



دانشگاه صنعتی اصفهان  
دانشکده مهندسی برق و کامپیوتر

اینترنت اشیا

گزارش پروژه ی کارشناسی

محمد مهدی امینی

استاد

دکتر منشی

## فهرست مطالب

عنوان	صفحه
فهرست مطالب	دو
فهرست تصاویر	سه
فهرست جداول	چهار
فصل اول : XMPP	پنج
۱-۱ معرفی	پنج
۱-۱-۱ معماری کلی	شش
۱-۱-۲ بر اساس XML	هفت
۱-۱-۳ لایه ی انتقال	هفت
۱-۱-۴ امنیت	هشت
۱-۱-۵ آدرس ها در XMPP	هشت
۱-۱-۶ افزونه ی Jingle	نه
۱-۱-۷ اینترنت اشیا	نه

## فهرست تصاویر

- ۱-۱ معماری کلی XMPP . . . . . شش
- ۲-۱ شمای کلی ی کارکرد سرور ها و gateway ها . . . . . شش
- ۳-۱ تصویر یک مکالمه ی ساده بین ۲ موجودیت را نشان می دهد که حداقل یک سرور باید در هر مکالمه حضور داشته باشد. در مرحله ی ایجاد شدن مکالمه، کلاینت ها درباره ی مسایل مختلفی مثل اهراز هویت و رمز نگاری توافق های لازم را انجام می دهند. . . . . هفت

## فهرست جداول

۱-۱ بررسی Poll یا Push بودن روش های حل مساله ی اطلاع رسانی . . . . . پنج

## فصل اول

### XMPP

#### ۱-۱ معرفی

Extensible Messaging and Presence Protocol (XMPP) یک پرتوکل ارتباطی لایه کاربرد است که بر قراری ارتباط به صورت Messaging را ممکن می سازد. این پرتوکل به عنوان امن ترین پرتوکل در نوع خود شناخته می شود و سعی شده مسایل مربوط به حریم شخصی نیز در طراحی آن در نظر گرفته شود. از میان کاربردهای مختلف آن می توان به موارد زیر به عنوان شاخص ترین ها یاد کرد:

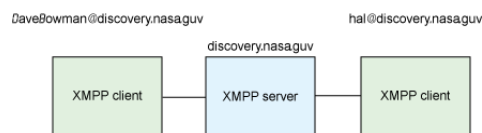
نوع	مثال
پایه Signaling	instant messaging, presence, multi-party chat, remote systems monitoring
انترنت اشیا publish-subscribe	gaming transfer, file video, VoIP, for signalling smart grid, and social networking services news feeds, geolocation, workflow systems, network management systems

جدول ۱-۱: بررسی Push یا Poll بودن روش های حل مساله ی اطلاع رسانی

بسیاری از سرویس های چت مثل Google Talk و WastsApp از این پرتوکل بهره جسته اند.

## ۱-۱-۱ معماری کلی

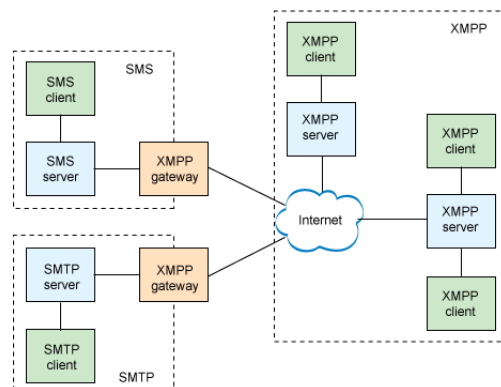
در معماری این پرتوکل هر کلاینت با یک نام که مختص خود اوست شناخته می شود که برای کلاینت ها امکان صحبت با یکدیگر را فراهم می کند. هر مجموعه کلاینت در قالب یک Domain (دامنه) و از طریق یک سرور به یکدیگر متصل هستند. کلاینت ها برای ارتباط با یکدیگر محدود به دامنه ی خودشان نیستند و میتوانند با کلاینت ها در دامنه های دیگر نیز ارتباط برقرار کنند.



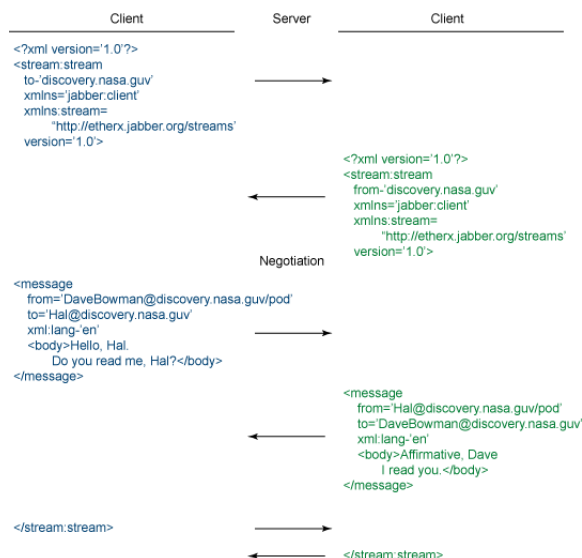
شکل ۱-۱: معماری کلی XMPP

سرور های دامنه های مختلف به منظور مسیر یابی بین دامنه ای، با یکدیگر صحبت می کنند. هر شخص به صورت آزادانه می تواند یک سرور XMPP راه اندازی کند. در واقع در این پرتوکل به یک سرور مرکزی رسمی نیاز نیست.

در معماری این پرتوکل موجودیت هایی به نام Gateway وجود دارند که امکان ارتباط سیستم های مبتنی بر XMPP با سیستم های مبتنی بر پرتوکل های دیگر را فراهم می کند. برای مثال یک Gateway می تواند پیام هایی که در قالب SMS هستند را به قالب XMPP تبدیل کرده و به برای کلاینت ها ارسال کند. Gateway ها توانایی ایجاد Session جدید و از بین بردن Session غیر قابل استفاده را دارند که باعث می شود عمل اهراز هویت کلاینت ها در سیستم های مبتنی بر پرتوکل های مختلف به صورت خودکار انجام شود.



شکل ۱-۲: شمای کلی ی کارکرد سرور ها و gateway ها



شکل ۱-۳: تصویر یک مکالمه ی ساده بین ۲ موجودیت را نشان می دهد که حداقل یک سرور باید در هر مکالمه حضور داشته باشد. در مرحله ی ایجاد شدن مکالمه، کلاینت ها درباره ی مسایل مختلفی مثل اهراز هویت و رمز نگاری توافق های لازم را انجام می دهند.

#### ۱-۲-۱ بر اساس XML

داده هایی که بین موجودیت های این پرتوکل تبادل می شوند در قالب XML هستند. بین هر دو موجودیت یک XML Stream ایجاد می شود. این Stream در واقع ۲ ارتباط یک طرفه است که همزمان بین ۲ موجودیتی که باهم صحبت می کنند برقرار است. با توجه به متن محور بودن XML سربار شبکه ی XMPP در حالت عادی زیاد تر از پرتوکل هایی است که داده ها را به صورت باینری ارسال می کنند. برای رفع این مشکل داده های XML را به صورت بهینه در قالب باینری serialize کرده و سپس ارسال می کنند. همچنین به دلیل متن محور بودن پرتوکل امکان ارسال داده های باینری با حجم بالا وجود ندارد. در عمل برای ارسال داده های باینری ابتدا باید آنها به قالب Base6۲ در آورد.

#### ۱-۳-۱ لایه ی انتقال

پرتوکی که به عنوان لایه ی انتقال XMPP به صورت پیش فرض در نظر گرفته شده است، TCP است. موجودیت هایی که قصد صحبت دارند ۲ ارتباط بلند مدت TCP همزمان برقرار می کنند. استفاده از TCP در مواردی مثل حضور کلاینت ها در پس دیوار آتش، گاهی ممکن نیست. در این مواقع از HTTP به عنوان Application layer transport protocol استفاده می شود که امکان برقراری ارتباط و حتی اهراز هویت کلاینت ها از طریق وب و پورت ۸۰ را فراهم می کند. در زمانی که از HTTP به عنوان پرتوکل لایه ی انتقال استفاده شود در واقع روش Bidirectional-streams Over Synchronous HTTP (BOSH) به کار گرفته می شود که ایجاد یک Stream دو طرفه ی HTTP است بین ۲ موجودیتی که قصد صحبت دارند. این روش امکان ارسال پیام به

صورت Notification با الگوی Push را فراهم می کند که کاملاً بهینه تر از الگوی سنتی Poll است.

در روش Poll سمتی که منتظر محتوای جدید است به طور مداوم (چند وقت یکبار) با ایجاد یک ارتباط جدید درباره ی وجود محتوای جدید سوال می کند و سپس ارتباط را قطع می کند. این روش به اطلاق شدید منابع ۲ طرف ارتباط منجر می شود. اما در الگوی Push طرفی که منتظر دریافت محتوای جدید است یک ارتباط بلند مدت با طرف منتشر کننده ی محتوا ایجاد می کند و سعی می کند این ارتباط را حفظ کند. در زمانی که محتوای جدید در دسترس بود، طرف منتشر کننده، محتوا را در کانال موجود ارسال میکند.

جایگزین به ظاهر بهینه تر، برای TCP، استفاده از وب سوکت به عنوان لایه ی انتقال است که امکان برقراری ارتباط کاملاً دو طرفه ی همزمان روی یک ارتباط TCP را می کند. تفاوت این روش با روش دوم، استفاده از یک ارتباط TCP بجای دو ارتباط همزمان است.

#### ۴-۱-۱ امنیت

بر خلاف دیگر پرتوکل های پیام رسانی، این پرتوکل به مسایل امنیتی در هسته ی خود توجه کرده است به طوری که اهراز هویت امن به کمک SALS و ارسال داده ها به صورت رمز شده به کمک TLS را به صورت پیش فرض و البته اختیاری در دسترس قرار می دهد.

#### ۵-۱-۱ آدرس ها در XMPP

آدرس ها یا Jabber ID ها در XMPP شبیه استاندارد ایمیل هستند با اندکی تفاوت تاثیر گذار. ساختار آدرس ها به شکل

[ resource "/" ] domain [ "@" node ]

DavidBowman@discovery.nasa.gov/terminal

که بخش Node و Resource اختیاری و بخش Domain اجباری است. قسمت Node نام الصاق شده به کلاینت، قسمت Domain نمایانگر شبکه ای که کلاینت در آن حضور دارد و قسمت Resource نام مکان ها یا دستگاهایی است که به کلاینت مرتبط هستند. این ساختار امکان وارد شدن یک کاربر به سرور XMPP بیش از یکبار را فراهم می کند. برای مثال یک ورود از طریق موبایل و یک ورود در زمان مشابه با دستگاه موقعیت یاب خودرو. بخش Resource نمایانگر موقعیت مکانی است که کلاینت از آن قصد ورود به سرور را دارد. که به واسطه ی آن کاربران در صورت تمایل می توانند ورود های کلاینت هایشان به سرور XMPP را از نظر مکانی دنبال کنند. البته resource ها چیزی بجز تگ های از پیش مشخص شده نیستند. با توجه به



اینکه مکان یابی (Routing) پیام های XMPP بر اساس JID و مستقل از IP انجام می شود، این پرتوکل گزینه ی مناسبی برای ایجاد Overlay روی شبکه های موجود است.

#### ۶-۱-۱ افزونه ی Jingle

یکی از افزونه های معروفی که برای XMPP طراحی شده، Jingle نام دارد که امکان Signaling برای انتقال فایل، صدا و تصویر و دیگر کاربرد ها را فراهم می کند. در واقع Jingle یک ابزار برای ایجاد و مدیریت جلسه های مبتنی بر Multimedia است که در دایره ی وسیعی از Application ها استفاده می شود و زمینه برای بکار گیری پرتوکل هایی مثل RTP را فراهم میکند.

#### ۷-۱-۱ اینترنت اشیا

ویژگی های XMPP مثل توانایی صحبت با سیستم هایی مبتنی بر پرتوکل های دیگر به واسطه ی Gateway ، پشتیبانی از الگوی publish/subscribe و پشتیبانی از اهراز هویت و رمز نگاری حتی برای کلاینت های موبایلی، آن را گزینه ی مناسبی برای بخش های متفاوتی از کاربرهای اینترنت اشیا کرده است.

## کتاب نامه

- [1] Washer, Peter. *Learning Internet of Things*. Packt, 2015.
- [2] XMPP. [Xmpp.org](http://xmpp.org).
- [3] Margaret Rouse, UART. [what-is.techtarget.com/definition/uart-universal-asynchronous-receiver-transmitter](http://what-is.techtarget.com/definition/uart-universal-asynchronous-receiver-transmitter), 2011.
- [4] M. Jones, Meet the Extensible Messaging and (XMPP), Presence Protocol. [www.ibm.com/developerworks/library/x-xmppintro/index.html](http://www.ibm.com/developerworks/library/x-xmppintro/index.html), 2009.