基于 Web 服务的交通数据交换过程①

尚龙华[1], 安毅生[1], 张绍阳[1], 唐 菁[2]

[1](长安大学 信息工程学院, 西安 710064)
[2](中交水运规划设计院有限公司, 北京 100007)

摘 要: 针对国内交通信息化快速发展过程中普遍存在的“信息孤岛”以及网络传输中数据的安全性、身份验证等问题, 提出了一种基于 Web 服务的数据交换方法, 该方法由格式化的交换数据包及服务接口调用过程组成, 交换数据包实现了交换数据的规范化, 服务接口调用过程则实现了数据交换过程的规范化. 以《船舶基础信息采集交换接口规范》中的数据交换为例, 给出了 xml 格式的数据包和 Web 服务接口, 实践表明该方法能够改进交通行业信息系统中数据交换模型与业务逻辑关联性弱的不足, 同时也提高了数据交换安全性.

关键词: 交通数据共享; 数据交换; Web 服务; XML 数字签名; XML 加密

Traffic Data Exchange Process Based on Web Service

SHANG Long-Hua[1], AN Yi-Sheng[1], ZHANG Shao-Yang[1], TANG Jing[2]

[1](School of Information Engineering, Chang’an University, Xi’an 710064, China)
[2](CCCC Water Transportation Consultants Co. Ltd, Beijing 100007, China)

Abstract: Aiming at the prevalent problem, information silos, in the transportation information system, as well as data security, authentication in network data transmission and other issues, a generic Web Service-based traffic data exchange method is proposed, which consists of formatted data exchange packet and service interface invocation. Among the method proposed, the data exchange packet is to standardize data, while the service interface invocation is to achieve data exchange process standardization. With the help of the example of data exchange in “Vessel based information collection and exchange interface specification”, which gives xml format packet and the Web service interface, it shows that the proposed method can not only improve the inadequate of data exchange method and business logic associated with weak in the information system of transportation industry, but also improve the security of data exchange.

Key words: traffic data sharing; data exchange; generic method; web service; XML signature; XML encryption

随着信息技术的进步和交通管理部门的应用需求, 相关部门建立了多种交通信息化系统. 但是这些系统大多沿用独立建设、功能单一的模式进行, 缺乏顶层设计, 虽然多种信息系统并存, 但是大多以“信息孤岛”的形式存在, 不能够满足智能交通系统发展的要求. 因此, 深入研究交通数据共享与交换机制以促进交通信息资源的共享, 拓展应用范围, 实现各业务系统的协同就成为交通信息化领域的重要挑战.

对于数据源和数据交换流程相对固定、数据量较大且数据交换周期性较强的应用场合, 汪祖云提出了多层结构的交通数据中心架构, 并对 4 种不同类型的数据交换需求进行了分析[1]; 韩海航等利用 ETL 技术实现了分布式异源数据的抽取、访问及数据同步复制[2]; 康红霞等利用 XML 对交通数据进行封装, 实现了异构数据异构系统间的交换[3]; 廖军、葛迪等结合陕西省和黑龙江省公路交通信息资源整合工程的实践, 提出了基于 ETL 的数据共享与交换机制, 实现了业务数据库和基础数据库中的数据抽取、转换、以及主题数据库中的数据加载功能[4,5]. 文献[6-8]提出了以面向服务体系结构(SOA)为框架, 采用松散耦合方式构建数据共

① 基金项目:交通运输部科技项目(2012364223500)
收稿时间:2014-07-07;收到修改稿时间:2014-08-18

享平台; 吕斌等利用 Web Service 技术给出了交通异构数据共享系统的信息集成方案, 并对其中的服务定位、服务发现及服务匹配策略等关键问题进行说明[9]; 文献[10]归纳了 Web 服务中存在的主要安全问题, 并分析了代表性的 Web 服务安全技术解决方案; 文献[11]采用目前 Web 服务中的主要安全技术来优化 Web 服务架构, 实现消息传递的机密性、完整性和不可否认性; 文献[12]则提出基于 XML 安全模型和 AJAX 异步传输技术的 Web Services 组件模型, 进而实现异构数据系统的整合.

交通行业中基于 ETL 和 Web Service 的数据共享与交换方法尽管能够解决交通行业信息系统中普遍存在的分布性与异构问题, 但也存在不足[3,6,7,9-11]:

(1)数据共享与交换模型与业务逻辑的关联性较差, 无法适应业务流程频繁变更的需求;

(2)服务接口无有效保护, 由于具体的调用参数是公开的, 因此容易被非法利用;

(3)对数据交换的过程缺乏有效的保护, 在开放的互联网环境中, 数据很容易被非法截获、窃取或者篡改等.

鉴于此, 本文将跨平台数据组织形式及数据交换交互过程保护作为切入点, 依据对交通行业使用的大量数据共享与交换规范的分析, 抽取规范中共性的交换规则, 针对交通数据交换过程进行研究, 提出了一种基于 Web Service 的交通数据交换方法(以下简称推荐数据交换方法).

其中, 采用交通行业中普遍采用的 XML 技术作为跨平台数据组织问题的解决方案, 并给出了具体的数据包组织规则; 而针对实时数据交换则采用 Web 服务结合 XML 签名加密技术, 从而有效解决实时交互过程中的数据保护问题. 相比于投资成本较高, 设计较为复杂的 ETL 数据交换解决方案, 本文实现了一种轻量级的交通数据交换解决方案, 同时有效保护了 Web 服务接口的调用及交互过程中的敏感数据.

1 交换数据包

XML 作为一种可扩展标记语言, 设计之初便是应对数据传输的需要, 同时其优越的平台无关性使得其可以独立于具体的应用程序被使用. 目前交通行业也多数采用 XML 技术解决跨平台数据组织问题, 本文依托已有的研究, 依然采用 XML 技术作为跨平台数据组织问题的解决方案, 同时给出交换数据的结构化表示方案(下面称为交换数据包).

为了区分交换数据的格式与信息实体, 我们把交换数据包定义为数据包头和数据包体两部分. 数据包头由数据包标识、数据包功能、数据包参考号等组成; 数据包体主要由若干数据项组成. 详细结构信息如图 1 所示.

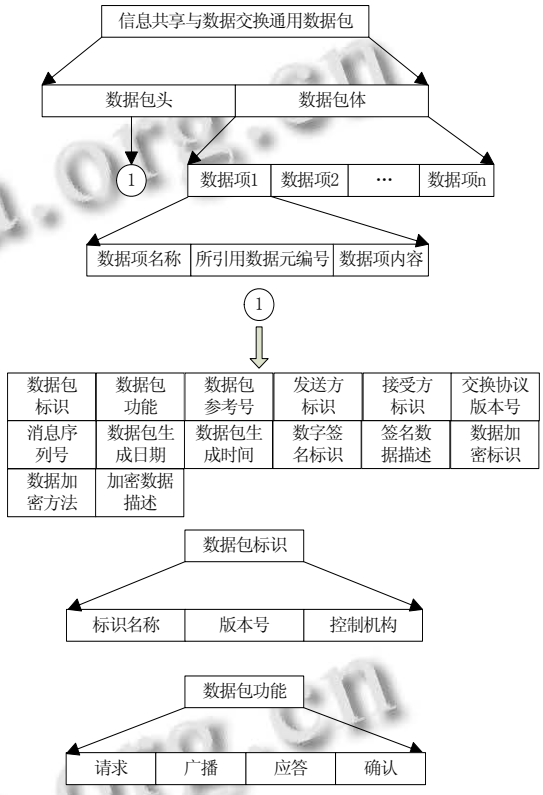

图 1 系统总体框图

针对该交换数据包, 相关 Schema 结构如下所示:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema …>
 <!--包含数据包头, 数据包体的声明-->
 <xs:element name="DataSharingPacket">
<xs:complexType><xs:sequence>
 <!--数据包头定义, 包含数据包标识、功能及参考号等相关信息-->
        <xs:element ref="DataPacketHeader"
 minOccurs="0" />
<!--数据包体定义, 包括 N 个数据项-->
        <xs:element ref="DataPacketBody"/>
 </xs:sequence></xs:complexType></xs:element>
…
</xs:schema>
```

由于篇幅有限，关于交换数据包头及数据包体详细定义请参考文献[13].

针对非实时数据交换，发送方应给出数据包头部分，以此标识数据包的来源等信息；针对实时数据交换，则无需指出数据包头部分，本文中所推荐的交通数据交换方法针对实时数据交换，其中采用 Web 服务结合 XML 签名加密技术，具体交互过程如下节所述.

2　交通数据交换交互过程

在推荐数据交换方法中，为了实现对接口和交互过程的保护，在服务提供方与服务调用方通过 Web Service 进行数据交换之前，要做如下准备工作，包括交换验证数字签名的证书(CA)，解密密钥和约定服务接口参数的具体 XML 格式. 准备工作完成后，按照如图 2 所示的交互过程实现服务接口的调用.

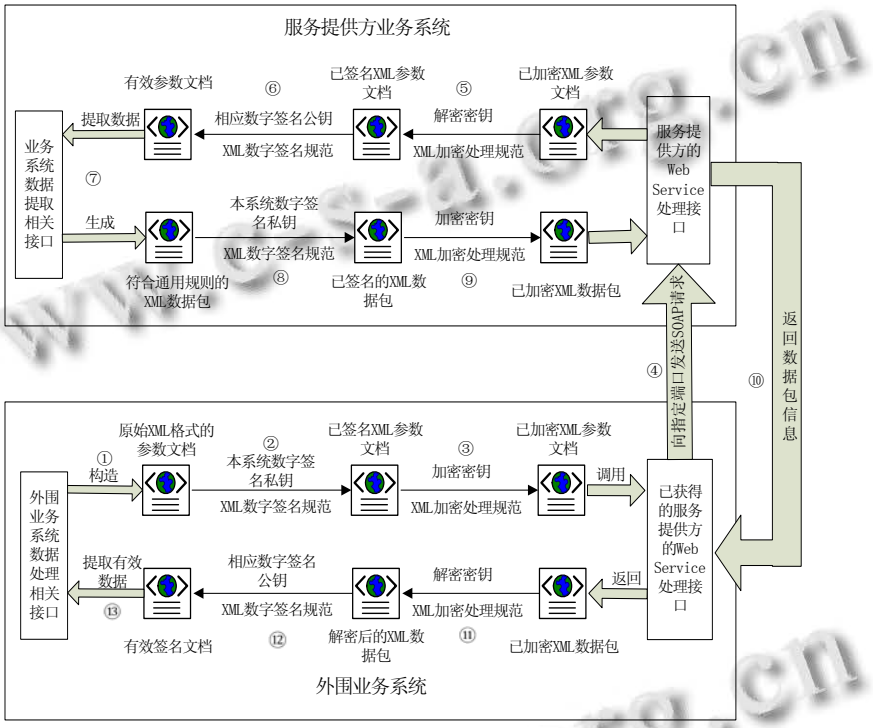

图 2　推荐数据交换方法交互过程示意图

针对图 2，具体介绍如下:

1) 外围业务系统按照已约定的参数文档格式构造 XML 文档，使用签名证书中的私钥对参数文档进行签名(如图 2 中流程①、②所示)，接着使用加密密钥对签名后的文档或文档片段进行加密(如图 2 中流程③所示)，最后调用服务接口向服务提供方发送请求信息(如图 2 中流程④所示);

2) 服务提供方接收到外围业务系统的请求信息后，首先根据业务系统已交换的解密密钥对所传入的文档进行解密(如图 2 中流程⑤所示)，成功解密后再利用相应的数字签名证书对签名信息进行校验(如图 2 中流程⑥所示)，若校验成功则调用相关函数对其中的数据进行解析并生成交换数据包(如图 2 中流程⑦所示).

3) 服务提供方根据上一小节所示的结构生成原始 XML 交换数据包，然后对交换数据包包体部分(<DataPacketBody/>元素)进行数字签名及加密处理，然后返回给外围业务系统，即图 2 中所示的流程⑧、⑨和⑩;

4) 外围业务系统根据服务提供方已交换的解密密钥对返回的数据包进行解密，成功解密后利用服务提供方已交换的数字证书公钥对数据包的签名进行校验，若校验成功则证明数据有效最后提取其中的结果数据，完成整个通信过程，即图 2 中所示的流程⑪、⑫和⑬.

3　应用实例

本节以《船舶基础信息采集交换接口规范》中的数据交换接口调用为例进行说明. 其中，该接口规范

中相比于其他的接口规范，增加了数据库表字段在相关数据库中的编号信息，可以更完整的体现对本文所提出的数据交换包的应用. 在该例中，其他业务系统通过 Web Service 接口从船舶基础数据库中读取船舶的基础信息:

ReadData<"tableName","具体船舶识别号","具体中文船名","3,6,7,8,9,10,11","CB_ EngNameVess","CB_CodePortReg","CB_CodeFlagSt","CB_IMO","CB_MMSI","CB_CallSign","CB_PrimRegNum", 7,10>

其中，接口的名称为 ReadData，实现了对具体船舶基础数据的读取，包括: “英文船名”, “船籍港代码”, “船旗国代码”, “IMO 编号”, “MMSI 编码”, “船舶呼号”, “船舶初次登记号”等共 7 项数据的 10 条记录.

下面从外围业务系统和服务提供方两方面详细介绍如何使用推荐数据交换方法.

3.1 外围业务系统

首先为了方便外围业务系统用户与服务接口提供方进行交互，在外围业务系统搭建了基于 B/S 架构的相关业务系统，负责构造请求信息及对请求结果进行校验，整个业务系统按功能分为构造参数文档模块、调用服务接口模块及解密及校验模块相应业务系统初始化界面如图 3 所示.

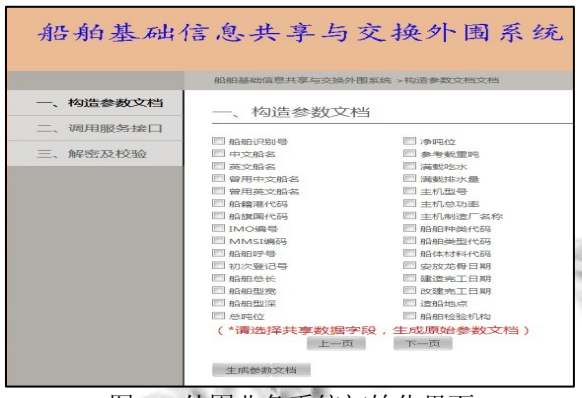

图 3 外围业务系统初始化界面

下面针对外围业务系统所完成的功能，简要介绍其实现细节.

3.1.1 构造符合约定的参数片段

针对本节开始中所指出的接口示例. 首先，双方约定服务接口参数的格式，这里约定采用 XML 格式的参数片段，按顺序将每个参数依次表示为一个 XML 元素<PARAM />，并规定参数片段的根元素为<PARAMETERS/>. 根据所约定的格式，外围业务系统构造的 XML 格式的参数片段示例如下.

```
<PARAMETERS>
<PARAM>VesselBasedInfo</PARAM>
<PARAM>1</PARAM>
…
<PARAM>10</PARAM>
</PARAMETERS>
```

3.1.2 参数文档签名及加密

在构造完成 3.1.1 小节所示的参数文档后，需要对其进行数字签名及加密处理，以此保证参数格式在网络传输过程中的安全性，这里对示例参数片段采用 X509 证书进行签名，之后采用对称加密算法 3DES 对已签名参数片段进行加密. 具体处理细节如下所述:

① 获取 X509 数字证书及目标文档数据流;

② 通过 JDK 密钥库工具类(KeyStore)获取 X509 证书私钥;

③ 使用 XML-Security 类库中的签名工具类及 XML 解析工具对目标文档解析并对目标元素进行定位并签名;

④ 依据 JDK 密钥工具类及 XML 解析工具获取对称密钥并加密已签名文档，返回给调用方.

最终结果数据文档示例如下所示.

```
<PARAMETERS>
<xenc:EncryptedData …>
 <!-- 省略了<xenc:EncryptionMethod/>及元素<ds:KeyInfo/>的内容>-->
…
<xenc:CipherData>
<xenc:CipherValue>
0+cRUMbrOWSSEg1RAfzmu…
</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>
</PARAMETERS>
```

3.1.3 解析服务提供方返回的数据

外围业务系统收到服务提供方返回的数据(如 3.2.2 所示)后，需要对其进行解密和签名校验，在确认返回数据有效的情况下提取其中的数据，其中所提取数据的数据类型可根据数据项名称或者数据项编号进行确定，进而完成相关业务处理，至此完成与 Web 服务提供方的整个交互过程. 数据解密及签名校验详细过程如下所示.

① 获取已签名并加密的 XML 文档;

② 通过 JDK 密钥库工具类获取交互双方交互之前已互换的对称密钥, 然后结合 XML 解析工具(本实例中采用 Apache Xcerse-Java 技术提供的工具类)对第①步中所获取的 XML 文档进行解密操作, 返回解密后的文档;

③ 获取 X509 数字证书公钥文件输入流, 使用 XML-Security 类库中的签名工具类对上述解密文档进行签名校验;

④ 若文档有效则提取其中的数据, 否则返回错误信息给数据提供方.

其中, 针对 3.2.2 小节所生成的数据包, 在客户端解密后的结果文档示例如下:

<DataSharingPacket><DataPacketBody>
<DataItem>
<!--此处为数据项的具体内容-->
…
</DataItem>
<!--以下省略了部分数据项的内容-->
…
<ds:Signature xmlns:ds="…">
<ds:SignedInfo>…</ds:SignedInfo>
<ds:SignatureValue>UTGxdoaTJiqPzSGCi84…</ds:SignatureValue>
<ds:KeyInfo>…</ds:KeyInfo>
</ds:Signature>
< /DataPacketBody></DataSharingPacket>

3.2 服务提供方

3.2.1 解密参数文档及校验

针对外围业务系统调用 Web 服务接口所传入的参数文档, 服务提供方需要对参数文档进行解密, 然后利用外围业务系统已交换的 X509 证书对文档的有效性进行校验, 在确认文档有效的情况下对其中的参数进行解析, 进而调用相应处理函数. 从而保证了服务接口调用的合法性, 文档解密及签名校验过程如 3.1.3 小节所述. 以 3.1.2 所传入的加密后的参数文档为例, 其解密结果文档示例如下:

<PARAMETERS>
<PARAM>VesselBasedInfo</PARAM>
<PARAM>1</PARAM>
…
<PARAM>10</PARAM>
<ds:Signature xmlns:ds="…">
<ds:SignedInfo>…</ds:SignedInfo>
<ds:SignatureValue>eiE4fMUg8oiCixFOJJI…</ds:SignatureValue>
<ds:KeyInfo>…</ds:KeyInfo>
</ds:Signature>
</PARAMETERS>

3.2.2 返回结果数据包

服务提供方在成功解密客户端传入的参数文档并确认其有效的前提下, 其将调用相关函数返回符合第 1 节中所述结构的 XML 数据包, 然后采用 X509 证书对其进行数字签名, 并利用 3DES 对称密钥对已签名文档进行加密处理, 最后将结果 XML 格式数据包返回给客户端. 数据签名及加密处理过程如 3.1.2 小节所述, 其中对签名的目标元素为交换数据包的包体.

针对上一小节中所提取的参数片段, 服务提供方返回的 XML 数据包示例如下.

<DataSharingPacket><DataPacketBody>
<xenc:EncryptedData xmlns:xenc="…" …>
<!-- 省略了 <xenc:EncryptionMethod/> 及元素 <ds:KeyInfo/>的内容>-->
…
<xenc:CipherData xmlns:xenc="…">
…</xenc:CipherData>
</xenc:EncryptedData>
< /DataPacketBody></DataSharingPacket>

4 结语

本文根据对行业内现有标准规范的总结分析, 同时基于 XML 安全规范、Web Service 等技术, 针对交通数据交换交互过程进行研究, 提出了一种交通数据交换通用方法, 以《船舶基础信息采集交换接口规范》中数据交换为例, 说明了该方法从交换数据包的生成到通过 Web Service 完成交通数据交换业务的实现方法和具体步骤. 针对交通行业内现存的异构数据环境而言, 无需更改原有系统的框架及业务逻辑, 同时很好的解决了异构数据平台数据交换的问题, 并保证了跨网络信息交互过程中的身份验证、安全性等问题, 弥补了现在行业内所采用的 ETL 及 Web Service 等实现方式的不足.

参考文献

1 汪祖云.交通数据中心总体架构与数据共享交换平台的设计研究.交通运输系统工程与信息,2008,8(3):23–28.
2 韩海航,张永智.数据交换与共享技术在交通行业数据资源

整合中的应用研究.计算机应用与软件,2007,24(9):109–112.
3 康红霞,刘建,王林,李聪.交通运输信息资源交换共享平台建设和应用.交通信息与安全,2011,29(3):116–122.
4 廖军.公路交通信息资源整合及系统实现研究[博士学位论文].西安:长安大学,2009.
5 葛迪.ETL 技术在交通信息资源整合工程中的应用研究[硕士学位论文].哈尔滨:哈尔滨工程大学,2010.
6 黄强,王薇,倪少权.基于 SOA 和 DDD 的铁水联运信息平台架构设计.计算机应用与软件,2013,30(6):124–126.
7 柴华,周兴社,杨刚,符宁,张海辉,王龙飞.基于企业服务总线的信息共享交换平台研究.微电子学与计算机,2008,25(4):116–120.
8 黄梦雄,朱勤东.交通地理信息公共服务平台设计与研究.交通信息化,2013,9:38–41.
9 吕斌,牛惠民.基于 Web Services 的交通信息集成系统的设计与实现.交通运输系统工程与应用,2007,7(6):39–44.
10 贺正求,吴礼发,洪征,王睿,李华波.Web 服务安全问题研究.计算机科学,2010,37(8):32–39.
11 李霞,张海涛,王晓勇.一种 Web 服务通信安全的优化方案.计算机科学,2012,39(8):59–61.
12 Xiao WX, Liu Z. The development of Web service composition based on XML security models and AJAX technology. International Journal of Advancements in Computing Technology, 2012, 4(19): 83–90.
13 交通运输信息系统数据交换通用规则.长安大学交通信息标准化技术研究所.http://std.chd.edu.cn/website/std_show.aspx?id=121.