中图分类号：TP399　文献标志码：B　文章编号：2095-641X(2016)11-0073-05　DOI：10.16543/j.2095-641x.electric.power.ict.2016.11.013

基于多用户模型的企业级即时通信系统的研究与应用

王纪军，李夫宝，王京
（国网江苏省电力公司 科技信通部，江苏 南京 210008）

摘要：随着移动互联网技术及智能化移动终端的不断发展，构建一套基于多用户模型的电力企业级的即时通信平台以满足员工内部安全、可靠的通信需求成为当务之急。文章基于XMPP协议，采用Openfire作为基础实现，构建了一种企业级即时通信系统。该即时通信系统通过端对端加密来保证客户端与客户端之间通信的安全性；通过建立Openfire集群来满足大规模用户即时通信的高性能需求；通过建立跨节点分布式Openfire服务来提高系统性能和稳定性。实践表明，该系统具有良好的消息安全性和可扩展性，能够有效保证多用户模型下系统的高效性和可靠性，较好地满足了企业级即时通信的需求。

关键词：XMPP；Openfire；即时通信；端对端加密；集群；跨节点

0　引言

即时通信（Instant Messaging，IM）是目前因特网上最快捷的实时通信方式，除了传送即时消息外，它还支持文件传输、语音通信、视频会议、网络电话、视讯会议、电子邮件收发等功能。

构建电力企业级即时通信平台不仅可以实现即时通信工具常用功能，如消息发送、文件传输、语音传输、视频传输等，而且还可以设计特殊功能组件满足自身的特定需要，如敏感词过滤、保护员工隐私、响应公司保密规定等。此外，在即时通信平台上，按照部门设置IM通信录，有利于查找部门好友、快速定位目标人员；集成国网邮箱系统，便于随时查看内网邮件；创建聊天群组，有利于公司内部信息上传下达，交流互动；构建消息中心，随时查看日程安排和工作提醒情况；从电力服务角度出发，利用即时通信工具能够实时响应客户需求，为客户提供智能互动服务。因此，即时通信平台的构建，对于满足用户个性需求、提高工作效率、增加客户体验、提升客户满意度具有重要的参考意义。

1　国内外即时通信研究概述

即时通信被认为是一种确认所选择的朋友或同事是否与因特网有连接，若有连接，允许和他们进行实时信息交换的能力。即时通信是一个实时通信系统，允许两人或多人使用网络实时地传递文字消息、文件，进行语音和视频交流[1-2]。

1.1　国内外研究现状

目前即时通信开发工具日渐成熟，主流的技术框架为Openfire、Tigase，两者均基于开放式即时消息传递和现场服务协议（Extensible Messaging and Presence Protocol，XMPP）。XMPP作为主流标准协议之一，拥有多个开源实现且具有开放性的特点，很多即时通信平台都基于此实现[3-6]。相较于Tigase，Openfire有很多优点。Openfire是一个实时协作服务器，基于开源Apache协议，利用网络进行管理，单

台服务器即可以支持上万并发用户[7]。Openfire 易安装和易管理，安全性和性能均优于其他框架，并且 Openfire 支持集群通信服务器，支持高性能插件开发和扩展。

随着 4G 时代的到来，网络已经能够支撑移动终端的即时通信，人们通过移动端线上交流不再只拘泥于简单的电话、文字会话、E-mail、留言、短信，手机用户可以利用充沛的网络带宽资源与其他用户进行文本传输、语音通话、长链接、甚至视频聊天。

1.2 存在的问题

虽然 Openfire 以其良好的性能和扩展性深得开发者的喜爱，但是利用 Openfire 进行即时通信软件开发时还存在以下几方面的不足：服务器端的数据安全不能得到有效保证；随着用户规模的不断扩大，单台服务难以满足高性能的需求；单节点故障易对即时通信系统核心业务产生影响。

2 相关技术简介

2.1 XMPP 协议

XMPP 全称为开放式即时消息传递和现场服务协议，它是一种基于可扩展标记语言（Extensible Markup Language，XML）的传递出席信息（Presence）和消息路由的协议[8]，可实现服务器之间的准即时操作，如即时消息（IM）的发送，在线现场探测[9]。该协议可以忽略操作系统和浏览器的差异，为异构网络互联提供了一种安全易用的方法，使得因特网用户能够向网上的任何用户发送即时消息。

2.2 XMPP 的基本网络架构

XMPP 是一个典型的客户机 / 服务器（Client/Server，C/S）架构，而大多数即时通信软件采用的是对等网络（Peer to Peer，P2P）架构。在 XMPP 网络结构下，2 个客户端进行通信时需要通过服务器来传递消息。这种架构能够大大简化客户端工作，充分发挥 C/S 架构的优势。

XMPP 中定义了 3 个角色：服务器、客户端和网关。服务器主要用于管理客户端之间的连接和会话，同时，为具有有效地址的 XML 节提供路由功能。此外，大多数 XMPP 服务器还为客户端提供了数据存储功能。网关主要负责异构即时通信系统间 XMPP 协议的转换，包括短信、MSN 及 ICQ 等异构系统。

XMPP 中，单客户端通过传输控制协议 / 因特网互联协议（Transmission Control Protocol/Internet Protocol，TCP/IP）连接到单服务器，其工作原理是：①节点与服务器建立连接；②服务器根据本地目录系统中的证书对节点进行认证；③服务器根据节点指定的目标地址将目标状态返回给节点；④服务器查找、连接目标节点，并进行相互认证；⑤节点与目标节点间进行通信。

2.3 XMPP 逻辑编址

XMPP 路由的核心是采用一种类似于电子邮件的逻辑编址方案。XMPP 网络结构中的一个实体即为一个节点，它采用 JID（Jabber Identifier）来表示一个用户。一个有效的 JID 格式为 node@domain/resource，其中包括：域名（domain identifier），节点（node identifier）和源（resource identifier）。地址中的域用来表示节点不同的设备或位置，可用普通的域名系统（Domain Name System，DNS）来解析。节点既可以表示用户，又可以表示应用或服务。资源用于识别属于用户的位置或设备等，同一用户在同一时刻可以通过多种资源与同一个服务器进行连接[10]。

2.4 XMPP 中的 XML 流

XMPP 传输的即时通信指令采用 XML 格式的纯文本，它的核心是在网络上分片断发送 XML 的流协议。XML 流是 XML 元素在网络中传输的载体，也是一个非常重要的可以被进一步利用的网络基础协议。当客户端与服务器端建立了 TCP 连接后，会在客户端和服务器端间初始化一个 XML 流。XML 流通过发送一个 <stream:stream> 标签来进行初始化，此后，通信实体间可进行进一步的信息交换。传递 XML 文本使得解析更为容易，也易于阅读，方便了开发和查错。

2.5 XMPP 中的 XML 节

XML 节是一系列结构化信息单元。XMPP 中包含 3 种顶级 XML 节，分别是：iq，message，presence；5 个通用属性分别是：to，from，id，type，xml[11]。

1）<iq />：定义请求语义，允许用户通过相应的 XML 格式进行查询和响应。<iq /> 节可被看作一个请求－响应机制。与 <message /> 节和 <presence /> 节不同，<iq /> 节是双向的。<iq /> 的 4 种类型分别为：get，set，result，error。

2）<message />：定义消息语义，用于在用户间发送消息。<message /> 节与 E-mail 系统中发生的通信类似，其与 <iq /> 节的不同之处在于，消息发送后，消息发送者无法得知消息是否已被目标用户接收。<message /> 的 5 种类型分别为：normal，chat，groupchat，headline，error。

3）<presence />：定义出席语义，用于确定用户的状态。<presence /> 节可以被看作是一种“出版 - 订阅”机制，订阅者通过向目标实体发送订阅请求以收到相关信息。

3 企业级即时通信平台设计

XMPP 协议的开源实现有多个，但目前市场上大部分基于 XMPP 的企业级即时通信系统都基于 Openfire，市场占有率高，代码可扩展性强，可维护性较高，因此本文选用 Openfire 作为 XMPP 的基础实现，在 Openfire 基础上构建移动即时通信系统。

3.1 消息安全性设计

XMPP 在客户端与服务器通信，和服务器与服务器通信中都使用安全传输层协议（Transport Layer Security，TLS）作为通信通道的加密方法[12]，但没有考虑服务器端的数据安全。当消息经由多个服务器时，一旦服务器被监听，XML 数据流被截获，由于 XMPP 的开源性特征，用户的信息安全会存在重大隐患[13]。

对于 XMPP 存在的服务器端安全问题，在该企业级即时通信平台中，采用端对端加密（End to End Encryption）的方式来解决 XMPP 的开源特征造成的安全隐患。端对端加密的实现思想为对通信实体进行加密。这样，即使 XML 数据流被截获，密文也无法被解析出，用户信息的隐私性得到保证。

端对端加密的实现过程分为以下 2 个步骤。

1）客户端进行握手，获取 session key。通信双方将经过一系列的安全验证达成握手，最终各获得一个密钥，即 session key。

2）采用 session key 对数据流进行加解密。通信双方完成客户端握手操作后获取到 session key，该 session key 只对这 2 个通信客户端可见。当客户端 A 发送数据时，数据流会由 session key 进行加密操作。在数据传递过程中，即使该数据流被截获了，由于 session key 是未知的，无法对数据流进行解密。当数据流到达客户端 B 时，客户端 B 通过 session key 对数据流进行解密，获取真实数据。

3.2 消息扩展性设计

XMPP 继承了 XML 灵活的发展性，使得基于 XMPP 的应用具有很强的扩展性。基于 XML 的结构化信息以 XML 节的形式在通信实体间交换和传递，可以基于核心协议，通过发送扩展信息来构建特定功能。

XMPP 将出席和相关消息嵌入 XML 结构化数据中，使其能够有效地路由至目标资源，充分发挥了 XML 在通用传输层的作用，保证了数据传递的高效性，最大程度简化了客户端的实现。

4 XMPP 可靠高效企信即时通信方案

4.1 建立集群 Openfire 即时通信系统

随着用户规模的不断扩大，单台服务器不能满足高性能的需求，因此需要研究高性能的集群插件，实现跨集群统一服务。每一用户位置存放在一个目标服务器，并且该服务器存放该用户的地址缓存信息。接收信息时，若接收到信息的服务器不是目标服务器，则由该服务器发送给目标服务器。集群 Openfire 即时通信系统如图 1 所示。

当 Openfire user2 与 Openfire user3 联系，两者可以通过目标服务器 B 直接进行即时通信；当 Openfire user2 与 Openfire user1 联系时，Openfire user2 需要通过缓存服务器中 Openfire user1 的缓存信息再搜索到目标服务器 A，从而完成与 Openfire user1 的通信。

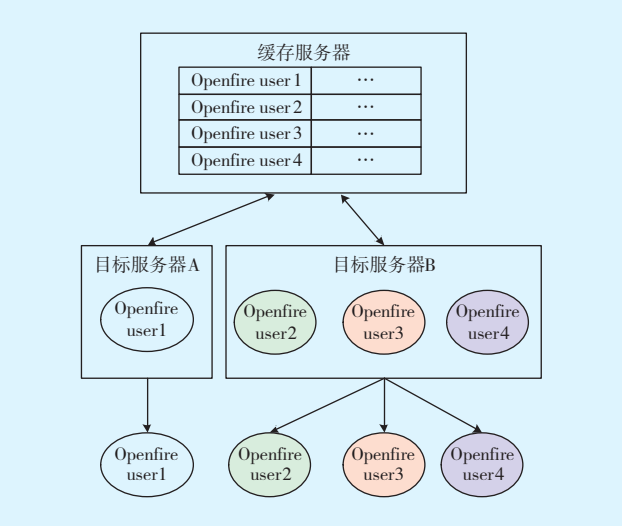

图 1 集群 Openfire 即时通信系统

Fig.1 Instant messaging system of Openfire cluster

4.2 建立跨节点分布式 Openfire 即时通信系统

为提高用户体验，减少单节点故障即时通信系统核心业务的影响，需要将单节点信息分配到多节点上。当某一节点出现故障时，支持节点自动迁移，以保证节点间通信，保持信息自由畅通。即时通信系统的总体架构如图 2 所示。

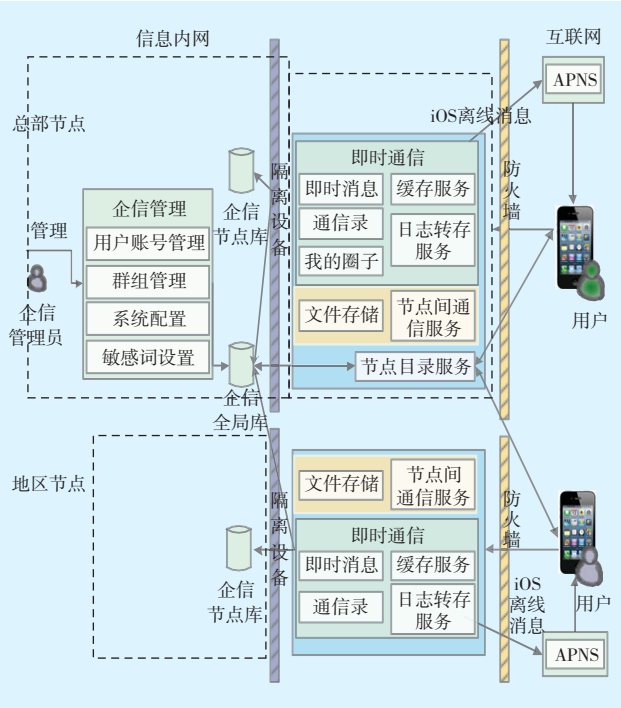

图 2 即时通信系统的总体架构

Fig.2 Overall architecture of the instant messaging system

在该架构中，企信全局库中存放用户账号信息、好友关系、群组、圈子动态、企信配置信息、敏感词设置等，企信节点库中保存节点的配置、离线消息等，节点目录服务用语给用户分配企信服务节点及其地址信息、域信息，即时通信服务给用户提供 XMPP 长连接消息服务，用于企信在线 / 离线消息的推送及接收。

企信即时通信服务流程如下：客户端使用已注册的账号进行登录，通过企信全局库获取用户信息进行认证，与企信即时通信服务节点建立长连接，查询企信全局库，获取用户通信录及离线消息。

当用户向目标用户发送消息时，首先将消息发送到节点服务器。节点服务器从缓存服务器中查询目标用户域，若不存在，则从企信全局库中查询。在缓存中查找目标域的地址，将消息发送到目标节点服务器。目标节点服务器判断目标用户是否在线，若在线将消息发送到目标用户，否则，将消息保存到离线消息全局库。

节点可动态扩展，可根据用户量和使用情况增加相应的服务，单节点故障不影响企信的正常使用。节点间通信通过节点间通信服务进行消息的转发。

5 结语

本文从企业即时通信的角度出发，提出了一套完整的基于多用户模型的电力企业级即时通信系统。该即时通信系统通过端对端加密来保证客户端与客户端之间通信的安全性；通过建立 Openfire 集群来满足大规模用户即时通信的高性能需求；通过建立跨节点分布式 Openfire 服务来提高系统性能和稳定性。经实践验证，该即时通信系统具有较好的消息安全性和可扩展性，能够有效保证多用户模型下系统的高效性和可靠性，较好地满足了公司的即时通信需求。

参考文献：

[1] NARDI B A, WHITTAKER S, BRADNER E. Interaction and outeraction: instant messaging in action[C]// Proceedings of the 2000 ACM Conference on Computer Supported Cooperative Work, 2000.

[2] DAY M, ROSENBERG J, SGANO H. A model for presence and instant messaging[R]. 2000.

[3] 来天平, 杨旭, 彭一明, 等. 基于XMPP协议的高校WEB即时通信系统的应用与集成研究[J]. 华东师范大学学报(自然科学版), 2015(S1): 360-367.
LAI Tian-ping, YANG Xu, PENG Yi-ming, et al. The construction and integration of university WEB instant communication application based on XMPP protocol[J]. Journal of East China Normal University(Natural Science), 2015(S1): 360-367.

[4] 袁宾奇. 基于XMPP的跨平台即时通信软件库的设计与实现[D]. 南京: 南京大学, 2013.

[5] 周士雄. 基于XMPP协议的移动平台即时通信系统的设计与实现[D]. 哈尔滨: 哈尔滨工业大学, 2013.

[6] OZTRUK O. Introduction to XMPP protocol and developing online collaboration applications using open source software and libraries[C]// Collaborative Technologies and Systems(CTS), 2010 International Symposium on. IEEE, 2010.

[7] SHARMA M. Openfire administration[M]. UK: Packt Publishing Ltd., 2008.

[8] BRAY T, PAOLI J, SPERBERG-McQUEEN C M, et al. Extensible markup language(XML)[EB/OL].[2016-08-20] World Wide Web Consortium Recommendation REC-xml[1998-02-10]. http://www.w3.org/TR/1998/REC-xml.

[9] 崔思哲. 基于XMPP协议的移动即时通信应用的性能优化[J]. 软件, 2016, 36(2): 163-165.
CUI Si-zhe. The optimization of instant messaging applications based on XMPP protocol[J]. Computer Engineering & Software, 2016, 36(2): 163-165.

[10] 兰素秋. 基于XMPP协议的IM系统在企业信息化中的应用研究[D]. 成都: 成都理工大学, 2010.

[11] 王璐. Web模式下基于XMPP的即时通信系统的设计与实现[D]. 北京: 北京邮电大学, 2010.

[12] SAINT-ANDRE P, ALKEMADE T. Use of transport layer security(TLS) in the extensible messaging and presence protocol(XMPP)[R]. 2015.

[13] 杨海, 赵文涛, 张乃千, 等. 基于Android的自主可控即时通信系统的设计与实现[J]. 电子设计工程, 2015, 23(6): 67-70.
YANG Hai, ZHAO Wen-tao, ZHANG Nai-qian, et al. Design and implementation of independent controllable instant message communication system based on Android[J]. Electronic Design Engineering, 2015, 23(6): 67-70.

编辑　张钦芝
收稿日期：2016-08-20


王纪军

作者简介：

王纪军（1976–），男，江苏靖江人，高级工程师（研究员级），从事电力通信技术研究与管理工作；

李夫宝（1984–），男，江苏徐州人，高级工程师，从事计算机软件开发工作；

王京（1988–），女，河南舞阳人，工程师，从事移动互联软件开发工作。

Research and Application of Instant Messaging System Based on Multi-user Model

WANG Ji-jun, LI Fu-bao, WANG Jing
(Ministry of Information Technology, State Grid Jiangsu Electric Power Company, Nanjing 210008, China)

Abstract: With the development of mobile Internet technology and smart terminals, it is necessary to construct an enterprise-level instant messaging system based on multi-user model. This paper proposed a reliable and efficient solution for enterprise-level instant messaging system based on XMPP and Openfire. The security of communication is guaranteed using an end to end method of encryption. In addition, an Openfire cluster is designed to meet the demands of large-scale users. What's more, distributed server groups that span nodes are built to improve the stability of system. Practice shows that the system has good information security and scalability. It can guarantee the security and effectiveness of communication between large-scale users, meet the instant messaging demands of enterprise -level.

Key words: XMPP; Openfire; instant messaging; end to end encryption; cluster; span-node