀티미디어 기능이 미흡하고 시스템 메모리가 작다)와 Windows CE(가장 쉬운 인터페이스를 갖고 있고 멀티 미디어 기능 및 통신 기능이 우수하지만 고사양 장비를 필요로 함)의 기술적 차이에서 비롯되는 많은 장단점 때문에 Wireless VPN을 설계/개발/생산/판매/서비스 하는 각종 업체들이 설계에서 서비스까지의 모든 단계에서 쉽게 '선택'을 못하는 실정이다. 유선 환경에서는 Windows 계열의 OS가 전체 시장의 90% 이상을 장악하고 있기 때문에 손쉽게 제품 개발을 할 수 있지만 무선 환경에서는 아직까지 시장을 장악하는 확실한 OS가 없기 때문에 Wireless VPN 업체는 IT 경기의 위축, PDA 시장의 활성화, Windows XP 출시, 미국 테러 사건 등 시장 진입에 앞서서 시장내외의 각종 조건에 상당히 민감하게 반응하면서 완벽한 결정을 내리는데 신중을 기하는 형편이다.

국내(대한민국) 환경에서는 기술개발 수준과 시장 상황을 고려해 볼 때 G 항목의 문제점만 해결된다면 빠른 시일내에 Wireless VPN 시장을 형성할 수 있으리라 판단한다. 그리고 G 항목의 문제점을 해결하는 가장 손쉬운 방법은 기존의 무선 통신사업자, 특히 무선과 유선 네트워크 환경을 동시에 보유한 KT 또는 SK텔레콤, 같은 기존의 통신 사업자들 및 LG텔레콤 등이 Wireless VPN 용 전용 단말기를 개발 또는 개발지원하고 그에 맞는 OS를 선정하여 개인이 아닌 일반 기업과 군, 그리고 공공기관과 금융권을 중심으로 Mobile VPN 마케팅을 펼치면서 시장을 형성시키는 것이 가장 빠르고 확실하게 G 항목의 문제점을 해결하는 방법 중의 하나이다.

III. Wireless VPN 프로토콜

VPN 기술을 구현하기 위해서 반드시 충족시켜야 하는 요구사항은 '안정성'과 '보안'이다. 그리고 VPN을 구성하는 모든 지점에 위치한 하드웨어와 소프트웨어간의 상호연동이 중요한 이슈가 된다. 이런 요구조건을 만족시키기 위해서 IETF(Internet Engineering Task Force)에서는 IPSec을 규정하게 되었고 이것은 TCP/IP로 구성된 네트웍 환경에서 안전한 통신을 가능케 해주는 핵심이 되었다.

IPSec이 기존의 보안 프로토콜에 비해서 많은 관심을 받게 된 가장 큰 이유는 Layer 3에서 동작한다는 것과 Open Standard 이면서 기밀성, 데이터 무결성과 데이터 근원지에 대한 인증 등 네트웍 보안에서 필요로 하는 각종 요소를 모두 구비하고 있기 때문이다. 이 때문에 유선 VPN에서 IPSec은 가장 많은 회사와 기술자들이 선택한 프로토콜이다. 무엇보다도 이종 기기간의 상호연동을 보장하고 인증 메커니즘, 암호 알고리즘과 보안 정책 등을 수립하는데 있어서 많은 유연성을 갖고 있는 것이 IPSec의 최대 강점이라고 할 수 있다.

IPSec을 구성하는 3대 요소는 AH(Authentication Header), ESP(Encapsulation Security Payload), IKE(Internet Key Exchange)이다. AH, ESP, IKE는 서로 유기적으로 동작하면서 네트웍 데이터를 안전하게 보호해 준다.

Wireless VPN에서도 IPSec이 국제적인 표준이라 할 수 있으나 다음과 같은 점에서 Wireline VPN과 환경상 차이가 있다.

A. Remote 접속이 데스크탑이 아닌, IP 기반으로 동작하는 휴대폰, PDA 등에 의해 이루어진다.
B. VPN용 무선 단말기에 사용되는 운영체제가 다양하다.
C. 접속 옵션이 다양하다(유선모뎀에 무선 단말기를 연결하여 접속, 전용 무선 모뎀을 이용한 접속, 무선 데이터 통신이 가능한 휴대폰 이용 등).
D. 무선 단말기의 이동시에 Cell과 Cell간의 핸드 오버가 존재한다.
E. 네트웍 통신 속도가 상대적으로 느리다.
F. 무선 단말기의 성능상 RSA 알고리즘 구현에 문제가 있다.
G. 무선 서비스 제공업체가 커버할 수 있는 지역의 제한이 있다.
H. 무선 서비스 제공업체간 로밍이 존재할 수 있다.

D, F, H 등이 Wireless VPN 제품 개발시에 가장 해결하기 힘든 문제라 할 수 있다. 그 중에서 Wireless VPN Client 소프트웨어 개발에 성공한 Certicom의 movianVPN 이란 무선 단말기용 소프트웨어의 성능 시험 결과를 보면 왜 F항목이 Wireless VPN의 구현에 있어서 걸림돌이 되는지를 잘 알 수 있다. MovianVPN은 240K의 메모리를 클라이언트 프로그램과 보안정책 DB 용으로 사용하며, 60K 메모리를 암호화 엔진용으로 사용한다. 이 제품은 빠른IKE를 위해서 163 비트 ECDH(Elliptic Curve Diffie-Hellman)알고리즘을 구현할 수 있으며768비트, 1024비트의 DH(Diffie-Hellman) 알고리즘도 구현할 수 있다. 이 제품을 16MHz의 Palm OS로 동작하는 드래곤볼 CPU에서 테스트한 결과를 보면 ECDH에 0.55초가 소요되며 DH에 39초 정도가 걸리는 것으로 성능평가 결과가 나와 있다.

이것을 보면 일반적으로 사용하는 DH알고리즘을

PDA와 같은 무선 단말기에서 사용하기 위해서는 단말기 자체의 처리 속도가 빠른 고사양 제품을 사용하거나 아니면 암호화 알고리즘을 속도가 빠른 알고리즘을 사용해야 함을 의미한다. 또한 처리 속도가 낮은 CPU를 사용하는 PDA 등에서 RSA 알고리즘을 구현하는데 문제가 있다는 것을 나타낸다. 또한 DH 알고리즘을 사용해서 키 생성 과정을 기다리는 도중에 유선 VPN 게이트웨이는 타임아웃 되어 버릴 수 있다.

무선 단말기의 느린 처리속도도 큰 문제이지만 기존의 Wireline VPN 게이트웨이들이 대부분 DH 알고리즘을 사용하기 때문에 ECDH를 사용할 경우 유선 Gateway와의 연동이 쉽지 않다는 것도 문제가 된다. 뿐만 아니라 ECDH 알고리즘의 보안에 의문을 갖는 사용자들이 상당수 존재한다는 사실이다. 하지만 실제로는 768 비트의 DH 보다는 163 비트의 ECDH가 보안과 속도 측면에서 훨씬 우수한 상태이다.

이 문제를 해결하는 방법은 크게 (1) 유선 VPN 게이트웨이가 ECDH 알고리즘을 지원하는 경우(아직까지는 현실성이 없어 보임) 또는 (2) 무선 단말기에 하드웨어 암호 가속 기능을 이용해서 DH 알고리즘을 처리하는 경우(하드웨어 개발 및 추가에 드는 비용이 상대적으로 크다.)가 있을 수 있다.

기존의 국내 CDMA 환경이라면 (2)를 구현하는데 문제가 되지만 CDMA 3G의 경우에 USIM 카드를 사용할 경우 (2)의 부담을 크게 경감할 수 있다.

IV. CDMA 1G, 2G, 2.5G 및 3G간의 Wireless VPN 구현 가능성 분석

Wireless VPN을 CDMA 3G에서 구현하기 위해서는 해결해야 할 문제점이 너무나 많이 있다. 우선 Wireless VPN이 CDMA 3G에서 구현이 가능한지 알아보기 위해서 Wireless VPN 환경이 아닌 일반 무선 인터넷 환경에 대해서 살펴보겠다.

무선 단말기로 유선 인터넷을 접속하여 데이터를 송수신하기 위해서는 단말기 내에 화면으로 표시해 주는 전용 브라우저 소프트웨어인 운영체제가 필요하며 무선단말기에서 통신속도나 화면표시등의 제약이 있으므로, 인터넷 표준 언어가 아닌 무선 단말기에 적합한 무선 인터넷 언어가 필요하다.

무선 단말기와 BTS간의 데이터 전송방식인 운영시스템에 따라 CDPD, 패킷전송, 회선전송 등으로 구분할 수 있다. 또한 무선 단말기와 유선 인터넷 접속을 위하여 상호변환을 위한 소프트웨어인 게이트웨이 프로토콜이 필요하다.

그림 1은 무선 인터넷이 구현되는 방식을 나타내고 있다. 이 그림에서 주목해야 하는 것은 Wireless 데이터가 어떤 방식으로 전송되느냐를 먼저 살펴야 한다는 것이다. 기본적으로 CDMA, TDMA, 그리고 GSM 방식은 회선 전송(Circuit-based Transmission) 방식을 사용한다. 회선 전송 방식은 사용자들에게 저속 데이터 전송속도를 제공하며 공중 인터페이스 리소스에 대한 활용성이 크게 떨어진다. 따라서 가용성이 매우 낮으며 다이얼 업(Dial-up)시에 많은 air time을 소요한다. 즉, 사용중에는 할당된 Channel을 독점하게 되므로 동일한 회선을 다른 가입자가 쓸 수 없게 되는 것이다.

이것을 극복할 수 있는 유일한 대안은 패킷 전송 방식을 사용하는 것이며 Mobile IP와 GPRS(General Packet Radio Service)는 회선 전송 방식의 문제점을 해결하기 위한 대표적인 기술들이다.

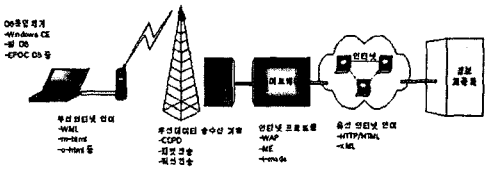

그림 3. 무선 네트워크 상에서 데이터 통신 과정

전통적인 회선전송 방식이 비효율적인 가장 큰 이유는 무선 데이터 서비스를 할 때 물리층에서 회선 가입자가 회선을 사용하던지 않던지간에 특정한 회선을 할당해 주어야 한다는 것이다. 반면에 패킷 전송 방식에서는 특정한 회선을 가입자에게 고정적으로 할당할 필요가 없다.

국내 환경에서는 기본적인 무선 네트웍이 회선 전송 방식을 택하고 있기 때문에 IS-95B 정도에서 Wireless VPN을 구현하는 것은 상당한 어려움이 있다. 데이터 전송 속도도 느리고 시스템 리소스를 제대로 활용할 수 없다는 것이 가장 큰 이유이다. 하지만 CDMA 2000 이상에서는 무선통신 사업자가 IP 기반에서 양방향 패킷 데이터 통신을 할 수 있도록 허용하고 있다. CDMA 3G에서는 각종 리소스를 보다 효율적으로 사용할 수 있는데 그 이유는 패킷 트래픽 채널이 동시접속 사용자 사이에서 공유가 가능하기 때문이다. 또한 무선통신 사업자들이 가입자들에게 보다 높은 통신속도(2Mbps)를 제공할 수 있어서 기존의 유선 ADSL 정도의 속도를 유지할 수 있는 것이 장점이다.

CDMA 3G는 Mobile VPN을 완벽하게 지원할 수 있는데 Simple IP와 Mobile IP 프로토콜을 동시에 활용할 수 있다. 가입자 측면에서 살펴보면 Simple IP와 Mobile 단말기가 MIP 프로토콜을 지원해야 한다는 것이다. 이것은 Palm OS 또는 Pocket PC에서는 기본적으로 제공이 안되는 기능이다. MIP(Mobile IP)의 표준은 IETF RFC 2002~2006 에 기술되어 있으며 RFC 2290, 2344를 포함한 기타 Draft에서 부가적인 VPN과 보안에 관련된 사항이 상세히 서술되어 있다.

향후에 CDMA 3G에서 Wireless VPN이 구현될 것은 분명하다. 하지만 Mobile IP가 가진 다음과 같은 문제점들 때문에 Wireless VPN의 완벽한 구현(완벽한 Mobile IP의 구현)에는 상당한 시일이 걸릴 것으로 예상된다.

V. Wireless VPN 구현방안

1. 하드웨어

시장이 필요로 하는 기능적 마케팅적 사항을 만족시키기 위해서는 다음과 같은 무선 단말기 하드웨어 사양이 지원되어야 할 것으로 판단된다.

가. 프로세서

1) RSA 및 ECC 등의 공개키 암호화 알고리즘 및 통신데이터 암호화를 위해 처리속도가 빠른 제품이 요구됨
2) 모바일 환경을 고려해서 전력소모가 낮아야 함
3) 전체제품의 가격 상승을 막기 위해 가격이 저렴해야 함
4) 제품의 안정성이 입증된 제품이어야 하고 공급이 원활해야 함

나. 메모리

1) VPN용 SW 및 단말기용 응용 SW 동작을 위한 충분한 메모리가 필요함
2) 전력소모가 작아야 함
3) 저가격 제품이여야 함
4) 암호화 연산속도를 높이기 위해 데이터 전송 속도가 빨라야 함

다. 전력공급

1) 충전이 용이하고 사용시간이 길어야 함
2) 다양한 동작 온도에서 배터리의 성능 저하가 가급적 없어야 함
3) 충방전 반복시 메모리 효과가 적은 제품이어야 함
4) 저렴한 가격이어야 함

2. 소프트웨어

Wireless VPN의 원활한 동작을 위해서는 다음 표와 같은 VPN Client 소프트웨어의 기능이 요구되어진다.

가. 관리

1) VPN 접속 상태 및 통신속도 확인 기능과, 각종 로그 관리 기능
2) 관제 서비스 및 원격 모니터링 기능

나. 유지보수

1) SW Online Update 기능
2) Scalability 제공

다. 운영체제

1) 국제적으로 널리 사용되는 Palm OS, Win CE, Embedded Linux 등을 지원해야 함

라. CDMA 3G 환경 지원

1) 가급적 단말기 제작 업체에서 TCP/IP 및 Mobile IP 관련된 통신 SW를 설계하는 것이 바람직
2) 필요할 경우 Mobile IP 지원 프로그램은 VPN 소프트웨어 제작 업체에서 설계하는 것이 바람직
3) QoS는 VPN 업체에서 추가 및 확장의 용이함을 고려해서 설계하는 것이 바람직

마. 유선 VPN Gateway와의 연동(Interoperation)

1) 반드시 표준규격에 맞추어 연동되어야 함
2) Major Wireline VPN Gateway와 연동 되어야 함

VI. 결 론

최근들어 무선 네트웍에서 유선 VPN으로 이루어진 기업망(Wireline VPN)에 접속하도록 하는 기술들과 각종 모바일 VPN 단말기에 대한 요구가 급증하고 있다. 하지만 국내의 경우 무선 네트웍에서 전송되는 데이터의 보안에 대한 기술력이 미흡하고 무선 단말기와 유선 호스트 사이의 종단간(end-to-end) 보안이 이루어지지 않아서 기존의 Wireline VPN과의 연동에 있어서 많은 문제점을 갖고 있다.

본 논문에서는 CDMA 3G 환경에서의 Wireless VPN에 있어서의 요구사항과 문제점을 분석하고 설계/구현 방안을 제시하였다. Wireless VPN의 최종 목표는 Wireline VPN과의 통합을 이루어서 진정한 Mobile VPN을 구현하는 것이다. 그러나 아직까지 Mobile IP 지원에 대한 국제표준이 완전히 정비되지 않은 상태이고 또한 Mobile VPN에 대한 기술적 검증이 이루어진 적이 없기 때문에 본 논문에서는 Wireless VPN에 초점을 맞추었다

참고문헌

[1] Forman, H. George and John Zahorjan. The challenges of mobile computing. In *IEEE Computer Magazine*, Vol.27, no. 4, April 1994, University of Washington.

[2] *Security principles for the Universal Mobile Telecommunications (UMTS) version 3.0.0*, ETR 050901, Special Mobile Group (SMG), July 1998.

[3] Fox, Armanda, and Steven Gribble, *Mobile Computing and Networking*: Security On the Move - Indirect Authentication Using Kerberos, University of California, Berkeley, CA, 1996, pp.155-164.

[4] *Wireless Application Protocol Architecture Specification*. WAP Forum Protocol Specification, July 2001.

[5]]http://www.wapforum.org/what/technical.htm. Accessed November 2001.

[6] WAP white paper . Closing the GAP by Algorithmic Research Ltd.

[6] http://www.arx.com/products/wapwhitep.html. Accessed November 2001