논문 2005-42TC-10-5

가상사설망의 성능개선을 위한 동적 키 재생성 주기 변경 알고리즘

(A Dynamic Key Lifetime Change Algorithm for Performance Improvement of Virtual Private Networks)

한 종 훈*, 이 정 우**, 박 성 한***

(Jong-Hoon HAN, Jung Woo LEE, and Sung Han PARK)

요 약

IPSec은 인터넷의 네트워크 계층의 IP 메시지를 위한 기밀성과 인증서비스를 제공하는 보안 프로토콜이다. Internet Key Exchange (IKE)는 안전하게 Security Association (SA)를 협상하고 키 재료를 제공하는 프로토콜이다. 본 논문에서는 IPSec을 적용한 가상사설망의 성능 개선을 위해 동적으로 키 재생성 주기를 변경하는 알고리즘을 제안한다. 제안하는 알고리즘은 보안 터널 수에 따라 키 재생성 주기를 변경한다. 성능 평가를 위해 Linux 2.4.18과 FreeS/WAN을 사용하여 구현한다. 구현한 시스템은 기존 프로토콜에 비하여 네트워크 처리율과 보안성 측면에서 성능이 개선됨을 보여주고 있다.

Abstract

IPSec is a security protocol suite that provides encryption and authentication services for IP messages at the network layer of the Internet. Internet Key Exchange (IKE) is a protocol that is used to negotiate and provide authenticated keying materials in a protected manner for Security Associations (SAs). In this paper, we propose a dynamic key lifetime change algorithm for performance enhancement of virtual private networks using IPSec. The proposed algorithm changes the key lifetime according to the number of secure tunnels. The proposed algorithm is implemented with Linux 2.4.18 and FreeS/WAN 1.99. The system employing our proposed algorithm performs better than the original version in terms of network performance and security.

Keywords: 가상사설망, 네트워크 보안, IPSec, IKE

I. 서 론

최근 인터넷의 발달로 많은 기업체에서는 인터넷과 같은 공중망을 이용하여 자사의 Wide Area Network (WAN) 백본처럼 사용하는 네트워크인 Virtual Private Network(VPN)을 구축하여 사용하고 있다. VPN의 구축에서 가장 필수적인 기능의 하나는 보안성이다. 그러나 현재 인터넷 네트워크 계층에서는 보안기능이 포함되어 있지 않다. 이를 해결하기 위하여 IETF에서는 네트워크 계층 보안 프로토콜 표준으로 IPSec을 정의하고 있다[1].

IPSec Gateway를 사용하여 VPN을 구성할 경우 각 Gateway간에 가상의 보안터널을 구성하여 터널링 방식

* 정회원, 삼성전자 통신연구소 차세대 단말팀
(Samsung Electronicsco. Telecommunication R&D Center)
** 정회원, 삼성SDS
(Samsung SDS SCM Business group)
*** 정회원, 한양대학교
(Department of Computer Science and Engineering, Hanyang University)
접수일자: 2005년3월28일, 수정완료일: 2005년10월10일

으로 암호화 된 데이터를 전송하게 된다. 가상의 보안 터널을 맺기 위해 키를 협상하고 전송하는 프로토콜이 Internet Key Exchange (IKE)이다[2]. IKE에서는 암호 키의 노출을 막기 위해 주기적으로 암호 키를 재생성 하여야만 한다. 암호 키를 재생성하는 과정은 계산집중적인 방식으로 이루어져 있어서 네트워크 성능을 저하시키는 주요 요인 중 하나이다.[3] 암호 키를 생성하는 과정을 어느 정도의 시간 간격으로 수행할지를 결정하는 값을 키 재생성 주기라한다. 적절한 키 재생성주기를 결정하는 것에 대해서는 연구가 되어있지 않아서 네트워크 관리자가 임의로 설정해서 사용하는 문제가 있고, 또한 망의 트래픽 상황에 관계없이 하나의 값으로 고정되어 있어서 비효율적이다.

IKE 프로토콜의 성능을 향상시키기 위하여 기존 연구에서는 SA연결 절차를 간소화 시키는 방법을 사용하였다. 이것은 SA 성립과정에서 표준적인 방법보다 연결 과정 중에 보안상 약점이 생길 수 있는 문제점이 있다.

따라서 본 논문에서는 SA 연결 절차는 표준 방법으로 유지하면서 보안터널 수에 따른 적절한 키 재생성 주기를 결정하고, 그 결과를 이용하여 각 터널의 트래픽 상황을 모니터링 하여 동적으로 키 재생성 주기를 변경하는 방법을 제안한다.

Ⅱ. IPSec

IPSec은 IP datagram을 위한 상호운용 가능한 암호 기반의 고품질 보안을 제공하도록 설계되었다. IPSec에서는 이러한 목표들이 Authentication Header (AH)와 Encapsulating Security Payload (ESP)의 두 가지 트래픽 보안 프로토콜과 키를 협상하고 관리하는 IKE 프로토콜의 사용을 통해 충족된다[4]-[6].

1. AH

내용을 AH 프로토콜[7]은 무결성, 데이터 근원 인증, 재전송 공격 방지 서비스를 제공한다. 그러나 AH는 자신이 보호하는 패킷을 암호화하지 않으며, 따라서 어떠한 기밀성 서비스도 제공하지 않는다. IPSec 처리에 의해서 AH가 들어가는 위치와 보호의 범위는 운용방법에 따라 달라진다. 먼저 트랜스포트 모드에서 AH 프로토콜로 인증하는 경우에는 원래의 IP 헤더의 일부 필드

Original IP packet

IP Header	Payload

New IP packet after applying AH

New IP Header	AH Header	Original IP Header	Payload

그림 1. 터널모드 AH 구조
Fig. 1. The tunnel mode AH structure.

(TTL등 전송 중에 달라질 수 있는 필드)를 제외한 전체 범위가 된다. 터널 모드에서 AH 프로토콜을 적용할 때의 헤더 구조는 그림 1과 같다.

2. ESP

ESP[8]는 데이터 기밀성, 데이터 근원 인증, 무결성, 재전송 공격 방지 서비스, 제한된 트래픽 흐름 기밀성을 제공한다. 기밀성 서비스는 패킷을 암호화하기 위한 암호알고리즘을 사용함으로써 제공된다. 트래픽 흐름 기밀성은 터널 모드에서만 제공된다. 터널 모드에서 ESP 프로토콜을 적용하는 경우 패킷의 구조는 그림 2와 같다.

Original IP packet

IP Header	Payload

New IP packet after applying ESP

New IP Header	ESP Header	Original IP Header	Payload	ESP Trailer	ESP Auth

그림 2. 터널모드 ESP 구조
Fig. 2. The tunnel mode ESP structure.

3. IKE

IPSec peer간 통신을 위해서는 암호화 알고리즘, 운용모드, 암호 키, 키의 수명 등에 대한 합의가 필요한데 이것을 IPSec에서는 Security Association(SA)라고 한다. 즉, IPSec을 이용하여 보안 통신을 하고자 하는 통신 쌍방은 보안 통신 시작 전에 상호 합의된 SA를 생성하고 유지하여야하며 통신 종료 시 이를 소멸시키는 단계를 거쳐 동작한다.

보안 네트워크 규모가 크지 않은 환경에서는 SA의

관리를 네트워크 관리자의 수작업으로 할 수 있다. 하지만, IPSec의 구축이 큰 규모의 네트워크로 확대되면 SA의 관리를 더 이상 수동으로 할 수 없고 자동화하여야 한다. 즉, 보안 통신을 하고자 하는 임의의 통신 쌍방은 SA의 생성, 유지, 소멸등 SA 관리 작업을 자동적으로 수행해 낼 수 있는 수단을 가져야 한다. IKE 프로토콜은 이러한 SA 관리 작업을 자동화하기 위한 목적으로 IETF에서 고안한 IPSec의 표준 키 관리 프로토콜이다. IKE는 ISAKMP, Oakley, SKEME의 관련 부분을 결합한 프로토콜이며, 2단계 SA 수립과정을 보호하기 위한 1단계 교환과 실제 데이터를 보호하기 위한 IPSec SA를 수립하는 2단계 교환으로 구성된다.

Ⅲ. 키 재생성 주기

IPSec을 적용한 보안게이트웨이를 이용하여 VPN을 적용할 경우 가장 큰 문제는 네트워크 성능의 저하이다. 네트워크 성능 저하의 주요 요인 중 하나로 키 재생성을 들 수 있다. IPSec은 암호화키의 노출을 막기 위해 주기적으로 키를 재생성 한다. 키의 재생성은 매우 복잡한 연산을 필요로 하므로 키를 자주 생성하면 네트워크 성능이 급격히 저하된다. 그러나 네트워크 성능만을 고려하여 키 재생성 주기를 너무 길게 하면 키가 노출될 가능성이 높아진다. 따라서 네트워크 성능과 보안성을 고려한 적절한 키 재생성 주기의 결정이 필요하다. 또한 보안 터널 수에 따른 고려가 필요하다.

1. 키 재생성주기의 동적 결정

VPN에서 모든 게이트웨이가 동시에 송수신을 하는 경우는 거의 없다. 망의 용도에 따라 다르지만 가능한 모든 연결의 90%정도가 사용될 수도 있고 20~30%만이 사용될 수도 있다. 그럼에도 불구하고 기존 방식에서는 VPN에 고정된 한 개의 키 재생성 주기만이 허용되기 때문에 가장 큰 값을 선택하거나 혹은 평균을 구하여 사용할 수밖에 없다. 이는 매우 비효율적이므로 본 논문에서는 트래픽 상황에 따라 동적으로 적절하게 키 재생성 주기를 변화시키는 알고리즘을 제안한다. 제안하는 구조는 전체적인 구조의 변경 없이 기존 프로토콜에 추가 할 수 있는 장점이 있다. 본 논문에서 제안하는 알고리즘의 전체 구성도는 그림 3과 같다.

IKE에서 SA를 효율적으로 관리하기 위한 묶음을 SA database (SAD)라고 한다. SAD내에서 SA는 Security Parameter Index (SPI) 및 송/수신지 IP 주소에 의해서 고유하게 식별된다. IPSec Traffic Monitor는 보안 터널의 활성화 여부를 감시한다. 각 보안 터널의 송수신 여부를 감시하여 활성화된 보안 터널의 수를 Key Lifetime Controller에게 보고한다. Key Lifetime Controller는 Key Lifetime Reference Table에서 터널 수에 해당하는 키 재생성 주기를 가져와서 SAD내 SA의 값을 변경한다. Key Lifetime Reference Table은 측정을 통해 임의의 터널 수 (T)에 따른 적절한 키 재생성주기 값 (P(T))을 저장하고 있다.

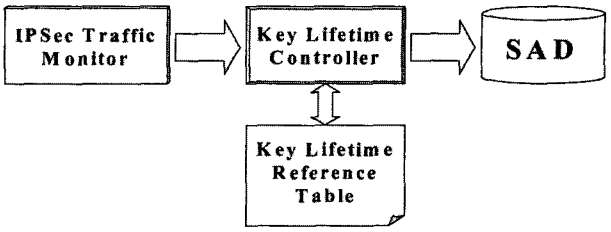
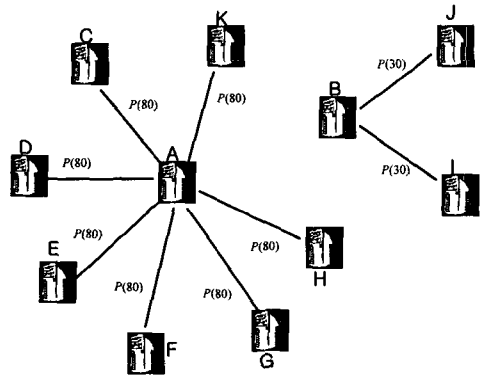
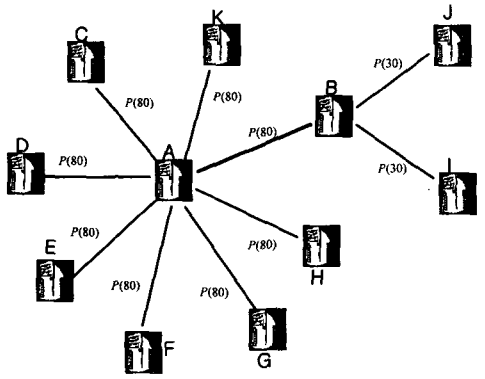


그림 3. 동적 키 재생성 주기 변경 알고리즘
Fig. 3. A dynamic key lifetime change algorithm.

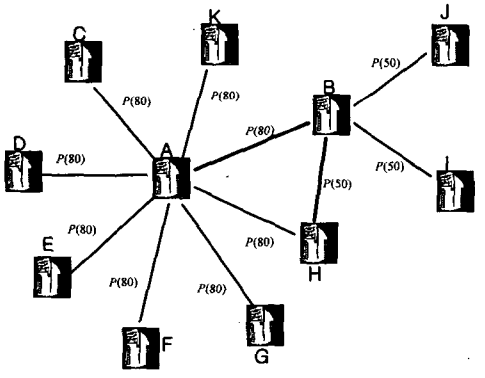
본 논문에서 제안하는 키 재생성 주기 알고리즘을 설명하기위해 그림 4와 같은 11개의 보안게이트웨이(SG)로 구성된 가상사설망을 가정한다. 11대의 SG가 존재하고 SG간의 각각의 연결은 10개의 보안터널을 사용하고 있다는 것을 나타낸다. P(T)를 결정할 때 T는 제안하는 알고리즘을 적용할 가상사설망의 트래픽 변화 특성에 따라 일정한 구간, 혹은 가변적인 구간으로 나눌 수 있다. 본 논문에서는 트래픽이 작은 구간에서 변화가 많고 트래픽이 큰 구간에서 변화가 적은 망을 가정하여 가변적인 P(T)를 구성하였다. 보안터널 수가 10개 이하인 경우 P(10), 11~30개 일때 P(30), 31~50개 일때 P(50), 51~80개 일때 P(80), 81~120개일 때 P(120)을 키 재생성 주기로 사용한다. 기존의 방법은 네트워크가 부트되면 미리 설정된 단 한개의 키 재생성 주기를 고정적으로 사용하므로 연결 가능한 최대 터널 수를 고려해야 한다. 따라서 기존의 방법을 사용할 경우 1대의 SG가 나머지 10대의 SG와 각각 10개의 보안터널을 사용한다고 가정하면 한 대의 SG가 연결 가능한 최대 터널 수는 100개이므로 현재 연결된 터널 수와 관계없이 항상 키 재생성 주기로 P(120)을 사용해야 한다. 그러나 제안하는 방법에서는 각 게이트웨이 별로 키 재생성 주기를 다르게 적용하여 사용하므로 그림 4(a)와 같이 A-B, B-H간 연결이 없는 경우 A는 P(80), B는



(a) A-B, B-H 연결 전



(b) A-B 연결 후



(c) B-H 연결 후

그림 4. 보안 터널 수에 따른 키 재생성 주기의 동적 변경

Fig. 4. A dynamic key lifetime change according to the number of secure tunnels.

P(30)을 키 재생성 주기로 사용하게 된다. 그림 4(b)와 같이 A-B간 터널이 활성화 되면 A는 P(80), B는 P(30)을 A-B간 보안터널의 키 재생성 주기로서 제시한다. Key Lifetime Controller는 이렇게 키 재생성 주기가 상충하는 경우 망 전체의 평균 traffic을 고려하여 긴 값을 채택하게 된다. Key Lifetime Reference Table에서 키 재생성 주기 값으로 P(80)을 가져와서 적용한다.

그리고, 그림 4(c)와 같이 B-H간 연결이 활성화되면 H는 P(30)을, B는 기존의 A, I, J 와 각각 10개의 터널에 H와의 터널 10개를 더해 총 40개의 터널이 연결되어 P(50)을 키 재생성 주기로 제안하고, 둘 중 더 긴 값인 P(50)이 키 재생성 주기로 채택된다. 이후 B는 i와 j에게 키 재생성 주기를 P(50)으로 변경하라는 메시지를 보내서 변경을 완료한다.

본 논문에서 제안하는 동적 키 재생성 알고리즘은 다음과 같다.

(i) 트래픽을 감지하여 각 SG와 이에 연결된 채널의 활성화된 보안 터널수를 조사

(ii) 보안 터널 수가 Key Lifetime Reference Table의 어느 구간 사이에 있는지 조사하여 적합한 키재생성 주기 결정

(iii) 서로 다른 키 재생성 주기를 사용하는 SG간 연결이 일어나는 경우 두 SG간의 키 재생성 주기는 두 SG가 사용하고 있는 키 재생성 주기 중 큰 값으로 변경

(iv) 새로운 연결로 인해 보안 터널수가 증가하여 키 재생성 주기가 변경될 경우 자신과 연결된 모든 SG에게 변경된 값으로 키 재생성 주기를 사용하도록 통보

(v) 통보받은 SG는 자기의 키 재생성 주기를 변경

그림 4는 제안하는 알고리즘의 예를 보여 준다.

2. 제안하는 알고리즘의 구현

FreeS/WAN은 리눅스에서 IPSec 프로토콜을 구현하는 공개 프로젝트 중의 하나이다. FreeS/WAN에서는 KLIPS라는 리눅스 커널 모듈과 Pluto라는 커널 밖에서 동작하는 데몬(daemon) 두 개의 구조로서 구현하고 있다.

KLIPS는 리눅스 커널 속에서 실제 IPSec packet의 처리, 암호화, 패킷 인증 값 계산, outgoing packet에 대해 ESP 헤더와 AH 헤더 생성, incoming packet에 대해 헤더의 해석을 처리한다. Pluto는 KLIPS와 달리, 리눅스 커널 속에서 동작하는 것이 아니라 데몬(daemon) 프로그램으로 커널 밖에서 동작한다. Pluto는 IKE 프로토콜을 구현하는 모듈로서 phase 1 ISAKMP SA의 생

성, 호스트간 인증과 다른 게이트웨이와의 협상을 처리하고 IPSec SA를 생성한 후 관련 파라미터를 리눅스 커널 속에서 동작하는 KLIPS에 전달하는 역할을 한다. Pluto안에 IPSec Traffic Monitor와 Key Lifetime Controller를 구현한다.

IPSec Traffic Monitor는 /proc/net/ipsec_eroute의 보안 터널별 통과한 패킷수를 참조하여 활성화된 터널의 수를 체크한다. 그림 5는 ipsec_eroute의 예제이다. 첫 번째 열이 통과한 패킷의 개수이고, 순서대로 송신 IP, 수신 IP, SA의 식별자이다. 식별자 뒤에는 수신 게이트웨이 IP가 붙는다. 각 터널별로 통과한 패킷수를 주기적으로 저장하여서 터널의 활성화 여부를 결정하고 Key Lifetime Controller에 보고한다.

```
251  192.168.1.2/32  -> 192.168.2.2/32 => tun0x14b0@
0    192.168.1.3/32  -> 192.168.2.3/32 => tun0x14b2@
910  192.168.1.4/32  -> 192.168.2.4/32 => tun0x14b4@
47   192.168.1.5/32  -> 192.168.2.5/32 => tun0x14ac@
115  192.168.1.6/32  -> 192.168.2.6/32 => tun0x14ae@
0    192.168.1.7/32  -> 192.168.2.7/32 => tun0x14a6@
196  192.168.1.8/32  -> 192.168.2.8/32 => tun0x14a8@
468  192.168.1.9/32  -> 192.168.2.11/32 => tun0x14a4@
```

그림 5. /proc/net/ipsec_eroute
Fig. 5. /proc/net/ipsec_eroute.

```
struct connection {
    char *name;
    lset_t policy;
    time_t sa_ike_life_seconds;        ①
    time_t sa_ipsec_life_seconds;      ②
    time_t sa_rekey_margin;
                :
                :
                :
```

그림 6. connection 구조
Fig. 6. Connection structure.

FreeS/WAN에서 SAD는 KLIPS에 구현되어 있는데 Pluto의 값을 참조한다. 이 값은 state 구조체 안에 connection 구조체가 포함된 이중 구조체의 형식으로 구현되어 있다. 그림 6은 connection 구조의 일부이다.

①, ②가 키 재생성 주기를 나타낸다. Key Lifetime Controller는 터널 수를 보고 받아 Key Lifetime Reference Table의 값을 가져온 뒤 SAD의 ①, ② 값을 변경한다.

Ⅳ. 시뮬레이션

키 재생성 주기는 모든 VPN에 적용할 수 있는 일반화된 값이 존재하지 않는다. VPN 게이트웨이의 수, 각 게이트웨이의 연산 능력, 설치된 곳의 인터넷 망 상태 등 여러 가지 요인이 복합적으로 작용하기 때문이다. 그러나 실험을 통한 예시를 참조하여 실정에 맞게 적용할 수 있을 것으로 사료된다. 따라서 본 논문에서는 실험을 위해 다음과 같은 테스트 베드 환경을 구축한다.

1. 테스트 베드 환경

본 논문에서는 Red Hat Linux 8 (kernel 2.4.18-14)를 OS로 하고 IPSec 공개구현 프로젝트인 FreeS/WAN 1.99[9]를 설치하여 보안게이트웨이를 구성한다. 하드웨어 사양은 펜티엄-3 700Mhz CPU, 256M 메모리이다. 각 게이트웨이는 직접 연결하고 여기에 네트워크 성능 분석기인 SmartBits 200을 사용하여 측정한다. AH, ESP를 적용하고 MD5, 3DES를 사용하였고, 인증방식으로 digital signature(RSA public key)를, 옵션으로 PFS를 사용한다.

2. 키 재생성주기 측정

보안 터널 수와 키 재생성 주기를 변화시키며 측정한 결과는 표 1과 같다. 표 1에서 보는바와 같이 보안터널이 1개인 경우 키 재생성 주기를 짧게 하여도 네트워크 성능에는 큰 변화가 없는 것을 알 수 있다. 그러나 보안 터널의 수가 늘어날수록 키 재생성 주기가 네트워크 성능에 큰 영향을 미치고 있음을 알 수 있다. 또한 보안 터널 수에 따라 급격히 네트워크 성능이 저하되는 구간이 있음을 알 수 있다. 이에 따라 이 구간보다 조금 긴 키 재생성주기를 선택하면 보안성과 네트워크 성능 사이에서 적절한 키 재생성 주기를 결정할 수 있다. 그리고 최대 전송율의 일정 비율 이상을 보장해야 한다. 따

표 1. 보안터널수와 키 재생성 주기에 따른 네트워크 처리율 (Mbps)

Table 1. Network throughput according to number of secure tunnel and key lifetime.

터널수 / 키주기(s)	1	30	50	80	120	250	500	750
28800/7200	32.01	29.18	28.95	28.90	28.78	28.30	27.54	27.20
20000/5000	31.99	29.05	28.94	28.89	28.55	28.29	27.31	26.17
16000/2000	31.98	29.41	28.95	28.89	28.44	28.28	26.20	24.72
12000/1500	31.98	29.31	28.95	28.32	28.05	27.59	25.10	23.71
8000/1000	31.98	29.30	28.95	28.19	27.96	25.78	24.27	22.39
4000/1000	31.98	29.20	28.91	28.11	27.74	24.85	23.37	21.01
1800/450	31.98	28.96	28.50	27.96	23.79	23.08	22.41	19.83
1800/225	31.97	28.89	28.25	27.88	23.04	22.87	22.03	18.35
800/200	31.94	28.57	27.81	24.65	22.92	22.20	20.17	15.21
800/100	31.95	28.87	27.78	24.09	21.67	20.01	19.15	14.65
400/100	31.76	28.40	27.80	23.82	19.67	17.34	14.78	11.50
400/50	31.61	27.88	27.30	23.05	18.66	16.19	6.93	4.94
200/50	31.60	27.67	24.05	22.77	17.36	15.20	4.42	2.45
200/25	31.60	27.38	23.07	21.77	16.05	12.67	3.01	
100/25	31.60	27.22	23.07	21.53	14.35	9.44		
50/25	31.60	27.31	23.45	20.92	12.45	5.29		
30/15	31.60	24.66	21.79	18.72	10.82	3.08		

라서 본 논문에서는 최대 전송율의 85%이상의 성능을 나타내는 구간을 키 재생성 주기로 결정한다.

3. 제안하는 알고리즘의 측정결과

제안하는 알고리즘의 성능을 평가하기 위해 다음과 같이 가정한다.

① 망의 최대 보안 터널 수는 750개이다.

② 보안 터널 수는 0개에서 시작하여 750개까지 75시간 동안 지수분포로 증가한다.

위와 같은 망에 기존 프로토콜과 제안하는 알고리즘을 각각 적용하여 얻은 네트워크 처리율은 그림 7과 같다.

제안하는 알고리즘은 매시간 변화하는 보안 터널 수에 따라 서로 다른 키 재생성 주기를 갖을 수 있기 때문에 제안하는 알고리즘과 기존 프로토콜을 키 주기별로 네트워크 처리율의 차이를 비교하는 것이 불가능하다. 따라서 생성된 모든 터널이 시간에 상관없이 동일

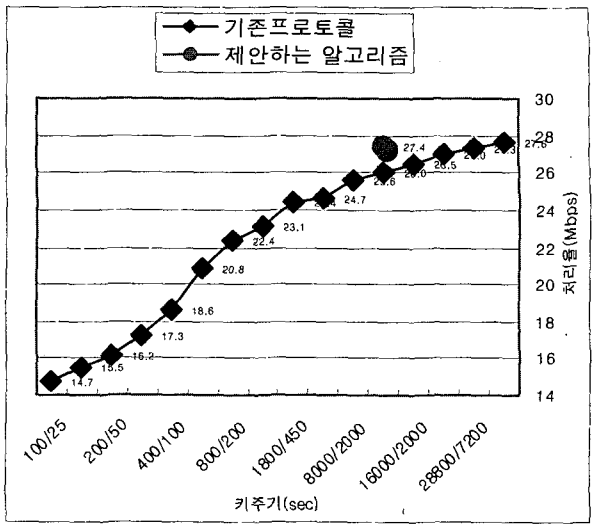


그림 7. 키 재생성 주기에 따른 네트워크 처리율 비교

Fig. 7. Comparison of network throughput according to key life time.

한 키 재생성 주기를 갖는 기존의 방식과는 직접적인 성능 비교를 할 수 없다는 것을 의미한다. 그림7에서는 제안하는 알고리즘에 있어서는 측정시간동안 변화한 키 주기의 평균과 네트워크 처리율의 평균을 가지고, 기존 프로토콜과 비교한다.

제안하는 알고리즘은 키 재생성 주기가 동적으로 변화하는데, 평균적으로 8000s/2000s 정도이고 네트워크 처리율은 27.4Mbps이다. 그림 7에서 보는 바와 같이 제안하는 알고리즘은 기존 프로토콜에 비해 비슷한 키 재생성 주기에서는 네트워크 처리율이 높고, 비슷한 네트워크 처리율에서는 평균 키 재생성 주기가 짧다. 따라서 제안하는 알고리즘이 기존 프로토콜보다 효율적으로 동작하는 것을 알 수 있다.

V. 결 론

VPN을 구성하는 방법은 네트워크계층에서 작용하는 IPSec과 어플리케이션계층에서 동작하는 SSL VPN이 대표적이다. IPSec을 이용할 경우 네트워크계층에서 동작하기 때문에 그 상위 계층에서 동작하는 프로그램의 수정없이 보안성을 제공할 수 있는 장점이 있다. 그렇지만 IPSec을 이용하여 VPN을 구성할 경우 암호화를 위한 계산작업과 암호화에 필요한 키를 주고받는 과정에 의해 네트워크 성능이 저하되는 문제점이 있다.

본 논문에서는 IPSec 적용후에 네트워크 성능이 저하되는 것을 막기 위하여 VPN의 트래픽 상황에 따른

키 재생성 주기를 제시하고 이를 바탕으로 동적으로 키 재생성 주기를 변화시키는 알고리즘을 제안한다. VPN의 최초 설치 시 측정을 통하여 적절한 키 재생성 주기를 결정하면, 이후 제안한 알고리즘을 사용하여 트래픽 상황에 따라 효율적으로 키 재생성 주기를 변화시킴으로써 네트워크 성능과 보안성을 개선할 수 있다.

참 고 문 헌

[1] Roger Younglove, "IP security: what makes it work?," *Computing & Control Engineering Journal* , Vol 12, No. 1, pp. 44-45, 2001.

[2] R. Perlman, C. Kaufman, "Key exchange in IPSec: analysis of IKE," *Internet Computing, IEEE,* Vol 4, No. 6, pp. 50-56, 2000.

[3] O. Elkeelany, M. Matalgah, K. Sheikh, M. Thaker & D. Qaddour, "Performance Analysis of IPSec Protocol: Encryption and Authentication," *IEEE International Conference on Communications,* Vol. 2, pp. 1164-1168, 2002

[4] Carlton R. Davis, IPSec : Securing VPNs, McGraw-Hill, 2001.

[5] IP Security Document Roadmap (RFC 2411)

[6] Security Architecture for the Internet Protocol (RFC 2401)

[7] IP Authentication Header (RFC 2402)

[8] IP Encapsulating Security Payload (ESP) (RFC 2406)

[9] FreeS/WAN project, www.freeswan.org

저 자 소 개

한 종 훈(정회원)
2002년 한양대학교 전자컴퓨터 공학부 학사.
2004년 한양대학교 컴퓨터공학과 석사.
2005년 현재 삼성전자 통신연구소 차세대단말팀
<주관심분야: 네트웍, Bluetooth, WPAN, IPsec>

이 정 우(정회원)
2003년 한양대학교 전자컴퓨터 공학부 학사.
2005년 한양대학교 컴퓨터공학과 석사.
2005년 현재 삼성SDS SCM사업단 주임컨설턴트
<주관심분야: 네트웍, Bluetooth, WPAN, IPsec>

박 성 한(정회원)
1970년 한양대학교 전자공학과 학사
1973년 서울대학교 전자공학과 석사
1984년 미국 텍사스주립대 전기 및 컴퓨터공학과 박사
2003년 대한전자공학회 회장
1986년~현재 한양대학교 전자컴퓨터공학부 교수
<주관심분야: 네트웍, Bluetooth, WPAN, IPSec, 영상처리>