모바일 IP 스푸핑 방지를 위한 포렌식 설계

A Modeling of Forensics for Mobile IP Spoofing Prevention

박순희*, 양동일**, 진광윤*, 최형진*

Sun-Hee Park*, Dong-Il Yang**, Kwang-Youn Jin*, and Hyung-Jin Choi*

요 약

정보기술 및 이동통신의 발전과 디지털 기기의 기능의 발달로 인해 디지털 기기의 보급이 활발해지면서 모바일 정보 기기의 보급이 늘고 있다. 대표적인 모바일 정보 기기로는 모바일폰이 있다. 모바일폰은 다양하고 편리한 기능을 가지고 있지만, 단말기용 바이러스 확산, 통신서버의 해킹, IP Spoofing 공격 등과 같은 보안 사고가 발생하는 문제점도 있다. 이러한 문제는 사회 질서를 파괴하고 혼란을 초래하는 범죄로서 인식되고 있다 모바일폰 관련 범죄에 대해서는 법적인 연구가 부족하고, 수사 관점에서도 복사나 이동, 삭제가 쉬운 디지털 자료의 특성 때문에 객관적인 증거임을 보장하기 위한 포렌식 증거의 무결성 입증이 필수적이다. 뿐만 아니라, Mobile IP는 이동에 대한 비밀성과 데이터에 대한 무결성을 보장할 수 있어야 한다. 본 논문에서는 디지털 포렌식 기법에 대해 소개하고, 모바일 포렌식 구조를 설계하여 실험에 적용함으로써 데이터 분석을 통해 얻은 해쉬값을 Mobile IP의 헤더 부분에 사용자 인증 옵션으로 사용하여 이동통신에서 발생할 수 있는 여러 가지 보안 문제들 가운데 Mobile IP Spoofing을 방지하기 위한 방법을 제안한다.

Abstract

Rapid development of the IT technology and mobile communications has increasingly improved many kinds of digital devices arise, as well as the mobile technology. However, the attacks (virus, hacking and Ip spoofing etc) have also increasingly grown dogged on any region including the society security. As the visual data is prone to copy, delete and move etc, it is necessary that attesting to the integrity of forensics evidence is crucial, as well as data transmission security.

This paper presents a framework model using digital forensics method and the results of its performance evaluation for mobile security. The results show that the integrity of the visual data can be obtain with high security and make a proposal refer to prevention of Mobile IP Spoofing attack using our hashing data.

Key words : IT, Spoofing, Mobile, Forensics, Security

I. 서 론

정보기술은 인류의 정보와 통신 기술을 의미하는데, 이는 과학기술의 발전에 의한 아날로그에서 디지털이동통신에 이르렀으며, 기기와 기능은 정보와 데이터 통신이 미디어혼합에서 멀티미디어통신으로 발달되었다.

그러나, 디지털이동통신과정에서 IP에 따른 단말정보를 가로채기나 시스템 공격으로 탈취한 거짓 IP(IP Spoofing)로부터 악의적으로 정보와 데이터의

* 강원대학교 컴퓨터과학과
** 한림성심대학교 인터넷비즈니스과
· 제1저자 (First Author) : 박순희 교신저자 : 최형진
· 투고일자 : 년 월 일
· 심사(수정)일자 : 년 월 일
· 게재일자 : 2012년 4월 30일

손실을 발생시킬 뿐만 아니라, 네트워크에서의 비논리적 사회공학적 활동이 발생할 수도 있다[13, 14].

본 논문에서는 정보통신 네트워크에서 발생되는 IP Spoofing 문제에 대한 방지 대책을 지능형 범죄수사에서 활용하는 디지털 포렌식 기법을 이용한다. 전통적으로 포렌식은 법의학 분야에서 지문, 모발, DNA 감식 등이 주류를 이루었다. 그러나 최근 다양한 정보기기들의 활용과 정보생산 및 유통에 있어서 95% 이상이 디지털 형태로 이용되고 있기 때문에 물리적 형태의 증거뿐만 아니라 전자적 증거를 다루는 디지털 포렌식 분야가 점차 확대되고 있다.

Ⅱ. 디지털 이동통신의 발전과 환경

2-1 정보통신의 의미

정보화 사회에서 우리는 인터넷의 발달로 매일 새로운 정보를 접하게 된다.

정보란 어떠한 자료나 지식을 표현하는 데이터를 의미한다. 정보로 표현할 수 있는 데이터의 종류에는 문자, 그림, 음성, 영상, 의사, 명령 등이 있으며 이러한 데이터를 일정한 약속에 의해 의미를 부여해 인간생활에 직접 또는 간접적으로 도움을 주는 모든 지식을 정보라 하며, 이러한 정보는 자료의 수집과 처리과정을 통해 우리에게 전달된다.

정보와 통신 두 분야는 서로 밀접하게 연관되어 상호보완적인 작용을 서로에게 주는 컴퓨터와 전기통신의 결합체로서 정보화 사회를 실현하는 수단으로 인식되고 있다. 즉, 정보통신이란 통신기술을 활용하여 정보를 전송하거나, 정보를 검색하고 자료를 공유하며 이를 토대로 새로운 정보를 생성하는 일련의 과정이라 정의할 수 있다. 이러한 정보통신기술은 정보화 사회를 만드는데 중요한 역할을 담당하고 있다[1].

2-2 이동통신의 의미

이동통신은 고정된 위치가 아닌 장소에서 이동 중에 무선으로 통신하는 방법으로, 가입자의 이동성(mobility)을 전제로 하여 무선전송매체인 자유공간을 이용하여 언제, 어디서나, 누구에게나 시간과 공간을 조절하여 정보를 송수신할 수 있는 것을 말한다.

2-3 이동통신의 역사

이동 통신의 역사는 1978년 미국의 AT&T사가 800MHz 대역의 AMPS(Advanced Mobile Phone Service system) 방식을 최초로 사용 하였다. 그 후 1979년 일본에서 세계 최초로 상용화하였고, 우리나라는 북미식의 AMPS 셀룰라 시스템을 도입하여 셀룰라 이동통신 서비스가 본격 개시됨으로써 이동전화 서비스의 대중화를 위한 기반이 구축되었다.

그림 1과 같이 이동통신의 발전 역사는 1세대 아날로그 이동통신, 2세대 디지털 이동통신, 그리고 3세대 IMT-2000, 4세대 방식으로 구분된다.

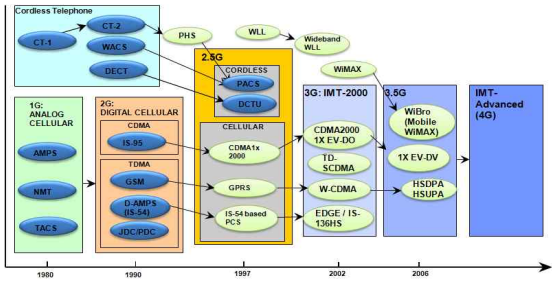

그림 1. 이동통신 방식의 발전사
Fig 1. History of Mobile Communication

2-3-1 1세대 아날로그 이동통신

1세대 아날로그 이동통신은 미국의 AMPS, 일본과 영국의 TACS(Total Access Communications System), 북유럽의 NMT(Nordic Mobile Telecommunications)로 분류된다. 표 1은 1세대 아날로그 이동통신의 특성을 비교한 것이다.

표 1. 1세대 아날로그 이동통신의 특성 비교
Table 1. Comparison of First-Generation Analog Mobile-Communication

구 분	AMPS	TACS	NMT-900	NMT-450	NTT
서비스제공 국가	미국	영국	북유럽	북유럽	일본
서비스 시기	1983년	1985년	1986년	1981년	1979년
대역폭	30KHz	25KHz	25/12.5KHz	25/20KHz	25KHz
전송속도	10Kbps	8Kbps	1.2Kbps	1.2Kbps	0.3Kbps
제공 서비스	음성통화				

2-3-2 2세대 디지털 이동통신

2세대 디지털 이동통신은 디지털의 도입으로 1세대 아날로그 무선접속 방식이 디지털 방식으로 전환되었다. 2세대 디지털 방식에는 시분할다중접속(TDMA : Time Division Multiple Access)와 코드분할다중접속방식(CDMA : Code Division Multiple Access)가 있다. CDMA는 미국의 퀄컴사가 개발한 확산대역 기술을 채택한 디지털 이동통신 방식으로 여러 사용자가 시간과 주파수를 공유하면서 신호를 송수신할 수 있는 시스템이다.

표 2는 2세대 디지털 이동통신의 주요 특성을 비교한 것이다.

표 2. 2세대 디지털 이동통신의 특성 비교
Table 2. Comparison of Second-Generation Digital Mobile-Communication

구 분	CDMA	TDMA		
	IS-95 A/B	GSM	D-AMPS IS-54	PDC
서비스제공 국가	한국, 미국	유럽	미국	일본
다중접속 기술	DS-CDMA	MC-TDMA	TDMA	TDMA/FDMA
서비스 개시 시기	1996년	1993년	1995년	1995년
대역폭	1,250KHz	200KHz	30KHz	25KHz
전송속도	9.6/64Kbps	22.8Kbps	13Kbps	11.2Kbps
제공 서비스	음성통화, 단순 Text, 4Gray 이미지, 4Poly 벨소리			

2-3-3 3세대 이동통신 IMT-2000

2003년 3세대 이동통신 시대로 접어들면서 음악이나 영상과 같은 멀티미디어 서비스 시대가 시작되었다. 3세대 이동통신 기술은 IMT-2000(International Mobile Telecommunication 2000)이라 명명하여 개발되었으며, 우리나라 및 미국에서 사용되는 동기식인 CDMA-2000 방식, 유럽에서 사용하는 비동기식인 W-CDMA 방식이 대표적이다.

기존의 이동통신서비스는 서비스별 전용단말기를 이용하여야 하였으며, 지역이나 국가별로 서로 다른 주파수와 기술방식을 사용함으로써 이동성에 있어서 한계를 드러냈다. 또한, 고객들은 무선 환경에서도 멀티미디어 서비스들을 유선으로 제공받는 서비스와 동등한 수준으로 이동, 무선 데이터, 영상 통신 등을 제공받기를 원했다. 뿐만 아니라, 통신 기술이 광대역화, 고속화, 디지털화되었고, 인터넷과 모바일의 융합이 도래하면서 IMT-2000의 등장은 당연한 일이었을지도 모른다[2].

IMT-2000 서비스는 음성뿐만 아니라 영상, 멀티미디어 서비스 등 다양한 정보이용과 전세계로 서비스 영역을 확대하는 글로벌 멀티미디어 서비스이다. 표 3은 기존 이동전화 방식과 IMT-2000 방식을 비교한 것이다.

표 3. 기존 이동전화 방식과 IMT-2000 방식 비교
Table 3. Comparison of Existing Mobile-Phone and IMT-2000

구 분	기존 이동전화	IMT-2000
데이터 전송속도	14.4Kbps	144Kbps/384Kbps/2Mbps
채널 대역폭	1.25MHz	5MHz
무선 접속표준	TDMA, CDMA	CDMA2000, W-CDMA
통화품질	보통(8~13Kbps정도)	우수(8~32Kbps정도)
제공 서비스	음성, E-mail, 저속인터넷	음성, E-mail, 고속 인터넷, 영상전화, m-커머스
이용지역	국가 내	전 세계

2-3-4 4세대 이동통신 : 융합시대

미래의 이동통신으로는 ATM(Asynchronous Transfer Modes), OFDM(Orthogonal Frequency Division Multiplexing), MC-CDMA(Multi-Carrier CDMA), MIMO(Multiple Input Multiple Output), 스마트안테나 등이 있다.

4세대 서비스는 유선과 무선을 통합한 초고속멀티미디어 서비스라고 할 수 있다. 4세대 이동통신에서는 언제, 어디서나, 어떠한 서비스라도 빠르게 제공받을 수 있게 될 것이다.

2-4 디지털 이동통신의 특성과 환경

이동통신 기술의 발전으로 2세대 및 2.5세대 이동

통신 세대부터 디지털 이동통신 환경이 되었고, CDMA2000 1x 방식이 개발되어 모바일 기기에서 무선인터넷 서비스가 시작되었다.

무선인터넷이란 무선 이동통신과 인터넷 서비스의 결합으로서, 이동 중에 무선으로 모바일 단말기를 이용해 인터넷 환경의 정보나 멀티미디어 데이터를 송수신하는 것을 말한다.

무선인터넷 서비스는 언제, 어디서나 이동 환경에서 이용할 수 있는 편리성을 제공하고, 실시간 대화식으로 정보교환을 할 수 있는 즉시성을 부여하며, 휴대형 단말기를 통해 다양한 콘텐츠를 활용할 수도 있다.

우리가 지금 살고 있는 정보화 사회는 디지털 기술에 의한 기술혁신이 자아내는 정보화라는 변화의 산물이다. 그와 동시에 정보화 사회는 새로운 기술혁신을 자극하고 촉진하면서 스스로 계속 변모하고 있으며, 그러한 변화과정에서 사회 구조와 조직 원리 및 삶의 세계에 막대한 영향을 미치고 있다.

전자기기의 모바일화가 빠르게 진전되고 있으며, 모바일 기기에 새로운 기능과 서비스가 결합되는 컨버전스화도 가속되고 있다. 최근에는 각종 사물에 RFID 칩이 내장되면서 언제 어디서나 정보를 획득하고 활용하는 것이 가능해졌으며, 휴대폰에 바이오센서, 위치확인 등의 기능이 탑재되면서 헬스, 보안 서비스 등이 실현되고 있다[3].

차세대 이동통신 기술은 사용자 요구사항, 기술적인 한계, 인터넷 기술의 현 개발 단계 등을 기반으로 다음과 같은 핵심 기능들이 미래의 네트워크를 기술하는 특징이 될 것이다[4, 5, 6].

(1) 향상된 무선 기술 및 안테나

무선장치는 다중경로 전송에서 이득을 얻기 위해 다양한 스마트 안테나 기술을 사용하여 무선 네트워크의 용량을 크게 향상시켜줄 것이다.

(2) 핵심망 융합

핵심망은 IP 기반의 네트워크를 구성하게 될 것이다. 신속하고 끊김없는 수평적 핸드오버는 오랜 기간 무선접속 네트워크에서 활용되고, Mobile IP와 같은 큰 규모의 이동성 기술을 통해 수직적 핸드오버가 지원될 것이다.

(3) Ad-hoc 기술

많고 다양한 통신 계층이 Ad-hoc 통신을 지원하게 될 것이다. 다중 홉 Ad-hoc 기술은 이웃 노드를 경유하여 통신하는 방법을 이용하기 때문에 장치의 통신 영역을 더욱 확장시킬 수 있으며, 간섭이 줄어들고 배터리 사용 기간이 증가할 것이다.

(4) 간단하고 개방된 서비스 플랫폼

미래의 네트워크는 네트워크의 지능을 네트워크 경계로 밀어내고 핵심망을 간단하게 유지하도록 만들 것이다.

Ⅲ. Mobile IP 스푸핑과 포렌식 기술

3-1 Mobile IP

Mobile IP는 노드들이 인터넷에 접속된 위치에 관계없이 지속적으로 패킷을 수신할 수 있도록 인터넷에서 호스트의 이동성을 지원하기 위한 프로토콜이다. 이동 노드가 자신의 홈 네트워크에서 다른 네트워크로 이동하여 위치가 변경되더라도 자신이 홈 네트워크에 있는 경우와 같이 홈 네트워크에서 이동 노드의 고유 주소로 전송되는 데이터들을 수신할 수 있도록 해주는 기술이다[7].

그림 2는 Mobile IP의 네트워크 구성을 나타낸 것이다. 홈 네트워크와 홈 에이전트, 외부 네트워크와 외부 에이전트, 이동 노드, 상대 노드와 라우터가 있는데, 이동 노드는 외부 에이전트와 홈 에이전트를 이동하면서 패킷을 전송하게 된다. 이때 종단 시스템의 상대 노드가 모바일 노드에 대한 파트너의 역할을 한다.

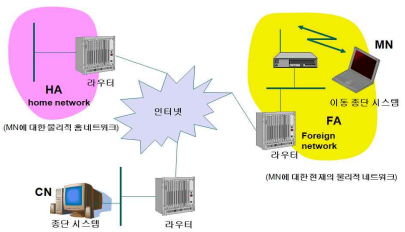

그림 2. Mobile IP 네트워크 구성
Fig 2. Composition of Mobile IP Network

3-2 Mobile IP의 동작방식

3-2-1 에이전트 광고

이동 노드는 자신이 어떤 서브넷에 위치하고 있는지를 알기 위하여 자신이 위치한 서브넷의 이동 에이전트가 누구인지를 확인하여야 한다. 이를 위하여 모든 이동 에이전트는 주기적으로 에이전트 광고 메시지를 통해 자신의 존재를 알린다. 경우에 따라서는 이동 노드가 에이전트 획득 메시지를 이용해 에이전트 광고 메시지를 요구할 수도 있다. 이동 노드는 이러한 에이전트 광고 메시지를 받아서 자신이 홈 네트워크에 있는지 아닌지 판단한다.

3-2-2 등록

에이전트 발견 절차에 따라 이동 노드가 외부 네트워크에 있다고 판단했을 경우, 이동 노드와 홈 에이전트는 등록 요청과 등록 응답 메시지를 교환함으로써 이동 노드의 의탁 주소를 홈 에이전트에 등록하게 된다. 홈 에이전트는 등록 메시지를 받으면, 필요한 정보를 자신의 라우팅 테이블에 저장을 하고 등록을 승인한 뒤 이에 대한 응답 메시지를 이동 노드에게 보낸다. 홈 에이전트가 등록 요청을 받아들인 후, 이동 노드의 홈 에이전트와 의탁 주소를 관련지어 관리한다.

그림 3은 이동 노드가 외부 에이전트를 통해서 홈 에이전트에 등록 요청을 보내고 등록 응답을 받는 Mobile IP 프로토콜의 등록 과정을 보인 것이다.

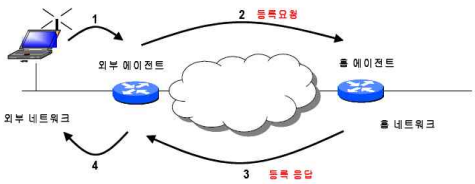

그림 3. Mobile IP 등록 과정
Fig 3. Registration Process of Mobile IP

3-2-3 터널링

이동 노드에게 패킷을 전송하는 방법에는 특정 호스트 라우팅(host specific routing), 소스 라우팅(source routing), 캡슐화(encapsulation)가 있다. Mobile IP에서 이 방법들 중 터널링 기법인 캡슐화를 사용하게 된 기술적인 이유는 성능과 보안 문제, 소스 라우트된 패킷을 차단하는 문제(ingress filtering), 인증 정보처리의 복잡함, 그리고 악의적인 중간 라우터에 의한 변경을 방지하기 위함이다.

터널링은 홈 네트워크 상에 위치한 홈 에이전트와 이동 노드가 속한 외부 에이전트 사이에서 이루어진다. 홈 에이전트는 이동 노드로 패킷을 보내기 전에 패킷을 캡슐화하여 외부 에이전트로 전송하고, 외부 에이전트는 수신한 패킷을 역캡슐화하여 이동 노드에게 전달하게 된다.

캡슐화는 패킷 헤더와 데이터로 구성된 하나의 패킷을 만들고, 이것을 새로운 패킷의 데이터 부분으로 밀어 넣는 메커니즘이다.

그림 4는 Mobile IP에 적용된 터널링을 나타낸 것인데, 하나의 터널은 터널 입구와 터널 종점 사이에서 데이터 패킷을 위한 가상 파이프(virtual pipe)를 만든다. 터널에 들어오는 패킷은 터널 안으로 전달되고, 변경되지 않은 형태로 터널을 떠난다.

그림 4. Mobile IP에 적용된 터널링
Fig 4. Tunneling applied on Mobile IP

그림 5는 IP 캡슐화 메커니즘을 보여주고 있다. 홈 에이전트는 목적지가 이동 노드인 원래의 패킷을 받은 후, 이것을 새로운 패킷의 데이터 부분에 밀어 넣고, 이 패킷이 의탁 주소로 라우팅되도록 새로운 IP 헤더를 설정한다.

그림 5. IP 캡슐화 메커니즘
Fig 5. IP Encapsulation Mechanism

3-3 이동통신에서의 공격

이동통신 기술이 발전하고 통신 환경이 점점 발달하면서 발생하는 문제점도 적지 않다. 대표적인 문제점으로는 단말기용 바이러스 확산, 피싱을 통한 개인정보의 유출, 통신서버 해킹 등과 같은 것들이 있다. 이렇게 이동통신의 문제점이 발생하는 원인으로는 첫 번째로 증가하는 무선데이터 통신을 들 수 있고, 두 번째로는 인터넷 접속을 관리하는 OS의 탑재를 들 수 있다. 이러한 이동통신 문제는 IT 기술과 사회공학적 공격이 결합된 기법이 증가하고 있는 추세이

다.

3-3-1 기술적 공격

무선 환경은 취약점을 내재하고 있으며, 다양한 제한요인이 존재하기 때문에 외부 공격자가 네트워크의 AP(Access Point)에 접근이 용이하다. 무선신호 범위 내에 존재하는 공격자는 보안성이 취약한 네트워크 AP를 경유하여 IP Spoofing, DoS(Denial of Service)공격을 통해 정보의 비밀성을 손상시킬 수 있다. 무선 환경은 유선환경에 비해서 도청이 용이하고, 반면 도청탐지는 어렵다[8].

기술적 측면에서의 공격은 스니핑(sniffing) 툴을 사용한 공격과 스푸핑(spooring)을 이용한 공격, 플러딩(flooding) 공격, 서비스 거부(denial of service) 공격과 분산 서비스 거부(distributed-denial of service) 공격의 다섯 가지 형태로 분류할 수 있다[9].

표 4는 무선 환경에서의 발생할 수 있는 보안 문제를 나타낸 것이다. 무선 환경에서는 장치의 분실이나 도난으로 인한 비밀성과 인증의 침해, IP 스푸핑으로 인한 비밀성과 무결성의 문제, 신호 방해 공격, 전원 정보 노출 등의 문제가 생길 수 있다.

표 4. 무선 환경에서의 보안 문제
Table 4. Security Concern in the Wireless Environment

보안 문제	침해 유형	원인 및 문제점
장치의 분실 및 도난	비밀성, 인증	장치 소유자가 인증 정보 소유
Rogue AP	인증	단방향 인증 환경에서 공격자 AP가 인증 없이 네트워크에 접근
IP Spoofing	비밀성, 무결성	무선 신호가 원하지 않은 사용자에게 전달
DoS	가용성	가용성 침해
신호 방해 공격	가용성	통신 채널 혼선
베터리 소진 공격	가용성	짧은 시간 내에 베터리 소진
전원정보 노출	기밀성	프라이버시 침해

3-3-2 사회 공학적 공격

사회 공학적 공격이란 시스템이나 네트워크의 취약점을 이용한 해킹기법이 아니라 사회적이고 심리적인 요인을 이용하여 공격하는 것을 가리키는 말로 흔히 미숙한 사용자들이 능숙한 해커의 사회 공학적 공격 대상이 된다.

사회 공학적 공격 기법은 접근 수단을 무엇으로 하느냐에 따라서 인간 기반 (human based)기법과 컴퓨터 기반(computer based) 기법으로 나눌 수 있다

(1) 인간 기반 기법

공격 대상에게 직접적인 접근이나 전화 등을 통해 접근하는 경우로서 중요한 고객이나 상위기관 직원 혹은 기술지원 요원 등으로 가장하여 경계심을 없애고 원하는 정보를 취득하는 방법을 의미한다.

(2) 컴퓨터 기반 기법

공격 대상에게 악성코드, 컴퓨터 프로그램 혹은 웹 사이트 등의 수단을 이용하여 접근하는 경우로서, 피싱(phishing), 스팸메일을 통한 악성코드 유포 등이 해당된다.

이처럼 사회공학적 공격은 그 적용 통로가 이메일, 인터넷 메신저, 모바일 등 사람에게로의 접근이 용이해지면서 적용범위가 확대되고 있다. 특히 최근에는 모바일 기기의 발전과 대용량화로 인한 보안 위험이 증가하고 있다.

3-4 디지털 포렌식

3-4-1 디지털 포렌식의 개요와 필요성

포렌식은 “법정의”, “공개토론이나 변론에 사용되는”, “수사와 법정에서의 증거 또는 사실 관계를 확정하기 위하여 사용하는 과학이나 기술에 관한” 이라는 의미를 갖는데, 최근에는 다양한 정보기기들의 활용과 정보생산 및 유통에 있어서 95% 이상이 디지털 형태로 이용되고 있기 때문에 물리적 형태의 증거뿐만 아니라 전자적 증거(elecronic evidence)를 다루는 디지털 포렌식(digital forensics) 분야가 점차 확대되고 있다.

디지털 포렌식은 법정 제출용 디지털 증거를 수집하여 분석하는 기술을 말하며 인권을 강조하는 요즘 IT 관련 기관과 기업을 중심으로 많은 관심이 집중되고 있다. 디지털 포렌식은 컴퓨터를 비롯하여 광범위한 디지털 장비를 그 대상으로 하며 이러한 장비와 기술을 이용하여 발생하는 범죄행위와 범죄자를 빠른 시간 내에 정확하게 찾아내고 범행에 사용된 증거를 확보하여 법정에 제출하는데 목적이 있다.

3-4-2 디지털 포렌식의 유형

디지털 포렌식은 크게 분석 목적에 따른 분류와 분석 대상에 따른 분류로 구분할 수 있다[10].

3-4-2-1 분석 목적에 따른 분류

디지털 포렌식은 분석 목적에 따라 해킹 등 침해 시스템의 로그, 루트킷, 백도어 등을 조사하여 침입자의 신원이나 피해내용, 침입경로 등을 파악하기 위한 분야를 의미하는 사고 대응 포렌식과, 범행 입증에 필요한 증거를 획득하기 위해 디지털 저장매체에 기록된 데이터를 복구하거나 검색하여 찾아내고, 회계 시스템에서 필요한 계정을 찾아 범행을 입증할 수 있는 수치 데이터를 분석하거나 이메일 등의 데이터를 복구 및 검색하여 증거를 찾아내는 것을 목적으로 하는 포렌식을 의미하는 정보 추출 포렌식의 두 가지로 분류할 수 있다[11].

3-4-2-2 분석 대상에 따른 분류

디지털 포렌식은 분석 대상에 따라 다음과 같이 몇 가지로 분류될 수 있다[12].

(1) 디스크 포렌식
디스크 포렌식은 물리적인 저장장치와 같은 각종 보조 기억장치에서 증거를 수집하고 분석하는 포렌식 분야이다.

(2) 시스템 포렌식
시스템 포렌식은 윈도우즈, 유닉스, 리눅스, 맥킨토시와 같은 컴퓨터 운영체제, 응용 프로그램 및 프로세스를 분석하여 디지털 증거를 확보하는 포렌식 분야이다.

(3) 네트워크 포렌식
네트워크 포렌식은 네트워크를 통해 전송되는 암호나 데이터 등을 특정 도구를 이용하여 가로채거나 서버에 로그 형태로 저장된 것을 접근하여 분석하거나 에러 로그, 네트워크 형태 등을 조사하여 단서를 찾아내는 포렌식 분야이다.

(4) 인터넷 포렌식
인터넷 포렌식은 인터넷으로 서비스되는 WWW(World Wide Web), FTP, USENET 등 인터넷 응용 프로토콜을 사용하는 분야에서 증거를 수집하는 포렌식 분야이다.

(5) 모바일 포렌식
모바일 포렌식은 휴대폰, 전자수첩, PDA, MP3 Player, 디지털 카메라, 휴대용 메모리카드, USB 저장장치 등 휴대용 기기에서 필요한 정보를 입수하여 분석하는 포렌식 분야이다. 유비쿼터스 컴퓨팅 시대의 도래와 이동성 기기의 확대 보급으로 다양한 종류의 멀티미디어 기기가 개발·보급되고 있는 시점에서 소형의 휴대용 기기의 데이터에 대한 범죄 증거의 확보는 매우 중요하다.

(6) 데이터베이스 포렌식
데이터베이스 포렌식은 데이터베이스로부터 데이터를 추출·분석하여 증거를 획득하는 포렌식 분야이다.

(7) 암호 포렌식
암호 포렌식은 문서나 시스템에서 암호를 찾아내는 포렌식 분야이다.

3-5 IP 스푸핑의 포렌식 요소

3-5-1 비밀성

비밀성(confidentiality)은 장치의 분실 및 도난, IP 스니퍼, 장치간의 동기화 등에 의해 침해될 수 있다. 비밀성을 유지하기 위해서는 트래픽 데이터 암호화, 키 관리 기법 제공, 이동형 장치 정보의 암호화, 서버 장치에서 저장 정보의 암호화, 저 전력 암호 알고리즘 등의 기능이 요구된다.

비밀성 제공의 범위는 크게 무선 전송 구간과 디바이스에 저장되어 있는 모든 정보가 해당되며, 디바이스들의 서비스가 중단된 후에도 위협은 여전히 계속될 수 있다. 이러한 경우의 비밀성 제공은 암호 기술을 사용하여 제공될 수밖에 없다. 물론 저장 정보도 암호화한 후 저장해 두는 것이 바람직하다.

무선 트래픽 상에서 비밀성을 보호하는 것이라면, 장치 자체가 가지고 있는 정보에 대한 비밀성도 중요하다. 또한 메타데이터를 보호하는 것도 고려해야 한다.

3-5-2 무결성

장치의 분실 및 절도, 악의적 프로그램 등에 의해 무결성이 침해될 수 있다. 무결성은 메시지 무결성과 객체 무결성으로 구분할 수 있다.

본적인 무결성 문제는 하나의 개체에서 다른 개체로 가는 메시지가 제3의 악의적인 개체에 의해 방해받지 않는 것이다.

무결성을 제공하기 위해서는 통신 프로토콜에서 원래의 데이터로부터 무결성을 위한 부가적인 정보를 만들어 내는 방법을 적용해야 하며, 통신하는 두 단말시스템 간에 무결성 정보를 전달하고 해석하는 기능이 필요하다.

3-5-3 인증

인증(authentification)에서의 기본 가정은 네트워크는 공격자들의 공격에 노출되어 있고, 안전하지 못하지만, 네트워크에 소속된 개체들은 그들의 비밀을 지킬 수 있는 능력이 있다는 것이다. 이를 해결할 수 있는 방법이 물리적인 매수 보호(physical tamper protection)장치이다. 높은 등급의 매수 저항(tamper resistance)장치를 사용한다면 공격자는 장치 내부에 유지되고 있는 비밀들에 대해 수정이나 접근조차 불가능 하게 할 수 있으나, 이는 가격이 너무 비싸고 어려운 문제이다. 이런 이유로 매수를 시도하는 공격자들을 추적할 수 있게 하는 매수 증거(tamper evidence) 장치를 이용하는 것이 더 나을 것이다.

Ⅳ. IP 스푸핑 방지를 위한 포렌식 설계

4-1 IP 스푸핑

IP 스푸핑이란 말 그대로 패킷을 전송할 때 소스 IP 주소를 속여서 다른 시스템을 공격하는 것으로 공격자가 자신의 정보를 숨기고 탐지를 피하기 위한 용도로서 역추적을 어렵게 만든다. 이러한 스푸핑 기법은 네트워크에 큰 위협이 될 수 있다.

모바일 네트워크에서 IP 주소가 조작된 패킷을 차단하는 방식으로는 ingress filtering, outgress filtering, RPF 등이 있으나 이들은 많은 라우터에 배포되 사용해야 효과가 있게 되는 제약이 있다. 그림 6은 IP 스푸핑 공격의 모형을 나타낸 것이다.

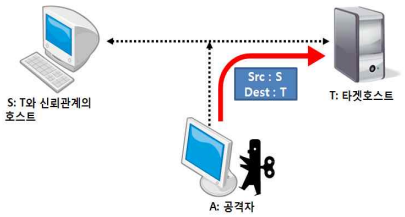

그림 6. IP 스푸핑 공격 모형
Fig 6. IP Spoofing Attack Model

IP 스푸핑은 인터넷에 연결된 사용자가 IP 패킷을 마음대로 조작하여 패킷을 전송할 수 있다는 사실을 이용한다. 수신 호스트가 패킷을 판별할 때 단지 패킷에 적힌 IP 주소만을 가지고 송신 호스트를 판단하기 때문에 수신 호스트는 패킷이 어디서 왔는지 명확하게 알 수 없다. 일반적인 경우 두 컴퓨터 사이의 인터네트워킹이 이루어질 때 오고 가는 IP 패킷 구조는 그림 7과 같다.

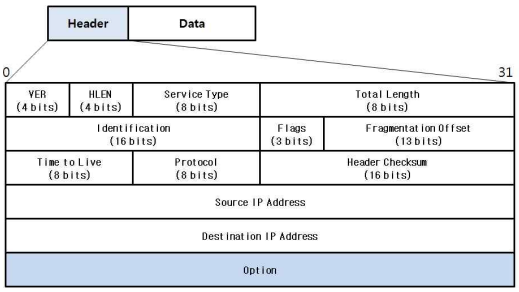

그림 7. IP 패킷 헤더 구조
Fig 7. IP Packet Header Structure

4-2 모바일 포렌식 구조 프로세스 설계

본 논문에서 설계한 포렌식 구조는 디지털 포렌식의 여러 분류 중 모바일 포렌식의 프로세스이다. 디지털증거처리 표준가이드라인과 기존에 개발된 여러 가지 포렌식 모델에서 사용하는 절차를 적절하게 재구성하여 설계하였다. 그림 8은 본 논문에서 제안하는 모바일 포렌식 구조의 프로세스를 도식화한 것이다.

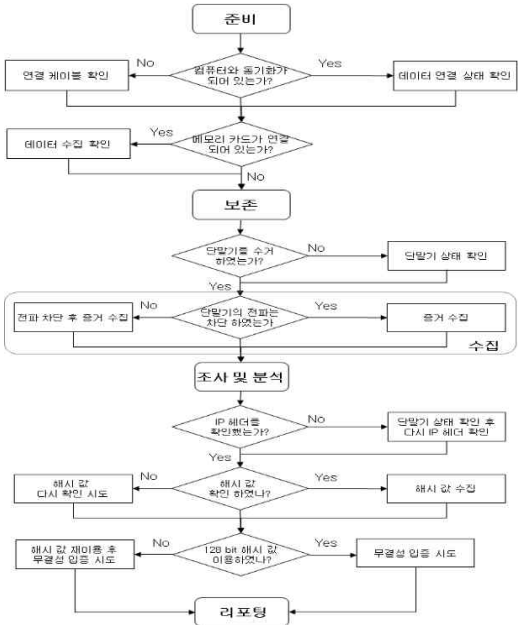

그림 8. 모바일 포렌식 구조 프로세스
Fig 8. Process of Mobile Forensic Structure

설계한 프로세스는 크게 준비, 보존, 수집, 조사 및 분석, 리포팅의 5단계로 나누어져 있으며, 각 단계별로 행해지는 세부 사항은 다음과 같다.

(1) 준비 단계

준비 단계(Readiness Phase)는 포렌식에 대한 중점 사항을 확인하고, 데이터의 무결성을 유지하기 위한 방안을 수립하는 단계이다.

(2) 보존 단계

보존 단계(Preservation Phase)는 디지털 데이터를 보존하고, 디지털 데이터를 포장하여 이송하고, 보관하는 단계이다.

(3) 수집 단계

수집 단계(Collection Phase)는 단말기로부터 정보를 수집하고, 디지털 증거물의 식별을 통한 포렌식 분석 도구를 선택하며, 실제적인 분석을 위한 단계이다.

(4) 조사 및 분석 단계

조사 및 분석 단계(Examination&Analysis Phase)는 수집된 정보에 대해 실제적인 조사와 분석이 이루어지는 단계이다.

(5) 리포팅 단계

리포팅 단계(Reporting Phase)는 모든 포렌식 절차상 일어난 사항들의 세부적인 요약본을 준비하는 과정이며 전체적인 결론에 도달하는 과정이다.

Ⅴ. 포렌식 적용 실험 및 Mobile IP 헤더 제안

5-1 포렌식 적용 실험

본 절에서는 위에서 설계한 절차를 바탕으로 하여 모바일 포렌식 적용 실험을 하였다. 실험의 목적은 앞에서 설계한 포렌식 구조 프로세스가 실무 적용에 얼마만큼 유용한지를 판단하기 위해서이다. 실험에 사용한 장비는 모바일 단말기로 휴대폰을 사용하였고, 휴대폰의 내용을 저장하기 위해 개인용 노트북 PC를 사용하였다. 그리고, 휴대폰과 PC를 연결하기 위해 USB 케이블을 준비하였으며, 데이터를 추출하고 분석하기 위해 QPST, Encase를 사용하였다.

휴대폰의 비밀번호를 입력하면 그림 9와 같이 휴대폰 안에 저장된 디렉토리와 파일을 볼 수 있다. 휴대폰의 기본적인 데이터와 내장 메모리의 루트 디렉토리에 있는 자료들을 확인할 수 있다. 디렉토리별 사진, SMS, DB 등의 파일들이 있다. 이 중에 단말기의 기본 모델정보와 SMS 파일을 PC에 저장한다.

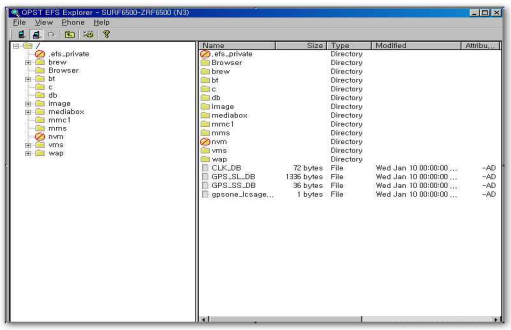

그림 9. 휴대폰 내용 확인 화면
Fig 9. Screen of Mobile-Phone Contents Confirmation Screen

5-2 단말기 분석도구를 이용한 데이터 분석

단말기의 데이터를 PC에 저장하였으면 단말기 분석도구를 이용하여 추출한 데이터들을 분석한다. 본

논문에서는 그림 10과 같이 휴대폰에서 추출된 데이터에 대한 로그 및 시간 등을 확인한다.

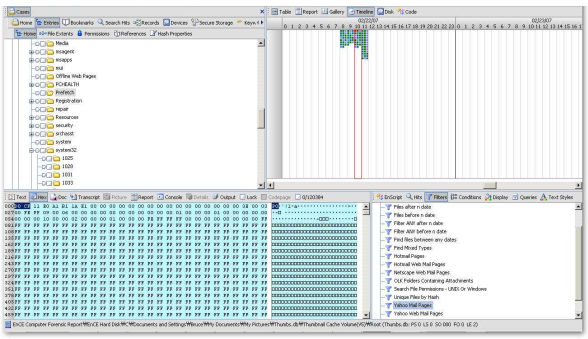

그림 10. 디지털 증거 분석 화면
Fig 10. Digital Evidence Analysis Screen

5-3 Mobile IP 헤더 제안

본 논문에서는 이동통신과 모바일 인터넷 환경에서 일어날 수 있는 IP 스푸핑 공격을 방지하여 개인정보를 보호하기 위한 방안으로 Mobile IP 헤더에 사용자 인증 옵션으로 모바일 정보기기의 해시값을 사용하는 방법을 제안한다. 해시값을 얻기 위해 디지털 포렌식을 활용하여 모바일 포렌식 프로세스를 설계하고 프로세스 모델을 바탕으로 실험을 하였다.

모바일 정보기기의 인증 헤더에 포함되는 인증 데이터 정보에 해시값을 적용한다. 그림 11은 Mobile IP 헤더의 구조를 도식화 한 것이고, 그림 12는 사용자 인증 옵션으로 해쉬값을 적용할 때와 적용하지 않을 때의 IP 스푸핑 발생 빈도를 측정하기 위한 알고리즘 일부이다. 128bit의 해시값을 체크하여 고유 해시값이 확인되면 스푸핑을 방지하게 되는 것이고, 고유 해시값이 확인되지 않으면 스푸핑 공격을 받기 쉽다.

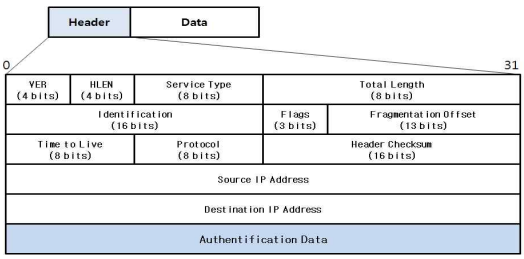

그림 11. Hash Authentication 옵션을 추가한 Mobile IP 헤더
Fig 11. Mobile IP Header Added Hash Authentication Options

```
int put_cmsg(struct msghdr * msg, int level, int type, int len, void *data)
{
        struct cmsghdr *cm = (struct cmsghdr*)msg->msg_control;
        struct cmsghdr cmhdr;
        int cmlen = CMSG_LEN(len); // include 128bits MD5 Hash Bits
        int err;

// check if the msg has valid source address by 128 bits MD5
if(check if the msg has valid source address by 128 bits MD5 )
   {
      OK
    } else {
              spoofingFailure++;
    }
...
}
```

그림 12. Hash Authentication 옵션 적용 알고리즘
Fig 12. Algorithm Applied Hash Authentication Options

Ⅵ. 결 론

본 논문에서는 변화하는 정보화 사회의 이동통신 환경에서 발생할 수 있는 여러 가지 보안 문제들을 살펴보고, 이 가운데 Mobile IP 스푸핑 문제에 대한 방지 대책을 제안하기 위해 디지털 포렌식 기법을 활용하였다. 디지털증거처리 표준가이드라인과 기존에 개발된 여러 가지 포렌식 모델에서 사용하는 절차를 적절하게 재구성하여 모바일 포렌식 프로세스를 설계하였고 설계 모델을 바탕으로 실험을 하였다. 그리고 이동통신의 데이터 유통과정에 대한 시나리오를 작성하여 실험을 통해 얻어진 해쉬값을 Mobile IP 헤더의 인증 데이터로 적용하는 알고리즘을 제시하였다.

이 방법은 데이터에 대한 무결성을 입증하여 법적 근거 자료로서의 효율을 높일 수 있다는 장점이 있다.

그리고 포렌식 적용 실험에서 추출한 데이터 중 단말기 모델에 대한 데이터를 분석해 얻은 해쉬값을 Mobile IP 헤더의 인증 옵션 데이터로 사용한다면 Mobile IP 스푸핑을 최소화할 수 있는 가능성은 충분히 있다고 사료된다.

향후 연구과제는 빠르게 변화하는 디지털 이동통신 환경에 따라 휴대폰뿐만 아니라 다른 모바일 정보기기의 정보보호에도 적용이 될 수 있는, 보다 정형화되고 표준화된 모바일 포렌식 프로세스를 개발하는 것이다.

참 고 문 헌

[1] 최영진, “미래 정보통신 전송방식에 대한 고찰”, 석사학위논문, *배재대학교*, 2004.
[2] 한인숙, “사용자 중심의 차세대 이동통신(4G) 발전방향”, 석사학위논문, *전남대학교*, 2004.
[3] 민병석, "모바일 컨버전스의 확산과 대응", *삼성경제 연구소*, 2005.
[4] BRAIN, Broadband Radio Access for IP based Network, IST-1999-10050, http://www.cordis.lu, http://www.ist-brain.org, 2001.
[5] DRIVE, Dynamic Radio for IP-Services in Vehicular Environments, IST-1999-12515, http://www.cordis.lu, http://www.ist-drive.org, 2001.
[6] WWRF, Wireless World Research Forum, http://www.wireless-worldresearch.org, http://www.wwrf.org, 2002.
[7] 박지연, “Mobile IP에서 안전한 멀티캐스트 서비스를 위한 보안 메커니즘 및 구조에 관한 연구”, 석사학위논문, *이화여자대학교*, 2003.
[8] 정영석, “인텔리전트 빌딩 시스템 구축과 네트워크 보안정책 수립에 관한 연구”, 석사학위논문, *전남대학교*, 2006.
[9] 크리스찬 반, “무선네트워크 해킹방지 솔류션”, *정보문화사*, 2003.1.
[10] 정용석, “포렌식을 활용한 개인정보보호 시스템 연구”, 석사학위논문, *건국대학교*, 2007.
[11] Kruse, W.G. & Geiser, J.G., "Computer Forensics Incident Respose Essentials", New York: *Addison-Wesley Professional*, 2001.
[12] 전상덕 외, “디지털 포렌식의 기술 동향과 전망”, *정보화정책 제13권 제4호*, pp3～19, 2006년.
[13] 안희국, “스팸메일 필터링을 위한 한글 변칙어 인식 방법”, *한국항행학회 논문지*, 제15권 제2호, 2011. 4.
[14] 허계범, “UML기반의 요구사항 추적 매트릭스 설계”, *한국항행학회 논문지*, 제15권 제3호, 2010. 6.

박 순 희 (朴順姬)

2007년 2월 : 강원대학교 이학석사
2009년 8월 : 강원대학교 이학박사
2007년 ~현재 한림성심대학, 강원대학교 시간강사
관심분야 : 온톨로지, 포렌식, 유비쿼터스

양 동 일 (梁東一)

2004년 2월 : 강원대학교 컴퓨터과학과 이학석사
2007년 8월 : 강원대학교 컴퓨터과학과 이학박사
2007년 ~현재: 한림성심대학교 인터넷비즈니스과
관심분야 : 소프트웨어공학, 유비쿼터스, 온톨로지

진 광 윤 (陳廣允)

1984년 2월 : 서울산업대학교 전자계산학과 공학사
1987년 2월 : 건국대학교 전자계산학과 공학석사
2004년 2월 : 경남대학교 컴퓨터 공학과 공학박사
1990년 3월 ~ 현재 : 강원대학교 컴퓨터공학과 교수
관심분야 : 정보보안, 유비쿼터스, 임베디드시스템

최 형 진 (崔亨振)

1990년 : 일본 동경공업대학 정보공학 공학박사
1990년 ~ 1991년 : 한국전자통신연구원 선임연구원
1991년 ~ 현재: 강원대학교 컴퓨터과학과 교수
관심분야 : 인공지능, 유비쿼터스, 영상처리