کلیه امتیازهای این پایان‌نامه به دانشگاه بوعلی سینا تعلق دارد. در صورت استفاده از تمام یا بخشی از مطالب این پایان‌نامه در مجلات، کنفرانس‌ها و یا سخنرانی‌ها، باید نام دانشگاه بوعلی سینا یا استاد راهنمای پایان‌نامه و نام دانشجو با ذکر مأخذ و ضمن کسب مجوز کتبی از دفتر تحصیلات تکمیلی دانشگاه ثبت شود. در غیر این صورت مورد پیگرد قانونی قرار خواهد گرفت. درج آدرس‌های ذیل در کلیه مقالات خارجی و داخلی مستخرج از تمام یا بخشی از مطالب این پایان‌نامه در مجلات، کنفرانس‌ها و یا سخنرانی‌ها الزامی می‌باشد.

مقالات خارجی

……..……, **Bu-Ali Sina University, Hamedan, Iran.**

مقالات داخلی

.....، گروه .....، دانشکده .....، دانشگاه بوعلی سینا، همدان.


بسم الله الرحمن الرحيم

تعهدنامه اصالت اثر

اینجانب همت دریایی دانشجوی دوره کارشناسی ارشد رشته فناوری اطلاعات گرایش شبکه‌های کامپیوتری دانشکده مهندسی به شماره دانشجویی ۹۴۱۳۱۸۴۰۰۷ که از رساله خود با عنوان:

ارائه ی یک مکانیسم مسیریابی کارآمد مبتنی بر اعتماد در اینترنت اشیا بر اساس پروتکل RPL

دفاع نمودهام، بدین وسیله متعهد می شوم:

نتایج مندرج در این پایان نامه توس اینجانب به دست آمده و از صحت و اصالت برخوردار است و در مواردی که از دستاوردهای علمی و پژوهشی دیگران اعم از پایا ن نامه، کتاب، مقاله و غیره استفاده کردهام، رعایت کامل امانت را نموده، مطابق مقررات، آن ها را ارجاع داده و در فهرست منابع و مآخذ اقدام به ذکر آنها نمودهام. تمام یا بخشی از این پایان نامه تا کنون توس اینجانب یا فر د دیگری برای دریافت هرگونه مدر تحصیلی(پایین تر،همسطح یا بالاتر)در هیچ کجا ارائه نگردیده است.

کلیه حقوق مادی و معنوی حاصل از این پایان نامه متعلق به دانشگاه بوعلی سینا بوده و هرگونه بهره مندی و یا نشر دستاوردهای حاصل از این پژوهش(و یا به صورت ترکیبی با اطلاعات دیگر)اعم از چاپ کتاب، مقاله، ثبت اختراع و غیره (چه در زمان دانشجویی و یا پس از فراغت از تحصیل)با هماهنگی استاد(ان)راهنما و مشاور و به نام" دانشگاه بوعلی صورت گیرد Bu-Ali Sina University" . "سینا "و یا در تمامی مقالات حاصل از این پایان نامه، برای چاپ و ارائه در مجلات داخلی و خارجی، کنفرانس ها و یا سخنرانی ها آدرس های ذیل را درج نمایم:

مقالات خارجی

....., Bu-Ali Sina University, Hamedan, Iran.

مقالات داخلی

....., گروه ....., دانشکده ....., دانشگاه بوعلی سینا، همدان.

حقوق مادی و معنوی تمام افرادی که در به دست آمدن نتایج اصلی این پایان نامه تأثیرگذار بودهاند را در مقالات مستخرج از پایان نامه رعایت نموده و در تمامی آن ها نام استاد(ان)راهنما و نشانی الکترونیکی دانشگاهی آنان را قید نمایم.

در کلیه مراحل انجام این پایان نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی داشته یا از آن ها استفاده کرده ام، اصل رازداری، ضواب و اصول اخلاقی پژوهش را رعایت نموده ام.

نام و نام خانوادگی دانشجو:

تاریخ

امضاء

سپاسگزاری

سر بر آستان جلال پروردگار بی‌همتا میسایم که دگربار توفیق اندوختن دانشی هرچند اندک را روزیام فرمود.

اکنونکه بر فراز سال‌های تحصیل به افتخار ایستاده‌ام، سرشارم از سپاس و ستایش ایزدی که من را عزت کسب عطا فرمود و یاری ام نمود تا در این سالها لبریز عشق پاک او باشم.

دانشگاه بوعلی‌سینا

مشخصات پایان‌نامه تحصیلی

عنوان:

ارائه ی یک مکانیسم مسیریابی کارآمد مبتنی بر اعتماد در اینترنت اشیا بر اساس پروتکل RPL

نام نویسنده: محمد پیشدار

نام استاد راهنما: یونس سیفی

نام استاد مشاور: محمد نصیری

دانشکده: مهندسی	**گروه آموزشی: کامپیوتر**	
رشته تحصیلی: فناوری اطلاعات	**گرایش تحصیلی: شبکه‌های کامپیوتری**	**مقطع تحصیلی: کارشناسی ارشد**
تاریخ تصویب پروپوزال: ۹۵/۸/۱۵	**تاریخ دفاع: ۹۶/۹/۱۸**	**تعداد صفحات: ۱۲۶**

چکیده:

اینترنت اشیاء تکنولوژی است که با ترکیب میکروکنترلرهای کم‌توان و تکنولوژی‌های ارتباطی امکان اتصال به اینترنت را برای اشیاء فراهم می‌سازد. معرفی کاربردهای فراوان تا به امروز باعث خبردهی پیش‌بینی‌ها، از آینده‌ای آمیخته با این تکنولوژی برای بشریت گردیده است.یکی از موانع گسترش استفاده از یک تکنولوژی عدم وجود امنیت اطلاعات در آن است.در اینترنت اشیا دانشمندان اهمیت امنیت اطلاعات را بسیار بالا می‌دانند. زیرا آسیب‌پذیری‌ها در این تکنولوژی می‌تواند از فضای مجازی خارج شده و بر محیط واقعی تاثیراتی گاه غیرقابل جبران بگذارند (نظیر قطعی برق در یک شهر).

یکی از نگرانی‌های عمده‌ی امنیت اطلاعات در اینترنت اشیاء، امنیت در لایه شبکه است. لایه‌ای از پشته‌ی پروتکلی که دانشمندان به دلیل ویژگی‌های خاص در اینترنت اشیا، پروتکل مسیریابی نوظهوری به نام RPLرا طراحی نموده‌اند. از جمله این ویژگی‌های خاص می‌توان به توان پردازشی، ذخیره‌سازی و منبع انرژی ضعیف در دستگاه‌های اینترنت اشیا و علاوه بر آن وجود مدل ترافیک خاص در این تکنولوژی اشاره نمود. با معرفی این پروتکل پژوهشگران پس از بررسی‌های امنیتی ضمن ارائه برخی حملات، آسیب‌پذیری RPL در برخی موارد را نشان دادند. در این پژوهش پس از بررسی های لازم علت شکل‌گیری بخش عمده‌ای از این حملات را عدم نظارت پدر بر رفتار فرزندان در توپولوژی درختی RPL موسوم به درخت DODAG یافتیم. سپس مکانیسمی برای تشخیص این حملات و بازیابی درخت ارائه کرده و روش پیشنهادی را در سیستم-عامل Contiki پیاده‌سازی و آنالیز نموده‌ایم. در این ارزیابی تاثیر روش پیشنهادی بر مصرف منابع شبکه، صحت و سرعت عملکردی آن تشریح گردیده است. موفقیت روش پیشنهادی در این عوامل کارآمدی آن را نشان می‌دهد.

واژه‌های کلیدی: اینترنت اشیاء، پروتکل مسیریابی RPL، امنیت در اینترنت اشیاء، امنیت در پروتکل RPL، سیستم عامل Contiki

فهرست مطالب

فهرست اشکال

فهرست جداول

فصل اول

مقدمه

۱-۱. مقدمه

درسال‌های گذشته با پیشرفت چشمگیر در محاسبات موبایل و تکنولوژی‌های بیسیم روشی جدید به نام اینترنت اشیاء[1] معرفی و با سرعت زیاد توانست توجه پژوهشگران در بسیاری از تحقیقات و صنایع را به سمت خود جلب نماید. ایده اصلی در اینترنت اشیاء، پیوند بین یک شیء و تکنولوژی‌های ارتباطی می‌باشد. هدف از ایجاد این تکنولوژی نیز انجام بسیاری از کارهای سخت و غیر ممکن برای انسان به وسیله اشیاء است.

معرفی ایده‌های کاربردی فراوان و بسیار مهم در این تکنولوژی خیلی زود باعث خبردهی پیش‌بینی‌ها از رشد سریع اینترنت اشیاء در آینده بشر گردید. وجود چالش‌ها و نگرانی‌های زیاد در مسیر تحقق این امر (حتی برخی نگرانی‌ها همچنان وجود دارند) موجب گردید دانشمندان به سمت ارائه راهکارهای مناسب حرکت نمایند **[۱,۲].**

۱-۲. اینترنت اشیاء چیست ؟

به شبکه‌های فراگیری که می‌توانند کنترل جهان واقعی را با جمع‌آوری، پردازش و آنالیز اطلاعات تولید شده توسط میکروکنترلرهای کم‌توان (به عنوان گره) انجام دهند اینترنت اشیاء می‌گویند. اشیاء در این تکنولوژی، قابلیت اتصال به اینترنت و مدیریت از راه دور را نیز دارا می‌باشند. همچنین میکروکنترلرهای کم‌توان را می‌توان، به صورت دستگاه‌های دارای ابزارهای جمع آوری اطلاعات از محیط و همچنین قابلیت ارتباطی تحت شبکه تعریف نمود.

وجود ویژگی‌های خاص در دستگاه‌های اینترنت اشیا را می‌توان از عوامل اصلی روبرویی این تکنولوژی با چالش‌های مختلف نام برد. از جمله این ویژگی‌ها می‌توان به قدرت پردازشی، قدرت ذخیره سازی و همچنین منبع انرژی ضعیف اشاره نمود **[۱,۲,۳].**

در ادامه به برخی از این چالش‌ها اشاره می‌نماییم.

۱-۳. چالش‌های اینترنت اشیاء

در این قسمت به برخی از چالش‌های پیش روی اینترنت اشیاء اشاره می‌نماییم **[۲,۳].**

۱-احراز هویت ضعیف: در دستگاه‌های اینترنت اشیاء به دلیل توان پردازشی و ذخیره سازی پایین از کلمه‌های عبور ضعیف جهت احراز هویت استفاده می‌گردد. این امر، امنیت اطلاعات در این تکنولوژی را با مشکلاتی روبرو کرده است.

۲-مدیریت کلید: به دلیل توان پایین دستگاه‌ها در اینترنت اشیاء استفاده از کلیدهای متقارن برای رمزنگاری در این تکنولوژی پیشنهاد می‌گردد. به همین دلیل چگونگی توزیع کلید دستگاه‌ها نیز از چالش‌های این تکنولوژی است.

1-Internet Of Things (Iot)

۳-آسیب پذیری‌های وب: استفاده از جلسه‌های امنیتی و گواهینامه‌های مدیریتی ضعیف در اینترنت اشیاء باعث ایجاد مشکلات امنیتی شدید در کاربردهای مورد استفاده‌ی تحت وب در این تکنولوژی گردیده است.

۴-چالش مصرف انرژی: منبع انرژی ضعیف در دستگاه‌های اینترنت اشیاء، استفاده از برخی توابع و یا کتابخانه-های مدیریتی رایج (در تکنولوژی‌های ارتباطی) را غیر ممکن و یا با مشکلاتی روبرو کرده است.

۵-چالش در خصوصی‌سازی[1]: وجود اطلاعات حساس و خصوصی (مانند اطلاعات بیماران) در کاربردهای مربوط به اینترنت اشیاء، نگرانی‌های زیادی در رابطه با حفظ حریم خصوصی کاربران ایجاد نموده است (به ویژه هنگام ترکیب با رایانش ابری[2]).

۶-چالش مدیریت داده‌ها : تولید اطلاعات فراوان در کاربردهای اینترنت اشیاء سازمان‌ها و مراکز داده را با مشکلاتی جهت پردازش و ذخیره‌سازی اطلاعات مربوطه روبرو نموده است.

علاوه بر چالش‌های نام برده شده اینترنت اشیاء دارای چالش‌هایی در رابطه با داده‌کاوی، نظارت بر دستگاه-ها،توان ذخیره‌سازی پایین و استانداردهای طراحی نیز می‌باشد.

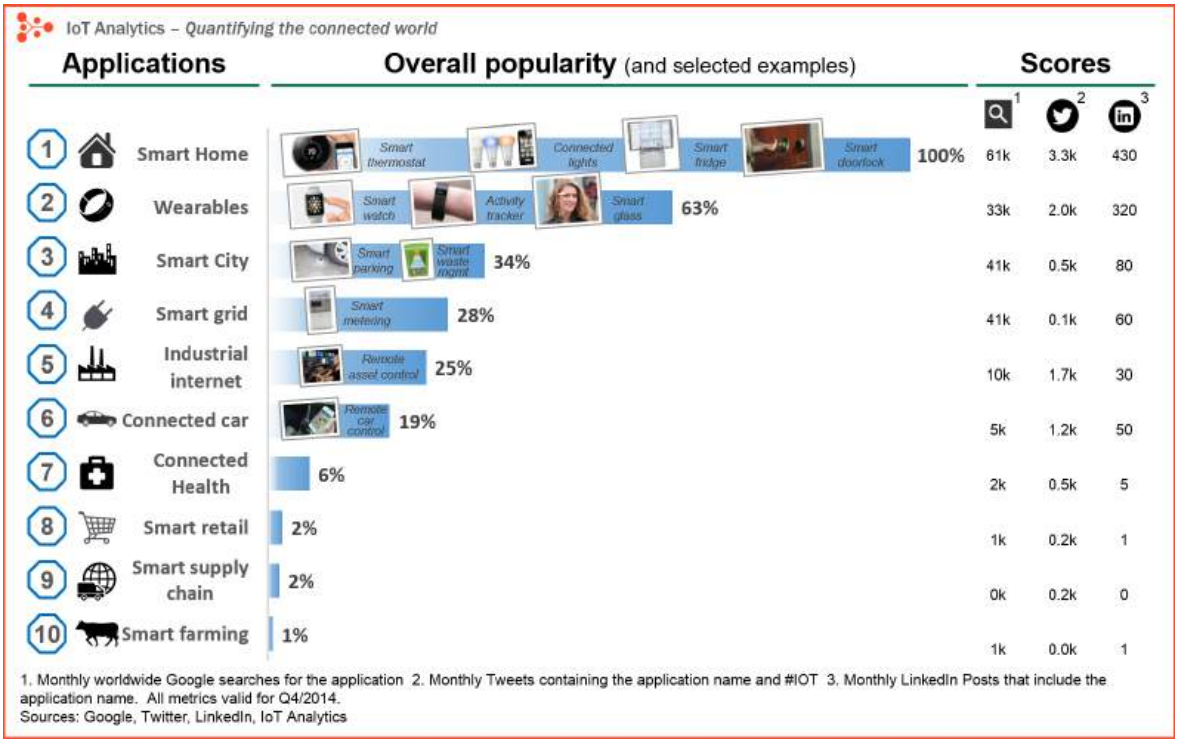
۱-٤. اهمیت امنیت در اینترنت اشیا

دانشمندان از اهمیت فراوان امنیت اطلاعات در اینترنت اشیاء خبر می‌دهند. دلیل این امر افزایش واگذاری بسیاری از کارها به اشیاء در زندگی آینده می‌باشد. در این صورت آسیب‌پذیری‌ها می‌توانند از فضای مجازی خارج و بر جهان واقع تاثیر مخرب بگذارند (نظیر قطع برق یک شهر). در برخی موارد این تاثیرات مخرب می‌تواند جبران‌ناپذیر نیز باشد **[۲,۳]**.

۱-۵. کاربردهای اینترنت اشیا

اینترنت اشیاء در سال‌های اخیر به یک موضوع داغ در صنعت و پژوهش‌های دانشگاهی تبدیل شده است. این فرآیند موجب معرفی ایده‌های کاربردی بیشتر برای این تکنولوژی با گذر زمان گردیده است. شکل ۱-۱ برخی از کاربردهای اینترنت اشیاء را نشان می‌دهد.

1-Privacy
2-Cloud Computing



شکل ۱-۱ : کاربرد های اینترنت اشیاء[٤]

۱-٦. پشته‌ی پروتکلی در اینترنت اشیاء

در شکل زیر می‌توانیم پشته پروتکلی اینترنت اشیاء را مشاهده نماییم.

لایه کاربرد	COAP
لایه انتقال	UDP
لایه شبکه	IPv6/RPL
سازگارکننده	6LowPan
لایه مک	۸۰۲.۱۵.۴
لایه فیزیکی	۸۰۲.۱۵.۴

شکل ۱-۲ : پشته‌ی پروتکلی اینترنت اشیاء در سیستم عامل Contiki [۲]

۱-۷. استاندارد ٤. ۱۵. ۸۰۲

این استاندارد مخصوص شبکه‌های نرخ ارسال پایین (LRPAN) تعریف شده است. در استاندارد ۸۰۲,۱۵,۴ تمرکز بر لایه فیزیکی و زیر لایه MAC از لایه پیوند داده می‌باشد. به کمک این تکنولوژی و همچنین استاندارد

وفق دهنده 6lowpan می‌توان از IPv6 را بر روی شبکه‌های سنسور بیسیم[1] نیز استفاده نمود. تاکید در این استاندارد برقراری ارتباط با کمترین هزینه و مخصوص دستگاه‌های نزدیک به هم می‌باشد**[۵]** .

برخی از ویژگی‌های مهم در این استاندارد عبارتند از**[۵]** :

۱-دسترسی Real-Time و مطمئن دستگاه‌های اینترنت اشیاء از رسانه اشتراکی با رزرو Time Slotهای مختلف

۲-اجتناب از ازدحام با CSMA/CA

۳-ارتباط امن

۴-وجود توابع مدیریت انرژی شامل تشخیص انرژی، کیفیت لینک

۵- استفاده از باندهای فرکانسی (۲۴۵۰/۹۱۵/۸۶۸ MHz)

۶- ۸۰۲,۱۵,۴ در چهارچوب اصلی می‌تواند فاصله‌ی ۱۰ متر و نرخ ارسال داده ۲۵۰Kbit/s را فراهم می‌سازد.

۱-۸. لایه RDC (Radio Duty Cycling)

این لایه به ذخیره سازی و کاهش مصرف انرژی در دستگاه‌های اینترنت اشیا می‌پردازد. این کار به وسیله‌ی خاموشی دستگاه در زمان‌های بیکاری و عدم ارسال صورت می‌پذیرد **[٦]** .

۱-۹. استاندارد 6LOWPAN

6lowpan مخفف دو مفهوم IPv6 و Low Power Wireless Personal Area Networks می‌باشد. مفهوم 6lowpan بر اساس قابلیت اجرایی پروتکل اینترنت بر روی هر دستگاه، سازماندهی گردید. بر این اساس حتی دستگاه‌های با قدرت پردازشی و ذخیره سازی پایین نظیر دستگاه‌های اینترنت اشیاء نیز می‌توانند از پروتکل IP استفاده نمایند**[۵]** .

در این مفهوم از کپسوله سازی و مکانیسم‌های فشرده سازی استفاده می‌گردد. این فرآیند به گونه‌ای است که بتوان از بسته‌های IPv6 در شبکه‌های مبتنی بر استاندارد ۸۰۲,۱۵,۴ نیز استفاده نمود. برخی توابع موجود در این استاندارد را می‌توان در زیر مشاهده نمود**[۵]** :

۱. وفق دادن اندازه بسته‌ها در دو شبکه IPv6 (حداقل MTU ۱۲۸۰ بایت) و ۸۰۲,۱۵,۴ (۱۲۷ بایت)
۲. تبدیل آدرس ۱۲۸ بیتی در IPv6 به آدرس ۶۴ بیتی در استاندارد ۸۰۲,۱۵,۴
۳. توابع مربوط به مکانیسم‌های مدیریت آدرس
۴. توابع امنیتی
۵. تطبیق تفاوت‌های موجود در طراحی دستگاه‌ها (به عنوان مثال وجود دستگاه‌های با ظرفیت پایین (در انرژی، پردازش و ذخیره‌سازی) در ۸۰۲.۱۵.۴ و استفاده از دستگاه‌ها با ظرفیت بالا در IPv6)

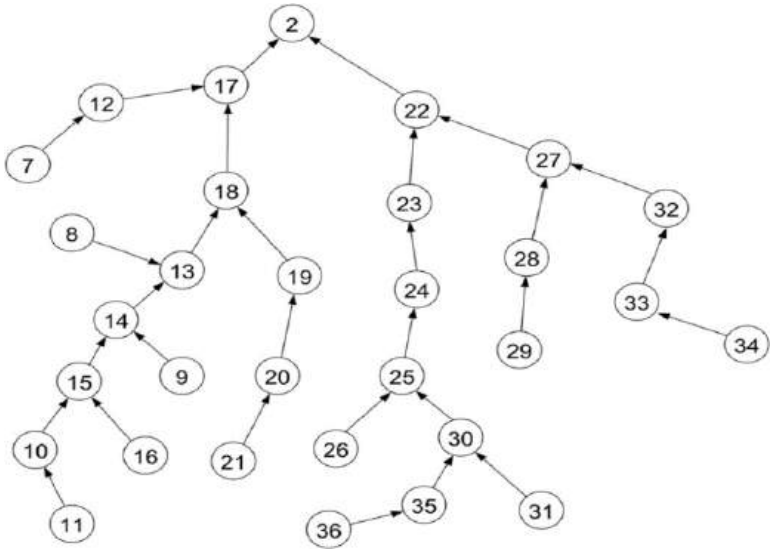
1-Wpan

۶. توابع مربوط به تفاوت در پارامترهای بهینه سازی: در IPv6 بهینه سازی بر روی پارامترهای مربوط به نرخ ارسال است اما در استاندارد ۸۰۲,۱۵,۴ مواردی نظیر مصرف بهینه انرژی و کاهش سایز کدها دارای اهمیت بیشتر می‌باشند.

۷. سازگاری فرمت بسته‌های IPv6 جهت استفاده در ۸۰۲,۱۵,۴

۱-۱۰. پروتکل RPL

این پروتکل بر اساس بردار فاصله[1] و IPv6 می‌باشد. گره‌ها در RPL بر اساس یک ساختار خاص به شکل درخت بدون دور (درخت DODAG[2]) تشکیل می‌گردند. در شکل ۱-۳ می‌توان نمونه ای از این ساختار را مشاهده کرد[3] **[۱,۷,۸,۹].**

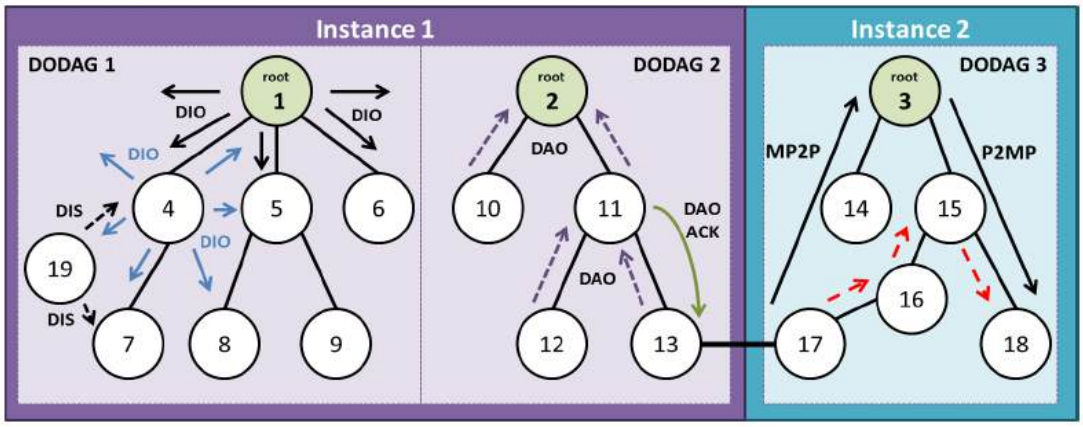


شکل ۱-۳ : نمونه ای از درخت بدون دور

یک شبکه در اینترنت اشیا می‌تواند به صورت یک یا ترکیبی از چند محدوده‌ی[4] پروتکل RPL تشکیل گردد. هر یک از این محدوده‌ها می‌تواند شامل یک یا چند درخت DODAG باشند. در شکل ۱-۳ دو محدوده‌ی پروتکل RPL نمایش داده شده است. محدوده شماره ۱ شامل دو درخت DODAG و در محدوده شماره ۲ تنها یک درخت از این نوع وجود دارد.

یک گره RPL می‌تواند به طور همزمان به چند محدوده RPL بپیوندد. این درحالی است که همان گره در یک محدوده تنها می‌تواند در یک درخت DODAG قرار گیرد.

1-Distance Vector
2- Destination Oriented Directed Acycle Graph
3- Routing Protocol For Low Power And Lossy Network
4-Instance



شکل ۱-٤ : دو محدوده RPL به همراه درخت‌های DODAG

در پروتکل RPL سه الگوی ترافیکی زیر در نظر گرفته شده است:

۱-یک نقطه به چند نقطه (نظیر ترافیک از ریشه به برگ‌ها)

۲-چند نقطه به یک نقطه (نظیر ترافیک از برگ‌ها به ریشه)

۳-نقطه به نقطه (مشابه پیکان‌های قرمز رنگ موجود در شکل ۱-۴)

۱-۱۱. ساخت و نگهداری DODAG

در این پروتکل برای ایجاد و نگهداری توپولوژی شبکه (درخت DODAG)، از انواع پیام‌های کنترلی در قالب بسته‌های ICMPV6[1] استفاده می‌گردد. این پیام‌ها به دسته‌های زیر تقسیم می‌گردند:

۱. پیام اطلاعات درخت(DIO[2]): این پیام توسط ریشه ایجاد و اطلاعات مورد نیاز برای پیکربندی، تشخیص پدران و همچنین نگهداری از درخت را منتشر می‌کند. سایر گره‌ها پس از دریافت این پیام اطلاعات مربوطه را از طریق بازارسال[3] این پیام در درخت منتشر می‌نمایند.

در این پیام اطلاعات زیر منتقل می‌گردد:

مقدار Rank : این مقدار نشان‌دهنده هزینه ارسال اطلاعات از طریق فرستنده پیام DIO (پیام DIO دریافتی)، تا ریشه درخت می‌باشد.

شماره ورژن: این مقدار نشان‌دهنده ورژن درخت DODAG مورد استفاده است. شماره ورژن تنها می‌تواند توسط گره ریشه تغییر نماید. مفهوم این تغییر عدم برپایی درخت جاری بوده و همچنین افزایش آن به منزله درخواست ایجاد درخت از ابتدا توسط گره ریشه می‌باشد (این کار در تعمیر درخت کاربرد دارد).

1- The Internet Control Message Protocol
2-Dag Information Object
3-Forward

مقدار DTSN[1]: این مقدار برای نگهداری مسیرهای رو به پایین (به سمت برگ‌ها) در گره‌ها به کار می‌رود.

MOP [2]: این مقدار مشخص کننده مد کاری مورد استفاده در درخت می‌باشد. در پروتکل RPL دو مد کاری اصلی زیر وجود دارد:

۱ - ذخیره‌سازی به صورت توزیع شده (Storing Mode): در این حالت گره‌ها دارای جداول مسیریابی بوده و می‌توانند برای زیر درخت خود عمل مسیریابی را انجام دهند.

۲- ذخیره‌سازی به صورت متمرکز (None Storing Mode): در این حالت گره‌ها فاقد جدول مسیریابی بوده و تمام پیام‌ها ابتدا به ریشه ارسال و سپس از آن‌جا مسیریابی می‌گردند (تمام مسیرها در ریشه ذخیره می‌شوند).

هر گره باید مد کاری درخت را رعایت نماید (این مد از طریق پیام DIO منتشر می‌گردد). درغیر این صورت گره مورد نظر تنها می‌تواند به صورت برگ به درخت بپیوندد. جدول ۱-۱ انواع مدهای کاری قابل استفاده در پروتکل RPL را نشان می‌دهد.

جدول ۱- ۱ : انواع مدهای کاری قابل استفاده در پروتکل RPL [۲۵]

انواع مدهای کاری قابل استفاده در پروتکل RPL
۱-عدم نگهداری مسیرهای رو به پایین
۲- ذخیره‌سازی به صورت متمرکز
۳- ذخیره‌سازی به صورت توزیع شده بدون پشتیبانی از MULTICAST
۴- ذخیره‌سازی به صورت توزیع شده باپشتیبانی از MULTICAST

شناسه درخت[3]: مشخص کننده درخت شامل گره ارسال کننده است. هر گره با دریافت پیامی از درختی به جز درخت جاری آن را حذف می‌نماید.

علاوه بر اطلاعات بالا گزینه‌های اختیاری [4]زیر نیز برای انتقال در این پیام وجود دارد.:

ویژگی‌های درخت: این گزینه برای انتقال ویژگی‌های خاص نظیر اطلاعات لینک‌ها، برخی گره‌ها و یا مسیرها در درخت استفاده می‌گردد.

اطلاعات مسیر: این گزینه برای نمایش اتصال یک مسیر با آدرس پیشوندی [5]مشخص از ریشه استفاده می‌گردد.

اطلاعات پیکربندی: این گزینه برای توزیع انتقال اطلاعات پیکربندی درخت می‌باشد.

آدرس‌های پیشوندی: این فیلد جهت توزیع آدرس‌های پیشوندی در درخت به منظور پیکربندی خودکار آدرس‌دهی در گره‌ها استفاده می‌گردد.

1- Destination Advertisement Trigger Sequence Number
2-Mode Of Operation
3-Dag Id
4-Options
5-Prefix

توصیف‌کننده مقصد: این گزینه برای انتقال اطلاعات مربوط به یک مقصد می‌باشد.

۲. پیام تبلیغ مقصد (DAO[1]) : این پیام برای انتشار اعلام وجود و همچنین اطلاعات یک یا چند مسیر رو به پایین (به سمت برگ‌ها) به طرف ریشه استفاده می‌گردد. از این طریق گره‌ها اطلاعات مسیریابی خود را به پدر ارجح خود منتقل می‌نمایند. در این پیام اطلاعات زیر منتقل می‌گردد:

شماره ترتیب: تمایز دو پیام از این نوع از طریق این شماره مشخص می‌گردد. همچنین به روز بودن یک پیام تبلیغ مقصد نیز از طریق شماره ترتیب تشخیص داده می‌شود.

شناسه درخت: این فیلد در این نوع پیام نیز وجود دارد.

علاوه بر اطلاعات بالا گزینه‌های اختیاری زیر نیز می‌تواند برای ارسال در پیام تبلیغ مقصد وجود داشته باشند:

تبلیغ یک مقصد: این گزینه برای نمایش امکان دسترسی به یک آدرس IPv6، آدرس پیشوندی و یا گروه همه‌پخشی[2] (در درخت DODAG)، از طریق گره فرستنده پیام استفاده می‌گردد.

اطلاعات انتقال: این گزینه برای انتقال صفات متعلق به مسیر مربوط به یک یا چند مقصد استفاده می‌گردد. بلافاصله یک یا چند گزینه تبلیغ مقصد پس از این گزینه قرار خواهند گرفت.

ویژگی‌های درخت: این گزینه در این نوع پیام نیز می‌تواند استفاده گردد.

۳. پیام درخواست اطلاعات درخت (DIS[3]): این پیام نشان‌دهنده درخواست اطلاعات پیکربندی مربوط به درخت جاری می‌باشد. دستگاه‌های (دستگاه‌های اینترنت اشیا) خارج از درخت با ارسال این پیام به برگ‌ها تقاضای پیام DIO جهت پیوستن به درخت را می‌نمایند.

پیام DIS شامل اطلاعات زیر است:

شناسه درخت: این فیلد در این نوع پیام نیز وجود دارد.

شماره ورژن : شماره ورژن درختی است که اطلاعات آن درخواست شده است.

طول پیام :نشان‌دهنده طول پیام می‌باشد. مقدار این گزینه به طور پیش‌فرض ۱۹ بایت است. طول پیام به دلیل امکان وجود گزینه‌های Pad (افزودن مقادیر بی‌ارزش جهت رساندن طول پیام به اندازه‌های مشخص بر اساس پروتکل) و اطلاعات درخواستی متفاوت می‌باشد.

۱-۱۲. نحوه ایجاد درخت DODAG

گراف DODAG در یک روش گام به گام ساخته می شود. ابتدا ریشه درخت، پیام DIO را ایجاد و به صورت همه پخشی منتشر می‌نماید. گره‌های موجود در محدوده ارسال (ارسال بیسیم) گره ریشه با دریافت این پیام ضمن به دست آوردن اطلاعات لازم جهت پیوستن به درخت، گره‌ی ریشه را به عنوان پدر خود در درخت انتخاب می‌نمایند. این گره‌ها پس از پیوستن به درخت بر اساس الگوریتم قطره چکان[4] (با سرآمدن زمانسنج موجود در

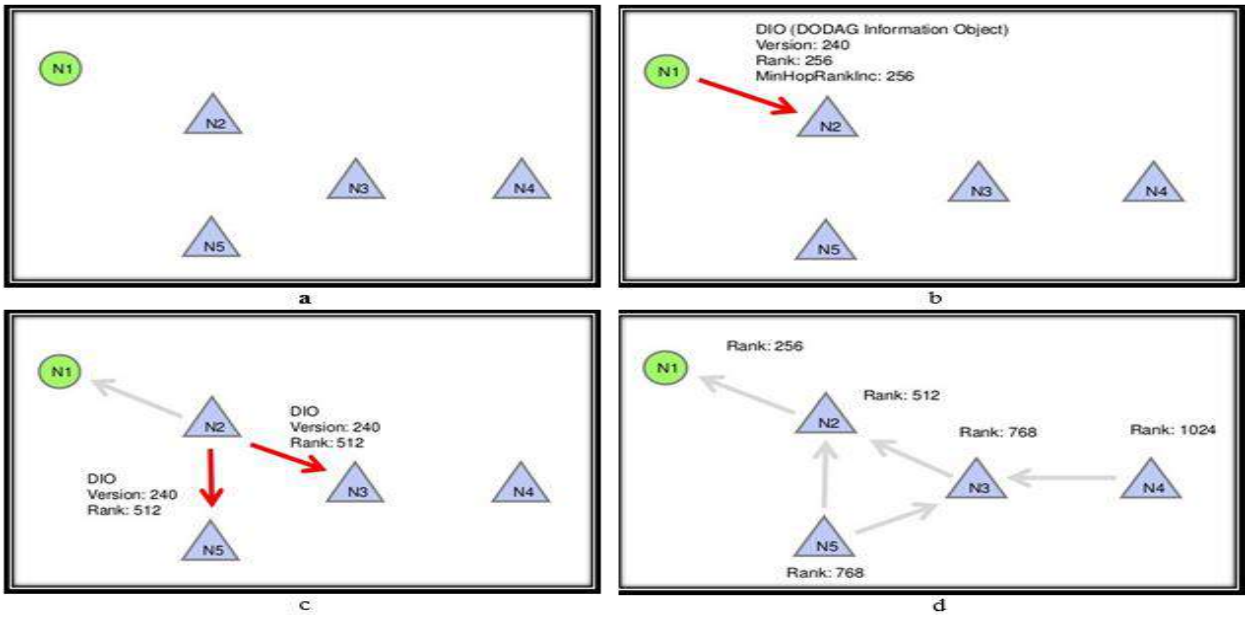
1-Destination Advertisement Object
2-Broadcast
3-DODAG Information Solicitation
1-Trickle Timer

هر گره براساس این الگوریتم) اقدام به بازارسال پیام DIO به صورت همه پخشی نموده و به این ترتیب اطلاعات به سمت برگ‌ها منتشر می‌گردند. قبل از بازارسال پیام‌های DIO، مقدار فیلد Rank با مقدار جاری آن در گره مورد نظر بروزرسانی می‌گردد. زمانسنج موجود در هر گره وظیفه ایجاد پایداری در درخت DODAG را داراست.

۱-۱۳. الگوریتم قطره چکان

رفتار این الگوریتم مشابه یک شیر آب است. در ابتدا قطره‌های این شیر با دوره تناوب کمتر فرود و رفته رفته طول این دوره افزایش خواهد یافت. بنابراین ابتدا سرعت سررسیدن زمانسنج بالا و به مرور زمان با پایداری شبکه این زمانسنج دیرتر سررسیده و اطلاعات با دوره تناوب بیشتری در درخت منتشر می‌گردند. پس از سررسیدن زمانسنج، گره مربوطه اطلاعات به روز شده را به صورت پیام DIO و در محدوده ارسال (ارسال بیسیم) خود به صورت همه پخشی منتشر می‌نماید. به این ترتیب ممکن است یک گره پیام‌های DIO را از طریق فرستنده‌های متفاوت دریافت نماید. این فرستنده‌ها پدران گره مربوطه را در درخت DODAG تشکیل می‌دهند. پس از این اتفاق گره مورد نظر بر اساس کمترین مقدار RANK بهترین پدرخود را به عنوان پدر ارجح [۱] انتخاب می‌نماید. گره‌ها از طریق پدر ارجح با کمترین هزینه به ارسال اطلاعات به سمت ریشه می‌پردازند **[۸,۹]**.

در شکل شماره ۱-۵ می‌توان مراحل تشکیل درخت را مشاهده نمود.



شکل ۱-۵ : نحوه ایجاد ساختار درخت DODAG

قسمت a : ریشه درخت (گره n1) شروع به ارسال پیام اطلاعات درخت (DIO) به صورت همه پخشی می‌کند. در قسمت b این پیام به همسایه گره n1 یعنی گره n2 رسیده و در قسمت c این پیام توسط ا گره به

2-Perrefered Parent

صورت همه پخشی منتشر می‌گردد. در اثر این‌کار، گره‌های n5 و n3 به درخت توپولوژی شبکه می‌پیوندند. نهایتا در قست d پیام اطلاعات درخت به همین ترتیب به برگ‌ها رسیده و درخت مربوطه شکل می‌گیرد.

با هر تغییر اعم از ایجاد و یا حذف در جدول مسیریابی گره، یک پیام DAO ایجاد و به پدر ارجح ارسال می‌گردد. به این ترتیب پدر گره مربوطه از این تغییر مطلع می‌گردد. گره پدر با دریافت این پیام DAO به بررسی و اعمال تغییرات احتمالی در جدول مسیریابی خود می‌پردازد. پس از این فرآیند گره پدر نیز پیام دریافتی را مجدد به پدر ارجح خود بازارسال کرده و به این شکل اطلاعات از پایین درخت به سمت ریشه منتشر می‌گردند.

نکته : مسیرها در هر گره پس از گذشت مدت زمان محدودی در صورت عدم استفاده حذف می‌گردند.

اطلاعات مسیرها در پروتکل RPL با توجه به مد کاری درخت (مد کاری از طریق پیام DIO توسط ریشه منتشر می‌گردد) می‌توانند به دو شکل در درخت ذخیره گردند. در ادامه این دو حالت تشریح می‌گردند:

۱-حالت Storing Mode: تمام گره‌ها در درخت دارای جدول ذخیره سازی جهت نگهداری اطلاعات هستند. بنابراین در این حالت اطلاعات به صورت توزیع شده در درخت DODAG نگهداری می‌گردد.

۲-حالت Non Storing Mode: در این حالت گره‌ها فاقد جدول مسیریابی بوده و تمام پیام‌ها ابتدا به ریشه ارسال و سپس از آن‌جا مسیریابی می‌گردند (تمام مسیرها در ریشه ذخیره می‌شوند).

با دریافت یک پیام DAO در یک گره در صورت استفاده از حالت ذخیره سازی، مسیر به جدول گره اضافه و در غیر این صورت پیام مورد نظر بدون ذخیره سازی و به صورت بازگشتی به پدر ارجح منتقل می‌گردد. پیام DAO می‌تواند با DAO-ACK تصدیق گردد.

۱-۱٤.مدیریت حلقه ها – ناسازگاری ها – و تعمیرها در پروتکل RPL

پروتکل RPL دارای مکانیسم‌هایی برای اجتناب از حلقه‌ها، تشخیص ناسازگاری‌ها و تعمیر توپولوژی DODAG در مواقع نیاز می‌باشد.

از ناسازگاری‌های پروتکل RPL می‌توان به موارد زیر اشاره نمود.

۱-ایجاد حلقه[1]

رخداد حلقه با هر پروتکل مسیریابی ناسازگار است زیرا این اتفاق باعث مصرف بیهوده منابع در برخی گره‌ها می‌گردد. تاثیر منفی حلقه‌ها در اینترنت اشیاء بسیار زیاد می‌باشد. دلیل این امر توان پردازشی، ذخیره سازی و همچنین منبع انرژی ضعیف در دستگاه‌های اینترنت اشیاء است **[۱,۷,۸,۹]**.

۲-مشاهده رفتاری خارج از پروتکل توسط گره‌ها

در ادامه به برخی از ناسازگاری‌ها در RPL اشاره می‌نماییم:

- در پیام‌های کنترلی RPL فیلدهای مشترکی وجود دارد. یکی از این فیلدها، پرچم O است که تنظیم آن در پیام RPL به معنی حرکت پیام در جهت رو به پایین و به سمت برگ‌ها در درخت DODAG

1-Loop

می‌باشد. اگر گره‌ای یک پیام کنترلی با پرچم O=1 و مقدار Rank بیشتر نسبت به خود دریافت نماید (و یا بالعکس) می‌تواند وقوع یک ناسازگاری را تشخیص دهد **[۱,۷,۸,۹]**.

- در پروتکل RPL نوع دیگری از این نوع ناسازگاری‌ها وجود داشته که تنها در حالت ارسال بسته از طریق یک مسیر رو به پایین و عدم اعتبار مسیر مربوطه در گام بعدی رخ می‌دهد. رفتار پروتکل هنگام وقوع این ناسازگاری به این صورت است که گره فرزند با تنظیم بیت F و ارسال مجدد بسته به پدر عدم اعتبار مسیر مربوطه را اطلاع‌رسانی می‌کند. گره پدر نیز با دریافت این پیام مسیر مورد نظر را از جدول مسیریابی خود حذف و از مسیر دیگری در صورت وجود اقدام به ارسال می‌نماید **[۱,۷,۸,۹]**.

۳-خرابی لینک‌ها و یا گره‌ها

خرابی لینک‌ها وگره‌ها باید در پروتکل مسیریابی به سرعت تشخیص داده شده و نقطه آسیب‌پذیر از فرآیند مسیریابی حذف گردد. در غیر این صورت منابع شبکه به صورت بیهوده و با هدایت اطلاعات به سمت نقطه آسیب‌پذیر از بین خواهند رفت **[۱,۷,۸,۹]**.

در صورت تشخیص ناسازگاری پروتکل RPL مکانیسم‌های تعمیر را فراخوانی می‌نماید. به طور کلی دو نوع تعمیر در RPL وجود دارد:

تعمیر محلی : در این تعمیر گره‌ها جهت عدم استفاده از مسیر آسیب‌پذیر اقدام به ارسال اطلاعات از طریق مسیر دیگر در صورت وجود می‌نماید **[۱,۷,۸,۹]**.

تعمیر همگانی : این تعمیر تنها توسط ریشه صورت گرفته و با افزایش مقدار شماره ورژن در پیام DIO آغاز می‌گردد. ریشه سپس به ارسال این پیام به صورت همه‌پخشی در محدوده ارسال (ارسال بیسیم) خود پرداخته و مراحل ایجاد درخت DODAG تکرار خواهند شد **[۱,۷,۸,۹]**. سایر گره‌ها با دریافت پیام DIO با ورژن جدید و بزرگتر از ورژن درخت فعلی به موارد زیر پی‌خواهند برد:

۱- درخت فعلی فاقد اعتبار است.

۲- ریشه با ایجاد درخت جدید در پی ترمیم شبکه است.

بنابراین گره‌ها با دریافت این پیام به درخت جدید پیوسته و اطلاعات قبلی خود را حذف خواهند نمود. بدین ترتیب ناسازگاری‌های موجود در شبکه رفع خواهند شد **[۱,۷,۸,۹]**.

۱-۱۵. لایه‌ی انتقال در اینترنت اشیاء

استفاده از پروتکل TCP برای این لایه در شبکه‌های اینترنت اشیا کارایی خوبی ندارد. دلیل این امر وجود الگوریتم کنترل ازدحام در پروتکل TCP است. این الگوریتم باعث کندتر شدن این شبکه‌ها (که دارای نرخ ارسال پایین و گم شدن بسیار بسته‌ها به دلیل استفاده از شبکه‌های بیسیم هستند) می‌گردد. بر این اساس پروتکل بدون اتصال UDP برای این شبکه‌ها مناسب‌تر به نظر می‌رسد **[۱,۷,۸,۹]**.

۱-۱۶.لایه کاربرد در اینترنت اشیاء

در این تکنولوژی به دلیل استفاده از پروتکل UDP در لایه انتقال استفاده از کاربردهای رایج نظیر پروتکل HTTP مناسب به نظر نمی‌رسید بنابراین دانشمندان استانداردهای دیگری از جمله COAP [1]را جهت رفع نیازمندی‌های اینترنت اشیاء در لایه کاربرد طراحی کردند **[۱,۷,۸,۹].**

از جمله ویژگی‌های این تکنولوژی می‌توان به موارد زیر اشاره نمود:

۱-سربار پایین

۲-پشتیبانی از چندپخشی در شبکه‌های دارای منابع ضعیف

۳- اتصال به شبکه‌ی بدون اعتماد اینترنت

COAP برای امنیت بیشتر می‌تواند از استاندارد DTLS [2]جهت مدیریت کلید، رمزنگاری داده و محافظت از جامعیت داده استفاده کند (این استاندارد جهت سازگاری با اینترنت اشیاء فشرده شده است). بنابراین به استاندارد COAP همچنین DTLS COAPS یا COAP ایمن نیز می‌گویند.

۱-۱۷.نگرانی‌های امنیتی در RPL

تا به امروز حملات و آسیب‌پذیری‌های زیادی بر علیه پروتکل RPL ارائه شده‌اند. برخی از این حملات از موارد رایج در شبکه‌های کامپیوتری بوده و برخی دیگر مخصوص پروتکل RPL به وجود آمده‌اند. در ادامه برخی از این حملات شرح داده می‌شود**[۱۰]**.

۱-۱۷-۱.حملات بر ضد منابع

در این حملات مهاجم[3] به دنبال ایجاد سربار در گره‌ها از طریق ایجاد ترافیک بیهوده و یا در حلقه انداختن پروتکل RPL است. هدف از این حملات مصرف بیهوده منابع مختلف از جمله انرژی، پردازش و غیره می‌باشد**[۲۲]**. در لیست زیر انواع این حملات آورده شده است.

- **حملات مستقیم**

در این حملات مهاجم به طور مستقیم به ایجاد سربار در گره ها می پردازد. حملات مستقیم شامل تولید ترافیک فراوان و از دسترس خارج نمودن برخی گره ها و لینک ها در شبکه است .در ادامه چند مورد از این حملات را بررسی می‌نماییم **[۱۰].**

۱-حملات Flooding

یکی از این حملات، Hello Flood است. این حمله در پروتکل RPL با ارسال مداوم پیام DIS به همسایگان

1-Constrained Application Protocol
2-Data Layer Transport Seciurity
3-Attacker

صورت می‌گیرد.این فرآیند تا زمانن تنظیم زمانسنج همسایگان به مقدار اولیه بر اساس الگوریتم قطره چکان ادامه می‌یابد. نتیجه این کار، اشباع گره‌ها و عدم رسیدگی آن‌ها به کارهای معمولی و وظایف خود می‌باشد **[۱۰]**.

۲-سرریز جدول مسیریابی گره ها در حالت Storing Mode

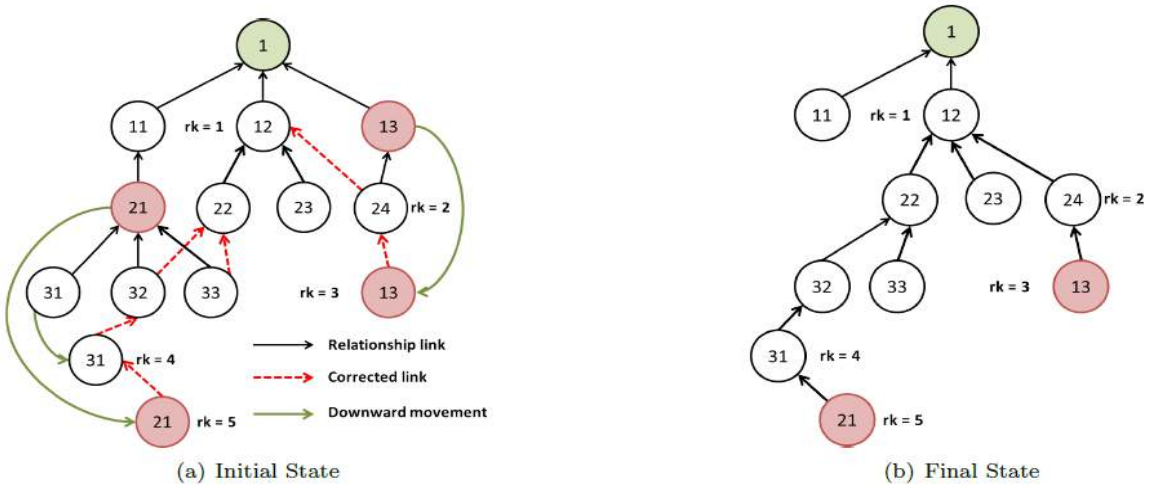
در این حمله با ایجاد مسیرهای جعلی از طریق پیام‌های DAO جداول مسیریابی گره‌های قربانی اشباع می‌گردد. به این ترتیب این گره‌ها دیگر فضایی برای ذخیره سازی مسیرهای واقعی دارا نمی‌باشند. در حقیقت این حمله با تولید ترافیک بیهوده در شبکه باعث مصرف منابع انرژی و پردازشی گره‌ها و در نهایت از دسترس خارج شدن آن‌ها می‌گردد **[۱۰]**.

- **حملات غیر مستقیم**

در این نوع از حملات گره مخرب بدون هیچ‌گونه تاثیر مستقیم باعث مصرف بیهوده منابع در شبکه می‌گردد. در ادامه نگرانی‌های از این نوع در RPL مورد بررسی قرار خواهند گرفت [۱۰].

۱-حمله افزایش مقدار Rank

در این حمله گره مخرب [۱] با افزایش ارادی مقدار Rank خود سعی بر طریق تغییر پدر ارجح در برخی گره‌ها می‌نماید. هدف گره مخرب از این امر ایجاد حلقه در درخت DODAG است. به دلیل هزینه بالای جلوگیری و بازیابی حلقه در RPL این حمله می‌تواند موجب سربار و مصرف منابع زیادی (از جمله انرژی) در گره‌ها گردد. در این حمله مهاجم همچنین در مکانیسم جلوگیری از تشکیل حلقه شرکت نمی‌کند. در شکل ۱-۶ می‌توانید این حمله را مشاهده نمایید که در آن گره ۱۳ و ۲۱ گره‌های مخرب می‌باشند [۱۰،۱۱].



شکل ۱-٦ : حمله افزایش Rank [۱۰]

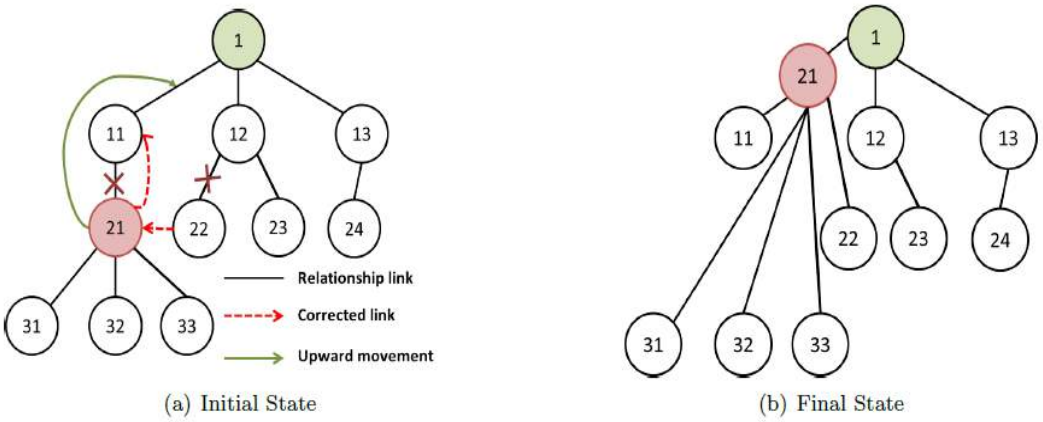
1-Malicious Node

۲-حملات ناسازگاری در DAG

در پیام‌های کنترلی RPL فیلدهای مشترکی از جمله پرچم O وجود دارد. تنظیم پرچم O در پیام RPL به معنی حرکت بسته در جهت رو به پایین و به سمت برگ‌ها در درخت DODAG می‌باشد. اگر گره‌ای یک پیام کنترلی با پرچم O=1 و مقدار Rank بیشتر نسبت به خود دریافت نماید (و یا بالعکس) می‌تواند وقوع یک ناسازگاری را تشخیص دهد. در هنگام وقوع ناسازگاری پروتکل RPL دارای یک مکانیسم بازیابی است. این مکانیسم پس از دریافت تعداد مشخصی از پیام‌های ناسازگار فعال و از تعمیر محلی و یا همگانی برای بازگرداندن درخت به شرایط صحیح استفاده می‌نماید[۱۰].

در این حمله گره مخرب با سوء استفاده از فیلد پرچم O به ایجاد ناسازگاری پرداخته و پروتکل RPL را مجبور به استفاده از مکانیسم بازیابی خود می‌نماید. به دلیل سربار موجود در این فرآیند منابع برخی گره‌ها مصرف شده و حتی ممکن است بعضی لینک‌ها از دسترس خارج گردند. از دسترس خارج شدن یک لینک می‌تواند باعث هدایت ترافیک به یک نقطه خاص و افزایش سربار در آن گردد. از پیامدهای افزایش سربار در یک گره نیز می‌توان به افزایش مصرف انرژی، کندی و حتی خاموشی آن اشاره نمود [۱۰].

در شکل شماره ۱-۷ می‌توان این حمله را مشاهده نمود (گره ۲۱ گره حمله کننده می باشد)



شکل ۱-۷: حمله ناسازگاری در DODAG [۲۲]

۳-حملات مربوط به Version Number

یک فیلد بسیار مهم در پیام DIO شماره ورژن می‌باشد. این فیلد متمایز کننده دو درخت DODAG در یک محدوده RPL است. شماره ورژن درخت تنها می‌تواند توسط ریشه افزایش یابد. در این حمله گره مخرب با افزایش مقدار ورژن در پیام DIO و بازارسال آن به صورت همه‌پخشی سعی می‌نماید تا گره‌های دریافت کننده را به اشتباه مجبور به تعمیر همگانی نماید. در نتیجه این‌کار سربار، مصرف بیهوده منابع و همچنین ازدحام در پروتکل RPL می‌تواند به وجود آید [۱۰،۱۱].

۱-۱۷-۲. حملات بر علیه توپولوژی

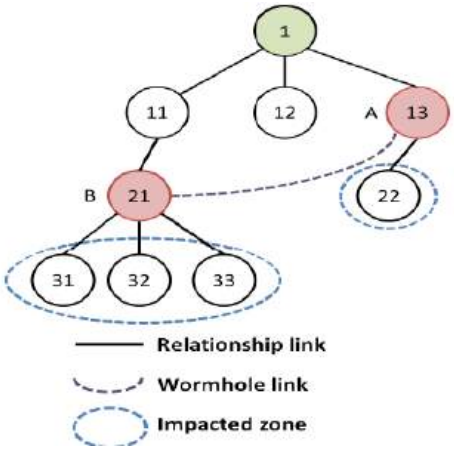
در این نوع از حملات گره مخرب به نوعی سعی بر تغییر توپولوژی صحیح و عملکرد RPL می نماید. در ادامه برخی از این حملات در RPL را شرح خواهیم داد.

۱-حمله Sinkhole

در این حمله گره مخرب به تبلیغ و جذاب نشان دادن خود (به عنوان مثال با کاهش مقدار Rank) جهت افزایش جذب ترافیک می‌پردازد. گره مخرب سپس به حذف و یا تغییر ترافیک هادی به سوی وی می‌پردازد. بدین ترتیب منابع و توپولوژی شبکه تحت تاثیر مصرف بیهوده و یا تغییر ناصحیح توپولوژی قرار خواهد گرفت[۱۱].

۲-حمله Wormhole

در این حمله گره مخرب به انتقال ترافیک به قسمت دیگری از درخت DODAG با کمک لینکی خارج از شبکه‌ی مورد حمله می‌پردازد. این حمله با ایجاد پردازش‌های بیهوده، سربار زیادی بر شبکه تحمیل می‌نماید. همچنین این انتقال‌ها توپولوژی اصلی درخت DODAG را برهم خواهند زد. در شکل ۱-۸ نحوه ایجاد حمله Wormhole نشان داده شده است (گره های ۲۱ و ۱۳ مخرب می‌باشند) **[۱۰,۱۱,۱۲].**



شکل شماره ۱-۸ : حمله Wormhole

۳-حملات تکرار

در این حملات گره مخرب یک پیام کنترلی صحیح را ضبط کرده و در زمانی دیگر به شبکه تزریق می‌کند. به این ترتیب مهاجم می‌تواند توپولوژی شبکه را از طریق درج اطلاعات غلط و فاقد اعتبار در جداول مسیریابی گره‌ها تغییر دهد. البته در پروتکل RPL شمارنده‌هایی برای جلوگیری از حملات تکرار وجود دارد. با وجود این شمارنده‌ها در مرجع **[۱۳]** نتایجی مبنی بر عملی بودن این حمله بیان شده است **[۱۱].**

۴-انتخاب بدترین والد [1]

در این حمله گره مخرب در لیست پدران خود به جای انتخاب گره بهینه بدترین گره را به عنوان پدر ارجح انتخاب می‌نماید. گره مخرب با این کار تاخیر و سربار را بر روی زیر درخت خود تحمیل می‌کند. عدم نظارت پدر بر عملکرد فرزندان دلیل رخداد این حمله است. عدم وجود نظارت مناسب یک نقطه ضعف اساسی برای RPL محسوب می‌گردد [۱۰].

۵-ناسازگاری DAO در حالت Storing Mode

هنگامی که در پروتکل RPL یک گره اطلاعاتی را از طریق ردیفی از جدول مسیریابی خود ارسال می‌نماید. در صورت عدم اعتبار آن مسیر در گام بعدی (گره فرزند) گره فرزند با ارسال یک پیام DAO شامل مسیر مربوطه و بیت F=1 پدر خود را از این موضوع مطلع می‌نماید. گره پدر نیز با دریافت این پیام مسیر مربوطه را از جدول مسیریابی خود حذف و در صورت وجود از مسیر دیگر اقدام به ارسال می‌کند.

در این حمله گره مخرب با سوء استفاده از این مکانیسم تمام پیام‌های رو به پایین پدر خود را ضمن تنظیم F=1 به پدر خود باز می‌گرداند. این عمل باعث تاخیر و منزوی شدن زیر درخت گره مخرب و حتی افزایش ازدحام در مسیرهای دیگر (ناشی از هدایت ترافیک فراوان) می‌گردد**[۱۴, ۱۱]**.

۱-۱۷-۳. حملات بر علیه ترافیک

در این نوع از حملات مهاجم با سعی بر سوء استفاده از ترافیک عبوری در جهت رسیدن به اهداف بداندیشانه‌ی خود تلاش می‌نماید. در ادامه به برخی از این نوع حملات اشاره می‌نماییم.

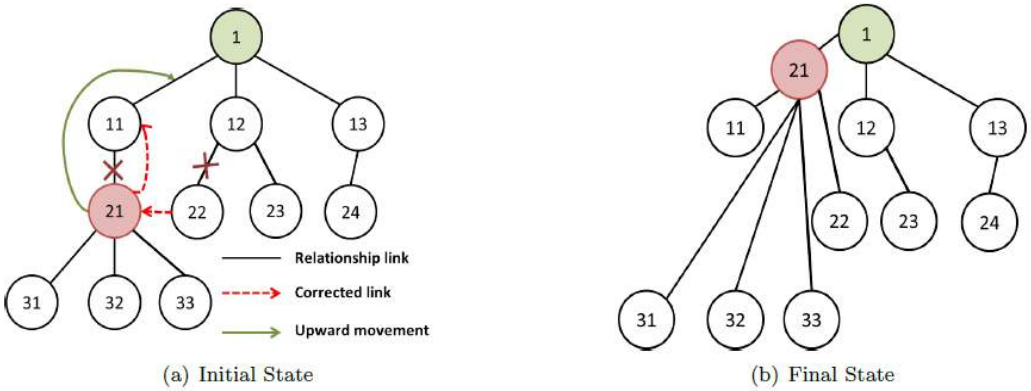
۱-حملات Sniffing

این حملات به معنی استراق سمع پیام های ارسالی در شبکه است. این حمله از حملات شایع در شبکه‌ها بوده و می‌تواند محرمانگی پیام‌ها را تهدید نماید. در این حمله گره مخرب می تواند اطلاعات مربوط به توپولوژی شبکه از جمله شماره ورژن و Id را مورد شنود قرار داده و در صورت امکان از این اطلاعات استفاده نامناسب به عمل آورد. تشخیص حملات Sniffing بسیار دشوار می‌باشد **[۱۰,۱۱]**.

۲-حمله کاهش Rank

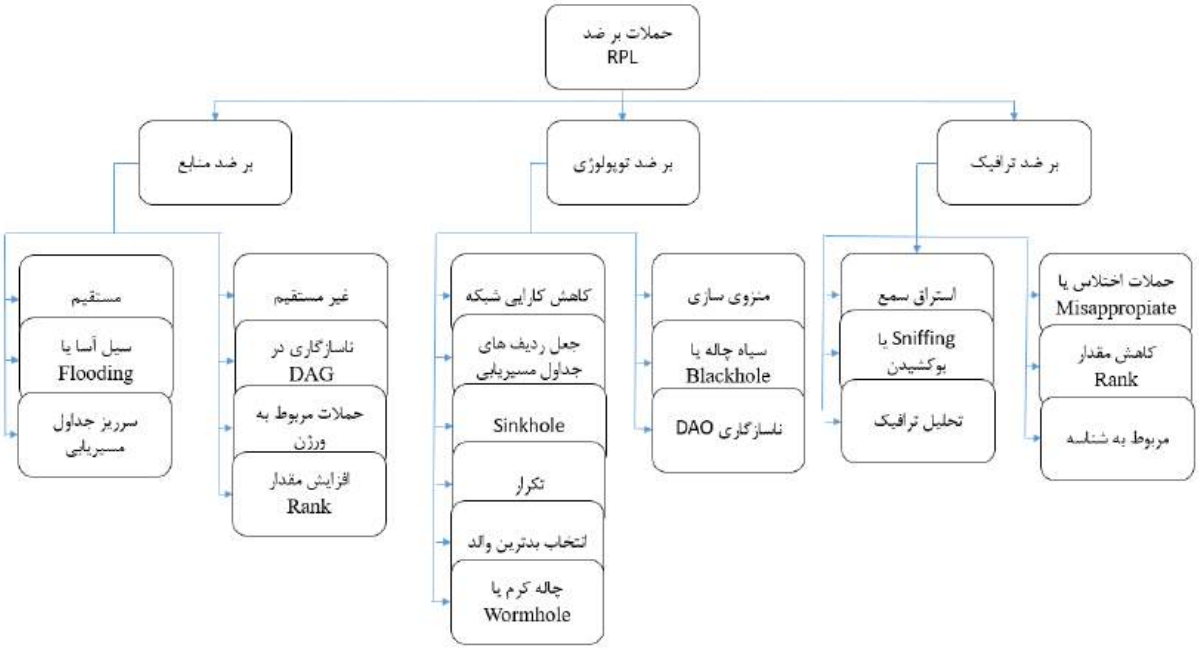
در این حمله گره مخرب با کاهش ارادی و خارج از قوانین مقدار Rank، سعی بر تغییر موقعیت خود در درخت DODAG و کاهش فاصله تا ریشه می‌نماید. در نتیجه این امر، با افزایش ترافیک عبوری از گره مخرب، مهاجم می‌تواند انواع حملات دیگر از جمله چاله خاکستری[۲]، سیاه‌چاله [۳]را اجرا کرده و تاثیر منفی بر عملکرد صحیح شبکه بگذارد. در شکل ۱-۹ حمله کاهش مقدار RANK که در آن گره ۲۱ گره مخرب می‌باشد مشاهده می‌گردد **[۱۰,۱۵,۱۶]**.

1-Worst Parent
۱-Sinkhole
۲-Blackhole



شکل ۱-۹ : حمله کاهش مقدار Rank [۱۰]

در شکل ۱-۱۰ می توان دسته بندی حملات معرفی شده در پروتکل RPL را مشاهده نمود.



شکل ۱-۱۰ : دسته بندی انواع حملات بر علیه پروتکل RPL [۱۰]

در جداول ۱-۲ الی ۱-۴ می توان لیست نگرانی های موجود را به همراه راه حل های ارائه شده در آنها و جزییات بیشتر مشاهده نمود:

حروف CIA در جداول زیر به ترتیب از چپ به راست به معنی محرمانگی (Confidenty) در اطلاعات و جلوگیری از دسترسی غیر مجاز ، حفظ جامعیت داده‌ها (Integrity) و جلوگیری از تغییر غیر مجاز آنها و در دسترس بودن (Availability) منابع شبکه برای افراد مجاز می‌باشند.

جدول ۱-۲ : حملات بر علیه منابع

نام حمله	پیشنیاز	اثر حمله	CIA	راه حل های ارائه شده	سربار
حمله Flooding	ندارد	باتری و لینک ها	A	ندارد	تدارد
حمله سربار بر جدول مسیریابی	حالت Storing Mode	باتری حافظه	A/I	ندارد	ندارد
حمله افزیش مقدا Rank	ندارد	باتری لینک ها	A	تشخیص حلقه و مکانیسم جلوگیری [۸]	ندارد (RPL پیشفرض)
حمله ناسازگاری DAG	هدر Option	باتری و لینک ها	A/I	کاهش شروع مجدد زمانسنج [۱۴]	پایین در راه حل های ارائه شده
حمله شماره ورژن	ندارد	باتری و لینک ها	A/I	احراز هویت شماره ورژن و مقدار Rank [۱۲]	پایین در راه حل های ارائه شده

جدول ۱-۳ : حملات بر علیه توپولوژی

نام حمله	پیشنیاز	اثر حمله	CIA	راه حل های ارائه شده	سربار
حمله استراق سمع	ندارد	اطلاعات مهم و محرمانه	C	رمزنگاری	وابسته به الگوریتم
حمله آنالیز ترافیک	ندارد	اطلاعات مهم و محرمانه	C	ندارد	ندارد
حمله کاهش مقدار Rank	ندارد	Rank گره	I	VERA [۲۲]– SVELTE [۲۵]- Rank Verification [۲۳]-[۲۴] Parent-Fail-Over	پایین-نامشخص
حمله Identify	ندارد	Rank گره	I	ندارد	ندارد

جدول ۱-٤: حملات بر علیه ترافیک

نام حمله	پیشنیاز	اثر حمله	CIA	راه حل های ارائه شده	سربار
جعل جدول مسیریابی	حالت Storing Mode	شبکه گره هدف	A/I	ندارد	ندارد
Sinkhole	ندارد	شبکه گره مخرب و همسایگان	A/I	Parent Fail Over-[۲۵] SVELTE [۱۲]	پایین
Wormhole	وجود دو Intruder	شبکه گره مخرب	A/I	درخت مرکل [۱۲]– اطلاعات جغرافیایی [۱۱]	نامشخص
انتخاب بدترین والد	ندارد	شبکه گره مخرب	A/I	ندارد	ندارد
سیاه چاله	ندارد	شبکه گره مخرب	A/I	Parent Fail Over-[۲۵] SVELTE [۲۳] و نظارت بر شمارنده ها [۵۰]	نامشخص
حمله ناسازگاری در DAO	حالت Storing Mode و سرآیند Option	شبکه گره هدف	A/I	ایجاد محدودیت در حذف اطلاعات جدول مسیریابی [۵۱]	پایین

۱-۱۸ نتیجه‌گیری

با مطالعه این فصل در می‌یابیم که امنیت اطلاعات در اینترنت اشیاء از اهمیت فراوانی برخوردار است. امنیت اطلاعات در اینترنت اشیا به لایه‌های مختلف پشته پروتکلی آن مربوط می‌گردد. در این فصل با تمرکز بر لایه شبکه در اینترنت اشیا به معرفی پروتکل RPL و نگرانی‌های امنیتی مختلف در رابطه با آن در قالب حملات متعدد پرداخته شد. این حملات را می‌توان به دو دسته زیر تقسیم نمود:

۱-حملات رایج شبکه در پروتکل RPL

Sinkhole، تکرار، استراق سمع، تحلیل ترافیک، حملات شناسه،سیاه‌چاله، Wormhole، جعل در جداول مسیریابی، Flooding و سرریز جداول مسیریابی

۲-حملات خاص شبکه در پروتکل RPL

حملات افزایش مقدار Rank، کاهش مقدار Rank، ناسازگاری در DAG ، ناسازگاری پیام DAO و حملات مربوط به مقدار ورژن درخت

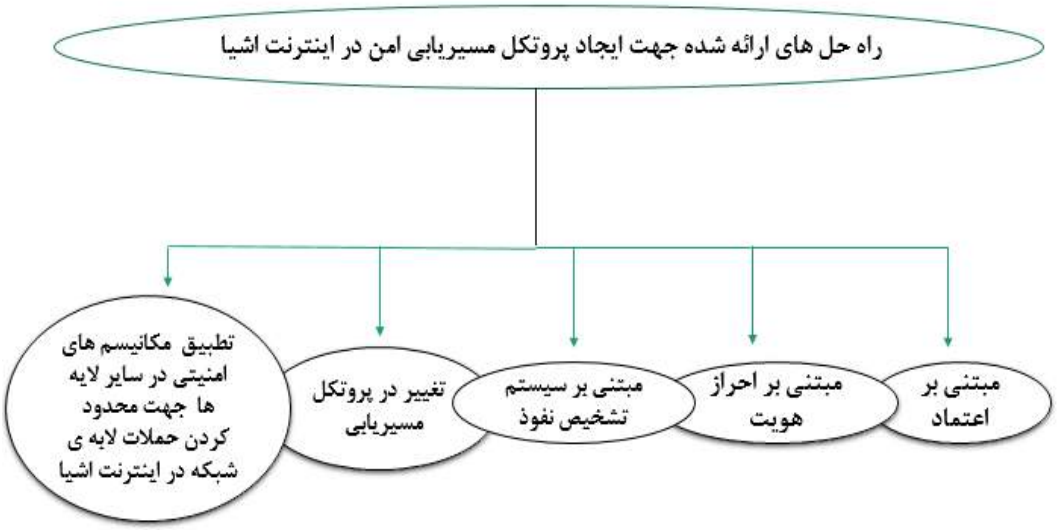
بر اساس اطلاعات موجود در این فصل نگرانی‌های امنیتی زیادی در مقابل پروتکل RPL وجود دارند. این نگرانی‌ها با توجه به اهمیت امنیت اطلاعات در اینترنت اشیاء می‌توانند به عامل بازدارنده برای رشد این تکنولوژی تبدیل گردند. پژوهشگران تا به امروز راه‌حل‌های معدودی را برای رفع این نگرانی‌ها ارائه کرده‌اند. در فصل بعد به بررسی این راه‌حل‌ها و آخرین وضعیت نگرانی‌های RPL تا به امروز پرداخته خواهد شد.

فصل دوم

پیشینه تحقیق

۲-۱. پیشینه تحقیق

وجود نگرانی‌های امنیتی مختلف در پروتکل RPL پژوهشگران را به ارائه راه حل های مختلف برای رفع این نگرانی ها سوق داد. تا کنون راه حلی برای رفع تمام این نگرانی‌ها و یا حتی بخشی از آنها ارائه نشده است. دسته‌بندی شکل ۲-۱ راه‌حل‌های موجود برای رفع نگرانی‌های پروتکل RPL تا کنون را نشان می‌دهد.



شکل ۲-۱ : دسته بندی راه‌حل‌های ارائه شده برای رفع نگرانی‌های پروتکل RPL

در موارد روش‌های مبتنی بر اعتماد و احراز هویت موجود در تقسیم‌بندی شکل ۱- ۸ روشی خاص برای پروتکل RPL تا به امروز ارائه نشده است. بنابراین در این موارد به نزدیک‌ترین کارهای مشابه و قابل تعمیم به پروتکل مسیریابی RPL خواهیم پرداخت. در ادامه در هر دسته از راه حل های معرفی شده نمونه‌هایی را معرفی می‌نماییم.

۲-۲. راه‌های مبتنی بر اعتماد

در این روش‌ها به نوعی از مفهوم اعتماد در زندگی روزمره برای مقابله با نگرانی‌های امنیتی در علوم ارتباطات استفاده می‌گردد. در این روش‌ها رفتار مخربانه (بر اساس تعریف اعتماد) از اعتماد سایر گره‌ها به گره مخرب خواهد کاست. در ادامه برخی از این روش‌ها مورد بررسی قرار خواهد گرفت.

۲-۲-۱. پروتکل TSRF (Trust aware secure routing framework in wsn)

این راه حل بر اساس مفهوم اعتماد[۱] گره‌ها به یکدیگر در فرآیند مسیریابی است. در این روش هرچه اعتماد به یک گره در مسیریابی بیشتر باشد رفتار آن گره نیز مطابقت بیشتری با قوانین پروتکل داراست. بی‌اعتمادی در TSRF به معنی پایبندی کمتر یک گره به قوانین پروتکل است **[۱۷]**.

در این مدل هر گره مسئول نظارت بر همسایگان خود و ارزیابی میزان اعتماد به آنها است. این اعتماد شامل ترکیب اعتماد مستقیم و غیر مستقیم می‌باشد. اعتماد مستقیم بر اساس مشاهدات خود گره در ارتباطات و اعتماد غیر مستقیم (یا اعتماد توصیه‌ای) از طریق توصیه‌های مربوط به گره‌های بدون تعامل مستقیم با گره مورد نظر می‌باشد**[۱۷]**.

محاسبه اعتماد در گره‌ها:

میزان اعتماد گره i به گره j به صورت t(I,J) نشان داده می‌شود.

$$t(i,j)^l = \alpha \times dt(i,j)^l + \beta \times \frac{\sum_{(k \epsilon C_j, k \neq i)}^{n} it(k,j)^l}{n-1}. \qquad [۱-۲]$$

در رابطه بالا :

همواره مجموع مقادیر α+β برابر ۱ می باشد

α ضریب قضاوت گره در مورد مشاهدات خودش و β ضریب توصیه‌هایی که در اعتماد کلی به یک گره مربوط می باشد

$dt(i,j)$ به معنی اعتماد مستقیم گره i به گره j

$it(k,j)$ به معنی اعتماد غیر مستقیم گره k در مورد گره j که در همسایگی گره j می باشد.

میزان اعتماد عددی بین صفر و یک می‌باشد.

محاسبه ی اعتماد مستقیم :

$$dt(i,j)^l = \gamma_1 \times dt_{P(j)}(i,j)^{l-1} + \gamma_2 \times dt_{N(j)}(i,j)^{l-1} + ids(i,j)^l, \qquad [۲-۲]$$

$P(j)\ (i,j)\ l-1$ به معنی میزان اعتماد مستقیم گره I به گره J بر اساس رفتار خوب در گذشته

$N\ (j)\ (i,j)\ l-1$ به معنی اعتماد مستقیم گره I به گره J بر اساس رفتار نامناسب در گذشته

$\gamma 1, \gamma 2$ متناسب با فاکتورهای گذشت زمان به تریب برای فراموشی رفتار خوب و رفتار بد می باشد

۱-Trust

$ids(i,j)$ رفتار جاری گره بر اساس سیستم تشخیص نفوذ [۱]که به صورت زیر تعریف می گردد.

$$ids(i,j)=\begin{cases}P(j), & \text{for } 0<P(j)<1\\ 0, & \text{for uncertain}\\ N(j), & \text{for } -1<N(j)<0,\end{cases} \qquad [۳-۲]$$

P(j) نشان دهنده ی رفتار خوب تشخیص داده شده از رفتار گره j

N (j) نشان دهنده ی رفتار بد تشخیص داده شده از رفتار گره j

برای مقابله با برخی حملات از جمله حملات On-Off (اجرای حمله به صورت دوره‌ای) متغیر گذشت زمانی به صورت زیر تعریف می گردد.

$$\gamma=\begin{cases}\gamma_1=e^{-\rho_1\times(t_c-t_{c-1})}, & \text{for } dt_{P(*)}\\ \gamma_2=e^{-\rho_2\times(t_c-t_{c-1})}, & \text{for } dt_{N(*)},\end{cases} \qquad [۴-۲]$$

Tc زمان جاری

Tc-1 زمانی که تعامل قبلی شروع شد

بر طبق معادلات بالا مقدار اعتماد کاهش خواهد یافت

معمولا مقدار زیاد برای رفتار بد یعنی r2 و مقدار کم برای رفتار خوب یعنی r1 تنظیم می گردد .

محاسبه اعتماد غیر مستقیم:

$$\sum_{(k\in C_j,k\neq i)}^{n} it(k,j)^l=\sum_{(k\in C_j,k\neq i)}^{n} dt(i,k)^l\times dt(k,j)^l. \qquad [۵-۲]$$

که به صورت زنجیروار و از طریق اعتماد مستقیم محاسبه می شود.

با رفتار مخربانه در گره مخرب میزان اعتماد به این گره از طریق توصیه‌ها ی همسایگان و یا مشاهده مستقیم در برخی گره‌ها کاهش خواهد یافت. بنابراین رفتار مخربانه گره در برخی نگرانی‌ها تشخیص داده خواهد شد **[۱۷]**. در سال ۲۰۱۷ این روش به پروتکل RPL بدون استفاده از زوال زمانی تعمیم یافت. در این تعمیم اعتماد مستقیم به صورت ترکیبی از این اعتماد در دوره ارسال پیام DIO قبلی (بر اساس الگوریتم قطره‌چکان) و مقدار آن در لحظه فعلی است. سایر موارد از جمله محاسبه اعتماد غیر مستقیم مشابه روش TSRF است **[۱۸]**.

۱-IDS

این روش می‌تواند با نگرانی‌های زیر مقابله نماید:

- حملاتی که در آن گره مخرب گاهی رفتار مخربانه نظیر حذف ارادی بسته‌های دریافتی انجام داده و گاهی این کار را نمی‌نماید.
- حملاتی که در آن مهاجمSelfish attack به دستکاری اطلاعات دریافتی پرداخته و سپس آن را به سمت گره قربانی ارسال خواهد نمود
- حملات Flooding
- حملاتی که در آن گره مخرب ارسال پیام‌های حاوی اطلاعات غلط خواهد پرداخت.
- حملاتی که در آن بیش از یک گره مخرب برای آسیب‌رسانی به عملکرد شبکه همکاری می-نمایند.

از نقاط ضعف این روش‌ها در مقابله با نگرانی‌های RPL می‌توان به موارد زیر اشاره نمود:

تعریف مفهوم اعتماد در این روش صریح نبوده و به صورت کلی گفته شده است. به دلیل عدم تعریف دقیق مفهوم اعتماد از رفع نگرانی‌های موجود در شبکه‌های سنسور بیسیم و RPL نیز به صورت کلی سخن گفته شده است.

۲-۲-۲. روش اعتماد بر اساس تصدیق دوگانه

بیشتر الگوریتم‌های مبتنی بر اعتماد نیاز به پشتیبانی از حالت Promicuous کارت شبکه برای جمع آوری توصیه‌ها از همسایگان در محاسبه‌ی اعتماد دارند. این فرآیند مصرف انرژی و حافظه، سربار ارتباطی را به همراه دارد که با شرایط دستگاه‌ها در اینترنت اشیا سازگار نیست **[۱۹]**.

در این روش سعی بر کاهش این سربار و مصرف انرژی با ارائه یک راه حل کارآمد و بهینه شده است. برای این منظور در این روش اعتماد مستقیم بر اساس تصدیق‌های سطح لایه لینک از ارسال داده‌ها در استاندارد ۸۰۲.۱۵.۴ و یک تصدیق دو گامی از طریق گره دوم موجود در مسیر مقصد محاسبه می‌گردد[۱۹].

در این روش گره ارسال کننده پیام در صورتی یک ارسال را موفق در نظر می‌گیرد که:

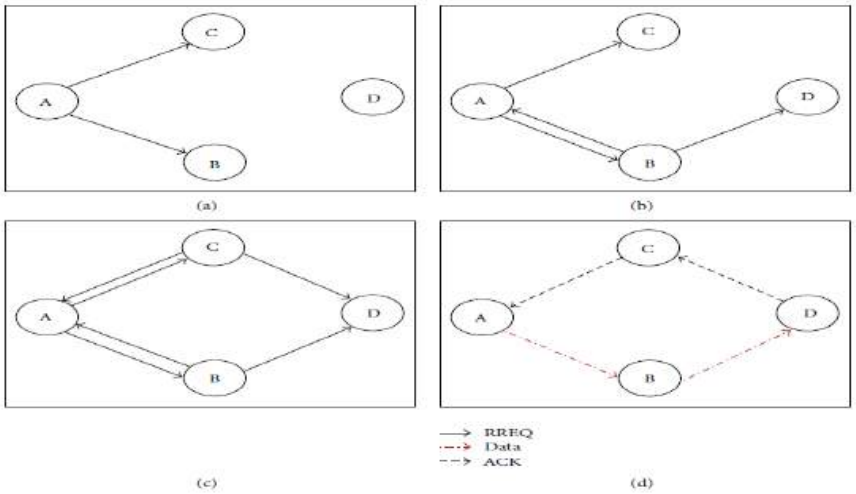
۱-گره ارسال کننده بتواند دریافت پیام به طور صحیح در همسایه‌اش (گام بعدی در مسیریابی) را تایید کند.

۲- ارسال‌کننده بتواند به نوعی متوجه ارسال صحیح پیام مربوطه به سمت مقصد توسط گره همسایه گردد.

در این روش مورد اول از طریق دریافت تصدیق در لایه دیتا لینک [۱]و مورد دوم از طریق دریافت تصدیق[۲] دوگامی به وسیله‌ی گره دوم موجود در مسیر بین ارسال‌کننده و مقصد پیام نتیجه‌گیری می‌شود **[۱۹]**.

۱-DataLink

۲-Acknowledge



شکل ۲-۲ : تصدیق‌ها در روش Two Way

به عنوان مثال در شکل شماره ۲-۲ گره S ارسال‌کننده پیام و گره D گره دوم در مسیر مربوطه تا مقصد می‌باشد. در مرحله کشف مسیر گره A پیام مربوطه را به صورت همه پخشی برای مقصد مشخص ارسال می‌نماید. پیام مربوطه در گره‌های B و C دریافت می‌شوند. این گره‌ها ضمن مطابقت مقصد پیام با آدرس خود یک تصدیق در لایه دیتا لینک را برای گره A ارسال می‌نمایند. در صورت مغایرت مقصد پیام با آدرس مربوطه، گره مورد نظر شروع به بازارسال پیام به صورت همه‌پخشی می‌نمایند. گره D با دریافت این پیام از دو مسیر ضمن تشخیص یک بار بازارسال شدن پیام مربوطه علاوه بر ارسال تصدیق در لایه دیتا لینک، یک تصدیق دو گامی نیز از طریق مسیر جایگزین (مسیری که پیام تکراری از طریق آن دریافت شده است) به گره A ارسال می‌نماید. گره A با دریافت این دو تصدیق انتقال پیام را موفقیت آمیز می‌داند و در غیر این صورت شکست را تشخیص می‌دهد **[۱۹]**.

محاسبه اعتماد: برای ذخیره سازی اطلاعات به دست آمده در مرحله نظارت از یک جدول که درایه‌های آن به صورت زیر می‌باشد استفاده می‌گردد:

(شماره گره، تعداد انتقال‌های صحیح، تعداد انتقال‌های ناصحیح، سطح اعتماد)

شماره گره: به تعداد همسایگان گره اشاره می‌کند

تعداد انتقال‌های صحیح: به دریافت تصدیق تک گام و دو گامی در زمانی کمتر از آستانه تعریف شده

تعداد انتقال‌های ناصحیح : به صورت عکس تعداد انتقال‌های صحیح تعریف می‌گردد.

سطح اعتماد به صورت زیر تعریف می‌گردد:

$$T_V = \left(\frac{T_s + \varepsilon}{T_s + T_f} \right) 100, \qquad [۶-۲]$$

TS: انتقال ها ی صحیح
TF: انتقال های شکست خورده
TV: سطح اعتماد

برای کاهش حجم ذخیره سازی عدد مربوط به اعتماد در محدوده‌ی صفر تا ۷ نظیر می‌گردد. اگر مقدار عدد اعتماد برای یک گره از یک آستانه مشخص بیشتر باشد آن گره معتمد و در غیر این صورت به آن گره اعتمادی وجود ندارد. انتخاب این آستانه در اثر آزمایش‌های فراوان به گونه‌ایست که روش مربوطه بیشترین کارآمدی را داشته باشد **[۱۹]**.

گره‌های مخرب در این روش دارای میزان اعتماد پایین در همسایگان خود بوده و از سایر گره‌ها تشخیص داده می‌شوند. این پروتکل مخصوص پروتکل RPL طراحی نشده است و برای سازگاری با آن نیازمند تغییراتی می‌باشد **[۱۹]**.

این روش می‌تواند با نگرانی‌های کلی زیر مقابله نماید:

- حمله سیاه‌چاله [1]: در این حمله گره مخرب ترافیک ورودی را به صورت ارادی حذف می-نماید.
- حملات جعل هویت[2]: در این حمله هکر سعی در جعل هویت و انجام رفتار بداندیشانه دارد.

رفتار بدخواهانه[3] : در این حملات گره مخرب با انجام رفتار خودخواهانه (نظیر حذف بسته‌ها و یا استفاده بیهوده از پهنای باند) سعی بر آسیب‌رسانی به برخی گره‌ها در اجرای صحیح وظایف خود بر اساس پروتکل مسیریابی می‌نماید.

این روش به دلیل عدم وجود مسیر جایگزین، در همه موارد کاربرد ندارد.

در روشی مشابه در پروتکل RPL اعتماد به صورت نسبت تعداد بسته‌های دریافت شده در گره همسایه به تمام پیام‌های ارسالی به وی محاسبه می‌گردد. این امر در هر گره برای همسایگان به ویژه پدر ارجح محاسبه می‌گردد. در صورت رفتار مخربانه نظیر حملات سیاه‌چاله و Sinkhole در یک گره اعتماد فرزندان گره مخرب به وی کاهش یافته و در نهایت رفتار مخربانه تشخیص داده خواهد شد **[۲۰]**.

۲-۳. راه‌حل‌های مبتنی بر احراز هویت

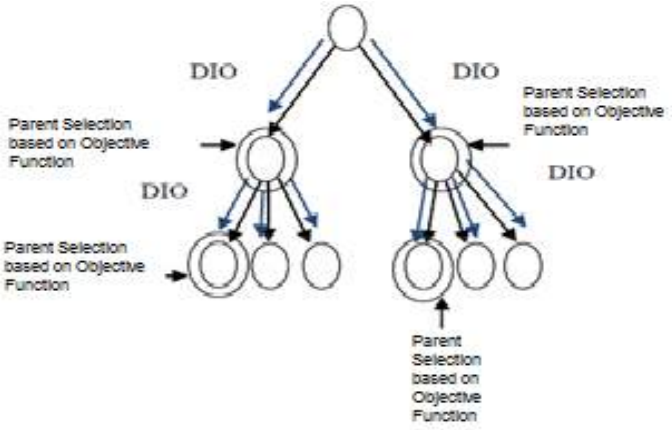
در این روش‌ها با افزودن امکان احراز هویت گره‌ها سعی بر تشخیص رفتار مخربانه در درخت DODAG و مقابله با برخی نگرانی‌های RPL شده است. در ادامه برخی از این روش‌ها مورد بررسی قرار گرفته شده است.

1-Blackhole
2-Spoofing
3-Selfish

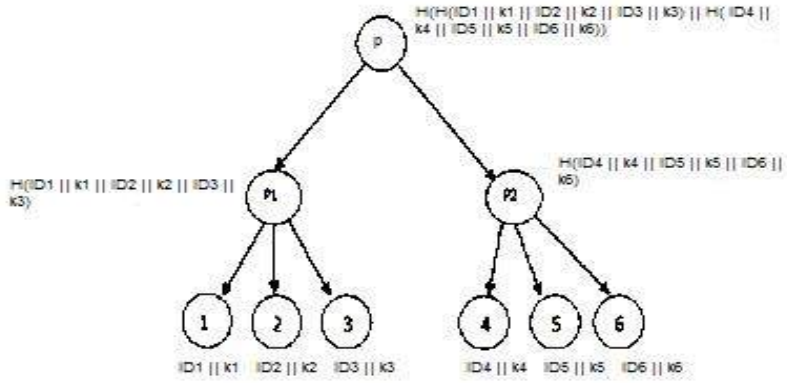
۲-۳-۱. درخت مرکل[1]

محققان این روش را جهت مقابله با حمله Wormhole پیشنهاد کرده‌اند. این روش بر اساس یک مکانیسم احراز هویت[2] که اطلاعات امنیتی در آن بر اساس پدران گره (در درخت DODAG) و در قالب یک تابع درهم‌سازی تولید می‌گردد است. اطلاعات امنیتی تمام گره‌ها ابتدا به شکل یک ساختار درختی به نام Merkel ذخیره گشته و سپس به ساختار درخت DODAG در پروتکل RPL نظیر می‌گردد **[۱۲]**.

در شکل‌های ۳-۳ و ۳-۴ می‌توان یک درخت DODAG و مرکل متناظر با آن بر اساس این روش را مشاهده نمود.



شکل ۲-۳: درخت DODAG نمونه در روش مرکل



شکل ۲-٤: درخت مرکل نظیر شده برای شکل شماره ۲-۳

4-Merkel
5-Authentication

در این روش گره فرزند در شروع ارتباط اطلاعات خود را به صورت یک‌طرفه درهم‌سازی کرده و با بررسی وجود آن در اطلاعات احراز هویت رسیده از طرف والد، می‌تواند گره ارسال کننده را احراز هویت نماید. در پروتکل RPL هر گره تنها می‌تواند از طریق پدر خود اطلاعات از سمت بالای درخت (سمت ریشه) را دریافت نماید **[۱۲].**

به این شکل اگر گره‌ای از سمت دیگر درخت قصد حمله Wormhole را داشته باشد این حمله به طور خودکار و با عدم احراز هویت گره ارسال کننده خنثی می‌گردد. سربار ارتباطی و پردازشی نقطه ضعف اصلی در این روش می‌باشد.

۲-۳-۲ روش SMRP [1]

اساس این روش احراز هویت ابزارهای اینترنت اشیاء از طریق ایجاد شناسه‌های یکتا در مرحله نصب شبکه می‌باشد. در لیست زیر ویژگی های اصلی SMRP آورده شده است **[۲۱]:**

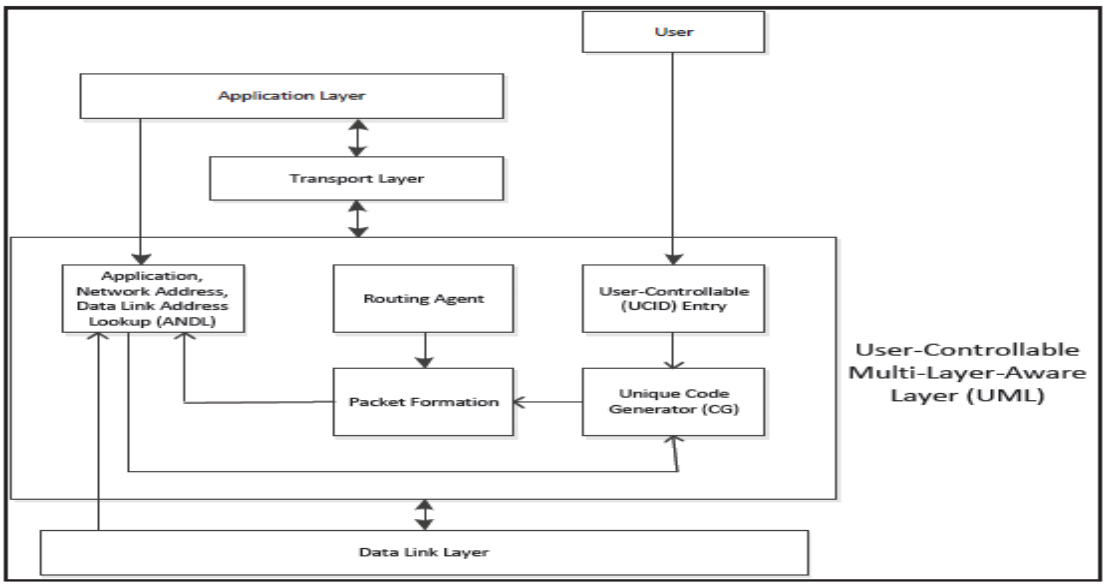
۱. قابلیت منزوی سازی دستگاه های اینترنت اشیاء بر اساس شناسه‌های قابل کنترل کاربران (UCID[2])، ابزارهای لایه کاربرد، آدرس فیزیکی و آدرس شبکه
۲. قابلیت تعریف منطقی و وفقی شبکه بر اساس دستگاه های اینترنت اشیاء
۳. فرآیند همزمان شکل‌گیری شبکه و احراز هویت دستگاه‌ها
۴. جلوگیری از نفوذ غیر مجاز از طریق افزودن اطلاعات امنیتی در پروتکل مسیریابی

SMRP پشته پروتکلی را در لایه شبکه در به صورت زیر تغییر می‌دهد:

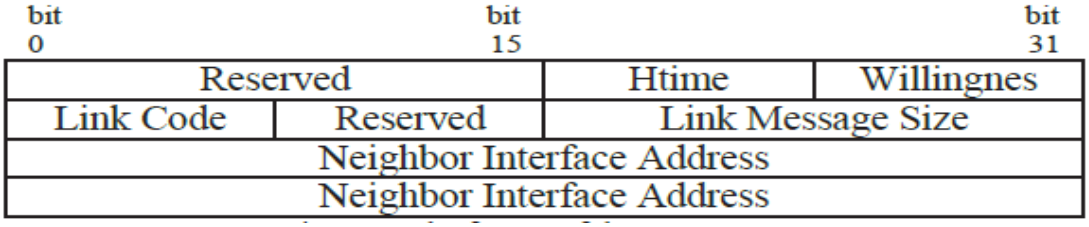
لایه شبکه SMRP با فراهم سازی شناسه کاربری قابل کنترل UCID و همچنین کاربردهای توافق شده، آدرس فیزیکی و آدرس لایه شبکه توسط ماژول ANDL [3]این اطلاعات به ماژول تولید شناسه یکتا(CG[4]) ارسال می‌گردد (شکل ۲-۵). در نتیجه این کار یک شناسه یکتا جهت احراز هویت دستگاه‌ها

توسط ماژول CG تولید گشته و مطابق شکل زیر در قالب بسته‌های Hello (شکل شماره ۲-۶) و در قسمت رزرو می‌گیرند **[۲۱].**

1-Secure Multi-Hop Routing For Iot
2-User_Controllable Entry
3-Application , Network Address , DataLink Address Lookup
4-Unique Code Generator

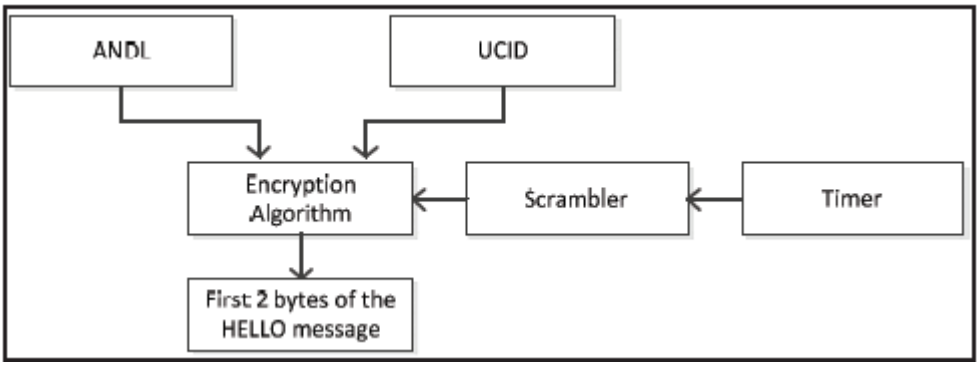


شکل ۲-۵ : پشته پروتکلی در روش SMRP [۲۱]



شکل ۲-٦ : سرآیند پیام Hello در روش SMRP [۱۱]

تولید شناسه یکتا توسط ماژول CG در شکل ۲-۷ نمایش داده شده است



شکل ۲-۷ : عملکرد Unique Code Generator (CG) در روش SMRP [۱۱]

در این ماژول همانطور که در شکل شماره ۲-۷ مشاهده می‌گردد زمان، شناسه UCID و اطلاعات فراهم شده توسط ماژول ANDL جهت تولید شناسه یکتا ۲ بایتی به الگوریتم رمزنگاری داده می‌شود. برای جلوگیری از شکل‌گیری رفتار بدخواهانه در این روش فراهم‌کنندگان سرویس، وسایل اینترنت اشیاء را بر اساس کاربردها، آدرس‌های فیزیکی وآدرس شبکه ثبت می‌نمایند. در نتیجه این فرآیند یک دستگاه به صورت پیشفرض قبل از پیوستن به شبکه دارای یک فایل رمز شده به وسیله‌ی فراهم کننده‌ی می‌باشد**[۲۱].**

دستگاه های SMRP از طریق ارسال پیام Hello به صورت همه‌پخشی به کشف همسایگان خود در بازه‌های زمانی مختلف اقدام می‌نمایند. با دریافت یک پیام Hello از طرف دستگاه همسایه در یک گره، سرآیند آن بررسی و تنها اگر بر اساس اطلاعات احراز هویت تولید شده در قسمت قبل دو دستگاه در یک شبکه باشند ارتباط برقرار می‌گردد. دو دستگاه در دو شبکه‌ی متفاوت، اجازه‌ی برقراری ارتباط را نخواهند داشت **[۲۱].**

این روش با عدم احراز هویت گره مخرب نگرانی‌های زیر را کاهش می‌دهد:

- سیاه‌چاله
- Sinkhole : در این حملات گره مخرب با حذف برخی از بسته‌های ورودی سعی بر هدر دادن منابع شبکه می‌نماید. تشخیص Sinkhole از حمله سیاه‌چاله سخت‌تر است.
- حملات جعل‌هویت

۲-۳-۳. روش VERA[1]

این روش با استفاده از زنجیره درهم‌سازی به مقابله با حملات کاهش مقدار Rank و جعل شماره ورژن در پروتکل RPL می‌پردازد. در این روش هر شماره ورژن، یک عضو از زنجیره درهم‌سازی مربوط به شماره ورژن‌ها می‌باشد (V_N,…..V_0). از طریق رابطه ۲-۷ می‌توان هر شماره ورژن را محاسبه نمود. در این رابطه h تابع درهم‌ساز، r عدد تصادفی و n بزرگترین شماره ورژن در زنجیر درهم‌سازی می‌باشند.

$$V_i = h^{n+1-i}(r) \qquad [۷-۲]$$

مقادیر Rank در شماره ورژن i با زنجیره درهم‌سازی دیگری نمایش داده می‌شود($R_{i,0}$,…..,$R_{i,l}$). مقدار Rank یکم در شماره ورژن i ام از طریق رابطه شماره ۲-۸ محاسبه می‌گردد. در این رابطه x_i عدد تصادفی است**[۲۲].**

$$R_{i,l} = h^{l+1}(x_i) \qquad [۸-۲]$$

گره ریشه در پروتکل RPL با این روش در هنگام شروع، پیام $\{V_0,INT_{VN},R_{1,l},\{V0,MAC_{v1}(R1,l)\}_{sign}\}$ را منتشر می‌نماید.گره‌های دریافت کننده بسته در صورت تایید امضا به مقادیر v_0 (شماره ورژن شروع رنجیر درهم‌سازی مربوط به شماره ورژن‌ها) و $R_{l,1}$ (بزرگترین مقدار Rank در زنجیره درهم‌ساز مربوط به شماره ورژن ۱) دسترسی پیدا می‌کنند. گره ریشه در آپدیت‌های

1-Version Number and Rank Authentication in RPL

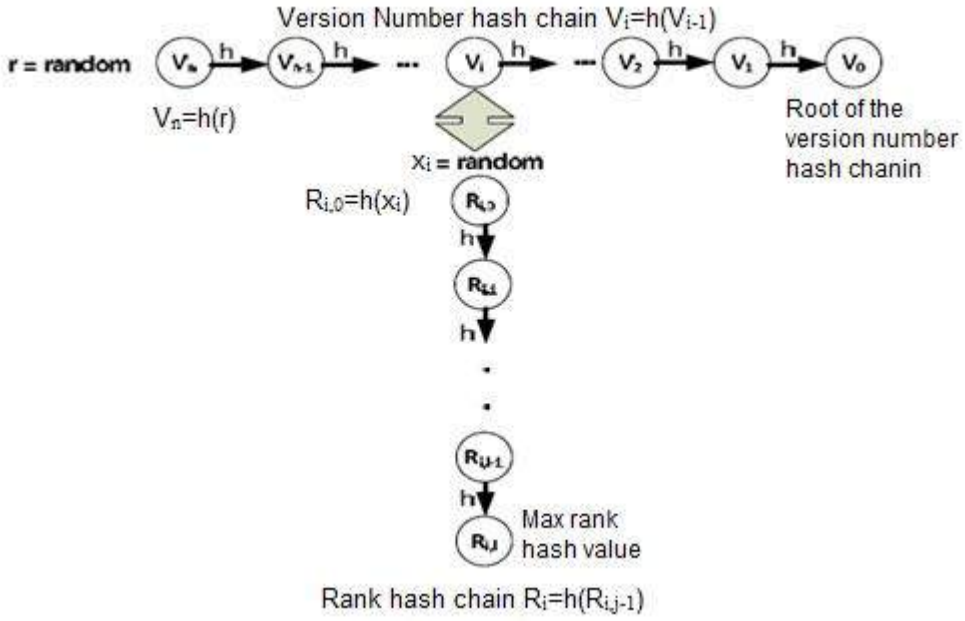
بعدی بسته $\{V_i , Init_{VN} + I, MAC_{Vi+1}(R_{I+1,l})\}$ را منتشر و سپس هر گره می‌تواند از طریق رابطه ۲-۹ به بررسی شماره ورژن بپردازد.

$$h(V_i) == V_{i-1} \qquad [۹-۲]$$

در نهایت هر گره می‌تواند بررسی مقدار RANK مربوط به پدر (j) در یک شماره ورژن را نیز از طریق رابطه ۲-۱۰ انجام دهد.

$$^{1}MAC_{Vi}(Ri,l) == MAC_{Vi}(h^{l-j}(R_{i,j})) \qquad [۱۰-۲]$$

با این روش حملات جعل شماره ورژن و یا تغییر در مقدار RANK تشخیص داده می‌شوند**[۲۲]**. شکل ۲-۸ زنجیره‌های درهم سازی در این روش را نشان می‌دهد. در این شکل زنجیره شماره ورژن به صورت افقی و زنجیره شماره Rank به صورت عمودی نمایش داده شده است.



شکل ۲-۸ : زنجیره‌های درهم‌سازی در روش VERA

از نقاط ضعف این روش می‌توان به موارد زیر اشاره کرد:

- آسیب‌پذیری در برابر حملات تکرار، ایجاد حملات جدید، عدم پیاده‌سازی و آنالیز

2-Message Authentication Code

- گم شدن بسته‌های کنترلی در صحت روش مربوطه موثر است.

۲-۳-٤. روش TRAIN

پژوهشگران در سال ۲۰۱۳ دو آسیب‌پذیری برای VERA ارائه کردند. این آسیب‌پذیری‌ها در لیست زیر آورده شده است **[۲۳]:**

۱- گره مخرب با جلوگیری از دریافت دو بروزرسانی متوالی آغازین گره ریشه در سنسورها توانایی ساخت هر Mac در روش VERA را داراست. به عنوان مثال گره مخرب با جلوگیری از دریافت بروزرسانی‌های V1 و V2 می‌تواند از طریق جعل زنجیره hash $R_{2,j}^{'}$ هر مقدار Rank دلخواهی را برای فرزندان خود ارسال نماید. گره مخرب این کار را از طریق کلید V2 موجود در بروزرسانی دوم انجام می‌دهد.

۲- امکان حمله تکرار برای زنجیره hash مربوط به والد یک گره در محدوده ارسال خود وجود دارد. با این کار گره مخرب مقدار Rank خود را کوچکتر از مقدار حقیقی نشان می‌دهد.

در روش TRAIN بهبودهایی برای VERA جهت مقابله با آسیب‌پذیری‌های فوق ارائه شده است **[۲۳].**

۱- پژوهشگران در این روش علت رخداد آسیب‌پذیری اول را عدم سازگاری و ارتباط کامل زنجیره Rank و زنجیره مربوط به ورژن‌ها می‌دانند. بر این اساس در این روش یک رمزنگاری تودرتو برای افزایش پیچیدگی این دو زنجیره پیشنهاد شده است. در این روش تمام عناصر زنجیره Rank برای تمام ورژن‌ها به صورت یک‌جا تولید شده و آخرین عنصر آن در سایر عناصر به کمک رمزنگاری مرتبط می‌شود. این امر مطابق جدول شماره صورت می‌گیرد.

جدول ۲-۱ : ارتباط عناصر زنجیره Rank با کمک رمزنگاری در روش TRAIN

$R_{i,l}$	use key k_i	cipher $c_i = enc_{k_i}()$
$R_{n,l}$	–	$c_n = R_{n,l}$
$R_{n-1,l}$	$k_{n-1} = c_n$	$c_{n-1} = enc_{k_{n-1}}(R_{n-1,l})$
...	...	...
$R_{2,l}$	$k_2 = c_3$	$c_2 = enc_{k_2}(R_{2,l})$
$R_{1,l}$	$k_1 = c_2$	$c_1 = enc_{k_1}(R_{1,l})$

همانطور که در جدول شماره مشاهده می‌گردد آخرین عنصر زنجیره Rank رمزشده و به عنوان کلید در رمزنگاری عنصر n-1ام به کار می‌رود. با این امر تغییر یک عنصر در گره مخرب موجب شکست در رمزگشایی و دسترسی به مقدار $R'_{i-1,l}$ نامعتبر در گره فرزند خواهد شد. به این ترتیب رابطه ۲-۸ (در روش VERA) در گره فرزند ناصحیح می‌گردد.

۲- برای مقابله با آسیب‌پذیری دوم از یک روش مبتنی بر چالش و پاسخ بر اساس زنجیره مقدار Rank استفاده شده است. در این روش گره مخرب (A) دارای مقدار Rank برابر با j+1 به علت حضور در محدوده ارسال پدر خود می‌تواند با حمله تکرار، مقدار Rank مربوط به پدر خود (گره B) را به جای Rank خود معرفی نماید. گره پدر(B و غیر مخرب) با مقدار Rank برابر با j پس تولید یک عدد تصادفی و رمزنگاری آن با $R_{i,j-1}$، نتیجه حاصله را به پدر خود (C) ارسال می‌نماید. گره پدر با این کار تقاضای رمزنگاری عدد تصادفی مربوطه را بر اساس زنجیره Rank در پدر خود (یعنی $R_{i,j-2}$) را می‌نماید.گره C با دریافت و رمزگشایی این پیام به رمزنگاری آن با $R_{i,j-2}$ می‌پردازد. این گره در نهایت نتیجه را به گره B برمی‌گرداند. گره B نیز با ارسال این مقدار به گره مخرب، از وی تقاضای بازارسال عدد تصادفی جهت احراز هویت را می‌نماید. گره مخرب به دلیل عدم دسترسی به مقدار $R_{i,j-2}$ از این کار عاجز است.

این روش با نگرانی‌های زیر در پروتکل RPL مقابله می‌نماید:

حمله شماره ورژن و حمله کاهش مقدار Rank

از نقاط ضعف این روش می‌توان به سربار نسبتا بالا بر گره‌های اینترنت اشیاء و تاثیر گم شدن بسته‌های کنترلی بر صحت کارکرد اشاره نمود.

۲-۳-۵. روش بررسی Rank[۱]

اساس این روش نیز زنجیره درهم‌سازی است. در این روش گره ریشه به انتخاب یک عدد تصادفی و درهم سازی آن می‌پردازد. این مقدار در پیام DIO منتقل شده و هر گره با دریافت آن مجدد تابع درهم‌سازی را اجرا می‌نماید. سپس مقدار حاصله مجدد به صورت پیام DIO منتشر می‌نماید. در حملات Sinkhole گره مخرب با هدف نزدیک‌تر شدن به ریشه پیام را بدون درهم‌سازی منتقل می‌سازد. هدف از این کار کاهش مقدار RANK و دلیل آن عدم دسترسی به مقدار درهم‌سازی شده در گره پدر است. در این روش هر گره مقدار درهم‌سازی ارسالی توسط پدر خود را ذخیره می‌نماید. پس از گذشت زمان و همگرایی درخت DODAG در هر گره‌ی N_i روابط زیر برقرار است **[۲٤]**.

$$\begin{aligned} p &= \hat{Rank}(N_i) \\ \hat{Rank}(N_i) &= Rank(N_i) - E_{\text{path}(i)} \end{aligned} \qquad [۱۱-۲]$$

$\hat{Rank}(N_i)$ به معنی تعداد درهم‌سازی‌های انجام شده بر روی N_i است. همچنین مقدار $E_{path(i)}$ نشان-دهنده تعداد گره‌های به خطر افتاده در مسیر بین گره N_i تا ریشه است(در این روش فرض بر افزایش مقدار Rank به صورت یک واحد در هر گام است). پس از گذشت زمان لازم برای اطمینان از همگرایی درخت

۱-Rank Verification

DODAG ریشه شروع به ارسال مقدار X_0 به صورت همه‌پخشی ایمن [۱]می‌نماید. هر گره در درخت با دریافت این مقدار می‌تواند X_p را با توجه به $\hat{Rank}(N_i)$ محاسبه نموده و با مقدار X_p حاصل از پدر خود مقایسه نماید. به این ترتیب برخی رفتار مخربانه تشخیص داده خواهد شد **[۲٤]**.

این روش با نگرانی‌های زیر در پروتکل RPL مقابله می‌نماید:

حملات Sinkhole و کاهش مقدار Rank

از نقاط ضعف مربوط به این روش می‌توان به سربار زیاد، ایجاد حملات جدید و همچنین تاثیر گم شدن بسته‌های کنترلی بر عملکرد روش مربوطه اشاره نمود.

۲-٤. تغییر در پروتکل مسیریابی

در این روش‌ها پژوهشگران از طریق افزودن و یا تغییر پروتکل‌مسیریابی RPL سعی بر رفع نگرانی‌های امنیتی این پروتکل می‌نمایند. در ادامه برخی از روش‌ها از این نوع معرفی خواهند شد.

۲-٤-۱. روش Parent Fail-Over

این روش از طریق عدم دریافت تعداد مشخصی از پیام‌ها در یک بازه زمانی خاص در گره ریشه (توسط سایر گره‌های درخت DODAG) وجود حمله Sinkhole را تشخیص می‌دهد. در این روش گره ریشه به پیام‌های DIO لیستی از گره‌هایی که این تعداد پیام از آنها دریافت نشده است اضافه می‌نماید. هر گره با دریافت یک پیام DIO حاوی نام خود پدر ارجح را در لیست سیاه محلی خود قرار داده و به تعمیر شرایط می‌پردازد **[۲٤]**.

از نقاط ضعف این روش می‌توان به موارد زیر اشاره کرد:

- این روش در برابر حملات Sybil و جعل هویت آسیب پذیر بوده
- انتخاب آستانه ناصحیح می‌تواند عملکرد این روش را با مشکل روبرو و حتی رفتار صحیح پروتکل به صورت حمله تلقی گردد.

۲-٤-۲ روش آستانه وفقی برای تشخیص ناسازگاری در RPL

پروتکل RPL در برابر ناسازگاری‌ها رفتار مشخصی از خود نمایش می‌دهد. پژوهشگران پس از بررسی این رفتار متوجه شدند که این پروتکل در برابر برخی ناسازگاری‌ها به طور بهینه عمل نمی‌کند. این موضوع به مهاجم اجازه می‌دهد که با ایجاد ناسازگاری‌های ساختگی در عملکرد RPL مشکلاتی به وجود آورده و حتی باعث تغییر توپولوژی درخت DODAG گردد **[۱٤]**.

طراحان پروتکل RPL برای اجرای رفتار مقابله‌ای با برخی ناسازگاری‌ها آستانه‌ای (عدد ۲۰) را بدون ذکر دلیل برای تعداد رخداد ناسازگاری‌ها در درخت DODAG در نظر گرفته‌اند. بر این اساس برخی حملات

۲-Secure

با سوءاستفاده از این ضعف موجود در پروتکل RPL به وجود آمدند. دانشمندان در این پژوهش متوجه شدند که با تغییر این آستانه به برخی مقادیر خاص، پروتکل RPL در برابر این حملات از خود رفتار بهینه‌تری نشان داده و فرصتی برای رسیدن به اهداف بداندیشانه برای گره مخرب پیش نمی‌آید **[۱٤].**

در نهایت پژوهشگران در سال ۲۰۱۵ تصمیم به تغییر این آستانه ثابت و تنظیم آن به صورت سازگار با شرایط شبکه گرفتند. این کار می‌تواند تاثیر حملات ناسازگاری در پروتکل RPL را کاهش دهد.

در این پژوهش آستانه به شکل زیر و به صورت وفقی محاسبه می‌گردد **[۱٤]:**

$$\lambda(r) = \lfloor \alpha + \beta.e^{-\Upsilon r} \rfloor$$

$$r = \frac{count(R)}{D(pkt)} \quad \alpha = 5, \beta = 15 \qquad [۱۲-۲]$$

طبق آزمایش های انجام شده بهترین مقدار برای Υ در بازه $20<\Upsilon<35$ می‌باشد.

Count R مقدار بسته های دارای ناسازگاری دریافت شده

D pkt تعداد بسته های معمولی دریافت شده

نکته : مقدار اولیه α جهت اطمینان از نرسیدن مقدار $\lambda(r)$ به مقدار صفر می‌باشد.

در این روش تا قبل از رسیدن تعداد پیام‌های دارای ناسازگاری به مقدار α تمام پیام‌ها بازارسال می-گردند. با گذر تعداد پیام‌های ناسازگار دریافتی از مقدار α محاسبه مقدار $\lambda(r)$ شروع می‌گردد. پس از این محاسبه تنها اگر تعداد پیام‌های ناسازگار از مقدار $\lambda(r)$ کمتر باشد پیام دریافتی حذف و زمان‌سنج ارسال DIO به مقدار اولیه تنظیم می گردد. از این طریق گره مخرب فرصت زیادی برای اجرای حمله ناسازگاری نداشته و با سرعت بیشتری به این نوع رفتار مخربانه واکنش نشان داده می‌شود **[۱٤].**

۲-۵. روش‌های با ایده سیستم تشخیص نفوذ

راه‌حل‌های این دسته به نوعی از ایده سیستم تشخیص نفوذ برای تشخیص رفتار مخربانه در RPL استفاده می‌نمایند. در این روش‌ها گره ریشه برای مقابله با نگرانی‌های RPL مشابه سیستم تشخیص نفوذ به بررسی بازخوردهای دریافتی از شبکه می‌پردازد. در ادامه یک نمونه از این روش‌ها را معرفی می‌نماییم.

۲-۵-۱. روش SVELTE

این روش یک سیستم تشخیص نفوذ برای اینترنت اشیاء است. SVELTE دارای سه ماژول می‌باشد که همگی در گره ریشه پیاده‌سازی می‌گردند. در ادامه به معرفی این ماژول‌ها پرداخته شده است **[۲۵].**

۱- 6LowpanMapper

این ماژول با ارسال یک پیام به تمام گره‌ها درخواست ارسال مجموعه‌ای از اطلاعات را تقاضا می‌نماید. هر گره با دریافت این پیام ارسال اطلاعات دوره‌ای به گره ریشه را شروع خواهد نمود. از جمله این اطلاعات می‌توان به شماره گره، شماره ورژن، پدر ارجح ، مقدار Rank و لیست همسایگان اشاره نمود. بنابراین از طریق این ماژول اطلاعات مربوط به گره‌های درخت به صورت دوره‌ای جمع‌آوری و به ریشه ارسال خواهد گردید. این ماژول یک دید کلی از درخت DODAG به گره ریشه خواهد بخشید.

۲- ماژول تشخیص

در این ماژول بر اساس اطلاعات دریافتی از طریق ماژول 6LowpanMapper به تشخیص ناسازگاری‌ها پرداخته می‌شود. یکی از ناسازگاری‌های مورد بررسی در این ماژول ناسازگاری در مقدار Rank است. در بررسی ناسازگاری‌های Rank تفاوت این مقدار در یک گره بر اساس دید ریشه (دید کلی) با مقدار Rank در دید همسایگان گره مربوطه (بر اساس اطلاعات ماژول 6LowPanMapper) پرداخته می‌شود. در صورتی که تفاوت این دو مقدار از میانگین در هر دو دید بیش از ۲۰ درصد باشد یک نقص برای هر دو گره ثبت می‌گردد. همچنین در بررسی‌ای دیگر اگر مقدار Rank یک گره از این مقدار در پدرش به اندازه حداقل افزایش مقدار Rank در یک گام کوچکتر باشد آنگاه به مقدار نقص‌های گره مربوطه یک واحد افزوده می‌گردد. در نهایت اگر تعداد نقص‌های یک گره بیش از یک آستانه مشخص باشد آنگاه گره مورد نظر مخرب تشخیص داده شده و از درخت حذف می‌گردد (البته SVELTE یک بار به گره مربوطه قبل از حذف شدن فرصت مجدد می‌دهد). در این ماژول بررسی ناسازگاری‌های دیگری نیز از جمله تشخیص در دسترس بودن گره‌ها صورت می‌پذیرد.

۳-ماژول دیواره آتش

در این ماژول یک دیواره آتش با قابلیت‌های محدود جهت محافظت گره‌های کم توان در درخت DODAG از شبکه اینترنت صورت می‌گیرد.

این روش می‌تواند با حملات زیر از نگرانی‌های مربوط به پروتکل RPL مقابله نماید:

حمله کاهش مقدار Rank، حملات Blackhole و Sinkhole و حملات مربوط به شناسایی[۱]

از نقاط ضعف این روش می‌توان به امکان هشدارهای اشتباه و عدم تشخیص حمله، امکان دید اشتباه شبکه در ماژول 6LowPanMapper، وجود سربار محاسباتی و ارتباطی و تاثیر گم شدن بسته‌های کنترلی بر صحت کارکرد روش اشاره نمود.

۲-۵-۲. روش تشخیص رفتار مخربانه از طریق ارسال هشدارها

در این روش هشدارهای مختلف از طریق گره‌های درخت به ریشه ارسال می‌گردد. ریشه درخت از طریق این هشدارها به تشخیص رفتار مخربانه کاهش مقدار Rank خواهد پرداخت. در این روش هر گره برای ارسال هشدار به ریشه به جای مقدار Rank جاری از آخرین مقدار همه‌پخشی آن به همسایگان استفاده

۱-Identity

می‌نماید. ریشه با دریافت این مقادیر ضمن در نظر گرفتن ناسازگاری‌های زمانی در اندازه‌گیری مقدار Rank، به تشخیص رفتار مخربانه در حمله کاهش Rank می‌پردازد. در این روش از یک مهر زمانی نیز برای کاهش هشدارهای اشتباه (به عنوان مثال ناشی از گم شدن بسته‌ها) استفاده می‌گردد **[۱۶].**

از نقاط ضعف این روش می‌توان به موارد زیر اشاره کرد:

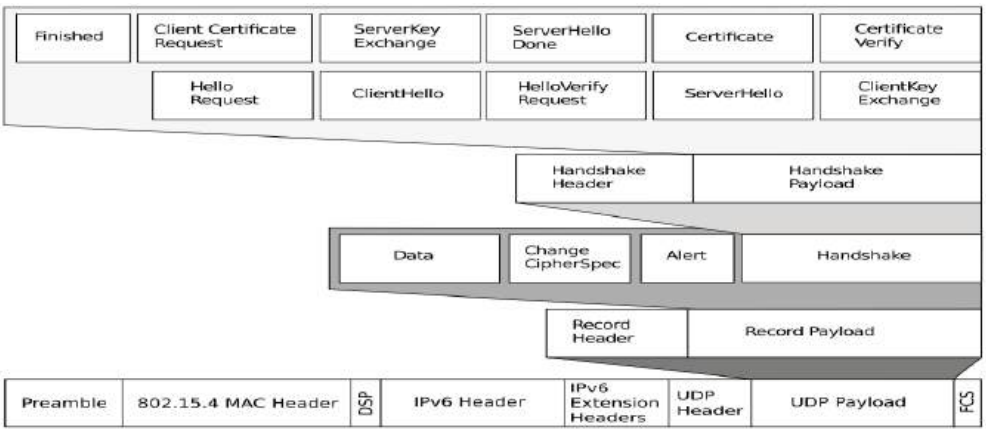
- همچنان هشدارهای اشتباه وجود دارند
- این روش سربار محاسباتی در ریشه ایجاد می‌نماید.

۲-۶. تطبیق مکانیسم های امنیتی در سایر لایه ها جهت محدود کردن حملات لایه ی شبکه

پروتکل‌های رایج امنیتی (در ارتباطات) به دلیل عدم سازگاری با ماهیت دستگاه‌های کم توان در اینترنت اشیا و همچنین احتمال گم شدن بالای پیام‌ها در این تکنولوژی قابل استفاده نیستند. به عنوان مثال پروتکل DTLS یا لایه انتقال امن به دلیل سربار و تعداد ارسال‌های بالا جهت ایجاد جلسه و احراز هویت دستگاه‌ها، مناسب استفاده در این تکنولوژی نیست. بر این اساس برخی پژوهشگران به دنبال تطبیق پروتکل‌های رایج امنیتی به گونه‌ای سازگار با اینترنت اشیا حرکت کردند. به این ترتیب این تکنولوژی نیز می‌تواند از مزایای این پروتکل‌های مورد امتحان قرار گرفته بهره‌مند گردد. در ادامه به یک مورد از این پژوهش‌ها اشاره شده است.

۲-۶-۱. پروتکل COAP سبک وزن

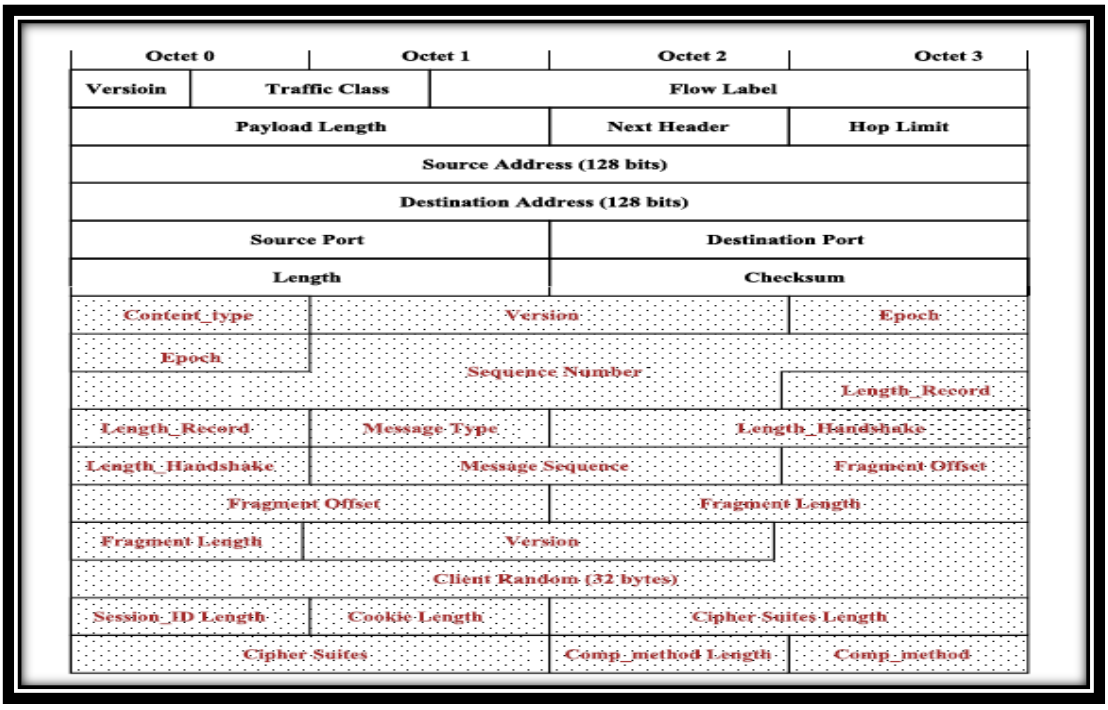
در این پژوهش هدف محققان استفاده از مکانیسم فشرده‌سازی موجود در تکنولوژی 6lowpan جهت فشرده سازی پروتکل‌های امنیتی انتها به انتهای معروف نظیر DTLS است. از این طریق می‌توان با برخی حملات موجود در لایه شبکه از طریق ایمن‌سازی در لایه‌های بالاتر مقابله نمود **[۲۶]**.



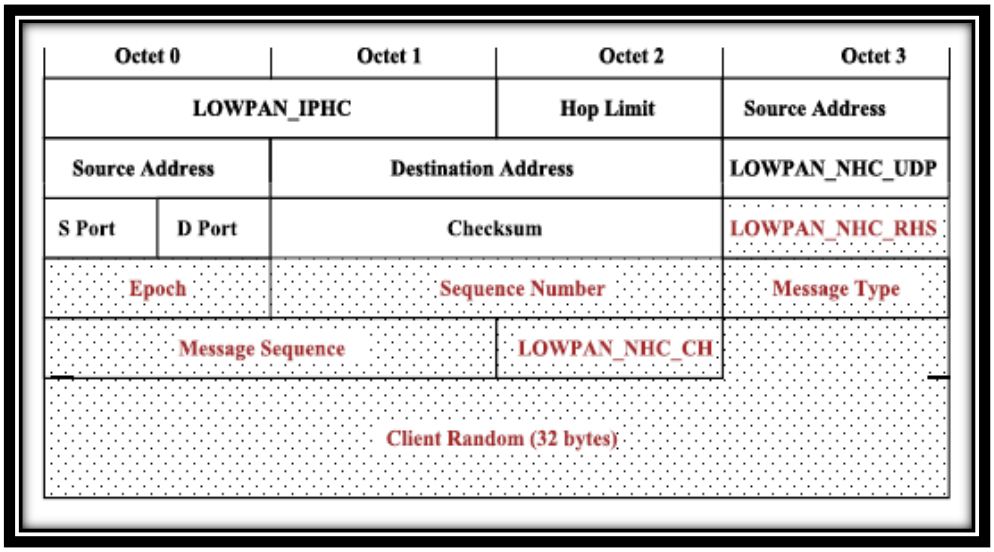
شکل ۲-۹: چگونگی قرارگیری اطلاعات در بسته ایمن شده با پروتکل DTLS [۱۹]

ساختار بسته ایمن به وسیله پروتکل DTLS در شکل شماره ۲-۹ نشان داده شده است. دانشمندان در این پژوهش با حذف و یا فشرده‌سازی برخی از قسمت‌های پیام در این شکل از جمله فیلد طول پیام ، ورژن در پروتکل DTLS و همچنین استفاده از مکانیسم فشرده‌سازی تکنولوژی 6lowpan در قسمت‌های Record و Handshake از پروتکل DTLS توانستند دیتاگرام IP/UDP شکل ۲-۱۰ (شامل یک CLIENT Hello Message) را به صورت شکل شماره ۲-۱۱ فشرده نمایند. به این ترتیب دستگاه‌های اینترنت اشیاء می‌توانند از مزایای پروتکل DTLS (امنیت انتها به انتها و در لایه انتقال) بهره‌مند گردند **[۲۶].**

این روش برخی نگرانی‌های لایه شبکه از جمله حملات تکرار را رفع می‌نماید. این روش را یک تجمیع از تکنولوژی COAP و DTLS فشرده شده برای به کار گیری در اینترنت اشیاء در نظر گرفت.



شکل ۲-۱۰ : دیتاگرام IP/UDP (شامل یک Client Hello Message) [۲۶]



شکل ۲-۱۱ : دیتاگرام فشرده‌شده شکل ٤-۲ [۲٦]

۲-۷. مقایسه

در این قسمت می‌توان مقایسه برخی کارهای پیشین را در قالب جدول ۲-۲ مشاهده نمود. در این جدول برخی از کارهای پیشین ارائه شده در رفع نگرانی‌های RPL به همراه دسته‌بندی آنها بر اساس شکل ۲-۱، لیست حملات مورد مقابله، بستر پیاده‌سازی و نقاط ضعف هر یک آورده شده است.

بر اساس پژوهش‌های موجود در جدول شماره ۲-۲ می‌توان برخی موارد در رابطه با نگرانی‌های امنیتی در RPL را استخراج نمود (بدیهی است که موارد مذکور تمام پژوهش‌های این حوزه نیست):

۱. تعداد راه‌حل‌ها برای رفع نگرانی‌های مربوط به توپولوژی در پروتکل RPL نسبت به سایرین بیشتر می‌باشد.
۲. برای برخی نگرانی‌ها در RPL تا به امروز هیچ راه‌حلی ارائه نشده است (از جمله حمله انتخاب بدترین والد و Flooding).
۳. در رابطه با حملات بر ضد منابع راه‌حل‌های بسیار معدودی ارائه شده است.
۴. راه‌حل‌های مبتنی بر احراز هویت بیشترین سهم در پژوهش‌های مربوط به رفع نگرانی‌های RPL را داراست.

جدول ۲-۲: کارهای پیشین در یک نگاه

نام پژوهش	دسته مربوطه	مقابله با حملات	پیاده سازی	ضعف
روش مدیریت گروه بر اساس اعتماد [۵۱]	اعتماد	حملات Black hole	Sensi	Cluster Headها در گروه داخلی برای ارتباط با گره Sink نیاز به مصرف انرژی زیادی دارند که باعث مصرف باتری سنسور Cluster Head می گردد
روش SVELTE [۴۸]	سیستم تشخیص نفوذ	حمله کاهش مقدار Rank	Cooja	هنوز فقط تست و پیاده سازی شده است،دارای سربار محاسباتی می‌باشد.امکان ارسال هشدارهای اشتباه همچنان وجود دارد.
روش TRAIN [۳۶]	احراز هویت	حمله شماره ورژن و حمله کاهش مقدار Rank	پلتفرمRIOT	سربار بالا، مشکل در مقیاس‌پذیری،گم شدن بسته‌های کنترلی در روش موثر است
روش بررس Rank [۳۵]	احراز هویت	حمله Sinkhole و حمله کاهش مقدار Rank	نا مشخص	سربار بالا و ایجاد حملات جدید، مشکل در مقیاس-پذیری، گم شدن بسته‌های کنترلی در روش موثر است
مسیریابی چندگامی ایمن برای اینترنت اشیا [۲]	احراز هویت	حملات Grayhole,blackhole، sinkhole و حملات جعل هویت	Physical Testbed	سربار بالا، مشکل در مقیاس‌پذیری
روش TSRF [۸]	اعتماد	حملاتOn-off حملات conflicting, behavior, حملات selfish badmouthing, و حملاتcollusion	Ns2	مصرف حافظه، سربار محاسباتی،مشکل وجود حافظه تاریخی در محاسبه اعتماد که میتواند حملات جدیدی را به وجود آورد
روش اعتماد بر اساس تصدیق دو گامی [۴]	اعتماد	حملاتselfish ،جعل هویت Blackhole , و حملات behavior	Ns2	عدم تشخیص حمله چاله خاکستری، و در محاسبه اعتماد حالت شبکه نقشی ندارد زیرا از گره های همسایه بازخوردی نمی‌گیرد.
کاهش ناسازگاری‌های توپولوژی در RPL[۲۰]	تغییر در پروتکل مسیریابی RPL	حمله ناسازکاری در Dodag	Cooja Contiki	امکان حمله همچنان وجود دارد
جلوگیری از حمله Wormhole با استفاده از درخت مرکل [۱۴]	احراز هویت	حمله Wormhole	Unknown	سربار ارتباطی و پردازشی به همراه دارد
روش Lithe [۱۹]	تطبیق مکانیسم های امنیتی در سایر لایه ها جهت محدود کردن حملات لایه ی شبکه	حمله Fragmentation	Cooja Contiki	با وجود فشرده سازی همچنان سربار پردازشی و رمزنگاری وجود دارد و همچنان در مقابل حملات نظیر Blackhole , Sinkhole و غیره آسیب پذیر می باشد
روش Vera [۳۴]	احراز هویت	حمله کاهش مقدار Rank و حمله Sinkhole	None	آسیب‌پذیری در برابر حملات تکرار، ایجاد حملات جدید، عدم پیاده‌سازی و آنالیز و گم شدن بسته‌های کنترلی در روش موثر است
روش Parent Fail Over [۳۵]	تغییر در پروتکل مسیریابی	حمله Sinkhole	Unknown	این روش در برابر حملات SYBIL و جعل هویت آسیب پذیر بوده و همچنین انتخاب آستانه ناصحیح می‌تواند عملکرد این روش را با مشکل روبرو و رفتار صحیح پروتکل حمله تلقی گردد.

۲-۸. نتیجه‌گیری

در این فصل راه‌حل‌های ارائه شده جهت مقابله با حملات لایه شبکه در پروتکل RPL دسته‌بندی و مورد بررسی قرار گرفت. همچنین در انتهای این فصل نیز به مقایسه این راه‌حل‌ها پرداخته شد. بر اساس مطالب موجود در این فصل برخی نگرانی‌های پروتکل RPL (از جمله حمله انتخاب بدترین والد) همچنان وجود داشته و تا کنون هیچ راه‌حلی برای آن‌ها ارائه نشده است. برخی دیگر از راه‌حل‌های امنیتی موجود در RPL نیز دارای نقاط ضعف فراوانی می‌باشند. با توجه به این امر و اهمیت امنیت در اینترنت اشیا (قسمت ۱-۴) نیاز به ارائه راه‌حلی برای کاهش نگرانی‌های RPL به عنوان بخش مهمی از این تکنولوژی است. نگرانی‌های بدون راه‌حل ارائه شده تا کنون از اولویت بیشتری (با توجه به اهمیت تمام نگرانی‌ها) برخوردار هستند.

فصل سوم

روش پیشنهادی

با توجه به کارهای پیشین انجام شده نیاز به ارائه راه حلی برای مقابله با برخی حملات نظیر حمله کاهش مقدار Rank و حمله انتخاب بدترین والد بیش از سایرین احساس می‌گردد. حتی در مورد این دو حمله نیز تفاوت‌هایی وجود دارد. حمله کاهش مقدار Rank راه‌حل‌های معدودی را داراست اما در مورد حمله انتخاب بدترین والد تقریبا تا به امروز هیچ راه حلی ارائه نشده است. بنابراین بر اساس نیاز در این پژوهش بر آن شدیم که به ارائه راه حلی برای مقابله با حمله انتخاب بدترین والد در پروتکل RPL بپردازیم.

۳-۱ .مدل مهاجم

در این پژوهش یک یا چند مهاجم با امکان دسترسی فیزیکی به یک یا چند سنسور دلخواه در درخت DODAG وجود دارد. مهاجم بدون هیچگونه محدودیتی به تمام کلیدها و اطلاعات موجود در گره‌های قربانی دسترسی دارد. این گره‌های قربانی بدون هیچ گونه مشکل در شبکه RPL شرکت نموده و به ارسال پیامهای مختلف (پیام‌های احراز هویت شده) می پردازند. در این پژوهش توانایی مهاجم محدود به منابع در گره‌های قربانی فرض شده است. به این ترتیب مهاجم نمیتواند آنتن‌های مستقیم ایجاد نموده و یا شناسه‌های مختلف داشته باشد.

۳-۲ .چرا بسیاری از حملات برای سوء استفاده از آسیب‌پذیری‌های RPL قابلیت اجرایی دارند؟

با توجه به بررسی‌های انجام شده دلیل شکل‌گیری بسیاری از حملات موجود برای سوء استفاده از آسیب-پذیری‌های پروتکل RPL عدم نظارت پدر بر رفتار فرزندان در تغییر پدر ارجح است. بنابراین رفتار مخربانه‌ی فرزندان در این امر از دید پدر مخفی می‌ماند **[۱۳].**

لیست زیر نشان‌دهنده حملاتی است که به نوعی از این نقطه ضعف سوءاستفاده می‌کنند:

۱-حمله انتخاب بدترین والد
۲-حمله کاهش مقدار Rank
۳-حمله افزایش مقدار Rank
۴-اضافه کردن اطلاعات جعلی در جداول مسیریابی گره ها
۵-حملاتی که برای جذب ترافیک از کاهش مقدار Rank استفاده می‌نمایند.

۳-۳ .راه‌حل پیشنهادی CPC-RPL (Change Parent Control RPL)

برای رفع این مشکل(با محوریت حمله انتخاب بدترین والد) در ادامه پژوهش یک روش کارآمد جهت تشخیص رفتار مخربانه در تغییر پدر ارجح و بازگرداندن پروتکل RPL (در صورت امکان) به حالت عادی ارائه شده است. برای این‌کار ضمن مطالعه رفتار پروتکل RPL در شرایط مختلف به بررسی چگونگی ایجاد حمله‌ی انتخاب بدترین

والد پرداخته شد. نتیجه این امر تشخیص تفاوت تغییر پدر ارجح توسط گره مخرب به صورت ارادی (حمله انتخاب بدترین والد) با زمان تغییر پدر ارجح بر اساس پروتکل و در شرایط عادی است.

در ادامه پس از تعریف مفاهیم زیر (مهم در درک ادامه مطالب) به این تفاوت‌ها اشاره می‌نماییم:

۱-پدر مور اشاره قبلی: گره‌ای که در اثر حمله انتخاب بدترین والد توسط گره مخرب به عنوان پدر ارجح انتخاب شده است.

۲-پدر ارجح جدید: گره‌ای که در اثر حمله انتخاب بدترین والد توسط گره مخرب از عنوان پدر ارجح تغییر یافته است.

۳-٤ .معیارهای تغییر پدر ارجح توسط یک گره در پروتکل RPL

در پروتکل RPL معیارهای متفاوتی برای تغییر پدر ارجح وجود دارد:

۱-بر اساس مقدار Rank

فرآیند انتخاب پدر ارجح بر اساس تعداد گام‌های بین گره مربوطه تا ریشه صورت می‌گیرد.

۲-بر اساس مقدار انرژی

فرآیند انتخاب پدر ارجح بر اساس مقدار انرژی باقی‌مانده در لیست پدران صورت می‌گیرد.

۳-بر اساس مقدار تخمین ETX

فرآیند انتخاب پدر ارجح بر اساس تعداد ارسال‌های لازم جهت دریافت بسته‌های ارسالی در ریشه است.

ETX : به معنی تعداد انتقال‌های مورد انتظار برای دریافت سالم یک بسته به مقصد مورد نظر است. مقدار ETX بین ۰ تا بینهایت متغیر می‌باشد.

$$\mathrm{ETX} = \frac{1}{1 - e_{pt}} \qquad [۱-۳]$$

e_{pt} : احتمال خطای بسته

نکته : مقدار ETX معمولا عددی بین ۲,۵ تا ۱ است.

سه معیار فوق در قالب دو تابع هدف زیر قرار می‌گیرند. در پروتکل RPL گره‌ها با توجه به تابع هدف به تغییر پدر ارجح ، بروزرسانی مقدار Rank و تغییر درخت DAG در صورت لزوم می‌پردازند.

۱-تابع 0OF

فقط معیار RANK در این تابع برای تغییر پدر ارجح وجود دارد.

۲-تابع MRHOF (The Minimum Rank with Hysteresis)

هر یک از ۳ معیار معرفی شده می‌توانند در این تابع هدف جهت انتخاب پدر ارجح مورد استفاده قرار گیرند. به صورت پیشفرض معیار ETX جهت این امر انتخاب شده است.

در این پژوهش تابع هدف 0OF (در نتیجه معیار RANK) جهت سادگی بیشتر انتخاب شده است. انتخاب سایر معیارها تاثیری در اصل روش پیشنهادی نخواهد داشت.

در تابع 0OF تغییر پدر ارجح بر اساس رابطه زیر صورت می‌گیرد:

$$M= Rank+ETX \qquad [۲-۳]$$

یک گره در هنگام انتخاب پدر ارجح از بین دو والد خود، گره‌ی با مقدار کمینه‌ی M را انتخاب خواهد نمود. مقدار Rank و ETX هر دو بدون واحد هستند. همچنین مقدار ETX در مقابل Rank بسیار کوچک بوده و تنها در اثر خروج گره والد از شبکه (به هر دلیل) می‌تواند از مقدار RANK بیشتر گردد(ETX<2 و RANK>256). مقدار RANK با ارسال پیام‌های DIO به صورت همه پخشی از طریق والدین به فرزندان رسیده و به این ترتیب گره مربوطه اقدام به محاسبه معیار بالا خواهد نمود.

برای تغییر پدر ارجح در یک گره باید اختلاف حداقل مقدار M مربوط به پدر ارجح فعلی و یکی از والدین بیش از یک آستانه مشخص باشد. دلیل این امر پایداری شبکه به‌وسیله جلوگیری از تغییرات زیاد پدر ارجح است. این آستانه با انتخاب معیارهای مختلف در تابع هدف برای انتخاب پدر ارجح تغییر خواهد نمود (این تغییر تنها تفاوت روش پیشنهادی در اثر تغییر معیار انتخاب پدر ارجح است).

با توجه به رابطه‌ی بالا می‌توان دلایل تغییر در پدر ارجح به صورت زیر در نظر گرفت:

$$\text{مقدار آستانه} <= |M_{\text{پدر ارجح جدید}}| - |M_{\text{پدر ارجح قبلی}}| \qquad [۳-۳]$$

این معادله بر اساس پروتکل RPL تنها می‌تواند در یکی از حالات زیر صحیح باشد:

۱- معیار M (M≈RANK) در پدر ارجح قبلی افزایشی بیش از مقدار آستانه داشته باشد.

۲- معیار M در پدر ارجح جدید کاهشی بیش از مقدار آستانه داشته باشد.

۳-مجموع میزان افزایش معیار M در پدر ارجح قبلی و کاهش این معیار در پدر ارجح جدید بیش از مقدار آستانه باشد.

مقدار RANK تاثیر مستقیم در مقدار M داشته و تغییرات مقدار ETX به تنهایی نمی‌تواند باعث تغییر پدر ارجح گردد (به جز در حالات خاص). دلیل تغییرات مربوط به مقدار RANK در یک گره تنها می‌تواند تغییر پدر ارجح توسط یکی از اجداد گره مذکور باشد.دلیل تغییرات مربوط به ETX را نیز می‌توان تغییرات RSSI، حرکت گره‌ها، Fadding و مشکلات مربوط به سیگنال‌ها در نظر گرفت. پدر ارجح جدید و قبلی با افزودن مکانیسمی به پروتکل RPL می‌توانند از مقدار تغییر مقدار M (تغییر مقدار RANK) خود در هر لحظه آگاه گردد.

با توجه به موارد موثر در تغییر پدر ارجح سعی بر ارائه روشی توزیع شده بر اساس تغییرات ضمنی شبکه شده است. روش پیشنهادی در این پژوهش بر اساس اعتماد به مسیرها (گره‌ها) است.

بر اساس ITU[1]-T X.509 قسمت ۳,۳,۵۴ اعتماد به صورت زیر تعریف شده است:

v‘یک موجودیت در صورتی می‌تواند ادعا کند که موجودیت دیگری مورد اعتماد وی است که آن دقیقا مطابق با انتظار وی عمل نماید.

اعتماد در RPL می‌تواند بر اساس معیارهای متفاوتی تعریف گردد. در برخی از پژوهش‌های انجام شده در RPL محاسبه اعتماد بر اساس موارد زیر صورت گرفته است :

۱- بر اساس تعداد بسته‌های دریافت شده در یک همسایه نسبت به تمام بسته‌های ارسالی به گره مذکور (از این تعریف برای تشخیص حمله Sinkhole استفاده شده است) [۱۸] .
۲- اعتماد به صورت اعتماد مستقیم در همسایگان و گزارش‌های غیر مستقیم از سایر گره‌ها (اعتماد غیر مستقیم) بر اساس موارد موثر در تغییر پدر مورد اشاره تعریف می‌گردد. این روش تعریف اعتماد تعمیم روش TSRF در کارهای پیشین به پروتکل RPL است [۲۰].

اعتماد در روش پیشنهادی به دلیل استفاده از نشانه‌های خاص برای تشخیص حمله انتخاب بدترین والد نمی‌تواند به صورت روش‌های بالا تعریف گردد. دلیل این امر در لیست زیر آورده شده است:

- نشانه‌های تشخیص حمله عوامل موثر در اعتماد را تغییر می‌دهد.
- در تشخیص حمله انتخاب بدترین والد نشانه‌های رفتار مخربانه باید در یک نقطه دارای دید کلی از شبکه دریافت (ریشه) و سپس تصمیم‌گیری صورت گیرد. بر این اساس به دلیل وجود احتمال عدم تعامل مستقیم ریشه با گره مخرب تنها اعتماد غیر مستقیم می‌تواند مورد استفاده قرار گیرد.

با توجه به تعریف اعتماد و نوع خاص مسئله مربوطه (تشخیص مخرب بودن یا مخرب نبودن گره‌ها در حمله انتخاب بدترین والد) که یک دسته‌بندی با خروجی و ورودی‌های گسسته است (ورودی مسئله دریافت نشانه‌های

1 .International Telecomunication Union

خاص است) اعتماد در این روش به صورت کیفی (معادله ۳-۴) و در چند سطح (گسسته) نسبت به هر مسیر تعریف شده است.

$$\text{اعتماد}: \begin{cases} \text{خیلی بالا} \\ \text{بالا} \\ \text{متوسط} \\ \text{پایین} \\ \text{خیلی پایین} \end{cases} \qquad [۴-۳]$$

در این روش موارد زیر برقرار است:

۱- هر گره مسئول نظارت بر رفتار فرزندان خود می‌باشد.
۲- گره پدر در صورت مشاهده رفتار مخربانه توسط فرزند (تغییر پدر ارجح به صورت خارج از قوانین پروتکل RPL)، به رفتار وی مشکوک می‌گردد.
۳- این موضوع (مشکوک شدن) به ریشه اطلاع داده می‌شود.

ریشه با دید کلی از تمام درخت و بازخوردهای مختلف، اعتماد به مسیرها را محاسبه و ثبت می‌نماید.کاهش اعتماد در ریشه متناسب با گزارش‌های مشکوکانه توسط گره‌های درخت است.
این اعتماد کیفی در پیاده‌سازی به اعداد نظیر می‌گردد. به این ترتیب امکان ترکیب روش پیشنهادی با هر روش محاسبه اعتماد دیگر نظیر موارد نامبرده نیز وجود دارد.

$$\text{اعتماد}: \begin{cases} \text{خیلی بالا} \\ \text{بالا} \\ \text{متوسط} \\ \text{پایین} \\ \text{خیلی پایین} \end{cases} \Rightarrow \begin{cases} 4 \\ 3 \\ 2 \\ 1 \\ 0 \end{cases} \qquad [۵-۳]$$

رابطه کاهش میزان اعتماد با توجه به دریافت گزارش مشکوکانه را می‌توان به صورت زیر تعریف نمود:

- دریافت گزارش مشکوکانه حاوی شک زیاد به یک آدرس پیشوندی = کاهش اعتماد آدرس پیشوندی به صورت زیاد در ریشه
- دریافت گزارش مشکوکانه حاوی شک کم به یک آدرس پیشوندی = کاهش اعتماد آدرس پیشوندی به صورت کم در ریشه

در صورت کاهش اعتماد یک مسیر به مقدار پایین و خیلی پایین (اعتماد<۱)، گره ریشه می‌تواند وقوع حمله در درخت را تشخیص داده و مکانیسم بازیابی را جهت بازگرداندن درخت به شرایط صحیح عملکردی بر اساس

پروتکل را اجرا نماید. همچنین نقاط منفی یک مسیر در ریشه به مرور زمان از بین رفته و اعتماد به آن مسیر مجددا افزایش خواهد یافت.

فرضیات روش CPC-RPL :

۱- میزان اعتماد در همه مسیرها در شروع پروتکل مقدار بالا است.
۲- حملات در لحظه شروع به کار شبکه نمی‌توانند رخ دهند.

۳-۵ .روش تشخیص حمله

در این قسمت مکانیسم‌ها و معیارهای اصلی مورد استفاده در روش پیشنهادی جهت تشخیص حمله ارائه شده است.

۳-۵-۱ .مکانیسم محاسبه تغییر مقدار RANK در آخرین بازه زمانی

در این روش ابتدا هر گره در بازه‌های زمانی مشخص، تغییر مقدار Rank را محاسبه می‌نماید. در صورتی که این مقدار، تغییر قابل توجهی نسبت به مقدار قبلی اندازه گیری شده (آخرین مقدار ارسالی در پیام DIO قبلی) داشته باشد این تغییر در گره و به صورت متغیری به نام change Mval ثبت می‌گردد.

۳-۵-۲ .بازه زمانی در محاسبه تغییر مقدار RANK

فرزندان با دریافت پیام‌های DIO متوجه تغییر مقدار Rank در والدین خود می‌گردند. به این دلیل بازه زمانی محاسبه تغییر مقدار Rank در یک گره به صورت اختلاف زمان ارسال دو پیام DIO به صورت متوالی در نظر گرفته خواهد شد.

۳-۵-۳ .توازن بین سربار ناشی از پیام‌های مشکوک مربوط به روش پیشنهادی و دقت روش

انتقال پیام حاوی اطلاعات مربوط به شک توسط پیام‌های DAO به سمت ریشه صورت می‌گیرد. در پیام DAO تنها قسمت بلااستفاده (۸ بیت) برای ثبت میزان شک،کوچکتر از مقدار Rank (۱۶ بیت) است.بنابراین با ارسال مقدار دقیق تغییر Rank و بدون نشانه‌ای از میزان شک به ریشه سربار زیادی به پروتکل RPL تحمیل خواهد گردید(تعداد ارسال‌ها بسیار افزایش خواهند یافت). بنابراین جهت محدود کردن تعداد پیام‌های مشکوک به یک مقدار قابل قبول نشانه‌های شک تنها مطابق جدول زیر (که به عددی کوچک نظیر می‌گردد) در پیام‌های DAO قرار می‌گیرند.

جدول ۳-۱ : وضعیت‌های تغییر Rank در پدر ارجح جدید و قبلی در بازه زمانی اخیر

پدر ارجح قبلی \ پدر ارجح جدید	کاهش بالا	کاهش پایین	افزایش بالا	افزایش پایین	عدم تغییر
کاهش بالا					
کاهش پایین					
افزایش بالا					
افزایش پایین					
عدم تغییر					

رنگ بنفش نشان‌دهنده وضعیت‌های با امکان عدم تشخیص صحیح حمله است. دلیل این امر عدم امکان نتیجه-گیری قاطع بر اساس مقدار آستانه مربوط به تغییر پدر ارجح است. در تمام این حالات هر دو پدر ارجح قبلی و جدید در یک بازه زمانی کوتاه باید اقدام به تغییر مقدار Rank خود و تبلیغ آن پرداخته باشند. رخداد این تغییرات به صورت تقریبا همزمان بسیار نادر است(در قسمت‌های بعد این مورد بررسی شده است).

رنگ سبز نشان‌دهنده وضعیت‌های عادی در پروتکل RPL برای تغییر پدر ارجح است.

رنگ قرمز وضعیت‌های وجود حمله و غیر عادی در پروتکل RPL را برای تغییر پدر ارجح نشان می‌دهد.

پدر ارجح جدید از بین حالات جدول شماره ۳-۱ تنها هنگام وجود امکان رخداد حمله در ردیف آخرین تغییر مقدار Rank خود به ارسال پیام مشکوک می‌پردازد. همچنین پدر ارجح قبلی نیز تنها در حالاتی از جدول فوق به ارسال پیام مشکوک می‌پردازد که در ستون مربوطه امکان وقوع حمله وجود داشته باشد. برای ارسال مقدار دقیق Rank نیز می‌توان از گزینه‌های اختیاری استفاده کرد. دلیل عدم ارسال مقدار دقیق Rank در روش پیشنهادی افزایش قابل توجه سربار اجرایی با افزایش پردازش‌های ناشی از گزینه‌های اختیاری موجود در پیام‌های DAO است.

هر گره هنگام محاسبه تغییر مقدار Rank یکی از مقادیر زیر را به عنوان میزان تغییر Rank به ریشه ارسال می‌نماید

- ۰ به معنی عدم تغییر
- ۱ به معنی با افزایش پایین
- ۲ به معنی افزایش بالا
- ۳ به معنی کاهش پایین
- ۴ به معنی کاهش بالا

میزان شک گره به رفتار مخربانه فرزند خود به صورت ضمنی در این عدد نهفته است. این امر متناظر با تعداد خانه‌های قرمز جدول ۳-۱ است. به صورتی که اگر تعداد این خانه‌ها دو برابر سایرین باشد آنگاه میزان شک گره به فرزند خود زیاد و در صورتی که تعداد خانه‌های قرمز کمتر از این مقدار باشد این میزان کم می‌باشد. همچنین در صورت عدم وجود خانه قرمز گره پدر نسبت به فرزند خود هیچگونه شکی نخواهد داشت. این میزان شک به صورت گزارش مشکوکانه به ریشه ارسال خواهد گردید. تشخیص حمله مربوطه بر اساس دریافت بازخورد از هر دو پدر ارجح قبل و بعد در حمله مربوطه صورت خواهد گرفت (ضمنی یا غیر ضمنی). به عنوان مثال دریافت دو پیام متوالی حاوی گزارش مشکوکانه از پدر ارجح قبلی (بدون دریافت بازخورد از پدر ارجح جدید) موجب کاهش اعتماد به مقدار پایین و خیلی پایین نخواهد گردید.

دلیل اصلی انتخاب ۵ سطح در تعریف اعتماد وجود گزارش‌های مشکوکانه متفاوت توسط پدر ارجح قبلی و بعدی در حمله انتخاب بدترین والد است. اصلی‌ترین دلیل استفاده از مفهوم اعتماد در این روش نسبت به روش‌های دیگر (نظیر درخت تصمیم) عدم وجود قطعیت در تشخیص رفتار مخربانه است. عدم قطعیت و اعتماد دو مفهوم جدایی ناپذیر هستند.

۳-۵-٤ .مشکوک شدن گره پدر به فرزند

فرآیند مشکوک شدن گره پدر به رفتار فرزندان خود در تغییر پدر ارجح در محل گره پدر و از طریق دریافت نشانه‌هایی از فرزندان صورت می‌گیرد. دلیل این امر وجود دید محلی در گره‌های درخت DODAG و در نتیجه گره پدر است. در ادامه این نشانه‌ها و فرآیند تولید گزارش مشکوکانه بر اساس هر یک در گره پدر را شرح خواهیم داد.

نوع اول : بر اساس پیام عدم وجود مسیر

هر گره با دریافت یک پیام عدم وجود مسیر از فرزندان مستقیم مقدار تغییر Rank خود در بازه اخیر را محاسبه

نموده و پس از آن مطابق جدول شماره ۶ به گره مربوطه مشکوک شده و پیام DAO را ضمن تنظیم مقدار شک در قسمت رزرو به سمت ریشه ارسال می‌نماید. به این ترتیب پیام DAO به همراه مسیر مشکوک به ریشه خواهد رسید.

نوع دوم : بر اساس دریافت یک مسیر با گام بعدی متفاوت نسبت به جدول مسیریابی فعلی

در صورت ایجاد یک مسیر رو به پایین جدید (با دریافت پیام DAO) با وجود آن با گام بعدی متفاوت در جدول مسیریابی گره مورد نظر به گام بعدی جدید در این مسیر (فرزند وی) مشکوک خواهد شد. این گره سپس در قسمت بیت‌های رزرو شده در پیام DAO مقدار متغیر Changemval را ثبت و پیام DAO را به پدر ارجح خود بازارسال می‌نماید. به این ترتیب پدر ارجح گره مربوطه نیز از موضوع مطلع خواهد شد. هر گره با دریافت پیام

DAO در صورت تنظیم مقدار Change Mval در آن،پیام مربوطه را با مقدار Change Mval قبلی به سمت پدر ارجح خود بازارسال می نماید. به این ترتیب پیام DAO به همراه مسیر مشکوک به ریشه خواهد رسید.

۳-۵-۵ .تغییر در جداول مسیریابی ریشه

جداول مسیریابی در ریشه با افزودن مقدار اعتماد به هر ردیف آن (یعنی هر مسیر) تغییر می‌نماید. در حالت اولیه این مقدار دارای میزان اعتماد بالا به هر مسیر می‌باشد (مقدار۴).

۳-۵-٦ .گم شدن بسته‌های کنترلی

پیام‌های کنترلی در پروتکل مسیریابی RPL در قالب بسته‌های ICMPv6 کپسوله می‌گردند. بنابراین احتمال مفقودی در ارسال برای آنها وجود دارد. برای حل این مشکل قابلیت اعتماد برای ارسال پیام‌های مشکوک با کمترین سربار به پروتکل UDP با استفاده از مکانیسم DAO-ACK موجود در RPL اضافه شده است.

۳-۵-۷ .رفتار پدر ارجح قبلی پس از حمله

هر گره براساس پروتکل RPL باید هنگام تغییر پدر ارجح بلافاصله با ارسال یک پیام عدم وجود مسیر (شامل آدرس خود) پدر ارجح قبلی را نیز باخبر سازد. گره والد با دریافت این پیام آدرس مربوطه را از جدول مسیریابی خود حذف می‌نماید. هر گره با حذف یک مسیر از جدول مسیریابی (به شرط اینکه آدرس مورد نظر مربوط به یکی از فرزندان مستقیم باشد) مقدار Change Mval محاسبه شده‌ی خود را در قسمت رزرو مربوط به پیام DAO قرار می‌دهد. سپس به وسیله‌ی ارسال قابل اعتماد[1] این پیام به پدر ارجح ، عدم وجود این مسیر از طریق خود را اطلاع می‌دهد. پدر ارجح نیز به دلیل تنظیم مقدار Change Mval در این پیام، آن را مجدد به سمت ریشه به صورت قابل اعتماد بازارسال می‌نماید. با توجه به افزودن قابلیت اعتماد احتمال گم شدن این بسته‌ها وجود ندارد.

۳-۵-۸ .رفتار ریشه در دریافت پیام DAO حاوی عدم وجود یک مسیر

با رسیدن این پیام به ریشه در صورت عدم وجود اعتماد نسبت به این مسیر (مطابق جدول شماره ۶) کاهش اعتماد نسبت به مسیر مربوطه در ریشه صورت می‌گیرد. در صورت کاهش شدید مقدار اعتماد (به مقدار پایین) وقوع حمله‌ی انتخاب بدترین والد تشخیص داده شده و مکانیسم بازیابی اجرا می‌گردد. در غیر این‌صورت میزان اعتماد براساس جدول شماره ۶ کاهش خواهد داشت.

نکته : در صورت رخداد حمله انتخاب بدترین والد پیام مشکوک از نوع عدم وجود مسیر زودتر از پیام مشکوک از نوع دریافت مسیر جدید با گام بعدی متفاوت بنابر دلایل زیر زودتر به ریشه خواهد رسید (به جز در موارد خاص):

۱- پیام از نوع عدم وجود مسیر از طریق مسیر کوتاه‌تر به سمت ریشه می‌رود.

1-Reliable

۲- پیام از نوع عدم وجود مسیر زودتر ارسال می‌گردد.

۳-۵-۹ .رفتار روش پیشنهادی در صورتی که مقدار ETX از مقدار Rank بیشتر گردد

در روش پیشنهادی هر گره در این حالت یک نشانه مشخص به پیام DAO اضافه می‌نماید. و با این کار علت تغییر پدر ارجح خود را به پدر جدید اطلاع می‌دهد. پدر جدید نیز با تنظیم مقدار شک و بازارسال پیام DAO ریشه را از این موضوع مطلع می‌سازد. گره ریشه با دریافت این پیام میزان اعتماد به آدرس مربوطه را کاهش می‌دهد. گره مخرب با هدایت ترافیک از طریق پدر ارجح جدید باعث حذف برخی مسیرها (به دلیل اتمام زمانسنج) در پدر ارجح قبلی و در نتیجه ارسال پیام مشکوک به سمت ریشه می‌گردد. گره ریشه با کاهش اعتماد حمله مربوطه را تشخیص می‌دهد. در هنگام ارسال این پیام توسط پدر ارجح قبلی ابتدا دسترسی به گره مربوطه را بررسی (وضعیت لینک) نموده و در صورت عدم دسترسی پیام DAO را بدون هیچگونه نشانه شک به سمت ریشه ارسال می‌نماید.

۳-۵-۱۰ .افزایش اعتماد به هر مسیر در ریشه

اعتماد کاهش یافته در هر مسیر در صورت عدم مشاهده رفتار مخربانه پس از گذشت مدتی مشخص دوباره به مقدار اولیه بازخواهد گشت. دلیل این امر حذف بی‌اعتمادی دائمی از مسیرهاست. افزایش اعتماد با توجه به دلیل تغییر پدر ارجح متفاوت است. در ادامه به این تفاوت‌ها اشاره می‌گردد:

۱. در حالتی که معیار Rank عامل تغییر پدر ارجح باشد: در این حالت کاهش اعتماد پس از گذشت حداکثر زمان تاخیر پیام در شبکه (T) و عدم تشخیص رفتار مخربانه به مقدار اولیه باز خواهد گشت.

۲- ETX>Rank عامل تغییر پدر ارجح می‌باشد : گره ریشه در صورت عدم اعتماد کامل به یک مسیر(اعتماد<۴) در هر ثانیه مقدار $\frac{\text{مقدار کاهش یافته}}{255+T}$ را به اعتماد اضافه می‌نماید. به این ترتیب نقاط منفی مربوط به مسیرها در ریشه با گذشت زمان از بین خواهند رفت. دلیل انتخاب این عدد دوره مربوط به عملکرد روش پیشنهادی است. این دوره به اندازه پایان زمانسنج و ارسال پیام عدم وجود مسیر در پروتکل RPL (به اندازه ۲۵۵) است.

۳-۶ .بهبود روش پیشنهادی

روش پیشنهادی در حالت فرزندی پدر ارجح جدید برای پدر ارجح قبلی رفتار مخربانه را تشخیص نمی‌دهد. برای حل این مشکل در مرحله مشکوک شدن پدر به گره فرزند بررسی زیر نیز به روش پیشنهادی افزوده شده است.

۱- آیا گام بعدی قبلی به عنوان فرزند گره مربوطه در حال حاضر می‌باشد؟ با صحیح بودن این مورد مقدار شک به صورت بسیار زیاد افزایش پیدا کرده و در پیام DAO تنظیم می‌گردد.

با این کار پدر ارجح قبلی به گره مخرب بسیار زیاد مشکوک می‌گردد.(اطمینان از مخرب بودن گره)

۳-۷ .مکانیسم بازیابی

در مورد حمله انتخاب بدترین والد مکانیسم بازیابی و حذف گره مخرب کارآمد نیست. زیرا حذف گره مخرب می‌تواند پیامدهای زیر را همراه داشته باشد:

۱- منزوی شدن زیر درخت مربوط به گره مخرب
۲- ایجاد سربار و تاخیر با حذف گره مخرب بر روی زیر درخت گره مخرب

در حمله انتخاب بدترین والد هدف گره مخرب ایجاد تاخیر در ارسال‌های مربوط به زیر درخت خود می‌باشد. با حذف گره مخرب در مکانیسم بازیابی و ارسال ترافیک از طریق مسیر دیگر به طور مجدد این سربار و تاخیر به وجود خواهد آمد. اما در مورد برخی دیگر از حملات نظیر حمله کاهش مقدار Rank که حذف گره مخرب موجب افزایش کارایی شبکه می‌گردد مکانیسم حذف گره مخرب از طریق روش لیست سیاه صورت می‌گیرد.

۳-۷-۱ .روش لیست سیاه برای حذف گره مخرب

در این روش گره ریشه پس از تشخیص گره مخرب در پیام‌های DIO خود آدرس گره مخرب را منتشر می‌نماید. هر گره با دریافت این آدرس آن را از لیست پدران خود خارج می‌نماید.

۳-۸ .اثبات صحت کارکرد روش پیشنهادی

در این قسمت به اثبات صحت کارکرد روش پیشنهادی بر اساس برهان خلف پرداخته شده است.

فرضیات در اثبات :

حمله انتخاب بدترین والد : در این حمله گره مخرب پدر ارجح خود را خارج از قوانین پروتکل RPL تغییر می‌دهد. در پروتکل RPL تغییر پدر ارجح با استفاده از تابع 0OF بر اساس معیار زیر صورت میگیرد:

$$M=Rank+Parent\ Link\ Metric \qquad [۳-۶]$$

تعاریف

$$Pa1= \text{پدر ارجح قبلی} \qquad [۳-۷]$$

$$Pa2= \text{پدر ارجح جدید}$$

هر گره برای تغییر پدر ارجح خود حداقل مقدار آستانه مشخصی را می‌پذیرد. تغییر پدر ارجح براساس پروتکل RPL تنها در صورتی انجام شود که مقدار M مربوط به پدر ارجح جدید دارای مقدار کمتری نسبت به پدر ارجح قبلی باشد و این مقدار از آستانه نیز بیشتر باشد.

بر این اساس :

M1 € Pa1 [۸-۳]

M2 € Pa2

تغییر پدر ارجح تنها در صورت برقراری معادله زیر اتفاق خواهد افتاد:

|M1|-|M2|>= مقدار آستانه [۹-۳]

این معادله به این معنی است که

۱- مقدار تغییر گره Pa1 به اندازه مقدار آستانه افزایش داشته و مقدار pa2 تغییر نکرده
۲- مقدار تغییر گره Pa2 به اندازه مقدار آستانه کاهش داشته و مقدار pa1 تغییر نکرده
۳- کاهش مقدار pa1 و افزایش مقدار pa2 در مجموع از آستانه بیشتر است

اثبات به روش برهان خلف

قضیه شرطی ۱: اگر تغییر پدر ارجح در گره ای بر اساس قوانین پروتکل RPL باشد آنگاه گره مربوطه گره‌ی مخرب (حمله انتخاب بدترین والد) نیست.

اگر تغییر پدر ارجح بر اساس قوانین پروتکل نباشد=P

گره مخرب نیست=Q [۱۰-۳]

P=>Q

فرض می کنیم نقیض حکم صحیح است

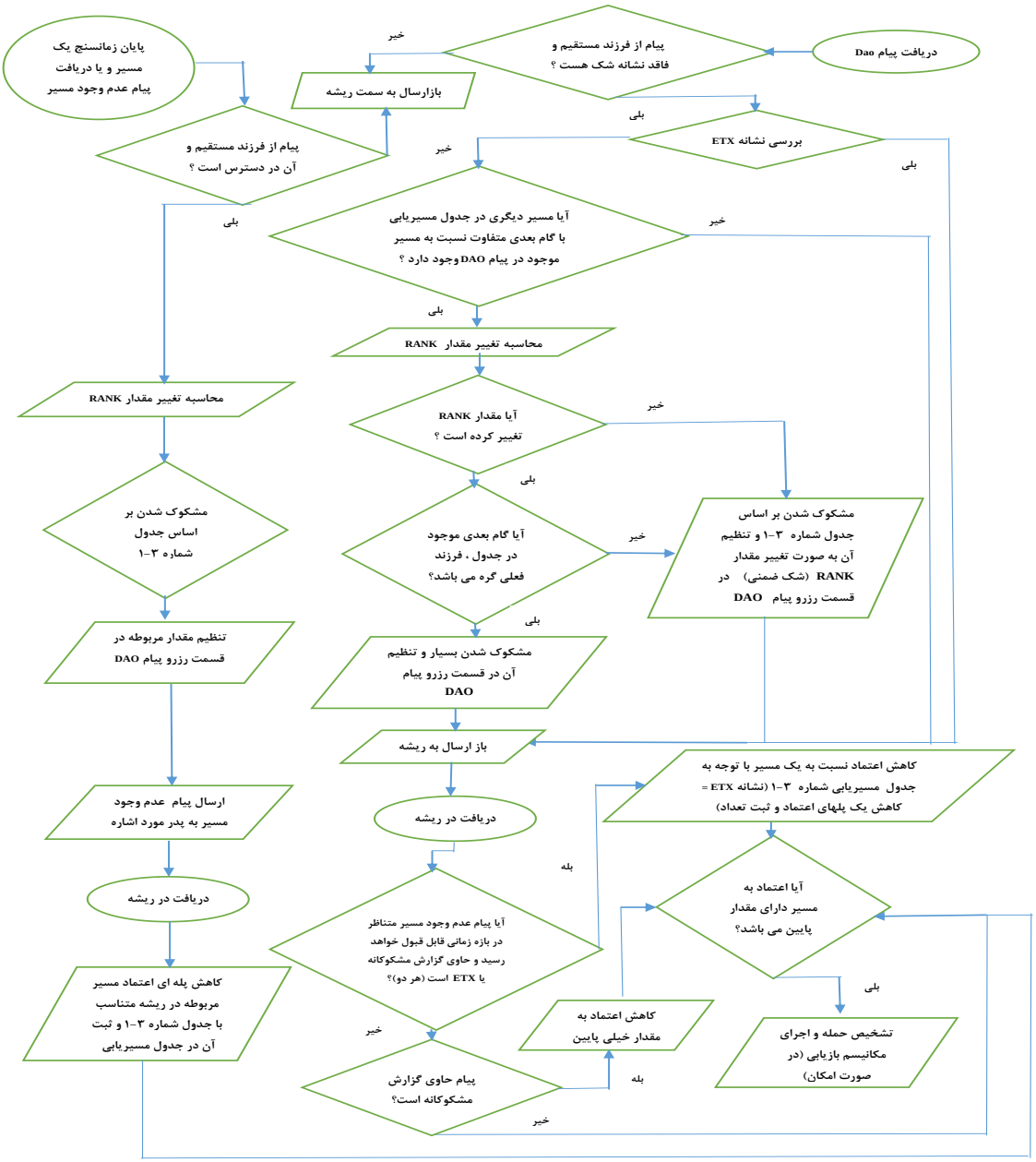
گره مخرب است=Q~ [۱۱-۳]

اگر گره مورد نظر حمله انتخاب بدترین والد را اجرا نماید. باید خارج از قوانین پروتکل پدر ارجح خود را تغییر دهد. بنابراین معادله زیر برقرار نبوده و فرض غلط است. در نتیجه حکم مربوطه صحیح خواهد بود.

|M1|-|M2|<= مقدار آستانه [۱۲-۳]

۳-۹ .فلوچارت روش پیشنهادی

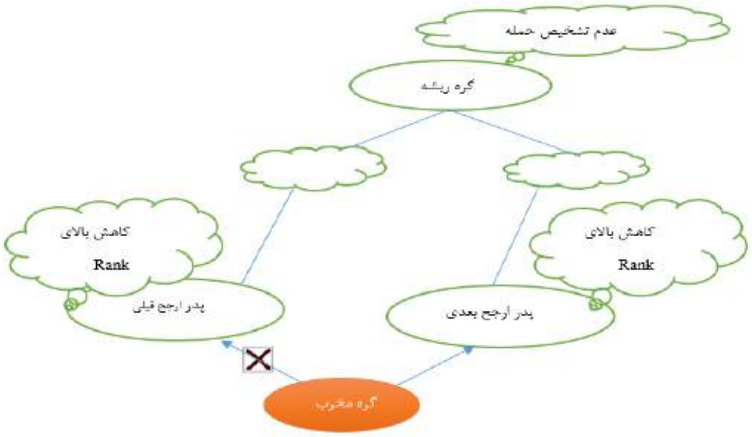
در شکل زیر می‌توان فلوچارت روش پیشنهادی را مشاهده نمود.



شکل ۳-۱ : فلوچارت روش پیشنهادی

۳-۱۰ . سناریو عدم تشخیص حمله توسط روش پیشنهادی

در حالاتی که پدر ارجح قبل و بعد در حمله انتخاب بدترین والد در وضعیت‌های بنفش بر اساس جدول ۳-۱ قرار داشته باشند و گزارش‌های مشکوکانه خود را در این حالت منتشر نمایند آنگاه بر اساس روش پیشنهادی و آستانه تغییر پدر ارجح نمی‌توان به صورت قاطع وقوع رفتار مخربانه را نتیجه‌گیری نمود. به عنوان نمونه در ادامه یکی از این حالات آورده شده است.



شکل ۳-۲ : سناریو عدم تشخیص حمله

در این شکل لحظه وقوع حمله توسط گره مخرب نشان‌داده شده است. بر اساس روش پیشنهادی پدران ارجح قبل و بعد در حمله انتخاب بدترین والد کاهش بالای Rank را در این لحظه (بر اساس آخرین انتشار پیام DIO) به دلیل شرایط شبکه دارند. بر اساس روش پیشنهادی گزارش‌های مشکوکانه دریافتی در ریشه با عدم تشخیص حمله مواجه خواهد شد. زیرا اعتماد مربوط به گره مخرب در ریشه در اثر این گزارش‌ها به مقدار خیلی پایین نخواهد رسید.

گره‌ها در درخت DODAG تمایلی به تغییر پدر مورد اشاره خود ندارند. این تغییر تنها در شرایطی که لینک ارتباطی با گره پدر ارجح مشکل پیدا نموده و یا گره دیگری که بتوان با هزینه‌ی کمتر (هزینه کمتر از آستانه تغییر پدر ارجح) نسبت به شرایط فعلی پیام‌های گره جاری را به مقصد رساند صورت می‌گیرد[۲۸]. بر اساس بررسی‌های انجام شده گره‌های درخت DODAG در حالت ایستا بدون وجود رفتار مخربانه در شبکه معمولا تغییری در پدر ارجح خود پس از پایداری درخت DODAG نخواهند داشت. این تغییر تنها در شرایط خاص نظیر خروج یک گره از شبکه (به جز گره‌های برگ) و یا پیوستن گره‌ای با مقدار Rank کمتر از پدر ارجح حداقل یکی از گره‌های درخت DODAG صورت خواهد گرفت. همچنین در صورت وجود تحرک در گره‌ها تغییر در مقدار Rank بدون وجود رفتار مخربانه در شبکه معمولا بر اساس الگوهای خاصی نظیر تغییر از بینهایت به یک مقدار

مشخص صورت می‌گیرد. بنابراین در هر دو حالت تحرک و عدم تحرک در گره‌های پدر ارجح قبل و بعد در وضعیت‌های محدودی در جدول ۳-۷ قرار گرفته و شرایط با احتمال عدم تشخیص صحیح رفتار مخربانه از نوع حمله بدترین والد (وضعیت‌های بنفش در جدول ۳-۷) در حالت معدودی اتفاق خواهند افتاد.

۳-۱۱ .حالات خاص

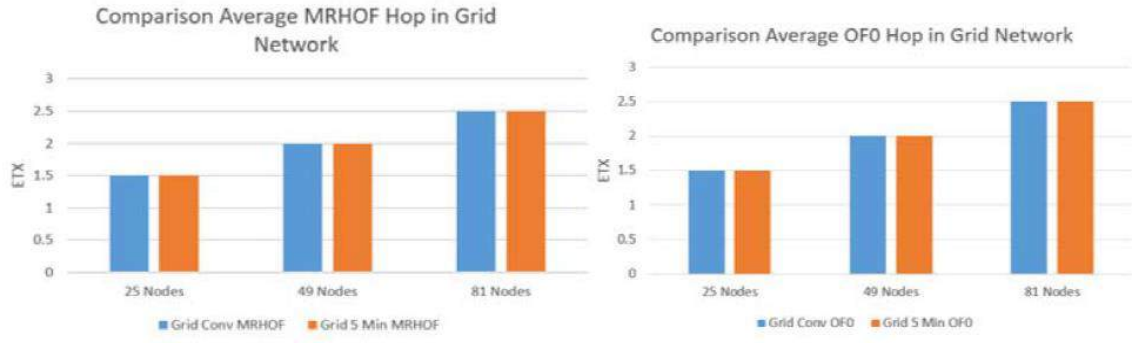
۱-عدم ارسال پیام DAO عدم وجود مسیر توسط گره مخرب به پدر ارجح قبلی : با این کار پیام مشکوک نوع دوم زودتر به ریشه رسیده و گره ریشه به اندازه حداکثر زمان تاخیر صبر نموده و با عدم دریافت پیام از این نوع حمله را تشخیص می‌دهد.

۲-تغییر پدر ارجح براساس افزایش متغیرETX نسبت به مقدار Rank : در روش پیشنهادی هر گره با تغییر پدر ارجح خود به این صورت باید یک نشانه خاص در قسمت رزرو قرار دهد و با ارسال آن به پدر ارجح جدید علت تغییر را به وی اطلاع می‌دهد. گره ریشه با دریافت این پیام در صورتی که از پدر ارجح قبلی پیام مشکوک با سرآمدن زمانسج مربوط به آن مسیر دریافت نماید حمله را تشخیص می‌دهد.

۳-عدم ارسال پیام DAO به پدر ارجح جدید: در روش پیشنهادی هر گره در پروتکل RPL با دریافت پیام DAO جدید در صورتی که قبلا ارسال کننده پیام در جدول همسایگان وی نباشد. آن را نخواهد پذیرفت.

۴ -ارسال با تاخیر پیام DAO عدم وجود مسیر به پدر ارجح قبلی توسط گره مخرب : در این حالت گره پیام مشکوک از نوع دوم زودتر به گره ریشه رسیده و با عدم دریافت پیام عدم وجود مسیر حمله مربوطه تشخیص داده خواهد شد.

۵-در شرایط بسیار خاص (با توجه به معیار انتخاب پدر ارجح به جز Rank نظیر انرژی و ETX) ممکن است مقدار ETX از معیار دوم کوچکتر بوده اما باعث تغییر پدر ارجح گردد. در این حالت نادر نیز حمله مربوطه تشخیص داده نمی‌شود.



شکل ۳-۳ : مقایسه متوسط مقدار ETX بر اساس توابع هدف [۴۵]

۳-۱۲ .رفتار روش پیشنهادی هنگام وجود بیش از یک گره مخرب از نوع حمله انتخاب بدترین والد

در هنگام وجود بیش از یک گره مخرب از نوع حمله انتخاب بدترین والد نیز روش پیشنهادی به درستی عمل می‌نماید. در ادامه اثبات این امر آورده شده است.

۳-۱۲-۱ .اثبات صحت عملکرد روش پیشنهادی در هنگام وجود بیش از یک گره مخرب (حمله انتخاب بدترین والد)

قضیه شرطی ۲ : اگر در یک درخت چندین گره (به جز ریشه) را انتخاب نماییم آنگاه حداقل بین یکی از این گره‌ها تا ریشه درخت گره انتخاب شده وجود ندارد.

قضیه ۳ : در روش پیشنهادی تمام پیام های از یک سطح بالاتر از گره مخرب تا ریشه منتقل می‌گردند.

حکم : اگر در درخت DODAG بیش از یک گره مخرب (از نوع انتخاب بدترین والد) وجود داشته باشد. آنگاه رفتار مخربانه (حمله انتخاب بدترین والد) براساس روش پیشنهادی در گره ریشه تشخیص داده می‌شود.

اثبات براساس استدلال استنتاجی

بر اساس قضیه شماره ۲ اگر بیش از یک گره مخرب در درخت DODAG وجود داشته باشد آنگاه حداقل در فاصله بین یکی از آن گره ها تا ریشه درخت گره مخرب دیگری وجود ندارد. این گره را گره A می‌نامیم. همچنین بر اساس قضیه شماره ۳ : در روش پیشنهادی تمام پیام‌ها از یک سطح بالاتر از گره مخرب به سمت ریشه منتقل می گردند.

در نتیجه اگر بیش از یک گره مخرب در درخت وجود داشته باشند رفتار مخربانه (انتخاب بدترین والد) گره A در ریشه تشخیص داده خواهد شد.

۳-۱۳ .رفتار روش پیشنهادی در برابر سایر حملات

با توجه به بررسی‌های انجام شده روش پیشنهادی در برابر حملاتی همراه با تغییر ارادی و بر خلاف پروتکل مقدار RANK نیز می‌تواند به درستی عمل نموده و شبکه را بازیابی نماید.

از جمله این حملات می‌توان موارد زیر را نام برد:

۱- حمله کاهش RANK

۲-حمله افزایش RANK

۳-حملاتی که برای جذب ترافیک به سمت آن‌ها از کاهش Rank استفاده می‌نمایند (Sinkhole ،Blackhole)

.

۴- در برابر حملاتی که با جعل مسیر در یک گره همراه هستند

۵-حمله Wormhole

در ادامه به توضیح چگونگی تشخیص حمله توسط روش پیشنهادی در برابر حملات نامبرده شده می‌پردازیم.

۳-۱۳-۱ .حمله کاهش Rank

در این حمله کاهش ارادی مقدار Rank به تغییر پدر ارجح در بسیاری از گره‌ها به سمت گره مخرب می‌انجامد. بنابراین سناریوی تشخیص مشابه حمله انتخاب بدترین والد تکرار و حمله مورد نظر در ریشه تشخیص داده می‌شود. در این حالت والد گره مخرب پس از حمله با دریافت پیام DAO حاوی مسیر جدید و یا موجود در جدول مسیریابی با گام بعدی متفاوت به آدرس مربوطه مشکوک می‌گردد. تفاوت این امر با گذشته عدم وجود آدرس موجود در پیام DAO در لیست فرزندان مستقیم گره مربوطه و همچنین عدم تنظیم مقدار شک در آن است. بنابراین گره مورد نظر ضمن تنظیم مقدار شک در پیام DAO وقوع حمله از نوع کاهش مقدار Rank را نیز به ریشه مطابق روش پیشنهادی خبر می‌دهد.

۳-۱۳-۲ .حمله افزایش Rank

در این حمله افزایش ارادی مقدار Rank در برخی از گره‌ها به تغییر پدر ارجح از گره مخرب به گره‌ای دیگر خواهد انجامید. بنابراین سناریوی تشخیص مشابه حمله انتخاب بدترین والد تکرار و حمله مورد نظر در ریشه تشخیص داده خواهد شد. تشخیص این حمله مشابه حمله کاهش مقدار Rank می‌باشد.

۳-۱۳-۳ . حملات جعل مسیر

در این حملات مسیرهای جعلی در جداول مسیریابی گره هدف ایجاد می‌گردند. بنابراین با گذشت زمان برخی دیگر از گره‌ها مسیرهای جدیدی با گام بعدی متفاوت نسبت به قبل دریافت می‌نمایند. این گره‌ها با اجرای روش پیشنهادی به این مسیرهای جعلی مشکوک شده و مقدار شک را در پیام Dao تنظیم می‌نمایند. پیام مربوطه به ریشه رسیده و با توجه به عدم دریافت پیام عدم وجود مسیر از مسیر مربوط به پدر ارجح قبلی حمله مربوطه تشخیص داده می‌شود.

۳-۱۳-٤ . حمله Wormhole

در این حمله گره مخرب پیام‌ها را از طریق لینکی خارج از Dodag به سمت دیگری از درخت ارسال می‌نماید. گره مخرب همکار در سمت دیگر درخت با انتشار مسیرهای جدید باعث شک برخی گره‌ها می‌گردد. به این ترتیب

با سرآمدن زمانسنج حداقل یکی از مسیرهای فاقد اعتماد در ریشه سرآید سناریو تشخیص حمله تکرار خواهد گشت.

۳-۱۳. نتیجه‌گیری

در این فصل با توجه به ویژگی‌های دستگاه‌ها در اینترنت اشیا به ارائه یک راه‌حل جدید جهت مقابله با حمله انتخاب بدترین والد پرداخته شد . سپس رفتار این راه‌حل در برابر افزایش تعداد گره‌های مخرب (از این نوع حمله) و همچنین برخی حملات دیگر در پروتکل RPL بررسی گشت. نتیجه این امر مقابله روش پیشنهادی در برابر افزایش تعداد گره‌های مخرب (از نوع حمله انتخاب بدترین والد) و همچنین حملات زیر بر ضد پروتکل RPL است:

۱-حمله انتخاب بدترین والد

۲-حمله افزایش Rank

۳-حمله کاهش Rank

۴-حمله جعل مسیر در جدول مسیریابی

۵-حملاتی که برای جذب ترافیک از تغییر مقدار Rank استفاده می‌نمایند.

۶-حمله Wormhole

در فصل بعد به ارزیابی روش پیشنهادی در برابر ادعاهای مطرح شده‌ی فصل جاری از جمله صحت عملکرد تشخیص حمله انتخاب بدترین والد، تشخیص سایر حملات (به دلیل تشابه حملات و کاهش حجم مطالب تکراری تنها حمله کاهش مقدار Rank بررسی شده است)، بازیابی درخت DODAG در برابر حملات با قابلیت بازیابی موثر (حمله کاهش مقدار Rank) و همچنین بررسی کارآمدی روش پیشنهادی با توجه به معیارهای مختلف در محیط شبیه‌سازی پرداخته شده است.

فصل چهارم

نتایج و بحث

در این فصل به ارزیابی صحت عملکرد CPC-RPL با توجه به ادعاهای مطرح شده در فصل سوم و همچنین میزان کارآمدی آن در محیط شبیه‌سازی پرداخته خواهد شد. برای این امر ابتدا به بررسی شبیه‌سازهای مختلف به مقایسه آن‌ها نیز بر اساس امکانات مناسب برای شبکه‌های سنسور بیسیم [1] و اینترنت اشیاء پرداخته شده است. انتخاب بستر آزمایش مناسب می‌تواند در نزدیکی نتایج به جهان حقیقی تاثیر به سزایی داشته باشد.

این مقایسه در جدول زیر آمده است:

جدول ٤-١ : مقایسه انواع شبیه‌سازها در قابلیت پیاده‌سازی شبکه‌های سنسور بیسیم[۱۵]

Simulator	Traffic Generation	Real SW Code Support	HW Platform	OS Support	Power Consumption	Security Measure	Limitations
NS-2 (The Network Simulator)	Traffic patterns	NO	NO	NO	YES	NO	No real traffic
NS-3	Traffic patterns	NO	NO	NO	YES	NO	No real traffic
TOSSIM	Statically or Dynamically	Only TinyOS	NO	TinyOS	With PowerTOSSIM	NO	Only for TinyOS code
UWSim	Dynamically	NO	YES	NO	NO	NO	Only for Under Water networks
Avrora	Real	YES	Limited	NO	YES	NO	Only for Mica2 sensor nodes
Castalia	Real	YES	NO	NO	YES	NO	Not a sensor specific platform.
GloMoSim	Statistical	NO	NO	NO	NO	NO	Statistical traffic, no energy models
Shawn	Not real	NO	NO	NO	NO	NO	No real traffic
J-Sim	Not real	NO	NO	NO	YES	NO	Low efficiency. No real traffic
Prowler	Probabilistic	NO	MICA (AVR) Mote	TinyOS	NO	NO	Probabilistic traffic.
ATEMU	Real	YES	AVR processor based systems	TinyOS	YES	NO	Only for AVR processor based systems
OMNeT++	Events	NO	YES With extension	NO	YES	NO	Slow. No real SW code
COOJA	Real	YES	YES	Contiki OS	YES	NO	Low efficiency. Limited number of simultaneous node types.

پس از بررسی‌های انجام شده، بنا بر دلایل زیر سیستم‌عامل Contiki نسخه ۲,۶ و شبیه‌ساز آن Cooja Emulator جهت پیاده‌سازی روش پیشنهادی انتخاب گردیده است.

۱- وجود مدل ترافیک حقیقی در سیستم‌عامل Contiki : ترافیک تولیدی همان ترافیکی است که در اینترنت اشیا توسط سنسورها می تواند تولید گردد.
۲- در نظر گرفتن محدودیت های سخت افزاری در دستگاه‌های اینترنت اشیاء
۳- در نظر گرفتن منبع انرژی
۴- وجود پیاده‌سازی پروتکل RPL در سیستم عامل Contiki

1-WSN

٤-١. سیستم عامل Contiki

Contiki سیستم عاملی مخصوص اینترنت اشیا که توان اتصال میکروکنترلرهای کم – توان با قدرت پردازشی پایین را به اینترنت داراست. این سیستم عامل علاوه بر متن‌باز بودن دارای یک جعبه ابزار برای ساخت شبکه‌های بیسیم پیچیده نیز می‌باشد [۳۷].

٤-١-١. ویژگی‌های سیستم عامل Contiki

۱-پشتیبانی از استانداردهای اینترنت

Contiki استانداردهای IPv4 و IPv6 را به صورت کامل پشتیبانی نموده و علاوه بر آن امکانات لازم برای استفاده از استانداردهای مخصوص شبکه‌های کم توان را نیز داراست. از جمله این استانداردها می‌توان به 6lowpan، RPL، COAP اشاره نمود. به وسیله لایه MAC در سیستم عامل Contiki حتی مسیریاب‌های بیسیم هم می‌توانند باتری محور عمل نمایند[۳۶].

۲-پیاده‌سازی سریع

کاربردها در این سیستم عامل بر اساس زبان C بوده و پیاده سازی آن‌ها سریع و ساده می‌باشد. به وسیله Cooja Emulator موجود در این سیستم عامل می‌توان کاربردها را قبل از استفاده در سیستم حقیقی تست و بررسی نمود[۳۷].

۳-انتخاب ساده سخت افزار

سیستم عامل Contiki بر روی دستگاه‌های بیسیم کم‌توانی و قابل دسترسی آسان از طریق اینترنت عمل می نماید[۳۷].

۴-جامعه فعال

پیاده سازی این سیستم عامل توسط یک تیم جهانی و با همکاری شرکت های معتبر نظیر Atmel, Cisco, Eth Redwire Llc, Sap, Thingsquare و بسیاری دیگر شده صورت گرفته و پشتیبانی می‌گردد[۳۷].

۵-متن باز[1] بودن

سیستم عامل Contiki متن باز بوده و می‌تواند در پروژه‌های تجاری و غیر تجاری به صورت رایگان مورد استفاده قرار گیرد. علاوه بر آن کدهای این سیستم عامل نیز به صورت کامل در دسترس می‌باشند[۳۷].

1-Open Source

٤-٢ . Cooja Simulator

Cooja شبیه ساز شبکه در سیستم عامل Contiki است. به کمک این ابزار می‌توان شبکه‌های مختلف از سنسورهای بیسیم را شبیه‌سازی نمود. در Cooja سنسورها می‌توانند حتی در سطح سخت افزار نیز شبیه‌سازی گردند. این امر به بررسی دقیق رفتار سیستم کمک شایانی می‌نماید. به دلیل جزئیات زیاد در شبیه‌سازی سنسورها در سطح سخت افزار سرعت شبیه‌سازی با Cooja کمی پایین بوده اما با این حال می‌توان با غیرفعال نمودن تولید جزئیات در شبکه‌های بزرگ سرعت بالا در شبیه سازی را نیز تجربه نمود[۲۹] [۲۸].

٤-٣. پروتکل RPL در سیستم عامل Contiki

در هسته این سیستم عامل پروتکل RPL به صورت طراحی پیمانه‌ای و در قالب چندین کلاس به زبان C پیاده سازی شده است. در ادامه به معرفی هر یک از کلاسهای آن می‌پردازیم:

۱- کلاس Rpl.C

در این کلاس امور مربوط به مسیرها در پروتکل RPL از جمله موارد زیر صورت می‌پذیرد:

- کاهش زمان عمر مسیرهای بلا استفاده در بازه اخیر و همچنین حذف مسیرهایی که عمر آن‌ها به سررسیده است.
- حذف تمام مسیرهای موجود در گره و یا درخت جهت تعمیر عمومی و یا شروع مجدد عملکرد گره
- حذف یک مسیر بر اساس گام بعدی مشخص (این امر در تعمیر محلی کاربرد دارد)

۲- کلاس Rpl-Icmpv6

در این کلاس پردازش‌های مربوط به دریافت و یا ارسال پیام‌های کنترلی در قالب بسته‌های ICMPV6 از جمله موارد زیر صورت می پذیرد:

- مدیریت پیام DIS ورودی
- مدیریت پیام DIS خروجی
- مدیریت پیام DIO ورودی
- مدیریت پیام DIO خروجی
- مدیریت پیام DAO ورودی
- مدیریت پیام DAO خروجی

در سیستم عامل Contiki دو نوع تابع هدف برای انتخاب پدر ارجح وجود دارد. این موارد در کلاس‌های شماره ۳ و ۴ آورده شده است.

۳- کلاس 0OF.C

این کلاس پیاده سازی تابع هدف 0OF است. در این کلاس تنها یک معیار برای انتخاب پدر ارجح (بر اساس مقدار Rank) وجود دارد. در این کلاس توابع زیر وجود دارند:

محاسبه مقدار Rank :

برای این امر به مقدار Rank مربوط به پدر ارجح یک مقدار ثابت (کمترین مقدار قابل افزایش) افزوده می‌گردد.

انتخاب پدر ارجح از بین دو والد:

ابتدا برای هر دو والد (پدر ارجح فعلی و والد کاندید برای مورد اشاره شدن) محاسبه زیر صورت می‌پذیرد:

[۴-۱] (مقدار RANK با انتخاب گره مورد نظر به عنوان پدر ارجح) + (شرایط لینک اتصال با گره مورد نظر)

سپس گره‌ی با کمترین نتیجه برای محاسبه بالا به عنوان پدر ارجح انتخاب می‌گردد. هر گره در تغییر پدر ارجح خود یک آستانه تغییر را نیز داراست. اگر قدر مطلق تفاوت مقدار محاسبه [۴-۱] مربوط به پدر ارجح فعلی از مقدار این محاسبه برای تمام گره‌های موجود در لیست پدران از مقدار آستانه (با توجه به معیار انتخاب پدر ارجح) کمتر باشد آنگاه گره مربوطه حفظ پدر ارجح فعلی را نسبت به تغییر آن ترجیح می‌دهد.
در این تابع مقدار آستانه MinHopRankIncrease+MinHopRankIncrease/2 می‌باشد. مقدار MinHopRankIncrease معادل ۲۵۶ می‌باشد.

انتخاب بین دو درخت[1]

گره مربوطه از طریق بررسی موارد زیر درخت برتر را انتخاب و به آن می‌پیوندد:

۱- درختی که دارای اولویت بیشتری است (در پیام DIO فیلدی برای اولویت درخت وجود دارد). اولویت‌ها متناسب با لایه کاربرد مورد استفاده در درخت مربوطه انتخاب می‌گردند.
۲- درختی که گره مربوطه در صورت پیوستن به آن وضعیت بهتری از نظر معیار مسیریابی خواهد داشت (به عنوان مثال مقدار Rank کمتر).

1-Dag

۳- درختی که بتواند انتظارات در لایه کاربرد را کاملا برآورده نماید. این انتظارات خارج از پروتکل RPL بوده و تنها گره ریشه در درخت DODAG از آن مطلع می‌گردد. به عنوان نمونه اتصال همیشگی برخی گره ها در شبکه می‌تواند به عنوان یک هدف برای لایه شبکه در نظر گرفته شود.

محاسبه شرایط لینک

شرایط لینک بر اساس معیار ETX محاسبه می‌گردد.

۴- کلاس MRHOF.C

در این کلاس تابع هدف MRHOF به صورت توابع زیر زیر پیاده‌سازی شده است.

انتخاب پدر ارجح

در این تابع سه حالت برای محاسبه معیار انتخاب پدر ارجح وجود دارد. یکی از این سه حالت می‌تواند انتخاب گردد(حالت پیشفرض بر اساس ETX [1]می‌باشد):

۱- بر اساس Rank

مقدار RANK با انتخاب گره مورد منظر به عنوان پدر ارجح + شرایط لینک اتصال با گره مورد نظر

۲- بر اساس ETX

مقدار ETX گره مورد نظر به عنوان پدر ارجح + شرایط لینک اتصال با گره مورد نظر

۳- بر اساس تخمین انرژی

مقدار تخمین انرژی گره مورد نظر به عنوان پدر ارجح + شرایط لینک اتصال با گره مورد نظر

در این تابع گره‌ی دارای معیار مسیریابی کمتر از بین لیست پدران به عنوان پدر ارجح انتخاب می‌گردد. هر گره در تغییر پدر ارجح یک آستانه تغییر را نیز داراست. اگر یک والد برای انتخاب به عنوان پدر ارجح کمتر از مقدار این آستانه (با توجه به معیار انتخاب پدر ارجح) جالب باشد آنگاه گره مربوطه حفظ پدر ارجح فعلی را ترجیح می‌دهد. در این تابع مقدار آستانه ۶۴ می‌باشد.

محاسبه شرایط لینک :

شرایط لینک نیز بر اساس معیار ETX محاسبه می‌گردد.

انتخاب بین دو درخت

انتخاب بین دو درخت در این کلاس نیز مشابه تابع 0OF صورت می‌پذیرد.

1-Estimate Transmition Count

۵- کلاس Rpl-Ext-Herader.C

در این کلاس مدیریت سرآیند توسعه پذیر IPV6 که در هر گام از مسیر باید مورد بررسی قرار گیرد (Eh Hop By Hop) با توجه به RPL صورت می‌گیرد.

۶- کلاس Rpl-Dag.C

تمام امور مربوط به درخت DAG در پروتکل RPL در این کلاس صورت می‌گیرد. در لیست زیر به برخی از این کارها اشاره شده است:

- امور مربوط به لیست پدران از جمله دستیابی به مقدار Rank، آدرس IP پدران، یافتن و تنظیم پدر ارجح فعلی، حذف پدران، افزودن یک گره به لیست پدران، یافتن درخت مربوط به گره والد
- بررسی ارسال پیام DAO
- تنظیم یک گره به عنوان ریشه درخت (این گره معمولا گره سرور می‌باشد)
- امور مربوط به آدرسهای پیشوندی نظیر بررسی تکراری بودن آدرس‌های پیشوندی و تنظیم آن‌ها
- ایجاد و تخصیص یک محدوده RPL
- ایجاد و تخصیص درخت
- پاکسازی درخت و محدوده RPL از موارد ذخیره شده
- انتخاب و پیوستن به یک درخت
- تنظیم تابع هدف مورد استفاده فعلی از طریق پیام DIO
- پیوستن به یک محدوده RPL
- تعمیر همگانی در محدوده RPL
- تعمیر محلی
- محاسبه مجدد مقدار RANK به کمک تابع هدف
- پردازش رویدادهای مربوط به پدران از جمله تغییر مقدار RANK و پیوستن به یک درخت دیگر
- پردازش پیام‌های DIO ورودی

۷- کلاس Rpl.H

در این کلاس تعاریف عمومی مربوط به پروتکل RPL مشخص می‌گردند. از جمله این موارد می‌توان به لیست زیر اشاره نمود:

- تعریف Rpl_Metric_Container
- تعربف پدران

- تعریف Prefix ها
- تعریف درخت DAG
- تعریف محدوده‌ها در پروتکل RPL
- لیست توابع با سطح دسترسی عمومی در پروتکل RPL

۸- کلاس Rpl-Conf.H

انجام تنظیمات و تعریفات عمومی Rplcontiki در این کلاس صورت می‌گیرد. از جمله این موارد می‌توان به لیست زیر اشاره نمود:

- فعالسازی یا عدم فعالسازی Log ها در پروتکل RPL
- انتخاب نوع تابع هدف (توابع 0OF و MRHOF)
- امکان محدود کردن همیشگی موقعیت یگ گره به برگ در یک درخت
- مقدار دهی حداکثر تعداد محدوده‌ها در پروتکل و همچنین حداکثر تعداد درخت‌ها در هر محدوده

۹- کلاس Rpl-Private.H

تعریفات خاص در پروتکل RPL در این کلاس صورت می‌گیرد. تعریف انواع پیام‌های کنترلی، انواع گزینه‌های اختیاری (در پیام‌های کنترلی)، گزینه‌های اختیاری موجود در سرآیند، مقادیر پیشفرض ثوابت و برخی متغیرها نظیر زمان‌سنج‌ها، طول عمر مسیرها، حداقل میزان افزایش Rank و مقدار اولیه آن و همچنین مقادیر اولیه مربوط به تخمین‌ها از جمله این تعاریف می‌باشند.

۱۰- کلاس Rpl-Timer

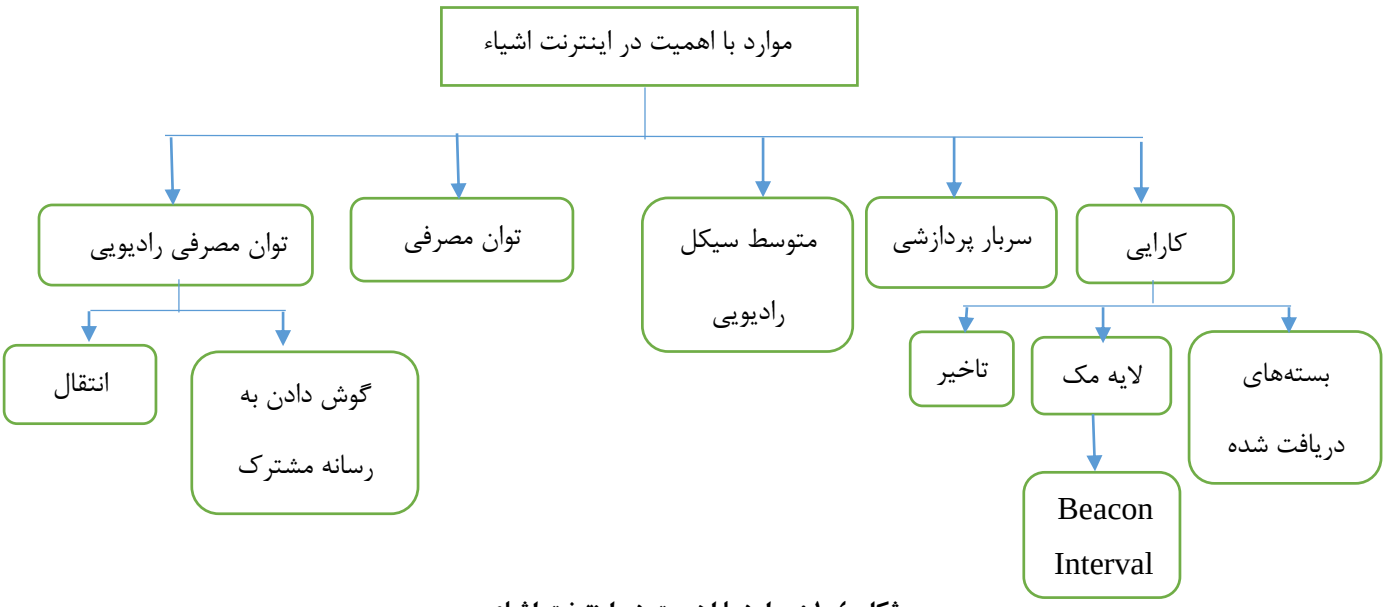
مدیریت زمان سنج ها در پروتکل RPL بر عهده این کلاس است. به همین منظور پردازش های زیر در کلاس Rpl-Timer صورت می‌گیرند.

- مدیریت زمانسنج دوره‌ای: در پروتکل RPL علاوه بر زمان سنج DIO زمانسنج دیگری جهت محاسبه دوره‌ای مقدار Rank و تغییرات مربوط به تعویض پدر ارجح و یا تعویض درخت وجود دارد. مدیریت این زمان‌سنج در این کلاس صورت می‌گیرد.
- مدیریت زمان سنج DIO: این مدیریت شامل فراخوانی پردازش‌های لازم جهت ارسال پیام DIO و همچنین محاسبه مقدار بعدی برای این زمانسنج می‌باشد.
- مدیریت زمانسنج DAO : این زمانسنج برای کاهش تعداد پیام‌های ارسالی به سمت ریشه طراحی شده است. یک گره در صورت آمادگی جهت ارسال پیام DAO به پدر ارجح ابتدا کمی صبر می‌نماید.

در این مدت در صورت نیاز به ارسال پیام‌های DAO دیگر تمام این پیام‌ها به صورت یک جا ارسال خواهند شد. تنظیم زمان‌سنج‌ها به مقدار اولیه نیز در این کلاس صورت می‌گیرد.

٤-٤ . ارزیابی

به دلیل استفاده از میکروکنترلرهای کم‌توان در اینترنت اشیا بررسی موارد موجود در شکل شماره ۴-۱ بسیار حائز اهمیت می‌باشد[۲۸]. بر این اساس در ادامه این پژوهش ضمن ارزیابی صحت کارکرد روش پیشنهادی، تمرکز بر تغییرات این موارد در اثر اجرای حمله انتخاب بدترین والد، روش پیشنهادی و یا اجرای هر دو به صورت همزمان می‌باشد.



شکل ٤-١ : موارد با اهمیت در اینترنت اشیاء

٤-٥. پارامترهای شبیه‌سازی

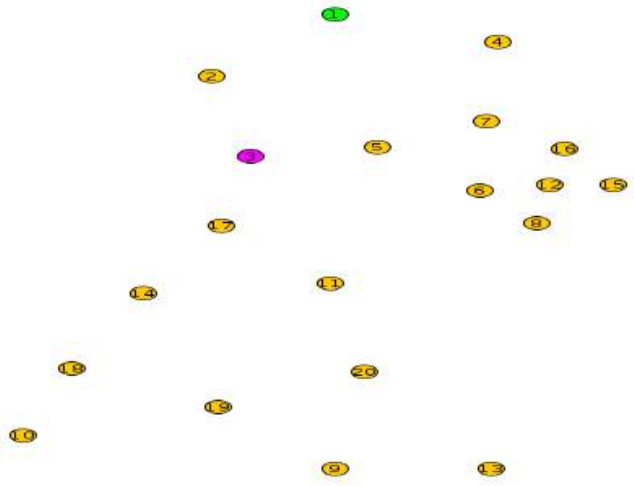
در ادامه از پارامترهای جدول ۴-۱ برای شبیه‌سازی‌های مختلف استفاده شده است. تعداد گره‌ها، توپولوژی و وجود تحرک در گره‌ها تفاوت شبیه‌سازی‌های مختلف در ادامه این پژوهش هستند.

جدول ٤-٢ : پارامترهای مورد استفاده در شبیه‌سازی‌ها

زمان شبیه‌سازی	۳۰ دقیقه
تعداد تکرار	۱۰ مرتبه برای هر آزمایش
منطقه تحت پوشش	۱۵۰ * ۱۷۵ متر مربع
تعداد گره‌ها	بین ۲۰ الی ۱۰۰
بازه زمانی ارسال بسته	۱۰ ثانیه
اندازه بسته	۴۲ بایت
پروتکل مسیریابی	RPL
استاندارد کنترل دسترسی	۸۰۲.۱۵.۴
مقدار اولیه اعتماد	۴
بازه بی‌اعتمادی	اعتماد = > 1
تعداد گره‌های مخرب	۱ یا ۳۰ درصد کل گره‌ها
مدل تحرک گره‌ها در صورت استفاده	Random Way Point
تعداد گره‌های متحرک (در صورت وجود تحرک)	۳۰ درصد کل گره‌ها

٤-٦. تاثیر حمله انتخاب بدترین والد بر پروتکل RPL

در ادامه تاثیر حمله انتخاب بدترین والد بر پروتکل مسیریابی RPL مورد بررسی قرار گرفته است. این ارزیابی در یک توپولوژی یکسان صورت گرفته است. فرآیند انتخاب توپولوژی به صورت تصادفی و دارای شرایط رخداد حمله انجام شده است.

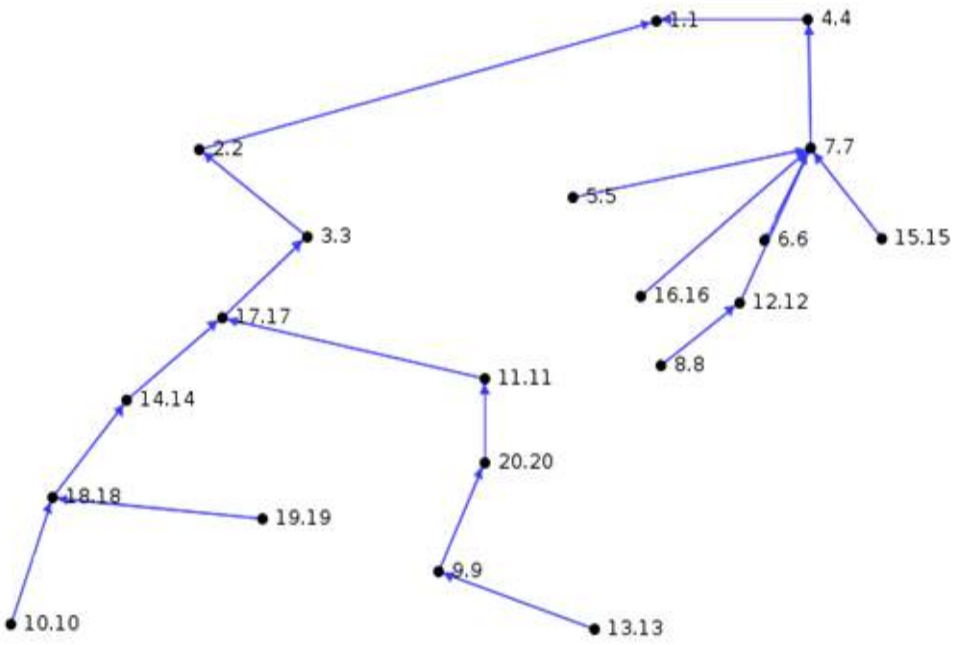


شکل ٤-٢ : درخت DODAG مورد آزمایش

٤-٦-١. پیاده‌سازی حمله انتخاب بدترین والد

برای پیاده سازی این حمله ابتدا یک زمان‌سنج برای گره شماره ۳ (گره مخرب) در توپولوژی شکل ۴- ۲ ایجاد نموده و مقدار اولیه آن را به مقدار مشخصی تنظیم نموده‌ایم. با پایان یافتن این زمانسنج گره شماره ۳ به جای انتخاب بهترین پدر خود به عنوان پدر ارجح بدترین والد را انتخاب می‌نماید. به این ترتیب حمله انتخاب بدترین والد قابلیت اجرایی یافته و تاثیر آن بر پروتکل RPL مشاهده خواهد گردید. پیاده سازی این کار با تغییر تابع Best_Parent در کلاس 0OF صورت گرفته است. سنسورهای مورد استفاده از نوع Tmote Sky می‌باشند.

برای مشاهده تاثیر این حمله در ادامه نمودارهای حاصل از اجرای توپولوژی فوق ابتدا بدون اعمال حمله در گره مخرب و سپس با وجود رفتار مخربانه در گره شماره ۳ آورده شده است. بالا بردن گره‌ها در شکل شماره ۴- ۳ تاثیری در عملکرد روش پیشنهادی نخواهد داشت.

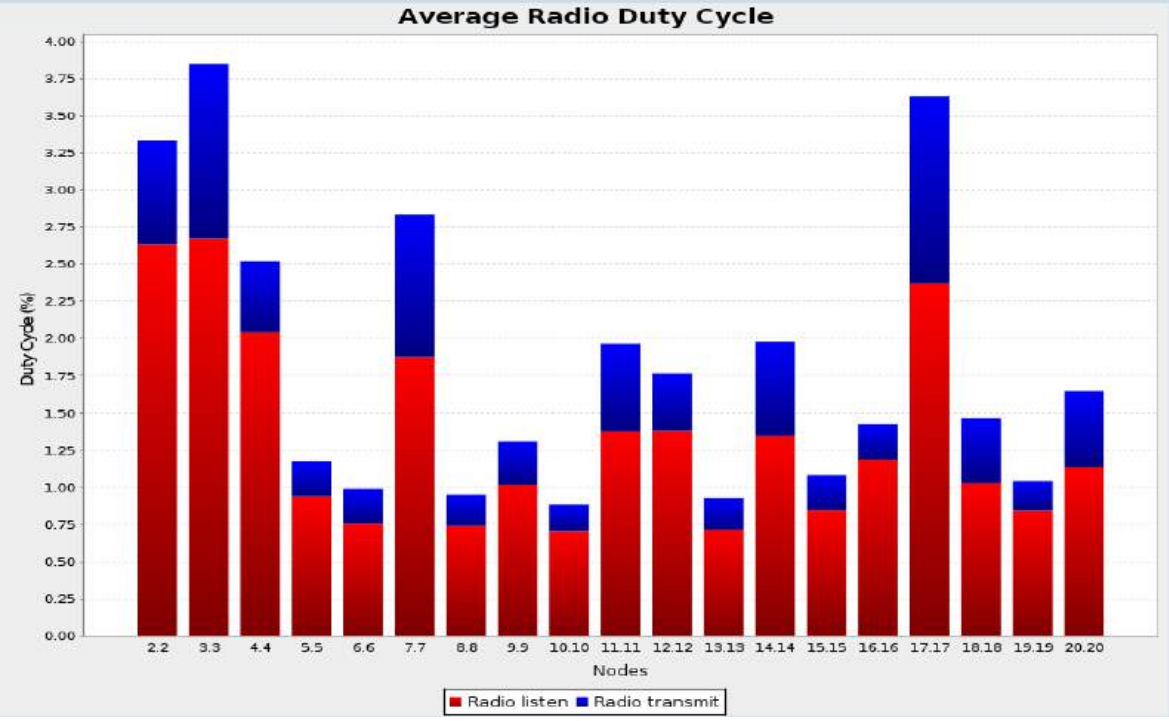


شکل ٤-٣ : توپولوژی درخت شکل ٤-٢ بدون وجود رفتار مخربانه در شبکه

با توجه به شکل شماره ۴-۳ بدون رفتار مخربانه در گره شماره ۳، هر گره در شکل‌گیری درخت DODAG ضمن انتخاب بهترین والد به عنوان پدر ارجح اطلاعات مربوطه را با کمترین هزینه به سمت ریشه ارسال می‌نماید. به این ترتیب هزینه ارسال ترافیک در جهت ریشه به حداقل مقدار خود نزدیک می‌گردد.

همانطور که در شکل شماره ۴-۳ مشاهده می‌گردد زیر درخت بزرگی اطلاعات خود را از طریق گره مخرب به سمت ریشه منتقل می‌نماید. بنابراین هزینه بازارسال اطلاعات توسط گره مخرب به سمت ریشه می‌تواند در کارایی و عملکرد درخت تاثیر به سزایی داشته باشد.

همچنین گره مخرب در این توپولوژی دو گزینه را جهت انتخاب پدر ارجح خود داراست (گره شماره ۲ و گره شماره ۵). این دو گره در محدوده‌ی ارسال گره مخرب بوده و می‌توانند به عنوان پل ارتباطی با ریشه انتخاب شوند. با انتخاب گره شماره ۲ اطلاعات زیر درخت مربوط به گره ۳ با کمترین هزینه به سمت ریشه منتقل و انتخاب گره شماره ۸ باعث عبور اطلاعات از مسیر طولانی‌تر برای رسیدن به ریشه می‌گردد. در این حالت شبکه سربار زیادی را تحمل می‌نماید.



شکل ٤-٤ :متوسط سیکل‌های رادیویی در گره‌ها در حالت بدون وجود رفتار مخربانه در شکل ٤-٣

در نمودار شکل شماره ۴-۴ می‌توان متوسط سیکل رادیویی را در گره‌های مختلف درخت شکل شماره ۴-۳ مشاهده کرد. گره‌های ۲ و ۳ و ۱۷ به دلیل بازارسال اطلاعات مربوط به زیرگراف‌های خود از ارتباطات رادیویی بیشتری نسبت به سایر گره‌ها برای گوش‌دادن به رسانه مشترک جهت جلوگیری از تصادم و ارسال صحیح استفاده می‌نمایند. در شبکه‌های بیسیم نسبت مصرف انرژی گوش‌دادن به رسانه اشتراکی بیشتر از ارسال در آن می‌باشد.این موضوع در شکل بالا کاملا مشهود است.

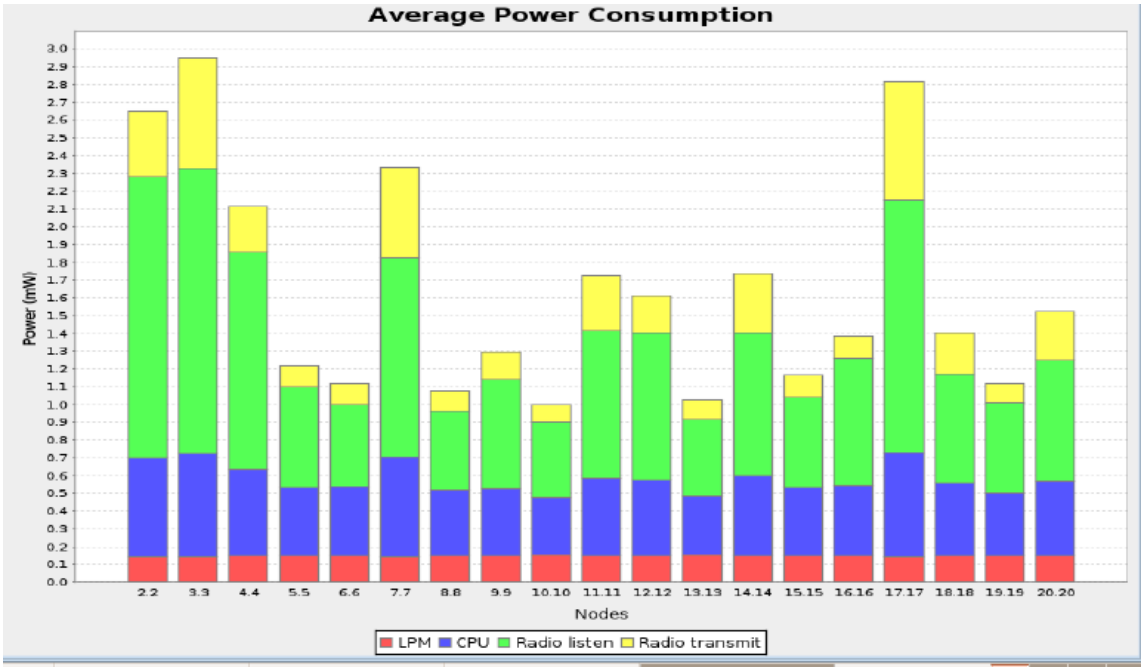
محاسبه دوره کاری بر اساس رابطه زیر صورت می‌گیرد:

$$Duty\ Cycle = \frac{Pw}{T} \qquad [۲-۴]$$

Pw : عرض پالس (زمانی که پالس فعال بوده است)

T : زمان کل دوره سیگنال

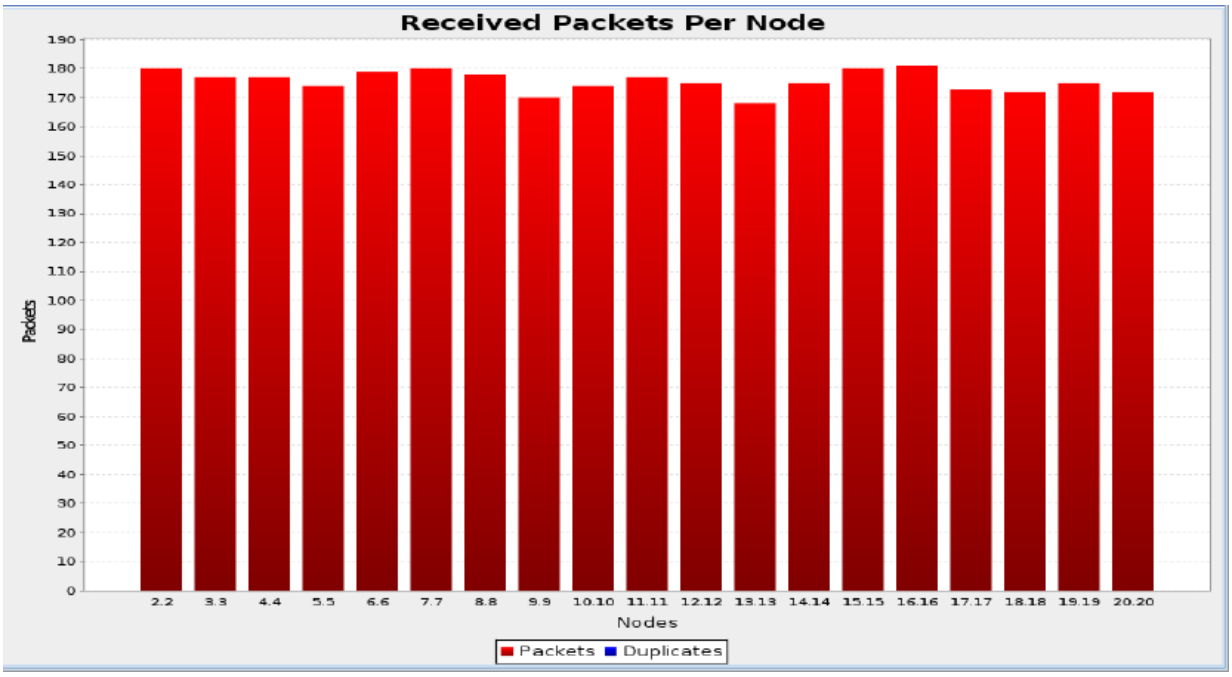
سیکل وظیفه رادیویی در گره‌هایی با ترافیک ورودی و ازدحام در رسانه مشترک رابطه مستقیم دارد. بر این اساس با حرکت از برگ‌های درخت به سمت ریشه عرض پالس صعودی خواهد بود.



شکل ٤-٥ :متوسط مصرف توان در گره‌ها در حالت بدون وجود رفتار مخربانه در شکل ٤-٣

با توجه به شکل شماره ۴-۵ گره‌هایی که زیر گراف بزرگ‌تری از طریق آنها به ریشه متصل می‌شوند استفاده بیشتری (متوسط توان مصرفی) از پردازنده، فناوری رادیویی (گوش دادن به رسانه اشتراکی و ارسال رادیویی) نسبت به سایرین دارند. بنابراین مصرف انرژی در این گره‌ها متناسب با فرایندهای کاری آنها بیشتر است. در حالت LPM به دلیل مصرف کم انرژی، تفاوت زمان گذرای هر گره در این حالت به خوبی مشخص نیست. گره‌های با مصرف پردازشی و رادیویی بالا، به طور متناسب زمان کمتری در حالت LPM می‌گذرانند.

در حالت Low Power Mode مصرف انرژی در تمام گره‌ها تقریبا یکسان است. در این حالت گره‌ها با هدف افزایش عمر منبع انرژی در شرایط عدم وجود اطلاعات برای ارسال یا هنگام اشتغال رسانه‌ی مشترک کمترین مقدار انرژی ممکن را مصرف می‌نمایند. زمان تقریبا یکسان گره‌ها در حالت LPM به معنی استفاده کارآمد از رسانه مشترک می‌باشد. با توجه به شکل روند مصرف توان در درخت با حرکت از برگ‌ها به سمت ریشه صعودی خواهد بود.



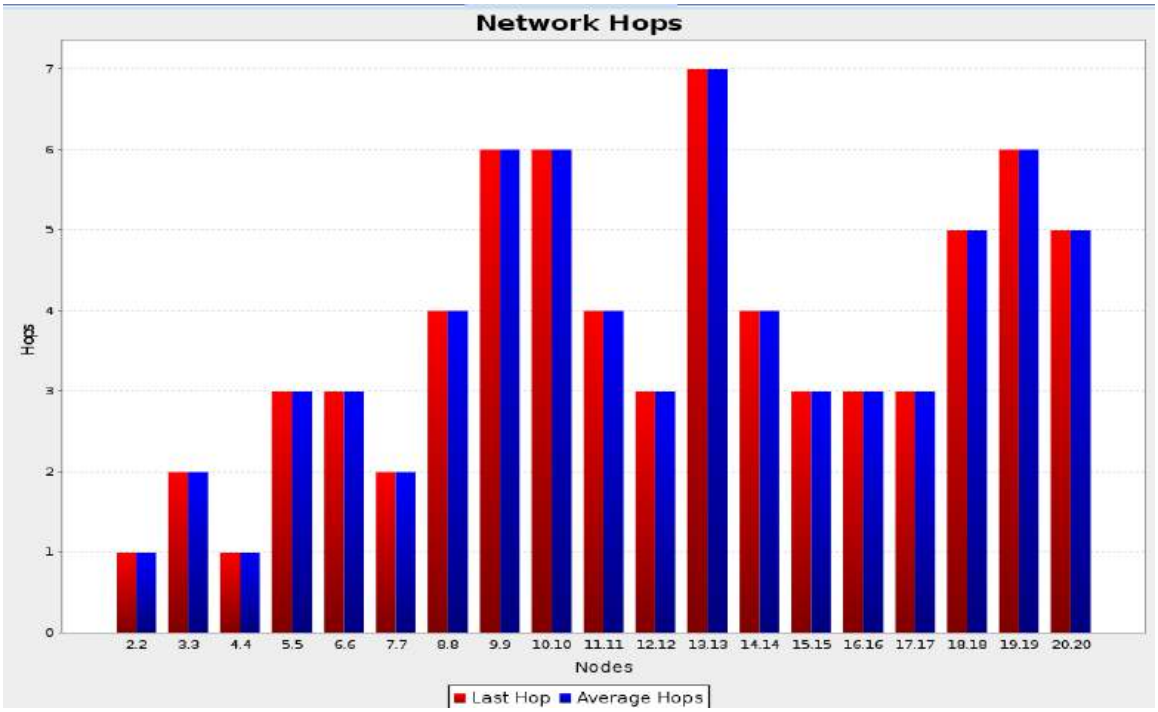
شکل ٤- ٦: تعداد بسته‌های دریافت شده در ریشه از طرف هر گره بر اساس توپولوژی شکل ٤-٣

همانطور که در شکل شماره ۴-۶ مشاهده می گردد ترافیک تولیدی در لایه کاربرد در یک بازه زمانی مشخص به صورت کامل و با رفتار صحیح از طرف پروتکل RPL به مقصد (گره ریشه) رسیده‌اند. همچنین هیچ بسته‌ای دوبار در یک گره دریافت نشده است. بنا بر دلایل زیر تعداد بسته‌های کمتری از برخی گره‌ها در ریشه دریافت شده است:

۱. گم شدن بسته‌ها به دلیل ازدحام و هرگونه عملکرد ناصحیح در پروتکل مسیریابی و یا پروتکل لایه مک که منجر به حذف بسته در گام بعدی گردد.
۲. وجود مسیر طولانی و پر ازدحام بین برخی‌گره‌ها تا ریشه

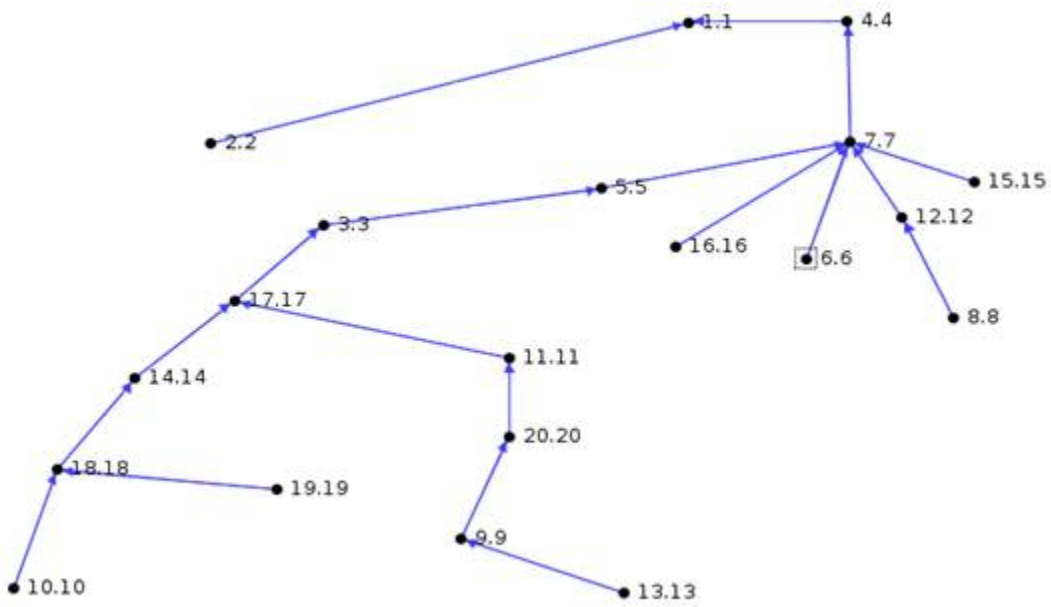
با توجه به شکل با حرکت از برگ‌ها به سمت ریشه تعداد بسته‌های دریافت شده از هر گره افزایش خواهد یافت. بر این اساس گم شدن بسته‌های ارسالی توسط گره پدر و یا وجود مسیر طولانی بین وی و گره ریشه بر درصد دریافت پیام‌های مربوط به فرزندان آن تاثیر مستقیم خواهد داشت.

همانطور که در شکل شماره ۴-۷ مشاهده می‌گردد هر گره با کمترین تعداد گام ممکن بر اساس ساختار شکل شماره ۴-۳ ترافیک زیر درخت خود را به سمت ریشه منتقل می‌نماید. بدیهی است که برگ‌های درخت در بیشترین عمق (گره‌های ۱۲،۱۳،۱۶) بیشترین تعداد گام تا ریشه را دارا باشند. در ادامه نمودارهای حاصل از اجرای حمله انتخاب بدترین والد در گره شماره ۳ آورده شده است.

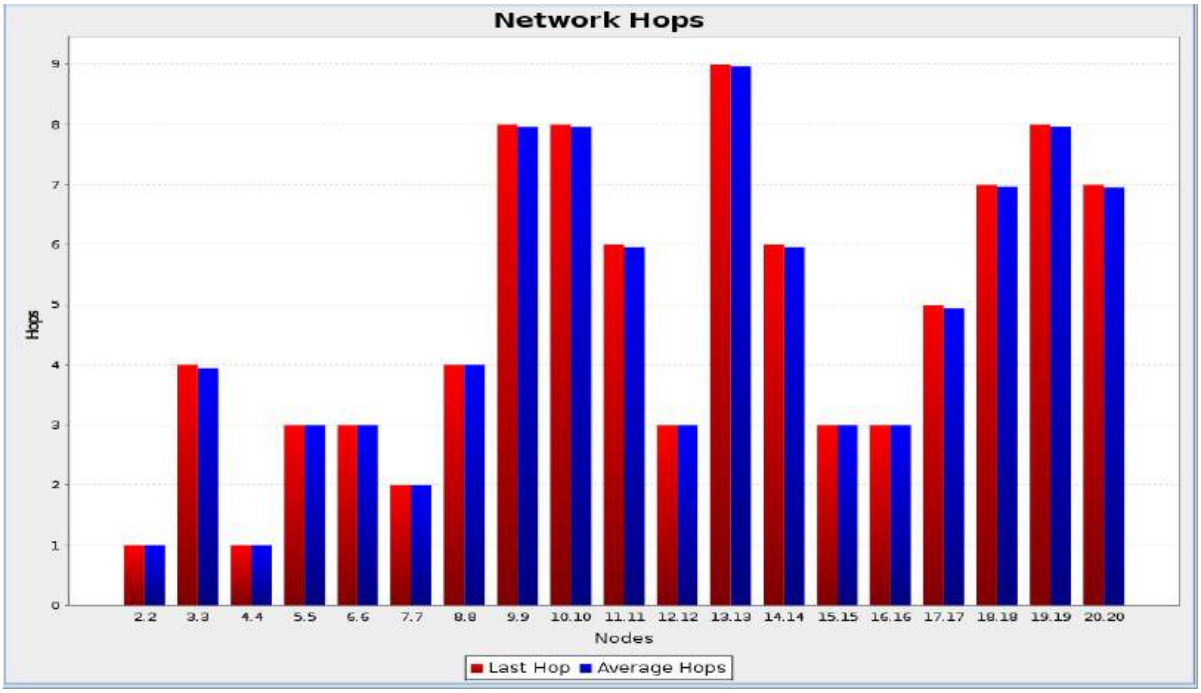


شکل ٤-۷ : تعداد گام‌های شبکه برای گره‌ها در حالت بدون وجود رفتار مخربانه در شکل ٤-۳

همانطور که در شکل شماره ۴-۸ مشاهده می‌گردد با اجرای رفتار مخربانه در گره شماره ۳، پدر ارجح در این گره به بدترین والد ممکن (گره شماره ۵) تغییر یافته است. با این کار زیردرخت مربوط به گره‌ی مخرب سربار زیادی جهت ارسال اطلاعات به سمت ریشه متقبل می‌گردد. دلیل این امر بازارسال ترافیک توسط گره مخرب از طریق مسیر پر هزینه‌تر (از طریق گره شماره ۵) به سمت ریشه می‌باشد.



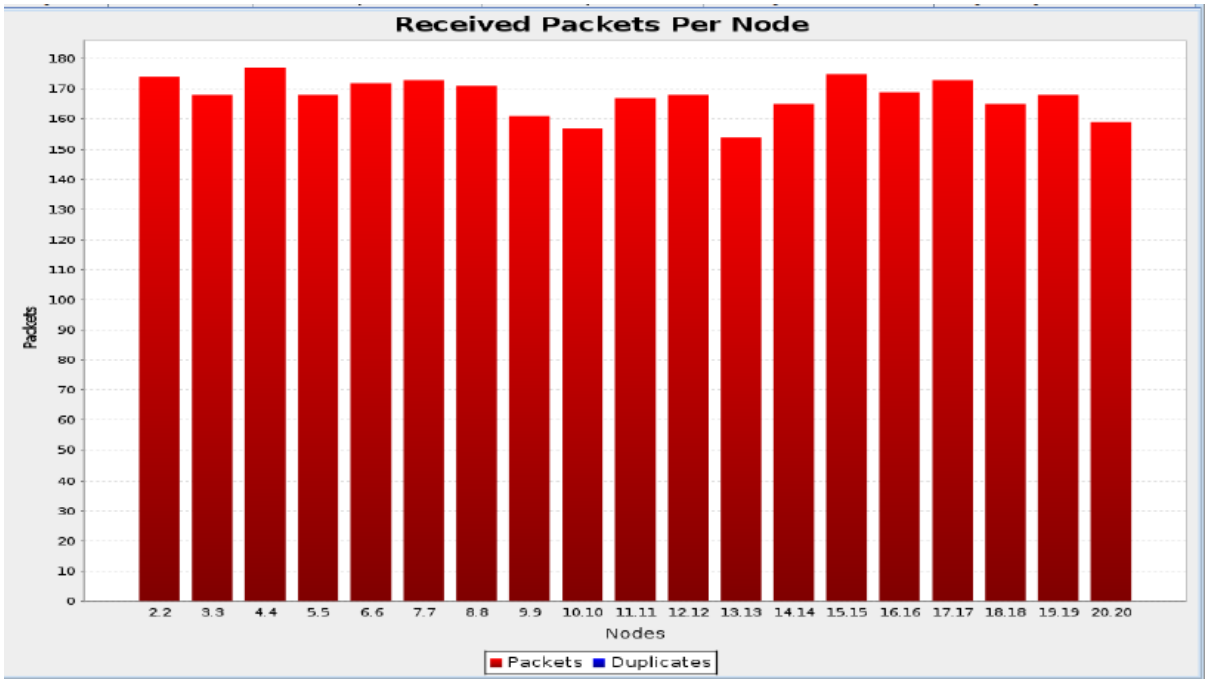
شکل ٤-٨ : توپولوژی حاصل از اجرای حمله Worst Parent گره شماره ۳ در شکل ٤-۲



شکل ٤-٩ :تعداد گام‌های شبکه در هر گره بر اساس توپولوژی شکل ٤-٨

تعداد گام‌های بین گره‌ی مخرب (یا زیر درخت مربوطه) تا ریشه به اندازه گام‌های تغییر مسیر حاصل از اجرای حمله (گره شماره ۸ تا ریشه) افزایش یافته است. دلیل این موضوع عبور ترافیک متعلق به زیر درخت گره مخرب از طریق گره شماره ۵ به سمت ریشه است. این موضوع در شکل شماره ۴-۹ سربار ناشی از این حمله را نشان می‌دهد.

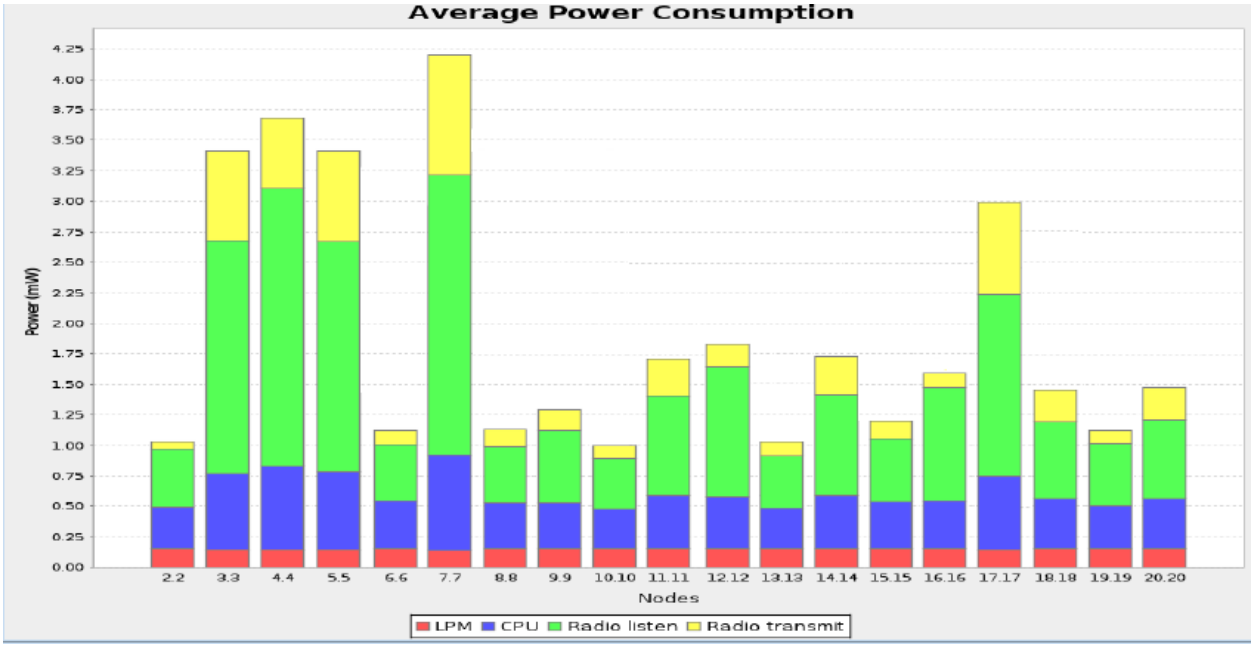
با اجرای حمله انتخاب بدترین والد ترافیک تولیدی متعلق به گره مخرب و زیر درخت مربوطه در بازه زمانی یکسان با شکل شماره ۴-۶ (بسته‌های دریافت شده در حالت عدم وجود رفتار مخربانه) به صورت محسوسی کاهش یافته است. دلیل این امر سربار عبور از مسیر اضافه‌ی مربوط به اجرای حمله برای هر بسته است. افزایش بار بر یک مسیر مشخص احتمال گم شدن بسته‌ها را نیز افزایش می‌دهد. این امر در شکل شماره ۴-۱۰ نمایش داده شده است. با توجه به شکل کاهش مذکور در برگ‌ها بیشتر می‌باشد.



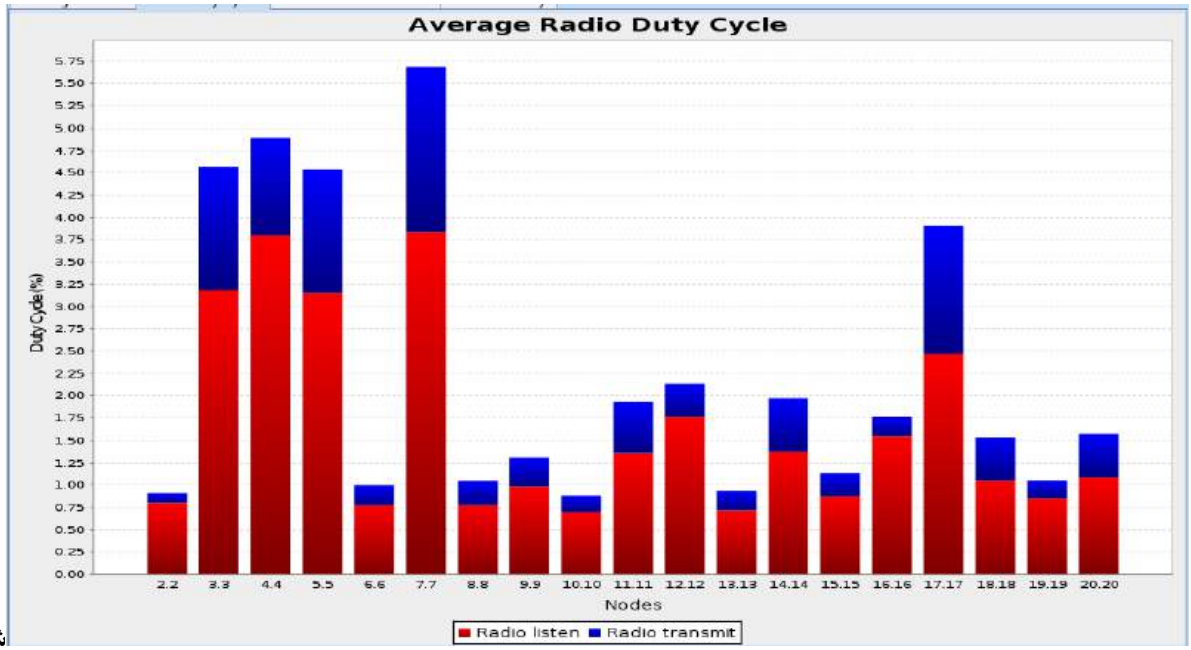
شکل ٤-۱۰ : بسته‌های دریافتی هر گره در ریشه بر اساس توپولوژی شکل ٤-۸

شکل شماره ۴-۱۱ متوسط مصرف توان در هر گره را بر اساس توپولوژی شکل ۴-۸ نشان می‌دهد. با توجه به شکل میزان مصرف انرژی در برخی گره‌ها از نظر پردازش و ارتباطات رادیویی نسبت به سایر گره‌ها به شدت افزایش یافته است.دلیل اصلی این امر افزایش عبور ترافیک از طریق این گره‌ها است (نظیر گره‌های ۷و۵). در این نمودار نیز گره‌ها مصرف انرژی تقریبا یکسانی را در حالت LPM سپری نموده اند. در حالت LPM به علت مصرف بسیار کم انرژی تفاوت‌ها در شکل بالا به صورت ناچیز دیده می‌شوند. با توجه به شکل روند تغییرات مصرف انرژی

در گره‌های درخت از برگ‌ها به سمت ریشه صعودی است. همانطور که در شکل نیز مشخص است حمله انتخاب بدترین والد در مصرف توان گره‌های زیر درخت گره مخرب تاثیری ندارد. دلیل این امر عدم اطلاع گره‌های زیر درخت گره مخرب از تغییر پدر ارجح ناشی از حمله مربوطه است.



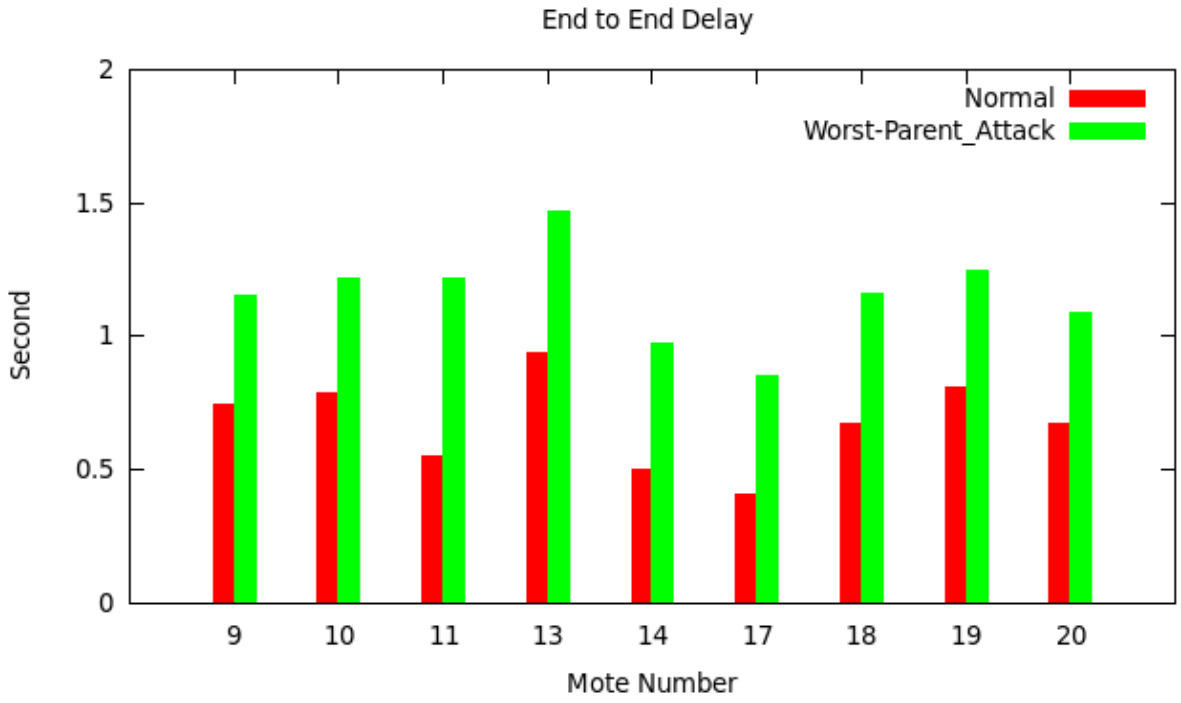
شکل ٤-١١ :متوسط مصرف توان در هر گره بر اساس توپولوژی شکل ٤-٨



شکل

٤-١٢ :متوسط سیکل‌های رادیویی در هر گره بر اساس توپولوژی شکل ٤-٨

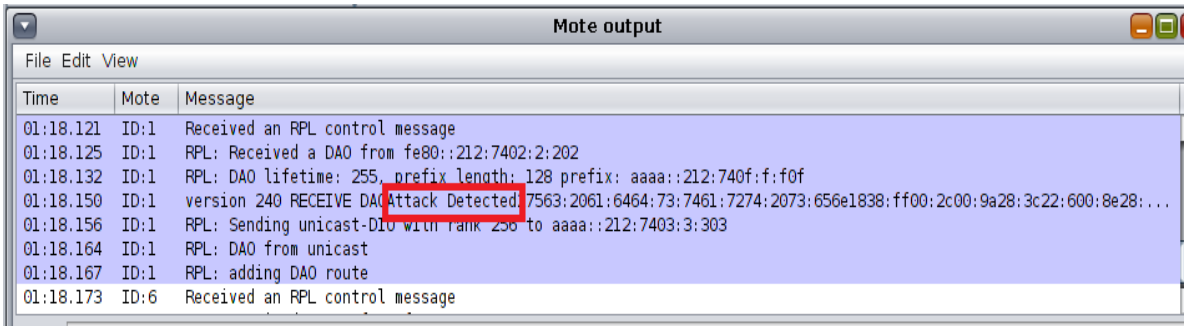
در شکل شماره ۴-۱۲ می‌توان متوسط سیکل رادیویی در هر گره را بر اساس توپولوژی شکل ۴-۸ مشاهده نمود. با توجه به شکل متوسط سیکل رادیویی در برخی گره‌ها در اثر اجرای حمله به شدت بالا رفته است. دلیل این امر نیز عبور ترافیک بیشتر از گره‌های مربوطه است. بنابراین با افزایش درصد دوره کاری گره‌های مذکور نسبت به قبل مدت زمان کارکرد آنها در گوش دادن به رسانه اشتراکی و ارسال رادیویی (افزایش زمان فعال بودن پالس در زمان کل دوره سیگنال رادیویی) نیز افزایش قابل توجهی داشته است. مشابه مصرف توان در شکل ۴-۱۱ به دلیل عدم اطلاع زیر درخت گره مخرب از تغییر پدر ارجح در حمله مربوطه متوسط سیکل رادیویی مربوط به این گره‌ها از اجرای حمله بدترین والد متاثر نشده است.



شکل ٤-۱۳ :تاخیر ناشی از اجرای حمله انتخاب بدترین والد

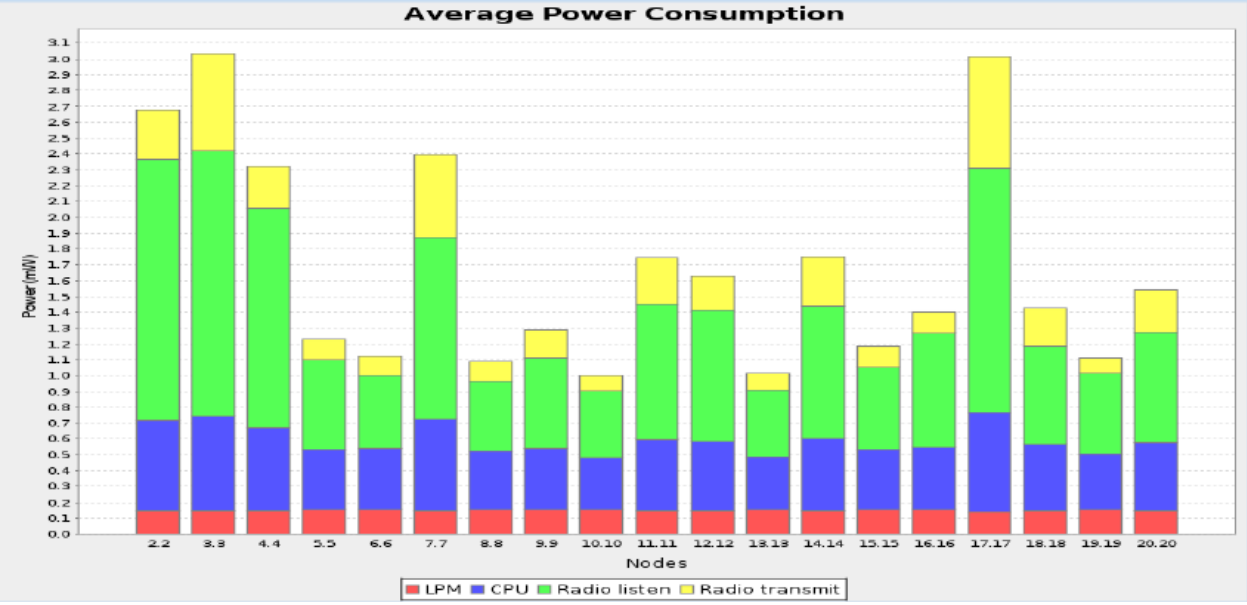
شکل شماره ۴-۱۳ نشان‌دهنده تاخیر ناشی از اجرای حمله انتخاب بدترین والد است. در برخی از گره‌ها افزایش تاخیر کاملا محسوس است. این افزایش در تاخیر به علت عبور ترافیک از مسیر طولانی‌تر و با ازدحام بیشتر گره‌ها (دسترسی سخت‌تر به رسانه اشتراکی) در بخش‌هایی از مسیر است. بر اساس شکل تاخیر دریافت بسته‌ها در گره ریشه با حرکت به سمت برگ‌ها صعودی می‌باشد.

٤-٧. بررسی روش CPC-RPL

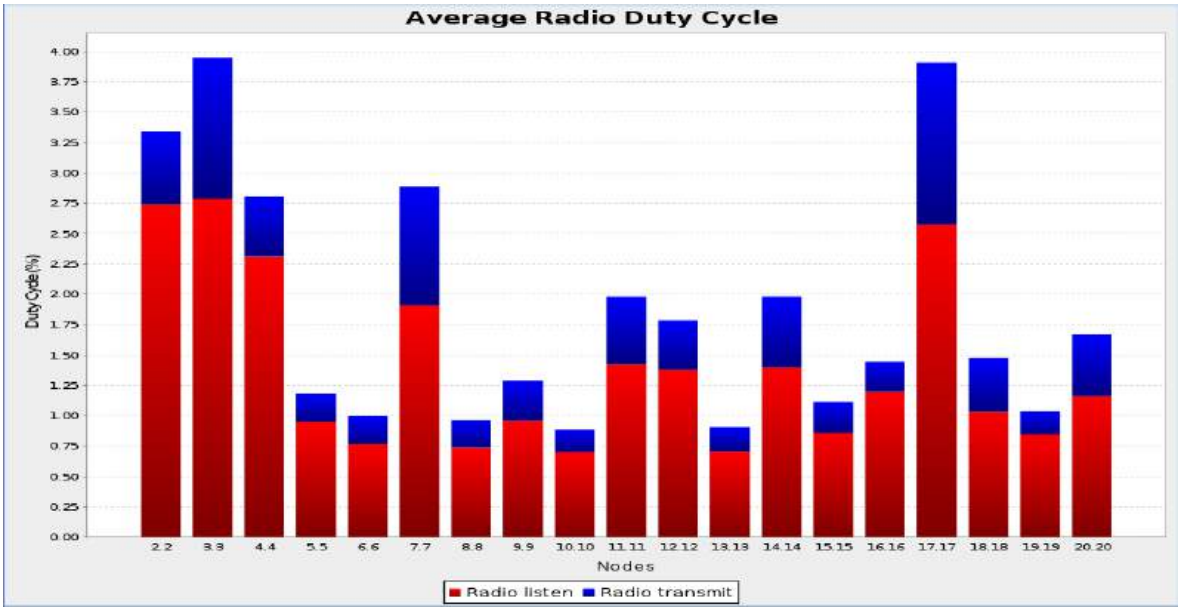


شکل ٤-١٤ : تشخیص حمله انتخاب بدترین والد در ریشه

همانطور که در شکل شماره ۴-۱۴ مشاهده می‌گردد با افزودن روش پیشنهادی به پروتکل RPL رفتار مخربانه (انتخاب بدترین والد) در ریشه تشخیص داده شده است. این امر در خروجی سنسور شماره ۱ در شکل توپولوژی ۴-۲ به صورت Log نمایش داده شده است. در ادامه این قسمت سربار ناشی از افزودن روش CPC-RPL به پروتکل RPL مورد بررسی قرار گرفته است. برای این کار بر روی توپولوژی شکل شماره ۴-۲ پروتکل CPC-RPL را اجرا و کارآمدی آن را علاوه بر میزان تحمیل سربار بر پروتکل RPL از دید دقت و سرعت در تشخیص نیز مورد بررسی قرار گرفته شده است. همچنین در انتهای این فصل امکان مقیاس‌پذیری روش پیشنهادی بررسی گردیده است. با توجه به شکل شماره ۴-۱۵ متوسط مصرف انرژی در تمام گره‌ها با افزودن روش پیشنهادی به پروتکل RPL نسبت به شکل شماره ۴-۵ تغییری نکرده است. بنابراین روش پیشنهادی از نظر مصرف انرژی سرباری را بر پروتکل RPL تحمیل نمی‌نماید.

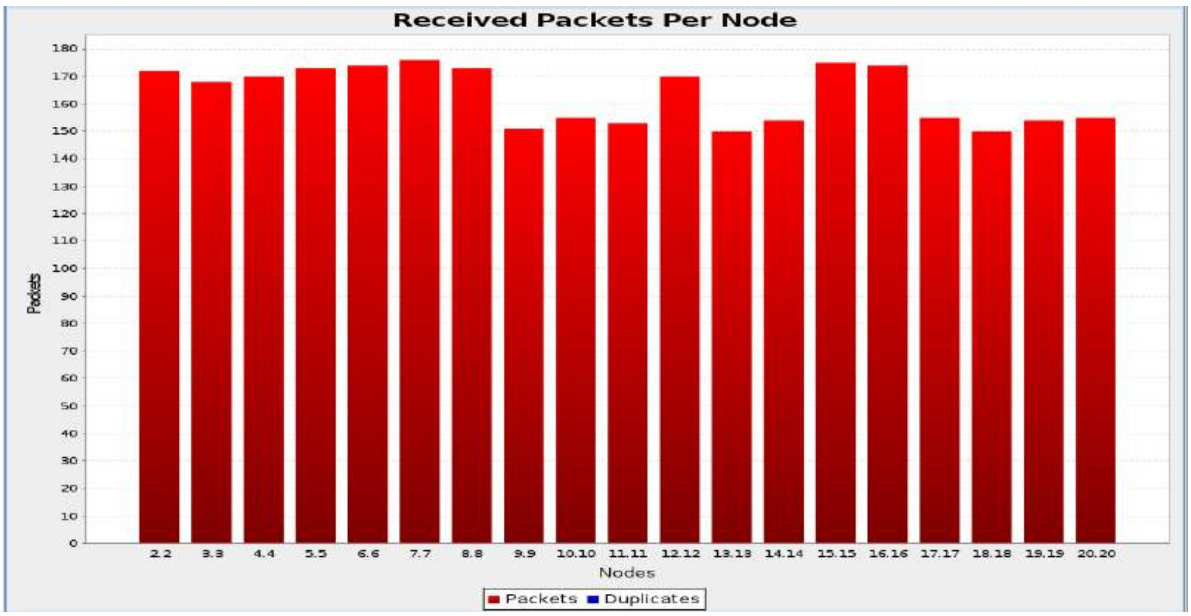


شکل ٤-١٥ : مصرف توان CPC-RPL در توپولوژی شکل شماره ٤-٢



شکل ٤-١٦ : متوسط سیکل رادیویی در CPC-RPL بر اساس توپولوژی شکل ٤-٢

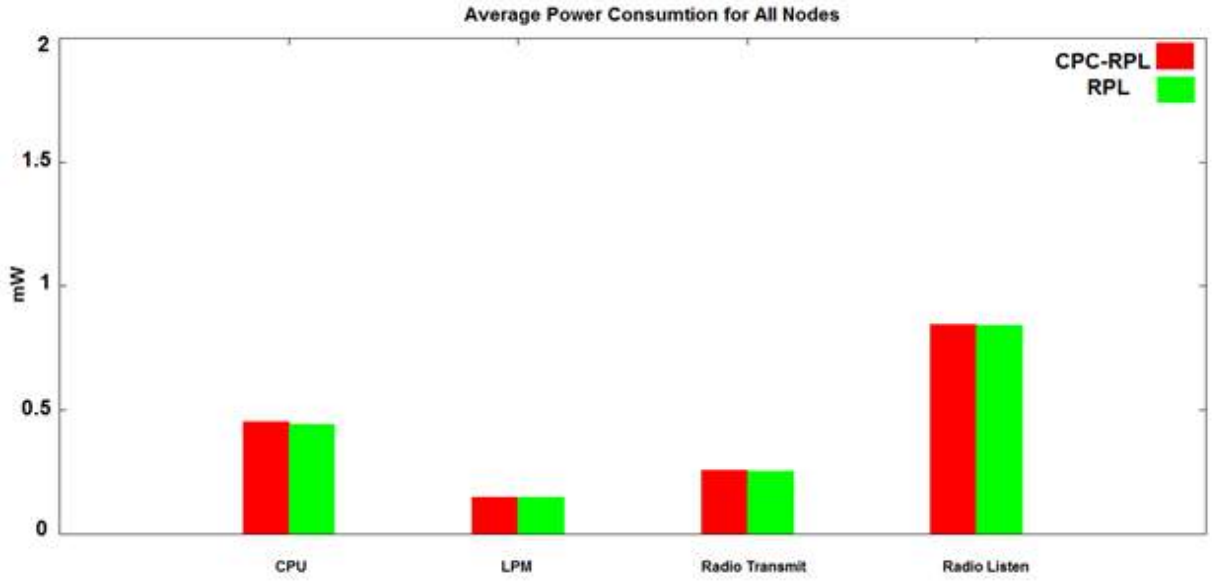
همانطور که در شکل شماره ۴-۱۶ مشاهده می‌گردد متوسط سیکل رادیویی نیز نسبت به پروتکل RPL در حالت عادی و بدون وجود رفتار مخربانه تغییری نداشته است. این امر برای تمام گره‌ها صادق می‌باشد. ثبات متوسط سیکل وظیفه رادیویی عدم افزایش مصرف انرژی را در پروتکل RPL به همراه روش پیشنهادی تصدیق می‌نماید.



شکل ٤-١٧ : بسته‌های دریافت شده به ازای هر گره در CPC-RPL بر اساس توپولوژی شکل ٤-٢

با افزودن روش پیشنهادی در تعداد بسته‌های دریافتی تغییر محسوسی نسبت به پروتکل عادی مشاهده نمی‌گردد. دلیل تفاوت‌های ناچیز احتمالی گم شدن بسته‌ها در اجراهای متفاوت است. بر اساس شکل ۴-۱۷ تعداد بسته‌های بیشتری از طرف گره‌های نزدیک‌تر به ریشه توسط Sink دریافت شده است. این امر به دلیل عبور ترافیک از طریق مسیر کوتاهتر و با نرخ کمتر در گم‌شدن بسته‌ها است.

شکل شماره ۴-۱۸ متوسط مصرف انرژی در تمام سنسورها را بر اساس مصرف انرژی ناشی از پردازنده، حالت LPM و مصرف رادیویی نشان می‌دهد. با توجه به شکل افزودن روش پیشنهادی به پروتکل RPL بدون وجود هیچ‌گونه سربار نیست. سربار ناشی از افزودن روش پیشنهادی به پروتکل RPL علاوه بر پردازنده بر مصرف انرژی رادیویی نیز موثر است. دلیل این امر وجود داده بیشتر برای ارسال رادیویی است (اطلاعات افزوده شده ناشی از گزارش‌های مشکوکانه).



شکل ٤-۱۸ : مقایسه متوسط مصرف توان در RPL و CPC-RPL

٤-۷-۱. معیار F-Measure در CPC-RPL

دقت و بازخوانی معیارهای کاربردی در حوزه بازیابی اطلاعات هستند که میزان تناسب اسناد بازیابی شده توسط سیستم را با نیاز کاربر تعیین می کنند. به جای این دو معیار، می توان از یک معیار ترکیبی برای ارزیابی کارایی بازیابی به نام F-Measure استفاده نمود:

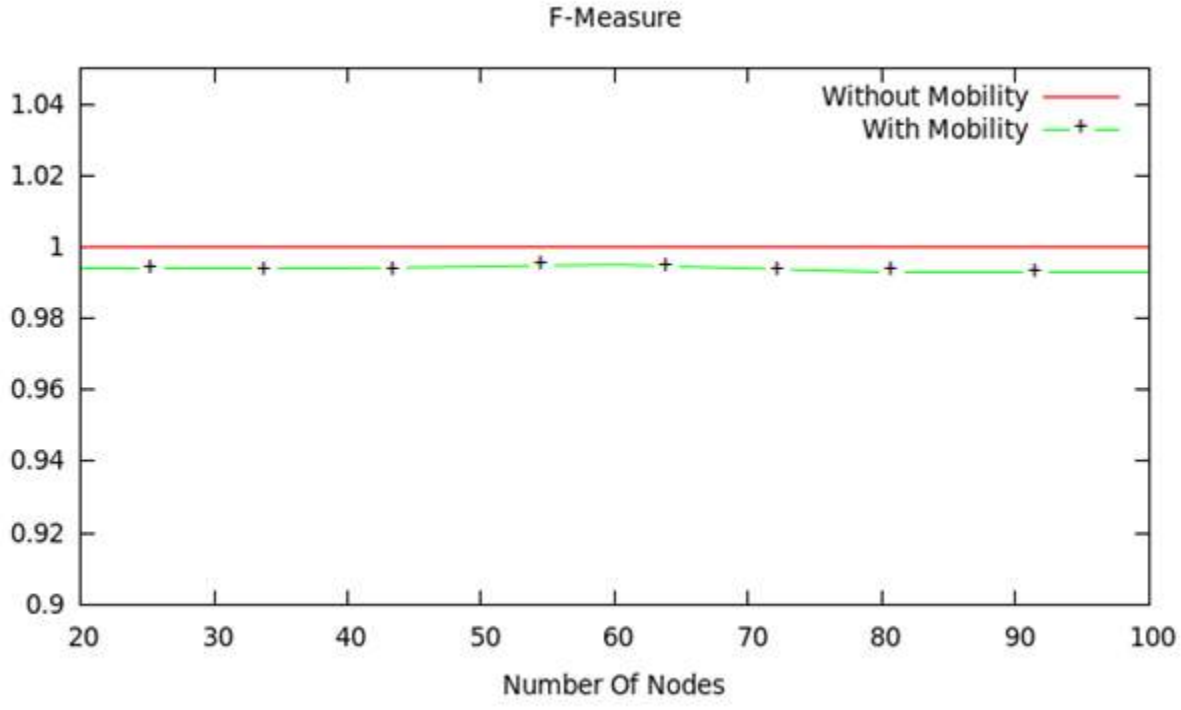
F-Measure= ۲*بازخوانی*دقت/(بازخوانی+دقت) [۴-۳]

این معیارها برای روش پیشنهادی به صورت زیر تعریف می شوند:

دقت= تعداد حمله‌های تشخیص داده شده صحیح \تعداد حملات تشخیص داده شده صحیح + تعداد حملات تشخیص داده شده غیر صحیح

بازخوانی= تعداد حملات تشخیص داده شده صحیح \تشخیص‌های غیر صحیح بدون وجود حمله + تعداد حملات تشخیص داده شده صحیح

در شکل شماره ۴-۱۸ معیار F-Measure روش پیشنهادی به همراه حرکت و بدون حرکت گره‌ها نشان داده شده است. برای محاسبه دقت روش پیشنهادی دو حالت با وجود تحرک در ۳۰ درصد از گره‌ها و بدون وجود تحرک در گره‌ها مورد بررسی قرار گرفته است. دو معیار دقت و بازخوانی مورد محاسبه قرار گرفته و سپس به وسیله این دو مقدار معیار F-Measure به دست آمده است.

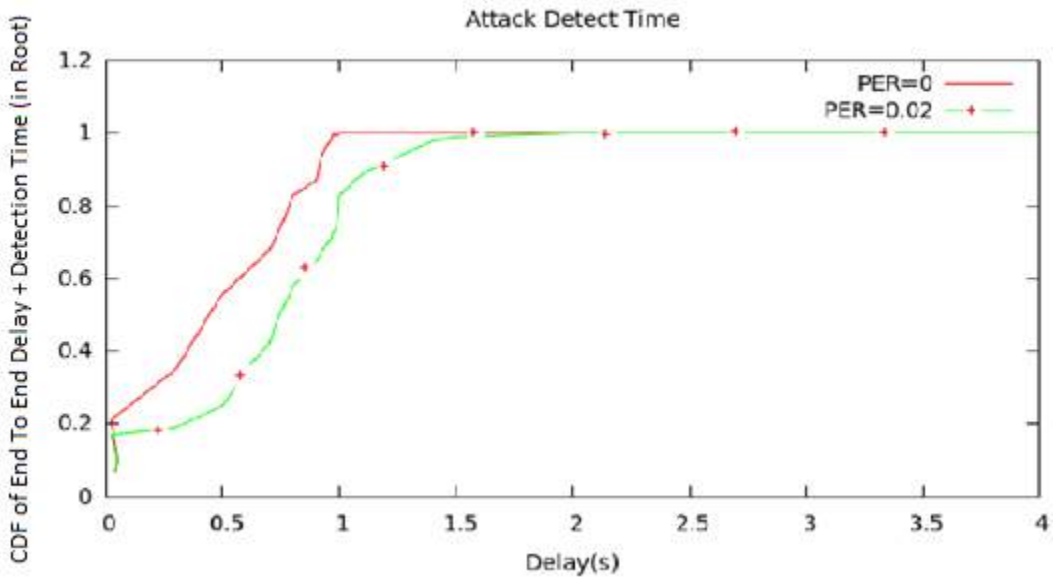


شکل ٤-١٩ : معیار F-Measure روش پیشنهادی با افزایش تعداد گره‌ها

٤-۷-۲. تاخیر تشخیص در CPC-RPL

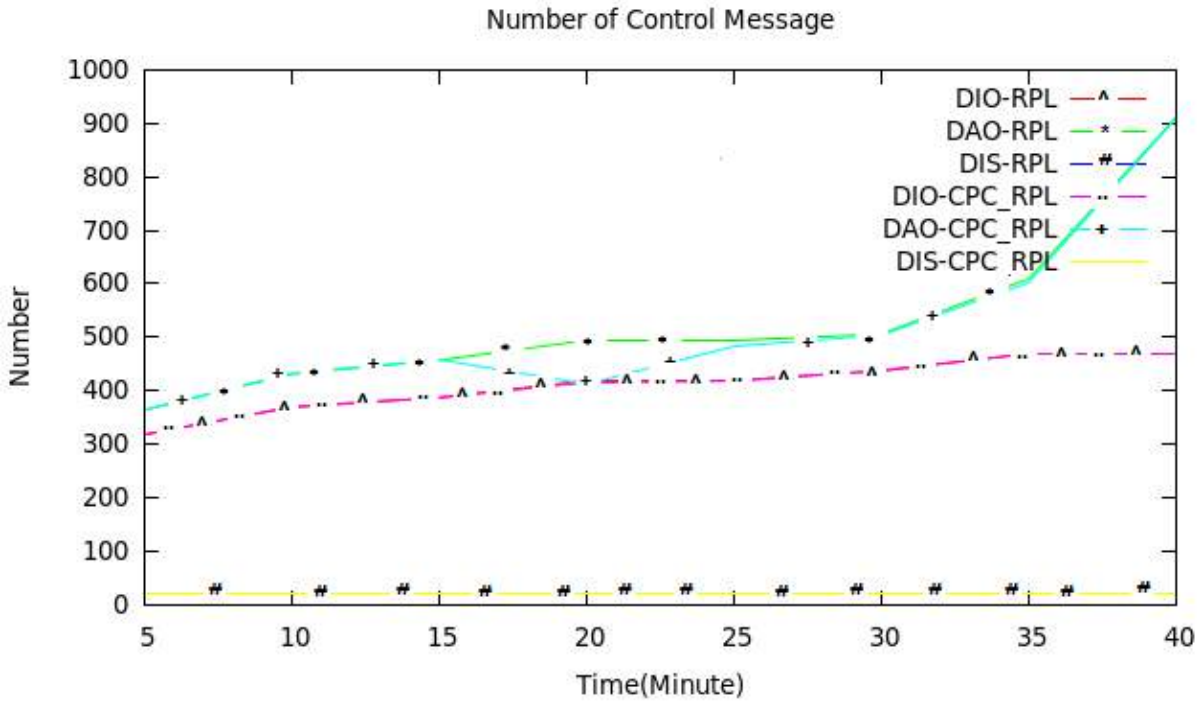
سرعت تشخیص روش پیشنهادی برابر با زمان تاخیر بسته‌های مشکوک (بسته مشکوک نوع دوم به جز موارد خاص دیرتر به ریشه خواهد رسید) و زمان پردازش لازم در گره‌ها می‌باشد. این امر برای ۱۰۰ سنسور با عدم خطا در بسته‌ها و همچنین نرخ خطای بسته‌های ۰,۰۲ در شکل شماره ۴-۲۰ مورد بررسی قرار گرفته است.

نکته : مورد استثنای مربوط به حالت تغییر پدر ارجح به دلیل RANK<ETX در این نمودار لحاظ نشده است. تاخیر تشخیص در این حالت حداکثر ۲۵۶ ثانیه می‌باشد.



شکل ٤-۲۰ : سرعت تشخیص حمله (به جز در مورد استثنا)

شکل شماره ۴-۲۱ تعداد پیام‌های کنترلی در پروتکل RPL را در مقایسه با روش پیشنهادی و RPL در شرایط بدون وجود رفتار مخربانه نشان می‌دهد. با توجه به شکل در پروتکل RPL به همراه روش پیشنهادی تغییر چندانی در تعداد پیام‌های کنترلی بدون وجود رفتار مخربانه مشاهده نمی‌گردد. این امر نشان‌دهنده‌ی سربار بسیار پایین روش پیشنهادی بر تعداد پیام‌های کنترلی است. بدیهی است که تشخیص رفتار مخربانه از نوع بدترین والد توسط روش پیشنهادی منجر به افزایش پیام‌های کنترلی خواهد گردید. همچنین اجرای مکانیسم بازیابی مربوط به روش پیشنهادی در مقابل برخی حملات نظیر کاهش مقدار RANK به دلیل بازیابی درخت DODAG (حذف گره مخرب) منجر به افزایش تعداد پیام‌های کنترلی از جمله DIO و DAO خواهد گردید. این امر در قسمت‌های بعدی مورد بررسی قرار داده شده است.



شکل ٤-٢١: مقایسه تعداد پیام‌های کنترلی در RPL و CPL-RPL

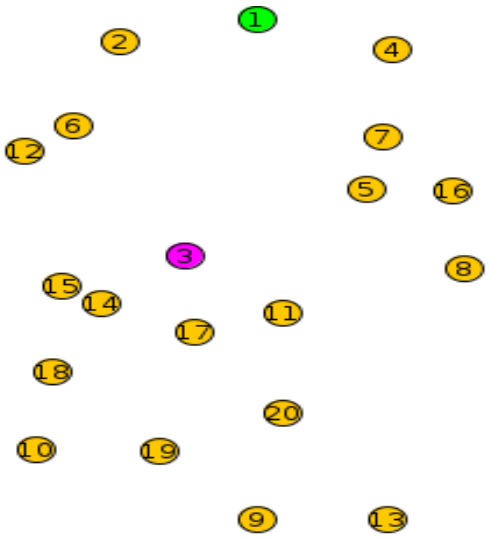
٤-٨. مکانیسم بازیابی

در این قسمت عملکرد مکانیسم بازیابی در CPC-RPL را بر روی حمله کاهش مقدار RANK بررسی خواهیم کرد. ابتدا تاثیر حمله کاهش مقدار Rank را بر روی پروتکل RPL نشان می‌دهیم.

٤-٨-١. بررسی تاثیر حمله کاهش مقدار Rank در پروتکل RPL

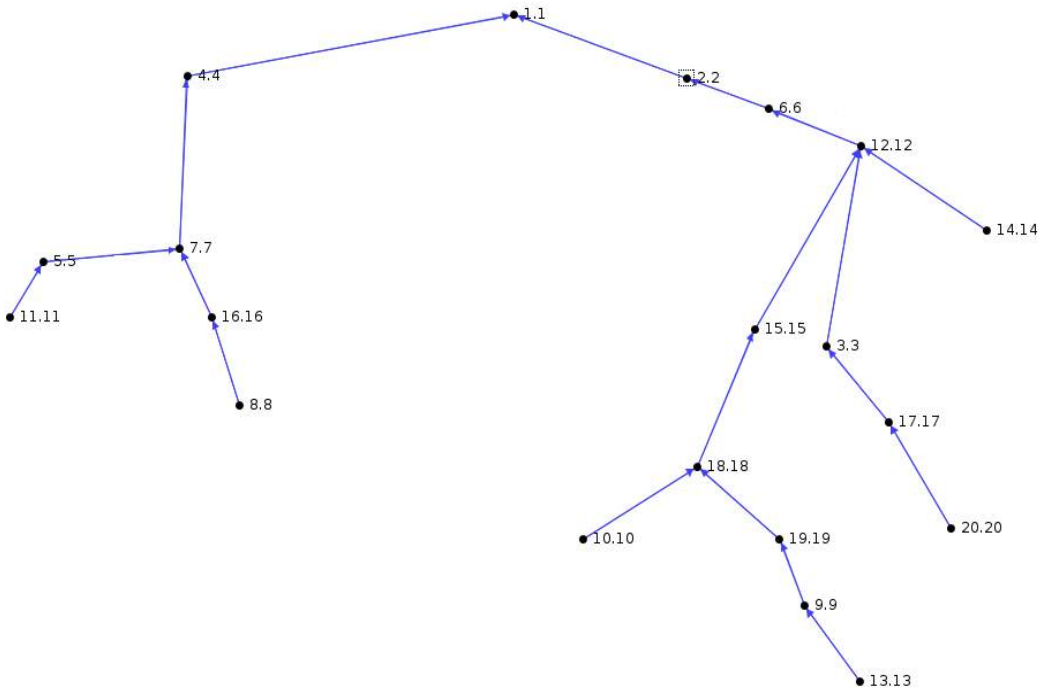
برای مشاهده تاثیر حمله کاهش مقدار Rank پس از انتخاب یک توپولوژی تصادفی دارای شرایط وقوع حمله کاهش مقدار Rank (گره مخرب با کاهش مقدار Rank خود بتواند پدر ارجح در برخی گره‌ها را تغییرو حمله مربوطه را شکل دهد) ابتدا پروتکل RPL را بدون وجود رفتار مخربانه و سپس آن را با وجود حمله کاهش مقدار Rank اجرا و بررسی می‌نماییم.

در توپولوژی شکل ۴-۲۲ گره شماره ۱ ریشه و در نقش دریافت‌کننده، گره شماره ۳ مخرب و از نوع حمله کاهش مقدار Rank می‌باشد. سایر گره‌ها بدون رفتار مخربانه و در نقش ارسال کننده می‌باشند. برای تاثیر بیشتر رفتار مخربانه در کارایی شبکه حمله کاهش مقدار Rank در پیاده‌سازی با حمله سیاه‌چاله ترکیب شده است. با این کار گره مخرب پس از جذب حجم بالای ترافیک به علت وقوع حمله کاهش مقدار Rank بسته‌های ورودی را نیز حذف می‌نماید.



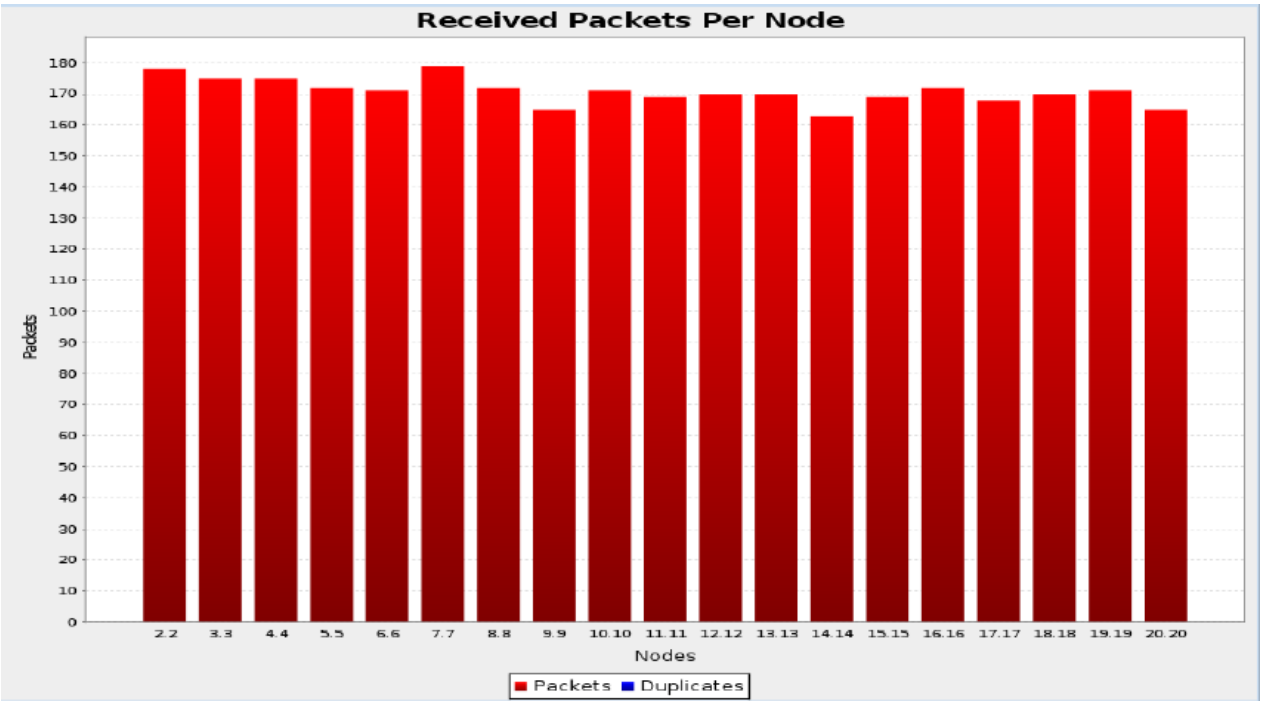
شکل ٤-۲۲ : توپولوژی تصادفی انتخابی جهت بررسی تاثیر حمله کاهش مقدار Rank و مکانیسم بازیابی

٤-۸-۲. نمودارهای مربوط به حالت عادی پروتکل RPL



شکل ٤-۲۳ : توپولوژی حاصل از اجرای پروتکل RPL در درخت DODAG شکل شماره ٤-۲۲

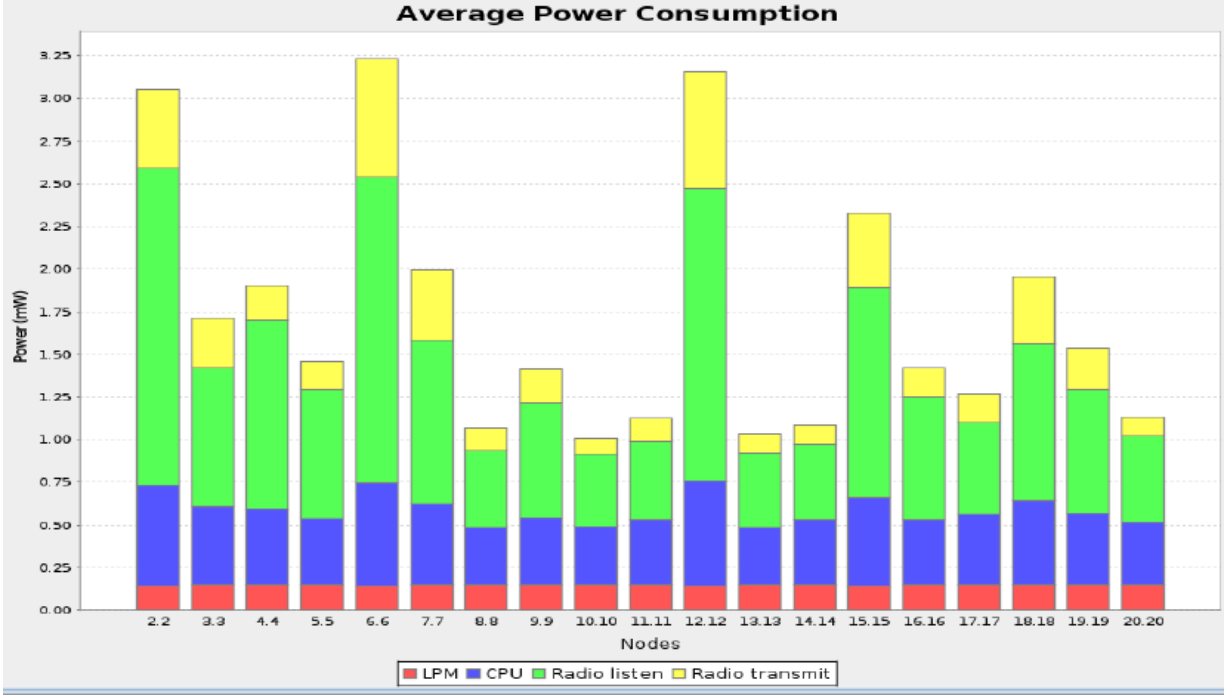
همانطور که در شکل شماره ۴-۲۳ مشاهده می‌گردد با اجرای پروتکل RPL بر روی درخت DODAG شکل شماره ۴-۲۲، هر گره بهترین والد خود را به عنوان پدر ارجح انتخاب می‌نماید. به این ترتیب ترافیک متعلق به گره‌ها از کوتاهترین مسیر به ریشه خواهد رسید.



شکل ٤-٢٤ : تعداد بسته‌های دریافت شده در توپولوژی شکل شماره ٤-۲۳

با توجه به شکل شماره ۴-۲۴ گره‌های دورتر و یا دارای مسیر پرازدحام‌تر در مسیر ارتباطی با ریشه تعداد بسته‌های کمتری نیز منتقل نموده‌اند. دلیل این امر گم شدن بسته‌ها و یا تاخیر در رسیدن به مقصد (ریشه) برای تعداد زیادی در ارسال‌ها می‌باشد.

شکل شماره ۴-۲۵ متوسط مصرف توان را نشان می‌دهد. با توجه به شکل گره‌های با ترافیک عبوری بیشتر دارای مصرف انرژی بالاتر نیز می‌باشند. این موضوع، امری طبیعی است زیرا پردازش و استفاده از تکنولوژی رادیویی در این گره‌ها بالاتر است. با توجه به شکل گره‌های شماره ۲،۶ و ۱۲ متوسط مصرف توان بیشتری نسبت به سایرین داشته‌اند. دلیل اصلی این امر حجم بالای ترافیک ورودی در این گره‌ها بر اساس توپولوژی درخت DODAG است.



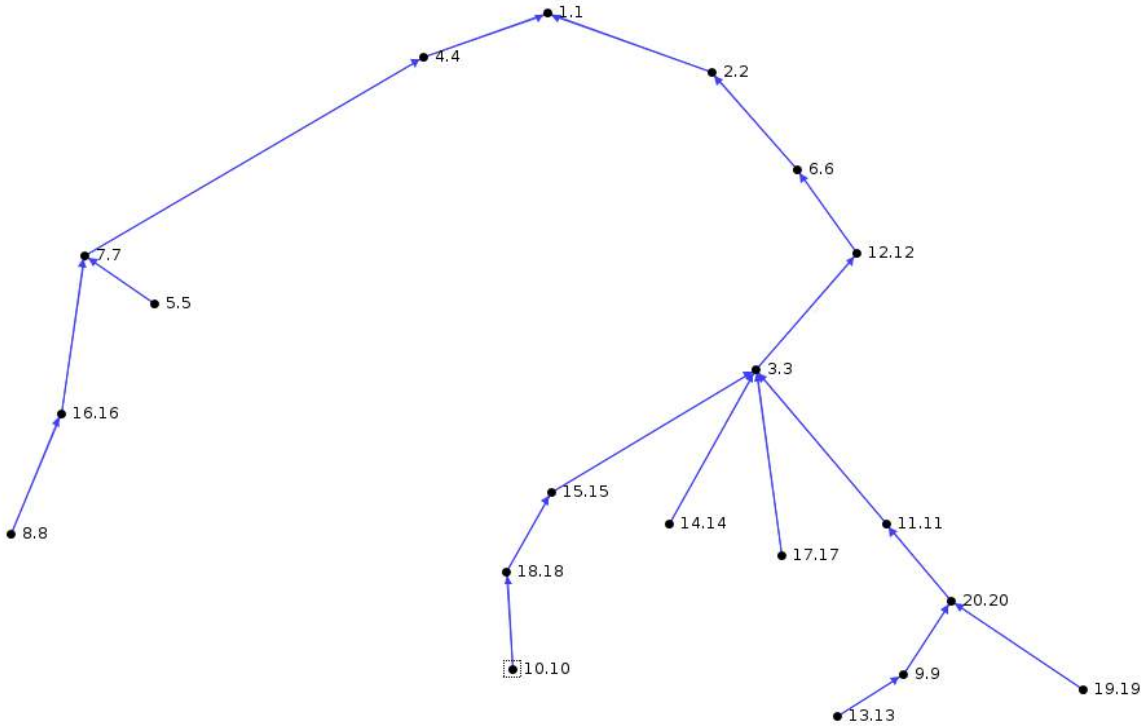
شکل ٤-۲۵ : متوسط مصرف توان بر اساس شکل شماره ٤-۲۳

٤-۸-۳. نمودارهای مربوط به تاثیر حمله کاهش مقدار Rank

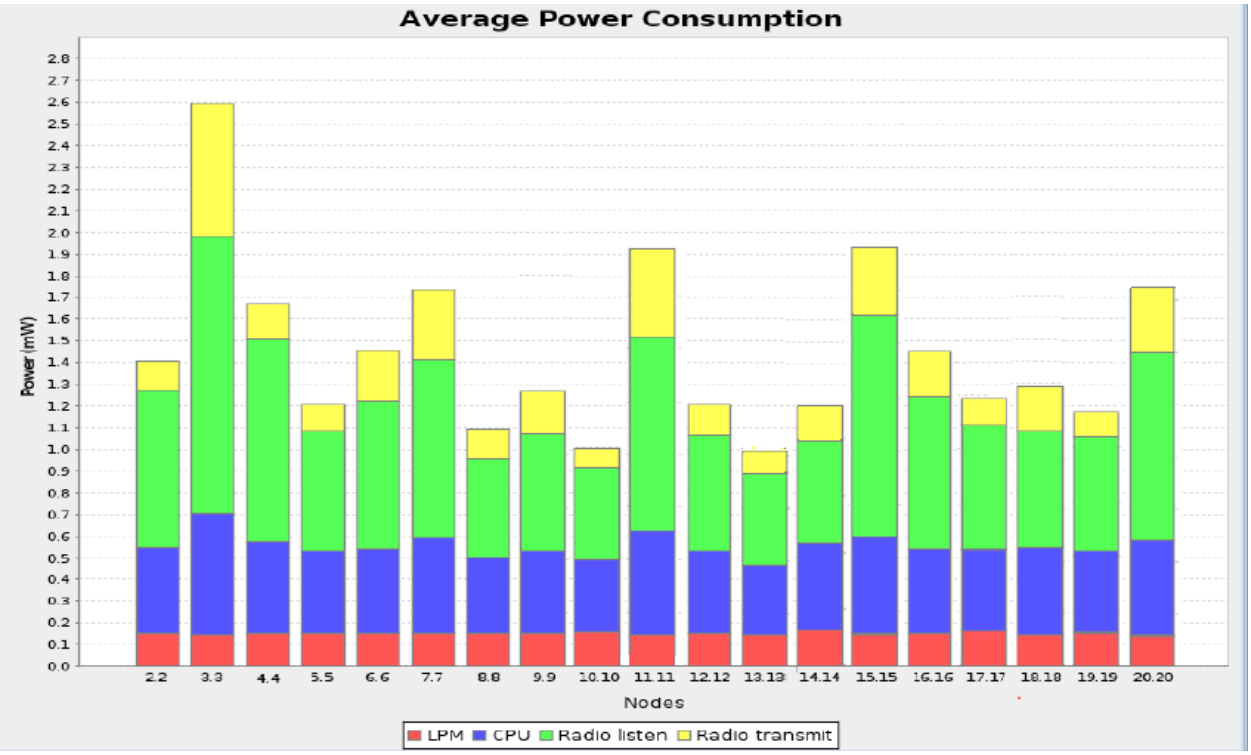
در ادامه نمودارهای مربوط به اجرای حمله کاهش مقدار Rank آورده شده است.

شکل ۴-۲۶ توپولوژی حاصل از اجرای حمله کاهش مقدار Rank توسط گره مخرب در درخت DODAG شکل ۴-۲۲ را نشان می‌دهد. با توجه به شکل، پس از اجرای حمله بسیاری از گره‌ها، گره مخرب را به عنوان پدر ارجح انتخاب کرده و ترافیک خود را از طریق آن به سمت ریشه منتقل می‌نمایند. کاهش مقدار Rank در گره مخرب به گونه‌ای است که گره‌های قربانی وجود مسیری بهتر از طریق گره مخرب به سمت ریشه را گمان می‌نمایند.

با توجه به شکل، گره‌های ۱۵،۱۴و۲۰ با تغییر پدر ارجح به صورت مستقیم و گره‌های زیر درخت آن‌ها نیز به صورت غیر مستقیم قربانی حمله مذکور می‌گردند. در ادامه تاثیر این امر را بر روی مصرف توان و کارایی شبکه مورد بررسی قرار خواهیم داد.



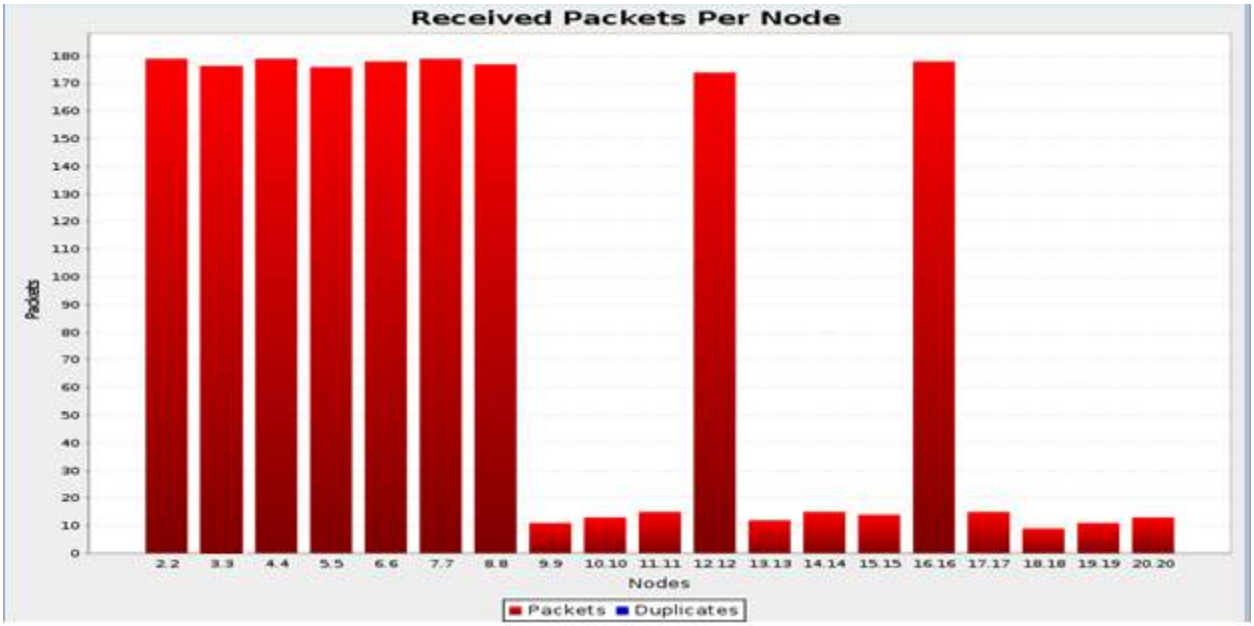
شکل ٤-٢٦ : توپولوژی حاصل از اجرای حمله کاهش مقدار Rank توسط گره مخرب در درخت DODAG شکل شماره ٤-٢٢



شکل ٤-٢٧ : متوسط مصرف انرژی بر اساس شکل شماره ٤-٢٦

با توجه به شکل شماره ۴-۲۷ پس از اجرای حمله کاهش مقدار Rank توپولوژی درخت DODAG به دلیل انتخاب گره مخرب توسط برخی Mote ها به عنوان پدر ارجح تغییر می‌نماید. با این کار در اثر حذف ترافیک ورودی (پس از حمله) توسط گره مخرب بازارسال ترافیک در بسیاری از گره‌ها (پدر و اجداد مربوط به گره‌های قربانی قبل از حمله) نسبت به حالت عادی و بدون رفتار مخربانه کاهش می‌یابد. این امر باعث کاهش مصرف انرژی در این گره‌ها به علت کاهش ترافیک ورودی در شکل ۴-۲۷ شده است.

در برخی گره‌های قربانی به دلیل تغییرات ناشی از حمله کاهش مقدار Rank در توپولوژی ترافیک بیشتری عبور می نماید. با توجه به این امر مصرف انرژی در این گره‌ها (پدر و اجداد گره مخرب) نسبت به حالت عادی بیشتر می‌گردد. به دلیل عدم وجود تصدیق از دریافت بسته‌ها در اینترنت اشیاء (استفاده از پروتکل UDP) گره‌های قربانی متوجه حذف اطلاعات توسط گره مخرب نخواهند شد.

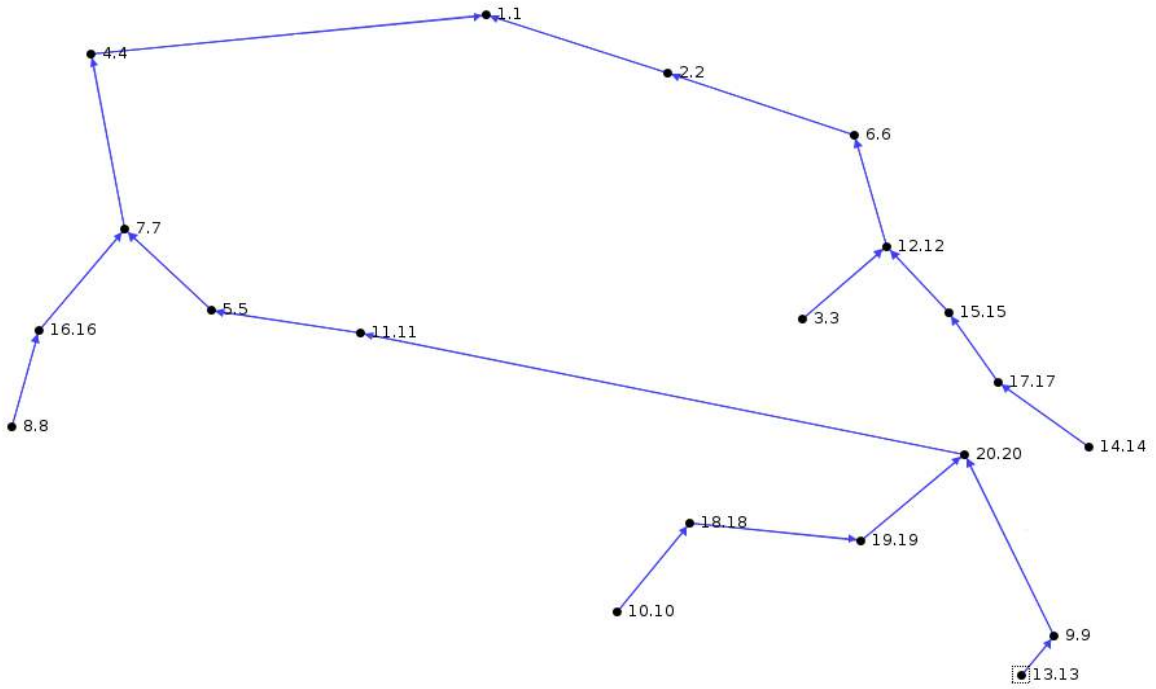


شکل ٤-۲۸ : بسته‌های دریافت شده بر اساس توپولوژی شکل شماره ٤-۲٦

همانطور که در شکل شماره ۴-۲۸ مشاهده می‌گردد در اثر اجرای حمله کاهش مقدار Rank گره‌های قربانی دیگر نتوانسته‌اند پیام‌های خود را از طریق شبکه به گره ریشه (Sink) برسانند. دلیل این امر حذف ترافیک عبوری متعلق به این Moteها در گره مخرب پس از اجرای حمله می‌باشد. تعداد بسته‌های دریافت شده‌ی سایر گره‌ها در ریشه به علت عدم عبور از گره مخرب تغییر محسوسی نداشته است.

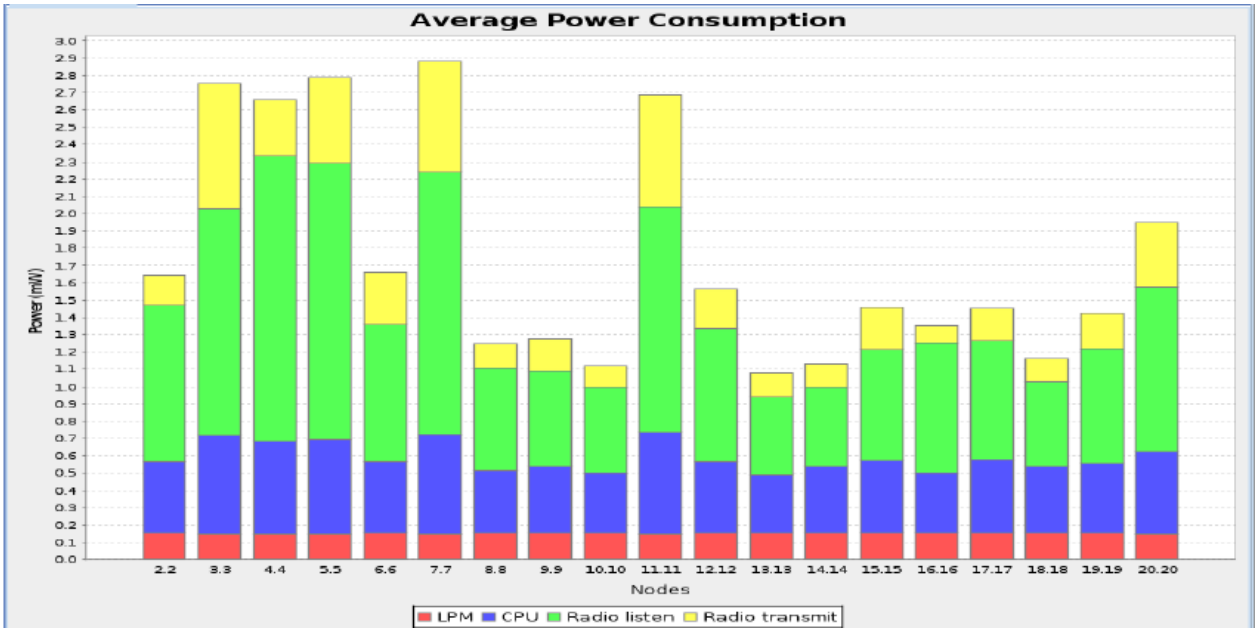
٤-٨-٤ . نمودارهای مربوط به مکانیسم بازیابی

در این قسمت به بررسی تاثیر مکانیسم بازیابی روش پیشنهادی در مقابل حمله کاهش مقدار Rank پرداخته شده است. توپولوژی و پارامترهای شبیه‌سازی در این قسمت با دو قسمت قبل (بررسی پروتکل RPL و حمله کاهش مقدار Rank) یکسان است. در ادامه ابتدا توپولوژی نهایی حاصل از اجرای مکانیسم بازیابی روش پیشنهادی (در درخت DODAG شکل ۴-۲۹) مورد بررسی قرار گرفته شده است.

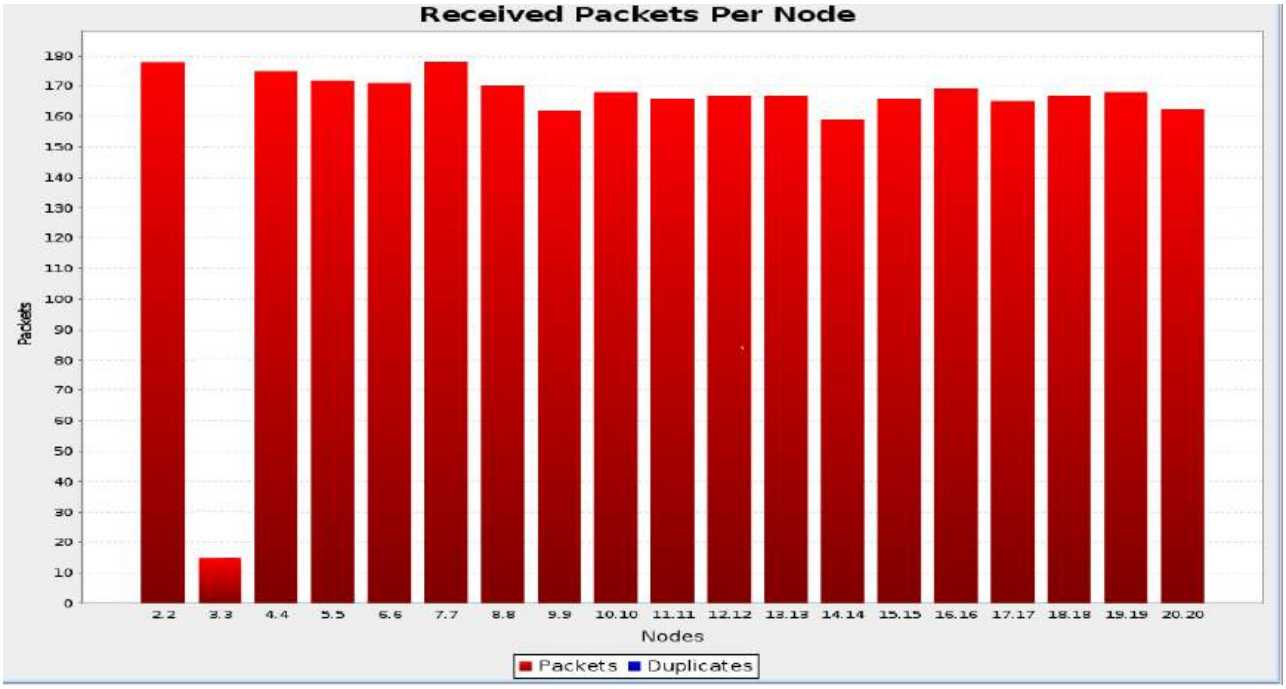


شکل ٤-۲۹ : توپولوژی حاصل از اجرای مکانیسم بازیابی روش پیشنهادی در توپولوژی شکل ٤-۲۲

با تشخیص حمله و اجرای مکانیسم بازیابی گره مخرب از درخت DODAG حذف و گره‌های قربانی مسیر دیگری را برای انتقال ترافیک خود به سمت ریشه برمی‌گزینند. حتی گره‌هایی که در حالت عادی گره شماره ۳ را به عنوان پدر ارجح خود انتخاب کرده بودند (گره‌های ۱۷و ۲۰ در شکل ۴-۲۳) با تغییر پدر ارجح خود به انزوای گره مخرب کمک می‌نمایند. اگر زیر درخت گره مخرب پس از حمله کاهش مقدار Rank مسیری برای دریافت پیام حاوی لیست سیاه در مکانیسم بازیابی نداشته باشد آنگاه این زیر درخت نیز به همراه گره مخرب از درخت DODAG حذف می‌گردد.

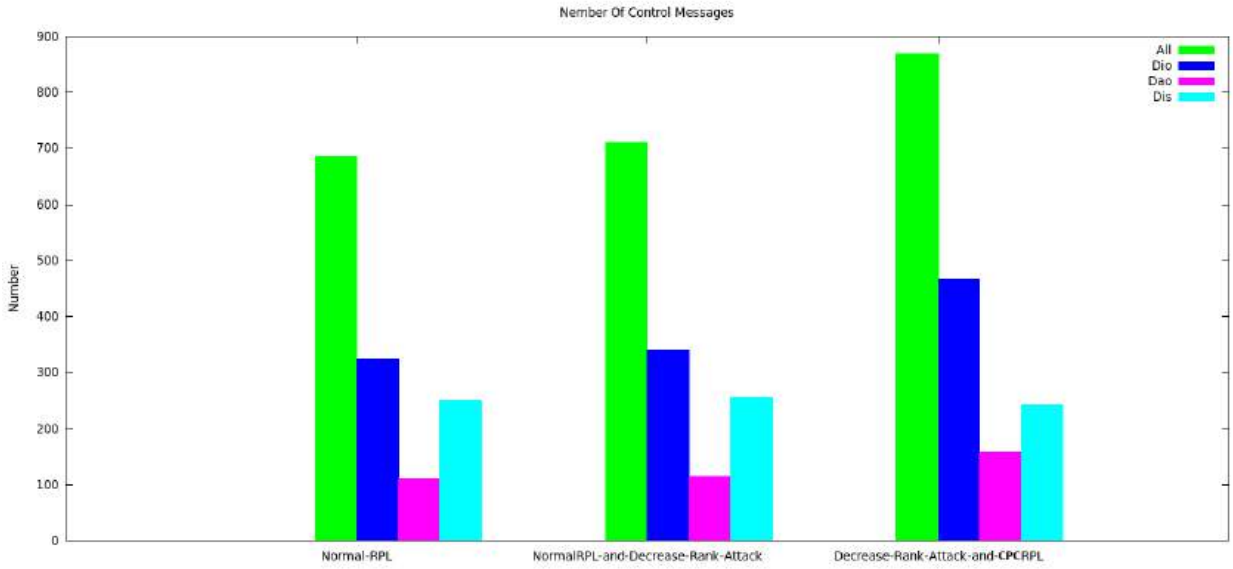


شکل ٤-۳۰: متوسط مصرف انرژی بر اساس توپولوژی شکل شماره ٤-۲۹



شکل ٤-۳۱: بسته‌های دریافت شده بر اساس شکل توپولوژی شماره ٤-۲۹

پس از حذف گره مخرب در شکل ۴-۲۹ گره‌های قربانی مطابق با پروتکل RPL بهترین پدر ارجح خود را جهت ارسال ترافیک به سمت ریشه انتخاب نموده‌اند. با این امر مصرف انرژی در تمام گره‌ها بر اساس حجم ترافیک ورودی بوده و مصرف انرژی از برگ‌ها به سمت ریشه صعودی خواهد بود. با حذف گره مخرب ترافیک مربوط به گره‌های قربانی (در حمله کاهش مقدار Rank) با عدم عبور از گره مخرب به طور مجدد در ریشه دریافت شده است. تعداد بسته‌های دریافتی هر گره در ریشه نیز نشان‌دهنده عملکرد صحیح روش پیشنهادی است.



شکل ٤-۳۲: مقایسه پیام‌های کنترلی پروتکل RPL و حمله کاهش مقدار Rank و مکانیسم بازیابی

همانطور که در شکل شماره ۴-۳۲ مشاهده می‌گردد با اجرای مکانیسم بازیابی (یک مرتبه) جهت حذف گره مخرب تعداد پیام‌های کنترلی در شبکه افزایش داشته است. دلیل این امر تنظیم مجدد زمانسنج مربوط به ارسال پیام DIO با دریافت لیست سیاه شامل آدرس گره مخرب است. این تنظیم مجدد جهت افزایش سرعت انتشار پیام‌های DIO صورت می‌گیرد. با تنظیم مجدد زمانسنج پیام DIO سرعت ارسال پیام‌های DAO نیز جهت به روزسازی شبکه افزایش می‌یابد. افزایش مربوط به ارسال پیام‌های DAO بیش از پیام‌های DIO است. در صورت اجرای مکانیسم بازیابی در حالی که هنوز مکانیسم بازیابی حمله قبلی در حال اجراست روند افزایش تعداد پیام‌های کنترلی را با کاهش روبرو خواهد گردید. دلیل این امر وجود الگوریتم قطره‌چکان در پروتکل RPL است. بر اثر این الگوریتم دریافت پیام بازیابی اولیه موجب شروع به هنگام‌سازی شبکه (تنظیم زمانسنج الگوریتم قطره چکان) می‌گردد. اجرای دوباره مکانیسم بازیابی تنها باعث تنظیم مجدد زمانسنج موجود در الگوریتم قطره چکان به مقدار اولیه خواهد گردید. بر این اساس اگر چند اجرای بازیابی متفاوت قبل از زمان بازیابی کامل شبکه (رسیدن به حالت پایدار) صورت بگیرد آنگاه روند افزایش پیام‌های کنترلی با کاهش چشمگیری نسبت به اجرای مکانیسم بازیابی نسبت به حالتی که تنها یک بار این عمل صورت گیرد روبرو خواهد گردید. اجرای مکانیسم‌های بازیابی

متفاوت برای حذف گره مخرب در حالت عدم تداخل در دو اجرای متوالی در هر اجرا سرباری مشابه حالت اول (تنها یک اجرا مکانیسم بازیابی بدون تداخل اجرای دیگر) را داراست. بنابراین می‌توان این افزایش را از مرتبه O(۱) دانست.

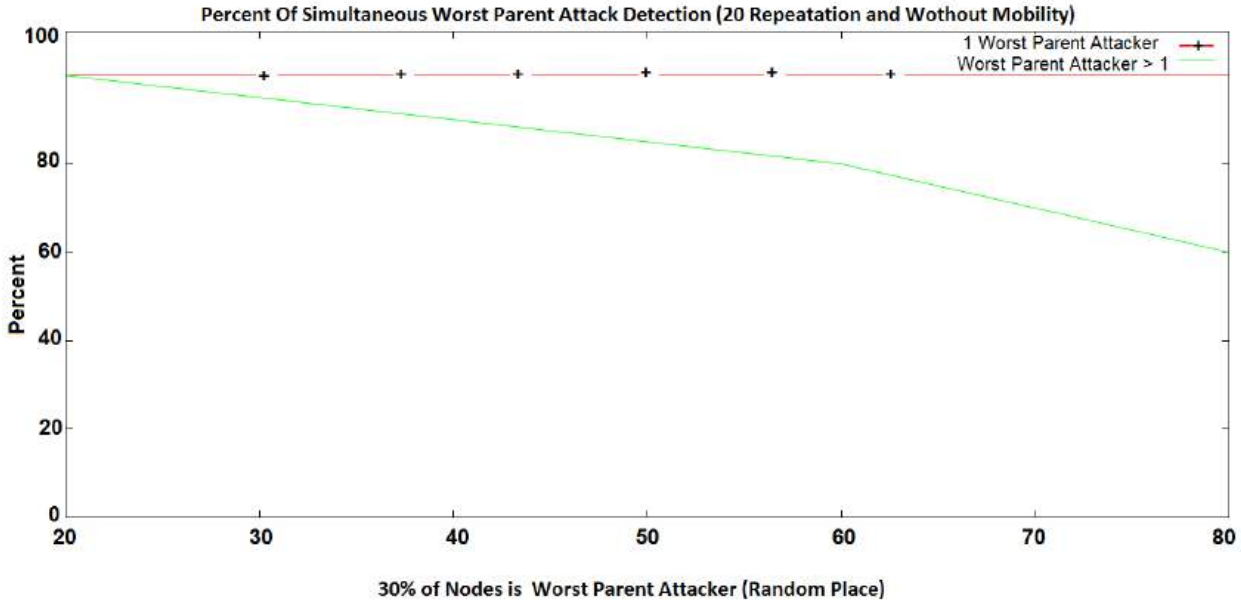
٤-۹. رفتار روش پیشنهادی در اثر افزایش تعداد گره‌های مخرب

با توجه به فصل سوم با افزایش تعداد گره‌های مخرب از نوع حمله انتخاب بدترین والد گره بالاتر تشخیص داده خواهد شد. تشخیص همزمان سایر گره‌های مخرب تنها در شرایط زیر اتفاق خواهد افتاد:

۱-گره‌های مخرب در درخت اجداد یکدیگر نباشند.

۲-در صورتی که گره‌های مخرب اجداد یکدیگر باشند: در این حالت امکان تشخیص همزمان وجد ندارد

نکته : در حالت دوم با حذف گره مخرب اول، گره مخرب دوم تشخیص و به همین ترتیب گره‌های مخرب بعدی در صورت وجود شناخته می‌شوند.



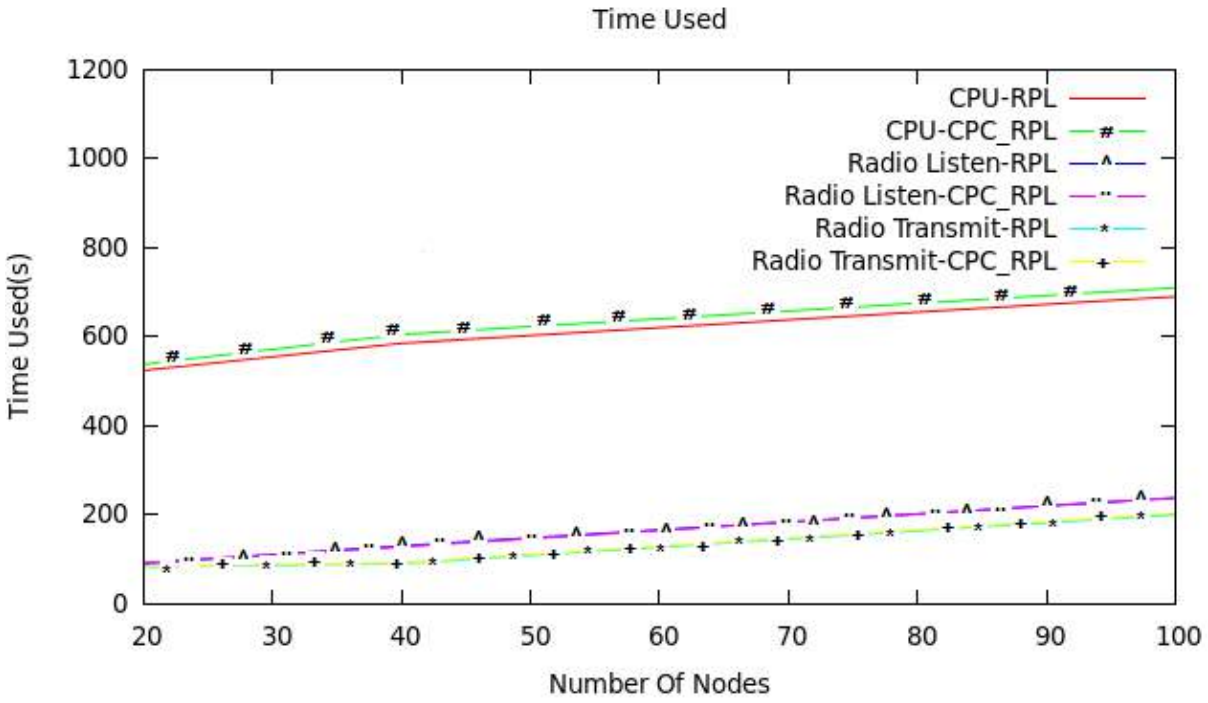
شکل ٤-۳۳ : رفتار CPC-RPL در مقابل افزایش تعداد گره مخرب از نوع حمله انتخاب بدترین والد

در شکل شماره ۴-۳۳ درصد تشخیص همزمان گره‌های مخرب (از نوع حمله انتخاب بدترین والد) با افزایش تعداد گره‌های مخرب نشان داده شده است. دراین بررسی ۳۰ درصد گره‌ها مخرب و به صورت تصادفی از میان

کل گره‌ها در هر توپولوژی مورد آزمایش (انتخاب توپولوژی نیز تصادفی است) انتخاب شده‌اند. با توجه به شکل افزایش تعداد گره‌های مخرب احتمال تشخیص همزمان رفتار مخربانه (از نوع حمله انتخاب بدترین والد و سایر حملات تحت مقابله روش پیشنهادی) را کمتر می‌نماید.

٤-١٠. قابلیت مقیاس‌پذیری در پروتکل CPC-RPL

در این قسمت برای سنجش قابلیت مقیاس پذیری در پروتکل RPL علاوه بر بررسی وجود سربار از دید مصرف انرژی (قسمت ۴-۷) به بررسی زمان سپری شده توسط هر سنسور در حالت پردازش و یا استفاده از تکنولوژی رادیویی به طور متوسط پرداخته شده است. این بررسی در بدترین حالت عملکردی برای روش پیشنهادی (گره‌های متحرک) صورت گرفته است. CPC-RPL در حالت تحرک گره‌ها به دلیل افزایش تغییر پدر ارجح در گره‌ها سربار بیشتری نسبت به حالت عادی دارد. این امر در دقت و سرعت روش پیشنهادی تاثیری ندارد.



شکل ٤-٣٤: متوسط مقدار زمان مصرفی گره‌ها در حالت پردازش، و تکنولوژی رادیویی نسبت به افزایش تعداد گره‌ها

همانطور که در شکل نیز مشاهده در CPC-RPL متوسط میزان زمان مربوط به پردازش و تکنولوژی رادیویی در هر سنسور نسبت به پروتکل RPL بدون روش پیشنهادی تقریبا یکسان می‌باشد. با توجه به شکل شماره ۴-

۳۳ این ثبات با افزایش تعداد گره‌ها همچنان باقی می‌ماند. بنابراین CPC-RPL روشی مقیاس پذیر است. در این بررسی ۳۰ درصد تعداد کل گره بر اساس مدل Random Way Point حرکت می‌نمایند.

مقدار فضای مورد نیاز روش پیشنهادی در رام مربوط به هر یک از سنسورهای Sky Mote (بر اساس گره‌های ارسال کننده) در پروتکل RPL برابر با ۷۱۶ بایت است. با توجه به اندازه ۴۸ کیلوبایتی کل فضای رام در این سنسورها فضای اضافی مربوط به CPC-RPL در کلاینت‌ها بسیار مناسب است. همچنین روش پیشنهادی نیازمند ۲۱۱ بایت فضای اضافه در RAM نیز می‌باشد. بنابراین سنسورهای Tmote Sky با فضای RAM ۱۰ کیلوبایتی قابلیت اجرای روش پیشنهادی در شبکه‌های به نسبت بزرگ را نیز دارا می‌باشند.

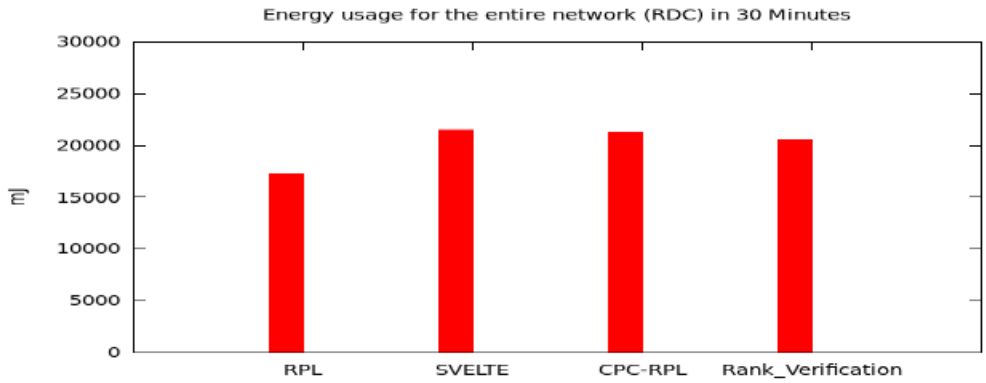
٤-۱۱. مقایسه روش پیشنهادی

در این قسمت به مقایسه روش پیشنهادی با کارهای پیشین خواهیم پرداخت. به دلیل عدم وجود روش برای مقابله با حمله انتخاب بدترین والد به مقایسه CPC-RPL با راه‌حل‌های ارائه شده در مقابل حمله کاهش مقدار Rank خواهیم پرداخت. تا به امروز ۴ راه‌حل ادعای مقابله با حمله کاهش مقدار Rank را کرده‌اند. لیست زیر این روش‌ها را نشان می دهد.

۱. روش بررسی مقدار Rank
۲. روش SVELTE
۳. روش VERA
۴. روش TRAIN

از ۴ مورد لیست بالا روش‌های ۳ و ۴ هنوز به طور مناسب پیاده‌سازی نشده و صرفا به ارائه راه‌حل پرداخته شده است (روش ۴ بهبود یافته‌ی روش ۳ است). بنابراین در این پژوهش نیز از پیاده‌سازی و مقایسه آنها با روش پیشنهادی صرف نظر شده است. بر اساس محاسبات و مراحل موجود در این دو روش وجود سربار و مصرف انرژی بیشتر نسبت به روش پیشنهادی در VERA و TRAIN پیش‌بینی می‌گردد. در ادامه CPC-RPL با روش‌های SVELTE و بررسی مقدار Rank از دید مصرف انرژی و فضای حافظه مقایسه شده است. برای این کار از توپولوژی و پارامترهای شبیه‌سازی یکسان در سیستم‌عامل Contiki استفاده شده است.

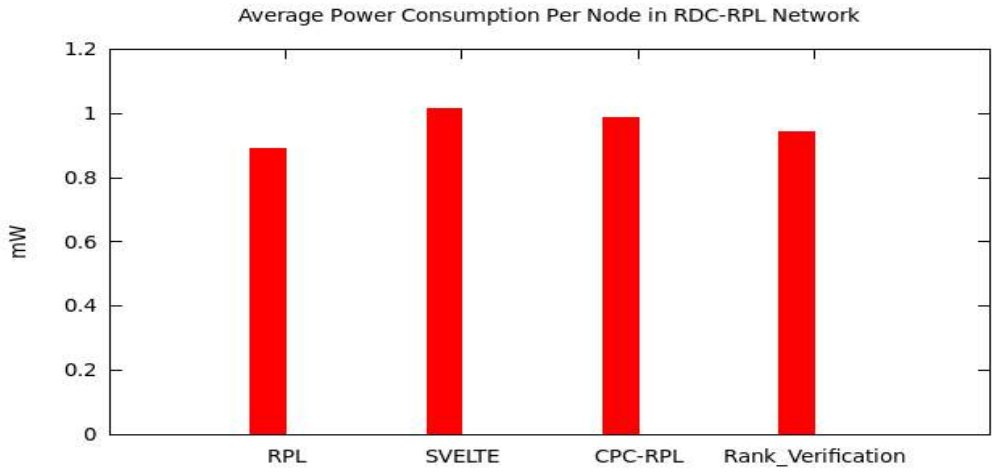
شکل ۴-۳۵ مصرف انرژی در گره‌های کلاینت را برای سه روش نامبرده و پروتکل RPL معمولی نشان می‌دهد. همانطور که در شکل نشان داده شده است مصرف انرژی در هر یک از راه‌حل‌های پیشنهادی نسبت به حالت عادی پروتکل RPL افزایش یافته است. با توجه به اینکه در روش بررسی مقدار Rank امکان گم شدن بسته‌های کنترلی در نظر نگرفته نشده و همچنین هر دو رقیب CPC-RPL با نگرانی‌های کمتری در پروتکل RPL مقابله می‌نمایند می‌توان مصرف انرژی در روش پیشنهادی را نسبت به رقبای خود مناسب‌تر دانست. بدیهی است که با افزایش گره‌ها در درخت DODAG اختلاف مصرف انرژی در روش‌های مذکور افزایش خواهند یافت.



شکل ٤-٣٥ : مقایسه روش پیشنهادی با کارهای پیشین بر اساس مقدار انرژی مصرفی در تمام گره‌های کلاینت در درخت DODAG

شکل شماره ۴-۳۶ متوسط مصرف توان در هر سنسور کلاینت را برای سه روش مذکور به همراه پروتکل RPL نشان می‌دهد. با توجه به برقراری رابطه مستقیم بین مصرف انرژی و توان موارد مطرح شده در رابطه با نمودار ۴-۳۵ برای نمودار ۴-۳۶ نیز صادق است.

$$Power\ (mW) = \frac{Energy\ (mJ)}{Time(s)} \qquad [۳-۴]$$

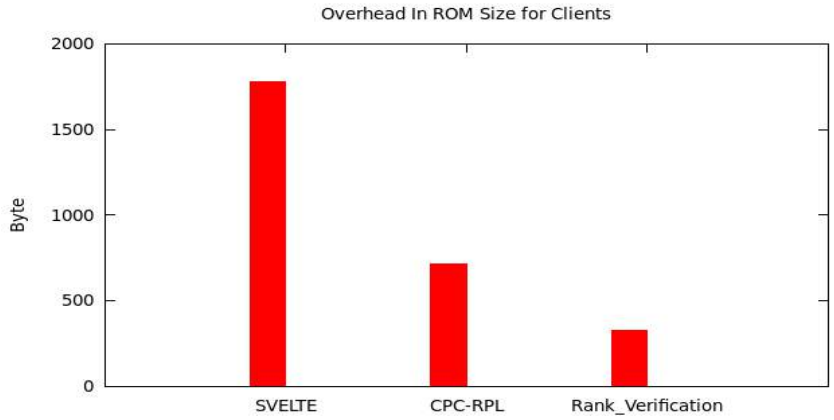


شکل ٤-٣٦ : مقایسه روش پیشنهادی با کارهای پیشین بر اساس متوسط توان مصرفی در گره‌های کلاینت

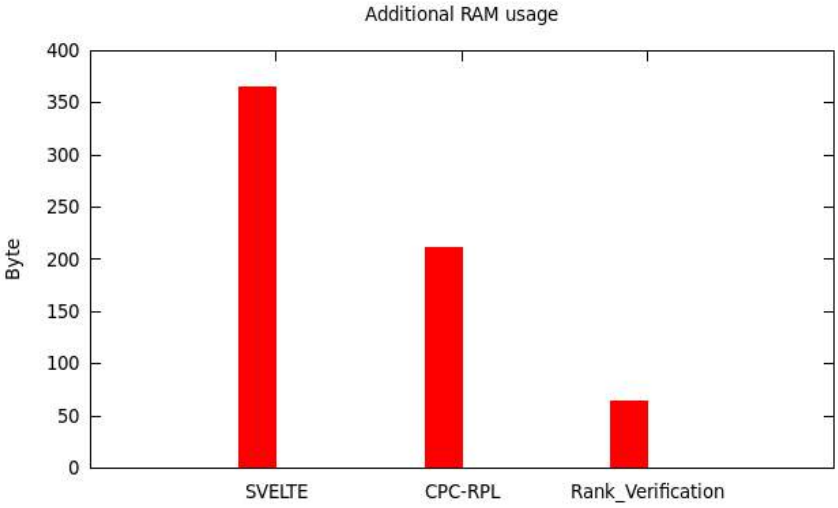
شکل شماره ۴-۳۷ سرباری که با افزودن هر یک از سه روش مذکور به پروتکل RPL عادی اضافه می‌گردد. را نشان می‌دهد. با توجه به شکل سربار CPC-RPL بر رام موجود در سنسورهای کلاینت در درخت DODAG از

روش SVELTE کمتر و از روش بررسی مقدار Rank بیشتر است. این امر همچنین در شکل شماره ۴-۳۸ نیز برای مقدار فضای مورد نیاز جهت اجرای روش‌های مذکور صادق است. بنابراین روش پیشنهادی از SVELTE در شبکه‌های به نسبت بزرگتر و در مقابل روش بررسی مقدار Rank در شبکه‌های کوچکتر قابل اجراست.

در حالت کلی با توجه به اینکه روش پیشنهادی با نگرانی‌های بیشتری نسبت به دو روش دیگر مقابله نموده و همچنین رقبای CPC-RPL به ویژه روش بررسی مقدار Rank دارای نقاط ضعف مهمی هستند. می‌توان عملکرد CPC-RPL را در مصرف فضای حافظه نیز مناسب توصیف نمود.



شکل ٤-۳۷ : مقایسه روش پیشنهادی با کارهای پیشین بر اساس سربار در فضای ROM



شکل ٤-۳۸ : مقایسه روش پیشنهادی با کارهای پیشین بر اساس افزایش مصرف RAM

در نهایت جدول زیر تمام موارد موجود در کارهای پیشین و روش پیشنهادی را در یک نگاه نمایش می‌دهد.

جدول ٤-٣:کارهای پیشین و روش پیشنهادی در یک نگاه

نام پژوهش	دسته مربوطه	مقابله با حملات	پیاده سازی	ضعف
روش مدیریت گروه بر اساس اعتماد [۵۱]	اعتماد	حملات Black hole	Sensi	Cluster Headها در گروه داخلی برای ارتباط با گره Sink نیاز به مصرف انرژی زیادی دارند که باعث مصرف باتری سنسور Cluster Head می گردد
روش SVELTE [۴۸]	سیستم تشخیص نفوذ	حمله کاهش مقدار Rank	Cooja	هنوز فقط تست و پیاده سازی شده است،دارای سربار محاسباتی می‌باشد.امکان ارسال هشدارهای اشتباه همچنان وجود دارد.
روش TRAIN [۳۶]	احراز هویت	حمله شماره ورژن و حمله کاهش مقدار Rank	پلتفرمRIOT	سربار بالا، مشکل در مقیاس‌پذیری،گم شدن بسته‌های کنترلی در روش موثر است
روش بررس Rank [۳۵]	احراز هویت	حمله Sinkhole و حمله کاهش مقدار Rank	نا مشخص	سربار بالا و ایجاد حملات جدید، مشکل در مقیاس-پذیری، گم شدن بسته‌های کنترلی در روش موثر است
مسیریابی چندگامی ایمن برای اینترنت اشیا [۲]	احراز هویت	حملات sinkhole ،Grayhole,blackhole و حملات جعل هویت	Physical Testbed	سربار بالا، مشکل در مقیاس‌پذیری
روش TSRF [۸]	اعتماد	حملاتOn-off ،conflicting حملات behavior, حملات selfish ،badmouthing و حملاتcollusion	Ns2	مصرف حافظه، سربار محاسباتی،مشکل وجود حافظه تاریخی در محاسبه اعتماد که میتواند حملات جدیدی را به وجود آورد
روش اعتماد بر اساس تصدیق دو گامی [۴]	اعتماد	حملاتselfish ،جعل هویت Blackhole , و حملات behavior	Ns2	عدم تشخیص حمله چاله خاکستری، و در محاسبه اعتماد حالت شبکه نقشی ندارد زیرا از گره های همسایه بازخوردی نمی‌گیرد.
کاهش ناسازگاری‌های توپولوژی در RPL[۲۰]	تغییر در پروتکل مسیریابی RPL	حمله ناسازکاری در Dodag	Cooja Contiki	امکان حمله همچنان وجود دارد
جلوگیری از حمله Wormhole با استفاده از درخت مرکل [۱۴]	احراز هویت	حمله Wormhole	Unknown	سربار ارتباطی و پردازشی به همراه دارد
روش Lithe [۱۹]	تطبیق مکانیسم های امنیتی در سایر لایه ها جهت محدود کردن حملات لایه ی شبکه	حمله Fragmentation	Cooja Contiki	با وجود فشرده سازی همچنان سربار پردازشی و رمزنگاری وجود دارد و همچنان در مقابل حملات نظیر و غیره آسیب پذیر می Blackhole , Sinkhole باشد
روش Vera [۳۴]	احراز هویت	حمله کاهش مقدار Rank و حمله Sinkhole	None	آسیب‌پذیری در برابر حملات تکرار، ایجاد حملات جدید، عدم پیاده‌سازی و آنالیز و گم شدن بسته‌های کنترلی در روش موثر است
روش Parent Fail Over [۳۵]	تغییر در پروتکل مسیریابی	حمله Sinkhole	Unknown	این روش در برابر حملات SYBIL و جعل هویت آسیب پذیر بوده و همچنین انتخاب آستانه ناصحیح می‌تواند عملکرد این روش را با مشکل روبرو و رفتار صحیح پروتکل حمله تلقی گردد.
روش CPC-RPL	تغییر در پروتکل مسیریابی و مبتنی بر سیستم تشخیص نفوذ	حمله انتخاب بدترین والد، حمله کاهش مقدار Rank، حمله افزایش مقدار Rank، جعل جداول مسیریابی، حملات Blackhole، Sikhole و Wormhole در برخی حالات	COOJA	امکان ایجاد حملات جدید را فراهم می‌سازد،امکان حمله در شرایط خاص وجود دارد (شرایط خاص در شبکه)

٤-۱۲. نتیجه‌گیری فصل

در این فصل پس بررسی و مقایسه شبیه‌سازهای مختلف برای ارزیابی روش پیشنهادی، سیستم عامل Contiki و در نتیجه شبیه‌ساز Cooja جهت این امر انتخاب گردید. پس از پیاده‌سازی حمله انتخاب بدترین والد در این سیستم‌عامل روش پیشنهادی نیز پیاده و در سه معیار زیر مورد ارزیابی قرار گرفت.

۱-معیارهای مربوط به انرژی : متوسط توان لحظه‌ای و توان آنی به تفکیک میزان مصرف پردازنده، گوش دادن و ارسال رادیویی، متوسط سیکل دوره‌ای رادیویی

۲-معیارهای مربوط به کارایی : تعداد بسته‌های دریافت شده، تعداد گام‌های هر گره تا ریشه در درخت، سربار پردازشی و رادیویی حاصل از روش پیشنهادی

۳-معیارهای مربوط به تشخیص حمله : تعداد تشخیص‌های موفق با افزایش گره‌های مخرب

فصل پنجم

نتیجه گیری، خلاصه و پیشنهادات

۵-۱. نتیجه‌گیری و پیشنهادها

در این پژوهش ضمن ارائه یک مکانیسم امنیتی برای پروتکل مسیریابی RPL در اینترنت اشیا به پیاده‌سازی و آنالیز آن نیز در سیستم‌عامل Contiki پرداختیم.

تحلیل نتایج حاصله موارد زیر را نشان می‌دهد.

- سربار روش پیشنهادی بسیار پایین است.
- روش پیشنهادی منابع انرژی دستگاه‌های اینترنت اشیاء را تحت تاثیر قرار نمی‌دهد.
- افزودن این مکانیسم به پروتکل RPL بسیار ساده می‌باشد.
- این روش علاوه بر مقابله با حملات انتخاب بدترین والد به طور بهینه و کارآمد در مقابل حملات کاهش مقدار Rank، افزایش مقدار Rank و ایجاد مسیرهای جعلی در جداول مسیریابی گره هدف نیز می‌تواند مفید باشد.

در این پژوهش کارآمدی روش پیشنهادی از دو دید زیر [۴۷] مورد بررسی قرار گرفته است.

۱. دید سخت‌افزاری : سربار پردازشی و توان مصرفی پایین (نمودارهای ۴-۱۴ الی ۴-۱۷)

۲. دید نرم‌افزاری : عملکرد صحیح، مقیاس‌پذیری (نمودارهای ۴-۱۸ الی ۴-۱۹ و قسمت ۴-۱۰)

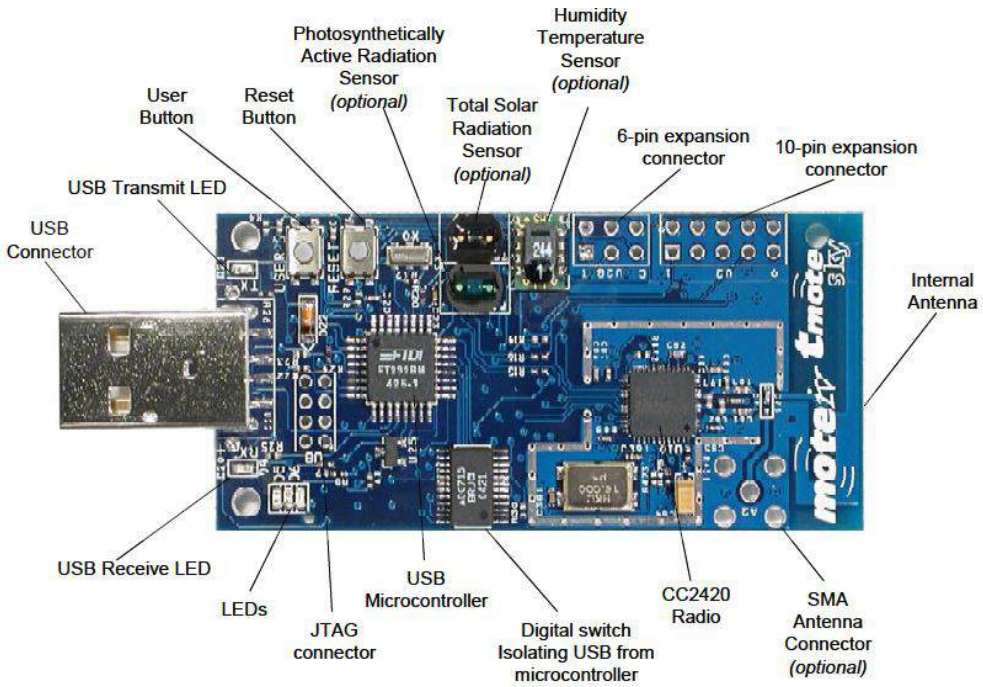
بر این اساس و با توجه به نمودارها و اشکال فصل چهارم، روش پیشنهادی مکانیسمی کارآمد برای بهبود پروتکل RPL در برابر نگرانی‌های امنیتی معرفی شده می‌باشد.

۵-۲. کارهای آتی

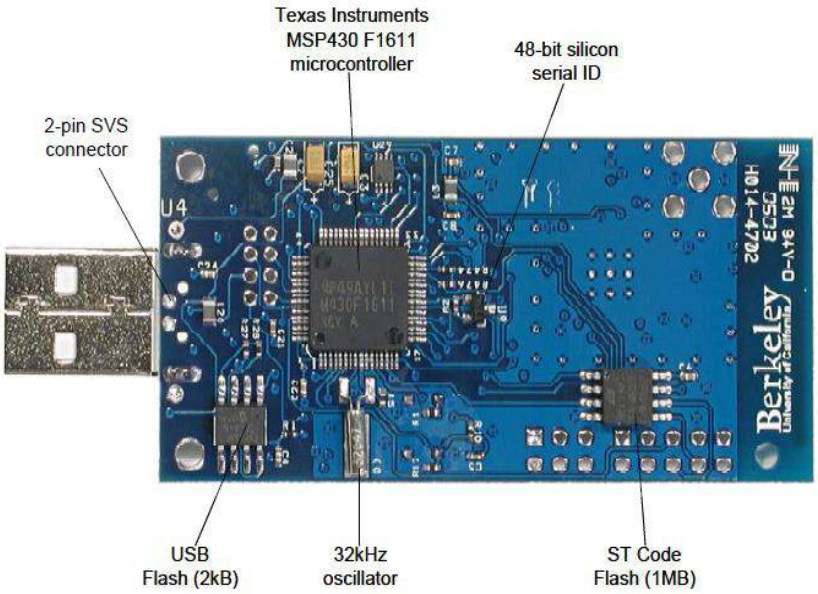
در آینده این پژوهش به موارد ذیل پراخته خواهد شد:

- بررسی حملات جدیدی که می‌تواند در اثر افزودن روش پیشنهادی به پروتکل RPL به وجود آیند
- بررسی انواع شرایط محیط واقعی در اینترنت اشیاء
- پیاده‌سازی روش پیشنهادی در بستر واقعی
- ایجاد امکان پیاده‌سازی Object Base در اینترنت اشیاء و تولید گزارش‌های کاربردی خودکار
- ایجاد ابزار تحلیل Formal برای اثبات ادعاها در اینترنت اشیاء

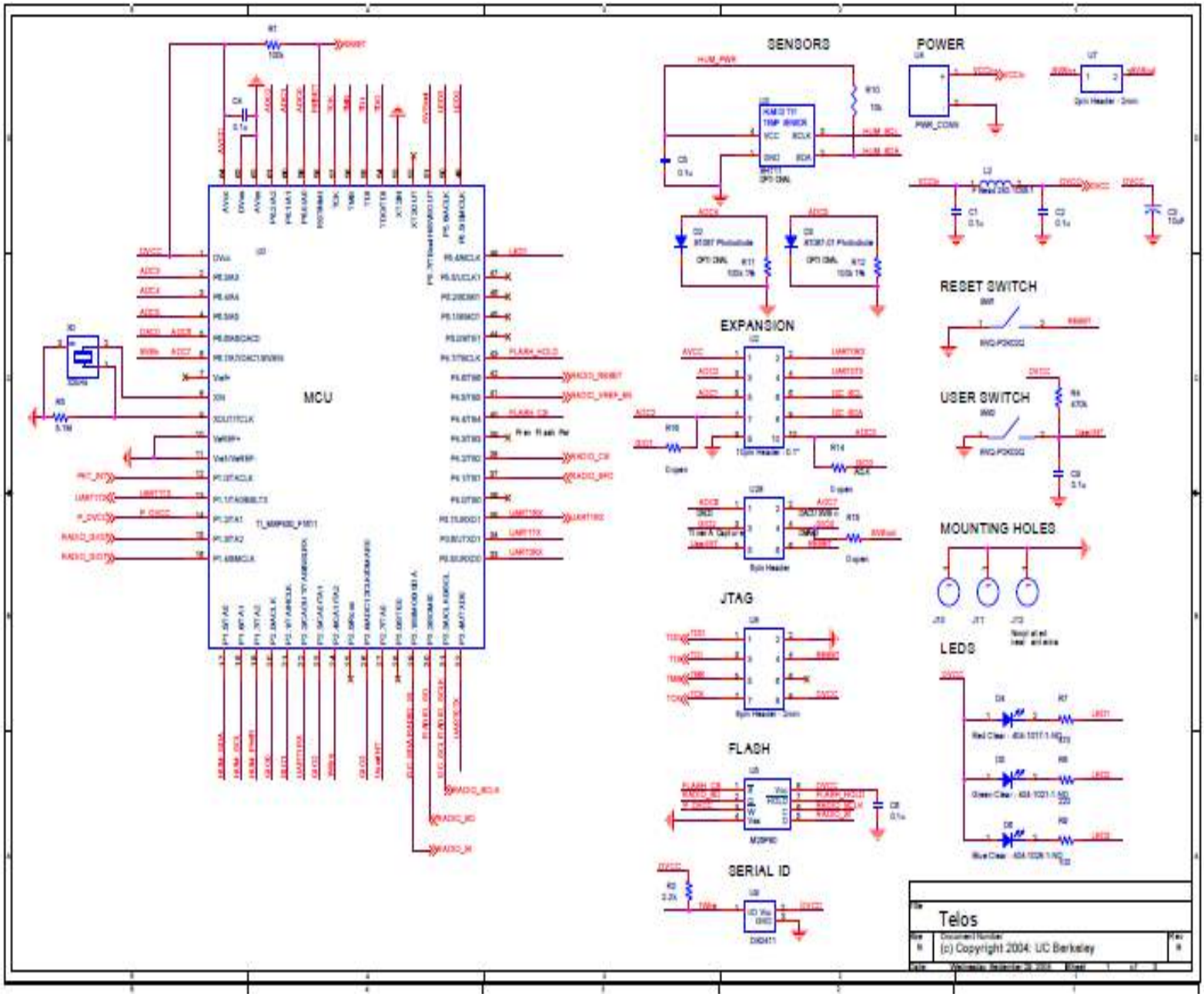
ضمائم



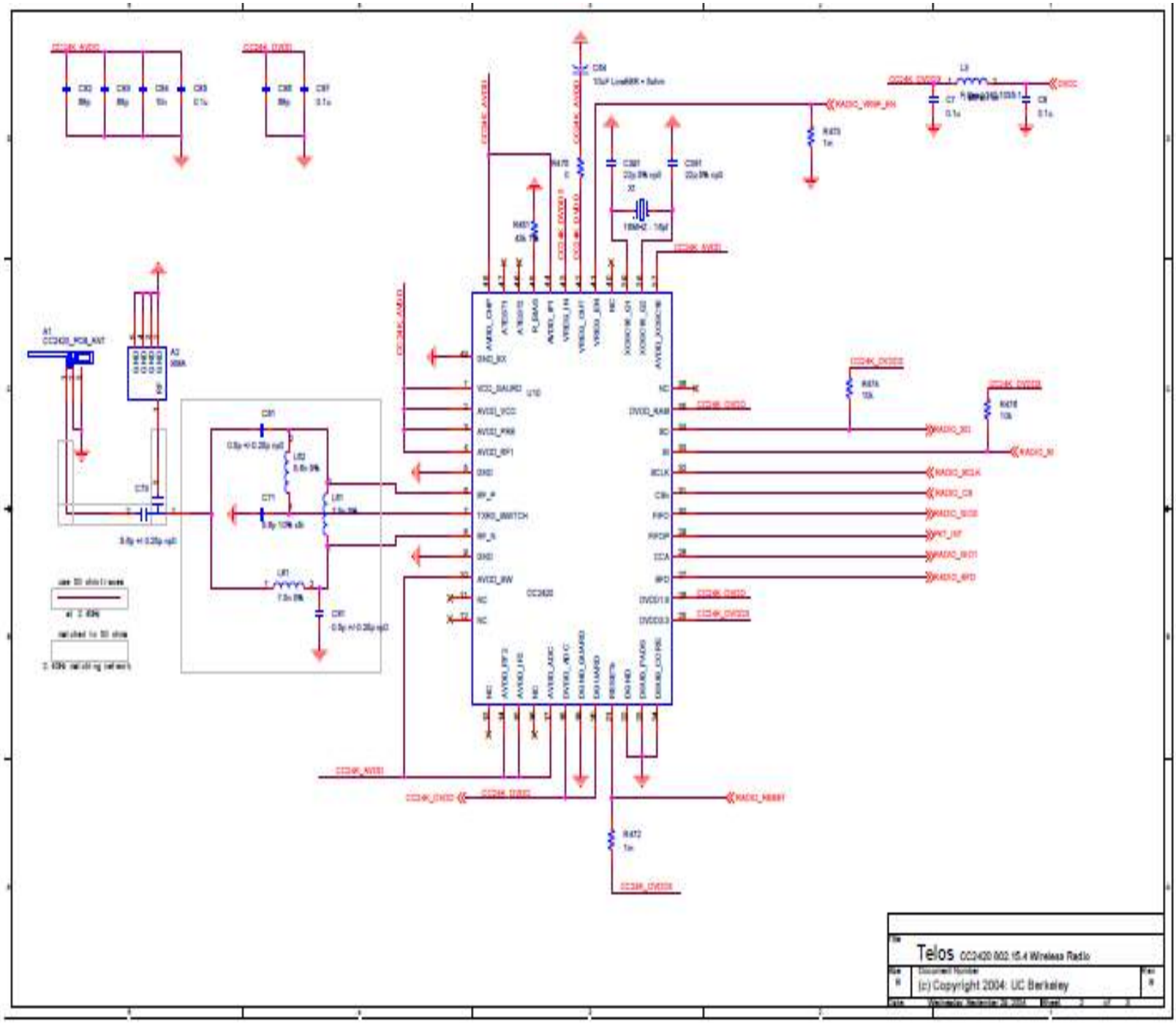
نمای جلو از ماژول Tmote Sky



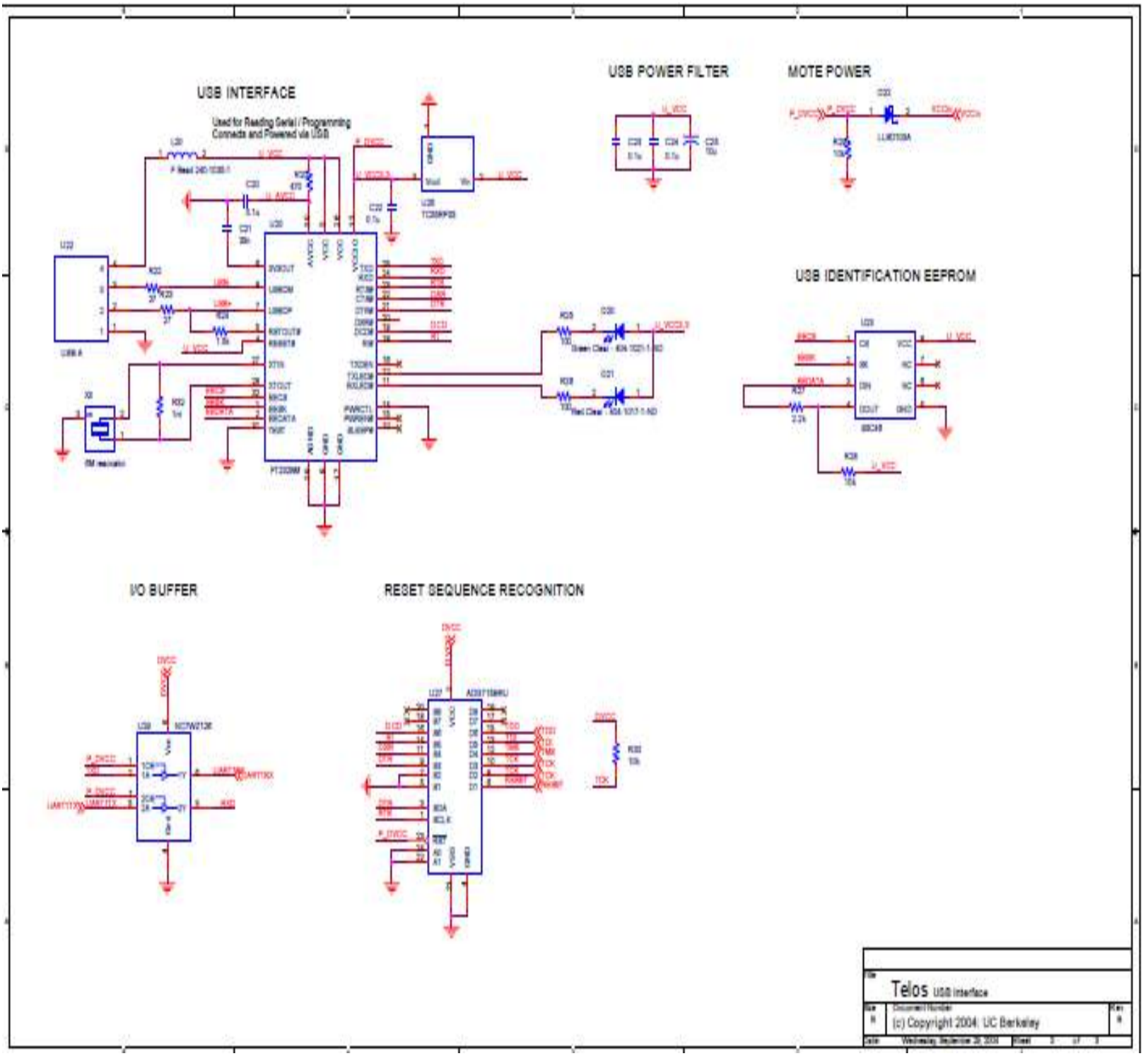
نمای پشت از ماژول Tmote Sky



Data Sheet مربوط به ماژول Tmote Sky (A)



(B) Tmote Sky مربوط به ماژول Data Sheet



Data Sheet مربوط به ماژول Tmote Sky (C)

Abstract

Internet of Things is a technology that enables objects to connect to the Internet by a combination of low-power microcontrollers and communication technologies. The introduction of many applications to date has made predictions of a future blended with this technology for humanity. One of the obstacles to the spread of the use of a technology is its lack of information security. On the Internet of Things, scientists consider information security to be very important, because vulnerabilities in this technology can go beyond the cyber space and sometimes cause irrecoverable effects on the real environment (such as power outage in a city). One of the major concerns of information security on the Internet of Things is the security of the network layer, a layer of the protocol stack that scientists have designed the emerging RPL routing protocol due to the special features on the Internet of Things. Among these special features, processing power, storage, and low-energy source in the devices of Internet of Things can be mentioned in addition to the existence of a specific traffic model in this technology. With the introduction of this protocol, researchers have shown vulnerability of RPL in some cases after security investigations, while providing some attacks. In this research, after the necessary investigations, we found that the reason for the formation of a considerable part of these attacks is the lack of father's supervision over the behavior of the children. Then we have provided a mechanism for detecting these attacks and tree retrieval. We implemented and analyzed the proposed method in the Contiki operating system. In this assessment , the impact of the proposed method on network resource consumption , accuracy and performance has been described . The success of the proposed method in these factors shows its efficacy

فهرست منابع و مآخذ مورد استفاده

[1] Airehrour, D. Gutierrez, J. and Kumar Ray, S. 2016. Secure routing for internet of things: A survey. Journal of Network and Computer Application: 14.

[2] Granjial, J. Monteiro, E. and Silva, J. 2015. Security for the Internet of Things: A survey of Existing Protocols and Open Research issues. IEEE Communications Surveys & Tutorials , Volume: 17, Issue: 3

[3] Jing, Q., Vasilakos A.V., Wan, J.,Lu, J. and Qiu, D. 2014. Security of Internet of Things: Prespectives and challenges. Wireless Networks , Volume 20, Issue 8, pp 2481–2501

[4] IOT Website (https://iotanalytics.com)

[5] Wikipidia (https://en.wikipedia.org/wiki/6LoWPAN)

[6] Contiki Os Tutotials (http://anrg.usc.edu/contiki/index.php/Contiki_tutorials)

[7] Iova, O., Picco, P. ,Istomin, T. and Kiraly, C. 2016 .RPL, the Routing Standard for the Internet of Things Or Is It?. IEEE COMMUNICATIONS MAGAZINE: 7.

[8] Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, J. and Alexander, R. 2012. RPL: IPv6 routing protocol for low-power and lossy networks, RFC 6550, IETF

[9] Levis, P., Clausen, T., Hui, J., Gnawali, O. and Ko, J. 2011.The Trickle Algorithm, RFC 6206 (Proposed Standard), Internet Engineering Task Force, Mar.

[10] Mayzaud, A. Biddonel, R. and Chrisment, I. 2016. A Taxonomy of Attacks in RPL-based Internet of Things .International Journal of Network Security, IJNS

[11] Wallgren, L., Reza, S. and Voigt, R. 2013. Routing Attacks and Countermeasures in the RPL-Based Internet of Things. International Journal of Distributed Sensor Networks: 12

[12] Idris Khan, F. Shon, T. and Lee, T. 2013. Wormhole Attack Prevention Mechanism for RPL Based LLN Network, Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on

[13] Mayzaud, A., Badonnel, R. and Chrisment, I . 2013. Monitoringand security for the internet of things.Emerging Management Mechanisms for the Future Internet, LNCS 7943, pp. 37- 40, Springer

[14] Mayzaud, A., Sheghal, A., Badonnel, A. and Chrisment, I. 2015. Mitigation of Topological Inconsistency Attacks In RPL besed Low Power Lossy Networks.International Journal of Network Management, Volume 25, Issue 5

[15] Rehman, A., Khan, M.M., Lodhi, M.A. and Hussain, B.H. 2016. Rank Attack using Objective Function in RPL for Low Power and Lossy Networks, Industrial Informatics and Computer Systems (CIICS), 2016 International Conference on

[16] Matsunaga, T., Toyoda, K. and Sasase, I. 2014. Low false alarm Attackers detection in RPL by considering timing inconsistency between the rank measurement.IEICE Communication Express, Vol 4 , No 11 ,340-345

[17] Duan, J. Yong, D. and Zhu, h. 2014. TSRF: A Trust Aware Secure Routing Framework in Wireless Sensor Network. Intenational Journal of Distributed Sensor Network: 15.

[18] Djedjig, N., Tandjaoui, D., Medjek, F and Romdhani, I. 2017. New Trust Metric for the RPL Routing Protocol. 2017 8th International Conference on Information and Communication Systems (ICICS)

[19] Anita, X., Manickam, M.L. and Bhagyaveni, M.A. 2014. Two-Way Acknowledgment-Based Trust Framework forWireless Sensor Networks. International Journal of Distributed Sensor Networks: 15.
[20] Djedjig, N.,Tandjaoui, D. and Medjek, F. 2015. Trust-based RPL for the Internet of Things .20th IEEE Symposium on Computers and Communication (ISCC)
[21] Le, A., Lee, J., Lasebade, A., Vinel, A., Chen, Y and Chai. 2013. The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks. IEEE Sensors Journal
[22] Dvir, A. Holczer T. and Buttyan, L. 2011. VeRA - Version Number and Rank Authentication in RPL. Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on
[23] Landsmann, M.,Wahlisch, M. and Schmidt, T. 2014. Topology Authentication in RPL.Computer Communications Workshops (INFOCOM WKSHPS), 2013 IEEE Conference on
[24] Weekly, K. and Pister P. 2012. Evaluating sinkhole defense techniques in RPL networks.Network Protocols (ICNP), 20th IEEE International Conference on
[25] Reza, S., Wallgren, L. and Voigt, T. 2013. SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Networks Volume 11, Issue 8, November 2013, Pages 2661-267
[26] Reza, S, Hossein, S., Kasun, H. and Hummen, R. 2016. Lithe: Lithweight secure Coap for The Internet of Things.Design Automation Conference (DAC), 2016 53nd ACM/EDAC/IEEE
[27] Ruen Chze, P.L., Leong, K.S. 2014. A Secure Multi-Hop Routing for IoT Communication. IEEE SENSORS JOURNAL, 5.
[28] Gaona Garcia, P., Montenegro-Marin, C., Prieto, J.D. and Nieto, Y.V. 2016). Analysis of Security Mechanisms Based on Clusters IoT Environments. Advances and Applications in the Internet of Things and Cloud Computing: 6.
[29] John, C. and Wahi, W. 2016. Security Analysis of Routing Protocols for Wireless Sensor Networks. International Journal of Applied Engineering Research: 8.
[30] Vinayagamoorthy, M. and Ramesh, R. 2016. Secure and Energy Efficient Transmission for Cluster-Based Wireless Adhoc Networks. International Journal of Basic Science and Engineering: 5.
[31] Mathur, A., Newe, T. and Rao, M. 2016. Defence against Black Hole and Selective Forwarding Attacks for Medical WSNs in the IoT. Sensors: 25.
[32] Ahmed, A., AbuBakar, K., Channa, MI and Waheed Khan, A. 2016. A Secure Routing Protocol with Trust and Energy Awareness for Wireless Sensor Network. Mobile Networks and Applications April 2016, Volume 21, Issue 2
[33] Diaz, A. and Sanchez, P. 2016. Simulation of Attacks for Security in Wireless Sensor Network, Sensors (Basel).18
[34] Brasser, F., Rasmussen, K.B., Sadeghi A.R. and Tsudik, G. 2016. Remote Attestaition for Low-End Embedded Devices: The Provers PersPective. Design Automation Conference (DAC), 2016 53nd ACM/EDAC/IEEE
[35] R Renofio, R.R., Pellenz, M.E., Jamhour, E., Santin, A., Penna, M.C. and Souza, R.D. 2016. On the Dynamics of the RPL Protocol in AMI Networks under Jamming Attacks. Communications (ICC), 2016 IEEE International Conference on

[36] Seeber, S., Sehgal, A., Stelte, B., Rodosek, G.D. and Schonwalder, J. 2013. Towards A Trust Computing Architecture for RPL in Cyber Physical Systems. Network and Service Management (CNSM), 2013 9th International Conference on
[37] Hidden, R. and Deering, S . 2003. Internet Protocol Version 6 (IPv6) Addressing Architecture. RFC 2373,Network Working Group
[38] Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A. and Richardson, M. 2015. A Security Threat Analysis for Routing Protocol for Low-power and Lossy Networks (RPLs), RFC 7416, Internet Engineering Task Force.
[39] Romdhani, I., Qasem, M., Al-Dubai, A.Y. and Ghaleb, B. 2016. Cooja Simulator Manula. Edinburgh Napier University
[40] Dunkels, A., Gronvall, B and Voigt T. 2004. Contiki - a lightweight and flexible operating system for tiny networked sensors. Local Computer Networks, 2004. 29th Annual IEEE International Conference on
[41] Tripathi, J. Oliveira, J.C. and Vasseur, J.P. 2010. A performance evaluation study of RPL: Routing Protocol for Low power and Lossy Networks. Information Sciences and Systems (CISS), 2010 44th Annual Conference on
[42] Karkazis, P. Trakadas, P. Zahariadis, TH. Hatziefremidis, A. and Leligou, H.C. 2012. RPL modeling in JSim platform. Networked Sensing Systems (INSS), 2012 Ninth International Conference on
[43] Contiki Os Website (http://www.contiki-os.org)
[44] luchi, K., Matsunaga, T., Toyoda, K. and Sasase, L. 2015. Secure parent node selection scheme in route construction to exclude attacking nodes from rpl network. IEICE Communication Express, Vol.4, No 11, 340-345
[45] Nassiri, M, Boujari, M and Azhari, S.V. 2015. Energy-aware and load-balanced parent selection in RPL routing for wireless sensor networks. International Journal of Wireless and Mobile Computing 9(3):231-239
[46] Buettner, M., Yee, G.V., Anderson, E. and Han, R. 2006 . X-MAC: A short preamble MAC protocol for duty-cycled wireless sensor networks. Conference: Proceedings of the 4th International Conference on Embedded Networked Sensor Systems, SenSys 2006, Boulder, Colorado, USA, October 31 - November 3
[47] Pradeska, N., Widyawan., Najib, W. and Kusumawardani, S.S. 2016. Performance Analysis of Objective Function MRHOF and OF0 in Routing Protocol RPL IPV6 Over Low Power Wireless Personal Area Networks (6LoWPAN). Information Technology and Electrical Engineering (ICITEE).
[48] Accettura, L, Grieco, L.A., Boggia, G. and Camarda, P. 2011. Performance Analysis of the RPL Routing Protocol. Mechatronics (ICM), 2011 IEEE International Conference
[49] Zeiss, B., Vega, D., Schieferdecker, I., Neukirchen, H. and Grabowski, J. 2007.Applying the ISO 9126 Quality Model to Test Specifications Exemplified for TTCN-3 Test Specifications. Software Engineering Conference
[50] Chugh, K., Aboubaker, L. and Loo, J. 2012.Case study of a black hole attack on 6lowpan-RPL," in Proceedings of the SECURWARE Conference, pp. 157
[51] Hui, J and Vasseur, J. 2012. The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams, RFC 6553 (ProposedStandard), Internet Engineering Task Force

[52] Krentz, K..F., Rafiee, H. and Meinel, C. 2013. 6LoWPAN security: adding compromise resilience to the 802.15.4 security sublayer Zurich, Switzerland. Present Proc Int Workshop Adapt Secur

Bu-Ali Sina University

Graduate Studies Thesis\Dissertation Information

Title: An Efficient Trust-Based Routing Mechanism For Internet Of Things Based On RPL Protocol

Author: Mohamad Pishdar

Supervisor(s): Dr Younes Seifi

Advisor(s): Dr Mohammad Nassiri

Faculty: Engineering

Department: Computer

Subject: Information Technology	**Field: Computer Networks**	**Degree: Master**
Approval Date: 2016/11/5	**Defence Date: 2017/11/26**	**Number of Pages:126**

Abstract:

Internet of Things is a technology that enables objects to connect to the Internet by a combination of low-power microcontrollers and communication technologies. The introduction of many applications to date has made predictions of a future blended with this technology for humanity. One of the obstacles to the spread of the use of a technology is its lack of information security. On the Internet of Things, scientists consider information security to be very important, because vulnerabilities in this technology can go beyond the cyber space and sometimes cause irrecoverable effects on the real environment (such as power outage in a city). One of the major concerns of information security on the Internet of Things is the security of the network layer. The layer of the protocol stack that scientists, due to the special features on the Internet of Things, have designed an emerging routing protocol called RPL. Among these special features, processing power, storage, and low-energy source in the devices of Internet of Things can be mentioned in addition to the existence of a specific traffic model in this technology. With the introduction of this protocol, researchers have shown vulnerability of RPL in some cases after security investigations, while providing some attacks. In this research, after the necessary investigations, we found that the reason for the formation of a considerable part of these attacks is the lack of father's supervision over the behavior of the children. Then we proposed a mechanism for detecting these attacks and retrieving the tree, and also implemented and analyzed the proposed method in the Contiki operating system. In this assessment , the impact of the proposed method on network resource consumption , accuracy and performance has been described . The success of the proposed method in these factors shows its efficacy

Key Words: Internet of Things, RPL, Security In RPL, Security In IOT, Contiki