

전술 네트워크를 위한 ILNP 기반 환경에서의 이동성 관리 기술

선경재¹⁾ · 김영한^{*2)} · 노홍준³⁾ · 박형원³⁾ · 한명훈⁴⁾ · 권대훈⁴⁾

¹⁾ 송실대학교 정보통신소재융합학과

²⁾ 송실대학교 정보통신공학과

³⁾ LIG넥스원(주) C4I연구소

⁴⁾ 국방과학연구소 제2기술연구본부

Mobility Management for ILNP-based Tactical Network

Kyoungjae Sun¹⁾ · Younghan Kim^{*2)} · Hongjun Noh³⁾ · Hyungwon Park³⁾ ·
Myounghun Han⁴⁾ · Daehoon Kwon⁴⁾

¹⁾ Department of ICMC Convergence Technology, Soongsil University, Korea

²⁾ Department of Electronic Engineering, Soongsil National University, Korea

³⁾ C4I R&D Center, LIG Nex1, Korea

⁴⁾ The 2nd Research and Development Institute, Agency for Defense Development, Korea

(Received 29 January 2020 / Revised 10 April 2020 / Accepted 24 April 2020)

Abstract

In the future Network Centric Warfare(NCW), changing to IPv6 based network environment is required to enable various future technologies such as the Internet of Things(IoT) and cloud technology which are expected to be introduced to the tactical network evolution. With the change to the IPv6 network, an ID/LOC(Identifier/Location) separation protocol that decomposes context of the IP address to location and identifier can enhance network capacity of increasing number of device and provide efficient mobility management in the tactical network that changes topology dynamically. In this paper, we choose ILNP(Identifier-Locator Network Protocol) as an ID/LOC separation for tactical network environment. In addition to ILNP-based tactical network design, this paper proposes a network-based mobility management scheme for providing efficient mobility management. Through numerical performance analysis, we show that the proposed scheme can reduce network loads more effectively than the conventional IP-based mobility management scheme and common handover procedure in ILNP.

Key Words : ID/LOC Separation(식별자/위치 분리), Mobility Management(이동성 관리), ILNP(식별자-위치 네트워크 프로토콜)

* Corresponding author, E-mail: younghak@ssu.ac.kr

Copyright © The Korea Institute of Military Science and Technology

1. 서론

단말이 급증하여 일찍이 IPv4 주소의 고갈로 인해 IPv6의 전환이 이루어진 민간 영역과는 달리, 한정된 단말 수로 구성되어 있는 전술 네트워크에서는 IP 기반 통신 단말의 증가로 인한 IPv4의 주소 고갈 문제는 현재까지 크게 고려되고 있지 않다. 그러나 네트워크 중심전(NCW: Network Centric Warfare)으로 변화하는 미래 전투 환경에서는 IoT(Internet of Things), 클라우드 기술 등의 다양한 미래 기술들이 도입될 것으로 예상되며, 이는 네트워크 연결성을 제공해야 하는 기기의 증가로 인한 IPv4 주소의 고갈 문제를 야기할 수 있다. 이에 따라, 군 전술환경에서 IPv6 주소를 도입하기 위한 논의는 2004년부터 진행되었으며^[1], 이에 따라 IPv6 주소 체계 수립을 위한 계획^[2]과 관련된 연구도 수행되었다.

미래 전투 환경에 추가될 다양한 전술 기기들은 이동 수단의 다양화와 작전 반경의 증가로 인해 여러 제대 간 이동하며 통신을 수행할 것이다. 따라서 IPv6 주소 기반의 환경으로의 변화와 함께, 전술망에서 고려해야 할 사항은 접속망 변화에 따른 신속한 주소 할당 및 이동성 관리 방안이다. 그러나 기존 IP 개념은 IP 주소가 위치와 식별자의 역할을 모두 내포하는 통합 개념으로, 고정적인 유선망 기반의 인프라에서는 문제가 없으나 무선 단말들이 급증하는 미래 모바일 기반의 전술 네트워크에서 접속 단말의 위치가 변경됨에 따라 IP 주소가 변하게 되어 여러 문제들을 야기할 수 있다. 이를 위해 MIPv6(Mobile IPv6), PMIPv6(Proxy Mobile IPv6) 등의 이동성 관리 프로토콜을 적용할 수 있으나, 초기 접속 시 할당받은 IP 주소를 이동 중에 유지하면서, 할당받은 IP 주소의 앵커역할을 하는 노드와의 시그널링 메시지 교환 및 터널링 기반의 패킷전달을 수행하는 이동성 지원 방식은 단일 앵커의 장애에 따른 안정성과 네트워크 내 최적화되지 않은 트래픽 전달 경로로 인한 지연시간 등을 야기한다. 특히, 이러한 문제점들은 주요 전술 노드들이 무선 링크로 연결되어 한정된 무선자원을 공유하여 사용하는 전술망 환경에서는 서비스 연결성과 네트워크 자원의 취약을 함께 고려해야 하는 어려운 문제에 직면할 수 밖에 없다.

위에서 언급한 제약들을 해결하기 위해, 본 논문에서는 IP 주소가 포함하고 있는 ID(Identifier) 정보와 LOC(Location) 정보를 분리하는 개념을 전술망 환경에

적용하고자 한다. ID와 LOC 정보의 분리를 통해, 전술망에서 각자의 체계들은 위치에 따라 변하지 않는 고정적인 신원 정보를 가지고 있어 이를 식별 가능하면서도, 이동 또는 네트워크 변경에 따른 위치 정보는 가변적으로 제공함으로써 네트워크 관리의 용이성과 단말 신원 고정을 통한 체계 관리의 용이성을 함께 제공하고자 한다. ID/LOC 분리를 위해 표준화된 몇 가지 프로토콜이 있으나, 본 논문에서는 ILNP(Identifier-Locator Network Protocol)를 전술망 환경에 적용한다. ILNP 기반 환경에서의 이동성 제공을 위해서 기존에도 ILNP 기반 환경에서의 이동성 관리를 위한 연구들도 진행된 바 있으나, 기존 방식들은 위치 정보의 변경이 일어날 때, 기존 위치로 오는 트래픽에 대해서는 여전히 터널링 기반의 최적화되지 않은 라우팅을 수행하며, 경로를 최적화하기 위해서 현재 세션이 연결되어 있는 모든 상대 노드에게 위치 정보의 업데이트 요청 메시지를 전달해야 하기 때문에 통신 상대 노드가 증가할수록 오히려 기존의 IP 기반 이동성 관리 프로토콜보다 네트워크 부하를 발생시킬 수 있다. 본 논문에서는 전술망 내 네트워크 노드에서 단말의 위치 정보 변화에 따라 임시적인 트래픽 경로를 제공하면서 통신 상대노드에 업데이트 메시지를 전송하지 않고도 경로를 최적화 할 수 있도록 하여 네트워크 노드 간 이동성 관리를 위한 절차를 최소화하면서 ID/LOC 분리 구조의 이점을 제공하고자 한다.

본 논문의 이후 구성은 다음과 같다. 2장에서는 ILNP 기본 개념 및 ILNP 구조에서의 이동성과 관련된 연구들을 분석하고 전술망의 특성을 분석한다. 3장에서는 제안하는 구조 및 이동성 절차를 기술하고 4장에서 정량적 분석을 통해 제안 기법의 성능을 평가한 후에 5장에서 결론을 맺는다.

2. 관련 연구 및 배경

2.1 ID/LOC 분리 구조의 필요성

ID/LOC 분리 구조는 전술한 바와 같이, IP 주소가 가지고 있는 “ID+Location” 개념을 분리함으로써, IP 주소에 대한 세션의 의존성을 최소화하기 위해 제안된 기술이다. 기존의 IP 기반 환경에서, 단말의 IP 주소는 “ID+Locator”의 개념을 가지고 있으며, 이를 통해 단말의 IP는 TCP 세션에 대해 식별 정보를 포함하는 동시에 네트워크 내 특정 라우터 내 서버넷에 속

하여 위치에 대한 의존성을 갖게 된다. 이러한 통합적인 개념은 전통적인 유선 기반의 정적 네트워크 환경에서는 문제없이 동작하였지만, 무선 단말의 등장으로 인한 동적 네트워크 환경으로의 변화 과정에서 문제를 야기하였다. 즉, 단말의 이동에 의해서 새로운 라우터 내 서브넷에 속하게 되면 기존에 단말이 사용하던 IP 주소가 네트워크 내 라우팅 테이블로 처리할 수 없게 되고, 이에 따라 단말의 통신을 위해서는 IP 주소를 이동한 라우터 내 서브넷에 속한 주소로 변경해야 한다. 문제는 IP 주소가 네트워크 계층의 송수신자 식별뿐만 아니라 전송 계층의 TCP에서 각 세션을 식별하기 위한 5-Tuple 값에도 사용되고, 경우에 따라서 응용 계층에서도 IP 주소를 식별자로 사용하고 있기 때문에^[3] IP 주소가 변경되면 기존의 서비스 연결성이 중단된다는 것이다. 이러한 단말 이동 시의 서비스 연결성 유지를 위해서, 표준화 기구인 IETF에서는 단말이 이동 시에도 IP 주소를 변경하지 않도록 하는 이동성 관리 프로토콜을 정의하였다. MIPv6^[4], PMIPv6^[5] 등의 이동성 관리 기술은 단말이 할당받은 주소의 서브넷을 보유한 라우터 내 해당 주소에 대한 앵커 기능을 통해, 단말이 다른 곳으로 이동하였을 때 단말 또는 단말의 새로운 접속 라우터와 시그널링 메시지 교환을 통한 터널링 기반의 패킷 전달을 수행하여 라우팅 인프라의 수정 없이 패킷의 도달성을 제공할 수 있도록 하였다. 그러나 이러한 이동성 관리 기법을 적용한다고 하더라도, 몇 가지 문제들이 존재한다. 첫째로는 확장성에 대한 것으로 갈수록 급증하는 무선 단말의 수에 따라 모든 단말에 대한 이동성을 제공하기 위해서는 네트워크 내에 이동성 프로토콜의 교환의 빈도가 급증하게 되고, 이는 전체 네트워크의 부하 및 성능의 저하로 이어질 수 있다. 두 번째로는 보안과 관련된 문제로서, 단말의 IP가 고정되어 있고, 단말의 위치를 앵커에서 지속적으로 추적할 수 있기 때문에 단말의 위치에 대한 프라이버시를 제공하지 못하게 된다^[6]. 이는 특히 본 논문에서 고려하는 전술망 환경을 고려할 때, 적군의 악의적 접근에 의해 주요 단말에 대한 지속적인 위치 추적이 가능할 수 있게 함으로써 잠재적 위협에 대한 취약성을 가지고 있게 된다.

위와 같은 문제를 해결하기 위해서, IP 주소의 식별자와 위치 정보 개념을 분리하기 위해 제안된 기술이 ID/LOC 분리 기술이다. 기본적으로 ID/LOC 분리 구조에서, 식별자인 ID는 단말의 신원 정보로서 반영구적 특성을 가지고, 이동 시에도 유지되는 정보로 정의된

다. ID는 단말의 전송 계층 및 응용 계층의 세션에 사용되는 정보로서, 해당 ID 값이 변하지 않는 한 해당 서비스의 세션 연결성이 지속될 수 있다. LOC는 단말의 현재 네트워크 접속 위치를 표현하는 정보로서, 이동에 따라 가변적으로 변하는 특성을 갖는다. 즉, LOC는 현재 단말의 접속 라우터의 서브넷에 속한 값을 가지며, LOC 값을 통해 외부에서 단말에게 패킷을 전달할 수 있다. LOC는 전송 계층 및 응용 계층에서 사용되지 않는 정보로 규정된다. ID/LOC 프로토콜은 네트워크 내에서 식별 정보와 위치 정보를 어떠한 방식으로 구분할 것인가에 대한 차이에 따라 여러 표준 프로토콜들이 제정되었으며, ID/LOC 분리 구조의 대표적인 프로토콜로는 LISP^[7](Location Identifier Separation Protocol)과 ILNP^[8](Identifier-Locator Network Protocol) 등이 있다. LISP은 단말에게 부여되는 주소와 네트워크 내 노드들간에 패킷 전달을 위해 사용하는 주소를 별도로 관리하여 단말의 ID와 네트워크의 LOC 매핑 정보를 통해 패킷을 전달한다. 그러나 LISP을 실제 적용하기 위해서는 기존의 IPv6 기반 네트워크 노드들을 LISP 기능이 탑재된 노드로 바꾸어야 하기 때문에 교체에 따르는 비용이 증가한다. 따라서 본 논문에서는 일반적인 IPv6 환경에서도 큰 변화없이 사용이 가능하여 실제 망의 적용이 용이한 ILNP 프로토콜의 적용을 고려하였다.

2.2 ILNP 프로토콜 개요 및 이동성 관리

ILNP 프로토콜은 2012년에 인터넷 표준화 기구인 IETF(Internet Engineering Task Forces)에서 표준화된 프로토콜로서, IPv6 주소의 128-bit 길이를 각각 64-bit의 식별 정보와 위치 정보로 구분한다. Fig. 1은 기존의 IPv6 주소와 ILNP 프로토콜 환경에서의 ID-LOC 결합 구조를 나타낸 것이다. 일반적인 IPv6 주소는 각 64-bit의 라우팅을 위한 프리픽스와 단말에서 구성하는 Interface Identifier로 구성된다. 이러한 IP의 주소 체계에 착안하여, ILNP에서는 128 bit의 IPv6 주소 필드를 64 bit씩 구분하여 위치 정보인 L64와 단말 식별 정보인 Node Identifier(NID)로 구성한다. IPv6와 유사한 ID/LOC의 구분은 기존의 IPv6 라우터들과의 호환 및 ICMP 메시지 및 IPv6 Neighbor Discovery 과정을 수정 없이 사용할 수 있으며, IPv6의 주소 할당 과정(Stateful, Stateless)도 동일하게 사용이 가능하다. ILNP 구조에서, 위치 정보인 L64는 단말의 첫 홉 라우터에 속한 prefix 정보로 구성되며 NID는 단말의 인터페이스

스 주소 또는 기타 정의된 값으로 사용할 수 있다. L64와 NID 값의 매핑 정보는 DNS 서비스를 L64-NID 매핑 정보로 운영함으로써 가능하다.

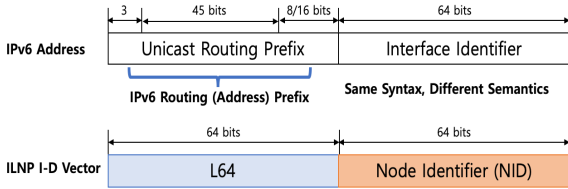


Fig. 1. Comparison between IPv6 address and ILNP ID/LOC structure

ILNP가 128bit의 IPv6 주소 필드를 그대로 사용하기 때문에 IPv6와의 차이점이 미미하다고 생각할 수 있으나, ILNP가 가지고 있는 가장 큰 특징은 기존의 5-tuple 기반의 세션 표현에 있어서 위치와 ID 정보의 밀접한 결합 관계를 분리하는 Naming Architecture를 새로 제안한 것에 있다. 기존의 IPv6 기반의 환경에서 네트워크 전송 계층인 IP 계층에서 사용하는 값과, TCP에서 세션을 구분하기 위해 사용되는 노드의 식별 값은 동일하다. 즉, IP 주소가 바뀌면, TCP 세션에서의 각 송수신 노드의 식별자도 바뀌기 때문에 세션이 끊어지게 되는 것이다. 그러나, ILNP 환경에서는 IP 계층에서 상대 노드를 인식하는 값과 전송계층에서 상대 노드를 인식하는 값이 다르며, 전송 계층에서 단대단 세션 노드를 식별하는 NID 값은 위치인 L64 값이 변하더라도 바뀌지 않는다. 따라서 IP 계층에서 L64 값이 변하더라도 세션의 연속성에는 영향을 주지 않기 때문에 단말의 위치 변화에 따른 전송계층에서의 영향을 최소화 할 수 있다. 이러한 NID와 L64 매핑 정보의 관리에 의해 단말의 접속점이 변경되는 핸드오프 과정에서, 단말은 새로운 위치의 네트워크 라우터로부터 L64 구성을 위한 값을 수신한다. 그리고 이를 통해 새로운 매핑 값을 구성한 후, 이를 현재 세션을 유지하고 있는 상대 노드에게 Location Update(LU) 메시지를 통해 알려줌으로써 새로운 NID-L64값을 기반으로 하는 IP 라우팅을 통해 패킷을 수신할 수 있다. 이는 기존 IP 기반 환경에서의 터널링 과정을 생략할 수 있어 네트워크에 프로세싱 비용을 효과적으로 줄일 수 있다. 다만, ILNP 기반 환경에서 단말의 이동에 따라 변경된 위치로의 라우팅 경로를 새로운 L64 값으로 업데이트 되는 동안 기존 경로로 패킷이 전달되

어 패킷의 손실이 발생할 수 있다. 따라서, ILNP 환경에서의 이동성 관리는 세션의 연속성 제공보다 이동 시 변경되는 L64-NID 매핑 정보를 업데이트 하는 과정에서 발생하는 패킷의 손실을 줄이고 효율적으로 위치 정보의 변경을 관리하기 위한 부분에 초점을 맞추고 있다. 대표적으로는 ILNP 기반 환경에서 MIPv6 기반의 이동성 관리 기법을 적용하여, 이동 시 기존 단말의 NID-L64 값에 대한 임시적인 터널을 단말의 기존 접속 라우터에서 수행하고자 한 연구^[9]가 있다. 그러나 이는 단말 기반의 이동성 지원을 위한 추가 기능이 단말에 구현되어야 하며, 특히 전송망과 같은 계층적 트리 구조에서 비최적화 라우팅 문제를 야기할 수 있고, 단일 엔커에 대한 장애 시 복구 문제와 같은 기존 MIPv6에서의 문제점을 그대로 가지고 있다. 또한, 기존 ILNP 기반의 이동성 환경에서는 단말이 이동 시, 현재 세션을 유지하고 있는 모든 상대 노드와 LU 메시지를 교환해야 하기 때문에, 세션을 유지하고 있는 노드의 수가 증가할수록 LU 메시지 전송 수가 증가하여 네트워크 내 시그널링 오버헤드가 발생할 수 있는 가능성이 있다.

2.3 전술 네트워크 환경 및 이동성 고려사항 분석

전술망은 상용 인터넷망과 매우 다른 구조적, 환경적 특성을 가지고 있다. 첫째, 전술망은 무선 링크를 기반으로 연결되어 있으며 주파수의 사용이 제한적이기 때문에, 유선 링크 기반의 상용망에 비해 상대적으로 낮은 전송속도를 가지고 있다. 둘째, 부대 단말이 접속하는 전술 기동망은 작전 기동에 따라 토폴로지가 변화하나 군의 상하위 체대 구조에 따라 계층적 트리 구조로 연결될 가능성이 높다. 셋째, 전술망에서는 작전에 따라 부대 또는 단말이 이동하는 상황이 빈번하게 발생할 수 있으며, 이로 인해 망의 토폴로지가 고정되어 있지 않고 동적으로 변화하는 특성을 가지고 있다. Fig. 2는 이러한 전술 기동망의 구조를 개략적인 예시로써 나타낸 것이다. 그림은 상위 체대에서 하위 체대로 다수의 트리 구조를 통해 통신소가 접속하는 예시를 보여주고 있다. 그러나 다계층 트리 구조 형태의 전술망에서, 개별 단말 또는 부대는 작전 상황에 따라 다양한 방향으로 이동하기도 한다. 이에 따라, 다양한 시나리오를 통합적으로 관리하기 위한 방안들이 요구된다. 특히 라우터들이 이동하는 환경을 고려할 때, 전술망의 정적 주소 체계 관리에 따라 라우터들의 인터페이스 주소 또는 서버넷 정보들은 고

정적으로 운영되어야 하기 때문에 이동에 따라 라우팅 프로토콜을 통해 라우팅 테이블의 업데이트를 수행해야 하며, 이는 전체 네트워크의 재구성에 상당한 지연을 초래할 수 있는 요인이 된다.

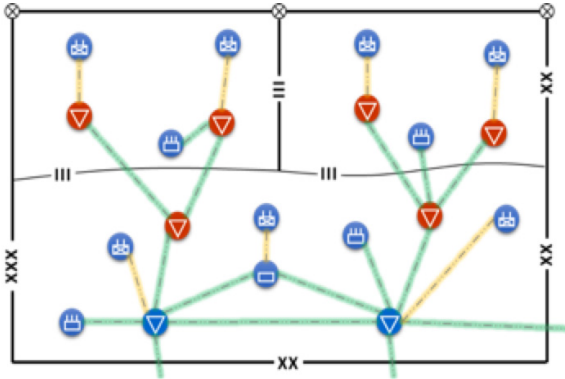


Fig. 2. Conceptual architecture of tactical network

기존의 전술망에서, 이동성 관리는 MIPv4 프로토콜을 사용하여 수행한다. 즉, 계층별로 할당된 서브넷 및 주소 체계에 따라 고정된 IP 주소를 가진 단말이 이동하여 타 부대의 라우터에 접속하면, 원 제대의 라우터 내 앵커 기능과의 시그널링 메시지 교환을 통해 단말의 새로운 접속 라우터와 앵커간 IP 터널을 설립하고 이를 통해 단말 IP로 오는 패킷을 전달한다. 이러한 MIP 기반의 이동성 관리 환경은 전술망에서 운영 시에 몇 가지 문제점을 야기할 수 있다. 첫째로, 계층적 트리 구조 환경에서 단말의 이동 위치에 따라 상위 계층의 라우터를 포함하는 비최적화된 트래픽 경로가 발생할 수 있으며, 이는 제한적인 자원으로 운영되는 전술망에서의 성능 저하 요인이 될 수 있다. 두 번째로, 일반적으로 앵커 기능이 고정되는 유선 환경이 아닌 라우터 기능이 이동할 수 있는 무선 링크 기반의 전술망 환경에서 앵커의 유실로 인한 단말의 통신 두절이 발생할 수 있다. 이러한 전술망 환경을 고려하여, PMIPv6 기반의 분산형 이동성 관리 구조를 제안한 연구^[10]가 진행되었다. 제안하는 구조는 계층적 트리 환경을 고려하여 PMIPv6 기반의 계층적 엔티티를 구성하는 한편, 앵커의 유실 및 네트워크 엔티티의 이동을 고려한 망 안정성 방안을 제안하였다. 그러나, 기존 IP 개념으로 인한 경로 설정 및 터널링 기반의 패킷 전달방식은 전술망에서의 프로세싱 비용의 증가를 가져올 수 있으며, 도메인 간 이동성 제공 등

의 상황에서 일부 비최적화되는 경로 및 지연시간의 증가가 불가피하다.

3. 본 론

앞서 언급된 전술망의 IP 기반 환경에서의 보안 취약한 주소 운영의 문제점 및 제어 프로토콜 기반의 터널링 방식으로 수행되는 이동성 관리의 비효율성을 해결하기 위해서, 본 논문에서는 ILNP 기반의 전술 네트워크 구조를 제안하고, 제안 구조에서의 이동성 관리 방안을 설계한다. Fig. 3은 제안하는 ILNP 기반의 전술망 구조를 나타낸 것이다. 제안 구조에서, 각 단말은 망계획에 따라 64-bit의 고정적인 NID 값을 부여받는다 고 가정한다. 단말의 부여받은 NID를 통해 인접 라우터에 접속하면, 라우터와의 RS(Routing Solicitation)/RA(Routing Advertisement) 메시지 교환을 통해 해당 라우터가 보유한 64-bit의 Locator를 할당받는다. 단말의 접속에 따라 Locator를 할당하면, 단말이 접속한 라우터는 전술망 내 분산 운영되는 DNS 서버에 해당 단말에 대한 L64-NID매핑 정보를 업데이트한다. 접속 단말과 통신하기 위해서, 상대 노드는 단말의 NID를 통해 L64 정보를 획득할 수 있고, 두 정보를 결합하여 이를 128-bit 정보로 구성한 후 IPv6 헤더의 목적지 주소로 설정함으로써 IPv6 라우팅을 기반으로 단말에게 패킷을 전송할 수 있다.

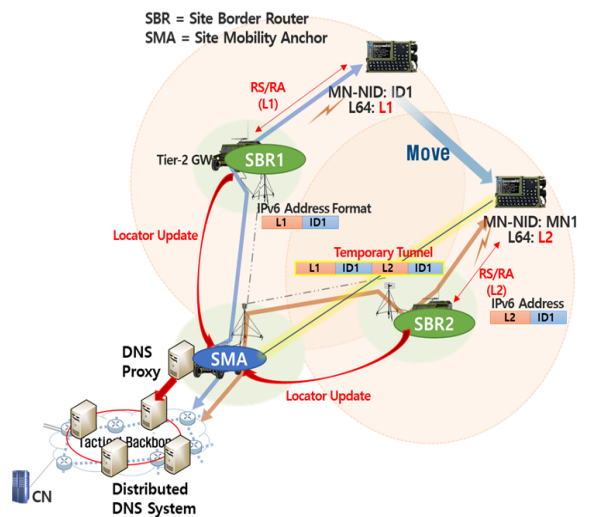


Fig. 3. ILNP based tactical network architecture

이동성 관리를 위해서, 본 논문에서는 단말이 이동성 관리 과정에 관여하지 않고 네트워크에서 단말 대신 이동성 관리를 수행하는 네트워크 기반의 이동성 관리 기법을 제안한다. 제안하는 이동성 관리를 위해서, 본 논문에서는 두 개의 새로운 네트워크 엔티티를 정의한다. 단말이 직접 접속하는 라우터에 구현되는 SMR(Site Mobility Router)은 MN에 대한 프록시 역할을 수행하는 기능으로, MN의 접속을 감지하고 MN에 L64 값을 할당하는 역할을 수행한다. 이와 함께, SMR은 상위 계층의 기능인 SMA(Site Mobility Anchor)에 업데이트된 매핑 정보를 LU 메시지를 통해 전달하여 네트워크 내 경로 업데이트를 요청한다. 상위 계층의 라우터에 구현되는 SMA 기능은 DNS 프록시 서버 기능을 수행하여 SMR로부터 수신하는 LU 메시지를 기반으로 상위 분산 DNS 시스템에 단말에 대한 NID-L64 매핑 정보를 업데이트한다. 이와 함께, SMA에서는 단말의 이동에 따른 NID-L64 매핑 정보의 변경 시 임시적으로 단말에 대한 기존 L64-NID 매핑 정보에 대한 터널링 기반의 패킷 전달을 수행한다. 즉, 기존 L64-NID 매핑 값을 목적지로 하는 IP 패킷 전달을 위해 단말의 새로 접속한 SMR과 임시 터널을 생성함으로써 단말의 트래픽이 단절되지 않도록 지원한다. SMA와 SMR간의 터널링 기반의 트래픽 전달은 캡슐

화를 위한 프로세싱 비용은 발생하지만, 전술망의 계층적인 구조 내에서 최적화된 경로를 제공하여 트래픽의 전달에 따른 지연시간은 미미하다. 추가적으로, SMA는 필요에 따라 단말 대신 직접 단말이 세션을 유지하고 있는 상대 노드인 CN(Corresponding Node)에게 LU 메시지를 전송하여 단말의 패킷을 전달할 수 있다. 그러나, 단말이 이동하여 업데이트된 NID-L64 매핑 정보가 통신 상대 노드에게 아직 전달되지 않은 경우에도 단말의 기존 매핑 정보로 오는 패킷은 SMA를 통해 단말에게 최대한 손실 없이 보낼 수 있으며, 기존의 바인딩 정보로 오는 패킷에 대해서도 터널링 기반의 패킷 전달을 수행할 수 있다.

제안 환경에서, 단말이 새로운 위치로 이동하였을 때 지원되는 이동성 지원 절차는 Fig. 4와 같다. 이동 단말인 MN이 기존의 SMR1에서 L64값인 Loc1을 할당받게 되면, SMR1은 SMA에게 MN의 NID-L64 매핑 정보를 LU 메시지를 통해 업데이트한다. SMA에서 각 분산 DNS 환경에 Update된 매핑 정보를 통해 CN은 MN의 NID-L64 매핑 정보를 받아 MN과의 세션을 설립할 수 있다. MN이 SMR1에서 SMR2로 이동하면, SMR2와의 RA/RS 메시지 교환을 통해 새로운 L64 값인 Loc2를 할당받는다. SMR2는 MN의 할당받은 Loc2에 대한 매핑정보를 LU 메시지를 통해 SMA에 업데이트

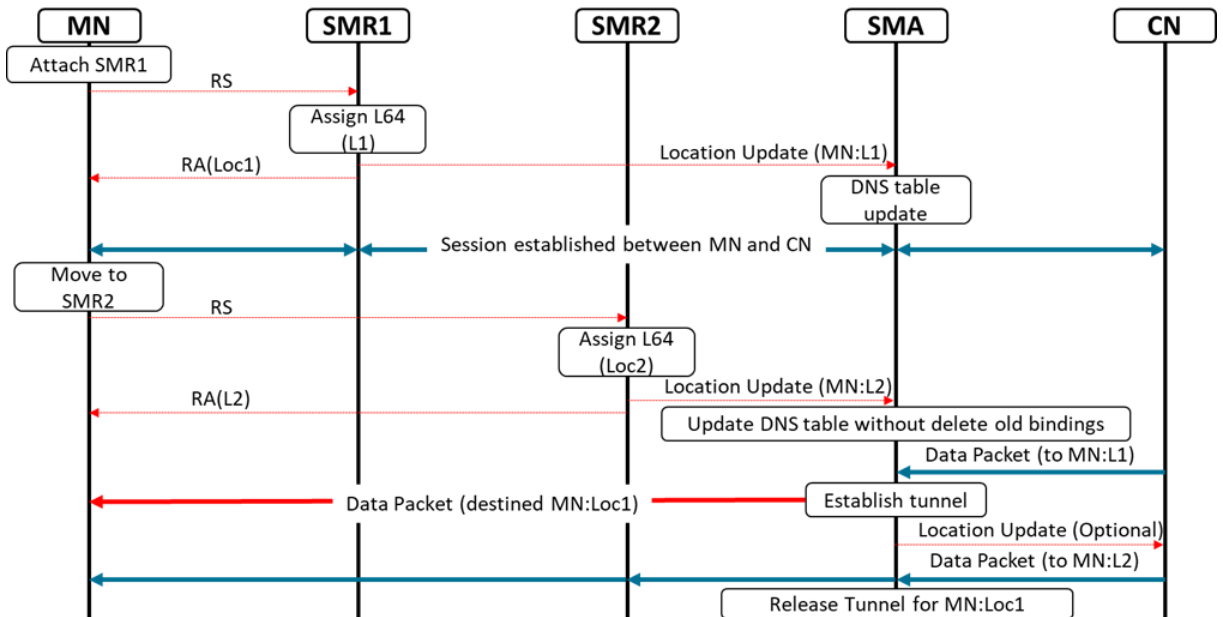


Fig. 4. Handover procedure in proposed architecture

이트하고, SMA는 새로운 NID-L64 매핑 정보를 DNS 테이블에 업데이트 함으로써 분산 DNS 데이터베이스 간 동기화를 수행하는 한편, 기존의 NID-L64(Loc1)에 대한 정보를 삭제하지 않고 일시적으로 유지한다. 이는 단말의 새로운 L64 바인딩 정보에 대한 Locator Update 과정이 적용되기 이전에 보낸 패킷에 대해서, 기존 NID-L64 값으로 구성되는 IPv6 형태의 주소를 처리하기 위한 것으로, 해당 값으로 오는 패킷들은 단말의 새로운 NID-L64 값으로 구성되는 주소를 목적지로 하는 IP 패킷 헤더로 캡슐화하여 단말의 이동 후 위치로 전송한다. 단말에서 현재 통신 중인 CN에게로 전송한 LU 메시지가 CN에 도착하여 CN에서 새로운 NID-L64 값을 목적지로 하는 패킷을 전달하기 시작하거나 기존 세션들이 종료되어 이전의 바인딩 된 주소로 오는 패킷이 더 이상 없는 경우에, SMA로는 더 이상 기존 NID-L64 값을 목적지로 하는 패킷이 오지 않을 것이며, 이는 SMA에서 각 바인딩 값에 대한 테이블 매핑 카운터를 통해서 감지할 수 있다. 따라서 일정시간동안 기존 NID-L64 값을 목적지로 하는 패킷이 SMA에 유입되지 않으면, SMA는 기존의 NID-L64 값을 삭제하고 새로운 값으로만 라우팅을 수행할 수 있다. 이러한 방식을 통해, 전송망 환경에서 네트워크 기능에 대한 이동성 빈도가 높은 단말의 직접접속 지점인 SMR 대신 상대적으로 더 안정적으로 운영되는 상위 계층 엔티티인 SMA를 통해 단말의 기존 NID-L64 바인딩에 대한 패킷 전달 역할을 수행하게 함으로써 전송망 환경에서 기존 L64에 대한 라우팅 종단점인 라우터의 유실 시에도 전달이 가능하게 하여 네트워크에서의 안정성을 제공할 수 있다. 또한, 서로 다른 CN과 세션을 설립하고 있는 MN의 경우, 기존 방식에서는 모든 상대 노드에게 LU 메시지를 보내야 하는 것과 달리 한번의 LU 메시지 전송으로 패킷의 경로를 전환할 수 있기 때문에 시그널링 오버헤드를 효과적으로 줄일 수 있다.

4. 성능 분석

본 논문의 성능 분석을 위해서, 기존 연구^[10]에서 분석을 위해 설정한 전송망 토폴로지 모델과 동일한 모델을 기반으로 IP기반의 이동성 관리 프로토콜과 ILNP 기반의 제안 기법과의 성능 차이를 정량적으로 분석하고자 한다. Fig. 5는 분석을 위한 토폴로지 모델을

나타낸 것으로, 계층적 트리 구조에서의 하위 네트워크 간에 이동 단말이 이동하는 시나리오를 표현한 것이다. 각 상위 계층의 네트워크 노드와 하위 계층의 네트워크 노드는 분석하고자 하는 프로토콜에 따라 그 역할이 정의된다. 예를 들어, MIPv6 프로토콜을 토폴로지 모델에 적용하는 경우에는 하위 네트워크 노드가 단말의 앵커 노드인 HA(Home Agent)에 해당하며, 상위 네트워크 노드는 일반 게이트웨이로써 동작한다. PMIPv6 기반 환경을 고려하면, 상위 노드는 단말의 앵커 노드인 LMA(Local Mobility Anchor)로, 하위 노드는 MAG(Mobility Access Gateway)로써 동작한다. 해당 분석 모델에서, 하위 계층의 네트워크 노드 간에는 직접링크가 존재하지 않는다. 상위 계층과 하위 계층 네트워크 기능간의 링크와 하위 계층과 이동 단말간의 링크는 둘 다 무선링크지만 전송망 환경을 반영하여 링크 특성에 따라 백본망의 상위 계층에서 전투 무선망의 하위 계층으로 연결되는 *a* 링크와 전투 무선망에서 하위 네트워크 체계가 단말과 연결되는 *b* 링크로 구분하고, *a* 링크와 *b* 링크의 전달 비용의 차이를 4:1 수준으로 반영하였다. 그림과 같은 토폴로지 모델을 기반으로, 기존의 연구^[10]에서 분석한 비용 분석 및 지연시간 분석 외에 본 논문에서는 이동 단말의 수에 따른 핸드오버 시에 발생하는 오버헤드를 기존 연구^[11]에서 제안한 성능 방법을 기반으로 추가 분석하였다.

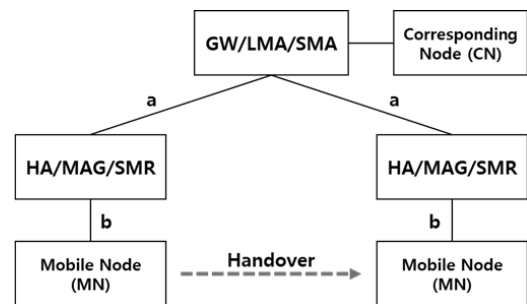


Fig. 5. Topology model for performance analysis

4.1 핸드오버 오버헤드 성능 분석

참조 연구^[11]에서는 네트워크 내 MN의 수 N_{MN} 과 세션을 유지하고 있는 CN의 수 N_{CN} 의 증가에 따른 시그널링 메시지의 오버헤드를 분석하였다. MIPv6 기반의 이동성 환경에서, MN의 이동에 따라 이동성 제공을 위한 BU(Binding Update) 메시지는 CN의 개수와

상관없이 MN의 홈 라우터인 HA와 한 번만 발생하며, 이는 다음과 같은 식으로 나타난다.

$$\text{Overhead} = N_{MN} \cdot (BU_{HA} + BAcK_{HA}) \quad (1)$$

PMIPv6 기반의 이동성 환경에서, MIPv6 기반 환경과 유사하게 MN의 이동에 따른 시그널링은 CN의 수와 무관하게 앵커인 LMA(Local Mobility Anchor)와 한 번만 수행한다.

$$\text{Overhead} = N_{MN} \cdot (PBU_{LMA} + PBAcK_{LMA}) \quad (2)$$

ILNP기반의 이동성 환경의 경우, MN이 새로운 곳으로 이동하여 핸드오버 수행 시, MN이 전송하는 LU 메시지는 현재 세션을 유지하고 있는 CN에게 각각 전송되며, 이는 다음과 같이 나타난다.

$$\text{Overhead} = N_{MN} \cdot N_{CN} \cdot (LU_{CN} + LUAcK_{CN}) \quad (3)$$

마지막으로, 제안하는 이동성 지원 환경에서, MN이 핸드오버를 수행하면 이동성 지원을 위한 LU 메시지는 단일 MN에 대해 CN의 수와 상관없이 SMR에서 SMA로 한번 발생한다.

$$\text{Overhead} = N_{MN} \cdot (LU_{SMA} + LUAcK_{SMA}) \quad (4)$$

시그널링 개수에 대한 오버헤드와 함께, 해당 시그널링 패킷에 대한 바이트 수를 계산하여 바이트 오버헤드를 함께 분석하였다. 각 시그널링 메시지의 크기는 Table 1과 같이 구성되며, 참조 연구^[11]에서 수행한 tcpdump 기반의 메시지 크기를 참조하였다. PMIPv6 환경에서의 시그널링 메시지의 경우, MIPv6 기반의 시그널링 메시지 크기와 동일하게 설정하였다.

Table 1. Packet size of signaling packets

Scheme	Message Type	Size(bytes)
MIPv6	BU(Binding Update)	110
	BACk(Binding Update Ack)	
PMIPv6	PBU(Proxy Binding Update)	110
	PBA(Proxy Binding Ack)	
ILNP	LU(Location Update)	86
	LUAcK(Location Update Ack)	

4.2 패킷 전달 비용 분석

단말의 핸드오버 시의 오버헤드 분석과 함께, 단말의 핸드오버에 따르는 패킷 전달 비용을 분석하였다. 패킷 전달 비용은 단말의 이동성 지원을 위한 시그널링 이후 패킷 전달을 위한 경로 및 각 네트워크 노드에서의 패킷 전달을 위한 프로세싱을 고려한 것으로서, 전술망의 제한적 환경 내에서 최대한 패킷 경로를 최적화하고 있는지를 가능할 수 있는 지표 중 하나이다. 이를 위해서, 기존 연구^[10]에서 전술망을 고려한 동일 토폴로지 모델을 적용하여 MIPv6, PMIPv6 적용 시 패킷 전달 비용 및 지연시간을 제안 기법과 비교하였다. 핸드오버 수행 시 기존 세션의 상대노드마다 모두 LU 메시지를 전송해야 하는 ILNP의 경우 해당 비교분석에서는 제외되었으며, ILNP 기반 이동성 관리 중 호스트 기반의 이동성 관리 기법^[9]은 MIPv6 적용 시나리오 절차와 동일한 시그널링 교환 절차를 가지고 있어 분석과 동일한 것으로 간주하였다. 패킷 전달비용인 PDC_{scheme} 는 바인딩 업데이트 이후, 단말의 패킷을 전달하기 위해 소요되는 네트워크 자원 비용을 산정한 것으로서, 패킷 도달률 λ_p 와 홈 간 패킷 전달 비용의 계산 함수인 $C_{cm}^{f,x}$ 의 곱으로 정의된다.

$$PDC_{Scheme} = \lambda_p C_{cm}^{f,x}(t_U) \quad (5)$$

식 (5)를 기반으로, MIPv6와 PMIPv6의 패킷 전달 비용은 다음과 같은 식으로 나타난다.

$$\begin{aligned} PDC_{MIPv6} &= \lambda_p C_{cm}^{f,4}(t_U) \\ &= \lambda_p \eta (C_b + 3C_a + 2PC_{HA} + 2PC_{GW}) \end{aligned} \quad (6)$$

$$\begin{aligned} PDC_{PMIPv6} &= \lambda_p C_{cm}^{f,2}(t_U) \\ &= \lambda_p \eta (C_b + C_a + PC_{LMA} + PC_{MAG}) \end{aligned} \quad (7)$$

제안 기법에서, 전술한 것처럼 핸드오버 이후 세션이 연결된 CN들이 기존 NID-L64 바인딩 정보를 계속 유지하는 경우에는 SMA와 SMR간의 터널링을 통해 패킷이 전달되며, 이 때 패킷 전달 비용은 다음과 같은 식으로 계산된다.

$$\begin{aligned} PDC_{proposal} &= \lambda_p C_{cm}^{f,2}(t_U) \\ &= \lambda_p \eta (C_b + C_a + PC_{SMA} + PC_{SMR}) \end{aligned} \quad (8)$$

제안 기법에서, 더 이상 기존의 NID-L64 값을 목적

지로 하는 패킷이 오지 않는 경우, SMA와 SMR간의 터널링이 아닌 일반 라우팅으로 패킷이 전달되며, 이 때 전달 비용은 다음과 같이 계산된다.

$$\begin{aligned}
 PDC_{proposal} &= \lambda_p C_{cm}^{f,2}(t_U) \\
 &= \lambda_p \eta (C_b + C_a + 2PC_{GW})
 \end{aligned}
 \tag{9}$$

η 은 제어 메시지 대비 데이터 패킷 메시지 크기의 비율로써 데이터 패킷 메시지 사이즈 s_d 를 제어 메시지의 사이즈인 s_c 로 나눈 값으로 정의된다. 패킷 전달

비용 산정을 위해서, Table 2와 같은 기본값을 참조하였다. 각 네트워크 엔티티에서의 프로세싱 비용인 PC 는 각 엔티티에서 바인딩 정보를 검색하거나 터널링을 위한 캡슐화 과정에 소요되는 비용으로써, 참조 연구^[11] 및 기존 연구들에서 제시하는 일반적인 값으로 산정하였다.

4.3 분석 결과

핸드오버의 오버헤드 성능 분석을 위해서, MN과 CN의 수를 0에서부터 100개까지 증가하며 핸드오버 시 발생하는 시그널링 메시지의 총 패킷 크기를 계산하였다. Fig. 6은 핸드오버 오버헤드의 분석 결과를 그래프로 나타낸 것이다. 그림에서 알 수 있듯이, ILNP의 기본 핸드오버 과정에서는 CN의 수가 증가함에 따라 기하급수적으로 핸드오버 시 시그널링 메시지가 증가하여 네트워크 내 패킷 바이트 수가 증가하지만, 제안 기법에서는 핸드오버 시 단말이 기존 세션에 대해 모두 LU 메시지를 전송하지 않고 SMA를 통해서 네트워크 경로를 제어하기 때문에 MIPv6 또는 PMIPv6 기반의 기존 ILNP 기법 대비 큰 오버헤드 감소를 나타내었다. 핸드오버 시 단일 시그널링 교환 과정만 수행하는 MIPv6 및 PMIPv6 기반 환경과 비교하였을 때는 차이가 크지는 않지만 제안 기법의 오버헤드가 감소하는 것을 볼 수 있는데, 이는 기존의 MIPv6 또는 PMIPv6의 시그널링 메시지의 크기보다 LU 메시지의 크기가 적기 때문으로, 이는 IPv6 기본 헤더에 기존 이동성 프로토콜과 같이 확장 헤더를 사용하지 않고도 이동성 제공이 가능하기 때문에 실제 패킷 크기가 감소하여 이동 단말이 많아질수록 네트워크 내 혼잡이 상대적으로 감소할 수 있음을 알 수 있었다.

Table 2. Notation for analysis parameters

Parameter	Description	Default Value
N_{MN}	Number of MN	1
N_{CN}	Number of CN	1
λ_p	Packet arrival rate	10
s_c	Control packet size	68 bytes
s_d	Data packet size	1500 bytes
C_a	Trasmission cost for the wireless link a	10
C_b	Trasmission cost for the wireless link b	40
$PC_{HA/LMA/SMA}$	Processing cost of HA/LMA	24
$PC_{MAG/SMR}$	Processing cost of MAG/SMR	12
PC_{GW}	Processing cost of legacy GW	8

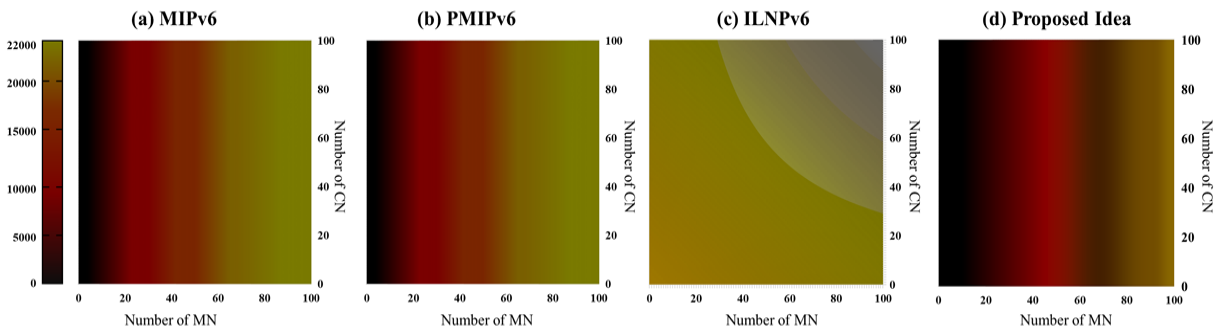


Fig. 6. Analysis results of handover overhead

Fig. 7은 패킷 도달율의 증가에 따라 패킷 전달 비용의 추이를 분석한 결과를 그래프로 나타낸 것이다. 제안 기법은 기존의 L64 값을 이용하는 경우에는 PMIPv6보다는 많은 전달비용을 나타내었으나, 새로운 L64 값으로 업데이트 된 이후에는 비교 기법들 중에 가장 낮은 패킷 전달비용을 보였다. 이는 새로운 NID-L64 값의 경우에 네트워크에서 패킷 전달을 위한 터널링 등의 특별한 동작이 필요없이 일반적인 라우팅으로 처리가 가능하기 때문에 네트워크 노드에서의 프로세싱 비용의 감소에 따른 것으로 보인다.

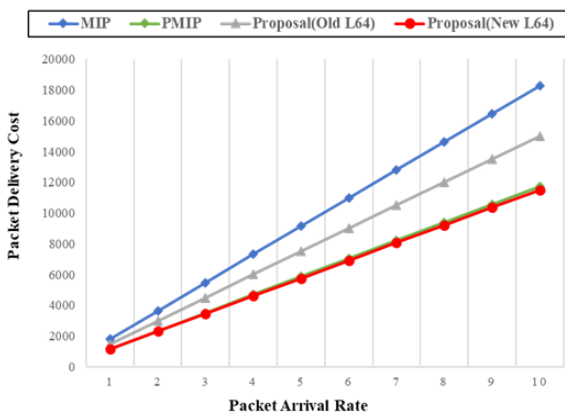


Fig. 7. Analysis results of packet delivery cost

5. 결론

본 논문은 전술망 환경에서 ID/LOC 분리에 따른 유연한 네트워크 관리 구조를 설계하고, 제안하는 ILNP 기반의 전술망 환경에서 이동성 관리를 효과적으로 제공하기 위한 네트워크 기반의 이동성 관리 기법을 제안하였다. 제안하는 구조는 전술망에서 기존에 고정적이고 영구적인 IP 할당체제로 인해 발생했던 확장성 및 네트워크 부하와 같은 문제를 IP의 개념을 분리함으로써 해결할 수 있으며, 특히 ILNP 기반의 ID/LOC 분리 구조의 도입을 통해 기존 IPv6 지원 라우터들과의 호환성 및 네트워크 적용의 용이성을 제공할 수 있다. ILNP의 핸드오버 시 상대 노드에게 위치를 업데이트하는 이동성 관리 기법은 통신 상대노드가 많을수록 네트워크 내 위치 업데이트를 위한 시그널링 메시지의 부하가 급증하기 때문에, 본 논문에서는 제한적인 자원을 가진 전술망 환경에서 시그널링

를 효과적으로 감소하고, 계층적 트리 구조 형태의 망 환경에서 경로를 최적화하기 위한 네트워크 기반의 이동성 관리 방안을 제안하였다. 분석을 통해, 제안하는 기법은 기존에 제안된 ILNP 기반의 이동성 관리 기법에 비해서 월등하게 핸드오버 오버헤드가 감소하였으며, MIPv6 및 PMIPv6 등과 같은 IP 기반의 이동성 관리 기법과 비교하여서도 네트워크 내 이동 단말의 수가 많아질수록 상대적으로 자원 효율적으로 이동성을 수행할 수 있음을 확인하였다.

ID/LOC 분리 기반의 환경에서 전술한 바와 같이 위치 의존성 탈피로 인한 단말의 신원 보안성을 제공할 수 있으나, 단말의 NID-L64 바인딩 정보가 항상 네트워크 내에서 접근이 가능해야 하기 때문에 바인딩 정보를 관리하는 분산 DNS 시스템의 보안성 강화 및 접근 제어 등의 추가적인 안정성 제공방안이 적용이 확장된다면 더욱 보안성이 강화된 전술 체계의 구성이 가능할 것이다. 이와 더불어, 전술망에서의 안정성 향상을 위해 네트워크 노드의 유실 또는 이동으로 인한 토폴로지가 변화할 때 이에 따라 동적으로 단말의 경로 최적화 및 세션 유지를 위한 확장 방안은 추후 연구를 통해 진행할 예정이다.

후 기

본 연구는 국방과학연구소가 지원하는 미래 전술망의 통합네트워킹 구조 및 상호연동 Gateway 기술연구 과제의 일환으로 수행되었습니다(UE161127ED).

References

- [1] K. Kim and S. Lee, "A Method for IPv6 Address Assignments of the Next Generation Defence Network," Journal of KIISE, Vol. 14, No. 4, pp. 441-445, 2008.
- [2] B. Jun, J. Kang, J. Yoo and K. Shin, "An Analysis of IPv6 Transition Status and Efficient Address Allocation for the Defense Information Systems," Korean Journal of Military Art and Science, Vol. 73, No. 3, pp. 227-249, 2010.
- [3] R. Braden, "Requirements for Internet Hosts - Communication Layers," IETF, RFC 1122, Oct. 1989.

- [4] D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6," IETF, RFC 3775, Jun. 2004.
- [5] S. Gundavelli, K. Leung, V. Devarapalli, K. Chwdhury and B. Patil, "Proxy Mobile IPv6," IETF, RFC 5213, Aug. 2008.
- [6] F. Qui, X. Li and H. Zhang, "Mobility Management in Identifier/Locator Spilt Networks," Wireless Personal Communications, Vol. 65, No. 3, pp. 489-514, 2012.
- [7] D. Farinacci, V. Fuller, D. Meyer and D. Lewis, "The Locator/ID Separation Protocol(LISP)," IETF, RFC 6830, Jan. 2013.
- [8] R. J. Atkinson and S. Bhatti, "Identifier-Locator Network Protocol(ILNP) Architectural Description," IETF, RFC 6740, Nov. 2012.
- [9] D. Phoomikiattisak and S. Bhatti, "End-To-End Mobility for the Internet Using ILNP," Wireless Communications and Mobile Computing, Vol. 2019, pp. 1-29, Apr. 2019.
- [10] K. Sun, Y. Kim, H. Noh, H. Park, M. Han and D. Kwon, "PMIP-based Distributed Mobility Management for Tactical Network," Journal of the Korea Institute of Military Science and Technology, Vol. 22, No. 5, pp. 1-13, 2019.
- [11] D. Phoomikiattisak and S. Bhatti, "Control Plane Handoff Analysis for IP Mobility," 9th IFIP Wireless and Mobile Networking Conference(WMNC), pp. 65-72, Jul. 2016.