공간 데이터의 안전한 전송을 위한 구조설계

장민영*, 임정은
*고려대학교 컴퓨터과학기술대학원 컴퓨터 공학과, 고려대학교 정보통신대학 컴퓨터학과
e-mail : sunny7511@nate.com, jelim@software.korea.ac.kr

Designing the structure for secure transmission of spatial data

Min-Young Chang* Jung-Eun Lim
*Dept. of Computer Engineering, Graduate School of Computer Science & Technology, Korea University
Dept of Computer Science & Engineering, Korea University

요 약

최근 컴퓨터 성능과 네트워크 속도의 발전은 다양한 형태의 데이터를 유선 혹은 무선 환경상에서 주고 받고 처리할 수 있게 해주고 있다. 또한 일차원적인 텍스트, 이미지, 음성, 동영상뿐만 아니라 다차원 형태의 공간 데이터도 다양한 형태의 서비스로 제공되고 있다. 하지만 공간 데이터에 대한 연구는 공간 데이터 표준, 서비스, 성능적인 측면에 대한 연구만 진행이 되었을 뿐 보안적인 측면에 대한 연구는 미비한 상태이다. 이에 XML 의 보안 기법을 공간 데이터에 적용하여 공간 데이터 자체에 대한 보안 레벨과 암호화를 적용하여 공간 데이터 전송을 위한 보안구조를 제시하고자 한다.

1. 서론

공간 데이터는 초기에 토지, 지질, 해양, 군사와 같이 일반인보다는 특정한 계층에서 사용되어 왔지만 이제는 일반인들도 다양한 환경에서 제공받고 있다. 공간 데이터 사용자는 standalone 뿐만 아니라 멀티-티어(multi-tier) 환경을 통해서 제공받고 있는데, 공간 데이터를 제공 받기 위한 네트워크는 TCP/IP 가 적용되었고, TCP/IP 는 다양한 위협에 노출된 구조를 갖고 있다[1-2]. 그리고 공간 데이터 역시 정보 자원이기 때문에 정보 보안 관점에서 정보의 가용성(availability), 기밀성(confidentiality), 완전성(integrity), 서비스의 책임성(accountability)을 반드시 유지해야 한다[3].

공간 데이터는 군사 좌표, 개인의 위치정보와 같이 보안을 필요로 하는 데이터를 가질 수 있다. 하지만, 보안에 대한 처리를 일반 데이터와 동일시 처리하기 때문에 공간 데이터가 가지는 특성을 제대로 살리지 않고 있는 현실이다. 이런 상황에서 공간 데이터에 대한 연구는 공간 데이터 표준, 서비스, 성능적인 측면에 대한 연구만 진행이 되었을 뿐 보안적인 측면에 대한 연구는 미비한 상태이다. 이에 공간 데이터의 보안을 위하여 공간 데이터의 콘텐츠 수준에서 암호화를 수행하여 공간 데이터의 정보 보안을 유지하도록 하고, 이를 위해 본 논문에서는 공간 데이터 보안을 위하여 XML 의 보안 기법과 공간 데이터 암호화를 위해 SEED 대칭형 암호화 알고리즘을 적용하여 공간 데이터 전송을 위한 보안 구조를 제안하려 한다.

2. 관련 연구

2.1 공간 데이터 구조 및 전송

OGC(Open GIS Consortium)는 글로벌 비영리 단체로 공간 그리고 위치 기반 서비스의 개발에 대한 표준을 제정하고 이끄는 단체이다[4]. 이 단체는 여러 공간 데이터 서비스에 대한 표준 제정작업을 수행 중인데, 그 중에서도 공간 데이터에 대한 서비스를 제공하기 위한 표준 공간 데이터 구조인 Simple Feature CORBA, SQL, OLE/COM, WKB(Well Known Binary)을 제공한다.

그리고 공간 데이터 구조의 표준 포맷을 발전하여 XML 의 확장구조로 공간 데이터에 대한 GML(Geographic Markup Language)을 제정하여 이미 OpenGIS Specification 을 제공하고 있다. 그리고 공간 데이터를 서비스하기 위한 방식으로 Web Coverage Service, Web Feature Service, Web Map Service 를 제공하고 있고, 공간 데이터의 전송을 HTTP 의 형태로 제공하고 있다. 또한, 현재 공간 데이터에 대한 웹 서비스를 위해 OGC Web Services SOAP Experiment Report (SOAP), OGC Web Services UDDI Experiment (UDDI)을 Discussion Papers 로 제안되고 있다.

2.2 XML 보안

XML(Extensible Markup Language)은 W3C(World Wide Web Consortium)에서 제정된 문서의 저장 및 전송을 위한 표준화 기술이다[5]. 이런 XML 을 W3C 에서는 다양한 범주 별로 나누어 관련 기술들을 제정하고 있다. 현재 XML 은 거의 모든 분야에서 표준으로 자리잡아 XML 문서를 데이터의 저장 및 교환수단으로 사용하고 있지 않은 분야가 거의 없을 정도이다.

W3C 에서는 XML 에 대한 보안 기술 관련하여 XML 암호화(XML Encryption), 키 관리(XML Key Management), 전자서명(XML Signature)를 지정하여 그에 대한 표준화 작업을 진행하고 있다[6-8]. XML 에 대해서 정보의 기밀성을 제공하는 XML 암호화는 XML 화 된 문서의 일부 혹은 전부 또는 일반 리소스 정보를 암호화하기 위해 필요한 스키마 정보를 제공하여 암호화나 복호화를 유지할 수 있게 한다.

2.3 암호화 알고리즘

데이터에 대한 암호화를 위해서는 데이터를 암호화하기 위한 관련 암호화 알고리즘이 사용되어야 한다. 일반적으로 암호화 방식은 비밀키(secret key)방식인 대칭형 암호화 방식(symmetric cryptography) 과 공개키(public key) 방식인 비 대칭형(asymmetric cryptography)로 나누어 구분된다. 각각은 다음과 같은 특징과 장단점을 가진다.

[표 1] 암호화 방식 비교

대칭형 암호화 방식	비 대칭형 암호화 방식
● Key 교환이 별도로 이루어진다. ● 성능이 높다 ● 기밀성을 제공한다. ● 목적: Data Encryption	● Key 교환의 필요가 없다. ● 상대적으로 성능이 떨어진다. ● 전자서명이 가능하다. ● 목적: Key Exchange, Digital signature

위와 같은 특징을 가지는 암호화 방식에서 본 논문에서는 공간 데이터에 대한 서비스가 제공되면서 동시에 보안을 요구하기 때문에 성능적인 측면과 데이터에 대한 기밀성을 동시에 만족할 수 있는 대칭형 암호화 방식을 사용하고, 이에 대칭형 암호화 방식으로 구성된 한국정보보호진흥원(KISA) 의 SEED 를 사용하고자 한다[9-10].

- 한국의 KISA 와 관련 전문 그룹에서 만든 128bit symmetric 키 블록 암호화 방식이다.
- 128bit 의 input/output 데이터를 가지며 128bit 의 키 길이를 가진다.
- 16 round 를 가지는 feistel 구조를 가진다.
- 두 개의 8 X 8 S-Boxes 를 가진다.
- Exclusive OR 와 modular addition 의 혼합된 연산을 가진다

3. 공간 데이터 보안 구조 설계

3.1 공간 데이터 보안 구조

본 논문에서 제시하고자 하는 시스템의 구성은 [그림 1]과 같이 구성되어 운영이 될 수 있다. 시스템의 구성은 기존의 환경에 가능한 변경을 가하지 않고 운영이 되어야 한다. 일반적인 경우 클라이언트는 공간 서버에 데이터를 요청하고, 서버는 클라이언트의 요청 사항을 처리하여 클라이언트로 되돌려준다. 하지만, 암호화 모듈을 적용할 경우 공간 데이터가 구성 다음의 순서로 암호화 처리가 이루어지게 된다.

① 공간 데이터 암호화 모듈에 암호화를 요청 - 보안 메타 데이터를 구성하여 공간 데이터에 대한 암호화 처리
② 암호화된 데이터를 전달하여 클라이언트에 보낸다. 이때 보안 메타 데이터를 구성하여 같이 보낸다.
③ 보안 메타 데이터를 이용하여 암호화된 데이터를 복호화하여 클라이언트가 처리할 수 있는 원본 데이터를 구성한다.
④ 복호화 된 데이터를 클라이언트의 비즈니스 및 프레젠테이션 레벨로 전달하여 암호화를 끝낸다.

[그림 1] 시스템 구조

3.2 공간 데이터 보안 모듈 구성

공간 데이터에 대한 암호화/복호화 모듈을 SPEDM (Spatial Data Encode/Decode Module)로 부르기로 하겠다. 그리고 SPEDM 는 SPMETA, SPPRE, SPENCODE, SPDECODE, SPSEED 의 최상위 모듈을 가지고 그 하

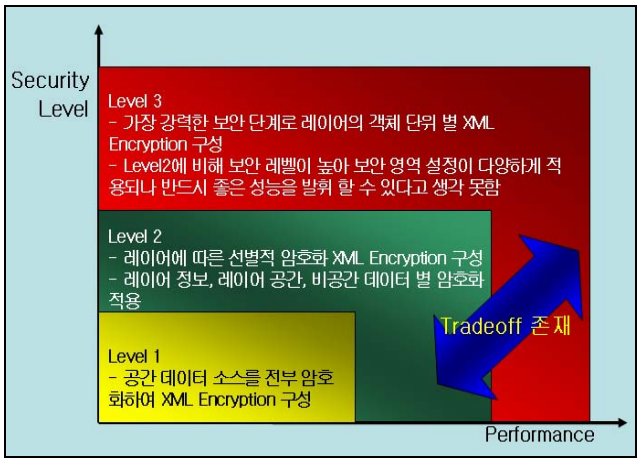
위에 세부적인 모듈로 구성된다.

[표 2] 보안 모듈구성

모듈	설명
SPMETA	공간 데이터를 구성하고 구성된 데이터를 보안 모듈을 적용하기 위해 공간 데이터에 대한 일반 정보 및 보안 정보를 구성하기 위해서 이용된다. 그리고 메타 정보를 이용하여 공간 데이터에 대한 암호화, 복호화에 이용하게 되는 것이다.
SPPRE	공간 데이터 제공 측에서 제공하는 공간 데이터를 표현하기 위한 것으로 기본적으로 바이너리 형태의 WKB, 텍스트, 이미지, GML(Geographic Markup Language) 문서 그리고 SPEDP 에서 제공하는 제 정의된 공간 데이터(POINT, LINE, POLYLINE, POLYGON, SHAPE etc)등이 있다.
SPENC SPDEC	SPMETA 와 SPPRE 를 통해 구성된 데이터를 XML 암호화 규약에 맞게 암호화하여 XML 을 생성한다. 또한, 다시 복호화 할 때 사용된다. 이때 암호화, 복호화는 관련 연구에서 제시한 SEED 알고리즘을 통해서 암호화, 복호화를 수행하게 된다.
SPSEED	SPENC 와 SPEND 의 내부에서 사용되는 SEED 암호화 알고리즘을 수행하기 위한 모듈이다.

3.3 공간 데이터 보안 레벨

공간 데이터는 일단 텍스트, 이미지, 음성, 동영상과는 전혀 다른 성격을 가진다. 그렇기 때문에 일반 보안 방식을 적용하여 암호화를 공간 데이터에 적용했을 경우 맞지 않게 된다. 그렇기 때문에 공간 데이터의 보안 레벨 설정은 공간 데이터의 특징 및 성능적인 측면에서 구성이 되어야 하는 것이다. 예를 들어 인터넷상에 보이는 지도를 생각해 볼 때 하나의 동을 보여줄 정도의 공간 데이터가 네트워크상으로 보내질 때 건물, 도로, 강, 지명 등의 다양한 레이어의 공간 데이터가 넘어가게 된다 이때 건물, 도로, 강, 지명과 같은 기본도 형태의 데이터는 보안을 위한 암호화가 이루질 필요는 없다. 하지만 개인의 위치가 표시되는 포인트 정보와 그에 대한 속성 텍스트 정보만이 보안을 위한 암호화가 이루어지면 될 것이다. 하지만, 군사상의 보안이나 보안 등급의 분류로 그 수위가 높을 시에는 암호화를 위한 성능적인 측면보다는 보안에 대한 측면이 더 강조 돼야 하기 때문에 공간 데이터의 전체 수준에서 보안을 위한 암호화가 이루어질 수도 있다. 이에 공간 데이터의 보안 레벨을 정의하고, 그 수준별 상황에 따라서 공간 데이터의 암호화가 이루어지도록 구성되어야 한다. 이런 보안 레벨에 대한 정의는 SPMETA 에 정의 되어 이루어지고 그 정보를 통해서 SPENC, SPDEC 에 의해 공간 데이터의 보안 암호화가 수행된다.



[그림 2] 보안 레벨 구분

3.4 공간 데이터 암호화 및 전송

공간 데이터의 암호화는 대칭형 암호화 방식인 SEED 에 의해서 이루어진다. SEED 는 비밀키 대칭형 방식으로 Data Encryption 에 주로 사용된다. 그렇기 때문에 공간 데이터 보안에 SEED 를 사용하고, 또한 비대칭형 방식에 비해 암호화 수준은 떨어지나 성능적인 측면에서 더 좋은 수행 속도를 제공한다. 즉 공간 데이터와 같이 대용량의 데이터를 암호화하는데 적합하다고 할 수 있다. 하지만, 비밀키 대칭형 방식에서는 상호 간의 암호화 키의 교환이 이루어져야 하는데 일반적으로 KDC(Key Distribution Center)를 통해서 이루어진다. 하지만, 여기서는 서버와 클라이언트 간의 상호 인증 과정에서 사용될 공개키를 바탕으로 공간 데이터 암호화를 위해서 사용될 개인키의 교환을 이루어지게 할 수 있다.

상호 간의 키에 대한 교환이 이루어지면 암호화 키, 공간 데이터, 그리고 보안 레벨이 구성된 메타 데이터를 이용하여 XML Encryption 문서를 생성하여 클라이언트로 보내게 된다. 그리고 클라이언트 측에서는 XML Encryption 문서와 메타 데이터를 전송 받아 원본 공간 데이터를 만들고, 그것을 데이터 비즈니스 혹은 프레젠테이션 레벨에서 활용하게 되는 것이다. 그 이후는 클라이언트의 데이터 처리 문제로 넘어가는 것이다.

4. 공간 데이터 보안 구현

공간 데이터 전송 보안의 구현은 시스템의 상호 운영성과 통합성, 그리고 플랫폼을 고려해서 구현이 되어야 한다. 또한, 성능도 그에 못지않게 중요한 요소가 되어야 할 것이다. 따라서 본 논문에서는 성능적인 측면을 고려한다면 C 언어로 구현을 해야겠지만 자바가 성능적으로 최근에 개선이 되었고, 자바의 상호 운

영과 통합성, 그리고 운영체제의 독립성을 고려해서 자바를 기반으로 구현을 하고자 한다.

실제 공간 데이터에 대한 암호화가 이루어지기 전의 XML 문서와 암호화를 통해 구성된 XML Encryption 문서는 다음과 같이 구성이 된다.

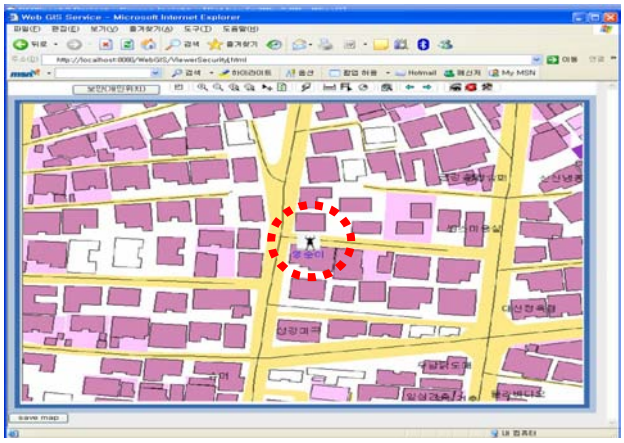
[예] 암호화가 이루어지기 전의 XML 문서(GML)

```
<?xml version="1.0" encoding="EUC-KR" ?>
<Exchange_file xmlns="http://www.w3.org/2000/10/XMLSchema"
    xmlns:gml=http://www.opengis.net/gml
    .....
    xsi:schemaLocation="dong_shcme.xsd"
    elementFormDefault="unqualified">
    ..........................
    <geoElement>
    <myLocation gml:id="myLocation-0">
    <point>
    <gml:point srsName="SRSNotUse">
    <gml:pos>194032,301321.0</gml:pos>
    </gml:point>
    </point>
    <locationID>740121-1834921</locationID>
    <personName>영희</personName>
    </myLocation>
    </geoElement>
....
```

[예] 암호화가 이루어진 후의 XML Encryption 문서 (Encrypted an XML Element)

```
..........................
    <geoElement>
    <myLocation gml:id="myLocation-0">
    <EncrypedData Type="…" xmlns="http://www.w3.org/2001/04/xmlenc
    #>
    <CipherData><CipherValue>
    DKJFOOODFNDKKEMSLEMFDSS
    </CipherValue></CipherData>
    </EncrypedData>
    <personName> 영희 </personName>
    </myLocation>
    </geoElement>
....
```

그리고 서버를 통해서 구성된 XML Encryption 문서는 클라이언트에서 보면 기존의 암호화가 적용되기 전과 동일한 화면 결과를 가질 수 있게 된다.



5. 결론 및 향후 발전 방향

본 논문에서는 공간 데이터를 콘텐츠 레벨에서 암호화를 이루어 제공하는 기법으로 공간 데이터 자체가 암호화되어 전송이 되기 때문에 보안 솔루션이 구성된 환경에서는 강력한 보안 수준을 제공하고, 별도의 보안 환경이 구축되지 않은 상황에서는 보안 상황을 제공한다. SPEDM 상에서는 가능한 공간 데이터 제공자의 공간 데이터를 그대로 수용하여 XML 문서를 구성하고, 다시 보안 레벨에 따라서 암호화를 이루기 때문에 기존 환경에 대한 부가적인 오버헤드 없이 인터페이스만 맞춰주면 될 것이다.

향후 본 논문의 발전 방향으로, 현재 시스템 모습은 보안 모듈을 적용하여 단지 보안이 이루어진 결과만을 제시하고 있다. 하지만 발전적으로 시스템이 활용되기 위해서는 다양한 인터페이스와 환경 그리고 성능적인 측면을 간과할 수 없기 때문에 보안 레벨의 다양화, 암호화 시간의 단축, 암호화 이전 XML 문서를 구성시의 성능 개선 등이 요구된다. 또한 새로운 메시지 전송 프로토콜로 부상하고 있는 SOAP(Simple Object Access Protocol)을 이용한 SOAP 의 보안 연계 [11], 그리고 XML Aware Networking[12]을 통한 더욱더 개선된 성능과 환경이 제시되어야 할 것이다.

참고문헌

[1]Harris b, Hunt R “TCP IP security threats and attack methods” Computer Communications V22, N.10, PP885-897, 1999.06

[2]Baltaus M. Lioy A. Maino F. Mazzocchi D, “Security issues in control, management and routing protocols,” The International Journal of Computer & Telecommunications Networking, V.34 N.6, PP.881~894 2000.12]

[3] 윤한성 정보 보안과 암호화-개념과 해설 21 세기사 2004 01 30 P18-19

[4] Open GIS Consortium http://www.opengeospatial.org/

[5] XML 1.0 Specification (Third Edition), http://www.w3.org/TR/REC-xml/ , W3C

[6] XML Encryption Requirements, http://www.w3.org/TR/xml-encryption-req/, W3C

[7] XML Encryption Syntax and Processing, http://www.w3.org/TR/xmlenc-core/ , W3C

[8] Decryption Transform for XML Signature http://www.w3.org/TR/xmlenc-decrypt/, W3C

[9] SEED 알고리즘 상세 명세서, http://www.kisa.or.kr/seed/data/Document_pdf/SEED_Specification_korean.pdf, 한국정보보호진흥원(KISA)

[10] SEED 개발 및 분석 보고서, http://www.kisa.or.kr/seed/data/Document_pdf/SEED_Self_Evaluation-Korean.pdf, 한국정보보호진흥원(KISA)

[11] SOAP Specification http://www.w3.org/TR/2003/REC-soap12-part1-20030624/

[12] Eugene Kuznetsov, XML Aware Networking XML as a family of new protocols, http://www.sys-con.com/xml/article.cfm?id=459