

위치기반서비스를 위한 보안정책에서의 시맨틱웹 활용

김종우*, 김창수*

*부경대학교 정보보호학과

Applying Semantic Web to Security Policy for Location Based Services

Jong-Woo Kim*, Chang-Soo Kim*

*Dept. of information security, Pukyong National University.

요약

위치기반서비스는 이동중인 사용자에게 위치와 관련된 정보의 제공을 중심으로 부가가치를 창출할 수 있는 정보를 제공하는 서비스로, 다양하고 방대한 분량의 데이터를 관리하기 때문에 분산환경에서 운용되는 것이 효율적이다. 본 논문에서는 위치기반서비스에서 이렇게 분산 저장된 리소스들에 대한 접근제어 정책을 공유하기 위해 시맨틱 웹 기술을 활용할 수 있는 방법을 제안한다. 이를 위하여 LBSPolicy 온톨로지를 정의하고 이를 기반으로 보안정책을 명세화할 수 있도록 하고, 이를 활용할 수 있는 서비스 구조를 제시한다.

I. 서론

위치기반서비스(LBS: Location Based Services)는 이동중인 사용자에게 위치와 관련된 정보의 제공을 중심으로 부가가치를 창출할 수 있는 정보를 제공하는 서비스로, 이동통신기술의 발달과 함께 최근 많은 연구 및 개발이 이루어지고 있다[6]. 이러한 위치기반서비스는 응급서비스, 자동차 항법 시스템, 관광안내 등과 같이 이동중인 사용자에게 위치에 기반한 다양한 정보를 제공함으로써 편리함을 제공할 수 있지만, 반대로 보안상의 위협도 내포하고 있다.

특히, 위치기반서비스에서는 고려되어지는 보안상의 문제는 다음과 같다. 첫째, 위치정보에 대한 불법적인 접근에 따른 프라이버시의 침해문제이다[6]. 이러한 문제는 리소스에 대한 접근제어를 통해 해결할 수 있는데, 특히 LBS에서는 다수의 사용자와 수많은 형태의 리소스를 대상으로 하기 때문에 다양한 보안정책을

표현할 수 있는 방법이 필요하다. 이러한 리소스에 대한 접근제어는 위치기반서비스의 유료 서비스를 위해서도 요구되어진다. 둘째, 보안정책의 상호운용성 문제이다[6]. 즉, 서로 다른 운용환경간의 로밍에서 보안정책을 공유할 수 있는 방법이 필요하다.

본 논문에서는 이러한 문제들을 해결하기 위해서 보안정책을 의미적으로 표현하고 공유할 수 있도록 시맨틱웹 기술을 도입하고자 한다. 시맨틱 웹(Semantic Web)[1]은 웹상의 정보에 의미를 부여함으로써 컴퓨터가 웹상의 자원(resource)에 대한 의미를 분석하고, 유사한 의미를 연관 지어 의미기반으로 정보를 처리하고 그 결과를 사용자에게 제공할 수 있는 기술이다.

본 논문의 2장에서는 시맨틱웹의 개념과 기술에 대해 기술한다. 3장에서는 이러한 시맨틱 웹 기술을 위치기반서비스의 리소스에 대한 접근제어에 활용하는 방안에 대해 기술하고, 4장

에서는 표현하는 방법에 대해 기술한다. 마지막으로 5장에서는 결론을 기술한다.

II. 시맨틱 웹

기존의 웹 환경에서는 정보의 검색을 위해 주로 AltaVista, Yahoo, Goole 등의 검색엔진과 같이 Keyword 기반의 검색을 사용한다. 이러한 Keyword 기반의 검색엔진에서의 정보검색은 사용자의 많은 시간 과 노력이 요구된다.

이러한 Keyword 기반의 검색의 문제점을 해결하고 검색의 정확성과 효율성을 향상시킬 수 있는 방법으로, 최근 시맨틱 웹 기술 및 그 응용에 대한 많은 연구가 이루어지고 있다. 최근에는 교육분야의 E-Learning, 의학분야, 건축분야 등에서 웹상의 산재되어 있는 전문지식들이 공유되고 통합될 수 있도록 많은 시맨틱 웹 응용 연구들이 진행되고 있다.

이러한 시맨틱 웹 기술들은 계층(Layer cake)화된 형태로 기술요소들을 구성하고 이들의 역할에 따라 연구 및 개발이 이루어지는 방법으로 접근하고 있다. 시맨틱 웹은 Unicode와 URI layer를 기반으로 한다. URI는 기존의 식별자 URL이 가진 단점을 보완하여 웹 자원의 연계 관리를 안정된 구조로 제공하는 불변의 고유 식별자로 활용되고 있다. 이 URI로 식별되는 이름들의 집합체 XML Namespace에서는 XML element types나 attribute names의 식별에 사용되며 출처 즉 정의 기관이 상이한 요소명 또는 속성명들 사이의 잠재적 충돌가능성을 방지할 목적으로 제정되었다.

그 상위에는 XML+XMLSchema 레이어로서 이는 XML의 기술이 사용자가 정의하는 태그(tag)를 사용하여 웹 문서에 구조화를 제공할 수 있는 개념이 제공되는 계층이 된다[9]. 그리고 XML+XMLSchema 레이어의 상위계층인 RDF+RDFSchema layer, Ontology layer를 통한 개념화된 명세서를 제시하며, Logic layer를 통한 속성의 제어, Proof layer를 통한 Logic의 Proof, 그리고 Proof를 신뢰할 수 있는지에 대한 Trust layer로써 제시되고 있다[2]. 특히, RDF와 Ontology는 시맨틱 웹에서의 핵심적인

역할을 한다.

RDF(Resource Description Framework)[4]는 웹상의 자원들간의 관계를 정의하기 위해 Subject, Predicate, Object 개념을 이용한 triple 구조로써 웹문서의 정보를 표현한다. 이렇게 표현된 정보는 컴퓨터에서 의미를 분석하고 처리 가능 하도록 하기위해 속성(properties)과 클래스(classes)의 명확한 정의와 클래스간의 관계, 속성간의 관계를 규정하고 있다.

웹 콘텐츠에 표현된 정보들의 의미부여하기 위해 URI로 인식되어 지는 자원들의 관계에서 의미를 부여하는데 많은 표현력을 지닌 온톨로지(Ontology)가 있다. 온톨로지는 의미를 표현하는 vocabulary가 강력하지만 많은 정보자원들을 연관시키기 위해서는 분산형으로 개발되어 한 파일이나 영역에 국한되지 않고 확장가능하고 정보간의 공유가 가능해야 한다.[9]

W3C에서 주도적으로 온톨로지 언어를 표준화하고 있으며 RDF/RDFS에서 제공되는 계층적인 관계를 확장하고 강화시키는 추세로 발전되어지고 있다. OWL(Web Ontology Language)[5][7]은 W3C에서 발표한 온톨로지의 공유와 출판을 위한 Semantic Markup Language로 사용하고 있다.

III. 제안 방법

위치기반서비스는 다양하고 대량의 정보를 관리해야 하기 때문에 분산화된 시스템을 기반으로 하는 것이 효율적이다. 이렇게 분산 저장된 리소스에 대한 접근제어를 위해서는 접근 제어 정책의 공유가 요구된다. 본 논문에서는 이러한 접근제어 정책을 의미적으로 공유하기 위해서 시맨틱 웹 기술을 활용하는 방안을 제안한다.

3.1 LBS 보안정책의 명세화

본 논문에서는 분산환경의 위치기반서비스 플랫폼에서 리소스에 대한 접근제어 정책을 명세화하기 위해 LBSPolicy 온톨로지를 사용한다. LBSPolicy 온톨로지는 RDF/XML 기반의

Policy 기술 언어인 Rei[2]를 사용하여 정의한다.

LBSPolicy는 다양한 조건의 접근제어 정책을 기술하기 위한 OWL-Lite기반의 온톨로지이다. LBSPolicy 온톨로지는 그림 1과 같이 Policy, Granting, Permission, Prohibition, Constraint 클래스로 구성되어진다. 그림은 LBSPolicy 온톨로지의 OWL 표현의 일부를 나타낸 것이다.

```
<owl:Class rdf:ID="Policy"/>
<owl:Class rdf:ID="Constraint"/>
<owl:Class rdf:ID="Prohibition">
  <rdfs:subClassOf>
    <owl:Class rdf:ID="Granting"/>
  </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:ID="Permission">
  <rdfs:subClassOf rdf:resource="#Granting"/>
</owl:Class>
<owl:ObjectProperty rdf:ID="grants">
  <rdfs:range rdf:resource="#Granting"/>
  <rdfs:domain rdf:resource="#Policy"/>
</owl:ObjectProperty>
```

그림 1. LBSPolicy 온톨로지의 일부

Policy 클래스는 접근하고자하는 리소스에 대한 보안정책들의 리스트를 정의하기 위해 사용되어진다. Policy 클래스는 grants 속성을 통해 실제 접근제어에 대한 정책을 명세화하는 Granting 클래스의 인스턴스를 연관시킨다. 아래의 예제는 ResourceA에 대한 접근제어 정책을 정의한 예로서, Perm_AccessResourceA와 Proh_AccessResourceA라는 두개의 접근제어 정책을 RDF로 명세화하고 있는 예이다.

```
<policy:Policy rdf:ID="ResourceAPolicy">
  <policy:grants rdf:resource=
    "#Perm_AccessResourceA"/>
  <policy:grants rdf:resource=
    "#Proh_AccessResourceA"/>
</policy:Policy>
```

실제 접근제어에 대한 보안정책은 Granting 클래스에 의해 명세화 되어진다. Granting 클래스는 Permission 클래스와 Prohibition 클래스를 하위 클래스로 가지며, 실제 접근제어에 대한

명세는 이들 하위 클래스에 의해 정의되어진다. 다음은 ResourceA에 대해 접근을 허용하는 정책을 명세화하는 Permission 인스턴스의 예이다. Permission 클래스는 아래 예제와 같이 actor, target, constraint 속성을 가지는데, actor는 리소스에 접근할 수 있는 사용자의 리스트를 명세화하고, target은 접근하고자 하는 리소스를 명세화한다. target 속성은 리소스에 접근하기 위한 URI를 객체로 가지게 되는데, 접근이 허용되는 경우에만 이 URI 정보를 반환하게 된다. Constraint 클래스를 사용하여 접근이 허용되는 사용자에 대한 제약조건을 명세화할 수 있으며, 이러한 Constraint 클래스의 인스턴스를 지정하기 위해 constraint 속성을 사용할 수 있다.

```
<policy:Permission rdf:ID=
  Perm_AccessResourceA">
  <granting:actor rdf:resource=
    "&subscriberlist"/>
  <granting:target rdf:resource=
    "&lbsResourceA"/>
  <granting:constraint rdf:resource=
    "#IsRegisterGroupA"/>
</policy:Permission>
```

Constraint 클래스는 특정 리소스에 접근하는 사용자를 보다 정확하게 명세화하기 위해 제약조건을 지정할 수 있도록 한다. 다음은 Constraint 클래스의 하나의 인스턴스를 나타낸 예시로, 사용자 리스트 중에 소속이 GroupA인 사용자만을 지정하는 예이다.

```
<constraint:SimpleConstraint rdf:ID=
  "IsRegisterGroupA">
  <constraint:subject rdf:resource=
    "#VarPerson"/>
  <constraint:predicate rdf:resource=
    "&subscriberlist;affiliation"/>
  <constraint:object rdf:resource=
    "&grouplist;GroupA"/>
</constraint:SimpleConstraint>
```

상기한 예에서 Granting 클래스나 Constraint 클래스의 인스턴스를 통해 명세화된 접근제어 정책이나 조건들은 다른 리소스에 대한 접근제어 정책을 표현하기 위해 재사용되어 질 수도 있다.

3.2 활용방안

그림 2는 분산 환경의 위치기반서비스의 일반적인 서비스 구조를 나타낸다. 위치기반서비스를 제공하기 위한 리소스들은 분산되어 저장되고, LBS Middleware에서는 이들 리소스들로부터 사용자가 요구하는 정보를 제공하는 기본적인 서비스들을 API로 제공한다. LBS Application 개발자들은 LBS Middleware에서 제공하는 API를 이용하여 다양한 위치기반 응용서비스를 개발하게 된다.

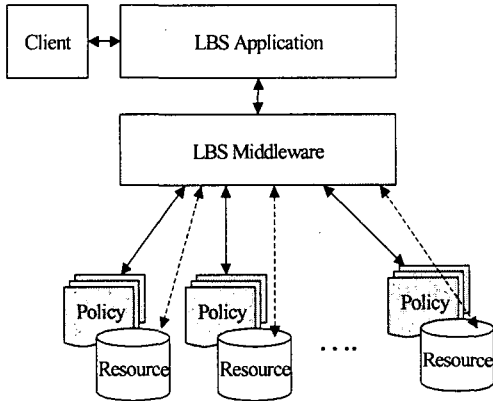


그림 2. 제안방법 활용을 위한 서비스 구조

LBS Middleware에서 리소스로 접근하는 방법은 다양하게 있을 수 있지만, 본 논문에서는 리소스에 접근하기 위해 URI를 사용하는 것으로 가정한다. 이때 LBS Middleware는 실제 리소스에 대한 URI가 아닌 해당 리소스의 Policy에 대한 URI를 저장하고, 리소스에 접근하기 전에 Policy 명세를 통해 서비스를 요청한 사용자의 접근 허용 여부를 판단하게 된다. 이때, 접근이 허용되면 3.1에서 기술한 바와 같이 해당 리소스에 대한 실제 URI를 반환하여 LBS Middleware가 실제 리소스의 정보에 접근할 수 있도록 한다.

IV. 결론

본 논문에서는 위치기반서비스에서 분산 저장된 리소스들에 대한 접근제어 정책을 공유하기 위해 시맨틱 웹 기술을 활용할 수 있는 방법을 제안하였다. 이를 위하여 LBSPolicy 온톨로지를 정의하고 이를 기반으로 보안정책을 명세화할 수 있도록 하였고, 이를 활용할 수 있는 서비스 구조를 제시하였다.

[참고문헌]

- [1] Berners-Lee, T., Hendler, J. and Lassila, O. "The Semantic Web", Scientific American, 2001.
- [2] L. Kagal, "Rei: A Policy Language for the Me-Centric Project" HPL-2002-270, Hewlett-Packard Company, 2002.
- [3] M. Lee, J. Kim, S. Park, J. Lee, S. Lee, "A Secure Web Services for Location Based Services in Wireless Networks", NETWORKING 2004, LNCS, No.3042, 2004.
- [4] Frank Manola, Eric Miller, "RDF Primer", <http://www.w3.org/TR/2004/REC-rdf-primer-20040210/>
- [5] Smith, M., D. McGuinness, R. Voiz, and C. Welty, "Web Ontology Language(OWL) Guide Version 1.0", <http://www.w3.org/TR/owl-guide/>, 2002.
- [6] Shioyang Wu, Kun-Ta Wu, "Dynamic Data Management for Location Based Services in Mobile Environments", Proc. 2003 Int. Conf. Database Engineering and Applications Symposium. IEEE, 2003.
- [7] 오삼균, "Web Ontology Language와 그 활용에 관한 고찰", 데이터베이스 연구, 18권 3호, 2002.9.