자동차 상태정보 관리를 위한 SOAP기반 보안 메시지 정보 전송

강무삼, 문영준, 강진혁, 이지성, 송왕철
제주대학교 컴퓨터공학과
e-mail: kangm3@hanmir.com, {juntheater, jinhyeok.kang}@gmail.com,
{eternal9697, kingiron}@gmail.com

SOAP based security message for managing status of Electric Vehicles

Moo-Sam Kang, Young-Jun Moon, Jin-Hyeok Kang, Jee-Sung Lee,
Wang-Cheol Song
Dept of Computer Engineering, Jeju National University

요 약

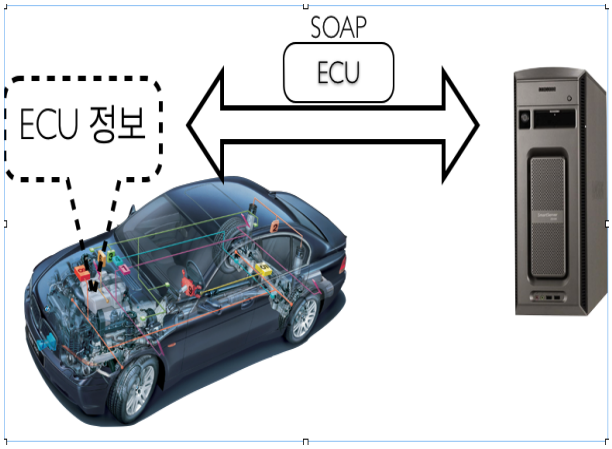
본 논문은 자동차에 대한 데이터의 보안성을 위한 시스템을 위한 것으로, 자동차의 데이터를 실시간으로 읽어드려, 이를 인터넷 상에 위치한 Web 서비스를 통하여 DB에 SOAP를 이용하여 서버에 저장하는 시스템이다. 통합된 시스템이 만들어지면, 현재 자동차의 상태정보를 읽어드려, 자동차의 상황정보를 보안이 강화된 통신을 통해 사용자에게 신뢰성이 높은 정보를 안전하게 제공할 수 있을 것이다.

1. 서론

최근의 자동차에는 ECU(Engine/Electronic Control Unit)이라는 장치에서 자동차의 각종 센서를 통해 얻은 데이터를 중심으로 운전자에게 많은 정보를 주고 있다. 이 정보는 운전하는데 보조 역할을 하고 있다.[1] 각종 센서에서 얻은 ECU의 정보를 바탕으로 하여 웹상에서 자동차에서 제공받은 ECU의 정보를 이용하여 운전자에게 다양한 정보를 받을 수가 있다. 하지만 차량에서 나오는 정보는 운전자의 운전경향에 대한 데이터, 운전경로, 사적인 데이터까지 보안처리가 고려되어야 만 한다. 웹상에서 자동차 ECU 정보를 공유하기 위해서는 보안 프로토콜을 기반으로 하여 정보를 공유를 해야 운전자에게 신뢰성이 높은 정보를 제공할 수 있다.

본 논문은 그림 1의 구상도에서와 같이 자동차 정보의 웹기반 서비스로의 전송을 SOAP 프로토콜[2]를 이용하여, 데이터를 송수신할 때 보안체계를 적용하는 것이다. SOAP 특성상, HTTP를 이용하여 인터넷상에 설치되어 있는 방화벽에 많은 제약을 해결하였다. 보안체계를 위한 WS-Security[3]라는 기술은 사용자 및 자동차 정보에 대한 보안성, 사용자 자동차에 대한 인증, 권한 부여, 무결성, 서비스거부 방지 등의 보안 처리를 특징으로 한다.

이를 위해 자동차로부터 현재 상태에 대한 정보를 ECU로부터 추출해낸다. 이를 XML형태의 데이터로 변환하고 SOAP 기반의 프로토콜을 이용하여 자동차 데이터 전송 및 저장을 하게 된다.



(그림 1) 전체 구상도

본 논문의 구성은 2장에서 관련연구를 살펴보고, 3장에서 SOAP 프로토콜 구현에 대한 부분을 기술 하였고, 4장에서 결론을 맺는다.

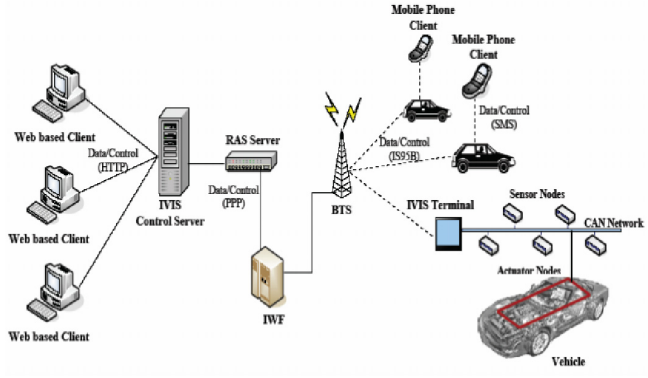
2. 관련 연구

2.1 웹기반 차량 정보 시스템

'웹기반 차량 원격 진단 및 관리를 위한 지능형 차량정보시스템 설계'[4]는 그림 2와 같이 CDMA 이동통신망을 이용하는 웹기반 차량용 무선원격제어 및 진단 시스템을 위한 지능형 차량정보시스템 이다. 개발한 '웹기반 지능형 차량 정보시스템'은 차량 내 지능형 정보단말과 인터넷 상의 서버-클라이언트 기반(Sever- Client Based)의 시스템

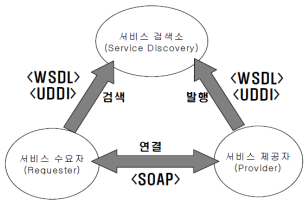
들이 상호 연동하는 시스템이다. 웹기반 제어(Web-Based Control)를 통해 언제 어디서든 웹브라우저(Web Browser)를 통하여 차량의 제어와 진단이 가능하며, 사용자는 차량 내에서 지능형 차량정보단말(Intelligent Vehicle Information Terminal, IVIT)을 이용하여 차량 진단 및 관리와 관련된 서비스를 외부 네트워크로부터 제공 받을 수 있다. 또한 CDMA 이동통신망을 기반으로 하므로 제어 조작자(Operator)와 차량 간의 이동성을 제공한다. 뿐만 아니라 인터넷 상의 차량제어서버를 이용하여 차량 진단을 위한 과거 차량 상태 내역 (Vehicle State History)을 제공해 줄 수 있기 때문에 보다 효과적인 차량 원격진단과 관리가 가능한 장점을 가진다.

본 논문은 차량 제어 정보, 차량 상태 정보 등의 중요한 정보를 보다 안전하게 전송하려고 한다.

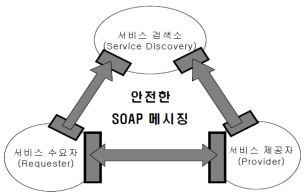


(그림 2) 지능형 차량 정보시스템의 아키텍처

2.2 SOAP(Simple Object Access Protocol)보안



(그림3)웹 서비스 개요도



(그림4)SOAP메시지 보안

'안전한 웹 서비스를 위한 SOAP 메시지 보안기술 연구'[5]라는 논문에서는 SOAP 보안을 중점적으로 설명하고 있다.

웹 서비스는 플랫폼 독립적으로 인터넷과 같은 네트워크를 통해 시스템간 연계, 통합과 자원 공유를 가능하게 하는 표준화된 XML(eXtensible Markup Language) 기반의 웹 기술을 사용할 수 있다. 이러한 웹 서비스 아키텍처는 서비스를 제공하는 서비스 제공자(Provider)와 서비스를 필요로 하는 서비스 수요자(Requester), 이들 사이를 중개하는 서비스 검색소(Discovery Service)로 구성된다. 그리고 이들 사이에서는 서비스를 발행(publish)하고, 이를 검색(find)하고 나서 제공자와 수요자 사이의 서비스에 대한 연결(interact)이라는 기본적인 세 가지 기능이 있다. 그림3에서와 같이 웹 서비스는 기본적으로 WSDL(Web Service Definition Language), UDDI(Universal Discovery and Integration of Business for Web), SOAP로 구성된다. WSDL은 웹 서비스 호출에 대한 인터페이스, 의미론(Semantics) 등을 기술하고 있는 XML 문서이고, UDDI는 서비스 탐색 및 게시를 위한 공개된 디렉토리이며, SOAP는 HTTP, SMTP 등과 같은 저수준 프로토콜을 통해 웹 서비스 상의 각 객체간 통신프로토콜이다.

웹서비스 특성상 서비스 구성원이 여러 네트워크에 분산되고 외부에서 접근이 쉽기 때문에 보안은 매우 중요하다. 그림4에서와 같이 서비스 수요자, 제공자, 검색소 객체간에는 어떤 환경에 있든지 간에 서로 데이터를 자유롭게 주고받을 수 있으며 어떤 애플리케이션이라도 서로 호출하여 사용할 수 있도록 되어 있기 때문에, 데이터 교환을 담당하는 통신 프로토콜인 SOAP의 보안은 무엇보다 중요하다.

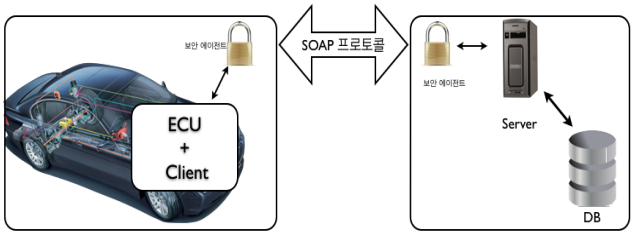
본 논문에서는 SOAP을 이용해서 구체적인 보안을 위한 메커니즘을 설계하고 있다.

2.3 임베디드 시스템을 이용한 자동차 감시

'(Controller Area Network)CAN 통신과 임베디드 시스템을 이용한 자동차 감시 시스템 구현'[6] 논문에서는 CAN 통신을 활용하여 자동차의 분산 제어를 위한 전자제어장치를 구성하고, 이를 관리하고 감시 할 수 있게 하였다. 메인 제어기에 임베디드 리눅스를 설치해 웹서버를 구현 하여 자동차 분산 제어 시스템을 무선 랜으로 인터넷을 통해 웹이나 PDA, 휴대폰과 같은 모바일 기기로 감시할 수 있는 시스템을 구현 하였다.

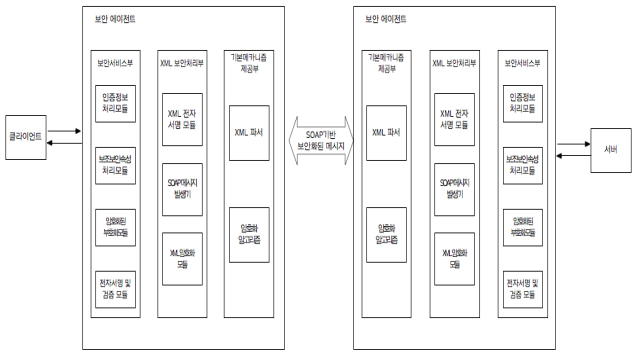
본 논문의 구현에서는 server를 외부에 배치해 외부적인 충격이나 온도와 같은 환경적인 영향을 덜 받게 구성 하였다. 필요시 데이터를 단순히 보여주는 기능 뿐 만 아니라 유용한 형태의 정보를 만들 수 있는 확장이 가능하다.

3. 설계



(그림 5) 전체적인 설계

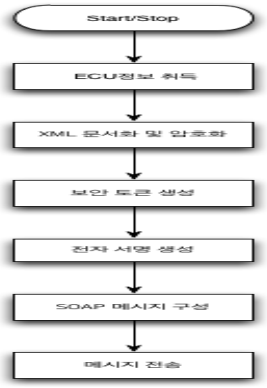
본 논문에서는 자동차에서 실시간으로 데이터를 읽어 데이터를 SOAP를 이용하여 DB에 저장하도록 그림 5와 같이 설계하였다.



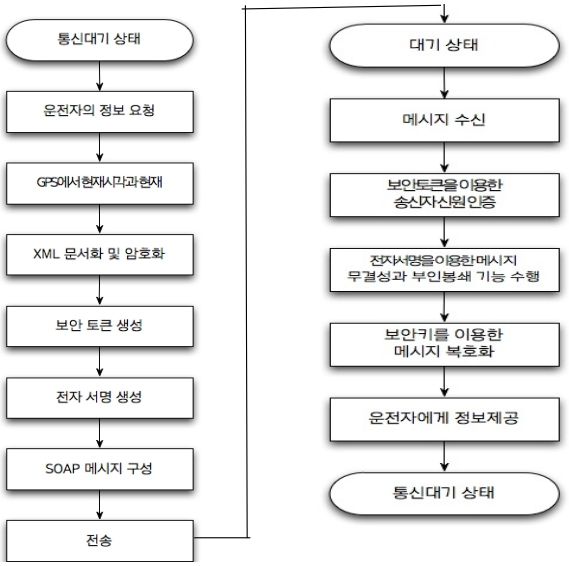
(그림6)보안에이전트의 구성

보안 에이전트는 그림 6과 같이 자동차의 클라이언트와 서버 측에서 각각 같은 기능을 가지고 위치하며, 보안 서비스부, XML 보안처리부, 기본 메카니즘 제공부로 구성되다. 보안서비스부는 인증 정보 처리 모듈과 보조 보안 속성 처리모듈, 암호 및 복호화 처리모듈, 전자서명 및 검증 모듈이 있다. 인증 정보 처리 모듈은 보안 토큰을 이용하여 메시지 전송자의 인증을 담당한다. 보조 보안 속성 처리모듈은 응답 공격이나 중간자 공격등을 방지하기 위한 목적으로 타임스탬프나 임의값 관리등의 처리를 한다. 보안 서비스 부에서 발생된 보안 메시지를 SOAP 프로토콜에 맞춰 보안토큰, 전자서명, 암호키를 헤더에 넣고, 암호화된 메시지를 몸체에 넣어 SOAP메시지 발생기로부터 메시지를 만든다. 보안 처리부에서는 SOAP 기반 보안처리가 기본적으로 XML 암호화 기법을 사용하므로 XML 전자서명 모듈과 XML 암호화 모듈을 갖고 있다. 기본 메카니즘제공부는 XML 파서 모듈과 암호 알고리즘 모듈로 이루어 진다. XML 파서 모듈은 클라이언트와 서버간에 주고 받는 메시지인 XML메시지를 만든다. 암호 알고리즘 모듈에서는 SOAP 메시지 발생기에서 만들어 낸 암호화된 메시지를 만드는 방법과 보안을 위한 다양한 암호화 기능들을 제공한다.

그림 7은 SOAP 메시지 전송 흐름도이다. 차량의 센서로부터 얻은 ECU 정보를 XML 형식으로 만들고 XML 수준의 암호화를 한다. 보안토큰을 생성하고 전자 서명을 생성해서 SOAP 메시지를 구성하여 전송하게 된다.



(그림 7) SOAP 메시지 전송 흐름도



(그림8)전기자동차의 최적 전기충전소 검색

그림 8은 전기동차의 최적 전기충전소 검색을 위한 흐름도이다. 그림 7과 같이 클라이언트에서 SOAP 메시지를 만들어서 전송하면 서버측에서는 메시지를 수신해서 보안토큰을 이용한 송신자 신원 인증을 한다. 인증 후에 전자서명을 이용한 메시지 무결성과 부인봉쇄 기능을 수행하게 된다. 마지막으로 보안키를 이용해서 메시지를 복호화 해서 얻은 정보를 운전자에게 제공하게 된다. 이 때 얻는 정보는 서버 측에 축척된 정보를 바탕으로 최적의 전기충전소를 검색해서 얻는 정보일 수도 있다.

4. 구현

ECU에서 취득한 데이터를 클라이언트가 XML 문서화 한다. C++로 프로그램밍 할 경우에는 소켓 통신을 하게 된다. 소켓을 생성해서 그림9에서와 같이 POST, Content-Length, Host, Content-Type, SOAPAction 등 HTTP Header와 그림 10에서와 같이 SOAP 메시지를 String형태로 저장해서 전송하면 된다. 이렇게 구성된 메시지는 통신채널을 통해 서버 쪽에 전송을 하게 된다. 그림 11은 SOAP Client 실행결과를 'wireshark'라는 네트워크 분석 툴로 네트워크에서 흐르는 패킷을 잡아서 보여주고 있다.

```
POST /axis/services/CarInformationService HTTP/1.0
Content-Length: 799
Host: 117.17.102.35:8080
Content-Type: text/xml; charset=utf-8
SOAPAction: ""
```

(그림 9) HTTP Header

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/so
   <SOAP-ENV:Body>
      <ns1:insertCarInformation xmlns:ns1="CarInformationService">
         <presentTime xsi:type="xsd:string">20110325182553</presentTime>
         <battery xsi:type="xsd:float">219</battery>
         <hearter xsi:type="xsd:int">1</hearter>
         <xLocation xsi:type="xsd:float">0</xLocation>
         <yLocation xsi:type="xsd:float">0</yLocation>
      </ns1:insertCarInformation>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

(그림 10) SOAP Message

(그림 11) SOAP Client 실행 결과

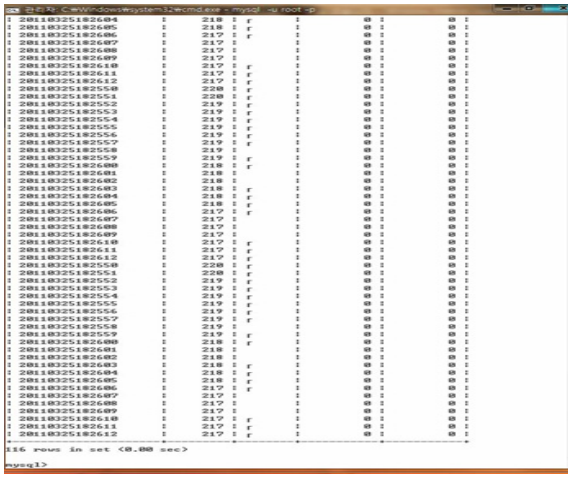
서버 측에서는 표1을 설치한다. SOAP메시지를 Class형태로 만들고 윈도우의 cmd 콘솔창을 이용하여 그림 12와 같은 WSDL을 생성하게 된다.

설치 프로그램	tomcat	axis	mySQL
설치 버전	jakarta-tomcat-4.0.4	xml-axis-beta1	최신버전

<표 1> 설치프로그램과 그에 따른 버전

(그림 12) WSDL

클라이언트에서 SOAP메시지를 보내면 그림 13과 같이 서버 측 데이터 베이스에 저장 된다.



(그림 13) Server 결과

5.결론

가까운 미래에는 어떤 환경에서 어떤 매체를 이용하든지 통신만 할 수 있게 된다면 차량의 정보를 실시간으로 얻을 수 있고 이를 바탕으로 좀 더 유용한 정보를 만들어 내어 인간의 실생활에 유익하게 쓰일 것으로 보인다.

본 논문에서는 안전한 통신을 위해 SOAP를 이용한 메시지 설계하였고 client/server 형태로 구현해 보았다. soap 메시지 생성시 보안에 관련된 사항은 설계로만 남아있고 구현은 하지 못한 상황이다. 실제 구현을 위해 자료를 찾아봐야 하겠다.

참고문헌

[1] 박현석,구본웅,엄태홍,회후락,최창율.“하이브리드 전기자동차의 BMS ECU 개발 및 모니터링”, 한국자동차공학회 2005년 심포지움(전기·전자, ITS 부문), 2005.8, page(s): 3-156
http://www.dbpia.co.kr/view/ar_view.asp?arid=816677

[2] http://www.w3.org/TR/soap/

[3] http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

[4] 김태환,최용운,이승일,홍춘기,이용두.“웹기반 차량 원격 진단 및 관리를 위한 지능형 차량정보시스템의 설계”, 한국정보과학회 2005 가을 학술발표 문집(Ⅰ)제32 제2호, 2005.11, page(s): 1-1093
http://www.dbpia.co.kr/view/ar_view.asp?arid=949930

[5] 박배효,이재일.“안전한 웹 서비스를 위한 SOAP 메시지 보안기술 연구”, 情報保護學會誌 第14卷 第4號, 2004.8, page(s): 1-116
http://www.dbpia.co.kr/view/ar_view.asp?arid=897962

[6] 양승현,이석원.“Controller Area Network(CAN 통신과 임베디드 시스템을 이용한 자동차 감시 시스템 구현”, 대한전기학회 제36회 하계학술대회 논문집, 2005.7, page(s): 2471-3244
http://www.dbpia.co.kr/view/ar_view.asp?arid=1344091