DOI:10.16208/j.issn1000-7024.2009.15.051

• 网络与通信技术 •

基于 JMS 的安全通信模型研究与设计

邓以克， 王 灿

(浙江大学 计算机学院，浙江 杭州 310027)

摘 要：面向消息中间件(MOM)的安全性是目前的一个研究热点，目的是设计确保数据传输完整性的安全机制。通过分析JMS的两种消息通信模型，针对它在安全性方面存在的不足，引入了数字签名和加密技术，提出了一个基于身份验证和混合加密的可扩展安全通信模型，并详细介绍了模型的各个组成部分。模型的基本思想是使用数字签名的信息进行双向身份认证，并且在消息传输的过程中，利用双方协商的会话密钥和非对称加密技术对消息进行加密。最后构建了原型系统对模型进行了验证，实验结果表明此模型提高了基于JMS的系统的安全性。

关键词：Java 消息服务；安全通信；高级加密标准；RSA 算法；数字签名；加密技术

中图法分类号：TP393 **文献标识码**：A **文章编号**：1000-7024 (2009) 15-3526-05

Research and design of security message communication model based on JMS

DENG Yi-ke, WANG Can

(College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China)

Abstract：Security of message-oriented middleware (MOM) is a hot research issue now. It aims at designing security mechanisms to ensure data integrity in transferring. The security flaws of JMS is analyzed by an in-depth study of the model. A scalable security message communication model is introduced which combines the power of user authentication and mixed encryption based on digital signature and encryption. The core idea of the model is to use the digit-signatured information to authenticate users on both sides. Meanwhile, a session key negotiated by both sides and a public-key encryption technology are employed to encrypt the message. Finally, we validate the model with a prototype system. Experimental results shows the model improve the security of JMS-based systems.

Key words：Java message service; security message communication; AES; RSA; digital signature; encryption

0 引 言

消息队列中间件 MOM(message-oriented middleware)是一种特定的中间件，它利用高效的消息传递机制进行平台无关的数据交换，并基于数据通信来进行分布式系统的集成。由于没有一个通用的标准，基于各种消息中间件的系统很难实现互操作和无缝连接，Java 消息服务(Java message service，JMS)是 SUN 公司提出的旨在统一各种消息中间件接口的规范，它提供了一组与具体实现无关的接口[1]。它支持发布/订阅(Pub/Sub)和点对点(P2P)两种消息模型，并提供消息过滤和事务处理等机制。JMS 在受到广泛关注和应用的同时，但由于其本身并没有包含强制性的安全机制，因此安全性也面临许多新的问题和挑战。

本文针对 JMS 规范在安全方面的不足，对基于 JMS 的消息通信进行研究，利用数字签名来实现双向的身份验证，并使用结合对称加密算法和非对称加密算法的混合加密机制对消息进行加密，此外，Topic 和 Queue 是 JMS 系统中的关键资源对象，因此为其设计了安全管理器来控制对这些资源的访问。

1 相关技术

1.1 数据加密

数据加密，指的是用户选择一个特定的加密算法对需要保护的明文数据进行处理，使之转换成为常人难以识读的密文数据，并且只有在输入相应的密钥后，通过特定的解密算法，将密文恢复成明文的过程称为数据解密。数据加解密的基本过程[2]如图 1 所示。

当前的加密技术主要分成两类：对称式加密和非对称式

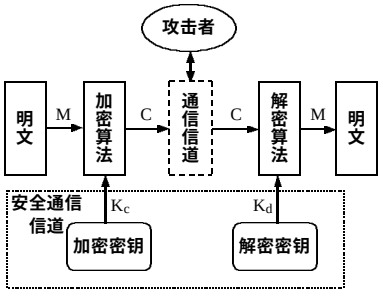

图 1 数据加密

收稿日期：2008-09-26；修订日期：2009-03-05。

作者简介：邓以克 (1985－)，男，硕士，研究方向为网络通信、多媒体技术； 王灿 (1974－)，男，讲师，硕士生导师，研究方向为信息检索、数据挖掘、机器学习、Web 数据管理等。E-mail：phinecos@163.com

加密。前者在加密和解密的过程中使用的是同一个密钥，目前这种加密技术被广泛采用。而后者在加密和解密的过程中所使用的不是同一个密钥，而是使用一对相互配对的公钥和私钥，其中公钥对外公开，而私钥则由加密者自己持有。

1.1.1 对称加密

对称加密技术的特点是加密和解密这两个过程中使用的加密密钥和解密密钥是同一个密钥。当前流行的对称密码算法有数据加密标准 DES 算法，高级加密标准 AES[3]。

当前 AES 算法的标准版本是 2000 年美国政府采用的 Rijndael 加密算法。Rijndael 算法是一个对密文数据进行分组，再对各个数据分块进行各项迭代运算的加密算法，它允许分组后的数据区块的长度以及密钥的长度自由变动。该算法的原型是 Square 算法，它的设计策略是宽轨迹策略。这个算法一共需要的迭代次数记为 N_d，它的取值由明文的数据区块长度和所选用的密钥长度来决定。当选择的密钥长度为 128 比特时，N_d 的大小为 10；当选择的密钥的长度为 192 比特时，N_d 的大小为 12；当选择的密钥的长度为 256 比特时，N_d 的大小为 14。

Rijndael 算法的加密过程分为 4 个阶段：密钥扩展，轮密钥加操作，N_r-1 次轮变换操作，最后一次轮变换操作。其中轮变换操作包括字节代换，行移位，列混淆和轮密钥加 4 个过程，而最后一次轮变换操作中包括字节代换，行移位和轮密钥加 3 个过程[4-5]。

Rijndael 算法作为新一代的高级加密标准，已成为对称密钥密码算法的首选。它将安全，高效，性能，方便使用及灵活性集于一身，使他成为 AES 的合适选择。特别是 Rijndael 算法在不同硬件和软件运行环境下表现出的性能始终非常良好，无论这些环境是否有反馈模式，它的密钥设置时间非常出色，密钥的灵敏性也很好。Rijndael 算法对于内存的要求也很低，这使得它可以广泛使用在那些空间受限制的环境中，即使处于这样的环境下，它也仍然可以表现出出色的性能。Rijndael 算法的操作可以很容易地抵御时间和空间上的攻击，此外，在提供这些保护的同时也没有影响 Rijndael 算法的性能。它内部的循环结构也使得它表现出有益与并行水平结构的较好的潜能。

1.1.2 非对称加密

与前面说的对称加密算法不同，非对称加密使用两个密钥：公钥和私钥，如果使用公钥对明文进行加密，则使用私钥才能进行解密；而如果使用私钥对明文进行加密，则只有使用相应的公钥才能进行解密。由于加密过程和解密过程使用的是不同的两个密钥，其中公钥可以公开出去，而私钥是加密者自己负责保密的，这就便于进行密钥的分发，从而解决了前面介绍的对称加密算法在密钥安全性方面存在的问题。

RSA 算法使用的密钥长度可以在 40 位到 2048 位之间变化，在加密时首先需要将明文数据分割成数据块，并且数据块的大小也是可变的，但它不能超过所使用的密钥的长度。RSA 算法将每一个明文块转换为与密钥长度相同的密文块。因此，密钥越长，加密效果就越好，但加密解密所需要的开销也越大，一般在设计系统时需要在安全性和性能之间进行折衷考虑。

当前典型的非对称密钥算法有 RSA 算法，RSA 算法的具体过程如下：

(1)计算公开密钥：随即选择两个互异的大素数 p,q，并且 p,q 必须保密，则公开密钥 $n = pq$。

(2)计算 $\delta(n) = (p-1)(q-1)$，随机选择一个整数 e, $1<e<\delta(n)$ 并且 $(e,\delta(n)) = 1$。

(3)计算私有密钥：$d = e^{-1} \pmod{\delta(n)}$。

(4)加密运算：$C = m^e \bmod n$，其中 m 为明文，C 为密文。

(5)解密运算：$M = C^d \bmod n$。

1.2 JMS

JMS(Java message service)是 SUN 及其伙伴公司提出的旨在统一各种消息中间件系统接口的规范。JMS 规范定义了一套通用的接口和相关语义，提供了如消息持久化，消息过滤和事务的服务。

它最主要的目的是允许 Java 应用程序访问现有的各种消息中间件。但为了对底层的实现进行抽象，使得应用开发人员不用与其细节打交道，规范没有指定底层消息传输的通信协议，一个特定的 JMS 实现可以提供基于 TCP/IP, HTTP, UDP 或其它的协议。

JMS 支持点对点(P2P)和发布/订阅(Pub/Sub)两种消息处理模型[7]。

1.2.1 点对点(P2P)模型

点对点模型是建立在消息队列的基础上的，每个客户端对应一个消息队列，客户端发送消息到对方的消息队列中，并且从自己的消息队列中读取来自其它客户端的消息。在这个消息模型中，消息的发送者发送消息到一个指定的队列，消息接收者从这个队列中接收消息。消息的发送和接收都是异步进行的。

一个队列可以有多个消息发送者和多个消息接收者，但是每个消息只能有一个消息使用者。此外，消息接收者还必须确认已经接收到消息了。具体模型如图 2 所示。

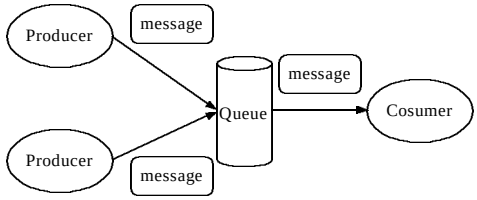

图 2 P2P 消息发送模型

1.2.2 发布/订阅(Pub/Sub)模型

在这个消息模型中，消息的发布者通过主题(Topic)这个渠道向订阅者发布消息，订阅者可以选择订阅的主题，发送到一个主题的所有消息都将发送给这个主题的所有订阅者。消息可以由一个或多个发送者以一个主题发送，所有订阅了这个主题的客户都可以接收到消息。主题使得消息的发布者和订阅者保持相互独立，不需要直接接触便可以保证消息的传递。在模型中，存在非持久化订阅和持久化订阅两种方式。前者只有当客户端处于活动状态，也就是和 JMS Provider 保持连接状态时才能接收到某个主题的消息，而当客户端处于离线状态时，发送到这个主题的消息就会丢失，无法收到。如果使用持久性订阅，客户端会向 JMS 注册一个识别自己身份的标识符，若客户端处于离线状态时，JMS Provider 会为它保存所

有发送到主题的消息,当客户再次连接到JMS Provider时,JMS Provider会对其标识符进行匹配,从而向客户端发送所有其离线时到达主题的消息。具体模型如图3所示。

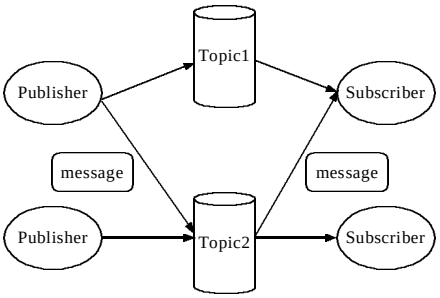

图3 Pub/Sub消息发送模型

1.3 JMS的安全问题

JMS规范中对于安全机制并没有给出任何明确的定义,而是将这些问题留给用户在实现JMS Provider时自行定义和实现。信息安全对于大多数应用来说都是需要严重关注的问题,而基于JMS的异步通信会面临许多潜在的威胁,例如:①攻击者在客户端伪造出虚假的身份来欺骗JMS Provider,从而成功登陆系统,获得系统资源的访问权;②如果没有对用户权限进行设置和审核,攻击者可以完全越过默认的权限,越界访问系统的一些关键资源;③基于JMS的消息传递默认是采用明文传输,攻击者可以轻易地获取传入和传出的明文流,对消息进行窃取和篡改。

2 系统模型

针对上述问题,本文提出了一个可扩展的安全通信模型,它采用基于数字签名的用户身份验证和对消息进行混合加密相结合的方式来增强JMS通信系统的安全性,模型的基本结构如图4所示。

模型主要包括以下几个部分:

(1)数字证书管理:负责为客户和服务器端申请数字证书,验证参与会话的对方身份的合法性。

(2)身份认证:认证模块采用RSA非对称算法实现客户端和服务器端双方之间的身份认证。

(3)会话密钥协商:参与会话的发送者和接收者一起协商用于会话使用的128位AES密钥。

(4)消息处理模块,主要负责消息的加密和解密,使用的密钥需要通过参与会话的双方协商后确定。

2.1 身份验证

在模型中,我们假定通信双方都有自己的一对公钥和私钥,并且通过各自的证书管理模块向CA认证中心申请自己公钥所对应的数字证书(数字证书遵循X.509格式)。身份认证的基本流程如图5所示。

(1)客户A和服务器B在初始化时都会向CA认证中心申请一个数字证书,其中包含了自己的公钥信息。A和B可以利用对方的公钥来验证彼此身份的真实性。

(2)发送端首先用自己的私钥对标识自身身份的信息(如用户名,密码等)进行数字签名[8]。首先使用128bit的MD5算

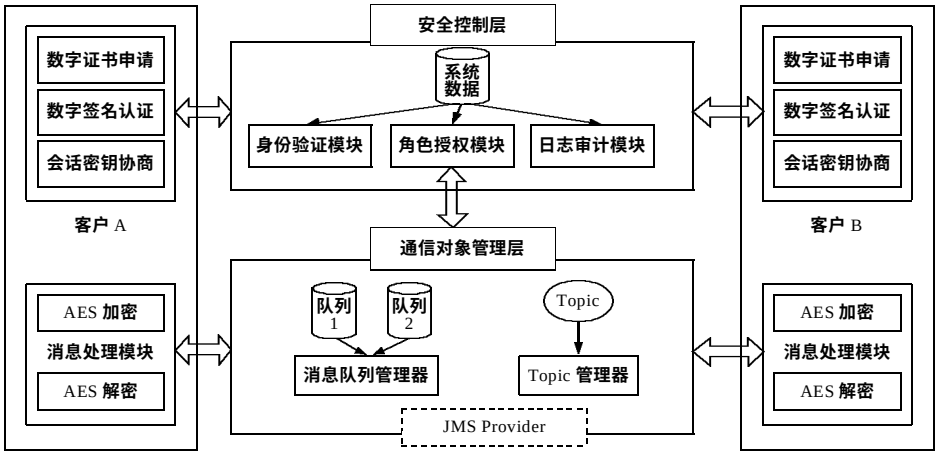

图4 基于JMS的安全消息通信模型

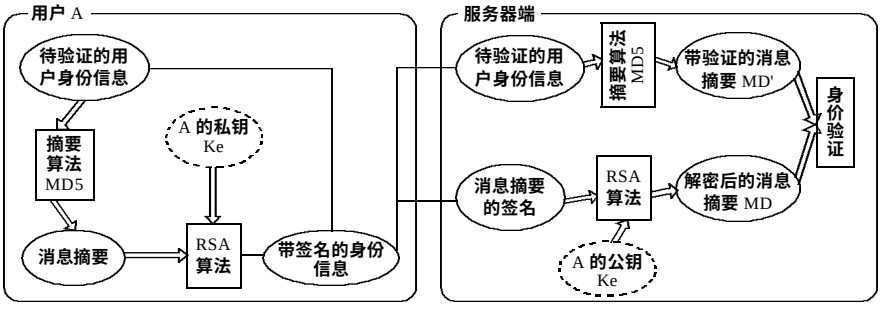

图5 身份认证流程

法计算身份信息的散列值，再使用 RSA 算法和自己的私有密钥对散列值进行 RSA 非对称加密。

(3) 接收方收到发送方的数字签名信息后，先从 CA 认证中心获取到发送方的公钥，通过RSA算法对散列值进行解密，然后再用 128bit 的 MD5 算法[9] 计算对方身份信息的散列值，然后对两个散列值进行比对，若两个散列值相等，则接收方确认发送方身份的真实性。

2.2　会话密钥协商

即使通信双方彼此之间验证过身份的合法性后，但中间的信道仍然是不安全的，攻击者可以截取或篡改信道中的明文信息。因此为了保障数据传输的安全性，我们可以让通信双方在会话开始时协商出一个密钥，接下来就双方使用这个密钥，利用对称加密算法 AES 对待传输的数据进行加密[10-11]。会话密钥协商如图 6 所示。

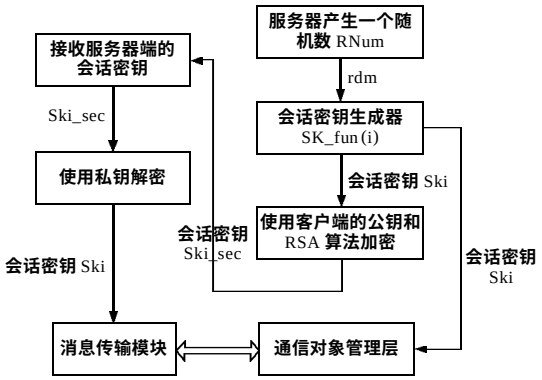

图 6　会话密钥协商流程

考虑到服务器端的可靠安全性程度较高，文中模型假定会话密钥由服务器端负责生成。

(1)服务器B产生一个随机数Rnum，并将其传入会话密钥生成器 Sk_fun(i)来产生一个会话密钥 Ski。

(2) 服务器 B 使用客户 A 的公钥 keyA，利用 RSA 算法对会话密钥Ski进行加密：Ski_sec = RSA(keyA)，产生加密后的会话密钥 Ski_sec。

(3) 客户 A 接收到服务器传来的加密后的会话密钥 Ski_sec，使用自己的私钥，利用 RSA 解密算法解密出原始的会话密钥 Ski。

(4) 由于对称加解密算法速度较快，此后会话中的消息传输都使用协商好的会话密钥 Ski 进行加解密。

2.3　对 Queue 和 Topic 的保护

考虑到服务器端的可靠安全性程度较高，文中模型假定会话密钥由服务器端负责生成。同时，相关的研究[12]表明，利用 SSL 可以有效地保护服务器端的数据安全。

Queue 和 Topic 是 JMS 最重要的两类核心对象，为了对它们进行安全性保护，我们在模型加入了 Queue 管理器和 Topic 管理器。为了简单起见，下面就只以对 Queue 的管理为例。

一个Queue管理器负责管理一个或多个本地的Queue，并且可以和分布式系统中其它的 Queue 管理器进行通信，通信的模型如图 7 所示。

在分布式系统中，当各个节点之间需要向彼此转发消息

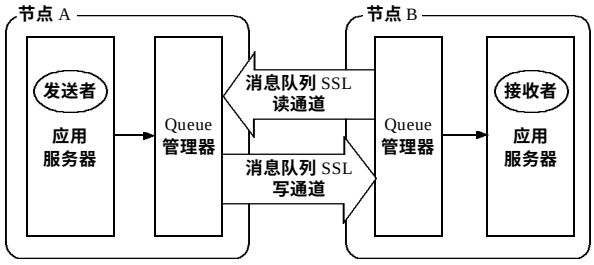

图 7　Queue 管理器

到所在的Queue中时，这些节点就在逻辑上组成一个会话组，而这个会话组的安全问题就值得进行考虑：①确保没有非法的Queue管理器加入到会话中来；②Queue管理器之间的通信数据的加密。

在会话组建立之时，首先确定参与会话的一个或多个节点作为主节点，其它的节点作为从节点。主节点中保存了参与当前会话组的所有节点的信息，例如节点的数目，IP 地址，节点的负载情况等。

一个新的 Queue 管理器如果想加入当前会话组，它必须通过主节点对其进行的身份验证。一旦它通过了身份验证，就会为它分配两个安全的 SSL 通道，一个用于向其它节点写数据的写通道，一个用于接收来自其它节点数据的读通道。此后，Queue管理器之间相互传输数据就可以使用这两个SSL通道进行。如果身份验证失败，则拒绝其对 Queue 的访问请求，从而达到对 Queue 的保护。

3　实验分析

我们使用 Java 实现了本文所描述模型的一个原型系统，并使用如下软硬件环境进行测试：服务器端为一台 Dell PowerEdge SC440 服务器，采用双核英特尔至强 3000 系列(Conroe)处理器，安装的操作系统为 Red Hat 9.0，两个模拟客户端使用 IBM 兼容机，操作系统采用 Fedora 9。

我们首先对不附加任何安全模块的JMS通信系统进行测试，统计在一段时间随着数据包数量发生变化时，整个系统的通信延迟时间。采用本文所描述的安全模型后，在原有通信延迟(t_0)基础上增加了数字签名用时(t_p)和消息加解密用时(t_e)，在此基础上再测试此时系统通信延迟时间随数据包数量发生变化，两者的比较结果如图 8 所示。

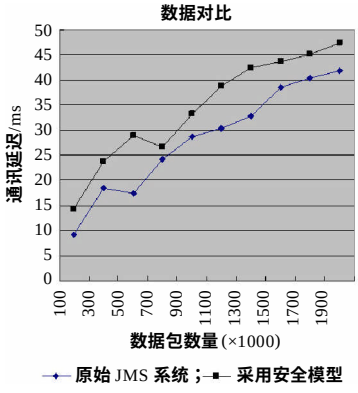

图 8　系统通信延迟时间

原始 JMS 系统平均延时：V_0 = 28.2(ms)，采用安全模型后平均延时：V_s = 34.3(ms)，测试结果表明：$t_p = t_0 \times 0.02$, $t_e = t_0 \times 0.06$，即采用该模型后大约增加了 8%的通信延迟，这是对于安全性要求比较高的系统来说，是处于可以接受的范围之内的。

以下是我们对这个模型安全性的评价：

(1)客户端和服务器端进行双向的身份认证，服务器节点之间通过主节点进行身份验证，有效地防止攻击方伪造身份对系统进行攻击。假如有攻击方冒充发送方发出一个身份验证信息给接受方，接收方收到信息后，先使用发送方的公钥，通过RSA算法对散列值进行解密，然后用MD5 算法再次计算身份信息的散列值，由于攻击方不知道发送方的私钥，因此解密出来的散列值和再次计算出来的散列值一定是不同的，那么就可以知道此信息来自非法的攻击者。

(2)会话密钥由安全性比较高的服务器端负责产生，由于在服务器端可以配置防火墙，代理服务器，入侵检测等多种安全性手段，因此会话密钥可以得到较好的保护。

(3) 利用协商好的会话密钥和 AES 加密算法对传输的消息进行加密，由于每次会话密钥都是由服务器端的密钥生成器对随机数进行处理后产生的，因此，对于第三方攻击者来说，想解密会话中传输的消息的难度大幅增加。

4 结束语

在消息中间件的实际应用中，往往会面临各种潜在的安全威胁，如何确保消息的完整性和机密性，具有重要的实用价值。本文介绍了 JMS 的两种消息模型：Pub/Sub 模型、P2P 模型；并分析了 JMS 在安全性方面的不足。针对这些不足，本文提出了一个可扩展的安全通信模型，利用数字签名技术进行身份验证，从而在数据传输时使用混合加密技术确保数据的安全，并进一步对 JMS 系统中的关键资源提供保护。随着消息中间件的广泛应用，将有更多基于 JMS 的系统投入应用，基于 JMS 的安全性机制研究具有广阔的应用前景。

参考文献：

[1] Monson-Haefel R,Chappell D A.Java message service[M].California:O'Reilly,2001.

[2] Douglas R Stinson.Cryptography theory and practice[M].北京:电子工业出版社,2002.

[3] 杨以光,于会智.基于 AES 和 RSA 加密的数据安全传输技术[J].电脑知识与技术,2006,8(3):84-86.

[4] 杜效伟.基于 AES 和 RSA 的数据加密技术方案[J].许昌学院学报,2008,27(2):80-84.

[5] 卢正鼎,廖振松. Rijndael 算法的研究[J]. 计算机工程与科学,2005,27(6):72-74.

[6] Dzung D,Naedele M,Von Hoff T P,et al. Security for industrial communication systems[J]. Proceedings of the IEEE,2005,93(6):1152-1177.

[7] Sun Inc. Java message service[EB/OL].http://java.sun.com/products/jms.

[8] 肖攸安,李腊元.数字签名技术的研究[J].武汉理工大学学报,2002,26(6):737-740.

[9] 张裔智,赵毅,汤小斌.MD5 算法研究[J].计算机科学,2008,35(7):295-297.

[10] 汪林林,肖常俊,张学旺.一种面向消息的安全传输中间件模型[J].计算机科学,2007,34(7):288-292.

[11] Amit Parnerkar,Dennis Guster,Jayantha Herath.Secret key distribution protocol using public key cryptography[J].Journal of Computing Sciences in Colleges,2003,19(1):182-193.

[12] Homin K Lee,Tal Malkin,Erich Nahum.Cryptographic strength of ssl/tls servers: current and recent practices[C].Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement,2007:83-92.

(上接第 3525 页)

在本系统中，所提取的特征项都是基于单词的，以后应该把基于短语和非文本属性的因素考虑进来，这样会进一步提高过滤的准确率。同时垃圾邮件过滤的精确率较大程度上取决于基于内容的过滤技术的性能，进一步探究和实现更高性能的基于内容的垃圾邮件过滤应用的分类算法也将是下一步的工作重点。垃圾邮件是全球性的问题，要彻底阻挡垃圾邮件，必须不断的提高技术和方法，同时加强和完善反垃圾邮件的法律法规，只有两者有机地结合起来，才有可能能从根本上消除垃圾邮件。

参考文献：

[1] 中国互联网协会反垃圾邮件中心.2007 年第四季度中国反垃圾邮件调查报告[EB/OL]. http://www.anti-spam.cn/pdf/2007_12_dc.pdf.

[2] Klensin J,Freed N,Moore K.Smtp service extension for message size declaration[EB/OL]. http://www.rfc-editor.org/rfc/rfc1870.txt.

[3] Myers J,Rose M.Post office protocol 3[EB/OL]. http://www.rfc-editor.org/rfc/rfc1939.txt.

[4] Platt J C.Fast training of support vector machines using sequential minimal optimization[C]. Schlkoph B. Advances in Kernel Method-Support Vector Learning. Cambridge,MA:MIT Press,1999:185-208.

[5] 詹川,卢显良,周旭,等.基于贝叶斯公式的垃圾邮件过滤方法[J].计算机科学,2005,32(2):73-75.

[6] 张羽.基于支持向量机理论的垃圾邮件过滤模型[D].成都:电子科技大学,2006.

[7] 邹汉斌,雷红艳,邓卫红.支持向量机在反垃圾邮件过滤中的应用[J].计算机工程与设计,2007,28(9):2015-2017.

[8] 林丹宁.反垃圾邮件关键技术研究与实现[D].杭州:浙江大学,2007.

[9] 李洋,方滨兴,王申.基于用户反馈的反垃圾邮件技术[J].计算机工程,2007,33(8):130-132.