2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

모바일 지리정보시스템에서 보안을 고려한 설계

[0]이상철*, 이충호*, 오영환*, 임기욱**, 배해영*

*인하대학교 전자계산공학과
**선문대학교 산업공학과
philmap@korea.com

Design for Security in Mobile GIS

[O]Sang-Cheol Lee*, Chung-Ho Lee*, Young-Hwan Oh*, Ki-Wook Rim**, Hae-Young Bae*

*Dept. of Computer Science & Engineering, INHA University

**Dept. of Industrial Engineering, SUNMOON University

요 약

PC 환경이 아닌 무선 인터넷 환경에서 제공되는 Mobile GIS(Geographic Information System)는 시간과 공간의 제약을 극복하고 실시간으로 지리정보를 얻을 수 있는 장점을 가지고 있으나, 사용자의 무선단말기와 서버 사이에 접속이 유지되어 있어야만 무선으로 GIS 서비스를 이용할 수 있다. 이는 현재 국내 무선 네트워크의 느린 속도와 비싼 이용 요금을 감안하면 Mobile GIS 가 대중화되는 데 장애요인이 되고 있다. 그리고 무선 인터넷 서비스가 급격히 증가하면서 Mobile GIS 는 보안상 약점을 드러낼 것으로 예측된다. 그러므로 본 논문에서는 공개된 불특정다수의 무선 네트워크 환경에서 발생할 수 있는 보안의 피해와 그에 따른 기본적 Mobile Security 서비스에 대해 알아보고, 정보보호 입장에서 Mobile Database 를 연구하였다. 또한 Mobile GIS 를 위한 WAP 게이트웨이에서 공간데이터의 유출 가능성을 발견하였고, 이를 위한 해결책으로 J2ME 의 Pre-verification 기능과 종단간 암호화(End-to-End Security) 기능을 Mobile GIS 설계에 적용하여 무선 환경에서 동적인 지도서비스와 더불어 공간 데이터의 보안을 유지할 수 있는 기법을 제시하였다. 이 연구를 통해 대역폭(Bandwidth)의 한계를 지닌 개방적 무선환경에서 Mobile GIS 와 같은 컨텐츠 프라이버시(Contents Privacy) 보호가 요구되는 분야에 응용될 수 있으리라 기대된다.

1. 서론

무선 인터넷 환경(Mobile Internet Environment)은 사용자가 양방향 페이저(Two-pager), 휴대폰(Cell phone), PDA 등의 이동 가능한 장비를 갖추고 무선 통신을 통해서 정보제공자로부터 시간과 공간의 제약을 뛰어넘어 원하는 정보를 얻어낼 수 있는 작업환경을 의미한다. GIS(Geographic Information System)는 인간생활에 필요한 지리정보를 효율적으로 활용하기 위해 모든 자료나 정보는 데이터베이스에 의하여 관리되고 표현된다. 즉, GIS 는 정보 표현에 있어 필요에 따라 다양한 형식으로 변화되는 장점을 가진다.

이처럼 최근 무선 인터넷의 급진적 증가를 배경으로 하여 시간과 공간의 제약을 극복하고 실시간으로 무선 지리정보를 얻어 실생활에 효율적으로 활용할 수 있는 Mobile GIS 가 등장하게 되었다.

그러나 Mobile GIS 는 아직 초기단계로, 응용 애플리케이션을 단순히 무선으로 다운로드 받아 네트워크의 비연결 상태에서 사용하는 스탠드얼론(StandAlone) 방식이 아니라, 클라이언트인 사용자는 지리정보를 서비스할 서버와의 상호 신호를 주고 받으며 진행되어야 한다. 즉, 무선단말기를 통해 사용자가 무선 네트워크상에서 찾고자 하는 지역에 해당되는 위도(Latitude)와 경도(Longitude)의 질의를 던지면 유선의 서버에서는 질의 요청된 지역에 해당하는 공간데이터를 사용자에게 전송하는 방식이다. 이때 사용자의 무선단말기와 서버간의 접속이 유지되어 있어야만 무선으로 GIS 서비스를 이용할 수 있는데 이는 현재 국내 무선 네트워크의 느린 속도와 사용자는 서비스 이용료와 더불어 망 사용료를 지불해야 하는 이용요금의 부담이 Mobile GIS 의 대중화에 장애요인이 되고 있다. 또한 Mobile GIS 서비스를 사용함에 있어 무선 인터넷 환경에서 사용자의 번호를 불법 사용하여 합법적인 사용자에게 엄청난 사용료를 과금 시킬 수 있고, 프로토콜의 불안전으로 사용자가 요구한 영역의 공간데이터가 도청 될 수 있는 컨텐츠 프라이버시(Contents Privacy)와 무선 네트워크 관리자가 특정 단말기 사용자의 위치 정보를 이용하여 추적 할 수 있는 위치 프라이버시(Location Privacy)

• 본 연구는 정보통신부의 대학 S/W 연구센터 지원사업의 결과임

등의 보안상 문제가 발생할 수 있다.

본 논문에서는 이러한 취지에서 J2ME 의 Pre-verification 기능과 종단간 암호화(End-to-End Security) 기능을 Mobile GIS 설계에 적용하여 무선의 환경에서 동적인 지도 서비스와 더불어 공간 데이터의 보안을 유지할 수 있는 기법을 제시하고자 한다.

본문의 구성은 2 장에서 기본적인 Mobile Security, Mobile Database 등의 관련연구를 하며, 3 장에서는 기존의 Mobile GIS 를 위한 WAP 게이트웨이에서 공간데이터의 유출 가능성을 제시하며, 4 장에서는 무선의 환경에서 동적인 지도 서비스를 받을 수 있고 정보보호를 고려한 Mobile GIS 를 제안하며, 5 장인 결론에서는 Mobile GIS 에서 보안의 의미를 되새기며, 향후 진행할 연구를 기술한다.

2. 관련연구

본 장에서는 공개된 불특정다수의 무선 네트워크 환경에서 발생할 수 있는 보안의 피해와 이에 대비한 기본적 Mobile Security 서비스에 대해 알아보고, 정보보호 입장에서 Mobile Database 에 대한 연구를 실시 한다.

2.1 기본적 Mobile Security 서비스

무선 인터넷 환경에서 사용자 번호를 도용하거나 불법 사용하여 합법적인 가입자가 과금시 큰 피해를 가져올 수 있고, 암호화 알고리즘이나 프로토콜이 안전하지 않은 경우 사용자의 통화정보는 도청될 수 있다. 또한 네트워크내의 인증센터나 기지국이 결탁하여 특정 단말기 사용자의 위치정보를 이용하여 사용자를 추적 할 수 있는 프라이버시 침해가 발생 할 수 있다[7]. 이런 무선 통신 환경에서 보안의 위협적 요소에 대비하여 Security 서비스를 고려하면 다음과 같다.

- 인증(Authentication)
  이동통신에서 인증이란 단말기를 소지한 사용자가 통화 초기에 설정된 비밀 정보를 서비스 제공자에게 증명하여 정당한 가입자임을 밝히는 절차이다. 이는 단말기의 불법 사용으로 인해 합법적인 가입자가 사용하지도 않은 서비스에 대한 과금의 피해를 방지하기 위한 대책으로 이동 통신 서비스 제공자인 통신 사업자에 대해서는 반드시 고려하여야 할 Security 서비스이다. 이러한 인증 작업은 인증 알고리즘과 인증 프로토콜에 의해서 이루어 질 수 있다.
- 암호(Encryption)
  무선 인터넷 환경에서 암호화되지 않은 공간데이터 정보가 무선 구간을 통해 쉽게 그리고 발각되지 않고 불법 도청이 일어날수 있다. 이러한 관점에서 무선 구간의 데이터정보는 반드시 암호화되어 보내어져야 한다. 이러한 암호화는 암호화에 사용될 키(Session Key)가 선행되어 공유되어야 하며, 반드시 인증 절차가 완료된 후에 수행되어져야 한다.
- 추적 불가능성(Party anonymity)
  추적 불가능성이란 송신자의 위치정보나 통화당사자에 대한 정보가 제 3 자에게 노출되어 추적되는 것을 방지하기 위해서 공개키 암호를 사용하여 무선 정보를 이용하는 사용자의 프라이버시를 보호해주는 기능이다. 그러나, 여전히 공개키 암호의 사용도 인증센터나 기지국 등의 결탁에 의해 개인 사용자의 위치정보나 사용자 정보는 침해를 입을 수 있으므로, 이때에는 익명의 통신 네트워크(Anonymous Communication Network)를 이용한 방식[1],[2]을 활용할 수 있다.
- 키 관리(Key management)
  무선 인터넷에서 암호화된 알고리즘에서 인증, 암호 그리고 추적 불가능의 서비스를 제공함에 있어 이러한 알고리즘이나 각종 방식에 사용되는 주요한 변수나 키들의 관리에 따라 시스템 전체의 안전이 위태로울 수 있다. 그러므로 키 관리에서 키의 생성,분배,주입 및 파기에 대한 것이 고려되어야 한다[7].

2.2 Mobile Database

네트워크 상에서 데이터베이스 보안으로 정보의 부적절한 노출을 방지하는 기밀성(Confidentiality)과 정보의 부적절한 변경을 예방하고 감지하며 타인이 다른 사람의 정보를 임의 또는 불법적으로 변경하지 못하도록 하는 무결성(Integrity), 데이터베이스 시스템이 제공하는 서비스에 대한 부적절한 거부를 예방하고 감지하는 가용성(Availability) 등이 고려되어야 한다. 즉, 데이터베이스에서 보안상 정보누출, 무결성 위배, 서비스 거부, 위법 사용 등이 주된 위협 요소가 되고 있다.

보안의 대부분 문제들은 기밀성과 관련되어 있는데 무선 인터넷의 관점에서 컨텐츠 프라이버시(Contents Privacy), 발신자와 수신자의 비연결성(Disconnection), 위치 프라이버시(Location Privacy) 등이 중요 요소들이다.

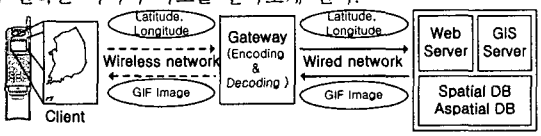
무선 연결 상태에서 데이터나 메타데이터 전송은 보안의 위협을 받는다. 즉, 무선 통신에서 통신 비용의 절약을 위해 사용자가 강제로 연결을 끊을 수 있고 또는 오류에 의해 연결 끊김(Disconnection)이 종종 발생하기도 한다. 이런 현상은 데이터의 복사 없이는, 데이터의 일관성(Consistency)에 위험을 줄 수 있다. 그러나 데이터베이스 시스템은 또한 예상치 못한 연결 끊김에 있어 데이터 손실을 피하기 위해 트랜잭션 회복(Transaction recovery)의 의무를 가지고 있다. 네트워크 분할의 빈도가 높으면 높을수록 고정된 네트워크보다 더욱 강력한 에러 회복이 요구된다. 이런 연결 끊김은 에러회복 이외에도 공격자들에게 무선단말기(Mobile unit) 또는 기지국(Base station)에 공격 구실을 제공한다[3].

또한 신원의 가장(Masking the identity)으로 데이터들은 부적당하게 공개될 위험이 발생한다. 더욱이 추가적인 노력없이 간단한 방법으로 공중파 정보의 접근이 가능하기 때문에 무선연결의 사용은 정보의 도청을 용이하게 한다. 이런 종류의 보안 위배는 탐지하기 매우 어렵다. 이런 모든 경우에서 정보보호는 사용자 인증과 데이터 프라이버시(Data Privacy)수행을 위한 암호화에 의존한다. 모바일 사용자들은 도메인의 인증 서버에 그들의 실제 신원이나 익명이 등록된다. 인증 서비스는 서로 간의 실제적인 통신에 있어서 상대방에게 신뢰를 제공해야 한다. 뒤이어 일어나는 통신은 공격과 도청에 대비하여 데이터 전송이 보호되어야 한다. 이 과정에서 인증을 위해 비대칭 암호화(Asymmetric encryption)와 안전한 무선 통신을 위해 대칭 암호화(Symmetric encryption)기법을 사용한다. 또한 분산된 프레그먼트들(Fragments) 사이에 내부의 데이터베이스 통신은 안전하게 구현되어야 한다[3]..

3. WAP 게이트웨이에서 공간데이터 유출 가능성

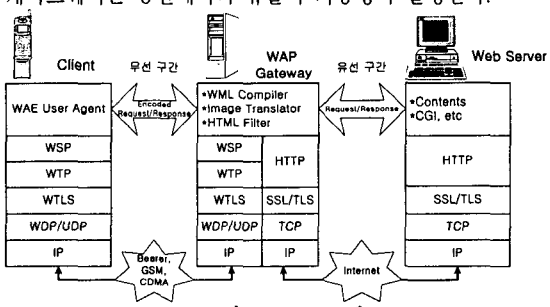
현재 Mobile GIS 를 위한 WAP 의 구조는 [그림 1]과 같다. 즉, 휴대폰 단말기나 양방향 페이저, PDA 등의 클라이언트 부분과 웹서버, GIS 서버, DB 등으로 구성된 서버 부분, 그리고 중간에 게이트웨이로 이뤄 졌다. 클라이언트와 게이트웨이 사이에는 무선네트워크로 연결되어 있으며, 서버와 게이트웨이 사이에는 유선네트워크로 이뤄진다. 그러므로 무선

단말기를 통해 지도 서비스를 받고자 하는 사용자가 선택한 지역의 위도와 경도 데이터가 무선망을 통해 게이트웨이로 전달되고 다시 유선망을 통해 그 데이터들은 서버로 전달되게 된다. 위도(Latitude)와 경도(Longitude)로 질의 된 영역의 벡터지도가 Image Generator 를 통해 GIF 이미지 파일로 컨버젼되어 서버에서 유선망을 통해 게이트웨이로 전송되고 다시 무선망을 통해 클라이언트로 전송되어 사용자는 자신이 원하는 지역의 지도를 받아보게 된다.



[그림 1] Mobile GIS 를 위한 WAP 아키텍쳐

Mobile GIS 에서 WAP 아키텍쳐가 상호운용성(Interoperability)과 확장성(Scalability) 등 을 제공하지만, [그림 2]에서 처럼 WAP 아키텍쳐가 유선망에서는 기존의 프로토콜인 SSL(Secure Socket Layer)을 그대로 사용하고 무선망에서는 무선환경에 적합한 프로토콜인 WTLS(Wireless Transport Layer Security)을 사용하는 연결 분리(Split connection)기법을 채택 함으로서 유선구간과 무선구간의 서로 다른 프로토콜을 가진다. 즉, WTLS 로 암호화(Encoding)된 데이터는 WAP 게이트웨이에서 복호화(Decoding)된 후 SSL 로 암호화되어 서버에게 전달되며, 반대로 SSL 로 암호화된 데이터는 WAP 게이트웨이에서 복호화된 후 WTLS 로 암호화되어 클라이언트에게 전달된다. 이런 과정에서 WAP 게이트웨이는 공간데이터 유출의 가능성이 발생한다.

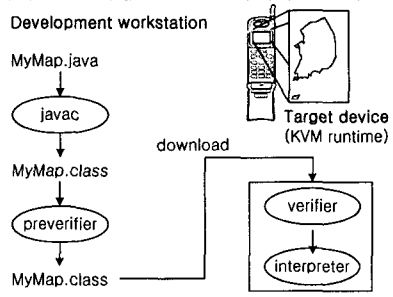


[그림 2] WAP 모델

그러므로 4 장에서 이런 문제점들을 보완한 무선환경의 동적인 Mobile GIS 를 설계하고자 한다.

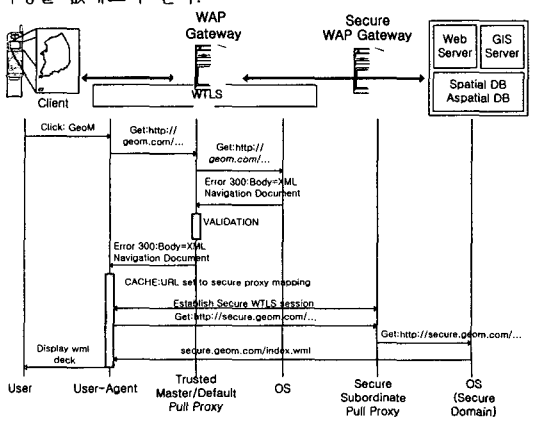
4. 동적이며 보안을 려한 Mobile GIS 설계

현재의 휴대폰 단말기의 경우 80386 정도의 프로세서와 2MB 정도의 플래시 메모리로는 기존의 PC 수준의 J2EE 나 J2SE 의 플랫폼을 탑재하는 것은 힘든 일이다. 또한 무선 인터넷 환경에서 Mobile GIS 를 통한 지리정보를 얻기 위해 사용자의 무선단말기와 서버간의 접속이 유지되어 있어야 하지만 무선 네트워크의 대역폭(Bandwidth)에는 한계가 있다. 그러므로 최대한 사용자의 무선단말기에 GIS 및 그래픽 기능 등을 임베디드(Embedded) 시켜 작은 파일 크기의 공간데이터를 전송 받게 하여 무선의 환경에서의 동적인 지도 서비스를 구현하며, J2ME 의 CLDC(Connected Limited Device Configuration)에서 클래스 파일 검증 단계를 통과하기 위해 자바 클래스 파일의 다운로드를 요구하여 낮은 레벨의 가상머신의 보안을 수행한다. 즉, CLDC 는 자바 가상머신(Java VM)이 부적절한 클래스파일들(Invalid Classfiles)을 인식하고 거부할 수 있는 기능이 필요하지만 J2SE 에 맞게 규정되어 무선 인터넷 단말기에서는 큰 메모리를 요구하게 되므로, CLDC 자체적으로 제안한 클래스 파일 검증 매커니즘을 사용하도록 한다. 자바 클래스파일 다운로드시 "Stackmap" 속성을 포함시킨다. 이 속성으로 클래스 파일 내의 각각의 메소드를 분석하는 "Pre-verification"에 의해 표준 클래스 파일에 더해진다. [그림 3] 에서와 같이 Pre-verification 은 사용자의 단말기에 클래스 파일이 다운로드 되기 이전 서버 시스템에서 수행된다. 이 Stackmap 속성은 클래스 파일을 대략 5%정도 증가시키나, 실제적으로는 적은 가상머신 코드를 가지며 일반적인 자바 가상머신보다 빠르게 수행된다. 또한 일반의 자바 가상머신의 검증단계보다 RAM 소비를 동적으로 처리하며 같은 레벨의 보안을 유지하게 된다.



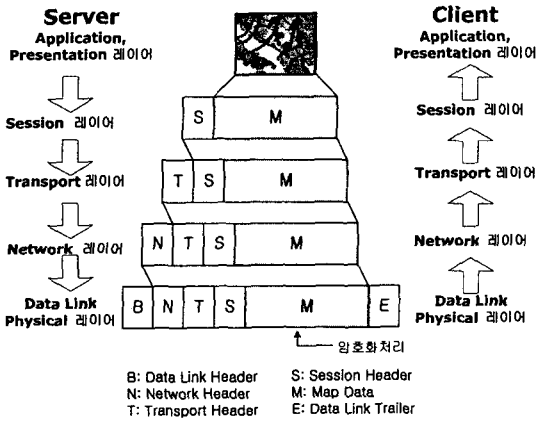
[그림 3] CLDC/KVM 에서 클래스파일 검증

Mobile GIS 가 운영되기 위해서 클라이언트인 사용자는 서버와의 상호 신호를 주고 받으며 진행되어야 한다. 즉, 무선단말기를 통해 사용자가 무선 네트워크상에서 Mobile GIS 서비스에 접속하여 원하는 지역의 위도,경도의 질의를 던지면 유선의 서버에서는 질의된 지역에 해당하는 공간데이터를 GIF 이미지 파일로 컨버젼(Conversion) 한 후 GIF 이미지 파일을 바이트 열로 변환하여 전송한다. 이때 [그림 2]처럼 WAP 게이트웨이에서 복호화와 암호화를 거치는 과정에서 공간 정보인 위도와 경도, GIF 이미지 파일들은 노출 가능성이 생기므로, 이를 대비한 종단간 암호화(End-to-End Security)가 제공 되어야 한다. 본 논문에서는 [그림 4]와 같이 웹서버 바로 앞에 또 하나의 Secure WAP 게이트웨이를 추가설치하며 이 구간은 안전한 영역(Secure domain)으로 유지한다. WAP 게이트웨이는 단순히 무선구간과 유선구간 사이의 중계 역할만 담당하도록 하여 WTLS 와 SSL 간의 변환 과정을 없애도록 한다.



[그림 4] A transport layer end-to-end security

즉, 종단간 암호화는 [그림 5]와 같이 모든 라우팅과 전송 처리에 앞서 이뤄지므로 메시지는 암호화 형태로 네트워크 상에서 전달되고 만약 네트워크에서 보안이 깨질 경우 데이터가 노출되더라도 데이터의 기밀성은 위협 받지 않게 된다.



[그림 5] 종단간 암호화(End-to-End Security)

그러나 데이터의 발신자가 발신사실을 부인하지 못하게 하며, 수신자가 수신사실을 부인하지 못하도록 방지하는 부인방지(Non-repudiation)가 또한 필요하다. 부인방지는 전송되는 모든 데이터에 대해 전자서명을 제공함으로써 가능하나, 많은 연산이 요구되며, 대역폭(Bandwidth)과 통신 속도의 한계를 가진 무선환경에서 비효율적이다. 그러므로,아래의 예와 같이 WMLScript 의 Crypto Library 에서 제공하는 Crypto.signText() 함수를 이용해 중요한 WML 문서에 대해서만 전자서명을 하도록 한다.

```
Var foo = Crypto.signText(" Coordinate of building\n
----------\n3 Name=Seoul Station \n1
X=200184.6734\n1 Y= 400063.3134\n1", 0,1, "\x37\x00\xB6\x96\
x37\xE3\x93\x48\x74\xD3\x98\x47\x53\x94\x34\x58\x97\xB5\
xD6"); //The application indicates the signature key
```

5. 결 론

본 논문은 지리정보를 무선 인터넷 환경에서 시간과 공간의 제약을 극복하여 실시간으로 제공할 수 있는 Mobile GIS 구현에 대한 연구를 하면서 개방적인 무선환경에서 현재의 무선 네트워크가 가질 수 있는 대역폭(Bandwidth)의 한계와 통신 속도를 고려하게 되었으며, 또한 공개된 불특정다수에게서 발생할 수 있는 네트워크와 데이터베이스의 보안의 위험성을 연구하였다. 또한 본 논문에서는 J2ME 의 CLDC 및 MIDP 를 이용하여 사용자의 무선단말기에 GIS 및 그래픽 기능 등을 임베디드(Embedded) 시켜 작은 파일 크기의 공간 데이터를 전송 받게 하며, Pre-verification 기능과 종단간 암호화(End-to-End Security) 기능을 고려하여 무선의 환경에서의 동적이며 보안을 고려한 지도 서비스를 설계하였다.

향후 연구로 이런 연구와 설계를 바탕으로 동적이며 안정적인 Mobile GIS 의 구현과 성능평가가 요구되어 진다.

참고문헌

[1] S.Houmura, R.Sakai and M.kasahara, "Schemes of Anonymous Channel on Communication Networks", Technical Report of IEICE, IT93-64, pp.7-11.1993

[2] D.A. Cooper and K.P.Birman, "Preserving Privacy in a Network of Mobile Computers", Proceedings of IEEE Symposium on Security and Privacy, pp.26-38. 1995

[3] Astrid Lubinski. "Security Issues In Mobile Database Access", KLUWER ACADEMIC PUBLISHERS, 1999

[4] C.Boyd, A.Mathuria. "Key establishment protocols for secure mobile communications: a critical survey", Computer Communications, 2000

[5] Upkar Varshney and Ron Vetter, "Emerging Mobile and Wireless Networks", Communications Of The ACM, pp.73-81, 2000

[6] WAP Forum, "WMLScript Crypto Library", Version 05-Nov-1999

[7] Artem Garmash, "A Geographic XML-based Format for the Mobile Environment", Proceedings of the 34th Hawaii international Conference on System Sciences, 2001

[8] 박춘식, "디지털 이동 통신을 위한 안전 대책", 한국통신학회논문지, 1996, Vol.21 No.3

[9] 류재철, "모바일 인터넷과 보안기술 동향", 정보보호연구회발표논문집, pp.23-39, 2001