이동성과 보안성 있는 멀티케스트 통신을 위한 군용 그룹 키 관리

정회원 정 윤 찬

Military Group Key Management for Mobile and Secure Multicast Communications

Younchan Jung* ***Regular Member***

요 약

군용 네트워크에서는 이동성과 보안성을 지원하기 위하여 네트워크의 물리적 구성 형태와 상관없이 IPSec ESP 터널들이 Full mesh 형태로 IPSec 장치들을 연결하고 있으며 이 장치들 간에는 멀티케스트 통신이 필요하다. IPSec 장치들은 변화하는 IPSec 터널들을 지원하기 위하여 멀티케스트 그룹키를 동적으로 갱신시킬 수 있어야 한다. 또 특정한 그룹을 형성하는 전술 단말 측면에서도 그룹 구성원 간에 보안성 있는 멀티케스트 통신을 제공해 주어야 한다. 이러한 단말 그룹 구성원의 이동성을 지원하기 위해서는 멀티케스트 그룹 키가 동적으로 갱신되어야 만 한다. 본 논문에서는 기존의 Diffie-Hellman (DH) 키 교환 방식 기술과 키 Tree 기술을 활용하여 동적인 상황변화에 따라 보안성 있게 그룹 키를 관리할 수 있도록 하는 방법을 제시한다. 제시하는 동적인 Tree 기반 키 관리의 장점은 변화가 심한 그룹 구성원이 서로 상대방으로부터 주기적으로 상황 정보를 받도록 하여 변화하는 상황에 맞추어 효과적으로 그룹 키를 갱신할 수 있다는 점이다.

Key Words : Military Networks, IPSec Tunnels, Tactical Terminals, Multicast Communications, Group Key Management, Key Tree

ABSTRACT

In mobile and secure military networks, full-meshed IPSec tunnels, which do correspond to not physical links but logical links between each IPSec device and its peer, are required to provide multicast communications. All IPSec devices need support in changing IPSec tunnels by a way of using a multicast group key which is updated dynamically. Tactical terminals, which often constitute a group, need also secure multicast communications in the same group members. Then, the multicast group key is required to be updated dynamically in order to support group members' mobility. This paper presents challenging issues of designing a secure and dynamic group key management of which concept is based on the Diffie-Hellman (DH) key exchange algorithm and key trees. The advantage of our dynamic tree based key management is that it enables the dynamic group members to periodically receive status information from every peer members and effectively update a group key based on dynamically changing environments.

* 가톨릭대학교 정보통신전자공학부 통신네트워크 연구실ycjung@catholic.ac.kr)
논문번호 : KICS2010-03-139, 접수일자 : 2010년 3월 31일, 최종논문접수일자 : 2010년 6월 7일

Ⅰ. 서 론

상용 네트워크가 ALL IP 컨버전스 네트워크로 발전하고 있는 것과 마찬가지로 군용 네트워크도 향후 10년 안에 IP 기반의 통합 네트워크로 전환될 것이다[1,2]. 군용 IP 네트워크는 보안성을 위하여 IPSec 기술을 사용할 수밖에 없으며, 이 때 키 교환 기술은 군용 IPSec 운용의 핵심 기술이 될 것이다. IPSec의 키 교환은 상용에서는 IKE (Internet Key Exchange (IKE) 기술의 사용이 권장되고 있다. 그러나 IKE에서는 오직 양자간 통신을 위한 키 교환 기술 표준이 정립되어 있다. 즉, IKE는 양자간 일대일 통신을 고려한 키 교환 방식일뿐만 아니라 이동 상황에서의 고려도 충분치 못한 실정이다. 그래서 동적인 군용 환경을 고려하고 지휘선 상의 그룹이 함께 통신할 수 있는 멀티캐스트 통신을 위한 MIKE (Multicast Internet Key Exchange) 기술의 연구가 시작되었다[3].

군이 이용하게 될 IP 기반 통합네트워크는 전략과 전술 부대를 모두 수용하는 형태가 될 것이며 기본적인 모습은 그림 1의 모습으로 가정할 수 있다[3]. 여기서 Black 네트워크는 네트워크의 물리적 구성 형태와 상관없이 그림에서 점선으로 표시된 것과 같은 IPSec ESP (Encapsulating Security Payload) 터널들이 완전 그물형으로 IPSec 장치 사이를 연결하게 된다. 접속 네트워크로 볼 수 있는 출발지 PT (Plain Text) 네트워크에서 발생한 패킷들은 Black 네트워크가 제공하는 IPSec ESP 터널의 입구에 해당하는 지역 IPSec 장치를 출발하여 터널 출구에 해당하는 원격 IPSec 장치에 도달할 때 까지 보안성 있는 터널 경로를 통하여 운반된다. 이 원격 IPSec 장치는 패킷을 목적지 PT 네트워크로 보내주게 된다.

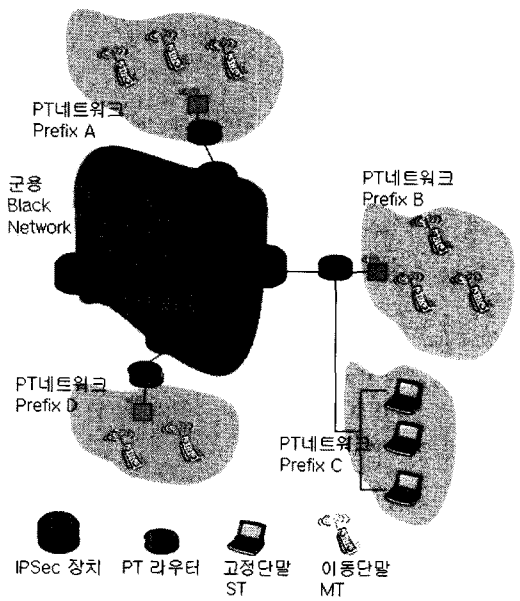

그림 1. ALL IP 기반 군 통신 네트워크의 운영

ESP 터널의 시작과 끝이 되는 IPSec 장치는 작전상 이동 상황 발생으로 장비가 동작불능 상태로 빠질 수가 있으며, 적의 공격에 의해서도 또한 운영이 멈출 수도 있다. 또 PT 네트워크도 작전상 이동 상황이나 적의 공격으로 접속 상황이 항상 변화할 수 있다. 군 네트워크와 상용의 네트워크가 다른 점은 각각의 IPsec 장치는 자신을 제외한 원격의 모든 IPSec 장치와 그 원격 IPSec 장치에 접속된 PT 네트워크의 상황정보를 파악하여 유지하고 있어야만 한다. 이러한 상황정보를 주고받기 위하여 IP 기반 네트워크에서 만이 가능한 멀티캐스트 통신 기술이 이용된다[3].

중요한 문제는 IPSec 장치 그룹의 멀티캐스트 통신에 이용되는 그룹 암호화 키 (그룹 키) 값을 어떻게 확보하는가 하는 과제이다[4-7]. 물론 사전에 이 그룹 키를 공유할 수도 있으나 군의 전술 네트워크와 같이 변화가 동적으로 일어날 수 있는 상황에서 수동으로 키 값을 자주 바꾸기란 시간도 많이 소요될 뿐만 아니라 신뢰성도 떨어진다. 왜냐하면 이런 목적의 그룹키는 IPSec 장치 중 하나라도 동작 불능이 되었다거나, 적의 공격이 예상될 때 또는 동작 불능상태에서 복구되는 시점에 이 그룹 키 값을 새로운 값으로 일률적으로 변경시켜 주어야 하기 때문이다. 이 논문에서는 먼저 IPSec 장치에서 사용할 멀티캐스트용 그룹 키 (IPSec 그룹 키)를 관리하는 알고리즘에 관한 연구를 수행한다.

두 번째 문제는 이동 단말이나 고정단말들의 어떤 특정한 그룹 내에 멀티캐스트 통신이 이루어져야 하는데, 이 때 보안성 있는 통신을 위해서는 단말 그룹 암호화 키 값이 확보되어야 한다. 그룹 구성 단말이 그룹 키를 공유하는 문제도 상용 운영 방식과는 완전히 다르다. 그룹 중 하나의 멤버가 갑자기 불통되거나 불통되었다가 복구될 때, 또는 신규 멤버가 그룹에 진입할 때의 모든 상황에서 이 그룹이 사용하는 그룹 키 (단말 그룹 키) 값을 변경해 주어야 한다. 이 논문에서는 동적 상황에 적응한 IPSec 그룹 키와 단말 그룹 키의 변경 방법을 연구하는 것이 최종 목표이다.

Ⅱ. 멀티캐스트 키 공유 기본 기술

2.1 Diffie-Hellman 방식 키 교환

Diffie-Hellman (DH) 방식은 두 사용자 간에 동일

키 값을 필요할 때 마다 생성하여 보유하는 방식이다[8,9]. 먼저 두 사용자 (Ui와 Uj)는 모두 소수인 어떤 q 값과 q 값의 원시근인 p 값을 알고 있다고 가정한다. Ui는 자신만이 알고 있는 비밀 값 k_i를 이용하여 블라인드 키 (*Blind Key*) $BK(k_i) = (q^{k_i}) \bmod p$를 만들어 Uj에게 보내준다. 마찬가지로 Uj는 자신만이 알고 있는 비밀 값 k_j를 이용하여 블라인드 키 $BK(k_j) = (q^{k_j}) \bmod p$를 만들어 Ui에게 보내준다. Uj의 블라인드 키를 받은 Ui는 다음식과 같이 k_{ij}를 구한다.

$$k_{ij} = (BK(k_j))^{k_i} \bmod p := k_i \circ BK(k_j) \quad (1)$$

또 마찬가지로 Ui의 블라인드 키를 받은 Uj는 다음식과 같이 k_{ji}를 구한다.

$$k_{ji} = (BK(k_i))^{k_j} \bmod p := k_j \circ BK(k_i) \quad (2)$$

결국 정수론에 따라 k_{ij}와 k_{ji}는 동일 값이 되므로 Ui와 Uj는 안전하게 동일 키 값을 보유할 수 있게 된다.

이처럼 두 사용자간에 동일 키를 보유할 수 있는 DH 방식을 확장하여 여러 멀티케스트 그룹 멤버가 그룹 키를 보유할 수 있게 하는 방법은 주로 키 Tree를 이용한다.

2.2 키 Tree

키 Tree를 사용하면 동적인 상황변화에 적응하여 신속한 그룹 키의 관리가 가능해진다[10,11]. 그림 2에서와 같이 8명의 멀티케스트 그룹인 경우를 가정하자. Tree의 각 노드는 고유번호와 위치 정보를 갖는다. 키 Tree의 특징은 모든 노드는 동일한 숫자의 자식을 갖는다. 이것을 Tree 정도 (Degree)로 표현하는데, 그림 2는 Tree 정도가 3인 경우이다. 사용자는 자기 자신으로부터 정점의 노드에 이르는 직접경로 상에 있는 키 값들만 알고 있다. 키 Tree의 정점 노드에 해당하는 키가 그룹 키 k_G가 되며 모든 그룹 멤버가 이를 공유하게 된다. 예를 들어 사용자 u_8은 k_8, k_{78}, $k_{1\text{-}8}$을 보유하는데 $k_{1\text{-}8}$은 k_G가된다. 키 패킷의 형태로 사용자 끼리 키 Tree에 관한 정보가 교환된다. 이 패킷들은 특정 노드의 위치에 해당하는 이 노드의 키 값을 포함하고 있다.

Tree의 운영은 집중식 방식과 분산식 방식으로 나눌 수가 있는데, 차이점은 III 장에서 상세하게 다루어진다.

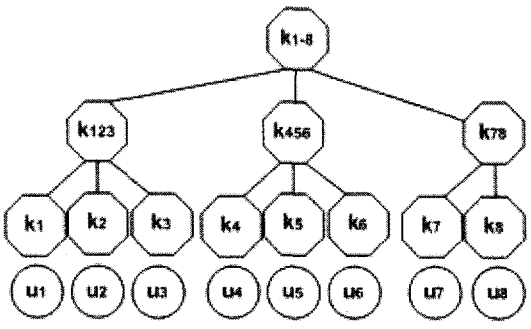

그림 2. 키 Tree

III. 멀티케스트 그룹 키 교환 방식 설계

3.1 IPSec 멀티케스트 그룹 키 교환 방식

IPSec ESP 터널들로 구성되는 Black 네트워크에서 멀티케스트 목적으로 이용될 그룹 키를 동적인 변화에 적응하여 IPSec 장치들이 공동으로 소유할 수 있게 해야만 한다. 이 경우는 집중식 분배 모드를 사용한다[12,13]. 집중식 분배 모드에서는 GC (Group Controller)가 키 Tree를 만들고 안전한 방법으로 그룹 키를 분배한다. 즉, 변화하는 상황을 확인하고 중앙에서 새로운 그룹 키를 분배할 수 있는 GC가 필요하다. 문제는 GC가 그룹 키 갱신의 판단 기준이 되는 정보를 어떻게 얻을 수 있는가 하는 점이다. 본 논문에서 제안하는 방법은 그림 4와 같이 모든 IPSec 장치는 존재알림 패킷을 주기 T 간격으로 GC에게 보내주어야 한다. 단 여기서 존재 알림 패킷은 암호화하지

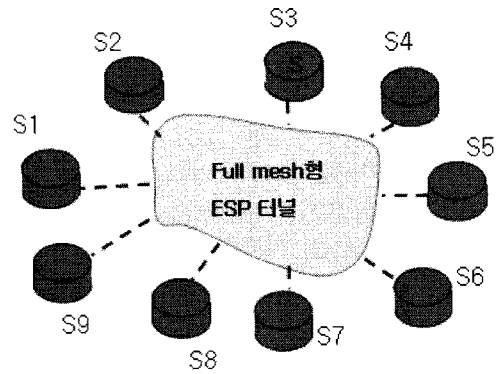

그림 3. IPSec 장치들 간의 멀티케스트 그룹 키

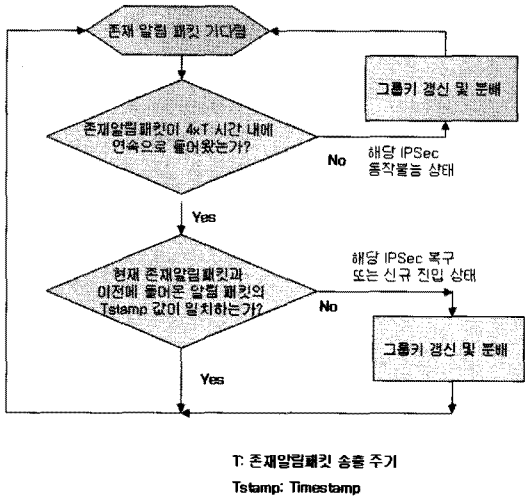

그림 4. GC의 그룹키 갱신 시점 파악

않은 형태로 보낸다. 모든 IPSec 장치로부터 존재알림 패킷을 받은 GC는 그룹 키를 갱신해야 할 시점을 판단하고 적절한 그룹 키 분배 절차로 들어간다.

집중식 분배 모드는 GC가 Tree와는 별도로 존재해야 하고, 키 트리와 멤버의 관리 및 그룹 키를 그룹 멤버에게 분배 역할을 담당한다. 즉, GC는 콘트롤러 자체일 뿐, 키 트리의 부분이 아니지만 키 트리의 구조와 모든 키를 알고 있다. 반면에, 각 멤버는 키 트리에 대한 정보가 없고, 오직 자신으로부터 정점노드까지의 경로에 속한 노드에 해당하는 키만 알고 있다.

집중식 분배 모드 주요 원리는 그룹 멤버 간에 데이터를 교환할 때, 키 트리의 보조키를 사용하여 서브 그룹과 안전한 통신을 하는 것이다[3]. 이때의 보조키는 오직 서브 그룹만이 알고 있다. 예를 들어, 그림 2에서 GC는 첫 번째 서브 그룹의 멤버인 u_1, u_2, u_3에게 보조키인 k_{123}으로 그룹 키 k_{1-8}을 암호화한 후에 보내준다. 즉, 이 때 GC에서 u_1, u_2, u_3에게 전송되는 패킷은 k_{1-8}이 k_{123}을 사용하여 암호화된 $\{k_{1-8}\}_{k_{123}}$이 된다.

그림 5는 집중식 분배 모드에서 그룹 멤버 중 u_9이 4×T 시간 동안 GC로 존재알림 패킷을 보내지 않아, GC는 Tree에서 u_9을 제거시키고 나머지 그룹 멤버들이 바로 그룹 키를 갱신할 수 있도록 하는 과정을 설명한다. GC는 새로운 그룹 키를 생성하고, 모든 그룹 멤버들에게 키 패킷이 포함되어 있는 키 갱신 요청 메시지를 멀티캐스트 한다. 이 메시지는 $\{k_{1-8}\}_{k_{123}}$, $\{k_{1-8}\}_{k_{456}}$, $\{k_{1-8}\}_{k_{78}}$, $\{k_{78}\}_{k_7}$, $\{k_{78}\}_{k_8}$ 정보로 구

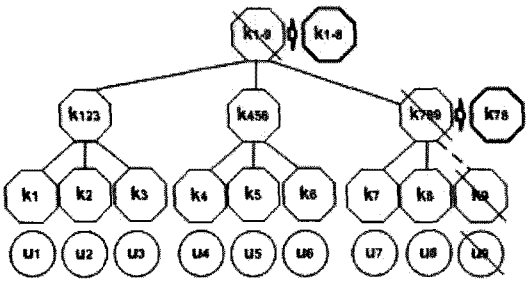

그림 5. 집중식 분배 모드에서 u_9이 Tree에서 제거될 때의 그룹 키 갱신

성되어 있다. 이 정보는 그룹에 남아 있는 모든 멤버들이 각각 수신하게 되고, 각각 필요한 정보를 활용하여 새로운 그룹 키 $k_G = k_{1-8}$를 보유하게 된다. 예를 들어 u_7은 메시지 정보 가운데, $\{k_{78}\}_{k_7}$을 자신의 k_7을 사용하여 복호화하여 k_{78} 먼저 구한다. 그 다음에 k_{78}을 사용하여 $\{k_{1-8}\}_{k_{78}}$을 복호화하여 새로운 그룹키인 k_{1-8}을 얻게 된다. 이 시점 이후 멀티캐스트 그룹의 그룹키는 k_{1-9}가 아니고 k_{1-8}이 사용된다.

3.2 IP 단말 멀티캐스트 그룹 키 교환 방식

상용의 무선 단말이 4G (4세대) 형태로 발전하고 유선 단말도 ALL IP 단말로 발전하는 것과 같이 차기 군에서 사용하는 단말도 IP 단말 형태가 될 것이다. IP 단말이 갖는 중요한 장점 중 하나는 원하는 그룹끼리만 통신하는 멀티캐스트 통신이 쉽게 구현될 수 있다는 점이다. 이렇게 되면 군의 역할 분담에 따라 구성되어 있는 그룹들 간의 멀티캐스트 통신이 쉽게 이루어질 수 있다. 같은 목적의 지휘 통제 선상에 있는 그룹이 함께 통신에 참여할 수 있다 (그림 6 참조). 이 경우도 보안성 있는 통신을 하기 위해서는 멀티캐스트 그룹이 공동의 그룹 키를 사용해야 한다. 그런데, 특히 전술 영역의 사용자들은 이동이 심하고 언제든지 적으로부터 공격을 받을 가능성이 더 높다. 그룹 멤버들 중 어떤 멤버에 상황 변화가 일어나면 빨리 나머지 그룹 멤버들은 그룹 키를 새로운 값으로 변경할 수 있어야 한다. 그런데 어떤 사용자의 단말에 문제가 발생하면 그 사용자가 개입하여 이 사실을 알려줄 수 있는 방법이 없다. 이런 이유 때문에 존재 알림 패킷을 주기적으로 멀티캐스트 해 주어야 한다.

단말 멀티캐스트 그룹을 위하여 분산식 동의 모드가 이용될 수 있다. 이 분산식 동의 모드에서는 멤버들 중 하나는 TM(Transaction Manager)이 되고, 오직

TM 만이 키 Tree를 갱신할 수 있고 그룹 키를 바꿀 수 있다[12,14]. TM은 집중식 분배 모드에서 처럼 고정되어 있는 것이 아니고 멤버 가운데 한 명이 TM이 되며 시간에 따라 TM 역할을 하는 멤버가 바뀌게 된다. 그러므로 각 멤버는 현재 어느 멤버가 TM인지를 알 수 있는 TM 상태 정보를 가지고 있다.

그림 7은 분산식 동의 모드에서 새로운 그룹 키로 갱신되는 과정을 보여준다. 먼저 u_8 이 그룹으로 신규 진입되는 경우를 살펴보자. u_8 은 암호화하지 않은 형태로 멀티케스트 주소를 이용하여 새로운 자신의 존재를 알린다. 이 정보를 받은 현재의 TM (그림 8에서 u_1)은 인증 과정을 거쳐 u_8 을 새로운 멤버로 인증하고 u_8 로부터 블라인드 키 BK(u_8)을 받는다. 이 과정이 새로 진입하는 사용자와 TM 사이에 이루어지는 초기 3 way handshake 과정이다. 그러면 TM에서는 BK(u_8)을 저장함으로서 새로운 노드가 키 Tree에 추가된다. 그리고는 새로운 노드로 부터 정점 노드까지의 경로 (그림 7에 가는 점선으로 표시)가 무효화된다. 다음으로 현재의 TM인 u_1 은 그림 8에서 표시한 'BK 키 정보 메시지'를 기존의 그룹멤버들과 새로운 멤버인 u_8 에게 함께 보낸다. 이 메시지는 무효화된 Tree 경로를 제외한 모든 Tree의 블라인드 키들을 포함하고 있으며 u_8 이 새롭게 TM 역할 임무를 수행할 것이라는 정보도 포함하고 있다. 'BK 키 정보 메시지'를 받은 u_8 은 새로운 TM 임무를 확인한다는 메시지를 u_1 에게 보내 주는 것을 시작으로 이후부터는 자신이 TM이 되는 것이다. 새롭게 TM이 된 u_8 은 곧바로 새로 유효화된 Tree 경로 (그림 7에 굵은 점선으로 표시)에 대한 블라인드 키를 계산한다. 그리고 'BK 키 갱신 정보 메시지' 에 BK(k_{78}), BK

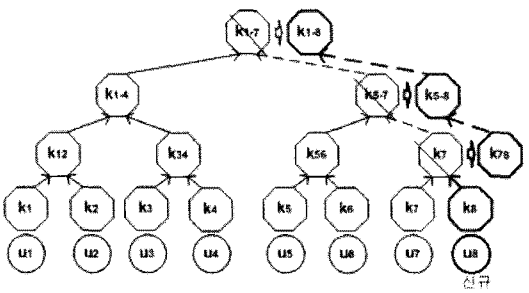

그림 7. 분산식 동의 모드에서 신규로 u_8 이 참여할 때의 그룹 키 갱신

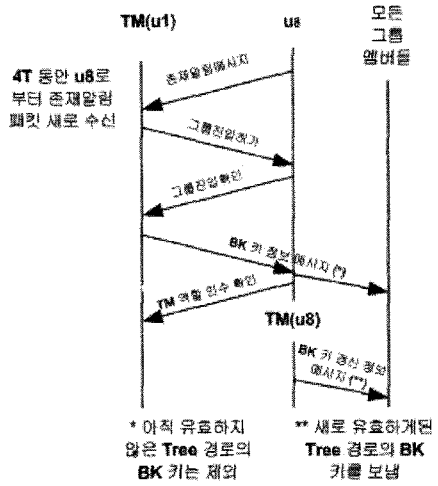

그림 8. 분산식 동의 모드에서 신규로 u_8 이 참여할 때의 TM 변경 및 그룹 키 갱신 절차

(k_{5-8})을 포함시켜 모든 그룹 멤버들에게 보내준다.

u_8 의 신규 멤버 가입으로 그림 8의 절차가 완료되면 u_2 가 새로운 그룹 키를 계산하는 식을 예로 들면 다음과 같다.

$$k_G = k_{1-4} \circ BK(k_{5-8}) \tag{3}$$

또 u_6 가 새로운 그룹 키를 계산하는 과정을 하나 더 예를 들면 다음과 같다.

$$\begin{aligned} k_{5-8} &= k_{56} \circ BK(k_{78}), \\ k_G &= k_{5-8} \circ BK(k_{1-4}) \end{aligned} \tag{4}$$

3.3 제안한 멀티케스트 그룹 키 교환 방식 특징

표 1에 집중식 분배모드와 분산식 동의모드의 특징을 비교 정리하였다. IPSec 장치들의 암호화된 멀티케스트 통신을 위해서는 집중식 분배 모드가 적절하다. 단점으로는 중앙 집중식으로 운영될 경우에는 GC의 생존성과 접근성이 확보되어야 한다. 이 문제를 해결하기 위해서는 1차 GC (Primary), 2차 GC (Secondary) 개념의 생존성 있는 GC 운영 개념이 정립되어야 할 것이다.

전방 정찰 멤버와 이들의 지휘 통제 선 상에 있는 멤버들 그룹이 보안성 있는 멀티케스트 통신을 할 수 있도록 하기 위해서는 분산식 동의 모드에 의한 그룹 키 교환 방식이 적절하다

표 1. 운영 모드에 따른 기술적 특징

운영 모드	집중식 분배 모드	분산식 동의 모드
키 생성	중앙	그룹의 멤버 자신
그룹키 생성 관여자	1	그룹의 모든 멤버
콘트롤러	고정적	동적
그룹 사이즈	제한 없음	소규모 그룹용
의도 목적	Black 네트워크를 구성하는 Full mesh형 ESP 터널의 이동성을 지원하고 보안성 있는 통신환경을 제공하기 위한 멀티케스트 그룹 키 교환	전방 정찰 부대와 같이 소규모 그룹들이 동적으로 변화가 심한 상태에서 보안성 있는 멀티케스트 통신을 할 수 있도록 하는 그룹 키 교환
멤버 상황 변화 인식 방법	멤버들이 내보내는 멀티케스트 존재알림 패킷 (암호화 안 됨)	좌동
존재알림패킷 송출 주기 T	30초	30초
동작불능 상태 간주 범위	2분 동안 존재알림 패킷이 없을 때	좌동

실제 운용 환경에서 전방과 후방 간의 연결에서 두 가지 모드가 혼용되어 사용되는 경우를 가정할 수 있다. 이 경우 후방의 집중식 분배 모드에서는 문제가 되지 않는다. 그 이유는 중앙의 서버가 키를 관리하기 때문이다. 문제는 전방에서 분산식 동의모드를 사용할 경우, 100% 분산 모드 운영에 맡겨 둔다고 가정하면 문제될 것이 없다. 그러나 만약 보안 관제 등의 목적으로 중앙에서 현재 전방에서 사용 사용 중인 그룹키를 알아야 할 필요가 있는 경우에는 분산식 동의 모드 방식은 심각한 문제를 야기할 수 있다. 만약 보안 관제를 위해 필요하다면 분산식 동의 모드에서 사용하는 그룹키 값이 변경될 때 마다 중앙 집중식으로 운영되는 후방의 서버에게 보고하도록 프로토콜이 개발되어야 한다.

특히 군 전술통신은 단말뿐만 아니라 네트워크도 이동이 많다고 가정하여야 하고, 적의 공격으로 동작불능 상태에 빠질 수 있다는 점을 고려하여야 한다. 본 논문에서 제안하는 단말 또는 네트워크의 상황변화를 인식하기 위하여 네트워크의 IPSec 장치와 단말로부터 존재알림 패킷을 주기적으로 멀티케스트하는 개념을 제안했다. 이동하는 전술 상황에서 IPSec 장치이건 단말이건 상관없이 동작 불능상태에 빠질 때에 이를 다른 장치가 알아낼 수가 없다. 그러므로 정상적인 상태에서는 주기적으로 존재알림패킷을 멀티케스트하고 반대의 상황에서는 상대방이 존재알림 송출이 정지된 장치를 동작불능 상태로 인식하도록 하고 있다. 이 논문에서 제안한 존재알림 패킷 송출 주기는 상용의 RIP 프로토콜이 네트워크 번호 광고 패킷을 송출하는 주기인 30초와 동일하게 맞추었다.

Ⅳ. 결 론

군용의 Black 네트워크는 네트워크의 물리적 구성 형태와 상관없이 IPSec ESP 터널들이 완전 그물형으로 IPSec 장치들을 연결하게 된다. 변화가 심한 동적 군 전술 네트워크 환경에 적응하기 위하여 IPSec 장치 그룹은 멀티케스트 통신이 요구되며 이를 위해 그룹 암호화 키를 필요로 한다. IPSec ESP 터널들로 구성되는 Black 네트워크에서 멀티케스트 목적으로 이용될 그룹 키를 동적인 변화에 적응하여 IPSec 장치들이 공동으로 소유할 수 있게 하기 위하여 집중식 분배 모드를 제안하였다.

군의 전술 네트워크 단말들의 어떤 특정한 그룹 내에 멀티케스트 통신이 이루어져야 하는데, 이 때 보안성 있는 통신을 위해서는 단말 그룹 암호화 키 값이 확보되어야 한다. 이를 위하여 분산식 동의 모드를 제안하였다.

본 논문에서는 제시한 방식의 기본은 Diffie-Hellman 키 교환 방식과 키 Tree를 사용하여 동적인 상황변화에 따라 신속히 그룹 키를 관리할 수 있도록 한 것이다. 특히 군 전술통신은 단말뿐만 아니라 네트워크도 이동이 많고, 적의 공격으로 동작불능 상태에 빠질 수 있기 때문에 이 상황변화를 실시간으로 다른 장치가 알아내는 것은 쉽지 않다. 이 논문에서는 주기적으로 평문 형태의 존재알림패킷을 멀티케스트하도록 하여, 그룹 멤버가 임의 장치의 정상운영/동작불능 상태를 실시간 추적 인식하도록 하고 있다.

참 고 문 헌

[1] INSC2/TASK2/DU/003, "*Secure Multicast Architecture*," Aug. 2004

[2] INSC II/TASK1/D/002, "Test and Demonstration Architecture," Feb. 2005

[3] Trung H. Tran, "Proactive Multicast-based

IPSec Discovery Protocol and Multicast Extension," *IEEE MILCOM,* pp.1-7, Oct. 2006

[4] T. Aurisch, "Using key trees for securing military multicast communication" *IEEE MILCOM,* Vol.3, pp.1377-1383, 2004

[5] C. Wong, M. Gouda, and S. Lam, "Secure Group Communications using Key Graphs," *ACM SIGCOMM'98,* 1998

[6] RFC 2627, D. Wallner, E. Harder and R. Agee "Key Management for Multicasts: Issues and Architectures,", Jun. 1999

[7] S. Rafaeli, L. Mathy, and D. Hutchison, "EHBT: An efficient protocol for group key management," *Third International COST Workshop (NGC 2001),* Nov. 2001

[8] RFC 2409, "The Internet Key Exchange (IKE)," Nov. 1998[2]

[9] RFC 2407, "The Internet Security Association Key Management Protocol," Nov. 1998

[10] C. K. Wong, M. G. Gouda, S. S. Lam, "Secure group communications using key graphs," *ACM SIGCOMM'98,* 1998

[11] T. Aurisch, "Using key trees for securing military multicast communication", *IEEE Milcom 04,* 2004

[12] T. Aurisch, "Optimization Techniques for Military Multicast Key Management," *IEEE MILCOM,* Vol.4, pp.2570-2576, 2005

[13] 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

[14] 정윤찬, 임진우, 김석중, 권오주, "군 네트워크에서 멀티캐스트 기반의 키 관리 기법 설계," *제12차 통신/전자 학술대회 프로시딩, 국방과학연구소(서울)* 10월 2008

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