NS-2를 이용한 WiBro상에서의 종단 간 보안 프로토콜의 성능평가 및 분석

(Performance Evaluation of End-to-End Security Protocols in WiBro using NS-2)

김 정 윤 [†] (Jung-Yoon Kim)
송 세 화 [††] (Sehwa Song)
김 인 환 [††] (In-Hwan Kim)
황 인 용 [†††] (In-Yong Hwang)
김 석 중 [†††] (Seok-Joong Kim)
최 형 기 [††††] (Hyoung-Kee Choi)

요 약 WLAN 및 3G의 장점을 고루 갖춘 WiBro 기술이 국제 표준으로 채택됨에 따라, 수많은 관련 연구가 진행되었다. 그러나, WiBro 표준은 종단 간 통신에 대해서는 정의하고 있지 않으며, 따라서 종단 간 보안을 제공하기 위해서는 별도의 보안 프로토콜의 적용이 필요하다. 대부분의 관련 연구들은 WiBro 표준 자체에 대한 성능 향상이나 보안 향상 등을 목적으로 진행되었지만, WiBro의 실제적인 응용에 대해서는 연구가 거의 진행되지 않았다. 우리는 WiBro를 IP 네트워크에서 활용하기 위한 방안으로, IPsec, TLS, DTLS와 같은 대표적인 종단 간 보안 프로토콜의 적용을 제안한다. 우리는 WiBro에 대한 종단 간 보안 프로토콜의 적용 가능성을 검토하고 그 성능을 검증하기 위해, NS-2를 이용하여 시뮬레이션을 수행하였다. 시뮬레이션 결과를 분석한 결과, DTLS가 TLS 및 IPsec보다 우수한 성능을 보였으며, 3가지 보안 프로토콜 모두 WiBro에 적용하기에 적합한 것으로 나타났다.

키워드 : 와이브로, 보안 프로토콜, 성능평가, 네트워크 보안

Abstract WiBro has advantages when both WLAN and 3G UMTS are adopted. Much research is being carried out in this area. However, the WiBro specification does not consider end-to-end security. Hence, another security protocol has to be adopted to support secure communication. Most previous research only focused on WiBro MAC performance improvement or security. In this paper, we adopt a security protocol such as IPsec, TLS, and DTLS, well known end-to-end security protocols, to make full use of WiBro in the IP network. Using NS-2 we simulated the adoption of end-to-end security protocol and evaluated performance and usability. Simulation shows DTLS had some performance advantages. All the protocols, TLS and IPsec are also suitable for use in WiBro.

Key words : WiBro, security protocol, performance evaluation, network security

· 이 논문은 2008년도 삼성탈레스(주)의 재원을 지원 받아 수행된 연구임

† 학생회원 : 성균관대학교 정보통신공학부
steal83@ece.skku.ac.kr
†† 비 회 원 : 성균관대학교 정보통신공학부
dreaminsh@ece.skku.ac.kr
playkih@ece.skku.ac.kr
††† 비 회 원 : 삼성탈레스 종합연구소
inyong08.hwang@samsung.com
seokjoong.kim@samsung.com
†††† 정 회 원 : 성균관대학교 정보통신공학부 교수
steal83@ece.skku.ac.kr

논문접수 : 2008년 12월 11일
심사완료 : 2009년 3월 18일

정보과학회논문지: 정보통신 제36권 제3호(2009.6)

1. 서 론

지난 몇 년간 무선인터넷의 사용량이 급증함에 따라, Wireless Local Area Network(WLAN, 802.11)[1], 3rd Generation Universal Mobile Telecommunication System(3G UMTS)[2] 등의 무선인터넷 기반 기술에 관한 다양한 연구가 진행되었다. WLAN은 고속의 인터넷 서비스를 낮은 비용으로 제공하여, 수많은 가입자들이 WLAN 기반의 무선인터넷 서비스를 이용하고 있다. 그러나, WLAN의 경우 충분한 이동성(mobility)을 지원하지 않기 때문에, 기존 연결(세션)이 끊어지는 문제가 빈번하게 발생할 수 있다. 이러한 이동성 지원 문제는, 장소에 구애 받지 않고 언제 어디서든지 인터넷 서비스를 제공하는 무선인터넷의 장점을 크게 감소시킨다. 한편, 이러한 이동성 문제를 해결하기 위한 방안으로, 3G UMTS 기반의 무선인터넷 서비스를 들 수 있다. 3G 이동통신망은 WLAN과 달리 사용자에게 충분한 이동성을 지원하여, 가입자들이 언제 어디서든지 무선인터넷 서비스를 제공받을 수 있도록 하였다. 그러나 3G의 경우 낮은 속도와 고가의 비용으로 인해 이용자의 수가 많지 않으며, 다양한 서비스를 제공하기에는 한계가 있다.

이러한 WLAN과 3G의 단점을 극복하기 위한 대안으로 WiBro[3]가 제안되었다. WiBro는 기존 WLAN과 3G의 장점을 고루 가지고 있는 차세대 무선인터넷 기술로서, WLAN에 가까운 고속의 인터넷 서비스를 제공할 뿐 아니라 높은 이동성까지 제공한다. WiBro 표준명세서(specification)에는 PHY 계층과 MAC 계층에 대한 구체적인 구성 및 동작원리가 정의되어 있다.

위에서도 설명했듯이, WiBro는 PHY 및 MAC 계층에 대한 표준이기 때문에, MAC 계층보다 상위에 존재하는 계층에 대해서는 별도의 기술이나 표준을 적용해야 하며, 이는 보안 기술에도 해당되는 사항이다. 즉, WiBro 표준만으로는 IP 네트워크(인터넷)에서의 종단간(end-to-end) 보안을 제공할 수 없다. 그러나, 안전한 인터넷 서비스를 제공하기 위해서는 종단 간 보안이 필수적이며, 종단 간 보안을 제공하기 위한 대표적인 표준으로는 IPsec[4], TLS[5], DTLS[6]가 있다. IPsec은 네트워크 계층과 전송 계층 사이, 그리고 TLS/DTLS는 전송 계층의 상위에서 동작하며, 이들은 송수신 메시지의 기밀성 및 무결성 등을 제공한다. IPsec과 TLS, DTLS의 보안성은 널리 알려졌으나, 성능 측면에서 그것이 무선 단말에 적합한지에 대한 검증은 충분히 이루어지지 않았다. 특히, WiBro 환경에서 IPsec과 TLS, DTLS의 적합성 분석에 관한 연구는 거의 진행되지 않은 실정이다.

우리는 NS-2(Network Simulator 2)[7] 기반의 시뮬레이션을 통해, IPsec과 TLS, DTLS가 WiBro의 성능에 미치는 영향을 분석하였다. 우리가 사용한 NS-2용 WiBro 모듈은 NIST에서 제공하는 802.16e 모듈[8]이며, 해당 모듈에서 사용되는 사용자 변수를 WiBro에 맞게 일부 수정하였다. 802.16e[9]는 Mobile WiMAX라고 불리는 IEEE 표준으로서, WiBro와 동일한 기술로 알려져 있다. 한편, 우리는 NS-2용 IPsec 및 TLS, DTLS 모듈을 직접 구현하였다. 그리고 NS-2용 WiBro 모듈에 IPsec과 TLS, DTLS를 각각 적용한 결과를 비교하고 분석하였다. 우리의 분석 결과에 따르면, WiBro에서 가장 우수한 성능을 나타내는 종단 간 보안 프로토콜은 DTLS이며, TLS 및 IPsec도 충분히 활용 가능한 것으로 나타났다.

이 논문의 이후 구성은 다음과 같다: 2장에서는 관련 연구를 설명한다. 3장에서는 종단 간 보안의 필요성과 종단 간 보안 프로토콜에 대해 설명한다. 4장에서는 WiBro에 IPsec, TLS, DTLS를 적용한 시뮬레이션의 수행 결과를 분석한다. 5장에서는 결론을 제시하고, 향후 연구에 대해 설명한다.

2. 관련 연구

본 논문은 WiBro에서의 종단 간 보안 메커니즘의 성능을 비교하고 있다. 우리는 종단 간 보안 메커니즘으로 IPsec과 TLS, DTLS를 사용하였으며, 이에 따른 네트워크의 성능 변화를 분석하였다. 반면, WiBro와 관련된 대부분의 연구들은 WiBro의 보안 강화 혹은 WiBro 보안의 효율성 향상에 초점을 맞추고 있다.

Sung Ya-Chin[10] 등은 3G와 WLAN이 통합된 시스템에서 IPsec으로 보호된 Voice over IP(VoIP)의 성능을 분석하였다. 해당 시스템에서 IPsec은 단말과 게이트웨이 사이에 송수신되는 패킷들을 보호한다. 한편, 저자들은 VoIP 사용 시 IPsec 에 의해 추가되는 오버헤드를 측정하고, 이러한 오버헤드는 VoIP 통신에 심각한 영향을 미치지 않는다는 결론을 내렸다.

Junbeom Hur[11] 등은 현재 802.16e 표준에 정의된 3가지 핸드오버 기법의 취약점을 분석하고, 안전한 핸드오버 기법을 제안하였다. 3가지 핸드오버 기법 모두 Base Station(BS) 간 핸드오버가 발생하면 기존 BS에서 사용되던 키를 현재 BS로 전달하게 되고, 현재 BS는 이를 사용하게 된다. 따라서 임의의 BS에서 공격자에 의해 키가 탈취된다면, 이후 모든 통신은 공격자에게 노출되는 문제가 발생한다. 이러한 전방향 안전성 문제를 해결하고 단말과 BS 간 비밀키의 재사용을 막기 위해, 저자들은 핸드오버 시 보안 협상(Security Association)을 다시 설정하는 방법을 제안하였다.

HUng-Min Sun[12] 등은 서로 다른 엑세스 서비스

네트워크(Access Service Network) 사이에서의 효율적이고 안전한 핸드오버 기법에 대하여 연구를 진행하였다. 보안을 유지하기 위해서는 핸드오버 시 재인증 과정이 반드시 수행되어야 한다. 그러나 재인증 과정을 수행하는 경우, 추가적인 지연 및 단말의 전원 소모가 발생하게 된다. 저자들은 이러한 비효율성을 제거하기 위해, 사전 인증(pre-authentication) 기법을 사용한다. 사전 인증 기법을 사용하는 경우, 핸드오버 시 인증을 위해 필요한 정보들이 사전에 전달되기 때문에, 재인증의 일부 과정이 필요하지 않게 되며, 핸드오버 시 지연 시간이 감소하게 된다. 또한, 저자들은 사전 인증 기법에 PKI구조를 접목시켜, 위장 공격(impersonation attack) 및 중간자 공격(man-in-the-middle attack)을 차단하고, 유연성 있는 보안 기능을 제공할 수 있게 하였다.

Sun-Hwa Lim[13] 등은 WiBro상에서 다양한 멀티미디어 서비스를 제공하기 위해, 연구 중인 WiBro-Evo 시스템에서의 효율적인 IP Multimedia Sub-system(IMS) [14] 인증 기법에 대해서 연구하였다. WiBro네트워크 상에서 여러 가지 실시간 멀티미디어 서비스를 제공하기 위해서는, WiBro 네트워크와 IMS 네트워크 간의 상호작용이 필요하다. 그러나, 기존 IMS에서 사용되던 인증 방법을 WiBro-EVO에서 사용하는 경우 막대한 오버헤드가 발생하게 되고, 따라서 IMS 인증 과정의 수정이 불가피하다. 저자들은 EAP-AKA[15]를 기본 인증 방식으로 설정하고, EAP-AKA의 인증 과정에서 마스터 세션 키(master session key)를 생성하여 이를 IMS 네트워크에 전달하여 IMS 인증을 진행하는 방법을 제안하였다.

AbdelNasir Alshamsi[16] 등은 IPsec과 Secure Socket Layer(SSL)[17]의 특징 및 기능을 비교하였다. 저자들에 따르면 IPsec과 SSL은 각각의 장단점이 존재하며, 프로토콜의 선택은 사용되는 서비스의 특징에 의존한다. 만약 통신을 수행하는 두 개체가 모두 SSL을 사용할 수 있고, 특수한 목적의 서비스를 사용할 경우, IPsec보다는 SSL을 선택하는 것이 더욱 적합할 수 있다. 반면, 다양한 서비스를 사용하거나, 게이트웨이를 통한 보안 통신(gateway-to-gateway communication)이 필요한 상황이면 IPsec이 더욱 적합하다. 저자들은 SSL의 HMAC길이가 더욱 길기 때문에, 메시지의 무결성 측면에서 SSL이 IPsec보다 더 안전하고, 방화벽에 대해서도 SSL이 더욱 뛰어난 호환성을 제공한다고 주장한다. 그러나 이는 이론적인 결론이며, 실제로는 IPsec과 SSL이 적용된 망의 특성에 따라 보안성 및 성능이 달라질 수 있다.

3. 종단 간 보안 프로토콜

WiBro 표준은 PHY 계층 및 MAC 계층의 구조와 동작에 대해 정의하고 있다. 그러나, 종단 간 통신은 MAC 계층의 상위 계층에서 정의되어야 하기 때문에, WiBro 표준으로는 종단 간 보안을 제공할 수 없다.

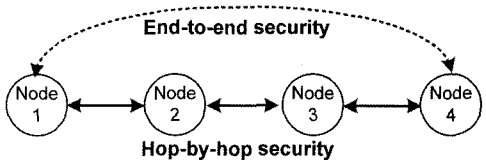

그림 1 종단 간 보안 및 홉 간 보안의 동작 구조

종단 간 보안이란, 통신을 하는 두 개체 사이에 존재하는 노드의 숫자나 종류와 상관없이, 통신 주체들이 공유하고 있는 비밀키를 이용하여 통신 보안을 제공하는 방식이다. 반면, 홉 간(hop-by-hop) 보안은 통신을 하는 두 개체 사이에 존재하는 중간노드마다 다른 암/복호화 알고리즘 또는 다른 비밀키를 사용하여, 매 구간마다 서로 다른 암호문을 전송하는 방식이다. 그림 1은 종단 간 보안 및 홉 간 보안의 동작 구조를 나타낸다.

종단 간 보안 방식은 홉 간 보안 방식과 비교하여 많은 장점을 가지고 있으며, 따라서 효율적인 통신 보안을 제공하기 위해서는 종단 간 보안을 적용하는 것이 필수적이다. 그림 2와 그림 3은 두 가지 보안 방식의 성능을 비교한 결과를 나타낸다.

그림 2를 보면, 홉의 개수가 증가함에 따라, 홉 간 보안에 소요되는 시간 (delay)이 종단 간 보안에 소요되는 시간보다 크게 증가하는 것을 알 수 있다.

그림 3은 종단 간 보안 및 홉 간 보안에 의해 추가적으로 발생하는 에너지 소모량을 나타낸다. 우리는 전체적인 에너지 소모량을 계산하기 위해 암호화, 복호화, 메시지 무결성을 위한 알고리즘의 수행에 소요되는 에너지 소모량을 구하였다[18]. 홉 간 보안의 경우, 홉이 증가할수록 네트워크에서 수행해야 하는 암호화/복호화의 횟수가 증가하기 때문에, 결과적으로 에너지의 소모

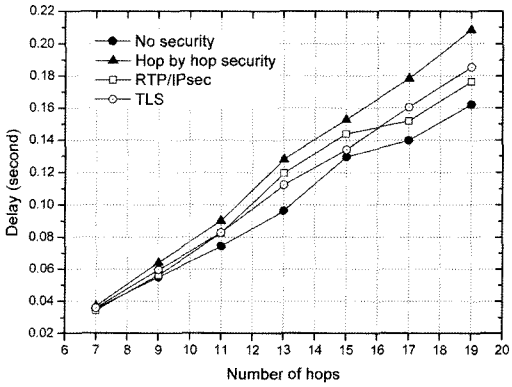

그림 2 종단 간 보안과 홉 간 보안의 전송 시간 비교

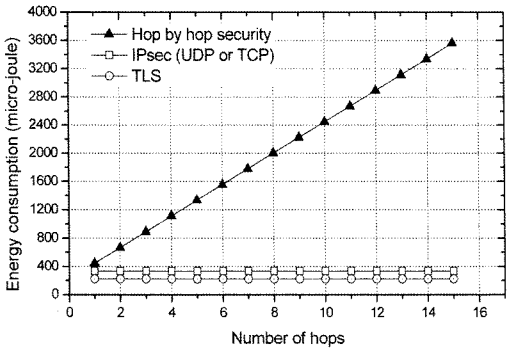

그림 3 종단 간 보안과 홉 간 보안의 에너지 소모량 비교

량도 홉의 개수와 함께 증가하게 된다. 종단 간 보안의 경우, 홉의 개수와 무관하게 에너지 소모량이 일정함을 알 수 있다.

한편, 대표적인 종단 간 보안 프로토콜에는 IPsec, TLS, DTLS가 있다. 우리는 NS-2용 IPsec, TLS, DTLS 모듈을 구현하기 위해, 각 보안 프로토콜의 표준에 제시되어 있는 초기 보안 설립 과정과 동일하게 NS-2 상에서 메시지를 송수신하도록 하였다. 또한, 암호화, 해쉬 등의 연산에 소요되는 시간은, 펜티엄3 800MHz 환경에서 1,000번 수행하여 얻은 평균(average) 값과 표준편차(standard deviation)를 측정한 결과에 대해, 가우시안 랜덤 분포(gaussian random distribution)를 적용하여 정해진 범위 내에서 랜덤성을 유지하도록 하였다. NS-2의 응용(application)에서 데이터를 전송하면, 이를 수신한 암호 모듈은 해당 세션의 보안 협상이 이루어졌는지 확인한 후, 만약 보안 협상이 이루어지지 않았다면 협상 과정(handshake)을 수행하여 보안 협상을 진행하도록 구현하였다. 만약 보안 협상이 이루어진 이후라면, 데이터의 암호화 및 무결성 제공에 소요되는 지연 시간과 메시지 헤더가 추가되도록 하였다.

3.1 IPsec(Internet Protocol Security)

IPsec[4]은 네트워크 계층에서의 대표적인 종단 간 보안 메커니즘이다. IPsec은 암호화, 인증, 무결성 보장, 재전송 방지 등의 메커니즘을 포함한다. IPsec은 네트워크 계층에서 동작하기 때문에 UDP, TCP 등과 같은 전송 계층 프로토콜에 관계없이 적용이 가능하다. 이러한 점에서 IPsec이 TLS에 비하여 더 범용적이라 할 수 있다. 한편, IPsec은 다양한 암호화 및 전송 방식을 지원한다. IPsec의 보안 방식에는, 무결성 만을 보장하는 Authentication Header(AH)와, 데이터의 암호화를 지원하는 Encapsulating Security Payload(ESP)가 존재한다. IPsec의 전송 방식에는, IPsec의 게이트웨이를 통해 메시지를 보호하는 tunnel mode와, 단말이 직접 메시지 보호를 처리하는 transport mode가 존재한다. AH, ESP, tunnel mode, transport mode에 대한 구체적인 설명은 IPsec 표준문서[4]를 참고할 수 있다. 본 논문에서는 ESP와 transport mode가 적용된 상황에 대하여 분석하였다.

3.2 TLS(Transport Layer Security)

TLS[5]는 HTTP를 비롯한 각종 응용에 대한 암호화를 지원하는 전송 계층의 보안 프로토콜이다. TLS는 record protocol, handshake protocol과 같은 sub-protocol로 구성되어 있다. 한편, TLS는 handshake protocol를 통하여 인증, 암호화 방식, 무결성 제공 방식 등을 협상하고, record protocol을 통하여 대칭 키 기반의 암호화를 제공한다. TLS는 TCP나 SCTP와 같이 신뢰할 수 있는 전송 계층 프로토콜의 상위에서 동작한다.

3.3 DTLS(Datagram Transport Layer Security)

DTLS[6]는 UDP와 같이 신뢰성 없는 전송 프로토콜의 상위에서 종단 간 인증 보안을 지원하기 위하여 제안되었다. 즉, TLS가 TCP 및 SCTP의 상위에서 동작하는 반면, DTLS는 RTP 및 UDP의 상위에서 동작한다. 따라서 DTLS는 순서화 되지 않은 메시지를 수용하며, 재전송을 고려하지 않는다. DTLS는 연결 협상 과정과 재전송 부분을 제외하면 TLS와 그 목적 및 동작이 동일하다.

4. 시뮬레이션 결과 분석

우리는 WiBro 환경을 시뮬레이션 하기 위해, 그림 4와 같은 네트워크 구조를 가정하였다. 즉, WiBro의 무선 노드인 Personal Subscriber Station(PSS)이 네트워크의 양쪽 끝에 존재하며, 각각의 무선 노드는 Radio Access Station(RAS) 및 Access Control Router(ACR)에 연결되어 있다. 그리고 각각의 RAS 및 ACR은 다수개의 유선 노드를 통해 연결되어 있으며, 유선 노드에는 background traffic을 생성하기 위한 또 다른 유선 노드가 연결되어 있다.

그림 5(a)는 NS-2용 WiBro 모듈을 사용할 경우 종

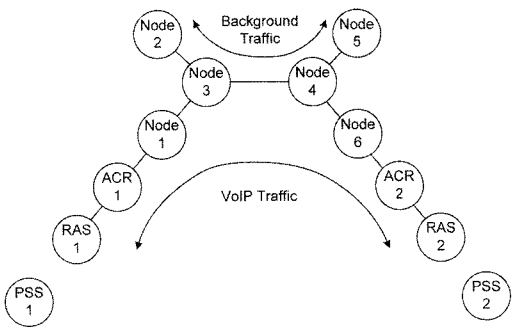

그림 4 시뮬레이션에서 가정한 네트워크 구조

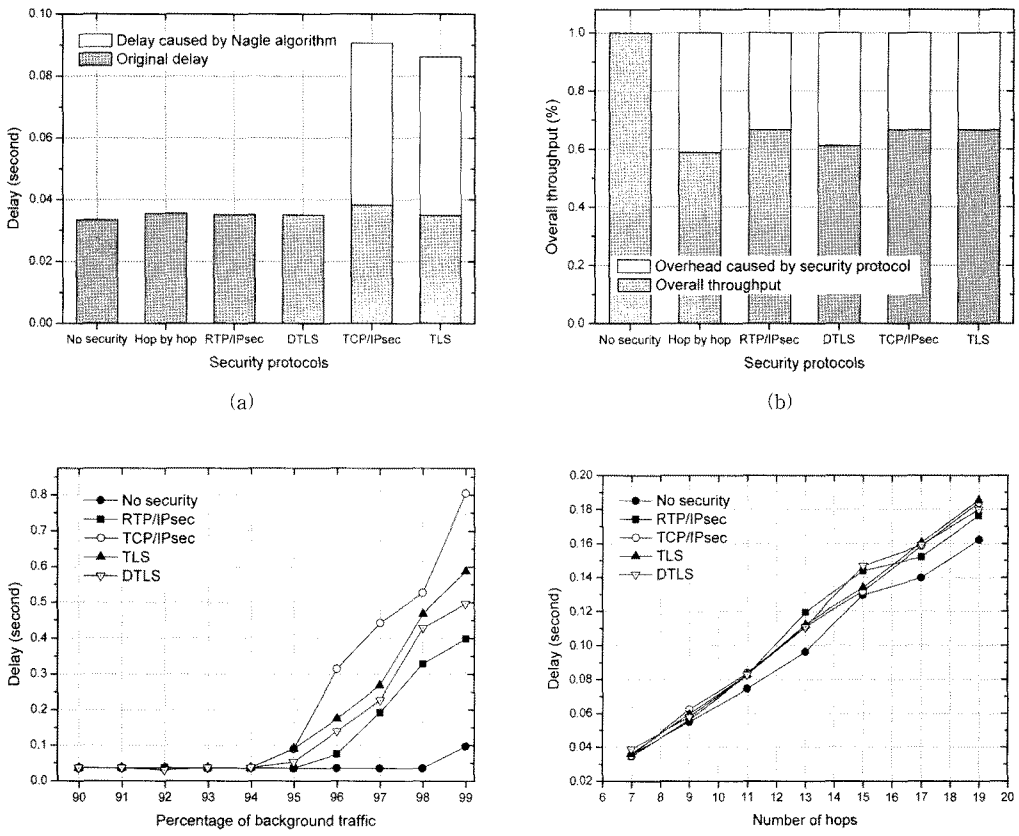

그림 5 WiBro 환경에서의 시뮬레이션 결과. (a) 전체 지연시간, (b) 보안 프로토콜이 차지하는 통신 오버헤드의 비율, (c) 전체 트래픽 중 background traffic의 비율에 따른 지연시간, (d) 홉 수에 따른 지연시간

단 간 통신에 소요되는 시간(delay)과, WiBro 모듈에 보안 프로토콜을 적용한 경우 종단 간 통신에 소요되는 시간을 비교한 그래프이다. 전체적으로 34~35 ms 정도의 시간이 소요되며, 이는 VoIP를 사용하는데 무리가 없는 수준의 지연시간이다. 한편, 보안 모듈을 탑재하였을 때 보안에 의해 추가되는 오버헤드는 약 2~4 ms이다. 이러한 오버헤드의 차이는 암호화 및 무결성 처리에서 발생하는 연산 지연시간과, 보안 프로토콜이 갖는 추가적인 헤더에 따른 통신 지연시간에 의해서 발생한다. 그림 5(a)에서 특징적인 것은 TCP에서 네이글 알고리즘(nagle algorithm)의 동작 유무(on/off)에 따라 지연시간이 크게 변화한다는 점이다. Nagle algorithm을 적용한 TCP/IPsec 및 TLS는 그림 5(a)에서 볼 수 있듯이 지연시간이 100ms에 근접하게 증가한다.

한편, VoIP의 경우 20바이트 정도의 작은 데이터가 지속적으로 발생하여 전송된다. Nagle algorithm을 사용하면 이 데이터를 즉시 보내지 않고 버퍼에 저장하기 때문에, 버퍼 대기 시간에 의해 전송 지연시간이 크게 증가하는 것이다.

그림 5(b) 그래프는, 전체 전송률(throughput) 중에서 보안에 소요되는 오버헤드를 비율로 나타낸 것이다. 평균적으로 보안에 소요되는 오버헤드는 전체 패킷의 30~40%를 차지한다. 그 이유는, VoIP패킷의 크기와 비교하였을 때 보안 프로토콜의 헤더가 상당한 비중을 차지하기 때문이다. TLS나 DTLS에 비해 비교적 헤더의 크기가 작은 IPsec은, 보안에 소요되는 오버헤드가 상대적으로 작다.

그림 5(c)는 background traffic을 대역폭의 90~99%까지 부여하였을 때, 각 보안 모듈이 WiBro의 종단 간 통신에 어떠한 영향을 미치는지 나타낸다. Background traffic이 100%에 가까워질수록, 각 보안 모듈을 적용한 종단 간 통신의 지연시간이 큰 폭으로 상승하는 것을 볼 수 있다. 특히 TCP/IPsec과 TLS의 경우 다른 모듈보다 더 빨리 지연시간이 증가하는 것을 확인할 수 있

다. 이는 TCP가 안정적인 종단 간 통신을 위해 혼잡 제어(congestion control) 및 패킷 재전송(packet retransmission) 기능을 제공하기 때문이다. TCP의 이러한 기능들은 안정적인 통신을 보장하는 대신, 전송 시간을 지연시키는 결과를 유발한다. 반면, VoIP와 같은 실시간 응용을 위해 설계된 Real-time Transport Protocol(RTP)의 경우, 기본적으로 TCP와 같은 안정적인 통신을 위한 기능을 제공하지 않기 때문에, TCP에 비해 전송 시간을 지연시키지 않는다.

그림 5(d)는 통신을 수행하는 개체들 사이에 존재하는 홉 수에 따른 전송 지연시간의 변화를 보여준다. 홉 수가 증가하면, 각 노드 별 전송 지연시간 및 큐잉(queueing) 지연시간이 발생하여, 전체적인 지연시간이 점차 증가하게 된다. 비록, 종단 간 보안을 적용한 경우의 통신 지연시간이 그렇지 않은 경우의 통신 지연시간보다 크지만, 두 경우의 지연시간은 홉 수가 19개일 때에도 기껏해야 3ms 밖에 차이가 나지 않는다. 그리고 홉 수가 7개 이하일 때에는 두 경우의 지연시간의 차이가 거의 없다. 따라서, 종단 간 보안을 적용한 경우의 통신과 그렇지 않은 경우의 통신은 대부분의 상황에서 거의 동일한 성능을 나타낸다.

5. 결 론

우리는 WiBro에서 사용할 수 있는 종단 간 보안 기술로서 IPsec, TLS, DTLS를 제시하였다. 이들 기술은 현재 인터넷에서 널리 활용되고 있는 대표적인 종단 간 보안 표준이다. 이들 프로토콜은 안전성 측면에서 매우 우수하지만, 성능 측면에서는 충분히 검증되지 않았다. 특히, 무선 단말과 같이 제한적인 연산 자원, 통신 자원, 배터리 자원을 보유한 환경에서는 성능 문제로 인해 IPsec, TLS, DTLS의 적용이 가능한지 검증할 필요가 있다. 또한, WiBro에서 사용되는 응용 서비스의 종류에 따라, 보안이 적용된 WiBro에 요구되는 최소 지연 시간(delay)이나 전송률(throughput) 등이 다르기 때문에, 서비스 제공자가 적절한 보안 기법을 선택하기 위해서는 WiBro에 IPsec, TLS, DTLS 등의 보안을 적용하였을 때 소요되는 각각의 지연 시간과 전송률을 시뮬레이션하고 분석할 필요가 있다.

우리는 NS-2를 이용하여 WiBro 환경에서 IPsec, TLS, DTLS를 적용했을 때의 성능을 검증함으로써, 이들 보안 프로토콜이 WiBro에서 얼마나 실용적인가를 분석하였다. NS-2용 WiBro 모듈은 NIST에서 제공한 802.16e 모듈을 수정하여 사용하였으며, NS-2용 IPsec, TLS, DTLS 모듈은 직접 구현하였다. 검증 결과, IPsec, TLS, DTLS 중 DTLS가 가장 우수한 성능을 나타냈으며, 위 3가지 보안 프로토콜 모두 WiBro 네트워크에 적용할 수 있는 것으로 나타났다.

본 연구는 WiBro 단말이 VoIP를 사용하는 경우에 대해 그 성능을 시뮬레이션하고 분석한 결과를 제시한다. 향후에는 VoIP 뿐 아니라, HTTP, FTP 등의 데이터, 그리고 동영상 등의 응용을 사용하는 경우에 대해서도 보안 프로토콜의 실용성 여부를 검증하고 연구해야 할 것이다. 뿐만 아니라, 향후에는 WiBro 이외의 다른 PHY/MAC 계층 프로토콜에 IPsec, TLS, DTLS를 적용한 결과를 시뮬레이션하고 분석함으로써, 보안이 적용된 WiBro의 성능을 보다 정확하고 객관적으로 평가할 수 있을 것이다.

참 고 문 헌

[1] IEEE 802.11-2007, "IEEE standard for Information technology - Telecommunications and information exchange between systems-Local and metropolitan area networks - Specific requirements Part 11 : Wireless LAN Meidum Access Control (MAC) and Physical Layer (PHY) Specifications," June 2007.

[2] 3GPP; Technical Specification Group Services and System Aspects, "UMTS Access Stratum Services and Functions, version 7.0.0, release 7," June 2007.

[3] Telecommunications Technology Association (TTA), "TTA Standard for Wireless Broadband (WiBro) Portable Internet: Specifications for 2.3 GHz band Portable Internet - PHY and MAC layers," 2004.

[4] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, November 1998.

[5] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246, August 2008.

[6] E. Rescorla and N. Modadugu, "Datagram transport layer security," RFC 4347, April 2006.

[7] The Network Simulator - NS-2, available at http://www.isi.edu/nsnam/ns/

[8] NIST, "IEEE 802.16 ns-2 code," available at http://www.antd.nist.gov/seamlessandsecure/doc.html

[9] IEEE 802.16e/D5-2004, "Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems - Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands," November 2004.

[10] S. Ya-Chin and L. Yi-Bing, "IPsec-Based VoIP Performance in WLAN Environments," IEEE Internet Computing, Vol.12, No.6, pp. 77-82, 2008.

[11] H. Junbeom, S. Hyeongseop, K. Pyung, Y. Hyunsoo, and S. Nah-Oak, "Security Considerations for Handover Schemes in Mobile WiMAX Networks," WCNC 2008, pp. 2531-2536.

[12] S. Hung-Min, L. Yue-Hsun, C. Shuai-Min, and S. Yi-Chung, "Secure and fast handover scheme based on pre-authentication method for 802.16/WiMAX infrastructure networks," TENCON 2007, pp. 1-4.
[13] Sun-Hwa Lim and Sang-ho Lee, "Efficient IMS Authentication Architecture based on Initial Access Authentication in WiBro-Evolution (WiBro-EVO) System," VTC 2007, pp. 904-908.
[14] 3GPP, 3rd generation partnership project; Technical specification group services and systems aspects, "IP Multimedia subsystem stage 2, Tech. Spec. 3G TS 23.228 version 6.2.0 (2003-06)," 2003.
[15] J. Arkko and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," RFC 4187, January 2006.
[16] A. Alshamsi and T. Saito, "A technical comparison of IPSec and SSL," AINA 2005, pp. 395-398.
[17] Alan O. Freier, Philip Karlton, and Paul C. Kocher, "The SSL Protocol Version 3.0," available at http://wp.netscape.com/eng/ssl3/ssl-toc.html
[18] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols," IEEE Transactions on Mobile Computing, Vol.5, No.2, pp. 128-143, 2006.

김 정 윤
2004년~2005년 안철수연구소 인턴. 2006년 성균관대학교 컴퓨터공학전공 학사 2008년 성균관대학교 전자전기컴퓨터공학과 석사. 2009년 현재 성균관대학교 휴대폰학과 박사과정. 관심분야는 차량 간 통신 보안, Pay-TV 보안, 무선통신망 보안

송 세 화
2008년 성균관대학교 정보통신공학과 학사. 2009년 현재 성균관대학교 전자전기컴퓨터공학과 석사. 관심분야는 Mobile IPv6, 무선 네트워크 보안

김 인 환
2008년 2월 성균관대학교 컴퓨터공학전공 학사. 2008년 3월~2009년 현재 성균관대학교 전자전기컴퓨터공학과 석사과정. 관심분야는 암호 프로토콜, VANET, 키 교환, 프라이버시 보호

황 인 용
1999년 경희대학교 공학사. 2001년 한국과학기술원 공학석사. 2008년 한국과학기술원 공학박사. 2008년~현재 삼성탈레스(주) 전문연구원. 관심분야는 통신시스템, 군통신망, NGN, QoS

김 석 중
1992년 성균관대학교 전자공학과 학사 2005년 성균관대학교 전자전기공학과 석사. 1992년~1999년 삼성전자(주) 선임연구원. 2000년~현재 삼성탈레스(주) 수석연구원. 관심분야는 통신시스템, 신호처리, 국방정보 및 제어, 위성항법시스템, 군사전자

최 형 기
정보과학회논문지 : 정보통신
제 36 권 제 3 호 참조