제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 (2003.5)

VPN망에서 MIPv6 이동성 해결 방안에 관한 연구

김덕기*, 문영성**
*한국관광대학 디지털콘텐츠과
**숭실대학교 컴퓨터학과
e-mail:alberto1@ktc.ac.kr*,mun@computing.ssu.ac.kr**

A Study on MIPv6 Mobility Solution in the VPN

Duckki Kim*, Youngsong Mun**
*Dept of Digital Contents, Korea Tourism College
**Dept of Computer Engineering, Soongsil University

요 약

최근 초고속인터넷의 급속한 확장과 무선 핫스팟(Hotspot)의 등장은 인터넷을 컴퓨터 통신의 중심에 두게 되었다. 이는 다양한 컴퓨터 통신의 매체들이 인터넷으로 통합되는 것을 의미하며 이러한 통합은 통신망의 물리적, 논리적인 구조에 많은 영향을 미치게 되었다.

본 논문은 Mobile IPv6와 VPN이 상호 연동하는 시나리오에서 발생되는 문제들을 추적한다. 끊김 없는 이동성을 제공하기 위해 제시된 솔루션을 분석하여, VPN 게이트웨이와 연동하는 GHA(Gateway Home Agent)의 하드웨어적인 구현을 제안하며 IPSec Based VPN이 아닌 환경과 새로이 제안된 내용들을 추가하여 성능분석이 가능한 테스트 베드의 구축을 제안한다.

1. Introduction

최근 초고속인터넷의 급속한 확장과 무선 핫스팟의 등장은 인터넷을 컴퓨터 통신의 중심에 두게 되었다. 이는 다양한 컴퓨터 통신의 매체들이 인터넷으로 통합되는 것을 의미하며 이러한 통합은 통신망의 물리적, 논리적인 구조에 많은 영향을 미치게 되었다. 이러한 통신망의 변화 중 가장 중심에 있는 것이 '이동성'을 보장하는 것이었다. 이를 위해 제안된 Mobie IP(MIP)[1]는 IP 주소를 기반으로 한 광범위한 이동성을 지원하는 해결 방안이다. Mobile IP에 의하면 Mobile Node(MN)은 자신의 홈 링크에 영구적인 Home Address를 가지고 있으며 방문한 링크로부터 임시적인 Care-of-Address(CoA)를 갖게 된다. 이때 홈 네트워크에 있는 라우터를 Home Agent(HA)라 부르며 HA는 MN이 다른 네트워크를 방문하여 등록하면서 받게 되는 CoA의 캐시를 관리한다.

이동성에 대한 관심과 함께 최근 많은 기업에서는 본사와 지사간의 중요한 데이터의 처리를 위해 전용선을 사용하던 방식을 바꾸어 인터넷 망을 이용한 가상 전용선 방식인 VPN(Virtual Private Network) [2], [3]을 도입하게 되었다. 이 VPN은 기존의 전용선과는 달리 인터넷 망을 그대로 사용하고 있기 때문에 비용이나 시간 등의 많은 절감을 기대할 수 있게 되었다.

Mobile IP의 등장은 이제 네트워크의 위상이 물리적으로 고정되지 아니하며 유, 무선에 상관없이 이동성을 보장할 수 있어야 한다. 바로 이런 이유로 Mobile IP의 구현은 필수적인 요소가 되었다. 또한 기존의 고가의 사설 망을 이용하여 전용선을 구축하던 것을 인터넷의 급속한 발전에 맞추어 인터넷의 인프라를 이용하는 IP VPN의 등장은 본사와 지사 또는 본사와 외근 중인 직원, 본사와 고객간의 안전한 채널을 형성할 수 있게 하였다. 그러나 MIP의 표준에 의하면 MN은 자신의 Binding Update를 위해 HA에게 등록 메세지를 전송하게 된다. 이러한 등록 메시지가 VPN을 통과하기 위해서는 반드시

VPN Gateway에 의해 등록 메시지의 패킷이 복호화되며 이러한 일련의 절차에 의해 MIP 원래의 목적인 이동성을 확보하기에 어려운 문제가 생겼다. 이러한 이유로 MIP와 VPN의 연동에 대한 연구는 실제 환경에서는 필수적인 연구라 할 수 있다.

본 논문은 Mobile IP와 VPN이 상호 연동하는 환경에서 발생되는 문제들을 도출하며 이러한 문제들을 해결하기 위해 제시된 방안들을 비교분석함으로써 더 나은 결과를 도출할 수 있도록 한다.

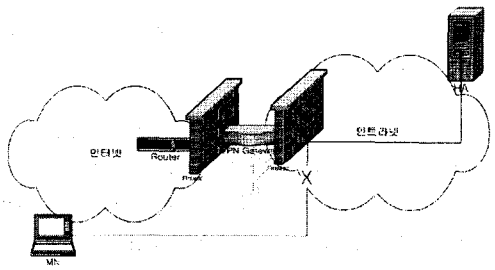
2. Mobile IP와 VPN 연동

2.1 연구를 위한 구현 시나리오[4],[5],[6]

실생활의 네트워크의 분류를 살펴보면 인터넷, 신뢰할 수 있는 인트라넷 그리고 인터넷과 인트라넷의 사이인 DMZ으로 구분할 수 있다. 일반적으로 인트라넷에 접근하기 위해서는 방화벽과 VPN 장비의 보호를 받아야 한다. 인트라넷은 방화벽과 VPN 장비의 보안 정책에 의해서만 접근할 수 있다.

HA가 VPN장비가 있는 안전한 네트워크 안에 있으며 MN이 외부로부터 자신의 HA에 등록을 시도하고 있다면 이러한 두개의 도메인 사이를 경유하게 되는 것이 문제가 될 수 있다. 다시 말해 MN은 자신의 변경 정보를 HA에게 전송할 것이다. 그러나 VPN Gateway는 이 패킷을 먼저 풀어볼 것이다. 이는 MN의 등록 요청이 바로 HA를 향하게 한 MIPv6의 표준 프로토콜을 위배하는 현상이다. 이러한 현상은 MN의 '끊김없는 세션 이동성'을 보장할 수 없게 한다.

여러 가지의 시나리오가 구성될 수 있지만 선행연구의 결과 문제가 발생되는 시나리오는 Mobile IP HA가 VPN 게이트웨이에 의해 보호되어지는 인트라넷 안에 구현되어있고 인트라넷 외부가 MN에 의해 직접 접근하지 않는 환경[그림 1]이다.



[그림 1] 문제 발생 구축 시나리오

2.2 문제 기술

인트라넷 외부를 움직이고 있는 MN은 자신의 HA에게 등록하기 위해 먼저 자신의 홈 VPN 게이트웨이와 IPSec 터널을 설립하여야 한다.

이 절차는 MN의 등록 메시지가 직접 HA에게 전달되지 못하게 하는 이유가 되고, MN으로부터 인트라넷 안에 있는 노드까지 MIP 트래픽이 VPN 게이트웨이 통과를 위해서 내부에서 IPSec 터널로 동작해야 하는 조건을 필요로 한다. 이 때문에 다음과 같은 중요한 문제가 발생하게 된다. MN은 CoA를 획득한 후 VPN 게이트웨이와 MN 간에 HA에 등록하기 위해 IPSec 터널을 설정한다. 이때 종단간(end-to-end) 보안 모델인 경우 IPSec 터널이 VPN 게이트웨이에서 끝나기 때문에 MN이 HA와 통신을 하기 위해서는 다시 VPN 게이트웨이와 HA사이의 IPSec 설정을 해야 하는 문제가 발생된다.

3. GHA(Gateway Home Agent) 해결 방안 분석

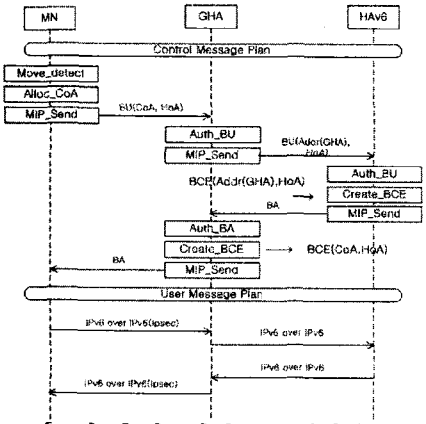
[7]에 의해 제안된 GHA(Gateway Home Agent) 해결 방안을 분석한다.

3.1 개요

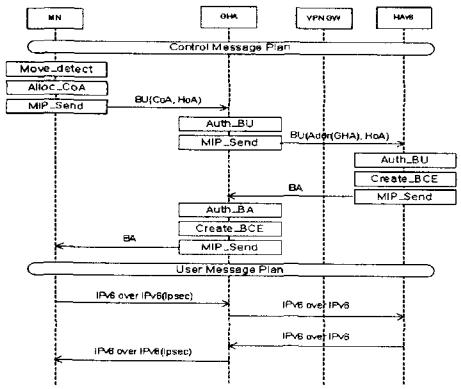
이 메커니즘은 계층적인 HA 구조를 사용하는데 여기에는 게이트웨이 홈 에이전트(GHA)라고 부르는 게이트웨이 기능을 가진 홈 에이전트가 포함된다. GHA와 HA의 관계는 MIPv4에서의 FA와 HA와의 관계와 거의 같다. MN으로부터의 바인딩 갱신 메시지는 먼저 GHA에 의해서 인증된다. 그 후에 인증이 성공한 경우라면, 바인딩 갱신 메시지는 HA로 포워딩된다. 바인딩 갱신 메시지를 수신하는 경우, HA는 그 메시지를 인증하고 바인딩 응답 메시지를 전송한다. 그러면 GHA는 바인딩 캐시 항목을 생성하고 바인딩 응답 메시지를 MN으로 전송한다. GHA는 MN으로부터 받은 COA를 가지고 자신에 대한 (MN-GHA) IPSec터널을 구성하는데 이 바인딩 캐시 항목을 사용한다. 그러므로 GHA와 MN은 만일 MN이 자신의 CoA를 변경한다 하더라도 IPSec을 재협상할 필요가 없다.

제안된 GHA 솔루션이 IPv6 인트라넷에서 작동되는 절차는 [그림 2]와 같다. 인트라넷 적용 시나리오의 경우, MN은 GHA를 자신의 게이트웨이로 사용해야 한다. 이는 MN이 자신의 망에 있는 VPN 게이트웨이만을 사용하는 것을 의미한다.

반면, 인터넷의 경우, GHA가 두개 이상의 인트라넷을 제공하고 각 인트라넷에 대해 GHA와 VPN 게이트웨이 간에 IPSec 터널이 설정되어 있다면 [그림 3]과 같은 절차에 의해 패킷이 전달되어질 것이다.



[그림 2] 인트라넷 IPv6에서의 절차



[그림 3] 인터넷 IPv6에서의 절차

3.2 GHA 솔루션 분석

GHA 솔루션의 장, 단점을 간단히 정리하면 아래의 [표 1]과 같다.

	장점	단점
1	IPSec 재설정 없음	추가적인 장비의 구축 필요
2	기존의 MIP 프로토콜 고수	Life time의 엄격한 동기화기법 필요
3	계층적 관리를 통한 관리 수월성 증가	NAT와의 상호연동 필요
4		인트라넷에 있는 CN과의 보안 협정 필요
5		MIPv4와의 연동 필요

[표 1] GHA 솔루션의 장단점

[표 1]에서 본 바와 같이 GHA 솔루션은 몇 가지의 중요한 단점을 지니고 있다. 이러한 단점들을 해소하고 더 나아가 IPSec Based VPN뿐만 아니라 다른 형태의 VPN과의 상호 연동을 높일 수 있도록 몇 가지 추가적인 해결 방안과 구현 시나리오를 제안한다.

4. 새로운 모델 제안

4.1 동기화 기법의 추가

GHA와 HA의 바인딩 캐시 엔트리의 라이프 타임은 비록 MN의 이동성을 보장하기에 충분하다고 가정할 수 있지만 GHA나 HA는 자신의 clock drift rate[8]를 지니고 있다. 이런 이유로 MN은 이동성을 제한받을 수도 있다. MN의 안정적인 이동성을 보장하기 위한 GHA와 HA간의 동기화 모듈의 추가를 제안한다. 기본적인 구조는 [9]에서 제안한 MN과 HA간의 Binding Update List 안의 Lift time을 설정하는 방법과 NTP(Network Time Protocol)에서 제안한 방법을 혼합하여 Lift time의 최대값을 구하는 방법을 제안한다. 제안한 방식을 간단히 설명하면 GHA와 HA 그리고 MN의 시간을 Clock Drift Rate를 제거한 표준시간으로 바꾸어 Lift Time을 설정하도록 하는 것이다. 수식은 [그림 4]와 같다.

1. 변수

L_remain_GHA = GHA이 가지고 있던 Lifetime

L_update_GHA = BU에 보내진 Lifetime

L_ack_HA = 받은 BA에서의 Lifetime

Cdr_GHA = GHA의 click drift rate

Cdr_HA = HA의 click drift rate

2. Life Time 산출 공식

max({L_remain_GHA(1-Cdr_GHA)} - ({L_update_GHA(1-Cdr_GHA)} - {L_ack_HA(1-Cdr_HA)})), 0)

[그림 4] 제안된 Life Time 산출 공식

제안된 Life Time 산출 공식에 의하여 최대값이 각각의 Life Time에 적용된다. 이 제안방식에 의하면 GHA, HA, MN은 각각의 clock drift를 지니고 있어도 마치 Global Clock을 지니고 있는 것과 같은 효과를 거둘 수 있다.

4.2 2-box 개념의 하드웨어 장비로써의 구현

해결 방안으로 소프트웨어 구동방식으로 구현했을 경우 MN과 VPN 게이트웨이 그리고 HA가 모두 소프트웨어를 업그레이드해야 하는 불편이 있으며 또한 기존의 VPN 게이트웨이에 과부하가 걸릴 것이 예상됨으로 하드웨어 장비방식의 구현을 제안한다.

5. 결론

본 연구는 MIP와 VPN이 구현된 실제 네트워크에서의 'seamless 이동성'을 수행하기 위해 제안된 방안들 중 차세대 인터넷 프로토콜(IPv6) 환경에서 동작하는 해결 방안들의 성능을 분석함으로써 IPv4와의 연동, 그리고 새로운 해결 방안 및 문제점들을 도출하는 것을 목표로 하여 동기화된 Life Time, 하드웨어적인 구현방식을 제시하였다.

본 논문에서 제안된 개선 해결 방안의 특징을 간단히 살펴보면, 끊김없는 이동성 보장을 위한 안정적인 Life Time을 설정할 수 있는 새로운 공식을 제안하였으며, 게이트웨이에서의 추가적인 오버헤드를 줄이며 소프트웨어 업그레이드를 피하기 위해 하드웨어 형태의 GHA를 제안하였다. 향후 연구에서는 기존에 제안된 GHA 솔루션에 대한 추가적인 연구와 새롭게 제안한 솔루션에 대한 테스트베드의 설계 및 성능 분석을 통하여 보다 정교한 MIP와 VPN과의 연동 연구가 필요하겠다.

참고문헌

[1] Perkins, C., "IP Mobility Support", RFC 2002, 1996.

[2] Ruixi Yuan, W. Timothy strayer, "Virtual Private Networks : Technologies and Solutions", Addison Wesley, 2001.

[3] James S. Tiller, "A Technical guide to IPSec Virtual Private Networks", Auerbach, 2000.

[4] Fraid Adrangi 외 3인, "Problem Statement and Requirements for Mobile IPv4 Traversal Across IPSec-based VPN Gateways", draft-ietf-Mobile IP-vpn-problem-statement-req-00, July 29, 2002.

[5] Fraid Adrangi외 3인, "Mobile IPv4 Traversal Across IPSec-based VPN Gateways", draft-adrangi-Mobile IP-vpn-traversal-02, July 29, 2002.

[6] S. Vaarala 외 5인, "Mobile IPv4 Traversal Across IPSec-based VPN Gateways", draft-ietf-mobileip-vpn-problem-solution-00, 2003.

[7] H. Ohnishi외 2인, "Mobile IPv6 VPN using Gateway Home Agent", draft-ohnishi-mobileip-v6vpngateway-01.txt, 2002.

[8] G. Coulouris외 2인, "Distributed Systems Concepts and design", Addison Wesley, 2001.

[9] D. Johnson외 2인, "Mobility Support in IPv6",draft-ietf-mobileip-ipv6-21.txt, 2003.