韓國 컴퓨터情報學會 論文誌
第13卷 第5號, 2008. 9.

2008-13-5-3-15

보안성과 전송 경로를 함께 개선한 NEMO의 통합적인 경로 최적화

조 경 산*, 신 덕 만**

Integrated NEMO Route Optimization to Improve Security and Communication Path

Kyungsan Cho*, DukMan Shin**

요 약

NEMO의 기술 표준안인 기본 지원 프로토콜(BSP)은 경로 최적화를 지원하지 않는 취약점이 있으므로, NEMO의 경로 최적화를 위한 여러 기법들이 제안되었다. 본 논문에서는 기존 기법들의 제한점을 개선하여 통신하는 두 노드가 외부 인터넷 또는 NEMO 내부 연결을 통해 연결된 경우 모두를 통합적으로 지원할 수 있는 NEMO 경로 최적화 기법을 제안한다. 제안 기법은 TLMR과 NEMO 외부의 노드 사이에 HA를 통하지 않는 최적화 경로와 개선된 보안성을 지원하는 프로토콜을 제공하고 TLMR에게 외부 인터넷을 통과하지 않는 내부 경로의 관리를 지원하도록 하여, NEMO 통신의 전송 경로와 전송 지연을 개선하고 보안 기능을 강화시킨다.

Abstract

Because BSP(Basic Support Protocol) of NEMO(Network Mobility) has important limitation of not providing route optimization, several route optimization schemes have been proposed. By analyzing and improving the limitations of the existing schemes, we propose an advanced integrated route optimization scheme for the communication through both the internal and external routing of nested NEMO. Our proposal includes a secure route optimization protocol which connects TLMR directly to an external node CN without passing through any HAs, and allows TLMR to control the internal path without passing through the internet. Thus, our scheme can strengthen the security as well as improve the path and delay of NEMO communication.

▸ Keyword : NEMO, BSP(Basic Support protocol), 경로 최적화(route optimization), 중첩 NEMO(nested NEMO), 보안(security),

• 제1저자 : 조경산
• 접수일 : 2008. 9. 3, 심사일 : 2008. 9. 23, 심사완료일 : 2008. 9. 25.
* 단국대학교 컴퓨터학부 교수 ** 단국대학교 대학원
※ 이 연구는 단국대학교 2008학년도 대학연구비 지원으로 연구되었음.

I. 서 론

개별 장치의 이동성을 네트워크의 이동성으로 확장한 NEMO(Network Mobility 또는 Network that Moves)는 인터넷의 접속점이 변화될 수 있는 이동 네트워크를 의미한다. NEMO의 내부에 위치한 개별 장치 노드인 MNN(Mobile Network Node)들은 라우터 MR(Mobile Router)을 통하여 인터넷에 접속된다. NEMO는 네트워크 속에 다른 네트워크가 접속되는 중첩 NEMO를 구성할 수 있다. 중첩 NEMO의 최상단 MR을 TLMR(Top Level Mobile Router)이라 한다.

NEMO의 통신방식 및 기술에 대한 표준안으로 제안된 NEMO 기본 지원 프로토콜(BSP: Basic Support Protocol)에서는 NEMO가 이동하게 되면 NEMO의 MR과 그 NEMO의 홈 링크에 위치한 HA(Home Agent) 사이에 양방향 터널을 구축하고, NEMO 안의 모든 MNN들은 이 터널을 이용하여 외부와 통신한다[1]. 따라서, 그림1과 같이 중첩 NEMO에서는 여러 터널(각 MR과 그의 HA 사이의 터널들)을 통과하여 패킷을 전송하므로 전송 지연이 증가하고 헤더 및 처리 과부하가 중첩의 수만큼 증가하며 이 문제는 NEMO 내부의 통신인 경우에는 더욱 심각하다[2].

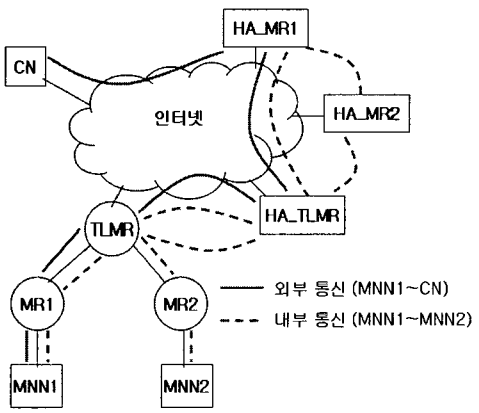

그림 1. BSP에 의한 통신 경로
Fig. 1. Communication Path of BSP

따라서, NEMO 통신의 두 노드인 MNN과 CN(Correspondent Node)사이의 통신에 경로 최적화가 필요하게 되었지만, NEMO의 BSP에서는 이를 제공하지 않으므로 NEMO의 경로 최적화를 위한 여러 기법들이 개별적으로 제안되었다.

기존 연구들은 MIRON[3], RRNP[4], MCGA[5]과 같은 비중첩 NEMO 구조에 대한 경로 최적화와 중첩 NEMO 구조의 경로 최적화 기법인 개선된 MIRON[6], BHT[7], RRH[8], HMIPv6[9] 및 NEMO 내부 통신에 대한 연구들[10-14]이 개별 구조의 경로 최적화를 단편적으로 제시하였다.

본 논문에서는 동일한 측도를 기반으로 기존 NEMO의 경로 최적화 연구를 비교 분석하여 NEMO의 이동성에 따라 변경되는 통신 구조에 통합적으로 적용할 수 있는 경로 최적화를 위한 설계 요구 사항들을 정의한다. 또한, 정의된 요구 사항을 만족하면서 기존 NEMO에서 고려하지 않았던 보안성을 추가한 개선된 경로 최적화 기법을 제안한다. 즉, TLMR과 NEMO 외부의 노드 사이에 HA를 통하지 않는 최적화된 경로를 제공하는 보안성이 강화된 프로토콜을 제안하고 NEMO 내부의 두 노드 사이의 통신은 TLMR이 외부 인터넷을 경유하지 않도록 최적의 경로를 제어하도록 하여, 외부 및 내부의 통신에 대해 통일된 제어를 제공하고 전송 지연과 처리 과부하를 감소시킨다.

본 논문의 구조는 다음과 같다. 2장에서는 기존 NEMO의 경로 최적화 기법들을 계통적으로 비교 분석하고, 공통된 평가 측도로 비교 분석한 결과를 근거로 개선된 경로 최적화 프로토콜 위한 설계 요구 사항을 정의한다. 3장에서는 정의된 요구 사항을 만족하는 경로 최적화 기법을 제안하고 제안 기법의 우수성을 제시하고, 4장의 결론으로 마무리한다.

II. 관련연구 분석

2.1 관련연구의 계통적 분석

본 절에서는 NEMO의 경로 최적화와 관련된 기존 관련 연구를 NEMO의 통신 구조에 따라 중첩 구조를 고려하지 않은 비중첩 NEMO 통신, 중첩 NEMO 통신 및 NEMO 내부 통신에 대한 세 유형의 경로 최적화 연구로 분류하여 분석한다.

비중첩 구조 NEMO의 경로 최적화 연구로는 MIPv6의 RR(Return Routability) 프로토콜을 응용한 다음의 제안들이 있었다.

MIRON 기법에서는 MIPv6의 RR 프로토콜을 비중첩 NEMO 구조에 적용하여 개별적 이동성을 갖지 않는 MNN(LFN: Local Fixed Node)의 경로 최적화를 제시하였다[3]. 즉, MR이 MNN을 대신하여 NEMO 외부의 CN에게 RR 프로토콜을 수행하여 MNN이 MR의 새주소 CoA로 이동하였음을 검증하고 비밀키를 생성한다.

RR 프로토콜에 네트워크 전치부의 검증을 추가하여 개별 노드가 아닌 NEMO에 할당된 prefix에 대해 NEMO 외부에 있는 CN과의 경로 최적화를 제시하는 RRNP 프로토콜도 제안되었다[4]. 또한, MR이 MNN을 대신하여 경로 최적화를 수행할 권한을 갖도록 MIPv6에서 활용된 CGA (Cryptographically Generated Address) 기법을 MNN과 MR의 공개키에 이중으로 적용하는 MCGA(Multi-key CGA)를 RR 프로토콜과 함께 사용하는 기법도 제안되었다[5].

앞의 제안들은 중첩 NEMO의 경로 최적화에 직접 적용할 수 없고 내부 통신을 효율적으로 처리할 수 없다는 문제점이 있으므로, 중첩 NEMO 구조에서 BSP의 비효율적인 경로를 개선하려는 다음의 연구들이 있었다.

MIRON 기법을 발전시킨 개선된 MIRON은 중첩 NEMO 구조에서 노드의 이동성을 지원하는 MNN(VMN; Visiting Mobile Node)에게 경로최적화를 제공하기위해, NEMO 내부에서 주소 할당을 위한 DHCP를 활용하고 RR 프로토콜을 적용하였다[6]. 중첩 NEMO의 TLMR이 하부 MR들의 경로 정보를 관리하는 BHT 기법에서는 MR과 TLMR사이의 터널에서는 중첩된 깊이만큼의 다중 캡슐을 통하여 패킷이 전달되도록 하였다[7]. 하나의 터널만을 경유하는 기법으로 RRH(Reverse Routing Header) 헤더에 MNN과 CN의 경로 상에 있는 MR들의 CoA를 표시하는 기법이 제시되었다[8]. RRH 헤더를 가진 패킷을 수신하는 HA는 NEMO에서 경유하는 MR들을 인식하고, TLMR과 HA사이에 하나의 터널만을 형성한다. HA 및 CN과의 메시지 교환을 줄이기 위하여, 라우터를 계층적으로 구성하는 Hierarchical Mobile IPv6 (HMIPv6) 기법도 제안되었다[9].

소개된 중첩 NEMO의 연구들은 외부 최적화 경로가 HA를 경유하도록 할뿐 아니라 NEMO 내부의 통신도 매우 비효율적인 경로를 가진다. 따라서, NEMO 내부 통신을 효율적으로 처리하기 위한 다음의 연구들이 있었다.

[10]에서는 각 패킷의 SRC 필드를 TLMR까지에 있는 MR의 CoA로 반복적으로 치환하여 각 MR과 TLMR은 자신의 하부에 있는 노드에 대한 위치 정보를 얻어 발송표(forwarding table)에 저장하여 각 MR이 NEMO 내부 통신의 최적화 경로를 형성하고, NEMO 외부 통신에 대해 HA_MNN을 경유하는 최적화 경로를 제시한다.

[11]에서는 중첩 NEMO의 각 MR에게 논리 주소인 HID(Hierarchy ID)를 할당하여 내부 경로 정보를 제공하고 각 MR은 목적지 주소의 prefix를 캐쉬에서 검색하여 논리 주소를 찾아 전송한다. 중간 MR들이 NEMO 내부의 목적지 주소에 대한 다음홉 정보를 발송표에 저장하여 내부 통신에 대한 경로 최적화를 제공하는 제안도 있었다[12]. ROPIO 제안은 MNN이 TLMR의 prefix를 이용하여 새로운 CoA를 형성하여 TLMR과 HA에게 등록하고, TLMR이 내부 경로를 제어하는 기법이다[13]. ROTIO 제안은 HA를 통과하여 2번의 캡슐화를 필요로하는 외부 경로를 제시하고, TLMR이 캐쉬에 저장된 경로 정보를 이용해 source routing을 통해 패킷을 전송하여 NEMO 내부 통신의 경로 최적화를 해결한다[14].

위에서 분석된 바와 같이 NEMO 내부의 통신은 TLMR과 중간 MR들이 경로 정보를 저장하여, [13]-[14]에서는 TLMR이 내부 통신 경로를 제어하며 [10]-[12]에서는 중간 MR이 직접 효율적인 내부 경로를 제공한다. 하지만, 이들은 효율적인 외부 경로를 제공하지 못하고, 내부 및 외부 통신에 대해 동일하게 적용하는 통일적인 경로 제어가 없었다.

2.2 평가 측도 및 비교 분석

본 절에서는 다음과 같은 공통된 특성 항목을 NEMO의 평가 측도로 선정하고, 앞 절에서 소개된 여러 최적화 프로토콜을 비교하고 분석한다. 기존 연구들에서 공통적으로 정보를 제공하지 않는 정량적 비교 분석 항목은 본 논문에서는 배제하였다.

1) **제안 기법의 적용 범위**
   앞에서 설명된 중첩 NEMO, 비중첩 NEMO 및 NEMO 내부 통신에 대한 적용 가능성을 분석한다.
2) **이동 주소의 등록 (BU: Binding Update)**
   이동한 MR(NEMO)이 새로운 CoA를 등록하는 BU(바인딩 갱신)의 유형을 분석한다. 가능한 BU의 대상은 HA 또는 CN 또는 TLMR이다.
3) **최적화 경로**
   MNN과 CN사이에 형성된 최적화 데이터 경로로 내부 통신과 외부 통신의 경로로 구별하여 분석된다. 내부 통신은 외부 인터넷을 경유하지 않도록, 외부 통신은 경유되는 HA의 수를 최소화하는지 분석한다.
4) **주소 설정 정보**
   이동 MR의 CoA 주소 설정 정보를 분석한다.
5) **경로 정보의 저장**
   전송 경로 및 주소 정보의 저장 내용을 분석한다.
6) **제공하는 보안 기법**

표1은 대표적인 기존 프로토콜들을 앞에서 제시된 평가 항목으로 비교한 것이다. 표1에서 NA는 관련 설명이 없음을 나타내고, (TLMR)은 TLMR이 내부 통신 경로를 제어함을 (MR)은 MR이 내부 통신 경로를 제어함을 나타낸다.

표 1. 기존 프로토콜들의 비교 분석
Table 1. Comparative Analysis of Existing Protocols

제안 기법	적용 범위	전송 경로(그림1의 구조에 대해) 1)MNN1-CN, 2)MNN1-MNN2	이동 등록 대상	주소 설정	주요 경로 저장정보	적용된 보안성
BSP(1)	모든 구조	1)MR1-TLMR-HA_TLMR-HA_MR1 2)MR1-TLMR-HA_TLMR-HA_MR1-HA_MR2-HA_TLMR-TLMR-MR2	HA	NA	NA	NA
NIRON(3)	비중첩, 외부	1)MR1-TLMR, 2)NA	CN, HA	NA	NA	RR
RRPN(4)	비중첩, 외부	1)MR1-TLMR, 2)NA	CN, HA	NA	NA	RR
개선된 MIRON(6)	중첩, 외부	1)MR1, 2)NA	CN, HA	동일 prefix	NA	RR
RRH(8)	중첩, 외부	1)MR1-TLMR-HA_MR, 2)NA	HA TLMR	NA	NA	NA
(10)	모든 구조	1)MR1-TLMR-HA_MNN 2)MR1-TLMR-MR2 (MR)	HA	NA	목적지, 다음홉	NA
ROTIO(14)	모든 구조	1)MR1-TLMR-HA_TLMR-HA_MR 2)MR1-TLMR-MR2 (TLMR)	HA TLMR	NA	경로상의 MR들	NA
(11)	중첩, 내부	1)NA 2)MR1-TLMR-MR2 (MR)	TLMR	동일 prefix, HID	MNP, HID	NA
ROPIO(13)	모든 구조	1)MR1-TLMR-HA_MR1 2)MR2-TLMR-MR2 (MR)	HA TLMR	TLMR의 prefix	MR, MNP	NA

2.3 개선된 경로 최적화 설계를 위한 요구사항

기존 연구의 분석을 근거로 개선된 NEMO의 경로 최적화를 위한 설계 요구 사항을 다음과 같이 정의한다.

1. 통합적인 적용 지원

NEMO는 이동성 특성 때문에 두 노드 MNN과 CN 사이의 구조에 따라 비중첩 NEMO, 중첩 NEMO 및 내부 통신의 세 통신 구조의 유형으로 실시간으로 변형이 가능하므로, 세 유형 모두에 동일한 방법으로 적용할 수 있는 통합적인 경로 최적화를 지원해야 한다.

2. NEMO의 이동 감지 및 등록 지원

다른 네트워크로 이동한 것 뿐 아니라 NEMO 내부에서의 이동도 감지할 수 있는 통합된 기법과 이동이 감지된 후에 상황에 맞게 적절한 이동의 등록이 필요하다.

3. 내부 및 외부 통신에 최적 경로 설정

NEMO의 내부에 있는 목적지 CN으로의 통신은 외부 인터넷을 통하지 않고 NEMO 내부에서 직접 전송해야하며, 이를 위하여 NEMO 내부의 MR들은 MNN들에 대한 경로 정보를 최소화하여 저장해야한다. NEMO 외부의 목적지 CN의 경우에 HA에게 이동 등록하고 HA를 경유하는 경로를 설정하는 것은 비효율적이며, 최적의 경로는 NEMO에서 CN까지의 직접 경로이다.

4. 보안성 지원

BSP 또는 중첩 NEMO 또는 NEMO 내부 통신을 위한 경로 최적화 제안은 기능면을 강조하였고, 보안적인 측면은 소외되었다. NEMO 내부 노드 사이에는 보안 연관이 존재한다는 가정이 가능하지만, NEMO 외부와의 안전한 통신을 위해서 주소 등록 과정과 이동 이후의 통신을 위한 보안성이 지원되어야 한다. 일부 기존 연구에서 적용한 RR 기법은 잦은 재수행의 문제점과 공격 취약점이 있으므로 보다 안전한 제안이 필요하다.

III. 개선된 경로 최적화의 제안

본 장에서는 앞 장에서 정의된 경로 최적화를 위한 설계 요구 사항을 만족시켜 NEMO의 이동성에 따른 다양한 구조에서의 통신에 동일하게 적용할 수 있는 개선된 경로 최적화 기법을 제안한다.

3.1 제안 기법의 개요

제안 기법은 동일한 nested NEMO 구조 내에서의 이동 감지와 NEMO 내부 통신의 경로 최적화를 위해 동일한 NEMO의 모든 MR들에게 동일한 prefix가 할당되도록 하고, 다양한

구조의 통신에 동일하게 적용되도록 모든 패킷은 TLMR을 통해 전송되도록 한다. 이동한 NEMO의 MR은 연결된 네트워크에 있는 상위 MR들로부터 RA(Route Advertizement)를 통해 (상위 MR 리스트, TLMR 정보, prefix)등의 정보를 수신하여 자신의 이동을 감지하고 TLMR을 인식할 수 있도록 한다. NEMO 내의 TLMR와 상부에 있는 중간 MR들의 정보를 수신한 이동한 MR은 자신의 위치와 경로 정보를 TLMR에게 등록한다. 이 등록 과정을 통해 TLMR과 중간 MR은 자신의 하부 구조에 대한 경로 정보를 얻는다.

NEMO가 이동한 후에 수행하는 새 주소의 등록(BU) 과정은 다음과 같다.

1. 동일 네트워크에서의 이동이면 TLMR에게만 새로운 위치를 등록한다.
2. 다른 네트워크로의 이동이면 다음을 순서대로 수행한다.
   - 새로운 CoA를 생성하고,
   - TLMR에게 새로운 위치를 등록한다.
   - HA에게 새로운 위치를 등록한다.
   - CN에게 새로운 위치를 등록한다.

전송 목적지 CN에게 새로운 위치를 등록한 이후의 경로는 그림2와 같이 외부 통신은 TLMR에서 직접 CN으로 전송되며 내부 통신은 외부 인터넷을 통과하지 않도록 TLMR이 제어한다.

3.2 안전한 BU 프로토콜의 제안

NEMO가 이동한 후에도 외부 CN과의 지속적인 통신을 위해 TLMR을 통해 CN에게 새로운 주소를 등록하도록 안전한 BU 과정의 프로토콜을 제안한다.

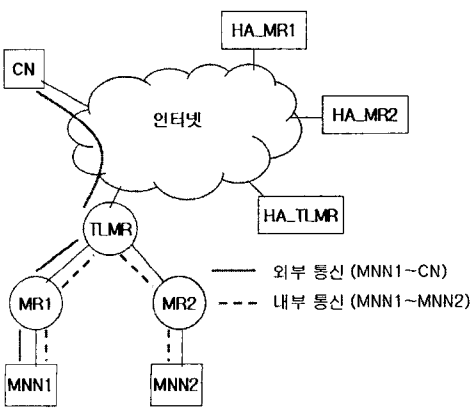

그림 2. 제안 기법에 의한 개선된 전송 경로
Fig. 2. Communication Path of Our Proposal

제안 BU 프로토콜은 MIPv6의 경로 최적화에 적용된 proxy 구조의 SUCV(Statistic Uniqueness and Cryptographic Verifiability) 최적화 프로토콜[15]에서 제시한 proxy 구조 및 Diffie-Hellman 비밀키 생성 기법을 함께 적용하여, TLMR과 CN 사이에 직접 경로를 설정함으로 RR 기법의 미진한 보안성을 보완한다. 수행 과정은 그림3과 같다.

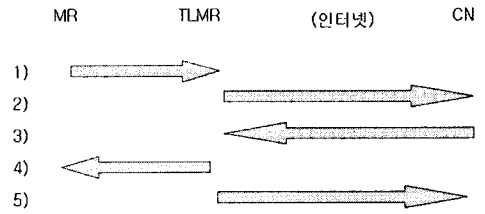

그림 3. CN으로의 BU 프로토콜 제안
Fig. 3. Proposal of BU Protocol to CN

1) MR이 새로운 네트워크로 이동했음을 감지하면, 이동된 네트워크의 TLMR에게 MNN의 이동을 CN에게 등록해 주도록 (HoA_MNN, CoA_MR, CN)를 전송한다.

2. 이동 MR로부터 BU 요청을 수신한 TLMR은 (HoA_MNN, CoA_MR, CoA_TLMR, 쿠키1)를 CN에게 전송한다. 쿠키1은 DoS 공격방지와 응답 검증 용이다.

3. CN은 TLMR에게 비밀키 형성을 위한 정보(gx)와 수신 확인용 쿠키1을 함께 전송한다.

4. TLMR은 수신한 gx와 자신의 gy를 이용해 세션키를 생성하여 MR에게 전송한다

5. TLMR은 세션키와 gy를 서명하여 CN에게 전송한다. CN은 TLMR의 공개키로 서명을 확인하고, 수신한 gy와 자신의 gx를 이용해 세션키를 검증한다.

위에서 보인 모든 BU 과정 이후에 MNN과 외부 CN 사이의 통신은 그림2에서 MNN-MR1-TLMR-CN의 최적 경로를 통해 세션키로 암호화하여 전송한다.

제안 프로토콜에서는 CN에게 최적 경로를 등록하는 과정도 안전하게 수행하며, 이후에도 Diffie-Hellman 기법으로 설정된 세션키로 암호화하여 안전하게 전송한다.

3.3 내부 경로 설정

이동한 NEMO의 MR은 RA를 통해 NEMO의 prefix와 TLMR 및 중간 MR들의 정보를 수신한 후에 이동 노드로의 경로 정보를 중간 MR들과 TLMR에게 전송한다. MR은 이동한 후에, RA를 통해 수신한 prefix를 비교하여 이동하였음

표 2. 제안 기법의 특성
Table 2. Characteristics of Our proposal

적용 범위	전송 경로(그림1의 구조에 대해) 1)MNN1-CN, 2)MNN1-MNN2	이동 등록 대상	주소 설정	주요 경로 저장 내용	적용 보안성
모든 구조	1) MR1-TLMR 2) MR1-TLMR-MR2 (TLMR)	CN TLMR	동일 prefix	MNN, 다음홉	SUCV

을 감지한다. 이동한 NEMO는 중간 MR들을 경유하여 TLMR에게 NEMO 내부의 경로 정보인 (TLMR까지의 경로 정보, 이동 MR의 새주소)를 등록하며, 중간 MR들은 이동 MR까지의 경로에 있는 다음홉 정보를 저장한다. TLMR과 중간 MR들이 저장하는 경로 정보는 그림4와 같다.

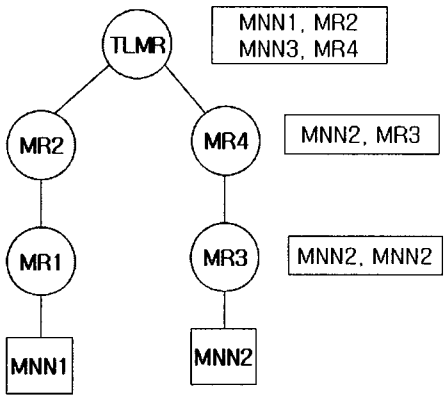

그림 4. 내부 경로 정보
Fig. 4. Internal Path Information

모든 패킷은 TLMR에게 전송되고, 만약 목적지가 NEMO 외부의 노드이면 TLMR은 패킷을 인터넷을 통해 목적지 주소로 전송하고 목적지가 NEMO 내부인 경우에는 TLMR이 그림2와 같이 수신한 패킷을 목적지로 전송한다.

TLMR은 수신한 패킷의 목적지 주소의 prefix에 따라 동일 NEMO내의 노드이면 저장된 경로 정보와 패킷의 목적지를 비교하여 경로 정보에 있는 다음 홉 주소의 MR로 전송한다. 이를 수신한 중간 MR은 저장된 경로 정보를 이용하여 계속 다음 홉으로 전송하여 목적지까지 전송한다.

3.4 제안 기법의 개선 분석

본 제안에서는 TLMR과 중간 MR들이 MNN에 대한 경로를 저장하며, TLMR이 패킷의 목적지를 확인한 후에 저장된 경로 정보를 이용해 중간 MR들을 경유하여 내부 목적지까지 또는 인터넷을 통해 외부 목적지까지 전송한다. 제안 기법을 2.2절의 평가 항목에 의해 분석하면 표2와 같다.

외부 통신은 TLMR이 HA를 경유하지 않고 직접 CN에게 연결하는 경로를 설정하고 내부 통신은 TLMR이 제어하여 외부 인터넷을 통하지 않도록 하여, 통일적인 제어를 제공하였고 전송 경로가 단축되고 전송 지연이 감소된다. 내부 통신을 위한 경로 정보도 통신 중인 각 MNN에 대해 (MNN, 다음 홉)로 최소화하여 경로 상의 MR들에게만 저장하므로 저장 용량의 부담이 적다. NEMO 내부의 노드들 사이에는 신뢰할 수 있다는 보안 연관이 존재한다는 가정에서 별도의 보안 기능을 추가하지 않았지만, 외부 통신의 경로 최적화 과정은 SUCV 기법을 변형 적용하여 잦은 재수행과 공격 취약성의 문제점을 가진 RR 기법을 활용한 기존 연구보다 보안성을 높였다.

IV. 결론

네트워크에 이동성을 부여한 NEMO 내부의 노드 MNN과 상대 노드 CN과의 전송 경로를 최적화하는 것은 두 노드 사이의 통신 구조에 따라 서로 다른 특성을 갖는다. NEMO의 통신은 비중첩 NEMO를 통한 통신, 중첩 NEMO를 통한 통신 및 NEMO 내부의 통신 중의 하나로 분류되며, 이동에 따라 통신 구조는 실시간으로 다양하게 변화될 수 있다. 본 논문에서는 기존 연구들의 취약점을 개선하여 NEMO 내부 구조의 중첩 여부와 무관하게 두 통신 노드 MNN과 CN이 인터넷을 통해 연결된 경우와 동일한 NEMO 내부에 존재하는 경우 모두를 지원할 수 있는 NEMO 통합적 경로 최적화 기법을 제안하였다.

NEMO 외부의 CN에 대한 통신 경로는 TLMR이 CN에게 BU를 수행하여 TLMR과 CN 사이에 HA를 경유하지 않는 최적화 경로를 설정하는 프로토콜을 제안하였으며 내부 통신은 외부 인터넷을 통하지 않고 TLMR이 경로를 제어하도록 하였다. 외부 경로를 위해 제안된 프로토콜에는 MIPv6에서 RR 기법보다 우수하다고 검증된 proxy 구조의 SUCV 기법에서 적용한 proxy 구조 및 비밀키 생성 기법을 함께 채택함

으로 이동 후의 등록 과정과 통신의 보안성을 강화하였고, 내부 통신을 위해 MR에 저장되는 경로 정보도 감소시켰다.

외부 통신과 내부 통신 모두 TLMR을 통해 통합적으로 제어되어 최적 경로를 제공하여 전송 경로를 단순화하고 전송 지연을 감소시켰다.

본 연구는 다양한 통신 구조를 지원하는 통합적 경로 최적화를 위한 제안과 이의 기능적 검증에 중점을 두었으며, 기존 연구에서 공통적으로 제공하는 정보가 부족한 트래픽 및 전송 효율성에 대한 정량적 분석은 제외되었다.

본 연구에서는 NEMO 내부 노드 사이에는 신뢰할 수 있는 보안 연관이 있다고 가정하고, TLMR은 신뢰할 수 있다고 가정하였다. 또한, 모든 통신이 TLMR을 경유하고, TLMR이 내부 경로 설정을 제어함으로 TLMR의 부하가 커질 수 있다는 문제점이 있기 때문에 본 연구의 적용 가능한 환경은 제한될 수 있다.

본 연구에서 제외된 트래픽 및 전송 효율성에 대한 정량적 분석 및 TLMR의 부하 경감과 NEMO 내부의 보안 연관 분석은 본 논문의 향후 연구 과제로 넘긴다.

참고문헌

[1] V. Devarapalli, R. Wakikawa, A. Petrescu and P. Thubert, "Network mobility (NEMO) basic support protocol," IETF, RFC3963, 2005

[2] C. Ng, F. Zaho, M. Watari and P. Thubert, "Network Mobility Route Optimization Solution Space Analysis," IETF, RFC4889, 2007

[3] C. J. Bernardos, M. Bagnulo and M. Calderon, "MIRON: mobile IPv6 route optimization for NEMO," Proc. of 4th Workshop on Appl. Services in Wireless Network, pp 189-197, 2004

[4] C. Ng and J. Hirano, "Extending Return Routability Procedure for Network Prefix (RRNP)," Internet Draft, draft-ng-nemo-rrnp-00.txt, 2004

[5] M. Jo and J. Kempf, "Secure Route Optimization for Network Mobility Using Secure Address Proxying," Proc. of ICMU, pp 84-90, 2006

[6] C. Bernardos, M. Bagnulo, M. Calderon and I. Soto, "Mobile IPv6 Route Optimisation for Network Mobility (MIRON)," Internet Draft, draft-bernardos -nemo-miron-01.txt, 2007

[7] H. Kang, K. Kim, S. Han, K. Lee and J. Park, "Route Optimization for Mobile Network by Using Bi-directional Between Home Agent and Top Mobile Router," Internet Draft, draft-hkang-nemoro- tlmr-00.txt, 2003

[8] P. Thubert and M. Molteni, "IPv6 Reverse Routing Header and its application to Mobile Networks,"Internet Draft, draft-thubert-nemo -reverse -routing-header-05.txt, 2004.

[9] H. Soliman, C. Catelluccia, K. E. Malki and L. Bellier, "Hierarchical mobile IPv6 mobility management (HMIPv6)," IETF, RFC4140, 2005.

[10] Y. Kim, K. LEE, H. KU, and E. HUH,"Route Optimization Via Recursive CoA Substitution for Nested Mobile Networks," LNCS 3981, pp. 827-836, 2006

[11] H. Park, M. Kim, and H. Cho, "Route Optimization Using Scalable Cache Management for Intra-NEMO Communication", LNCS 4611, pp. 739-747, 2007

[12] S Baek, J. Yoo, and H. Cho, "Route Optimization for Intra Communication of a Nested Mobile Network," Proc. of WNEPT 2006, 2006

[13] L. Li-Hua, L. YUan-an, "Route Optimization solution based on extended prefix Information option for Nested Mobility Network," Proc. of Wireless Communications, Networking and Mobile Computing, pp. 1792-1796, 2007

[14] H. Cho, T. Kwon, and Y. Choi, "Route Optimization Using Tree Information Option for Nested Mobile Network," IEEE Journal on Selected Areas in Communications, vol. 24, No. 9, pp. 1717-1724, 2006

[15] 원유석, 조경산, "SUCV를 개선한 MIPv6 바인딩 갱신 프로토콜," 정보처리학회논문지 C, 제13-C권, 제3호, pp. 267-274, 2006

저 자 소 개

조 경 산

1979년 서울대학교 전자공학과(학사)
1981년 한국과학원 전기전자공학과 (공학석사)
1988년 텍사스 대학원(오스틴) 전기전산공학과(Ph.D.)
1988년~1990년 삼성전자 컴퓨터부문 책임연구원, 실장
1990년~현재 단국대학교 컴퓨터학부 교수
관심분야: 네트워크 시스템 및 이동통신 보안, 컴퓨터시스템

신 덕 만

2006년 한국성서대학교 인터넷정보학 (학사)
2008년 단국대학교 대학원 정보컴퓨터과학과 (석사)
관심분야: 이동통신, 통신 보안