이종 네트워크 환경에서 다중 인터페이스 단말을 활용한 끊김 없이 안전한 서비스 프레임워크†

(Seamless and Secure Service Framework using Multiple Network Interfaces Terminal in Heterogeneous Environment)

윤 성 현*, 이 순 석**, 김 상 하***
(Sunghyun Yoon, Soon Seok Lee, and Sang-Ha Kim)

요 약 정보통신기술의 지속적인 발전에 따라 인터넷 상에서 전자금융거래, 전자상거래와 같이 개인정보의 보안이 중요시 되는 민감 서비스의 확산이 빠른 속도로 전개되어 가고 있다. 이에 따라 개인정보의 보호는 물론이고 개인정보를 활용하는 민감 서비스 자체의 안전성 보장이 매우 중요시 되고 있다. 아울러 스마트폰의 대중화와 더불어 무선인터넷이 보편화 되면서, 기존 유선환경을 중심으로 제공되었던 서비스들은 점차 유무선 통합 환경으로 확산되어가고 있다. 따라서 새로운 환경에 적합한 안전하고 안정적인 통신 패러다임이 요구되고 있다. 이 논문은 사용자 정보와 네트워크 정보를 함께 이용함으로써 사용자 단말과 민감 서비스를 제공하는 서버간 끊김 없이 지속적인 안전 관계를 유지할 수 있게 하는 서비스 프레임워크를 제안한다. 제안하는 서비스 프레임워크는 개인정보가 유출되더라도, 단말을 분실하지 않는 한 제 3자에 의한 부정사용을 원천적으로 차단한다. 또한 점차 보편화 되고 있는 이종망간 이동 환경에서 단말의 이동에 따라 가입자 망이 변경되더라도 안전한 서비스 환경을 안정적으로 제공한다.

핵심주제어 : 서비스 연속성, 서비스 안전성, 이종 네트워크, 다중 네트워크 인터페이스

Abstract As the Information and Communication Technologies continue to advance, some sensitive services (e.g. e-commerce, on-line financial service, and etc.) have spread rapidly. Accordingly, ensuring the safety of the sensitive service itself using personal information as well as the protection of personal information Is becoming very important. In addition, with the popularization of smart phone and the universalized use of wireless Internet, many services that have been provided on the basis of the conventional wired network are increasingly propagating to wired and wireless converged network environment. These changes in the network environment requires new paradigm for the pursuit of safe and stable communication. In this paper, we propose seamless and secure service framework that can facilitate a sustainable secure connection between the user terminal and the sensitive service system by using both the personal and network information. The proposed service framework is capable of isolating the source of authorized use by a third party of the personal information as far as the user terminal is not lost, although some personal information is disclosed. Besides, it can

† 이 논문은 2011년 MKE 지식경제 기술혁신사업 (산업융합원천기술개발사업) 연구비 지원에 의해 연구되었음 "All-IP 융합 네트워크 구축을 위한 유선-LTE-WiBro-B4G 망 통합용 단일 제어체계 액세스 시스템 기술개발".
* 한국전자통신연구원 유무선융합네트워크연구팀, 제1저자
** 한국전자통신연구원 융합네트워크연구부, 제2저자
*** 충남대학교 컴퓨터공학과, 교신저자

provide a seamless and safe service environment even if the access network is changed by relocation of terminals in the heterogeneous mobile network environment.

Key Words : service safety, service continuity, heterogeneous network, multiple network interfaces

1. 서 론

최근 정보통신 서비스의 이용이 보편화 되고 인터넷 기술이 지속적으로 발전함에 따라 인터넷을 이용한 서비스는 매우 다양해지고 있으며, 전자 상거래, 전자 정부 등과 같이 과거 주로 오프라인 환경에서 제공되거나 행해졌던 서비스들 중 대다수가 이미 무선 환경을 포함한 온라인 영역에서 활발히 이루어지고 있다[1][2]. 이에 따라 개인정보의 활용을 통한 인증 및 결제 등과 같은 민감서비스의 신뢰성 또한 매우 중요시 되고 있다. 특히 온라인 주식거래, 전자상거래, 인터넷 뱅킹과 같은 전자 금융 서비스처럼 개인정보에 민감한 서비스들은 일단 사용자의 신뢰가 무너지면, 향후의 거래도 지속적으로 회피하게 되는 평판 리스크의 비중이 크기 때문에 서비스 안전성이 매우 중요하게 다루어져야 한다 [30].

현재 인터넷을 통한 민감 서비스를 이용함에 있어, 사용자 인증에 주로 사용되는 방법은 ID/Password, Mobile OTP, 공인 인증서(Digital Certificates) 등과 같은 개인정보에 기반한 방법이다. 따라서 바이러스 감염, 악성코드 또는 악성 앱 등에 의한 개인정보의 유출을 막기 위해 백신 프로그램, 방화벽 등 보안 프로그램이 지속적으로 개발되고 있지만, 이미 알려진 악성 프로그램을 제거하기 위한 용도로 사용되는데 그치고 있는 실정이다. 따라서 단말의 보안 수준이 아무리 높아도 개인정보 유출의 위험성은 항상 존재할 수 밖에 없다 [31][32]. 비단 온라인 환경에서뿐만 아니라 오프라인 환경에서도 개인정보의 유출은 개인정보 관리업무 미숙, 내부자 고의 유출, 보안카드와 같은 개인정보 미디어의 절도 및 분실, 사용자 부주의에 따른 구매 기록 추적 및 수집, 직권 오남용에 따른 정보열람 등과 같이 다양한 방법에 의해 이루어질 수 있다.

일단 유출된 개인정보는 불법 거래를 통해 악의적 사용자들에게 광범위하게 유통 될 수 있다. 더욱이 통상 사용자는 자신의 개인정보 유출을 인지하지 못하는 경우가 대다수이므로, 악의적 사용자에 의한 개인정보 도용 사고로 이어질 가능성이 매우 높은 문제가 있다. 즉, 기존 개인정보에 의존한 인증방법은 개인정보가 유출된 상황에 대한 대비책이 매우 취약하다 할 수 있다. 비록 서비스 안전성의 필수 요건이 되는 사용자 인증에 있어 유출된 개인정보의 도용을 막을 수 있는 다양한 방법이 시도되고 있지만 [28][33], 개인정보 유출 및 도용은 클라이언트 영역에서 시스템 영역까지 수많은 다양한 방법으로 시도되고 있기 때문에, 비록 대부분의 영역이나 기법에 대한 보안 수준이 만족된다 하더라도, 일부 특정 영역에서 보안의 허점이 발생한다면, 안전성을 담보하기 어렵다 [30].

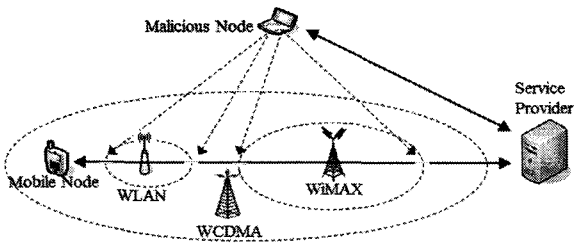
한편, 근래의 인터넷 환경은 유무선의 경계가 사라지고 서비스의 무게중심이 점차 유선에서 무선으로 이동하고 있는 패러다임 변화 (Paradigm Shift)가 급격히 진행되고 있다. 전 세계적으로 유선인터넷 사용자는 정체되는 반면 무선인터넷 이용자는 지속적으로 증가하고 있으며[3][4], 상대적으로 통신환경이 낙후된 후진국 및 개발도상국에서는 막대한 초기비용 절감 및 빠른 인프라 구축을 위해 오히려 유선보다는 무선이 주된 통신인프라로서 자리잡아가고 있다 [5].

이러한 시대적 상황에 따라, 과거 유선 환경에 최적화되어 제공되었던 풍부한 서비스들 또한 언제 어디서나 이용할 수 있도록 무선환경에 적합한 서비스로 빠르게 전환되어 가고 있다. 특히 최근에는 소형 컴퓨터라 할 수 있는 스마트폰의 대중화에 따라 무선 인터넷을 이용한 서비스의 사용이 그 어느 때보다 매우 활발해지고 있으며, 현재의 모바일 디바이스는 점차 다중인터페이스를 가진 복합 단말로 진화하고 있기 때문에 [34], 무선 환경의 증가세는 점차 가속화되고 있다.

그러나 무선인터넷 서비스 사용이 급격히 증가하면서, 단일 액세스 기술만으로는 폭발적으로 증가하는

무선 데이터 트래픽의 성장속도를 원만하게 수용할 수 없게 되었다. 이런 한계성으로 인해 이종망간 이동이(또는 사업자간 이동) 보편화 되고 있으며, 이런 환경에서는 사용자의 이동에 따라 단말의 네트워크 연결상태가 수시로 변경되므로 보안 세션의 연속성이 문제가 된다.

그림1은 이종망간 이동환경에서 발생 가능한 잠재적 보안 허점을 나타낸다. 사용자 단말은 다양한 접속망을 통하여 서비스 시스템에 접근할 수 있지만, 각 접속망에 따라 단말과 서비스시스템간에는 서로 다른 보안 채널이 형성되기 때문에, 단말이 이동함에 따라 접속망이 변경되면 결제 및 인증과 같은 보안세션이 필요한 서비스를 보장하기 어렵다. 더 나아가 다양한 액세스 망을 통해 단말과 서비스시스템간 보안세션이 체결될 수 있는 특성 때문에, 악의적 사용자가 개인정보 도용을 통해 정상 사용자를 가장한 접근을 시도할 경우에는 정상 사용자에 의한 접근과 개인정보 도용에 의한 접근의 차이를 구분할 수 없다. 이러한 문제를 해결하기 위해서는 이종망간 이동 환경에서 사용자가 이동함에 따라 수시로 가입자 망이 변경되어도 끊김 없이 일관된 보안 세션을 보장해 줄 수 있는 실시간 보안 연속성 기술이 새로이 요구된다.



<그림 1> 잠재적 보안 허점

이 논문은 이종망간 이동 환경에서 접속망에 무관하게 단말과 서비스 시스템간 상호 신뢰성을 제공하고, 사용자의 이동에 따라 접속망이 변경되어도 보안 세션의 연속성을 보장하는 서비스 프레임워크를 제안한다.

이 논문은 다음과 같이 구성한다. 2장에서는 문제해결을 위해 기존에 진행되었던 사항들을 살펴보고, 3장에서는 제안하는 서비스 프레임워크를 위한 클라이언트/서버 기반 매니지드 구조, 클라이언트 및 서버 기능구조, 클라이언트와 서버간 프로토콜 등을 설명한다. 4장에서는 안전성 보장이 요구되는 서비스의 제공 및 이용을 위한 서비스 시나리오를 제시하고, 5장에서는 성능 측정을 위한 시험환경을 구성하고 실험을 통해 제안하는 서비스 프레임워크의 우수성을 입증한다. 마지막으로 결론 및 향후 연구사항을 정리한다.

2. 관련 연구

정보통신기술의 발달과 더불어 민감 서비스를 안전하게 제공하기 위해 다양한 기술이 연구되어 왔다. 특히 개인정보에 가장 민감한 서비스 중 하나인 전자금융 서비스는 서비스의 특성상 상대적으로 가장 안전한 서비스 이용 수단을 제공하여 왔다. 금융거래의 효율성 및 편리성을 추구하기 위해 전자금융서비스는 인터넷이 보편화 되기 이전부터 패킷망에 비해 상대적으로 안전한 회선망을 기반으로 발전하였다.

유선전화망에서 지능망 기술을 이용한 서비스로 제공되었던 폰뱅킹(모바일뱅킹)은 개인정보와 네트워크 회선정보를 함께 이용함으로써 매우 안전한 서비스 인증 수단을 제공한다[6][7]. 폰뱅킹은 지정된 사용자 뿐만 아니라 사용자에게 지정된 회선에서만 서비스 이용을 승인하므로, 설령 개인정보가 유출되어 악의적 사용자에게 도용된다 하더라도 지정된 회선 이외에서는 서비스 이용을 승인하지 않으므로 매우 안전한 인증 수단이지만, 회선망에 종속적인 기술이므로 패킷 기반의 이종 네트워크 환경에서는 적용이 쉽지 않다.

통신환경이 회선 중심에서 패킷 중심으로 전환되면서 인터넷을 이용한 서비스들이 생활의 일부로 자리 잡게 되었고, 이에 따라 상대적으로 안전에 취약한 TCP/IP 기반 인터넷을 보완하기 위해 다양한 기술들이 연구되었다.

IPSec은 Network Layer에서 IP 패킷을 보호하기 위한 가장 대표적인 기술로서, 통상 VPN (Virtual Private Network) 구현에 많이 이용된다 [23]. IPSec을 이용한 네트워크 보안은 상위 레이어에 존재하는 기존 응용에 수정을 가할 필요가 없는 장점이 있지만, 한편으로는 상위 레이어에서는 IPSec의 동작을 알 수 없기 때문에 모든 IP packet이 암호화되어 전송되므로

선택적으로 사용할 수 없는 단점이 있다. 따라서 효율성 문제로 인하여 전체 네트워크를 IPSec을 이용하여 보호하는 것은 어렵다.

SSL(Secure Socket Layer)/TLS(Transport Layer Security)는 웹 서버와 브라우저간의 안전한 통신을 위해 개발되었으며, TCP 상위 계층에서 동작하므로 TCP를 이용하는 모든 종류의 응용에 적용이 가능하다 [8][9]. 따라서 응용에 대한 선택적인 제어를 통하여 특정 데이터에 대해 메시지를 암호화 할지 여부를 결정할 수 있으므로 IPSec보다 유연한 환경을 제공한다.

WTLS는 TLS를 무선 환경에 맞게 변형한 프로토콜이다. 무선 환경에 적합하게 만들기 위하여 관련 인자들의 길이를 줄이고, 전송계층으로 UDP를 사용한다는 차이점이 있지만, WTLS는 TLS를 기반으로 개발된 프로토콜이기 때문에 구조상의 큰 차이는 없다 [11].

이들은 동작하는 계층은 다르지만 네트워크 보안에 필요한 Confidentiality, Integrity, Client/Server Authentication 등의 기능을 제공한다. 그러나 금융관련 서비스에 필요한 Non-Repudiation은 제공하지 않는다. 또한 IP 계층을 근간으로 하고 있기 때문에, IP 주소변경에 매우 민감하게 동작할 수 밖에 없다. 예로서, IPSec의 SA(Security Association) 는 SPI(Security Parameter Index), Destination address, Security protocol에 의해 유일하게 식별되므로, 이동노드의 경우 주소가 변경된다면, 변경될 때마다 새로운 SA를 생성해야 한다. 이는 안전성과는 무관하게 노드의 이동에 의해 발생되는 것이므로, 네트워크는 SA 재생성에 따른 오버헤드만큼 성능저하를 초래하게 된다. 따라서 이동환경과 같이 IP 주소의 변경이 수시로 발생하는 상황에서는 적용하기 어렵다.

MOBIKE는 Fixed Line 영역에서 적용되었던 기존 IKEv2를 Mobile 영역으로 확장한 기술로서, IP주소가 변경되는 경우 기존 보안 세션을 업데이트 할 수 있는 메커니즘을 가지고 있다 [10]. 그러나 업데이트에 따른 지연으로 인해 실시간성을 보장하기 어렵고, NAT(Network Address Translation)에 대한 지원이 부족하기 때문에 실시간 이동환경이 보편화 되고 있는 근래의 통신환경에는 적합하지 않다.

최근의 통신환경은 다시 유선중심에서 무선중심으로 급격히 전환되고 있다. 현재 이런 환경을 효과적으로 지원하기 위해 WiFi, WiMAX, 2G, 3G 등의 다양한 접속 네트워크들이 공존하고 있으며, 모바일 디바이스들은 다양한 접속망에 접근할 수 있도록 다수의 네트워크 인터페이스를 기본적으로 탑재하여 출시되고 있다. 특히 스마트폰으로부터 촉발된 무선인터넷 서비스의 이용이 빠르게 확산되면서, 이러한 상황은 점차 가속화되고 있다.

그러나 현재의 서비스 이용 환경은 각 접속망들의 독립적인 특성으로 인해 (단말이 접속망간 이동시) 서비스가 지속적으로 연결되지 못하고 단절되어 있는 상황이다. 따라서 다양한 네트워크 인터페이스를 가진 단말이라 하더라도, 서비스의 연속성은 단일 액세스에서만 보장된다.

이는 IP 주소가 가지는 양면성 때문에 비롯된다. 현재의 인터넷은 IP 중심 계층구조 (Layered Architecture)로 이루어져 있고, IP주소는 네트워크 계층에서 호스트의 위치를 인식하는 Locator로, 전송 및 응용계층에서는 호스트 및 세션을 식별하는 ID로 사용된다. 이런 특성은 ID의 변경 없이 Locator를 변경할 수 있는 능력이 요구되는 이동성, 멀티 호밍, 번호 재사용, 보안 등 다양한 측면에서 서비스 장애 요인이 된다.

HIP (Host Identity Protocol)는 호스트의 identifier와 locator의 분리를 통해 이동성 및 멀티호밍 등을 지원한다 [14]. HIP는 identifier를 public key와 hash 함수를 사용함으로써 우수한 보안성까지 지원하지만 (public key인 Host Identity(HI)는 128 bits 값으로, 이를 hash함으로써 Host Identity Tag(HIT)가 생성), IP 아키텍처가 아닌 새로운 아키텍처의 도입을 요구하기 때문에 적용이 쉽지 않다.

LISP(Locator/ID Separation Protocol)는 네트워크 기반의 기술로서 HIP등의 기존 기술의 단점인 기존 단말과의 호환성을 해결하였다[15]. LISP는 네트워크 계층을 분리하여 상위 IP 계층의 IP주소는 ID로, 하위 계층의 IP주소는 로케이터로 사용하는 분리된 아키텍처를 도입함으로써 호환성, 확장성 등을 해결하였으나 이동성을 충족시키지 못하고 있다.

ILNP는 IP 주소가 Network Prefix와 Interface ID로 구성되어 있는 점에 기인하여, IP 주소를 토폴로지 측면에서 의미가 있는 Locator 영역과 호스트를 나타내는 ID 영역으로 분리하여 사용함으로써 이동성과

멀티 호밍을 해결하고자 하였다[16]. 그러나 DNS에 저장되는 Locator 값을 이용하기 때문에, 인터넷에서의 글로벌 계층구조에 따른 다중 캐쉬로 인한 업데이트 지연 및 실시간 검색의 한계 문제를 해결해야만 한다.

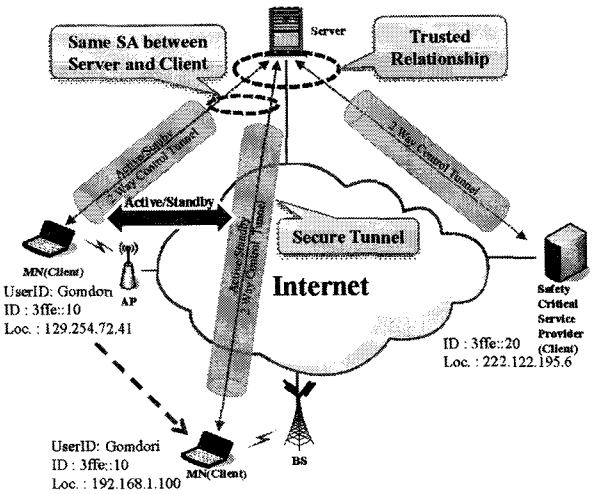
이렇듯 인터넷 세션 계층의 불완전성은 이제 보편적 서비스로 여겨지는 인터넷의 지속적 성장에 매우 커다란 걸림돌이 되고 있다. 더욱이 무선 인터넷 서비스의 사용이 확산되면서 일반화 되고 있는 이종망간 이동 환경에서는 안전하고 원활한 서비스 제공에 매우 큰 장애 요인이 되고 있다. 따라서 단말이 이종망간 이동할 경우에도 서비스의 연속성을 보장하고, 단말과 서비스 시스템이 서로를 신뢰할 수 있는 안전하고 안정적인 기술이 시급히 요구되고 있다.

3. 제안하는 서비스 프레임워크

이 논문은 이종망간 이동환경에서 끊김 없이 안전한 서비스 이용을 위한 기반구조로서 클라이언트/서버 기반의 이종망간 관리 구조를 제안한다. 그림 2는 제안하는 이종망간 관리구조이다.

이종망간 관리 구조는 복수의 네트워크 인터페이스를 가지는 이동 단말에 탑재되는 클라이언트 기능과, 이동 단말에 부여된 고유 식별자를 기반으로 단말을 실시간으로 관리하는 서버 기능으로 구성된다. 망은 IPv4, IPv6 모두 가능하다.

클라이언트는 단말이 가지고 있는 복수의 네트워크 인터페이스를 관리하고, 서버와 터널 기반의 안전한 관계를 형성하고 유지한다. 클라이언트는 현재의 링크 상태에 따라 Active 및 Standby 인터페이스를 설정하고, 이후 단말이 이동함에 따라 변경되는 상태를 지속적으로 반영한다. 각 인터페이스에 대해 클라이언트와 서버 사이에는 보안 터널이 설정되고, 이 터널을 통해 클라이언트와 서버는 보안 통신을 수행한다. 클라이언트는 이동중인 단말이 접속하는 액세스망이 변경됨에 따라 Active/Standby 터널에 대해 MBB(Make Before Break) 방식으로 터널 절체를 수행한다. 클라이언트와 서버 사이의 안전관계는 단말에 부여된 ID를 기반으로 설정되므로, 단말의 액세스 망이 변경되어도 클라이언트와 서버 사이의 안전관계는 일정하게 유지된다. 단말의 고유식별자는 IPv6 또는 IPv4 주소를 사용하여 기존 기술과의 호환성을 유지한다.



<그림 2> 이종망간 관리구조

서버는 무결성을 보장하는 신뢰할 수 있는 네트워크 정보관리 시스템으로 구성된다. 서버는 단말에 부여된 고유 식별자를 기반으로 단말의 현재 상태에 따라 변경되는 네트워크 정보를 관리한다. 서버는 항상 단말의 현재 상태를 인지하고 있으며, 이를 통해 단말들 간의 신뢰성을 제공하고, 안전한 데이터 교환을 중재한다. 아울러 필요시 거래 이력(Transaction history)을 저장하여, 추후 분쟁 해결에 사용할 수 있다

제안하는 서비스 프레임워크는 이종망간 관리구조를 기반으로 이동성 및 보안성을 제공하는 클라이언트 소프트웨어, 이동관리, 터널관리, 보안관리 기능을 제공하는 서버 소프트웨어, 클라이언트와 서버 소프트웨어간 동작절차를 정의하는 프로토콜 등으로 구성된다.

3.1 클라이언트 기능구조

클라이언트 소프트웨어는 단말에 탑재되는 소프트웨어 모듈로서, 데스크 탑, 랩탑, PDA, 스마트폰 등과 같이 네트워킹이 가능한 대부분의 사용자 단말에 실장 될 수 있다. 또한 웹 서버, 스토리지 서버, 인증 서버 등과 같은 서비스 시스템에 실장 할 수도 있다.

클라이언트 소프트웨어가 탑재되는 단말은 고정노드도 있지만, 복수의 네트워크 인터페이스를 가지는 이동 단말의 경우에는 각 네트워크 인터페이스가 지원하는 접속망의 중첩범위에 따라 터널 절체에 의한 이종망간 이동성이 지원된다.

클라이언트 소프트웨어는 단말을 식별하는 ID와 단말의 위치를 나타내는 Locator를 동시에 고려한다. Client ID는 IPv4 또는 IPv6 주소로서 private 또는 public address가 될 수 있으며, 각 Client와 Server가 터널 기반의 통신을 할 때 사용하는 논리적인 주소이다. 반면 Locator는 단말이 가진 복수의 네트워크 인터페이스마다 별도로 할당되는 주소로서, 각 접속망의 특성에 따라 주소의 특성이 결정된다.

클라이언트 기능구조는 단말에 장착된 다수의 인터페이스에 대해 각 인터페이스의 상태를 관리하는 기능, 서버와의 통신을 통해 단말의 각 네트워크 인터페이스에 대해 서버와의 터널을 생성, 삭제, 관리하는 기능, 서버와의 키 교환 및 안전관계를 수립하고 유지하기 위한 기능, 사용자 인터페이스를 위한 기능 등으로 이루어진다.

1) Heterogeneous Interface Handover Function (HIHF)

HIHF는 두 개 이상의 이종 네트워크 인터페이스를 가지는 단말에서 각 Network Interface의 상태(Up/Down/Add/Del)를 주기적으로 검색하여 최적의 네트워크를 결정하고, 각 인터페이스에 대해 상태에 따라 Active와 Standby모드를 결정한다. 현재 단말의 네트워크 인터페이스 중에서 네트워크 설정 조건에 가장 적합한 인터페이스를 Active Interface로 설정하고, 차선의 인터페이스를 Standby Interface로 설정한다. 네트워크 설정 조건은 사용자 선호도, 인터페이스의 대역폭, 네트워크 혼잡 상태, 접속요금부담, 평균 접속 시간 등을 고려하여 사전에 정의될 수 있다. 한번 설정된 Active, Standby 인터페이스는 단말의 이동에 따라 변화하는 네트워크 상태에 따라 지속적으로 변경된다.

2) Tunnel Management Function (TMF)

Active/Standby 인터페이스가 설정되면, 클라이언트는 서버와의 signaling을 통해 각 인터페이스 별로 Active/Standby 터널을 생성한다. 생성된 터널은 지속적으로 변경되는 인터페이스 설정 상태에 따라 TMF에 의해 갱신되거나 삭제된다. 터널의 생성/삭제/갱신은 TMF 내부에 관리되는 터널 테이블에 적용되고, 이 터널 테이블을 통해 현재의 터널 상태를 확인 할 수 있다.

3) Security Management Function (SMF)

클라이언트와 서버 사이에는 끊김 없이 안전한 통신 채널이 설정되어야 하며, 이를 통해 인증 및 보안 관련 메시지들이 전달되어야 한다. SMF는 클라이언트와 서버가 주고 받는 다양한 보안 관련 메시지를 생성하고 전달하는 기능을 제공하며, 안전한 통신 채널 설정을 위한 인증, 동적 키 교환 메커니즘, 메시지 암/복호화 등의 기능을 제공한다.

4) User Interface Function (UIF)

클라이언트 소프트웨어는 단말에 탑재되어 동작하므로, 사용자와의 상호작용은 필수적이다. UIF를 통해 사용자는 서버 등록, 정책 설정 등의 클라이언트 소프트웨어의 사용자 기능을 동작할 수 있고, 단말의 네트워크 정보를 포함하여 클라이언트의 상태를 모니터할 수 있다.

3.2 서버 기능구조

서버소프트웨어는 서버에 탑재되는 소프트웨어 모듈이다. 서버는 터널관리기능, 보안관리기능 등과 같이 프로토콜 수행과 관련하여 클라이언트의 각 기능에 대응하는 기능요소를 포함하면서, 클라이언트위치관리기능, 클라이언트인증기능, 성능관리, 로그관리기능 등과 같이 서버 소프트웨어 고유의 기능을 가진다.

1) Performance Management Function (PMF)

서버는 동시에 많은 수의 가입자를 수용해야 하므로 최대한 성능을 고려하여 설계되어야 한다. 이를 효과적으로 지원하기 위해 서버는 다중 Thread 방식으로 동작한다. 서버의 쓰레드로는 서비스 중인 터널의 생존시간을 점검하여 효율적인 자원관리를 위한 타이

머 쓰레드, 동시에 수신된 메시지의 누락방지를 위한 큐 쓰레드, 큐에 저장된 메시지의 효율적인 처리를 위한 프로세스 쓰레드 등으로 구성되며, 각 쓰레드 간에는 Semaphore를 적용하여 데이터를 보호한다.

2) Client Location Management Function (CLMF)

서버는 각 클라이언트 소프트웨어를 장착한 이동단말을 관리할 수 있는 데이터베이스를 유지한다. 이를 위해 각 이동단말의 클라이언트 ID와 Locator를 관리한다. 클라이언트 ID, Locator는 모두 IPv4 또는 IPv6 주소이다. 클라이언트가 연결되면, 서버는 클라이언트 ID와 Locator를 함께 저장하고 유지하며, 클라이언트의 이동에 따라 변경된 클라이언트의 상태를 반영한다.

3) Client Authentication Function (CAF)

서버는 클라이언트의 가입자 정보를 유지하고, 이를 통해 서버로 접근하고자 하는 클라이언트를 인증한다. 최초 클라이언트 인증이 성공적으로 완료되면, 클라이언트와 서버 사이에는 터널 기반의 안전관계가 형성되고, 이는 클라이언트와 서버와의 연결이 끊어질 때까지 지속된다.

4) Log Management Function (LMF)

서버는 추후에 발생할 수 있는 분쟁 해결 등을 위해 클라이언트와 주고받는 모든 거래 이력을 기록한다. 서버는 클라이언트와의 통신에서 발생하는 절차에 대해 언제(타임스탬프), 누가(ID), 어디서(Locator), 무엇을(Message) 하였는지에 대한 이력을 보관함으로써, 금융관련 서비스와 같은 민감 서비스에 요구될 수 있는 Non-Repudiation기능을 제공할 수 있다.

3.3 프로토콜

제안하는 서비스 프레임워크는 클라이언트/서버 기반의 프로토콜로 구성되며, 클라이언트와 서버는 터널 기반의 안전관계를 형성한다. 또한 클라이언트의 접속망이 변경되면 통신중인 접속점을 끊고 재접속해야 하는 기존 방식에서 탈피하여, 복수의 네트워크 인터페이스를 Active/ Standby로 운용하여 끊김 없는 서비스를 제공할 수 있다.

먼저, 클라이언트는 가장 좋은 연결성을 가진 인터페이스를 Active interface로 설정하고, 이후 Active interface가 reachability를 잃을 경우, standby interface를 다시 active interface로 설정한다. 즉, 클라이언트는 연결성이 확보된 Active 인터페이스와 Standby 인터페이스간 전환으로 끊김 없는 연결성을 확보한다.

1) Make Before Break (MBB) Handover

지금까지 IP네트워크에서 서비스 연속성을 제공하기 위한 많은 연구가 진행되어 왔으며, 대부분의 연구는 이동단말의 접속구간이 변경되는 곳에서 핸드오버 지연을 줄임으로써 끊김 없는 서비스를 제공하기 위해 노력하였다. 그러나 이들은 이동단말이 한 번에 단지 하나의 접속망에 연결된다는 가정에 기반을 두고 있다. 이러한 조건 때문에 새로운 네트워크 노드에 접속하기 위해서는 현재 네트워크에 연결된 접속을 끊어야 한다.

이러한 BBM (Break Before Make) 형태의 핸드오버는 Cellular, GSM, WCDMA 등 상대적으로 넓은 커버리지를 가지는 이동통신망에서는 유효하지만, Wireless LAN과 같이 단말의 이동속도에 비해 커버리지가 협소한 네트워크에서는 적용이 쉽지 않다. 그러나 여러 개의 네트워크 노드에 동시에 접속할 수 있다면 이동 단말은 현재의 접속을 끊기 전에 새로운 망으로 접속을 설정할 수 있고, 이에 따라 핸드오버 latency의 영향을 줄이거나 최소화 할 수 있다. 이것은 이동단말에 여러 개의 네트워크 인터페이스를 장착함으로써 가능하다.

이 논문에서는 패킷 손실이 없이 끊김 없는 서비스 연속성을 제공하기 위해 복수의 인터페이스를 사용하는 MBB (Make Before Break) 핸드오버 방식을 제안한다. 제안하는 방안은 이동단말에 두 개 이상의 네트워크 인터페이스를 장착하여 하나의 인터페이스가 데이터 통신을 위하여 사용(Active)될 때 다른 인터페이스는 (Standby) 더 좋은 연결을 제공할 수 있는 네트워크를 탐색 (scanning) 하기 위하여 사용된다. 새로운 연결을 위한 네트워크가 발견되고 현재의 인터페

이스보다 더 좋은 값을 갖게 되면 새로운 인터페이스가 데이터 전송을 떠맡게 되고 Active였던 원래의 인터페이스는 Standby 인터페이스로 전환되어 네트워크 탐색 역할을 맡게 된다. 이렇게 함으로써 이동단말은 접속망의 종류에 상관없이 이전 네트워크와의 연결을 유지하면서 패킷 손실이 없는 핸드오버를 제공할 수 있다. 이동단말에 탑재되는 복수의 인터페이스는 동종망과 이종망을 모두 수용할 수 있다.

2) Tunneling

클라이언트와 서버가 연결되면, 우선 둘 사이에는 상호 통신을 위한 터널이 형성된다. 일단 클라이언트와 서버간 터널이 설정되면, 보안 및 이동성을 고려하여 클라이언트와 서버의 통신은 반드시 터널을 통해서 이루어진다.

클라이언트와 서버 간에 설정하는 터널은 Active 터널과 Standby 터널로 구분한다. Active 터널은 단말이 데이터 송·수신에 사용하는 활성화된 터널이고, Standby 터널은 단말이 이동을 위하여 사전에 DHCP, 접속인증 등의 절차를 통해 통신이 가능하도록 Locator 할당을 완료해 놓은 보조터널이다.

터널은 클라이언트의 ID와 Locator의 유형에 따라 IPv4-IPv4 또는 IPv6-IPv4의 형태로 구성될 수 있다. 그러나 보편적으로 IPv4 네트워크를 사용하는 현재의 네트워크에서는 NAT를 고려해야만 한다. 클라이언트가 NAT 내부에서 서버에 연결되는 경우, 이동단말의 Locator는 서버에 보이지 않게 되므로 NAT Traversal을 통해 이를 회피하여야 한다. 따라서 NAT 내부의 클라이언트와 서버 간에는 NAT Mapping Table을 유지하기 위한 UDP Port 정보의 활용을 위해 IPv4-UDP-IPv4 또는 IPv6-UDP-IPv4 터널이 형성된다. 클라이언트와 서버간 터널은 다중 Locator 기반으로 설정된다. 클라이언트의 이동성 지원은 Active 터널과 Standby 터널을 Switch-over하는 것으로 정의되며, Switch-over 시점의 판단은 클라이언트에 의해 이루어진다.

3) Security

보안은 유선 환경뿐 아니라 무선 환경에서도 큰 이슈가 되고 있다. 보안 특성을 제공하기 위해서는 전원을 포함한 자원 사용에 있어서 큰 부담을 가져야 하기 때문에 이동 단말에 대한 보안 제공은 많은 어려움이 따른다. 특히, 제안하는 이종망간 관리 구조는 서버에 많은 부하가 집중되기 때문에 기존 방식들에 비해서 간단하면서도 안전한 특성을 갖는 보안 방식이 필요하다.

유선환경을 중심으로 IP계층에서 사용되고 있는 대표적인 보안기술인 IPsec [23]은 동적으로 키를 교환하기 위한 IKE(Internet Key Exchange) [22], Authentication 및 Integrity를 위한 AH(Authentication Header) [24], 암/복호화를 위한 ESP(Encapsulating Security Payload) [25] 등의 보안기능을 제공하고 있다. 그러나 키 교환을 위한 IKE는 많은 연산량과 메시지 교환이 필요하며, PKI(Public Key Infrastructure)와 같은 보안 인프라를 필요로 하기 때문에 이동환경에 적용하기에는 많은 부담이 따른다.

클라이언트	서버
$P = lID \parallel rID \parallel sID \parallel sPW$ $x \in_R Z_p$ $X = H_1[P] \bullet (g^x \bmod p)$	$\xrightarrow{X}$
$\xleftarrow{Y, MSG_S, AUTH_S}$	*Verify that X is not 0* $P = lID \parallel rID \parallel sID \parallel sPW$ $y \in_R Z_p$ $\sigma = (\frac{X}{H_1[P]})^y = g^{xy} \bmod p$ $K_{mod} = H_2[P \parallel g^x \bmod p \parallel g^y \bmod p \parallel g^{xy} \bmod p]$ $K_A = PRF[K_{mod} \parallel \sigma \parallel sID \parallel sPW \parallel 0]$ $Y = H_1[P] \bullet (g^y \bmod p)$ $MSG_S = [SA\ parameters]$ $AUTH_S = KH[Y \parallel MSG_S]_{K_A}$
$\sigma = (\frac{Y}{H_1[P]})^x = g^{xy} \bmod p$ $K_{mod} = H_2[P \parallel g^x \bmod p \parallel g^y \bmod p \parallel g^{xy} \bmod p]$ $K_A = PRF[K_{mod} \parallel \sigma \parallel sID \parallel sPW \parallel 0]$ *Verify* $AUTH_S$ $MSG_L = [SA\ parameters]$ $AUTH_L = KH[MSG_L]_{K_A}$	$\xrightarrow{MSG_L, AUTH_L}$
	Verify $AUTH_L$

p = prime, g = generator, symbol '||' = concatenation, H[ ] = hash function [26], PRF[ ] = pseudo random function[27], lID = Local ID, rID = Remote ID, sID = Subscriber's ID, sPW = Subscriber's password, SA parameters = necessary information in order to create the SA (e.g. AH/ESP header type, a list of supported algorithms, security parameter index, Diffie-Hellman Group and etc.)

<그림 3> mPAK 절차

PAK(Password-based Authenticated Key exchange) [21] 는 상대적으로 가벼우면서도, 가입자 정보를 이용한 상호 인증 절차를 수행하여 키를 안전하게 교환하는 방법을 제공한다. 제안하는 서비스 프레임워크는 PAK에 보안 정책 협상을 위한 파라미터들을 추가함으로써 클라이언트와 서버간에 보안 정책을 협상할 수 있도록 개선한 mobile PAK (mPAK)를 사용한다.

클라이언트가 부트후 처음으로 서버와 통신을 개시할 시점에는 클라이언트와 서버간 아무런 보안 채널이 설정되지 않은 상태이다. 따라서 클라이언트와 서버간 최초 인증의 과정은 가입자 정보에 의존하게 된다. 서버는 가입자 정보를 통해 클라이언트의 접근을 승인하고, 이 과정에서 터널생성에 필요한 키를 분배하기 위해 mPAK를 수행한다. 그림 3은 mPAK의 절차를 나타낸다.

mPAK는 키생성을 위한 seed로서 클라이언트의 가입자 정보뿐만 아니라, 클라이언트와 서버의 ID까지 포함한다. ID는 클라이언트/서버의 이동 및 변경 상태와 무관하게 클라이언트/서버를 식별할 수 있기 때문에 ID를 기반으로 설정된 클라이언트와 서버의 안전관계는 일정하게 유지될 수 있다.

mPAK 절차를 통해 클라이언트와 서버간 가입자 인증과 키분배가 완료되면, 터널 생성을 위한 제어 메시지(Tunnel Request, Tunnel Ack)는 mPAK의 결과로 생성된 키를 이용한 Keyed Hash를 통해 보호될 수 있다.

최초 터널이 생성되면, 터널의 변경 및 유지를 위한 메시지를 포함하여 클라이언트와 서버간 모든 통신은 터널을 통해 이루어진다. 터널을 통해 주고 메시지의 보안은 클라이언트와 서버와의 안전관계가 변경되지 않으므로 IPSec AH, ESP 등을 통해 보호할 수 있다.

4. 서비스 시나리오

인터넷 서비스를 이용하는 형태는 서비스 이용자와 서비스 제공자의 상호작용으로 구성된다. 따라서 인터넷 서비스를 이용함에 있어, 안전한 서비스의 보장은 사용자와 서비스 제공자간의 상호 신뢰에 기반한다.

제안하는 서비스 프레임워크는 클라이언트/서버 기반으로 동작하며, 클라이언트와 서버간에 설정되는 끊김 없이 지속적인 안전관계에 기반하여 서버는 클라이언트의 신원을 언제나 보장할 수 있다. 따라서 클라이언트들간의 신뢰성은 서버를 통해 확보될 수 있다.

인터넷 서비스의 안전한 이용을 위한 행위의 주체는 서비스를 이용하는 단말(Mobile Node; MN), 민감 서비스를 제공하는 서비스제공자(Safety Critical Service Provider; SCS), 그리고 사용자 단말과 서비스 제공자간 상호 신뢰성을 제공하기 위한 중재자의 역할을 담당하는 중재노드 (Seamless and Secure Service support Node; SSSN) 로 구성될 수 있다.

단말과 서비스제공자에는 클라이언트 기능이 탑재되고, SSSN에는 서버 기능이 탑재된다. MN은 모바일 인터넷 디바이스로서, 복수의 네트워크 인터페이스를 가진다. 클라이언트와 서버는 별도의 서비스 가입절차를 통해 이미 등록과정에 필요한 서로의 정보를 저장하고 있다. 클라이언트는 서버로의 접속 경로가 되는 서버 ID를 가지고 있으며, 서버는 클라이언트 ID, 클라이언트 네트워크 인터페이스 종류, 사용자ID, 사용자 Password 등의 가입자 정보를 가지고 있다.

MN 과 SCS에 탑재된 클라이언트는 최초 전원이 켜지면 SSSN으로 등록을 수행한다. 등록 과정에서 서버는 이미 가지고 있는 클라이언트의 가입자 정보를 통해 클라이언트를 인증하고, 각 클라이언트와의 보안 통신에 필요한 키를 생성하고 분배한다.

서버로의 등록이 성공적으로 완료되면, 생성된 키를 기반으로 클라이언트와 서버간에는 터널 기반의 양방향 안전관계가 설정되고, 클라이언트와 서버간 전달되는 모든 메시지는 안전관계가 설정된 터널을 통해 이루어지게 된다. 안전관계는 클라이언트와 서버의 ID를 기반으로 설정되므로, 한번 체결된 안전관계는 클라이언트 및 서버가 다운되거나, 별도의 이유에 의해 고의로 해제하지 않는 이상 지속적으로 유지된다.

클라이언트와 서버가 아닌 다른 네트워크 시스템과의 통신은 터널을 통해 전송되지 않는다. 단순한 웹서핑처럼 안전성 보장이 요구될 필요가 없는 일반적인 서비스를 위해 서버의 부담을 가중시킬 이유는 없다.

클라이언트와 서버간 터널 기반의 안전관계가 설정되면, 서버는 클라이언트 ID를 기준으로 접속망 종류, 접속 위치, 접속 시간 등과 같은 클라이언트의 네트워크 접속정보를 지속적으로 관리하며, 필요한 경우 클라이언트의 접속 이력을 저장할 수도 있다. 이는 클라이언트와 서버와의 주기적 메시지 교환과, 클라이언트의 네트워크 연결상태 변경에 따라 클라이언트가 서버로 전달하는 상태변경요청에 의해 이루어진다.

MN은 이동성을 제공하기 위한 복수의 네트워크 인터페이스를 가지고 있기 때문에, 접속 위치에 따라 다양한 접속망에 연결될 수 있다. 따라서 MN의 네트워크 연결 상태는 수시로 변경되기 때문에,

MN에 탑재된 클라이언트는 각 네트워크 인터페이스의 연결상태를 지속적으로 모니터하여 주 접속망과 보조 접속망을 효율적으로 전환한다. 전환 과정에서도 네트워크 연결성은 계속 유지하고 있기 때문에 MN은 끊김 없는 서비스 이용이 가능하다.

SCS는 서비스 제공자로서, 서비스 가입자의 요청에 의해 다양한 서비스를 제공한다. 서비스는 안전성이 요구되지 않는 일반 서비스와 안전성이 요구되는 민감 서비스로 구분할 수 있다. 일반 서비스와 달리 민감 서비스를 제공하기 위해서는 사용자의 확인이 필수적이므로, 일반적으로 민감 서비스를 제공하는 서비스 제공자는 이미 해당 서비스에 대한 가입자 확인 절차를 기본적으로 가지고 있다.

MN으로부터 민감 서비스 제공을 요청받게 되면, SCS는 기존 가입자 확인 절차를 통해 정상적인 가입자인지를 확인하고자 한다. 따라서 MN은 SCS에 가입자 정보를 제시하게 되고, SCS는 제시된 가입자 정보의 확인을 통해 서비스 제공 여부를 결정한다. 가입자 정보의 확인에는 서비스 이용자를 확인할 수 있는 사용자 식별자가 반드시 요구된다. 사용자 식별자는 통상 개인정보로 이루어지며, 민감 서비스에 이용되는 사용자 식별자는 기본적으로 (주민번호, 사회보장번호, 여권번호 등) 여러 도메인에서 공통적으로 사용할 수 있는 공통식별자를 포함한다.

SCS는 기존 가입자 확인 절차 외에 별도로, 서버에게 서비스 제공을 요청하는 MN이 유효한지 질의한다. 이 때, SCS는 가입자 확인 절차를 통해 확보한 서비스 요청자의 공통식별자와 서비스요청 단말의 접속위치를 서버에게 전달한다.

SCS로부터 단말의 유효성 확인을 요청 받은 서버는 주어진 정보를 통해 서비스를 요청하는 단말이 MN인지를 판단한다. 서버는 서비스 요청자의 공통식별자를 통해 가입자 정보를 찾고, 서비스 요청 단말의 접속 위치가 가입자 정보에 매핑하는 단말의 현재 접속위치와 일치하는지를 검사한다. 두 접속 위치의 일치 여부에 따라, 서버는 가입자 정보의 단말이 유효한지, 아닌지를 SCS에게 전달한다.

서버로부터 서비스요청 단말의 유효성을 전달받은 SCS는 이를 근거로 서비스 요청 단말이 정상 단말인지를 판단하고, 추후의 활용을 위해 거래 이력을 서버에 (또는 별도의 이력관리시스템으로) 전달하고, 서비스요청을 승인한다.

이러한 네트워크 기반의 확인 절차를 통해 가입자 정보가 유출된 경우를 대비할 수 있다. 가입자 정보가 유출되어 악의적 사용자에 의해 도용되는 경우, 기존 가입자 확인 절차를 통과 하여도 서버의 확인절차를 통과하지 못하기 때문에 악의적 사용자의 단말을 통해서는 서비스를 제공받을 수 없다. 또한 접속망에 무관하게 일관된 안전관계를 보장하기 때문에 이종망간 이동환경에서 끊김 없는 안전성을 제공한다.

5. 구현 및 성능 측정

이 논문에서 제안하는 서비스 프레임워크의 안전성을 시험하기 위해 클라이언트 소프트웨어, 서버 소프트웨어, 그리고 클라이언트와 서버간 프로토콜 등을 구현하고, 이들의 성능을 시험하기 위한 시험환경(test bed)을 구성하였다. 시험환경은 SSSN, MN, SCS 세 개의 기능요소로 구성된다. SSSN 에는 제안구조의 서버 소프트웨어가 탑재되고, 사용자 단말(Mobile Node; MN) 및 안전 서비스 시스템(Safety Critical System; SCS)에는 클라이언트 소프트웨어가 탑재된다. 각 기능요소의 세부 사양은 표 1과 같다.

클라이언트와 서버의 ID는 IPv6주소를, 로케이터는 IPv4주소를 사용하였다. 클라이언트와 서버간 터널은 IPv6-IPv4 터널을 적용하였으며, 서버와의 각 터널을 통해 통신하는 메시지의 보호는 IPSec ESP를 적용하였다. 클라이언트가 동작하는 중에는 다중 인터페이스를

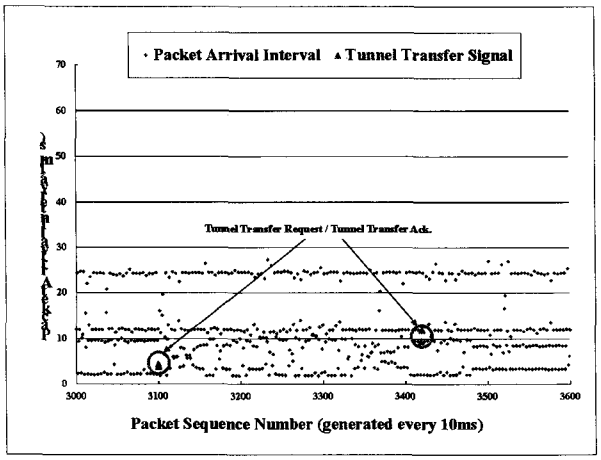
<표 1> 실험환경

구분	SSSN	MN	SCS
OS	Linux 2.6	Windows XP Tablet	Windows XP SP2
CPU	Intel Xeon 3GHz 8Core	Genuine Intel 800MHz	Intel T2400 1.83GHz
Memory	4GB	1GB	1GB
ID	IPv6 Address	IPv6 Address	IPv6 Address
Tunnel EP	IPv4 Address	IPv4 Address	IPv4 Address
Security	IPSec ESP	IPSec ESP	IPSec ESP
NIC	Gigabit Ethernet	802.11 a/b/g (dual)	Gigabit Ethernet

통해 항상 서버와의 끊김 없는 보안 터널이 설정된다.

그림 4는 클라이언트/서버간 보안터널이 형성된 후, 서버와의 보안 터널을 통해 MN과 SCS간 메시지 전송 실험에 대한 결과를 나타낸다. MN은 SCS로 터널의 성능에 영향을 미치지 않을 고정 크기의 패킷을 지속적으로 전송하고 (10ms마다 64byte ICMP 패킷), SCS는 수신된 패킷을 wireshark [29]를 사용하여 측정하였다.

x축은 패킷 시퀀스 번호이고, y축은 패킷 도착 간격을 나타낸다. 패킷 도착 간격은 실험환경에 의존적이므로, 일반적인 환경에서는 무시할 만한 수준이다. MN이 이동하면서 MN에서는 인터페이스 터널간 핸드오버가 발생하지만, 패킷 전송 성능에 아무런 영향이 없이, 끊김 없이 절체 되었고, MBB 방식에 따라 터널 절체에 따른 전송 지연 및 패킷 유실이 없음을 알 수 있다. 이는 MN의 접속망 변경에도 보안 공백(Security Hole)이 생기지 않음을 나타낸다.



<그림 4> 패킷전송실험결과

실험 결과, 이종망간 실시간 이동에도 클라이언트와 서버간에는 성능저하 없이 보안세션이 유지됨을 알 수 있었다. 이 실험을 통해 제안한 이종망간 관리구조가 끊김 없는 안전한 서비스 제공에 매우 적합함을 알 수 있었다.

6. 결 론

현재 스마트폰을 포함한 모바일 디바이스는 다중인터페이스를 가진 복합 단말로 진화하고 있다. 대부분의 모바일 디바이스는 항상 켜져 있고, 다중 인터페이스를 통해 항상 데이터를 수신할 수 있는 상태로 동작한다. 이에 따라 가까운 미래에 하나의 이동 단말로 다양한 액세스망을 통해 서비스를 제공받는 이종망간 이동환경이 도래하고 있다.

모바일 디바이스는 휴대성 및 이동성을 추구함으로써, 가급적 소형크기의 단말로 구현될 수 밖에 없으며, 이로 인해 고성능의 프로세서를 탑재하는데 한계가 있다. 백신 소프트웨어와 같은 전통적인 호스트 보안 기술이나 키 관리와 같은 계산량이 많은 기능은 모바일 디바이스의 성능을 큰 폭으로 저하시키는 요인이 된다.

이 논문은 네트워크 수준에서 이종망간 이동환경에서 끊기지 않는 보안 세션을 유지함으로써, 인터넷 기반 통신 환경에서 민감 서비스를 제공하는 서비스 제공자와 서비스를 이용하는 이동단말 사용자에게 서로 믿을 수 있는 상대임을 확인 해주고, 사용자의 이동에 따라 접속망이 변경되더라도 안전한 데이터 채널의 연속성을 보장해주는 서비스 프레임워크를 제안하였다. 또한 그 시험환경을 구성하고 실험을 통해 성능을 입증하였다.

제안한 서비스 프레임워크는 가까운 미래에 도래가 예상되는 무선 기반의 이종망간 이동이 빈번해지는 환경에서도 보안채널의 연속성을 보장함으로써 결제, 인증 등과 같이 안전성 보장이 필수적인 민감 서비스를 제공하기 위해 매우 적합하리라 기대한다.

향후 상용 시스템 수준의 기술적 안정성을 추구하기 위해, 대용량 가입자 처리 기술, 클라이언트 모듈 변조 방지 기술, 거래이력 관리 및 부인 방지 기술, 서버 이중화, 단말 자원관리 등의 보완이 필요하다.

참 고 문 헌

[1] Pay-Buy-Mobile Business Opportunity Analysis - Public White Paper, GSMA, Nov. 2007.

[2] Global M-Payment Update 2005, Arthur D. Little, 2006

[3] The Mobile Internet Report, Morgan Stanley, Dec. 2009.

[4] Measuring the Information Society - The ICT Development Index, International Telecommunication Union(ITU), 2009
[5] Best Practice for Mobile Financial Services, Mobey Forum, 2008
[6] R. Sundarraj and J. Wu, "Using Information-Systems Constructs to Study Online- and Telephone-banking Technologies," Electronic Commerce Research and Applications, vol. 4, Jul. 2005.
[7] S. Barnes and B Corbitt, "Mobile Banking: Concept and Potential," International Journal of Mobile Communications, vol. 1, Sep. 2003.
[8] T. Dierks, The Transport Layer Security (TLS) Protocol Version 1.2, IETF RFC 5246, August 2008.
[9] SSL, http://en.wikipedia.org/wiki/Secure_Sockets_Layer
[10] P. Eronen, "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", IETF RFC4555, June. 2006.
[11] WTLS, "Wireless Transport Layer Security Protocol Specification," WAP Forum, http://www.wapforum.org/, Nov. 1999.
[12] E. Rescorla, A.Schiffman, "The Secure HyperTextTransfer Protocol," August 1999, IETF RFC 2660.
[13] B. Ramsdell, S/MIME Version 3 Message Specification, Jun. 1999, IETF RFC 2633.
[14] R. Moskowitz and P. Nikander, Host Identity Protocol (HIP) Architecture, RFC 4423, May 2006.
[15] D. Farinacci, et al., Locator/ID Separation Protocol(LISP), draft-farinacci-lisp-07.txt, April 2008
[16] R. Atkinson, INLP Concept of Operations, Internet-draft, August 2009
[17] Erik P. Harris et al., "Technology Directions for Portable Computers," Proceedings of the IEEE, 636-658, April 1995.
[18] J. Arkko, V. Devarapalli, and F. Dupont, Using IPsec to protect mobile IPv6 signaling between mobile nodes and home agents, IETF RFC 3776, Jun. 2004.
[19] G. O'shea and M. Roe, "Child-proof authentication for MIPv6(CAM)," ACM Computer Communication Review, vol. 31, no. 2, 2001
[20] Y. Qiu, J. Zhou, and F. Bao, "Protecting all traffic channels in mobile IPv6 network," IEEE Wireless Communications and Networking Conf., pp. 160-165, Mar. 2004.
[21] Password-authenticated key exchange(PAK) protocol, ITU-T Rec. X.1035, 2007.
[22] C. Kaufman, Internet key exchange(IKEv2) protocol, IETF RFC 4306, Dec. 2005.
[23] S. Kent, Security Architecture for the Internet Protocol, IETF RFC 4301, Dec. 2005.
[24] S. Kent, IP authentication header, IETF RFC 4302, Dec. 2005.
[25] S. Kent, "IP encapsulating security payload(ESP)", IETF RFC 4303, Dec. 2005.
[26] D. Eastlake and P. Jones, US secure hash algorithm 1(SHA1), IETF RFC 3174, Sep. 2001.
[27] D. Eastlake, J. Schiller, and S. Crocker, Randomness requirements for security, IETF RFC 4086, Jun. 2005.
[28] E. -J. Yoon, E. -K. Ryu, and K. -Y. Yoo, "An improvement of Hwang-Lee-Tang's simple remote user authentication scheme," Computer & Security, vol.24, pp.50-56, 2005.
[29] Wireshark, http://www.wireshark.org
[30] 김소이, "전자금융사고 발생유형 및 대응현황", 금융결제원, 지급결제와 정보기술 제38호, pp.34-62, 2009년 10월.
[31] 김영진 외, "U-정보사회에서의 포괄적 네트워크 보안관리 방안," 정보보호학회지, v.18, no.3, pp.74-80, 2008년 6월.
[32] 이원철 외, "전자금융거래시스템 취약점 분석 및 안전성 강화방안 연구," 정보보호학회지, v.15, no.4, pp.44-49, 2005년 8월.
[33] 주영도 외, "랜덤 Nonce 기반 사용자 인증 스킴의 안전성 개선에 관한 연구," 한국산업정보학회

논문지, v.15, no.3, pp.33-40, 2010년 9월.
[34] 이승익, "SBC 기반 차세대 이동형 단말기 개발," 한국산업정보학회논문지, v.14, no.4, pp.30-36, 2009년 12월.

논 문 접 수 일 : 2011년 09월 22일
1차수정완료일 : 2011년 10월 10일
게 재 확 정 일 : 2011년 12월 04일

윤 성 현 (Sunghyun Yoon)

- 충북대학교 전자계산학과 학사
- 충북대학교 컴퓨터과학과 석사
- 한국전자통신연구원 유무선융합네트워크연구팀 선임연구원

- 관심분야 : Network Architecture, Network Evolution Strategy, B4G systems 등

이 순 석 (Soon Seok Lee)

- 성균관대학교 산업공학과 학사
- 성균관대학교 산업공학과 석사
- 성균관대학교 산업공학과 박사
- 한국전자통신연구원 융합네트워크연구부 부장

- 관심분야 : Converged Network Architecture, Network Design, Network Engineering 등

김 상 하 (Sang-Ha Kim)

- 서울대학교 학사
- University of Huston 석사
- University of Huston 박사
- 충남대학교 정보통신공학부 교수

- 관심분야 : Internet Routing, Wireless Sensor Networks, 4G, Mobility, Multicast 등