논문 2010-47IE-4-7

WiBro망에서 보안성이 확립된 기업용 Mobile-VPN 구축 방안 연구

(The Study of Building Security-Established Enterprise Mobile-VPN on WiBro Network)

조 도 현*, 강 대 석**, 한 규 정**, 지 영 하**, 한 완 옥***

(Do-hyeoun Cho, Dae-seok Kang, Kyu-jeong Han, Yung-ha Ji, and Wan-ok Han)

요 약

Mobile Internet 개념인 WiBro Data Service는 최근 무선 데이터 통신의 규모는 스마트 폰이나 WiBro 서비스 등의 보급에 힘입어 최근 빠르게 성장하고 있다. 이에 따라 무선 인터넷 분야에서 무선구간 보안성 확보 문제와 네트워크 구간의 보안성 확보 문제 강조되고 있다. 본 논문에서는 이러한 문제에 대한 해결 방안으로 기존에 구현되어 있는 기술들을 결합하여 Public 망 개념인 WiBro Network에서 기업 가입자의 보안성 확보를 위한 Mobile-VPN구축 방법을 제안하고자 한다.

Abstract

Recently, WiBro service as a mobile internet has been being extended. The market of wireless data communication has been being extended rapidly due to the increase of mobile data communication service supply such as smart-phone, WiBro service and so on. As the result, security is also emphasized in the mobile Internet. In this paper, we propose the methods that tighten up security in the upcoming Enterprise Mobile-VPN service on WiBro network.

Keywords : Mobile-VPN, WiBro, VPN, PBR, TEK

Ⅰ. 서 론

Mobile Internet인 WiBro 서비스는 데이터 통신을 위주로 하고 있으며 이제 도입초기 단계이다. 무선데이터 통신 시장은 WiBro, 스마트 폰 등의 보급으로 급격히 확장되고 있으며 이에 따른 Mobile Internet망에서의 보안의 중요성도 강조되고 있다[1].

기업용 Mobile-VPN(Virtual Private Network) 서비스는 Mobile Internet상에서 기업의 사내 망에 접근을 허가 받은 Mobile 단말이 해당 망에 접근할 때 보안적인 문제를 발생하지 않도록 해주는 서비스를 말한다[2].

WiBro망에서 기업용 Mobile-VPN을 구현하기 위해서 선행 되어야 할 것은 가입자간 통신의 보안성 확보이다. WiBro 망은 기존의 Internet 망에 직접 연결 되어 있어 서 OPEN망 성격이 강하기 때문에 망 차 원에서의 가입자 보안 문제에 대한 solution은 폐쇄망이나 다른 VPN망에 비해 취약할 수밖에 없다.

따라서 WiBro망에서 기업 자체망과 연동하는 망의 보안성 확립을 위해서는 무선구간 보안성 확보 문제, 네트워크 구간의 보안성 확보 문제 등의 해결이 중요한 과제로 대두되었다[2~3].

본 논문에서는 위 두 가지 문제에 대한 해결 방안으

* 정회원, 인하공업대학 디지털전자과
(Dept. of Digital Electronics, Inha Tech. Col.)
** 정회원, KT 무선연구소
(Wireless R&D Center, KT)
*** 정회원, 여주대학 자동차과
(Yeoju Institute of Technology)
접수일자: 2010년9월15일, 수정완료일: 2010년12월7일

로 기존에 구현되어 있는 기술들을 결합하여 WiBro 망에서 Mobile-VPN을 구축하고자 한다.

Ⅱ. 본 론

1. 무선구간의 보안성 확보 문제

무선구간 보안성 확보 문제의 경우 Broadcast 구간인 무선 단에서 가입자 통신의 기밀성(Confidentiality) 및 무결성(Integrity) 을 확보 하여야 한다.

WiBro 무선구간의 암호화 기능은 기지국(RAS : Radio Access Station)와 단말(MS) 사이의 무선구간(R1 Interface)에 대해 IEEE802.16e 및 WiMAX Forum NWG에 따라 베어러 트래픽(Bearer Traffic)에 대한 기밀성 및 무결성을 제공 한다. 또한 PKMv2(Privacy and Key Management) 기반 EAP 인증 방식에 따라서 가입자 인증 및 인증 후 베어러 트래픽을 암호화하기 위해 TEK(Traffic Encryption Key)을 분배하는 과정을 포함한다. 무선구간의 보안성을 확보하기 위해 적용 가능한 방안은 인증 프로토콜, 데이터 암호화, KEY분배가 있다[1~4].

1) 인증 프로토콜

인증 프로토콜을 구현하기 위하여 PKMv2 기반 EAP 인증방식을 사용하는데 EAP-AKA, EAP-TLS (X.509), EAP-TTLS가 있다. EAP-AKA는 USIM/UICC인증, EAP-TLS는 디바이스 인증을 지원하고 EAP-TTLS는 디바이스와 사용자 결합 형태의 인증방식을 지원한다[4].

그림 1은 WIBO Network Entry 과정 중 인증 단계를 도식화 한 것이며 아래의 인증 과정은 크게 EAP Protocol을 통한 인증 과정과 인증 과정 후 key할당 과정으로 구분된다.

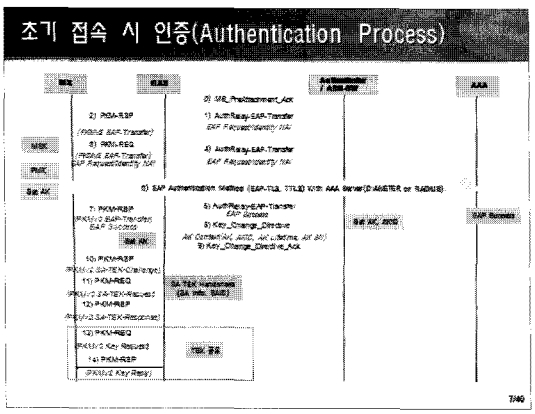

그림 1. WIBO Network Entry의 인증 단계
Fig. 1. Authentication Process in Network Entry.

2) 데이터 암호화

암호화 방식으로는 AES-CCM(128bit)방식을 사용하여 베어러 트래픽에 대한 기밀성 및 무결성을 지원한다. AES(Advanced Encryption Standard)는 암호화 프로토콜이며 AES-CCM은 AES의 한 종류로써 데이터의 비밀성 및 기밀성을 제공한다.[4~5]

그림 2는 기지국, 단말 구간에서 Bearer Traffic 암호화 기능을 ON 하였을 경우 MAC message를 Capture 하여 data의 암호화 여부를 확인한 것이다.

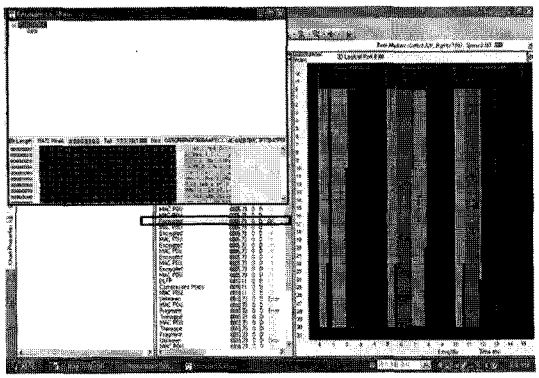

그림 2. 암호화된 Bearer Traffic
Fig. 2. Encrypted Bearer Traffic.

3) KEY 분배

단말, 기지국간 상호 인증이 완료되면, 서로 인증키를 공유하게 되며 인증키는 단말과 기지국이 공유하고 있는 비밀키로 인증키로 부터 무결성 보장을 위한 키, TEK 암호화를 위한 KEY 등 필요한 모든 키를 생성한다. 인증 이후 단말과 기지국은 SA-TEK Challenge/Request /Response 메시지를 통해 기지국이 단말의 요

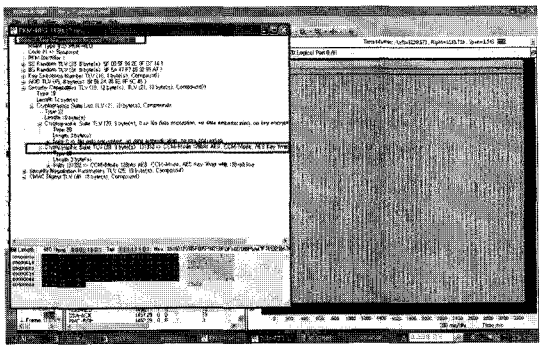

그림 3. SA-TEK Challenge(PKM-RSP)
Fig. 3. SA-TEK Challenge(PKM-RSP).

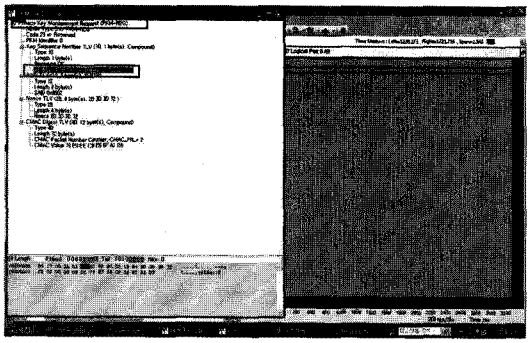

그림 4. SA-TEK Request(PKM-REQ)
Fig. 4. SA-TEK Request(PKM-REQ).

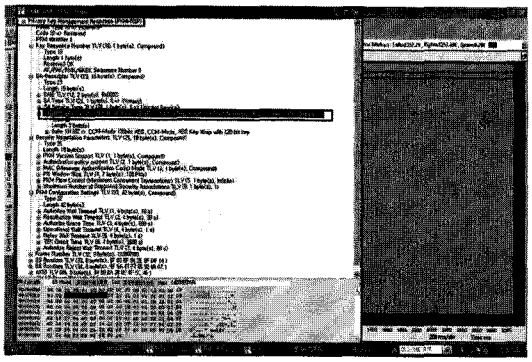

그림 5. SA-TEK Response(PKM-RSP)
Fig. 5. SA-TEK Response(PKM-RSP).

청에 따라 암호화 적용 여부를 결정한다.[4~5]

그림 3, 4, 5는 TEK 기능을 Enable 하였을 경우 SA-TEK Challenge/Request/Response 과정 및 Bearer Traffic암호화를 위한 CCM-MODE 128bit AES 암호화 방식을 확인 할 수 있다.

2. 네트워크 구간의 보안성 확보 문제

네트워크 구간의 보안성 확보 문제의 경우 유선 단에서 기업자체 망과 WiBro망 사이의 연동 시에 발생 할 수 있는 네트워크 보안 문제를 해결 하여야 한다.

네트워크 구간의 보안성을 확보하기 위해서는 인터넷 쪽의 일반 사용자들에 대해서 기업용 WiBro 단말로의 접근 경로가 원초적으로 차단되어야 하며 동일한 제어국에 수용된 일반 가입자도 해당 단말에 접근이 불가능해야 하고 그 상태에서 WiBro망과 기업 가입자 망이 연동되어야 한다.

이를 위해서는 다음 4가지 기능이 제어국에서 지원되어야 한다.

1) 제어국에서 복수의 IP Pool 운용 기능

제어국은 기업용 가입자 및 일반 가입자를 위한 복수의 IP Pool을 운용 할 수 있어야 한다. 즉, 인증•과금 서버(AAA : Authentication Athorization Account)와 연동하여 해당 기업용 가입자는 해당 IP Pool에서 ip를 할당받고 일반 가입자는 pulbic IP Pool 에서 ip를 할당받는 것이다. 또한 기업용 IP Pool은 인터넷상에서 routing이 되지 않는 private ip로 구성하여 일반 인터넷 사용자의 접근경로를 원초적으로 차단하여야 한다.[6]

2) GRE tunnel 인터페이스 기능

가입자에서 할당 된 private ip가 가입자 G/W까지 forwarding 되기 위해 제어국과 가입자 G/W간 GRE (Generic Routing Encapsulation) tunnelling 인터페이스를 구성하여 WiBro망과 가입자망 연동시킨다.[2]

그림 6과 같이 4대의 router를 구성하여 GRE기능 및 PBR기능을 검증 한다.

그림 7과 같이 2번 ROUTER와 R4 Router에 GRE 인터페이스 설정을 한다.

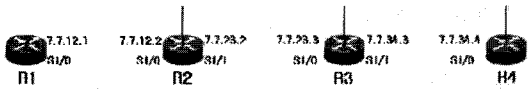

그림 6. Network 구성도
Fig. 6. Configuration map of Network.

```
R2#sh run int t0
Building configuration...

Current configuration : 104 bytes
!
interface Tunnel0
 ip unnumbered Loopback15
 tunnel source 12.2.2.2
 tunnel destination 12.3.3.3

R4#sh run int t0
Building configuration...

Current configuration : 104 bytes
!
interface Tunnel0
 ip unnumbered Loopback13
 tunnel source 12.3.3.3
 tunnel destination 12.2.2.2
```

그림 7. R2 Router와 R4 Router에 GRE 인터페이스 설정
Fig. 7. GRE Configuration in the R2 and R4 Router.

3) PBR(Policy-Based Routing) 기능

PBR 지원 기능 중 Source-Based routing 기능을 이용하여 해당 기업용 가입자에게서 발생한 트래픽을 해당 GRE 인터페이스로 forwarding하는 방식으로 private ip 기반의 기업용 가입자 트래픽을 WiBro 망에서 기업용 가입자 G/W까지의 인터넷 구간에서 양 방향으로 유통 시킨다.[6]

그림 8은 R2 Router의 Serial 1/0 Interface에 PBR

```
R2#sh run int s1/0
Building configuration...

Current configuration : 142 bytes
!
interface Serial1/0
 ip address 7.7.12.2 255.255.255.0
 ip policy route-map pbr


!
route-map pbr permit 10
 match ip address 1
 set interface Tunnel0
!
route-map pbr permit 20

access-list 1 permit 11.11.11.0 0.0.0.255 log
```

그림 8. R2 Router의 Serial 1/0 Interface에 PBR 설정
Fig. 8. PBR Configuration in the R2 Serial 1/0 Interface.

```
R1#ping
Protocol [ip]:
Target IP address: 16.1.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 11.11.11.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 16.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 11.11.11.1
!!!!!
```

그림 9. R1 Router에서 R4 router의 16.1.1.1 address 로 Ping Test
Fig. 9. Ping test from R1 to R4 16.1.1.1.

설정으로써 GRE 설정과 연동하여 설명하면 R1 Router에서 Source Ip 가 11.11.11.0/24 대역의 PACKET이 2번 Router의 Serial 1/0 interface로 들어오면 해당 packet은 GRE Interface로 Fowarding 되어 R3 Router에 11.11.11.0/24 및 Destination Ip(16.1.1.1)에 대한 Routing 정보가 없어도 해당 Packet은 Network 구간을 통과하여 서로 간에 통신이 가능하다.

그림 9는 R1 Router에서 R4 Router의 16.1.1.1 address를 가진 Interface로 Ping 보냈을 Tunnel 구간을 이용하여 R3 Router에 Routing 설정 없이 통신을 가능함을 보여준다.

4) WiBro 단말간 통신시 Next-hop 변경 기능

해당 제어국에서 가입자 단말간 통신시 해당 트래픽에 대한 Next-hop을 변경하여 해당 트래픽을 제어국 자체 내에서 처리하지 않고 상위의 장비로 Forwarding 하고 그 상위의 장비는 자체내의 routing 정보에 의해서 해당 트래픽을 다시 제어국으로 Forwarding한다.

제어국과 상위 장비 사이의 인터페이스에 ACL

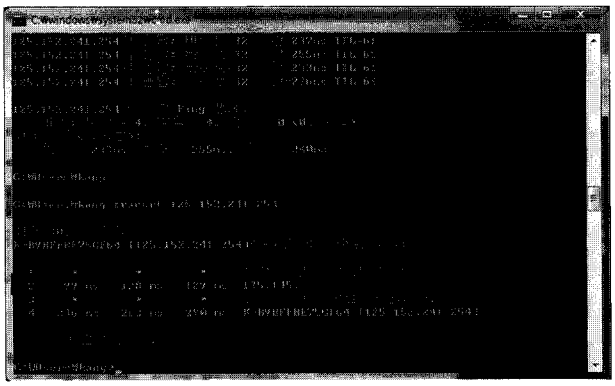

그림 10. 동일 ACR에 수용된 WiBro단말 간에 traceroute 수행
Fig. 10. Traceroute between WiBro Station and Wibro Station.

(Access Control List)을 설정 하여 Public WiBro단말에서 기업용 WiBro 가입자로 향하는 트래픽에 대해서 해당 패킷의 Source Ip를 기업 자체 망에서 사용하는 Ip로 제한 하는 패킷 filtering 정책을 설정하여 WiBro 일반 단말에서 WiBro 기업용 단말로 가는 트래픽을 차단한다.[7]

그림 10은 동일 ACR에 수용된 WiBro단말 간에 Traceroute를 수행한 결과로써 그림에서 보이는 125.145.x.x IP는 ACR 상단의 L3 Switch IP로써 단말간의 통신 시 ACR내에서 Packet Fowarding이 되지 않고 상위 장비로 Packet이 Fowarding 된 후 다시 ACR로 Forwarding 되는 것을 확인 할 수 있다.

이 기능을 이용하여 ACR, L3 Switch사이에 ACL을 설정하여 Public WiBro 단말과 기업용 WiBro단말간의 통신을 제한 할 수 있다.

III. 결론 및 향후 연구방향

WiBro망에서 기업 자체망과 연동하는 망의 보안성 확립하고, 네트워크 구간의 보안성 확보하기 이하여 WiBro 망에서 Mobile-VPN을 구축을 제안 하였다.

제안된 구축 방식에 의하여 단말과 인증•과금 서버간 EAP type 의 인증을 수행한 후 인증•과금 서버를 통해서 사용자 베어러 트래픽을 암호화하기 위한 TEK(Traffic Encryption Key)를 key분배 과정을 통해서 할당 받는다. 그후 TEK를 이용하여 AES-CCM방식으로 베어러 트래픽을 암호화 하여 무선 구간의 보안성을 유지하게 된다.

유선구간에서는 기지국과 제어국간 베어러 트래픽에

대해 GRE를 통한 Tunnel을 형성하고 제어국 단에서는 인증•과금 서버와 연동하여 해당 가입자를 위한 IP pool에서 private IP를 할당한다. 해당 IP에 대해서 PBR의 Source-Base routing 기능을 이용하여 해당 가입자의 GRE 인터페이스로 패킷을 forwarding하며 일반 WiBro 단말과 기업용 WiBro 단말과의 통신은 제어국의 next-hop 변경기능과 ACL 정책으로 차단하게 된다. 가입자 내부 네트워크 및 G/W에서는 제어국의 해당 기업용 가입자 IP pool 대역에 대해서 routing처리를 하여 기업 mobile 단말과 가입자 내부 서버 간 연동 경로를 유지하여 WiBro 기반 Mobile-VPN을 실현할 수 있다.

또한, 무선구간 및 유선구간의 보안성을 확보하기 위하여 필요한 기술 중에서 데이터 암호화, KEY 분배 및 WiBro 단말간 통신시 Next-Hop 변경 기능, 제어국에서 복수의 ip pool 운용기능은 WiBro 전문 장비에 기적용되어 있으며 GRE tunnel interface 기능, PBR기능별도의 장비를 통해 구현할 수 있다.

제시한 기술들은 망 차원에서 보안성을 확보하는 방안일 뿐이며 최종적으로 가입자를 수용하기 위해서는 Mobile 단말 에서 End to End 접속시험, 단말 효용도 시험 등에서 문제점이 발생되지 말아야 하는데 현재 WiBro 무선인터넷 서비스는 현재 서비스 초기 단계이나 무선 데이터 서비스와 같이 많은 발전 요인을 내포하고 있다.

특히 WiBro 망에서 보안성 문제의 해결을 위한 후속 연구가 진행되고 가시적인 성과를 거두는 경우에는 이동성 단말이나 무선으로 서비스하기에 어려운 지역 혹은 고가의 시설비가 들어가는 지역에 저렴한 비용으로 구축 가능하여 기업용 Solution으로 커다란 기여가 예상된다.

또한 Service Provider측면에서는 일반 고객 및 기업 고객의 Mobile Internet 수요를 동시에 수용 가능하여 서비스 활성화와 매출 증대에 크게 기여 할 수 있을 것이다.

참 고 문 헌

[1] 김경민, 변해선, 이미정, "Mobile VPN", 전자공학회지, 제33권 제8호, pp74-85, 2006.

[2] Nokia, "The Envolution of Mobile VPN and its implications for Security", White Paper, 2005.

[3] Shneyderman, *Mobile VPN: Deliering Advanced Services in Next Genertion Wireless Systems*, Wiley, pp235-248, 2002.

[4] 배성수, 최동훈, 최태규, *와이브로 기술과 시스템*, 세화출판사, 2006.

[5] 한국전자통신연구원, *암호학의 기초*, 경문사, 1999.

[6] ERIC KNIPP, *시스코 네트워크 보안*, 에이콘 출판사, 2005.

[7] 삼성전자(주), *WiBro 시스템 운용과정*, 삼성전자(주), 2006.

저 자 소 개

조 도 현(정회원)
1990년 광운대학교 전자공학과 석사 졸업.
1998년 광운대학교 제어계측 공학과 박사 졸업.
1991년 LG전자 중앙연구소 근무
1998년 삼성종합기술원 근무
현재 인하공업대학 디지털전자과 교수
<주관심분야 : 회로 및 시스템 설계>

강 대 석(정회원)
1998년 서경대학교 응용통계학과 졸업.
1999년~현재 KT 무선연구소
<주관심분야 : Network 보안>

한 규 정(정회원)
1986년 광운대학교 전자공학과 졸업.
1988년 광운대학교 전자공학과 석사 졸업.
현재 KT 무선연구소 Access망개발 2팀장
<주관심분야 : Network 보안>

지 영 하(정회원)
경북대학교 전자공학과 졸업
2008년 헬싱키대학 HSE-MBA
현재 KT 무선연구소 무선네트워크 개발담당 상무

한 완 옥(정회원)
1987년 광운대학교 전자공학과 석사 졸업.
1995년 광운대학교 전자공학과 박사 졸업.
1996~현재 여주대학 전자과, 자동차과 교수
<주관심분야 : 회로 및 시스템 설계>