이동성과 보안성 만족 군용 통신을 위한 IPSec 기반 네트워크 설계

정회원 정 윤 찬*

IPSec based Network Design for the Mobile and Secure Military Communications

Younchan Jung* ***Regular Member***

요 약

군용 환경에서 동적으로 변화하는 PT (Plain Text) 네트워크들이 Black (Blk) 네트워크를 통하여 서로 보안성 있는 통신을 하기 위해서는 Blk 네트워크를 형성하는 완전 그물형 IPSec 터널이 필요하다. 이동성과 보안성이 요구되는 Blk 네트워크에서 IPSec 터널과 보안 방안, 즉 SPD (Security Policy Database)를 동적으로 재구성하는 것은 어려운 과제이다. 본 논문에서는 기존의 IPSec 터널 터널 모드 기술과 IPSec 비밀 키 관리 기술을 바탕으로 하여 군 네트워크에서 요구하는 이동성과 보안성 능력을 제공하기 위해서 구비해야 할 기술인 DMIDP (Dynamic Multicast-based IPSec Discovery Protocol) 기술과 관련된 핵심 기술을 체계적으로 제안한다. 또 제안된 DMIDP 기법에서 나타날 이동성 및 보안성과 관련된 성능에 영향을 미치는 주요 변수와 이들의 운영 방법을 도출하고 제안된 변수 상태에서의 DMIDP 운영 효율성을 분석한다.

Key Words : IPSec Tunnels, Military Networks, Security Policy Database, Virtual Private Network, IPSec Discovery Protocol

ABSTRACT

Full-mesh IPSec tunnels, which constitute a black network, are required so that the dynamically changing PT (Plain Text) networks can be reachable across the black network in military environments. In the secure and mobile black networks, dynamically re-configuring IPSec tunnels and security policy database (SPD) is very difficult to manage. In this paper, for the purpose of solving mobility and security issues in military networks, we suggest the relating main technologies in association with DMIDP (Dynamic Multicast-based IPSec Discovery Protocol) based on existing IPSec ESP (Encapsulating Security Payload) tunnels and IPSec key managements. We investigate the main parameters of the proposed DMIDP techniques and their operational schemes which have effects on mobility and analyze operational effectivemess of the DMIDP with proposed parameters.

Ⅰ. 서 론

대규모 군용 네트워크에서 가상 사설망, 즉 VPN (Virtual Private network)식 IPSec 터널을 운영하기 위한 SPD(Security Policy Database)의 수동 설정은 운영자의 작동 오류 가능성, 긴 SPD 설정시간, 동적 네트워크 환경에 부적합한 이유로 인하여 운영하기가 어렵다[1,2]. 그 이유는 군 전술네트워크에서는 IPSec

* 가톨릭대학교 정보통신전자공학부 통신네트워크 연구실 (ycjung@catholic.ac.kr)
논문번호 : KICS2010-03-137, 접수일자 : 2010년 3월 31일, 최종논문접수일자 : 2010년 8월 19일

장치로 보호되는 PT(Plain Text) 네트워크들이 서로 통신할 수 있도록 완전 그물형 형태의 IPSec 터널이 이용되는데, 전술 상황에 따라 PT 네트워크 들이 이동 중에 연결이 끊어지거나 적의 공격으로 네트워크가 파손될 수도 있기 때문에 이런 동적 상황에서 SPD 정보를 수동 운영하게 되면 네트워크의 이동성 및 보안성을 지속적으로 제공할 수 없기 때문이다[3].

그림 1에서 나타낸 바와 같이, Black(Blk) 네트워크는 IPSec 장치들로 IPSec 터널을 구성하고 있다. 즉, 이 구간은 IPSec 터널모드 기술 중에서 ESP (Encapsulating Security Payload)에 의해 보호되는 CT (Cipher Text) 영역을 나타낸다. Red 네트워크는 군부대 내에서 운영되는 네트워크로 PT (Plain Text) 형태로 운영되는 접속 네트워크 형태이다[4-6]. 여기서 Blk 네트워크는 상용의 Core 네트워크에 해당되며 운영 형태는 두 가지 형태로 분류될 수 있다.

첫 번째 운영 형태는 그림 2에서 보여주는 것과 같이 점선으로 연결된 링크 구간이 ESP 터널 모드로 운영되는 군전용 Blk 네트워크 이다. 여기는 상용 이용자의 접근이 ESP 터널 모드 운영에 의해 완전히 차단된다. 두 번째의 Blk 네트워크 운영 방법을 그림 3에 나타내었다.

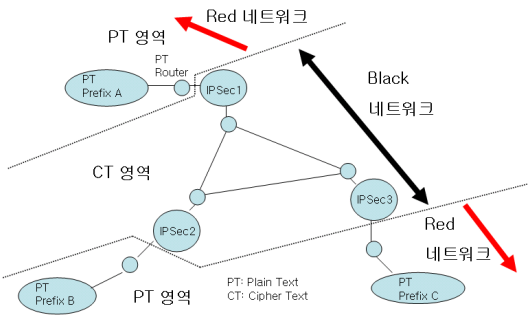

그림 1. Red 네트워크와 Blk 네트워크

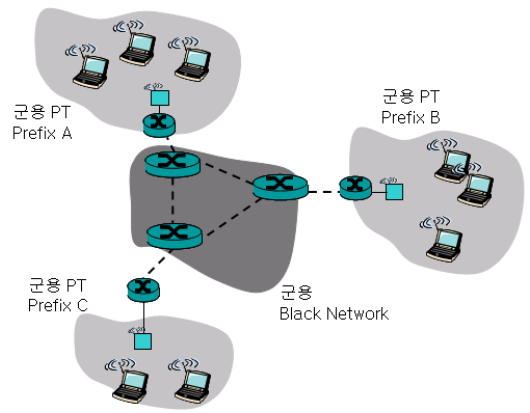

그림 2. 군전용의 Blk 네트워크 운영

그림 3의 민군 겸용 Blk 네트워크 운영기술도 IPSec ESP 터널 모드 기술에 의하여 구현될 수 있다[7]. 가장 중요한 특징은 지역적으로 멀리 떨어져 있는 군용 A 네트워크와 B 네트워크 간에는 VPN 네트워크 형태로 상용의 Core 네트워크 안에 안전한 터널이 구축된다. 이처럼 상용의 Core 네트워크 자원을 군용 VPN으로 이용하는 경우의 가장 큰 장점은 그림 2에서와 같은 군전용의 Blk 네트워크를 구축할 필요가 없다는 점이다. 즉, 군용 A 네트워크 가입자는 군용 B 네트워크 가입자와 마치 별도의 군전용 Blk 네트워크가 있는 것처럼 안전하게 상용 네트워크를 통하여 통신할 수 있다. 이를 가능하게 하는 기술이 IPSec ESP 터널 모드 기술이다. 뿐만 아니라 군용 A 네트워크 가입자는 상용 Y 네트워크 가입자와 보안성 없는 통신을 민군 상호 운영할 수 있다. 이와 같은 기술은 군 통신에서의 녹색 (Green) 기술이라고 볼 수 있는데, 상용과 군용은 물리적으로는 같은 네트워크를 이용하면서 군전용의 VPN을 제공해 줌으로서 군 네트워크 입장에서는 마치 그림 2처럼 전용으로 네트워크를 이용하고 있는 것과 차이가 없도록 운영된다는 점이다. 이것은 네트워크 구축비용을 절대적으로 감소시킬 수 있는 기술로서 민군이 이중의 네트워크 구축 없이 하나의 네트워크 구축으로 상용과 군용의 양쪽 요구를 모두 만족시킴은 물론 민과 군의 상호 운영 까지 자연스럽게 가능하게 해준다.

이 논문의 구성은 다음과 같다. II 장에서 군용 IPSec 터널 운영의 기반 기술이 되는 상용의 ESP 터널 모드 일반 기술과 IPSec 비밀 키 관리 기술을 조사하고 있다. II 장의 상용 기술을 바탕으로 하여 군 네트워크에서 요구하는 이동성과 보안성 능력을 제공하기 위해서 구비해야 할 기술인 DMIDP (Dynamic Multicast-based IPSec Discovery Protocol) 기술과

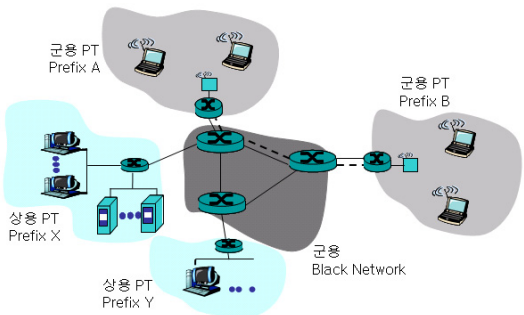

그림 3. 민군 겸용의 Blk 네트워크 운영

관련된 핵심 기술을 3장에서 체계적으로 정립하고 있다. 4장에서는 정립된 DMIDP 운영에서 이동성 및 보안성과 관련된 성능에 영향을 미치는 주요 변수들을 제안하고 제안된 상황에서의 성능을 분석한다. 그리고 5장에서 결론을 기술하고 있다.

Ⅱ. ESP 터널 모드 일반

2.1 IPSec 터널 모드

IPSec 터널 모드를 운영하기 위하여 ESP 프로토콜을 사용하여야 한다. ESP 프로토콜은 인증을 위하여 사용할 수도 있으나 대부분 대칭키를 사용하여 Blk 네트워크를 통과하는 Inner IP 데이터그램을 암호문으로 만든다. 이 때 ESP 헤더에는 SPI (Security Parameters Index) 필드를 붙여 준다. 터널의 끝인 원격 IPSec 장치에 데이터그램이 도착하면 SPI 필드 값을 조사한 후, 이 SPI 값에 대응되는 SA (Security Association) 값을 찾아서 암호문 형태의 Inner IP 데이터그램을 복호화하여 원래의 IP 데이터그램으로 복구한다. SA는 터널의 시작과 끝에서 어떻게 암호화를 적용할 것인지를 결정하는 정보를 가지고 있다. 그러므로 터널의 시작 IPSec 장치에는 여러 개의 SA들이 SA 데이터베이스 (SADB) 형태로 유지되고 있다. SA가 포함하고 있는 가장 중요한 정보는 터널모드로 암호화에 사용할 키 값과 암호화 알고리즘 이름이다. 결론적으로 터널이 하나 만들어진다는 것은 해당 SA가 만들어져서 터널의 시작과 끝에 존재하고 있다는 것과 같다.

터널의 시작과 끝에 해당하는 IPSec 장치에는 SPD (Security Policy Database)를 가지고 있다. 그림 1에서 Red 네트워크로 부터 어떤 데이터그램이 Blk 네트워크로 진입해 오면 해당 IPSec 장치는 이 데이터그램의 헤더에 있는 출발지 IP 주소와 목적지 IP 주소 정보를 가지고 SPD를 조사하여 해당 SA를 찾아내게 된다.

이때 만약 해당 SA가 없으면 새로운 SA를 만들어야 하는데, 이때 SA가 포함하게 될 비밀키 값을 터널의 시작점과 끝점이 공유해야 하는 일이 중요해 진다. 이 과정은 다음절의 키 관리에서 설명한다.

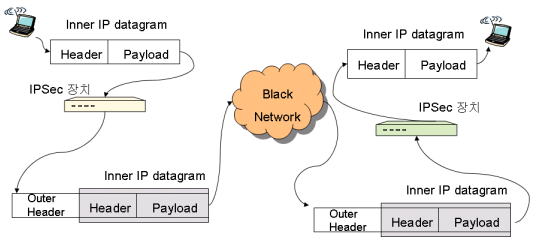

그림 4. IPSec 터널 모드 운영

2.2 IPSec 비밀키 관리

일반적으로 최근에 상용에서 사용하고 있는 키관리 방법은 원천적으로 DH (Diffie-Hellman) 키 교환 알고리즘에 바탕을 두고 있다. DH 알고리즘은 두 가지의 장점을 가지고 있는데, 하나는 필요할 때 마다 바로 키 값을 양쪽에서 만들어 보유할 수 있다는 점이고, 또 다른 하나는 상호 간에 두개의 포괄적 변수 값만 합의되어 있으면 키 교환이 이루어질 수 있다는 점이다. 그러나 DH 방식은 해결해야만 할 약점을 안고 있었다. 키 교환에서 상대방의 확인 절차가 없다는 점과, man-in-the middle 공격 (제3자 개입 공격)에 취약하다는 점이다. 또한 Clogging 공격, 즉 악의적으로 키 교환을 수없이 반복시켜 상대방의 정보처리 능력을 마비시키는 공격에 대한 대비책이 없다는 점이 약점이다.

최근의 키 교환 방식에서는 Clogging 공격에 대비하여 서로 Cookie 교환을 하도록 하고 있으며, Reply 공격을 대비하여 1회성 비밀 값 을 사용하고, 인증을 위하여 전자 서명을 사용 한다[8-10].

Ⅲ. 군용 목적의 동적 IPsec 탐지 프로토콜

이동성과 보안성이 요구되는 Blk 네트워크에서 IPSec 터널과 보안 방안, 즉 SPD 를 동적으로 재구성하기 위해서는 멀티케스트 채널을 이용하여 주기적으로 ‘‘존재알림 (Hello) 패킷과 PT 네트워크 번호 광고 패킷을 교환하여 실시간으로 동적인 군 환경에 적응할 수 있는 프로토콜이 필요하다.

3.1 <존재알림> (Hello) 패킷 운영

보통 존재알림 패킷은 평문 형태로 보내고 광고 패킷은 암호문 형태로 멀티케스트 IPSec 터널을 통하여 보낸다. 광고 패킷이 멀티케스트되면 모든 IPSec 장치는 그물형으로 형성 되는 모든 터널의 원격 IPSec 장치에 소속된 SA 값들과 SPD 값들을 보유하게 된다.

2장에서 설명한 바와 같이 IPSec 장치에는 PT 인터페이스가 존재하는데, PT 네트워크로부터 오는 패킷들은 SPD 정보를 확인하고 선택된 SPD가 알려주는 SA 정보에 따라 암호화 처리되어 암호문 형태의 패킷으로 Blk 네트워크로 진입하게 된다. 즉, ESP 프로토콜에 의해 암호화 처리되어 Blk 네트워크를 가로

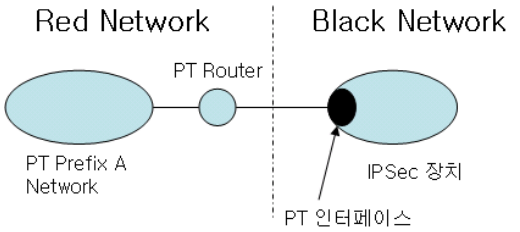

그림 5. SPD 정보에 따른 PT 네트워크 패킷의 Blk 네트워크 진입

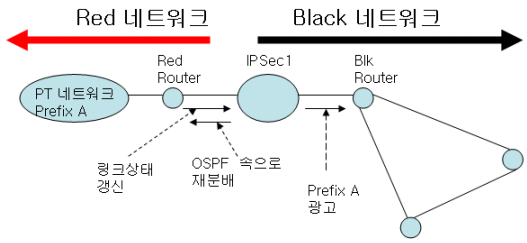

그림 6. IPSec 장치와 PT/CT (Red/Blk) 라우터

질러 나아가게 된다.

군용 Blk 네트워크의 운영 환경은 매우 동적이라는 것을 가정해야만 한다. Blk 네트워크를 구성하는 IPSec 장치는 적으로부터 공격을 당하거나, 이동 상황의 발생으로 잠시 동작불능 상태에 빠질 수 있다. 이 경우를 위하여 정상 동작하는 모든 IPSec 장치는 존재알림 패킷을 주기 T의 간격으로 보내게 된다. 그런데 어떤 원격 IPSec 장치로부터 4배의 존재알림 패킷 송출 주기 시간 동안 아무런 알림 패킷이 없으면, 그 IPSec 장치는 동작불능 상태인 것으로 간주한다. 이렇게 동작불능 IPSec 장치가 발견되면 이 원격 IPSec 장치와 관련된 모든 SPD가 지워지게 된다.

3.2 <PT 네트워크 번호 광고> 패킷 운영

동적으로 변화하는 군의 네트워크 환경을 지원하기 위하여 IPSec 장치는 라우팅 알고리즘인 OSPF (Open Shortest Path First)나 RIP (Routing Information Protocol)가 PT 인터페이스에서 작동하고 있어, PT 라우터 (그림에서 Red 라우터) 뒤에 연결된 PT 네트워크 번호들을 학습하게 된다.

Red 네트워크에서 Blk 네트워크 방향으로 일어나는 일을 살펴보면, OSPF/RIP 라우팅 프로토콜에 의하여 그림 6의 IPSec1에서는 PT 네트워크 번호 A 정보가 갱신되며, 이와 연관된 SPD 정보가 동적으로 갱신된다. 그리고 활동 모드인 경우 T 초 간격으로 지역 PT 네트워크 번호를 멀티케스트 형식으로 광고하게 된다. 반대로 Blk 네트워크에서 Red 네트워크 방향으로 일어나는 일을 살펴보면, 원격 IPSec 장치가 요청한 어떤 SPD 갱신 요청 정보는 PT 인터페이스를 통하여 OSPF/RIP 라우팅 프로토콜의 라우팅 테이블로 재분배 된다. 결과적으로 Red (PT) 라우터는 지역 IPSec1과 원격 IPSec 장치 사이에 원격 IPSec에 속한 PT 네트워크 번호들에 대한 SA와 SPD를 가지고 있을 경우에 국한하여 자신의 라우팅 테이블 안에 원격 PT 네트워크 번호에 해당하는 경로를 가지게 된다.

3.3 군용의 동적 네트워크 운영을 위한 요구 조건

CT 네트워크: CT 네트워크는 IP 멀티케스트 라우팅을 지원하여야만 하는데, IPSec 장치가 멀티케스트 호스트 역할을 담당해야 한다. 두개의 멀티케스트 주소가 필요하다. 하나는 평문 형식의 <존재알림>패킷들을 보내기 위하여 사용하고 다른 하나는 암호문 형식의 <PT 네트워크 번호 광고> 패킷들을 보낼 때에 사용한다.

PT 네트워크: IPSec 장치의 PT 인터페이스에는 RIP나 OSPF와 같은 AS (Autonomous System) 내부에서 동작하는 라우팅 알고리즘이 돌아가야 한다. 그래서 PT 인터페이스는 IPSec 장치가 직면하는 PT 네트워크들의 변화에 입각하여 동적으로 SPD를 갱신할 수 있게 한다.

키 관리: DMIDP는 IPSec 장치가 ESP 터널 모드로 동작하도록 요구하고 있다. 그렇다면 DMIDP는 프로토콜 키와 데이터 키를 요구한다. 프로토콜 키는 사전에 공유하고 있는 키이며 PT 네트워크 번호 광고 패킷을 멀티케스트 주소를 이용하여 IPSec 터널을 통하여 내 보낼 때 이 정보를 암호화 하기 위하여 사용한다. 또 하나의 키인 데이터 키는 PT 네트워크들 사이에 보내는 데이터를 암호화하기 위하여 사용하는 키이며 고정된 키를 사용할 수 있으나, IPSec 터널을 경유하는 트래픽에 대한 보안 관제가 이루어지도록 하려면 고정된 키 값들을 중앙 집중식으로 관리할 수 있도록 키 관리가 설계되어야 한다.

3.4 동작 불능 IPSec 장치 탐지

동일 원격 IPSec 장치로부터 존재알림 패킷이 4배의 존재알림 패킷 송출 주기 동안 없으면 DMIDP는 존재알림이 없는 IPSec 장치를 동작불능 상태에 빠졌다고 간주한다. 그러면 DMIDP는 동작불능 IPSec 장치와 관련된 모든 SPD 정보를 제거시킨다. 또 어떤 원격 IPSec 자치가 동작불능 상태에 빠진 이후에 정상 복귀되는 시점을 찾아낸다. 어떤 원격 IPSec 장치

가 복구되었을 때, 이 IPSec 장치와 관련된 모든 SPD 정보가 제거된다. 원격 IPSec 장치가 복구되었으나, 관련 SPD 정보를 제거한다는 것이 모순처럼 보일지 모르나 이것이 이 프로토콜의 특징이다. 이렇게 하는 이유는 오래된 정보의 불일치 문제를 차단하기 위함이다.

모든 IPSec 장치는 동일한 주기로 존재알림 패킷을 멀티케스트 주소로 보내주게 되는데, 이 패킷에 포함된 정보는 IPSec 장치가 새로운 동작을 시작한 시점의 Timestamp 값이 된다. 즉, 연속적인 존재알림 패킷은 모두 작동 시작 시점의 동일한 Timestamp 값을 멀티케스트하게 된다. 그렇다면 동일한 IPSec 장치로부터 수신한 존재알림 패킷의 Timestamp 정보가 바뀌었다면, 이 사실을 수신한 DMIDP는 그 IPSec 장치가 죽었다가 복구되었다는 것을 인식한다. 그러면 방금 복구한 그 IPSec 장치와 관련된 모든 현재까지의 SPD 정보를 지우게 된다. 그렇다면 이 IPSec 장치와 관련된 SPD 정보는 어떻게 다시 만들어지는가가 문제이다. 해결 방법은 간단하다. 새로운 SPD 정보는 복구된 IPSec 장치가 보내주는 <PT 네트워크 번호 광고> 패킷을 받고 난 후에 바로 새로운 SPD 정보가 만들어져 추가 된다.

3.5 대역폭 절약 모드 운영

동적으로 변화하는 네트워크 환경이지만 항상 변화하는 것은 아니다. PT 네트워크들이 변화가 없는 안정된 상태에 머무를 수가 있다. 이런 경우에는 해당 IPSec 장치는 <PT 네트워크 번호 광고> 패킷을 내보낼 필요가 없다. 지역 입장에서 [존재 알림 패킷 송출 주기×4] 시간 동안 아무런 SPD 정보 변화가 없으면 즉, 지역 PT 네트워크의 변화가 없으면 이 지역은 안정 상태가 된다. 이처럼 지역 IPSec 장치에서는 소속된 PT 네트워크의 변화가 없으면 대역폭 절약 모드로 동작하게 되는데, 이 경우 DMIDP는 최소 크기의 <존재 알림> UDP 데이터만 CT 네트워크로 멀티케스트 전송한다. 만약 SPD가 갱신되면 DMIDP는 절약 모드의 반대 개념인 활동 모드로 바뀌게 된다. 활동 모드에서 DMIDP는 안정 상태에 도달하기 전 까지 주기적으로 <PT 네트워크 번호 광고> 패킷을 송출하게 된다.

3.6 동적 라우팅

Blk 네트워크에서 하나의 터널 시작을 나타내는 IPSec 장치는 다른 모든 원격 IPSec 장치들에 대하여 완전한 그물형의 SA 및 SPD 값들을 보유하고 있다. Blk 네트워크를 통과하려고 유입되는 PT IP 패킷은 관련 SPD가 주어질 경우에 한하여 암호화 되어 적절한 IPSec 터널을 통과할 수 있다.

그림 1에서 IPSec3 장치에 연결된 PT 네트워크[C](Prefix(번호) C)가 문제가 생겨 동작불능 상태에 빠진 경우를 가정하자. 먼저 IPSecC는 지역의 PT 네트워크[C]가 죽은 것을 지역 라우팅 프로토콜의 도움으로 알아낸다. 그러면 IPSec3은 지역에 속한 변경된 PT 네트워크 번호들로 구성된 PT 네트워크 번호 광고 패킷을 만들어 Blk 네트워크 방향으로 멀티케스트한다. 그러면 IPSec3 지역의 PT 네트워크 변경 사실이 IPSec1과 IPSec2에게 알려지게 된다. 그러면 IPSec1과 IPSec2는 각각 IPSec3와 관련된 변경된 네트워크에 대한 SPD 정보를 갱신한다. 결과적으로, DMIDP는 지역 라우팅 프로토콜이 알려주는 네트워크 변화 정보를 획득하면 이 사실을 다른 모든 IPSec 장치들에게 광고하는 역할을 담당한다. 또 지역 IPSec 장치가 원격 IPSec 장치에 속한 PT 네트워크의 변화를 알았을 때, 이를 지역 PT 라우터에게도 바로 알려준다. 이는 IPSec 장치의 SPD 정보가 OSPF/RIP 라우팅 데이터베이스를 통하여 PT 라우터에게 전달되기 때문에 가능하다. 결과적으로 어떤 IPSec 장치가 원격 PT 네트워크에 대한 SPD 정보를 가지고 있다는 사실은 지역 PT 라우터에도 원격 PT 네트워크 번호에 대한 라우팅테이블 값, 즉 경로 값을 갖고 있다는 의미이다. 다른 말로 표현하면 지역 IPSec 장치에 원격 PT 네트워크에 대한 SPD 정보가 없으면 동일 지역 PT 라우터에도 이 원격 PT 네트워크 번호에 대한 경로 값이 없다는 의미이다.

IPSec 장치에서 작동하는 DMIDP는 임의의 PT 네트워크가 다른 구역의 IPSec 장치로 옮겨가는 것을 가능하게 한다. 그림 7에서 IPSec2는 PT 네트워크[B]가 이탈되었다는 사실을 PT 라우터 B의 OSPF/RIP 라우팅테이블이 알려준 정보로부터 탐지한다. 그러면 IPSec2의 DMIDP는 이 변경 사실을 광고패킷의 형태로 IPSec1과 IPSec3에게 알려준다. 이 광고 패킷을 받은 IPSec1과 IPSec3는 PT 네트워크[B]에 관한 SPD 정보를 제거하게 된다.

이동이 완료되어 새롭게 접속하는 경우를 그림 8에서 보여준다. IPSec3는 PT 네트워크[B]가 새롭게 접속되었다는 사실을 PT 라우터 C의 OSPF/RIP 라우팅 테이블이 알려준 정보로부터 탐지한다. 그러면 IPSec3의 DMIDP는 이 변경 사실을 역시 광고패킷의 형태로 IPSec1과 IPSec2에게 알려준다. 이 광고 패킷을 받은 IPSec1과 IPSec2는 PT 네트워크[B]에 관한

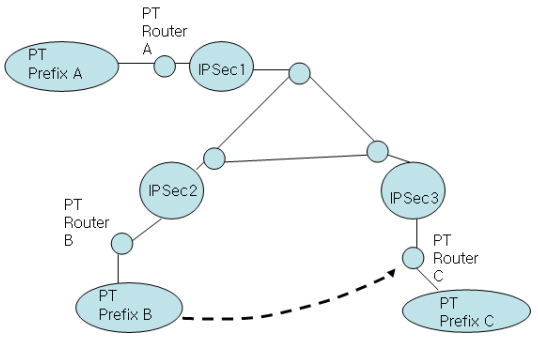

그림 7. IPSec2에서 PT 네트워크[B]의 이탈

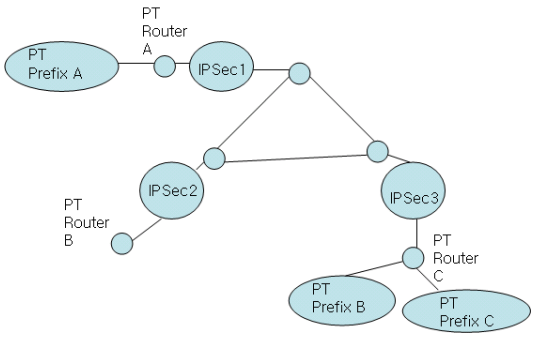

그림 8. IPSec3에 PT 네트워크[B] 신규 접속

SPD 정보를 새롭게 생성하게 된다.

Ⅳ. 군용 동적 환경 적응 중요 변수 설계

4.1 DMIDP 패킷 송출

존재알림패킷 송출주기 T: IPSec의 DMIDP가 주기적인 간격으로 자기 자신의 존재를 모든 다른 IPSec에게 멀티케스트한다. 이 주기 T 값은 평균적인 IPSec의 동작불능 상태 빈도에 따라 결정되어야 하나 RIP에서 광고 패킷을 30초 간격으로 내보내는 점을 고려할 때, T 값은 30초로 설정되는 것이 적절하다 (그림 9 참조).

활동모드/절약모드: T 값을 30초로 설정했을 경우에 2분 동안 어떤 IPSec 장치와 연관된 PT 네트워크 번호의 변화가 없으면 절약 모드로 운영된다. 절약 모드에서는 최소한의 알림 정보, 즉 해당 IPSec 번호와 Timestamp 값을 포함하는 4Bytes 정도의 정보만을 30초 주기로 멀티케스트한다. 절약모드가 아닌 기간은 활동 모드로 동작한다. 활동모드 기간 동안 관할 지역의 PT 네트워크 번호를 포함하는 광고 정보와 IPSec 번호 및 Timestamp 정보를 포함하는 (광고 + 알림) 패킷을 30초 주기로 멀티케스트 한다 (그림 9 참조).

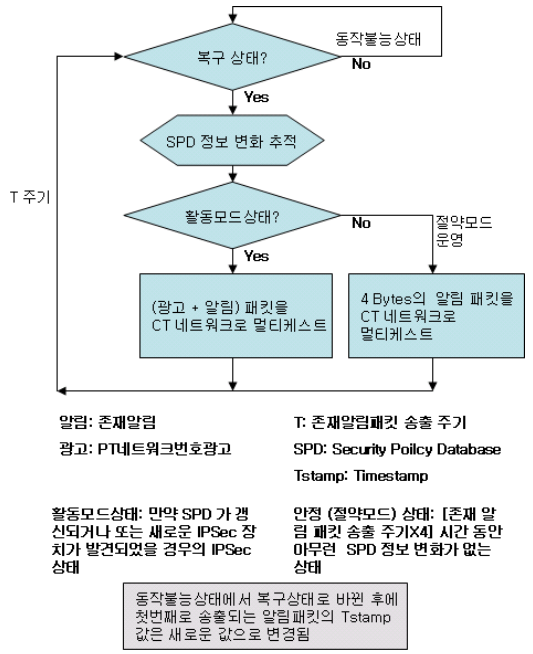

그림 9. IPSec에서 송출하는 DMIDP 패킷 운영

4.2 DMIDP 패킷 수신 처리

원격 IPSec 장치 동작불능 판단: 주기 T 값의 4배 시간, 즉 2분 동안 원격 IPSec 장치로부터 알림 패킷이 도달하지 않으면 해당 IPSec 장치가 동작불능 상태에 빠진 것으로 간주하고 해당 IPSec과 관련된 모든 SPD 정보를 제거 한다 (그림 10 참조).

원격 IPSec 장치 복구 판단: 원격 IPSec 장치로부터 수신한 알림 패킷 정보가 포함하고 있는 Timestamp 값을 추적한다. 만약 현재 값과 바로 이전 패킷의 값이 다른 상황이 발생하면 이IPSec 장치가 동작불능 상태에서 복구되었다고 판단한다. 바로 해당 IPSec과 관련된 모든 SPD 정보를 제거 한다 (그림 10 참조).

신규 SPD 정보 생성 시간: 원격 IPSec 장치로부터 수신한 광고 패킷 정보가 포함하고 있는 PT 네트워크 정보를 확인하고 변경된 네트워크 번호 (Prefix)가 있으면 이 새로운 네트워크에 관한 SPD 정보를 바로 생성한다. 광고 패킷이 30초 간격으로 멀티케스트되기 때문에 어떤 PT 네트워크가 이동 후에 새로 접속되어 서비스를 받기 위해서는 최대 30초의 시간이 필요하다. 즉, 새로운 PT 네트워크[X]에 대하여 다른 모든 PT 네트워크가 경로 정보를 갖기 위해서는 최대 30초의 시간이 필요하다 (그림 11 참조).

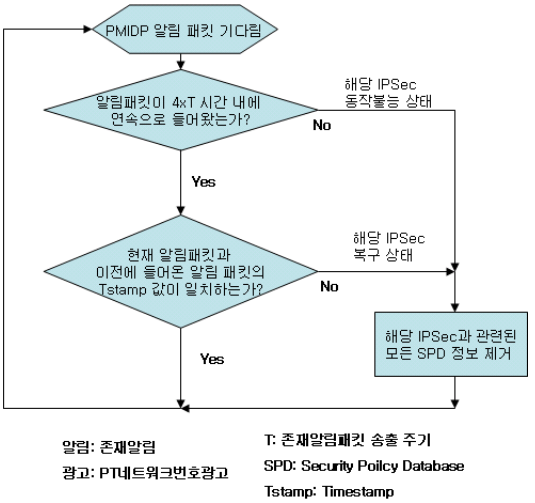

그림 10. IPSec 장치에서 DMIDP 존재알림 패킷 수신 후 처리

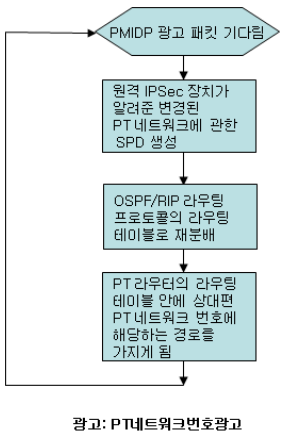

그림 11. IPSec 장치에서 DMIDP PT네트워크번호광고 패킷 수신 후 처리

4.3 제안 기법의 효율성 분석

군용 환경 적응을 위해 제안하는 기법에서는 존재알림패킷 송출주기 T를 30초로 제시하였으며, 2분 동안 어떤 IPSec 장치와 연관된 PT 네트워크 번호의 변화가 없을 경우 이 시간 이후를 절약 모드로 정의했다. 또 PT 네트워크 변화가 나타나면 다시 활동 모드로 변환되도록 하였다. 절약모드에서는 해당 IPSec 번호와 Timestamp 값을 포함하는 최소한의 정보만을 30초 주기로 멀티케스트하도록 하여 DMIDP용 패킷 트래픽 량을 획기적으로 줄일 수 있도록 하였다. 원격 IPSec 장치의 동작불능 판단 기준을 주기 T 값의 4배 시간, 즉 2분 동안 원격 IPSec 장치로부터 알림 패킷이 도달하지 않으면 해당 IPSec 장치가 동작불능 상태에 빠진 것으로 간주하고 해당 IPSec과 관련된 모든 SPD 정보를 제거하도록 하였다. 원격 IPSec 장치가 복구되었다고 판단하는 기준은 원격 IPSec 장치로부터 수신한 알림 패킷 정보가 포함하고 있는 Timestamp 값을 비교해 보았을 때, 현재 값과 바로 이전 패킷의 값이 다른 상황이 발생하면 이 IPSec 장치가 동작불능 상태에서 복구되었다고 판단하고 즉시 해당 IPSec과 관련된 모든 SPD 정보를 제거하도록 하였다.

특히 이동이 심한 전술 PT 네트워크의 운용을 위하여 필수적인 신규 SPD 정보 생성은 물리적으로 이동 접속 후 30초 내에 새로운 네트워크에 관한 SPD 정보를 바로 생성할 수 있도록 DMIDP 운용 관련 변수가 설정되었다.

V. 결 론

본 논문에서는 동적인 군용 PT 네트워크가 CT 네트워크인 Blk 네트워크에 접속되어 어떻게 통합 네트워크로 동작할 수 있는가를 제시하였다. 먼저 Blk 네트워크의 운용은 IPSec ESP 터널모드로 운용되지만 군 전용의 Blk 네트워크로 운영될 수도 있고, 상용 네트워크와 물리적으로는 공용으로 운영되나 논리적으로 군용과 상용이 완전 별개인 VPN Blk 네트워크 로 운영되는 두 가지 방안을 제시하였다. 두 번째 방안은 전방과 후방으로 멀리 떨어진 군용 PT 네트워크들을 상용의 네트워크를 공용하여 마치 군용 전용의 Blk 네트워크를 구성하는 것과 똑 같은 성능을 보장 받을 수 있도록 하는 중요한 기술이다. 군용으로 추가적인 비용 없이 상용의 네트워크 자원을 이용할 수 있는 기술이기 때문에 군용 네트워크의 녹색 기술이라 할 수 있다.

두 번째로 전술 환경에서 PT 네트워크들의 움직임이 심한 상황에서 지속적인 통신 서비스가 가능하도록 해주는 멀티케스트 기반의 IPSec 탐지 프로토콜 기술을 제시하였다. 특히 군용 동적 환경에 효과적으로 적응할 수 있도록 하는 DMIDP 운용에서 중요한 설계 변수인 존재알림패킷 송출주기 T를 30초로 제시하였으며, 2분 동안 어떤 IPSec 장치와 연관된 PT 네트워크 번호의 변화가 없을 경우 이 시간 이후를 절약 모드로 정의했고, PT 네트워크 변화가 나타나면 다시 활동 모드로 변환되도록 하였다. 절약모드에서는 최소한의 정보만을 30초 주기로 멀티케스트하도록 하였다. 원격 IPSec 장치의 동작불능 판단 기준을 2분으로 정의하고, 해당 IPSec 장치가 동작불능 상태에 빠진 것

으로 판단되면 해당 IPSec과 관련된 모든 SPD 정보를 제거하도록 하였다. 또 신규 SPD 정보 생성은 물리적으로 이동 접속 후 30초 내에 새로운 네트워크에 관한 SPD 정보를 바로 생성할 수 있도록 변수가 설정되었다.

향후 연구 과제로는 군용 Blk 네트워크를 상용의 네트워크를 활용한 VPN 형태로 운용할 때 작용 기술에 따른 CT 네트워크에서의 보안 강도 분석연구를 수행할 계획이다.

참 고 문 헌

〔1〕 INSC2/TASK2/DU/003, “Secure Multicast Architecture,” Office of Naval Research, the United States, Aug. 2004

〔2〕 INSC II/TASK1/D/002, “Test and Demonstration Architecture,” Office of Naval Research, the United States, Feb. 2005

〔3〕 정윤찬, 임진우, 황인용, 허미정, “멀티케스 기반의 Proactive IPSec 탐지 프로토콜의 설계,” 제12차 통신/전자 학술대회 프로시딩, 국방과학연구소(서울) 10월 2008

〔4〕 RFC 2407, “The Internet Security Association Key Management Protocol,” Nov. 1998

〔5〕 RFC 2401, “Security Architecture for the Internet Protocol,” Nov. 1998

〔6〕 RFC 2406, “IP Encapsulating Security Payload (ESP),” Nov. 1998

〔7〕 L. Gong, “Enclaves: Enabling Secure Collaboration over the Internet,” *IEEE J. Select. Areas Commun.,* pp.567-575, Apr. 1997

〔8〕 RFC 2409, “The Internet Key Exchange (IKE),” Nov. 1998

〔9〕 A. Perrig, D. Song, and J. Tygar, “ELK, a new protocol for efficient large-group key distribution,” *IEEE Security and Privacy Symposium 2001,* May. 2001

〔10〕 Brian J. Matt, Matt Mundy, “Adaptive Multicast Key Management for Tactical Networks,” *IEEE MILCOM,* pp.1-10, Oct. 2006

〔11〕 Trung H. Tran, “Proactive Multicast-based IPSec Discovery Protocol and Multicast Extension,” *IEEE MILCOM,* pp.1-7, Oct. 2006

정 윤 찬 (Younchan Jung) 정회원

1980년 2월 경북대학교 전자공학과 졸업

1990년 2월 KAIST 전기 및 전자공학과 석사

1994년 8월 KAIST 전기 및 전자공학과 박사

1996년 3월~현재 가톨릭대학교 정보통신전자공학부 교수

<관심분야> 네트워크 QoS, VoIP, 네트워크 보안, 군 통신 네트워크 설계