무선랜에서의 VPN 에이전트에 관한 연구

김신규° 김효진 송주석
연세대학교 컴퓨터산업공학부
{skkim°, hyojin, jssong}@emerald.yonsei.ac.kr

Study of VPN Agent in Wireless LAN

SinKyu Kim° HyoJin Kim JooSeok Song
Dept. of Computer Science, Yonsei University

요 약

이동성과 보안성을 동시에 갖추기 위해, 무선 통신을 이용한 VPN 기술의 사용이 증가하고 있지만 효율적인 이동성을 지원하는 모바일 기기의 특성상 연산 능력이 많이 부족하다. 이에 따라 무선랜을 통해 VPN 기술을 사용할 경우 단말기가 무선랜을 위한 암호화/복호화와 VPN 접속을 위한 암호화/복호화를 동시에 수행하는 데에는 많은 무리가 따르게 된다. 이러한 문제를 해결할 수 있는 방안으로, 본 논문에서는 무선랜 환경에서 단말기와 직접 통신을 하는 AP에 VPN 에이전트를 설치하여 무선 단말기가 필요로 하는 VPN 접속을 대행해 주는 방법을 제시한다.

1. 서 론

근래에 무선 랜(Wireless Lan)이 발달함에 따라 유선의 한계를 뛰어 넘어 자유로운 네트워크 접속이 가능하게 되었다. 이에 따라 언제 어디서든 컴퓨터를 사용할 수 있는 전방위 컴퓨팅(Ubiquitous Computing)이 점점 현실화되어가고 있지만, 무선이라는 매체의 특성상 기밀성(confidentiality)이 완벽히 보장되지 않는 한계를 지니고 있다.

무선에서의 이러한 보안상의 취약점을 보완하기 위해, 현재 무선 랜에서는 WEP(Wired Equivalent Privacy)이라는 보안 프로토콜을 사용하고 있다. 하지만, WEP은 여러 취약점을 가지고 있음이 밝혀져서, 이러한 취약점을 해결하기 위해 강력한 암호 알고리즘인 AES(Advanced Encryption Standard)를 사용하는 새로운 보안 프로토콜이 IEEE 802.11i Task Group에서 표준화 작업을 통해 정립되고 있는 중이다[1]. 하지만 대개 강력한 알고리즘은 강력한 보안성을 제공하지만 좀더 복잡한 계산을 필요로 한다는 한계를 가지고 있다.

한편, 보안 프로토콜과 더불어 VPN(Virtual Private Network)의 필요성도 점점 높아지고 있다.
교통, 통신의 발달로 한 도시의 산업이 단지 그 도시뿐만 아니라 다른 도시, 더 나아가 세계 각국들과 연관되게 되었고 기존의 문서를 통한 업무를 디지털화하면서 각 지사 간, 기업 간, 직원간의 통신이 많아졌다. 그러므로, 원격지에서 기업 본사의 사설망에 접근해야 할 경우가 많아지게 되었다. 하지만, 일반적으로 사설망은 구축 비용이 많이 들기 때문에, 인터넷과 같은 공중망을 이용하여 마치 사용자가 한 회사의 사설망을 사용하는 것처럼 해주는 VPN 기술이 많이 사용되고 있다[2].

이렇게 현재 요구되는 기능을 휴대성을 갖춘 이동 단말기에 탑재하기 위해서는 고성능의 계산능력이 필요하다. 하지만 효율적인 이동성을 지원하는 모바일 기기의 특성상 계산 능력이 많이 부족하기 때문에 무선랜을 통해 VPN 접속을 할 경우 무선랜을 위한 암호화/복호화와 VPN 접속을 위한 암호화/복호화를 동시에 하는 데에는 많은 무리가 따르게 된다.

이에 대한 대안으로 본 논문에서는 무선랜에서 단말기와 직접 통신을 하는 AP(Access Point)에 VPN 에이전트를 설치하여 무선 단말기가 필요로 하는 VPN 접속을 대행해 주는 방법을 제시한다. 이러한 경우 단말기에서는 VPN 서버와의 접속을 위한 암호화/복호화를 수행하지 않아도 되므로 많은 계산을 줄일 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 무선 랜에서 단말기와 AP 그리고 VPN 서버간에 일어나는 VPN 사용 방법들의 문제점에 대해 살펴본다. 3장에서는 우리가 제안하는 방법을 소개하고 4장에서는 시뮬레이션을 통한 기존 방법과의 비교 분석을 해보며, 5장에서 결론을 맺는다.

2. 기존 무선환경에서의 VPN 사용방법의 문제점

무선 환경에서 단말기와 AP간, 그리고 단말기와 VPN 서버가 통신하기 위해서는 단말기가 두 번의 복잡한 연산을 수행해야만 하는 오버헤드가 발생한다. 하지만 단말기는 보통 노트북이나 PDA, 휴대폰과 같이 이동성을 갖기 때문에 이런 복잡한 연산을 수행하기에는 그 연산 능력이 많이 떨어지는 한계를 갖는다.

이러한 기존 방법의 한계점을 보완하기 위해서 이 논문에서는 AP에 VPN 에이전트를 두어, 에이전트가 단말기 대신에 복잡한 연산을 해주는 방법을 제안한다.

3. 제안알고리즘

VPN 에이전트는 단말기와 직접 통신을 하는 AP에 설치되어, VPN 서버와 연동하여 무선 단말기가 필요로 하는 VPN 접속을 대행해 주는 역할을 한다.

2. 위 20mm 아래 20mm, 왼쪽 20mm, 오른쪽 20mm, 머리말 10mm, 꼬리말 0mm

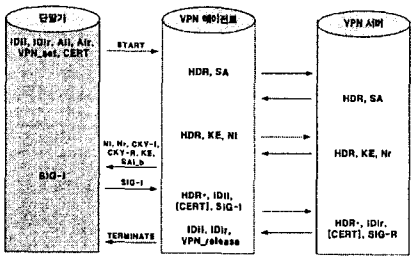

그림 1 새로 제안된 서명과 함께 인증을 제공해주기 위한 main mode의 동작 과정

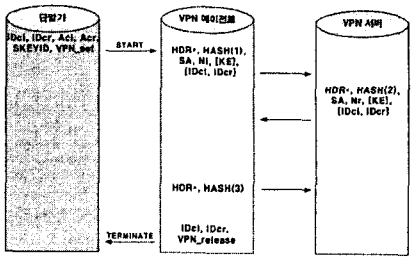

그림 2 새로 제안된 quick mode 동작 과정

VPN 구성을 위해, VPN 에이전트는 단말기 대신에 VPN 서버와 함께 ISAKMP SA를 Phase 1에서 먼저 협상한 다음, IPSec SA를 Phase 2에서 협상하게 된다.

[그림 1]은 새로 제안하는 방법을 IPSec의 서명과 함께 인증을 하기 위한 Phase 1의 Main mode에서의 프로토콜로 설계하였다. 단말기와 VPN 에이전트, VPN 서버간에 쓰이는 각각의 요소들은 기존 방법들과 대부분 동일하며, Aii와 Air은 각각 단말기와 VPN 서버의 주소를 나타낸다. VPN_set은 단말기가 VPN 에이전트에게 VPN을 시작할 것이라는 것을 알려주는 것을 말하며, VPN_release는 반대로 VPN 에이전트가 단말기에 VPN을 종료한다는 것을 알려주는 것이다.

먼저 단말기가 VPN 에이전트에게 자신의 아이디와 주소, 그리고 VPN을 할 VPN 서버의 아이디와 주소를 자신의 신원 증명서인 CERT와 함께 VPN_set 메시지를 VPN 에이전트에게 보내면서 VPN 구성은 시작된다.

VPN 에이전트는 VPN 서버와 HDR과 SA을 주고받고, VPN 에이전트가 VPN 서버에게 HDR, KE, Ni을, VPN 서버가 VPN 에이전트에게 HDR, KE, Nr을 보낸다. 그리고 VPN 에이전트는 Ni, Nr, CKY-I, CKY-R, KE, SAi_b를 단말기에 넘겨주어 단말기가 SIG-I를 계산할 수 있게 해준다. 이렇게 단말기가 계산한 SIG-I는 VPN 에이전트에게 보내져서, VPN 에이전트는 VPN 서버와 다시 그들의 아이디와 인증서, 그리고 SIG-I 혹은 SIG-R을 서로 주고받게 된다. VPN 에이전트는 마지막으로 단말기와 VPN 서버의 아이디를 이제 VPN을 끝낸다라는 의미로 VPN_release와 함께 단말기에게 전송함으로써, VPN 협상 과정의 Phase 1의 Main mode를 끝마치게 된다. 이 과정으로 인해 ISAKMP SA가 협상된다[8].

Phase 2의 quick mode를 [그림 2]처럼 새롭게 설계했다.

이 과정에서 쓰이는 단말기와 VPN 에이전트, VPN 서버간 각각의 요소들은 기존 방법들과 대부분 동일하며, Aci와 Acr은 각각 단말기와 VPN 서버의 주소를 나타낸다.

먼저 단말기가 VPN 에이전트에게 자신의 아이디와 주소, 그리고 VPN을 할 VPN 서버의 아이디와 주소를, main mode에서 이미 설정된 SKEYID와 함께 VPN_set 메시지를 VPN 에이전트에게 보내어 VPN을 시작한다.

VPN 에이전트는 VPN 서버와 HDR*, SA, KE와 함께 단말기와 VPN 서버의 아이디, 그리고 해쉬값과 난수 값을 서로 주고받은 후, HDR*과 HASH(3)를 VPN 서버에게 보내어 Quick mode를 완성한다.

VPN 에이전트는 그 다음, 단말기와 서버의 아이디를 이제 VPN을 끝낸다라는 VPN_release와 함께 단말기에게 전송함으로써, IPSec SA가 협상된다[8].

위와 같은 과정으로, 단말기는 VPN 에이전트를 통하여 VPN 서버와 VPN을 구성한다. 또한, SA나 KE와 같은 VPN을 위한 연산들은 VPN 에이전트가 대신해주고, 세션키와 인증과 같은 사항만 단말기가 계산해주므로 단말기에 대한 오버헤드가 많이 감소하게 된다. 즉, 이와 같이 단말기에서는 VPN 접속을 위한 암호화/복호화를 계산을 수행하지 않아도 되므로 그에 따른 오버헤드를 줄일 수 있다. 특히 VPN 에이전트와 VPN 서버간에는 기존의 협상 방법을 변형시키지 않고, 기존에 VPN 에이전트와 VPN 서버간에 쓰이던 프로토콜과 장비들을 바꿀 필요가 없어서 기존 방법들과의 강한 호환성을 갖는 장점이 있다.

4. 성능평가 및 분석

이 장에서는 기존의 무선 랜 환경에서 VPN 사용 방법과 본 논문에서 제안한 방법의 성능을 평가하고 분석해 본다. 시뮬레이션은 NS(Network Simulator)-2를 이용하였다[10].

4.1 시뮬레이션 모델

시뮬레이션 환경은 IPSec의 두 가지 모드 중 부하가 큰 ESP(Encapsulation Security Payload) 모드에 대해서 시뮬레이션 해 보았고 여기서 사용하는 암호 알고리즘은 Triple DES-CBC이다. 시뮬레이션을 통한 성능 평가 시 가장 중요한 Parameter는 VPN 사용을 위한 암호화/복호화 시간과 키 교환 과정 시 발생하는 오버헤드이다. Mobile Node의 연산능력은 50MHz로 설정하였고 VPN Agent는 233MHz로 설정하였다. 이에 따른 파라미터 값은 [표 1]에 설명되어 있다[11][12]. 평가 Metric은 일정크기의 데이터를 초기화부터 TCP를 통해 전송 완료하는데 걸리는 시간으로 설정하였다. 시뮬레이션은 10회 실시하여 mean 값을 취하였다.

표 1. 시뮬레이션 피라메터

Item	Value
모바일 노드에서의 Triple DES 암호화 능력	0.01ms/Byte
VPN Agent에서의 Triple DES암호화 능력	0.001ms/Byte
VPN Server의 Triple DES 암호화 능력	∞
기존에 걸리는 VPN설정 협상 시간	5.67 Sec
제안한 알고리즘에서 걸리는 VPN설정 협상 시간	6.42 Sec

4.2 시뮬레이션 결과 및 분석

초기 VPN, TCP Connection 설정부터 데이터 전송을 완료하기까지의 시간을 측정한 결과는 [그림 3]과 같다. 그래프에서도 알 수 있듯이 전송 데이터 량이 적을 경우에는 VPN 연결 설정을 위한 초기 협상과정에서 기존의 방법에 비해 제안방법이 좋지 않은 성능을 가지게 된다. 이에 따라 10KByte, 50KByte 전송에서는 기존의 방법이 더 좋은 성능을 낸다. 하지만 전송 데이터 량이 많아질수록 제안 방법이 급격한 성능 향상을 보여줌을 알 수 있다. 이는 저 성능의 클라이언트에서 이루어지는 VPN 관련 암호화/복호화를 고성능의 VPN Agent가 대행하여 주기 때문이다. 시뮬레이션 결과 5MByte의 데이터를 보낼 경우에는 127.4%의 성능향상 효과가 있었다.

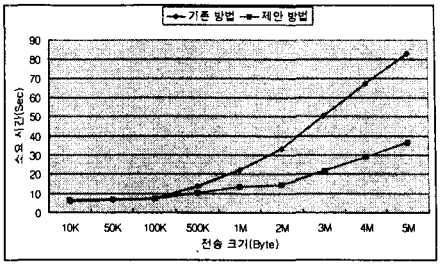

그림 3 데이터 크기별 전송 소요시간

5. 결 론

본 논문에서는 무선 랜 기반에서 VPN을 구성할 경우, 단말기가 이중의 복잡한 계산을 해야함으로 인한 오버헤드를 VPN 에이전트를 이용하여 줄이는 방법에 관해 연구하였다. 이 방법은 위에서 보여진 시뮬레이션 결과를 보아서도 알 수 있지만, 기존의 방법에 비해 고용량의 데이터를 전송할 경우 그 성능 면에서 많은 향상된 면이 있음을 알 수 있다. 또한, 기존의 클라이언트와 VPN 서버간의 IKE를 이용한 VPN 협상 방법을 변형시키지 않으므로 기존의 프로토콜이나 장비들과 강한 호환성을 갖는다는 장점이 있다. 하지만, 본 논문에서 제안하는 사항은 만약 VPN Agent가 악의적인 접근자에게 크래킹을 당하거나 노출될 경우, 보안성을 제대로 제공해줄 수 없다는 취약점이 있다. 앞으로 VPN Agent가 크래커에 의해 공격을 당하더라도 방어 할 수 있는 프로토콜과 처음부터 중간의 Agent를 고려한 VPN 설정 협상에 대해 연구해 본다.

6. 참고문헌

[1] Federal Information Processing Standards Publication 197, Announcing the ADVANCED ENCRYPTION STANDARD (AES), November 26, 2001.
[2] Ruixi Yuan, W. Timothy Strayer, Virtual Private Networks, Technologies and Solutions, Addision-Wesley Professional Computing Series, 2001.
[3] William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan, "Your 802.11 Wireless Network has No Clothes", March 2001.
[4] 김신효, 강유성, 정병호, 조현숙, 정교일, "무선 LAN 정보보호 기술 표준화 동향", 정보호호학회지, 12(4), August 2002.
[5] 이태진, "국외 무선 LAN 기술 동향", 한국 전파 진흥 협회, 2002년 2월.
[6] C. Sanchez-Avila & R. Sanchez-Reillo, The Rijndael Block Cipher (AES Proposal) : A Comparison with DES, IEEE, 2001 .
[7] Martti Kuparinen, "ISAKMP and IKE", 1998.
[8] D. Harkins, D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, 1998.
[9] Radia Perlman, Charlie Kaufman, "Analysis of the IPSec Key Exchange Standard", IEEE, 2001.
[10] NS Team, "Network Simulator 2, http://www.isi.edu/nsnam/ns/", Southern California University, 2002
[11] Manish Karir, "IPSec and the Internet", CHSCN M.S. 99-9, 1999
[12] Jose Caldera, Dionisio De-Niz, Junichi NaKaGaWa, "Performance Analysis of IPSec and IKE For Mobile IP on Wireless Environment", Carnegie Mellon Univ., 2000