یازدهمین کنگره ملی سراسری
فناوریهای نوین در حوزه توسعه پایدار ایران
11th National Congress of
the New Technologies in Sustainable Development of Iran
senaconf.ir

بررسی پروتکل RPL در اینترنت اشیاء

مریم عیسوندی

دانشکده فنی مهندسی، دانشگاه لرستان، خرم‌آباد، maryam.isvandi@gmail.com

چکیده

اینترنت اشیاء یکی از پرکاربردترین و جذاب‌ترین تکنولوژی‌ها در آینده نزدیک می‌باشد که کاربردهای متفاوتی از قبیل شهر هوشمند، سلامت هوشمند و خانه هوشمند را در پی خواهد داشت. درکنارمزایای فوق العاده‌ی اینترنت اشیاء این فناوری با چالش‌های مختلفی روبرو است، یکی از اولین مشکلات تحقق این فناوری استفاده از دستگاه‌ها با توان پردازشی، ذخیره‌سازی و منبع انرژی ضعیف و همچنین مدل ترافیکی خاص در اینترنت اشیاء است. این امر موجب عدم سازگاری پروتکل‌های رایج مسیریابی در علم ارتباطات با این فناوری می‌شود. به همین خاطر پروتکل مسیریابی RPL به منظور رفع نیازهای مسیریابی در اینترنت اشیاء ایجاد گشت . RPL یک پروتکل مسیریابی بردار-فاصله برای شبکه‌های کم قدرت و با اتلاف است که از IPv6 استفاده می‌کند. دراین مقاله به بررسی این پروتکل مسیریابی و تشریح نحوه عملکرد آن پرداخته می‌شود.

واژه‌های کلیدی

اینترنت اشیاء، پروتکل، مسیریابی، RPL.

۱. مقدمه

مفهومی که ما از اینترنت در ذهن داریم یک شبکه‌ی جهانی است که در آن رایانه‌های شخصی، تلفن‌های همراه و غیره و همچنین انسان‌ها در هر جایی توسط این دستگاه‌های متصل به شبکه با هم ارتباط برقرار می‌کنند. حال دنیایی را در نظر بگیرید که در آن اینترنت از مفهوم فعلی خود فراتر رفته و اشیاء اطرافمان را نیز در خود جای می‌دهد؛ در اینجا مفهومی شکل می‌گیرد به نام اینترنت اشیاء[1]. اینترنت اشیاء، شبکه‌ای از اشیاء با قابلیت شناسایی واضح عناصر است که به کمک هوش نرم‌افزاری و حسگرها، امکان اتصال از هر مکان به اینترنت را داشته و با استفاده از زیرساخت‌های مخابراتی اینترنت، چیزها یا اشیاء را برای تبادل اطلاعات با تولیدکننده، اپراتور و یا سایر دستگاه‌های متصل، توانمند می‌سازد. این فناوری به اشیاء فیزیکی (برای ارائه‌ی اطلاعات خاص)، اجازه درک کردن و کنترل از راه دور از طریق اینترنت را می‌دهد و فرصت‌هایی برای یکپارچه‌سازی بیشتر بین دنیای فیزیکی و سیستم‌های کامپیوتری به وجود آورده که موجب بهبود کارایی، دقت و سود اقتصادی می‌شود.

همانند تمامی شبکه‌ها یکی از مسائل مهم در اینترنت اشیاء مسیریابی بسته‌ها است، مسیریابی به معنای انتخاب بهترین مسیر برای انتقال داده به مقصد موردنظر می‌باشد. بیشتر دستگاه‌هایIOT امروزه از میکروپردازنده‌ها و میکروپروسسورها استفاده می‌کنند و امکان ندارد قادر به پیاده‌سازی پروتکل‌های پیچیده مسیریابی مورد استفاده در اینترنت مانندBGP یا OSPF باشند، نمی‌توان انتظار داشت که درون لامپ‌های led که هوشمند هستند یک پردازنده قوی به همراه مقدار قابل توجهی RAM و ROM وجود داشته باشد. پس لازم است پروتکل‌های مورد استفاده در اینترنت اشیاء به نحوی طراحی شوند که در دستگاه‌هایی با مقدار حافظه و قدرت پردازشی محدود قابل پیاده‌سازی باشند. در ادامه پس از معرفی اجمالی اینترنت اشیاء و پروتکل‌های مختلف آن به بررسی و تحلیل نحوه عملکرد پروتکل مسیریابی RPL[2] می‌پردازیم.

۱،۱. مفاهیم پایه اینترنت اشیاء

اینترنت اشیاء شامل سنسورها و عملگرهایی است که در اشیاء فیزیکی جاسازی شده‌اند و از طریق شبکه‌های بی‌سیم یا باسیم به همدیگر متصل شده‌اند و اغلب از همان پروتکل اینترنت (IP) برای اتصال به اینترنت استفاده می‌کنند. یک شبکه IOT لزوما بخشی از اینترنتی که ما می‌شناسیم نیست. منظور از شیء هرآن چیزیست که کامپیوتر نباشد مثل ساعت، ترموستات، سنسورها، ماشین و این اشیاء مجهز به امکانات کامپیوتری می‌شوند تا بتوانند ارتباطات شبکه‌ای را برقرار کنند. این اشیاء از لحاظ منابع محدود هستند بدین معنی که قدرت پردازش آنها کم و حافظه اندک و باتری محدود دارند.

معماری اینترنت اشیاء نیز همانند معماری اینترنت از ساختار لایه‌ای پیروی می‌کند. در شکل ۱ یک معماری چهار لایه ای برای اینترنت اشیاء شامل لایه حسگرها ، لایه شبکه ، لایه مدیریت خدمات و لایه برنامه نشان داده شده است که در ادامه توضیحات مختصری از هر لایه خواهیم گفت[۱].

- **لایه حسگرها:** این لایه اتصال حسگر و شبکه را فراهم می‌کند و شامل فناوری‌ها و امکاناتی است که هدف اصلی این سطح، شناسایی دستگاه‌ها و بررسی اطلاعات جمع‌آوری شده از دنیای حقیقی به کمک سنسور مربوطه می‌باشد. اطلاعات در این لایه به صورت بلادرنگ جمع‌آوری و پردازش می‌شود. حسگرها بر اساس کاربرد و نوع های داده گروه‌بندی می شوند(نظیر حسگر های محیطی و حسگر های نظامی و حسگر های بدن و منزل)
- **لایه شبکه:** این لایه امکانات شبکه‌ای مورد نیاز را فراهم و فناوری‌های متعددی را استفاده می‌کند. هدف این سطح انتقال اطلاعات جمع‌آوری شده از سطح حسی به هر یک از سیستم‌های پردازش اطلاعاتی از طریق شبکه‌های مخابراتی موجود

---

[1] Internet of things

[2] Routing Protocol for Low Power and Lossy Networks

همچون اینترنت، شبکه موبایل یا دیگر شبکه‌های معتبر می‌باشد. این لایه باید از حجم بالای داده اینترنت اشیاء تولید شده توسط حسگرهای بی‌سیم و دستگاه‌های هوشمند حمایت کند. عملکرد این لایه صرف نظر از ماهیت شبکه (خصوصی، عمومی و یا ترکیبی) باید مطمئن و مستحکم باشد. حسگرهای اینترنت اشیاء به کمک فناوری‌های مختلف قادر به حمایت از پروتکل-های مختلف و شبکه‌های ناهمگون می‌باشند.

- **لایه مدیریت خدمات:** این لایه مسئولیت تجزیه و تحلیل اطلاعات، کنترل امنیت، مدلسازی فرآیندها و مدیریت دستگاه را بر عهده دارد. داده‌های حسگر اینترنت اشیاء که به طور متناوب ارسال می‌گردند نیازمند فیلترینگ می‌باشند چراکه حجم داده ارسالی بسیار زیاد است و لازم است با توجه به نوع خواسته، فرآیند فیلترینگ بر روی آنها اعمال شود. مدیریت جریان اطلاعات، دستیابی اطلاعات، یکپارچه‌سازی و مکانیزم‌های دستیابی به اطلاعات از دیگر وظایف مهم لایه‌ی سرویس معماری اینترنت اشیاء می‌باشد. سرویس‌های اینترنت اشیاء می‌بایست امنیت، حریم خصوصی، محرمانگی و یکپارچگی را تضمین نمایند که شامل تایید هویت و مجوز اشیاء به اشیاء ،تایید هویت و مجوز کاربر به کاربر، کنترل دستیابی شی به شی و غیره می‌باشد.
- **لایه برنامه:** این لایه کاربردهای عملی اینترنت اشیاء را بر اساس نیازهای کاربران و انواع مختلف صنایع از قبیل خانه هوشمند، محیط هوشمند، حمل و نقل هوشمند، بیمارستان هوشمند و غیره را شناسایی و تحقق می‌بخشد. برنامه‌ها را می‌توان بر اساس نوع شبکه در دسترس، همگرایی، اندازه، مدل کسب و کار، نیازهای بلادرنگ و...گروه بندی کرد. ابعاد شبکه، پهنای باند مورد نیاز و نوع اتصال به شبکه در برنامه‌های اینترنت اشیاء متفاوت است و هریک ملزومات مختص به خود را دارا می‌باشند. آشنایی با نیازهای هر برنامه در ایجاد زیرساخت لازم و بکارگیری فناوری مناسب در هر لایه بسیار ضروری است.

شکل ۱. معماری چهار لایه اینترنت اشیاء[۱]

۲. بررسی پروتکل‌ها و استانداردهای اینترنت اشیاء در لایه‌های مختلف

اینترنت اشیاء تأثیر شگرفی بر جنبه‌های مختلف زندگی بشر خواهد داشت، لذا لازم است برای ارتباطات بین اشیاء مختلف پروتکل‌ها و فناوری‌های مناسبی انتخاب گردد. پروتکل ها و استانداردهای زیادی تا به حال ارائه شده است تا کار فراهم‌کنندگان سرویس و برنامه نویسان را ساده‌ترکند. به این منظور گروه‌های زیادی ایجاد شده‌اند تا پروتکل‌هایی را در حمایت از اینترنت اشیاء ارائه دهند. همچون W3C, IETF, EPCglobal, IEEE, ETSI. جدول ۱ نمونه‌هایی از پروتکل های اینترنت اشیاء در لایه‌های مختلف را نشان می‌دهد [۲-۶]. همانطور که در جدول ۱ مشخص است هر یک از چهار لایه در معماری چهار لایه‌ای اینترنت اشیاء پروتکل‌های مختص خود دارند که در این مقاله به بررسی پروتکل RPL پرداخته می‌شود. RPL یک پروتکل مسیریابی اینترنت است که برای شبکه‌های حسگر بیسیم توسط کارگروه مهندسی اینترنت مشخص‌شده است. این پروتکل که همچنین به‌عنوان پروتکل لایه شبکه شناخته می‌شود پروتکل مسیریابی بردار-فاصله برای شبکه‌های کم قدرت و با اتلاف است که از IPv6 استفاده می‌کند [۷]. در قسمت بعد به تشریح نحوه عملکرد این پروتکل پرداخته می‌شود.

جدول ۱. نمونه‌هایی از پروتکل‌های اینترنت اشیاء[۲]

Application Protocol		DDS	CoAP	AMQP	MQTT	MQTT-NS	XMPP	HTTP REST
Service Discovery		mDNS				DNS-SD		
Infrastructure Protocols	Routing Protocol	RPL						
	Network Layer	6LoWPAN					IPv4/IPv6	
	Link Layer	IEEE 802.15.4						
	Physical/ Device Layer	LTE-A	EPCglobal	IEEE 802.15.4		Z-Wave		
Influential Protocols		IEEE 1888.3, IPSec					IEEE 1905.1	

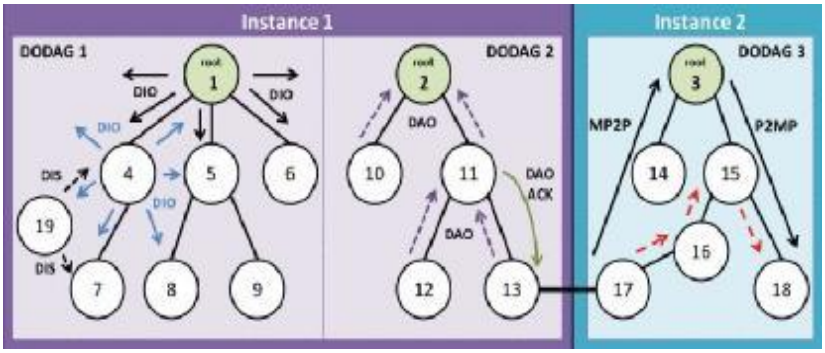
۳.پروتکل مسیریابی RPL

RPL یک پروتکل مسیریابی بردار- فاصله[۳] با رویکرد پیشگیرانه و براساس IPv6 میباشد که توسط انجمن IETF طراحی و در سند استاندارد RFC 6550 استاندارد شده است. RPL به طور خاص برای کاربردهای جمع‌آوری داده (به عنوان مثال الگوی ترافیک MP2P[۴]) بهینه سازی شده است .همچنین پشتیبانی از الگوی ترافیک P2MP[۵] را فراهم میکند در حالی که پشتیبانی غیرمستقیم برای الگوی P2P[۶]را نیز فراهم می‌کند. RPL با چهار سناریوی متفاوت توسعه داده شده است: شبکه های شهری، اتوماسیون ساختمان، اتوماسیون صنعتی و اتوماسیون خانگی.این پروتکل در لایه‌ی networking عمل می‌کند و چندین تکنولوژی لایه‌ی link از جمله IEEE 802.15.4را پشتیبانی می‌کند [۸].

RPL مبتنی بر مفهوم توپولوژی گراف بدون دور جهت‌دار[۷] است و در واقع شبکه فیزیکی خود را به صورت DAG سازماندهی می‌کند. DAG یک ساختار درخت مانندی تعریف می‌کند که مسیرهای پیش‌فرض بین گره‌ها را مشخص می‌کند. بااین‌حال، یک ساختار DAG بیش از یک درخت معمولی است، در DAG یک گره ممکن است چند والد داشته باشد اما در مقابل، در درخت‌های کلاسیک فقط یک والد می‌تواند داشته باشند. درواقع RPL گره‌ها را به‌صورت DAG مقصدگرا یا ریشه‌گرا (DODAG)[۸]سازمان‌دهی می‌کند که گره‌های مقصد یک مسیر پیش‌فرض به درگاه اینترنت به عنوان ریشه‌های DAG فراهم می‌کنند. یک شبکه ممکن است شامل یک یا چند DODAG باشد که با همدیگر یک نمونه[۹] RPL با یک شناسه واحد مشخص می‌کنند. یک شبکه ممکن است چند نمونه RPL را به‌طور هم‌زمان اجرا کنند اما این نمونه‌ها به‌طور منطقی مستقل از هم هستند. یک گره ممکن است به چند نمونه RPL متصل شود اما باید تنها به یک DODAG داخل هر نمونه متعلق باشد. یکی از ویژگی‌های پروتکل مسیریابی RPL این است که هر دو توپولوژی مش و سلسله

[3] Distance-Vector
[4] Multipoint to Point
[5] Point to Multipoint
[6] Point to Point
[7] Directed Acyclic Graph (DAG)
[8] Destination-Oriented DAG
[9] Instance

مراتبی را ادغام می‌کند. ازیک‌طرف، یک توپولوژی شبکه مبتنی بر RPL ذاتاً سلسله مراتبی است، به‌طوری‌که گره‌های اساسی را مجبور به خودسازمانی به عنوان یک یا چند DODAG برمبنای روابط والد به فرزند، می‌کند. از سوی دیگر، RPL توپولوژی مش را پشتیبانی می‌کند به‌طوری‌که اجازه می‌دهد هر زمان که موردنیاز است مسیریابی به‌جای والدها و فرزندان از طریق گره‌های با والد مشترک انجام شود. این ترکیب مش و سلسله مراتبی انعطاف‌پذیری بزرگی ازنظر مدیریت توپولوژی و مسیریابی فراهم می‌کند[۸]. شکل ۲ مثالی از یک شبکهRPL متشکل از دو نمونه و سه DODAG را نشان می دهد.



شکل ۲. مثالی از شبکه RPL با دو نمونه و سهDODAG [۸]

نام دیگر ریشه گراف، LBR [۱۰]می‌باشد که ترافیک درون دامنه شبکه را به سایر دامنه‌های IPv6 مثل اینترنت متصل می‌کند. بسته‌های RPL می‌توانند بر اساس سه الگوی ترافیکی ارسال شوند که در شکل۲ در DODAG سوم نشان داده‌شده است:

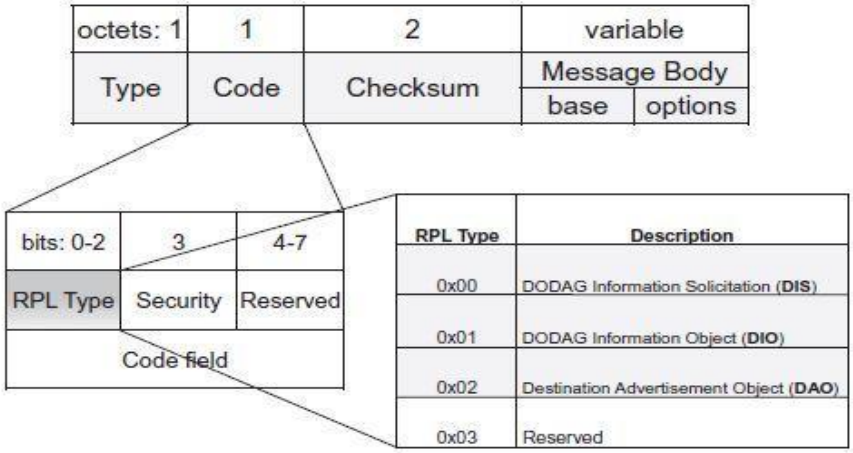
- ترافیک چندنقطه‌ای به تک نقطه‌ای از برگ‌ها به سمت ریشه با استفاده از مسیرهای روبه بالا
- ترافیک تک نقطه‌ای به چندنقطه‌ای از ریشه به سمت برگ‌ها با استفاده از مسیرهای رو پایین
- ترافیک نقطه‌به‌نقطه با خطوط خط‌چین قرمزرنگ و با استفاده از هر دو مسیر رو به بالا و رو به پایین

مسیرهایی که ترافیک را از گره‌های معمولی یا برگ‌ها به LBR یا ریشه (به طور مثال ترافیک MP2P) منتقل می‌کنند، مسیرهای رو به بالا نامیده می‌شوند در حالی‌که مسیرهایی که ترافیک را از ریشه DODAG به سایر گره‌ها(به طور مثال ترافیک P2MP) منتقل میکنند، مسیرهای رو به پایین نامیده می‌شوند. برای ساختن مسیرهای رو به بالا، هر گره‌ی درون شبکه باید یکی از همسایگانش را به عنوان والد مقدم(قدم بعدی)به سمت ریشه انتخاب کند .به طور مشابه، هر گره‌ای که مایل به شرکت در مسیریابی رو به پایین است باید خودش را به یکی از والدهایش ترجیحا والد مقدم اعلام کند. جزئیات ساخت مسیرهای رو به بالا و رو به پایین را در بخش‌های بعدی نشان می‌دهیم.

۱،۳. پیام‌های کنترلیRPL

پیام‌های RPL به‌عنوان نوع جدیدی از پیام‌های کنترل ICMPv6 مشخص‌شده است که ساختار آن در شکل ۳ نشان داده شده است.

[10] LLN Border Router



شکل۳. پیام کنترل RPL

پیام کنترل RPL متشکل است از: ۱. یک سرایند ICMPv6 که شامل سه فیلد نوع، کد و Checksum است. ۲. یک بدنه پیام شامل یک پیام پایه و یک تعداد option هست. فیلد نوع، نوع پیام کنترل ICMPv6 را مشخص می‌کند که ۱۵۵ در مورد RPL تنظیم می‌شود (تائید شده توسط IANA). فیلد کد، نوع پیام کنترل RPL را مشخص می‌کند. برای تبادل اطلاعات مسیریابی مورد نیاز برای ساخت توپولوژی شبکه و مسیرها، RPL چهار نوع پیام کنترلی از نوعICMPv6 (به استثنای پیام‌های امنیتی) معرفی می‌کند که در زیر شرح داده شده است:

DODAG Information Object (DIO): هر پیام DIO شامل سه قسمت اطلاعات اساسی میباشد: شماره نسخه DODAG ، معیار مسیریابی و رتبه فرستنده .این پیام شامل اطلاعات شبکه است که به یک گره اجازه می‌دهد که یک نمونهRPL را پیدا کند، پارامترهای پیکربندی آن را یاد بگیرد و انتقال دهد، به یکDODAG خاص متصل شود، مجموعه‌ای از والدهای کاندید را انتخاب کند و DODAG را حفظ و نگهداری کند.

Destination Advertisement Object (DAO): یک بسته‌ی DAO برای انتشار دادن اطلاعات مقصدش به طرف بالا و در طول DODAG به سمت ریشه استفاده می‌شود به طوری‌که مسیرهای رو به پایین از ریشه به گره‌های مرتبط ساخته می‌شود .پیام توسط یک فرزند برای اعلان کردن آدرس‌ها و پیشوندهای آنها، به والد انتخاب شده فرستاده می‌شود و یک پیام تک پخشی است .در حالت storing ، DAO به صورت تک پخشی برای والدهای انتخاب شده فرستاده می‌شود .در حالت non-storing ، این پیام برای ریشه، تک پخشی است.

DODAG Information Solicitation (DIS): این پیام توسط یک گره RPL برای درخواست یک DIO از گره‌های همسایه به منظور اتصال به DODAG استفاده می‌شود.

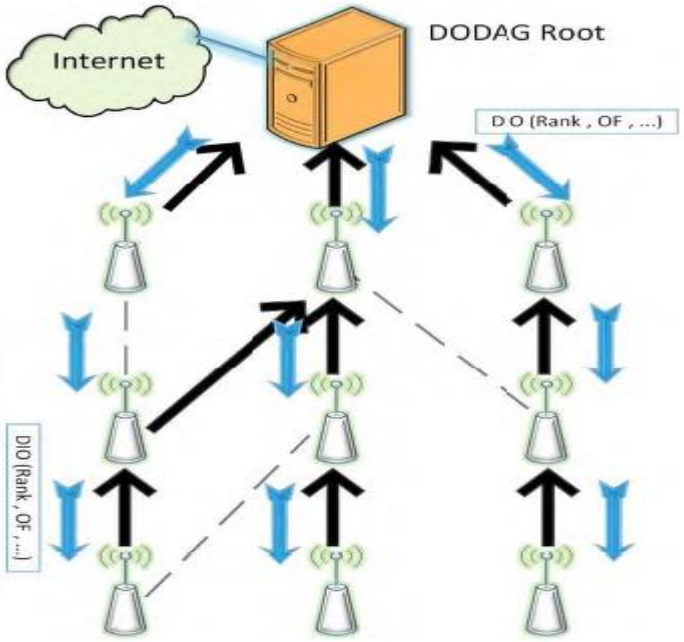
Destination Advertisement Object Acknowledgement (DAO-ACK): این پیام به صورت تک پخشی است و برای تصدیق دریافت DAO ، توسط یک دریافت کننده DAO به فرستنده DAO فرستاده می‌شود.

۲،۳. مسیرهای رو به بالای RPL

در RPL فرآیند ساخت DODAG و مسیرهای رو به بالا توسط پیام‌های DIO کنترل می‌شود. علاوه بر سایر اطلاعات مسیریابی، پیام-های DIO ، رتبه که موقعیت نسبی گره با توجه به ریشه DODAG می‌باشد، و سیاست مسیریابی که تابع هدف[11] (OF) نامیده می-

[11] Object Function

شود را انتقال می‌دهد . تابع هدف مشخص می‌کند که چگونه یک گره رتبه خود را محاسبه می‌کند و والد مقدمش را انتخاب می‌کند. در RPL، مسیرهای رو به بالا از هر گره به ریشه DODAG برای تسهیل ارتباط MP2P ساخته می‌شوند . به طور مشخص، ساخت DODAG توسط ارسال پیامهای DIO از ریشه به همسایگانش آغاز می‌شود. ریشه در این پیام، رتبه خود و تابع هدفی که باید استفاده شود را اعلام می‌کند .هنگام دریافت DIO ، گره ، در مرحله اول: آدرس فرستنده را در مجموعه والد کاندیدش(گروهی از گره‌هایی که رتبه ای کمتر از رتبه‌ی فعلی گره درون یک نمونه خاص RPL را دارند) اضافه می‌کند، در مرحله دوم: رتبه خود را محاسبه می‌کند، در مرحله سوم: والد مقدمش را از بین والدهای کاندید انتخاب می‌کند، و در نهایت،DIO دریافتی را با رتبه خود به روز رسانی می‌کند و سپس رتبه محاسبه شده را به سایر گره‌های همسایه ارسال می‌کند. هر گره‌ای مجموعه‌ای از همسایه‌های یک قدمی را دارد، که مجموعه همسایه‌ی کاندید نامیده می‌شود .گره همچنین می‌تواند DIO دریافتی را براساس برخی معیارهای تعریف شده در مشخصات RPL نادیده بگیرد .این فرآیند ادامه دارد تا زمانی که تمام گره‌ها مسیرهایشان را در جهت رو به بالا به سمت ریشهDODAG ایجاد کنند .زمانی‌که گره، مقداری داده برای ارسال به ریشه دارد، فورا داده‌ها را به والد مقدم ارسال می‌کند .گره‌ی والد داده‌ها را به والد خودش ارسال می‌کند و فرآیند به همین ترتیب ادامه می‌یابد تا زمانی‌که به ریشه‌یDODAG برسد .در شکل ۴، روند انتشار پیام‌های DIO که توسط ریشه آغاز می‌شود، نشان داده شده است، همچنین توپولوژی DODAG و مسیرهای رو به بالا را نشان می‌دهد که پیکان مشکی پر رنگ از فرزند به والد مقدم می‌باشد و خط چین، والد کاندید دیگر را نشان می‌دهد[۸].



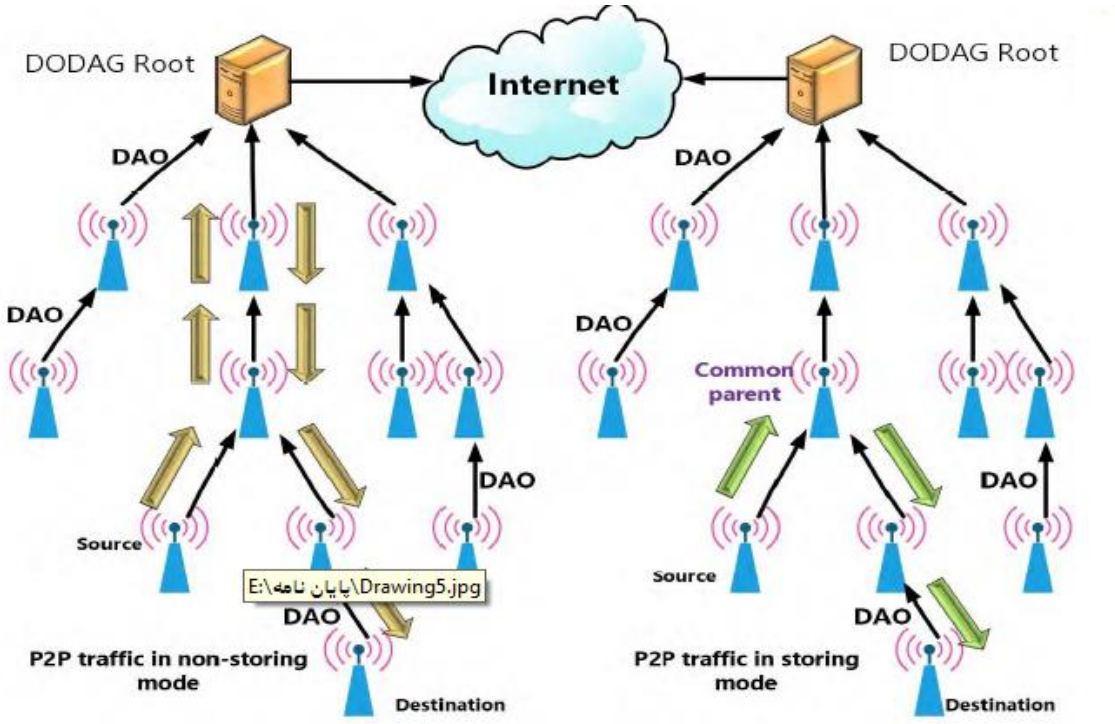
شکل۴. مسیریابی رو به بالا

۳،۳. مسیرهای رو به پایینRPL

به منظور تسهیل ابرتباط P2MP و P2P باید مسیرهای رو به پایین ایجاد و نگهداری شوند. RPL برای این هدف از پیام‌های DAO استفاده می‌کند .گره‌ای که مایل است خود را به عنوان یک مقصد قابل دستیابی از دیدگاه ریشه اعلام کند، یک DAO به صورت تک پخشی به والد مقدمش ارسال می‌کند که در آن پیشوند مقصدش را اعلام می‌کند . پردازش DAO دریافتی توسط والد به حالت عملیات فعلی اعلام شده در پیام‌های DIO وابسته است. برای این منظور، RPL دو حالت برای ایجاد و نگهداری مسیرهای رو به پایین به نام‌های storing (table-driven)و non-storing (source routing) مشخص می‌کند .در حالت ذخیره‌سازی (storing) هنگامی که یک والد یک DAO از یکی از فرزندانش دریافت می‌کند ابتدا پیشوند مقصد اعلام شده را به صورت محلی در جدول مسیریابی اش همراه با آدرس

فرستنده DAO ، به عنوان قدم بعدی برای رسیدن به آن مقصد ذخیره میکند؛ و سپس DAO دریافتی را برای تضمین انتشار مقصد اعلام شده به طرف بالا به سمت ریشه DODAG به والد مقدمش ارسال می‌کند.

در حالت غیرذخیره سازی (non-storing) ، DAO منتشر شده همچنین آدرس والد مقصد را علاوه بر پیشوند مقصد اعلام شده منتقل می‌کند .در اینجا، والدی که یک DAO دریافت می‌کند فقط آن را به والد مقدمش بدون نگهداری هیچ حالت مسیریابی ارسال می‌کند تا زمانی‌که در نهایت توسط ریشه DODAG دریافت شود .به محض اینکه ریشه DODAG ، پیام DAO ارسالی را دریافت می-کند، اطلاعات دریافتی را در جدول مسیریابی اش به شکل رابطه والد - فرزند نگهداری می‌کند . بنابراین هنگامی که ریشه نیاز به برقراری ارتباط با یک مقصد مشخص را دارد، مسیر مبدا آن مقصد را به هدر بسته ضمیمه میکند و بسته را به قدم بعدی ارسال میکند. گره‌ای که آن بسته را دریافت می‌کند، به سادگی هدر مسیریابی مبدا را برای تعیین اینکه بسته را باید روی چه اینترفیسی ارسال کند، بررسی خواهد کرد .RPL همچنین پشتیبانی از الگوی ترافیکی P2P را فراهم می‌کند که در آن، یک گره با گره دیگر در شبکه ارتباط برقرار می‌کند .بنابراین، زمانی که یک گره نیاز به ارسال یک بسته به گره دیگر درون DODAG را دارد، بسته در ابتدا به طرف بالا و به سمت DODAG ارسال می‌شود تا زمانی که آن به یک جد(نیا)برسد که مسیر شناخته‌شده ای به گره مقصد دارد . این گره جد، همان جد مشترک مبدا و مقصد می‌باشد که در شکل ۵ مشاهده می‌کنید .سپس بسته توسط آن جد از طریق مسیریاب‌های میانی به سمت پایین DODAG و در نهایت به گره مقصد ارسال می‌شود .در شکل ۵ ، انتشار پیامهای DAO و دو حالت عملیاتی شبکه و جریان بسته بین دو گره در ترافیک نقطه به نقطه نمایش داده شده است[۸].



شکل۵. مسیریابی رو به پایین

۴. اهمیت IPv6 در اینترنت اشیاء

امنیت و یکپارچگی مهم‌ترین مسائل در فضای شبکه مبتنی بر اینترنت اشیاء می‌باشند، که در آن ارتباطات امن بدون دخالت ضروری است. برای تشدید و ایجاد درجات بالاتری از امنیت، نیاز است که برای سناریوهای اینترنت اشیاء، حتما IPv6 پیاده‌سازی شود، که از رمزنگاری دو گانه پویا در هنگام تولید کلید و اصالت سنجی نیز برخوردار باشد. روش مبتنی بر IPv6 می‌تواند با الگوریتم‌های کاملا امن

فعال گردد، که نسبت به دخالت خارجی مصون می‌باشند. با افزایش پیاده سازی اینترنت اشیاء در عرصه‌های گوناگون، کار کردن بر روی جنبه‌های امنیتی اینترنت اشیاء ضروری می‌شود، این مهم با اطمینان یافتن از امنیت مسیرهای بسته‌ها جهت جلوگیری از تجاوز، و مطمئن شدن از امن بودن ارسال‌ها و دریافت‌ها قابل دستیابی است [۱۱-۹].

۵. نتیجه‌گیری

در این مقاله به بررسی و مطالعه‌ی ساختار پروتکل RPL پرداخته شد. همزمان با ارائه پروتکل RPL و به دلیل اهمیت فراوان امنیت اطلاعات در اینترنت اشیا، پژوهشگران بسیاری به بررسی حفره‌های امنیتی این پروتکل پرداخته و با گذشت زمان آسیب‌پذیری‌های متعددی در آن یافت شد. در صورت به خطر افتادن امنیت این پروتکل، امنیت دنیای اینترنت اشیاء را به خطر می‌اندازد. این پروتکل دارای نقاط ضعف امنیتی می‌باشد که نمی‌توان آن‌ها را هنگام استفاده نادیده گرفت. آشنایی با ساختار و نحوه‌ی عملکرد پروتکل به شناخت نقاط ضعف و مزایا و معایب آن کمک می‌کند. تحقیقات زیادی در زمینه‌ی امنیت این پروتکل و ارائه‌ی راهکار مناسب جهت برقراری امنیت انجام شده است، بخش قابل توجهی از نگرانی‌های امنیتی این پروتکل تاکنون دارای دست کم یک راه حل بوده اما بسیاری از آنها نیز همچنان هیچگونه راه حلی ندارند و می‌توانند زمینه مطالعه پژوهشگران باشند .علاوه بر این راه حل‌های موجود نیز در کنار نقاط قوت خود دارای ضعف‌های قابل توجهی نیز هستند که زمینه را برای پژوهش جهت ارائه یک راه حل بهینه و کارآمدتر فراهم می-سازند..

منابع

[1]Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.
[2]A.Al-Fuqaha, M.Guizani, M.Mohammadi, M.Aledhari, M.Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols and Applications", IEEE Communications Surveys & Tutorials, vol. 17, pp. 2347-2376, 2015.
[3] Z. Yang, Y. Peng, Y. Yue, X. Wang, Y. Yang and W. Liu, "Study and application on the architecture and key technologies for IOT," in Multimedia Technology (ICMT), 2011 International Conference On, pp. 747-751, 2011.
[4] J.Lin, W.Yu, N.Zhang, X.Yang, H.Zhang, W.Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications", IEEE Internet of Things Journal, 2017.
[5] S.Kraijak, P.Tuwanut, "A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends", Communication Technology (ICCT), 2015 IEEE 16th International Conference on, 2015.
[6] W. Colitti, K. Steenhaut, N. De Caro, B. Buta and V. Dobrota, "Evaluation of constrained application protocol forwireless sensor networks," in Local & Metropolitan Area Networks (LANMAN), 2011 18th IEEE Workshop On, 2011, pp. 1-6.
[7]Abdul Rahman Reem, Shah Babar,"Security analysis of IOT Protocols: A Focus in COAP", IEEE 3 rd MEC International Confrence on Big Data and Smart City, pp. 1-7, 2016.
[8] T. Winter, P. Thubert, A. Brandt, J. Hui, R.Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander,"RPL: IPv6 routing protocol for low-power and lossy networks", RFC 6550, IETF. 2012.
[9] M Ammar, G. Russello and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks", Journal of Information Security and Applications ,Volume 38, February 2018, Pages 8-27, 2018 .
[10] J. Granjial, E. Monteiro, and J. Silva,"Security for the Internet of Things: A survey of Existing Protocols and Open Research issues." IEEE Communications Surveys & Tutorials ,Volume: 17, Issue: 3. 2015 .
[11] V. Adat and B. B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture", Telecommunication Systems Volume 67, Issue 3, pp 423–441, 2018.
[12] L. Wallgren, S. Raza and T. Voigt,"Routing Attacks and Countermeasures in the RPL Based Internet of Things", International Journal of Distributed Sensor Networks, Volume 2013.