دومین کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات
Homepage: http://i4c.iust.ac.ir

تشخیص حمله کاهش مقدار RANK در پروتکل مسیریابی RPL و بازیابی شبکه

محمد پیشدار[۱] ، یونس سیفی[۲]، محمد نصیری[۲]

۱- دانشجوی کارشناسی ارشد فناوری اطلاعات – دانشگاه بوعلی‌سینا

۲- استادیار گروه کامپیوتر دانشگاه بوعلی سینا

چکیده

تکنولوژی اینترنت اشیاء [۱]در سال۱۹۹۹میلادی با هدف اتصال اشیاء به شبکه‌های ارتباطی معرفی شد. ظهور ایده‌های کاربردی فراوان خیلی زود نوید از آینده‌ای روشن برای این تکنولوژی می‌داد. یکی از اولین مشکلات بر سر راه تحقق این امر استفاده از دستگاه‌های با توان پردازشی، ذخیره‌سازی و منبع انرژی ضعیف و همچنین مدل ترافیکی خاص در اینترنت اشیاء بود. این امر موجب عدم سازگاری پروتکل‌های رایج مسیریابی در علم ارتباطات با این تکنولوژی بود. به همین خاطر پروتکل مسیریابی RPL [۲]در سال ۲۰۱۲ به منظور رفع نیازهای مسیریابی در ایده اینترنت اشیا ایجاد گشت. با افزایش به-کارگیری اینترنت اشیا و واگذاری بسیاری از کارها در زندگی روزمره به اشیا، آسیب‌پذیری‌ها می‌توانند از فضای مجازی خارج و بر جهان واقع تاثیر مخرب بگذارند. در برخی موارد این تاثیرات منفی حتی می‌تواند جبران ناپذیر نیز باشد نظیر قطع برق یک شهر. بنابراین با توجه به اهمیت بالای امنیت در اینترنت اشیاء پس از ایجاد پروتکل مسیریابی RPL پژوهشگران بسیاری شروع به بررسی آن از نظر امنیتی با توجه به شرایط خاص این تکنولوژی پرداختند. نتایج این پژوهش‌ها نشان‌دهنده آسیب‌پذیری این پروتکل در برابر حملات رایج شبکه و حتی وجود برخی حملات جدید مخصوص این پروتکل می‌باشد. در این پژوهش بر حسب نیاز به ارائه روشی جهت تشخیص حمله کاهش مقدار RANK از حملات مهم بر علیه پروتکل RPL و بازیابی شبکه پس از این حمله پرداخته شده است. در این پژوهش همچنین روش مربوطه را در سیستم-عامل Contiki پیاده‌سازی و آنالیز نموده‌ایم.

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

۱. مقدمه

۱. Internet Of Things
۲. Routing Protocol for Low Power and Lossy Networks

با معرفی ایده اینترنت اشیا در سال ۱۹۹۹ مهم‌ترین نگرانی بر سر راه گسترش این تکنولوژی عدم سازگاری روش‌ها و یا پروتکل‌های رایج ارتباطی با آن به نظر می‌رسید. مهم‌ترین دلیل این ناسازگاری‌ها وجود ویژگی‌های خاص در اینترنت اشیاء از جمله توان پردازشی، ذخیره‌سازی و منبع انرژی ضعیف در دستگاه‌های این تکنولوژی است.

دانشمندان برای حل این مشکل به فکر تطبیق پروتکل‌های رایج ارتباطی با اینترنت اشیاء و یا ارائه پروتکل‌های جدید خاص این تکنولوژی افتادند. در همین راستا در سال ۲۰۰۵ تکنولوژی ۸۰۲.۱۵.۴ که مخصوص لایه فیزیکی و انتقال داده در شبکه‌های کم‌توان با نرخ بالا در گم شدن بسته‌ها است طراحی شد. دانشمندان این تکنولوژی را برای لایه فیزیکی و انتقال داده پشته پروتکلی اینترنت اشیاء نیز مناسب دیدند. اما در لایه شبکه، ویژگی‌های خاص در دستگاه‌های اینترنت اشیاء و علاوه بر آن مدل ترافیکی خاص (معمولا از اشیا به سمت یک گره مشخص) دانشمندان را به سمت طراحی پروتکل‌های جدید و سازگار با این تکنولوژی حرکت داد. در همین راستا دانشمندان در سال ۲۰۱۲ پروتکل مسیریابی RPL را به عنوان گزینه سازگار با لایه شبکه در اینترنت اشیاء طراحی و ارائه نمودند. پس از ارائه پروتکل RPL و اهمیت امنیت در اینترنت اشیا، پژوهشگران بسیاری به بررسی امنیتی آن پرداخته و آسیب‌پذیری های متعدی نیز برای آن ارائه شده است. امروزه برخی از این نگرانی‌ها همچنان باقی مانده و راه‌حلی برای آن‌ها ارائه نشده است. در این پژوهش برآن شدیم که با ارائه یک روش کارآمد برخی از این نگرانی‌ها را از بین ببریم. در ادامه ابتدا به تشریح برخی مفاهیم مهم پرداخته سپس کارهای پیشین را مورد بررسی قرار داده و در نهایت روش پیشنهادی، آنالیز و نتیجه گیری را شرح می‌دهیم[3,7,10].

۲. مفاهیم مقدماتی

در این قسمت مفاهیم مهم در این پژوهش شرح داده خواهند شد.

۲–۱. پروتکل مسیریابی RPL

اینترنت اشیا تکنولوژی است که بر اساس ایده پیوند اشیا با یکدیگر از طریق شبکه‌های ارتباطی نظیر اینترنت ایجاد شده است. هدف از ایجاد این تکنولوژی سپردن برخی کارها به اشیا که انجام آن برای انسان سخت یا غیر ممکن است یا هدف بهبود کیفیت زندگی و مدیریت هرچه بهتر منابع می‌باشد.

برای به واقعیت پیوستن این تکنولوژی دانشمندان با توجه به استفاده از سنسورهای کوچک با توان پردازشی و منبع تامین انرژی محدود، ایجاد و یا سازگار نمودن پروتکل‌ها و تکنولوژی‌های موجود با اینترنت اشیا را نیاز دانستند. بر همین اساس و در قسمت مسیریابی به دلیل ویژگی‌های خاص این تکنولوژی نظیر جهت و نوع ترافیک، نرخ شکست بالا در ارسال‌ها، پروتکل جدیدی به نام RPL در سال ۲۰۱۲ ایجاد شد. با توجه به پیش‌بینی‌های استفاده فراگیر در آینده و همچنین پیشگیری از عدم مواجهه با کمبود فضای آدرس، اینترنت اشیا از همان اول بر اساس آدرس Ipv6 بنا نهاده شد.
در این پروتکل توپولوژی شبکه درختی بوده و برای ایجاد آن از پیام‌های کنترلی در قالب بسته‌های Icmpv6 ارسال می‌گردد. این پیام‌ها به دسته‌های زیر تقسیم می گردند[3,14]:

۱-پیام اطلاعات درخت[۱]: این پیام مطابق با پروتکل توسط ریشه‌ی درخت (در شکل ۲ گره شماره ۲) و به صورت همه پخشی[۲] در محدوده انتشار بیسیم این گره ارسال می‌گردد. پیام اطلاعات درخت شامل اطلاعات مورد نیاز برای پیکربندی و نگهداری از درخت است. سایر گره‌ها با دریافت این پیام ضمن پیوستن به درخت، گره ارسال‌کننده را به عنوان پدر خود

۱.Dodag Information Object
۲. Broadcast

در درخت انتخاب می‌نمایند. این گره‌ها نیز به طور مجدد پیام اطلاعات درخت را به صورت همه پخشی ارسال می‌نمایند. به این ترتیب پیام اطلاعات درخت به گره‌هایی که در محدوده ارسال بیسیم ریشه قرار ندارند نیز خواهد رسید. هر گره با دریافت پیام اطلاعات درخت از مسیرهای مختلف ضمن شناختن پدران خود بر اساس اطلاعات موجود در این پیام‌ها گره کم هزینه‌تر در ارسال تا ریشه را به عنوان پدر مورد اشاره[۱] انتخاب کرده و ترافیک خود را از طریق این گره به سمت ریشه منتقل می‌نماید[3,14]. در پروتکل RPL معیار Rank برای انتخاب پدر مورد اشاره استفاده می‌گردد. این معیار دارای رابطه مستقیم با جایگاه گره در درخت است. به این معنی که هرچه مقدار Rank مربوط به یک گره بالاتر باشد فاصله‌ی آن از ریشه نیز بیشتر می‌باشد.

۲-پیام تبلیغ مقصد[۲]: این پیام برای انتشار وجود یک مسیر رو به پایین (به سمت برگ‌ها) در جهت بالای درخت استفاده می‌گردد به این معنی که گره‌ها اطلاعات مسیریابی خود را به پدر مورد اشاره خود منتقل می‌کند.

در پروتکل RPL دو مد کاری وجود دارد.

۱- ذخیره‌سازی اطلاعات در گره‌ها و به صورت توزیع شده صورت می‌گیرد. در این حالت هر گره مسئول عمل مسیریابی است. در صورت عدم وجود مسیر پیام مربوطه جهت مسیریابی به پدر مورد اشاره منتقل می‌گردد. معمولا این مد به صورت پیش‌فرض استفاده می‌گردد.

۲- ذخیره سازی اطلاعات به صورت متمرکز و تنها در ریشه است. در این حالت تمام پیام‌ها برای مسیریابی به ریشه ارسال می‌شوند.

۳-پیام درخواست اطلاعات درخت: وقتی یک گره خواهان پیوستن به یک درخت می‌باشد این پیام را به همسایگان خود ارسال و تقاضای پیام اطلاعات درخت را می نماید.

با توجه به اهمیت امنیت اطلاعات در اینترنت اشیا پژوهشگران پس از انتشار این پروتکل آسیب‌پذیری‌های نسبتا زیادی بر علیه آن پیدا نمودند که این آسیب‌پذیری ها را می توان به صورت زیر دسته بندی نمود[۱] .

۱. حمله به منابع شبکه : هدر دادن آنها به طوری که گره ها از انجام عملیات عادی خود باز بمانند.
۲. حمله به توپولوژی: در این حملات توپولوژی شبکه به گونه ای که باعث کاهش کارایی شبکه و یا در عملکرد پروتکل تاثیر منفی بگذارد تغییر می کند .
۳. حملات بر علیه ترافیک : در این حملات مهاجم[۳] سعی بر بهره‌گیری از ترافیک می کند به صورتیکه یا به دنبال به دست‌آوری اطلاعات از ترافیک می باشد و یا سعی بر جعل ترافیک می کند.

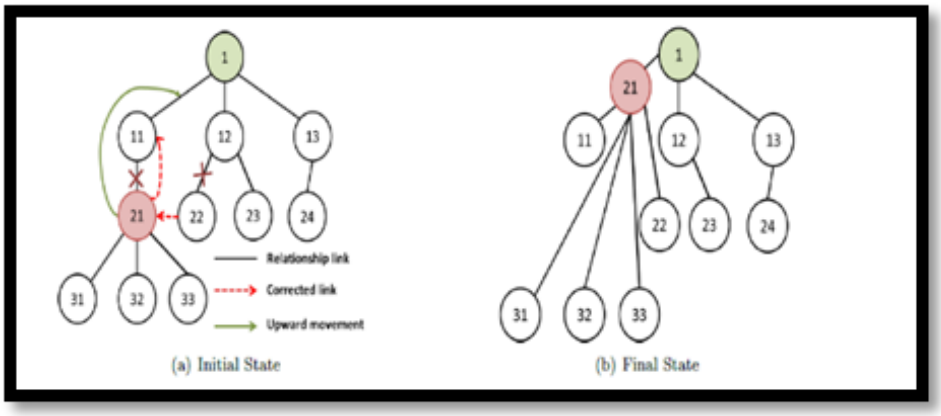
در ادامه این پژوهش ابتدا مفاهیم مهم در درک ادامه مقاله توضیح داده شده است سپس کارهای پیشین ،توضیح روش پیشنهادی ، پیاده‌سازی ، ارزیابی و در نهایت نتیجه‌گیری آورده شده است.

۲-۲. حمله کاهش Rank

یکی از مهم ترین حملات بر ضد پروتکل RPL حمله کاهش مقدار Rank است. این حمله مخصوص پروتکل RPL بوده و تا به امروز راه‌حل‌های معدودی برای مقابله با آن ارائه شده است. در این حمله هدف گره مخرب افزایش جذب ترافیک و قرارگیری در مکانی نزدیک به ریشه در درخت است. برای این منظور گره مخرب به کاهش ارادی و خارج از

۱. Perrefered Parent
۲. Destination advertisement Object
۳. Attacker

پروتکل مقدار Rank خود می‌پردازد. پس از این کار مهاجم می‌تواند با اعمال انواع حملات نظیر چاهک[۱]، سیاه‌چاله بر روی ترافیک ورودی بر عملکرد صحیح شبکه تاثیر منفی بگذارد. حملات سیاه‌چاله و چاهک حملاتی هستند که گره مخرب در آنها از طریق حذف پیام‌های دریافتی موجب مصرف بیهوده منابع در شبکه می‌گردد. در شکل زیر حمله کاهش مقدار Rank که در آن گره ۲۱ گره مخرب می‌باشد مشاهده می‌گردد[۸].



شکل ۱ : حمله ناسازگاری DAO

۳. کارهای پیشین

برای مقابله با حمله کاهش مقدار Rank در پروتکل RPL تا کنون روش‌های معدودی ارائه شده است. در ادامه این روش‌ها مورد بررسی قرار گرفته است.

۳-۱. روش VERA[۲]

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 $(V_N,\ldots..V_0)$. از طریق رابطه $V_i = h^{n+1-i}(r)$ 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.

مقادیر Rank در شماره ورژن i با زنجیره درهم‌سازی دیگری نمایش داده می‌شود$(R_{i,0},\ldots..,R_{i,l})$. مقدار Rank یکم در شماره ورژن i ام از طریق رابطه زیر محاسبه می‌گردد.

$$R_{i,l} = h^{l+1}(x_i) \qquad (۱)$$

در این رابطه x_i عدد تصادفی است. گره ریشه در پروتکل RPL سازگار با این روش در هنگام شروع اطلاعات $\{V_0,INT_{VN},R_{1,l},\{V0,MAC_{v1}(R1,l)\}_{sign}\}$ 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

۱. Sinkhole
۲. Version Number and Rank Authentication in RPL

درهم‌ساز مربوط به شماره ورژن ۱) دسترسی پیدا می‌کنند. گره ریشه در بروزرسانی‌های بعدی پیام را به همراه مقدار زمز شده‌ی $\{V_i , Init_{VN} + I, MAC_{Vi+1}(R_{I+1,l})\}$ منتشر می‌نماید سپس هر گره می‌تواند از طریق رابطه ۲ به بررسی شماره ورژن بپردازد.

$$h(V_i) == V_{i-1} \quad (۲)$$

همچنین هر گره می‌تواند به بررسی مقدار RANK مربوط به پدر (j) در یک شماره ورژن از طریق رابطه زیر نیز بپردازد.

$$MAC_{Vi}{}^{۱}(Ri,l) == MAC_{Vi}(h^{l-j}(R_{i,j})) \quad (۳)$$

با این روش حملات جعل شماره ورژن و یا تغییر در مقدار RANK تشخیص داده می‌شوند[۱۶]. از نقاط ضعف این روش می‌توان به موارد زیر اشاره کرد:

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

۳-۲. روش Parent Fail-Over

این روش از طریق عدم دریافت تعداد پیام‌های مشخص در یک بازه زمانی و در گره ریشه (توسط سایر گره‌های درخت) وجود حمله چاهک را تشخیص می‌دهد. در این روش به پیام‌های اطلاعات درخت لیستی از گره‌هایی که پیامی از آنها دریافت نشده توسط ریشه منتشر می‌گردد. هر گره با دریافت یک پیام اطلاعات درخت که خود در آن لیست باشد. پدر خود را در لیست سیاه محلی خود قرار داده و به تعمیر شرایط می‌پردازد.از نقاط ضعف این روش می‌توان به موارد زیر اشاره کرد:

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[۱۷].

۴-روش پیشنهادی

در این پژوهش برای ارائه روشی جهت مقابله با حمله کاهش مقدار Rank به مطالعه رفتار RPL در شرایط مختلف برابر این حمله پرداخته شد. نتیجه این کار یافتن تفاوت در تغییر پدر مورد اشاره به صورت ارادی (توسط گره مخرب در حمله مورد نظر) و در حالت غیر ارادی و در چارچوب قوانین پروتکل RPL است. در روش پیشنهادی از نشانه‌های مربوط به این تفاوت برای تشخیص حمله مذکور استفاده شده است.

تغییر پدر مورد اشاره در پروتکل RPL بر اساس مقدار Rank (فاصله تا ریشه) صورت می‌گیرد. بر اساس این پروتکل در هر گره و در هر زمان، وجود گره‌ای با مقدار Rank کمتر از پدر مورد اشاره فعلی در لیست پدران، موجب تغییر پدر مورد اشاره در آن گره می‌گردد. افزودن پدر جدید به لیست پدران ناشی از دریافت پیام اطلاعات درخت (شامل مقدار Rank آن) است. گره مربوطه در فرآیند تغییر پدر مورد اشاره ضمن عدم ارسال ترافیک از طریق پدر مورد اشاره قبلی به ارسال ترافیک از طریق پدر مورد اشاره جدید به سمت ریشه می‌پردازد.

۴-۱. نشانه‌های تشخیص حمله کاهش مقدار RANK

۱. Message Authentication Code

در حمله کاهش مقدار Rank تغییر پدر مورد اشاره در بسیاری از گره‌ها به سمت گره مخرب می‌انجامد. با این کار والد گره مخرب پس از حمله پیام تبلیغ مقصد حاوی مسیر جدید و یا موجود در جدول مسیریابی اما با گام بعدی متفاوت دریافت می‌نماید. اجرای این حمله بر پدر مورد اشاره قبلی نیز تاثیر می‌گذارد. پدر مورد اشاره قبلی بنابر یکی از دلایل زیر از عدم وجود مسیر مربوط به گره مخرب با خبر می‌گردد.

۱- دریافت پیام عدم وجود مسیر

بر اساس پروتکل RPL با تغییر پدر مورد اشاره گره مربوطه با ارسال پیام تبلیغ مقصد حاوی عدم وجود مسیر پدر مورد اشاره قبلی را از این تغییر با خبر می‌نماید.

۲- به پایان رسیدن زمانسنج مسیر مربوط به گره مخرب به دلیل عدم ارسال اطلاعات از طریق پدر مورد اشاره قبلی پس از حمله

در روش پیشنهادی پدر مورد اشاره قبلی و جدید با رویداد اتفاق‌های نامبرده یک پیام تبلیغ مقصد به همراه تنظیم نشانه امکان رخداد حمله به پدر مورد اشاره خود ارسال می‌نمایند. هر گره نیز با دریافت پیام تبلیغ مقصد حاوی نشانه‌ی حمله بدون تغییر این نشانه پیام تبلیغ مقصد را به پدر مورد اشاره خود باز ارسال می‌نماید. به این ترتیب پیام‌های تبلیغ مقصد حاوی نشانه‌های حمله به گره ریشه خواهد رسید. گره ریشه با دریافت هر دو نشانه مذکور و با دید همگانی از درخت، حمله مربوطه را تشخیص می‌دهد.

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 تصدیق پیام تبلیغ مقصد موجود در RPL اضافه شده است.

۴-۲. مکانیسم بازیابی

مکانیسم توضیح داده شده در قسمت قبل تنها باعث تشخیص حمله کاهش مقدار Rank می‌شود. در این قسمت به بازیابی درخت از تغییرات ایجاد شده در اثر اجرای این حمله می‌پردازیم برای این امر گره مخرب از درخت مربوطه حذف می‌گردد. مکانیسم حذف گره مخرب از طریق روش لیست سیاه صورت می‌گیرد. در این روش گره ریشه پس از تشخیص گره مخرب در پیام‌های اطلاعات درخت خود آدرس گره مخرب را منتشر می‌نماید. هر گره با دریافت این آدرس آن را از لیست پدران خود خارج می‌نماید.

۵-ارزیابی

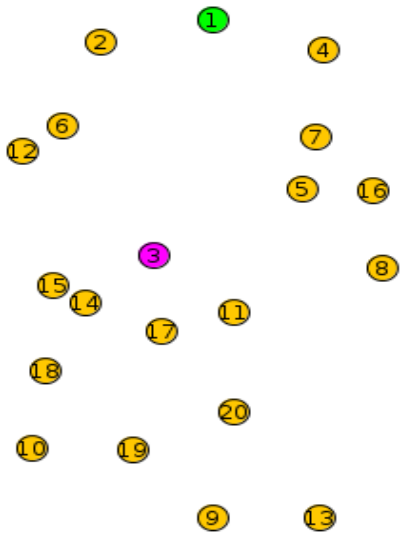
در این قسمت عملکرد روش پیشنهادی را مورد بررسی قرار خواهیم داد. برای این امر ابتدا در توپولوژی شکل شماره تاثیر حمله کاهش مقدار Rank را نشان خواهیم داد. فرآیند انتخاب توپولوژی تصادفی بوده و در آن گره شماره ۳ گره مخرب و گره شماره ۱ ریشه درخت می‌باشد. برای مشاهده تاثیر بهتر مکانیسم بازیابی بر ترافیک گره‌های شبکه، گره

مخرب پس از اجرای حمله کاهش مقدار Rank و جذب ترافیک حاصله به حذف بسته‌های ورودی نیز می‌پردازد. به این ترتیب از دریافت ترافیک متعلق به گره‌های قربانی در ریشه جلوگیری می‌گردد.

برای شبیه‌سازی روش پیشنهادی از شبیه‌سازی Cooja در سیستم‌عامل Contiki استفاده شده است. پارامترهای مورد استفاده در شبیه‌سازی در جدول شماره ۱ نشان داده شده است.

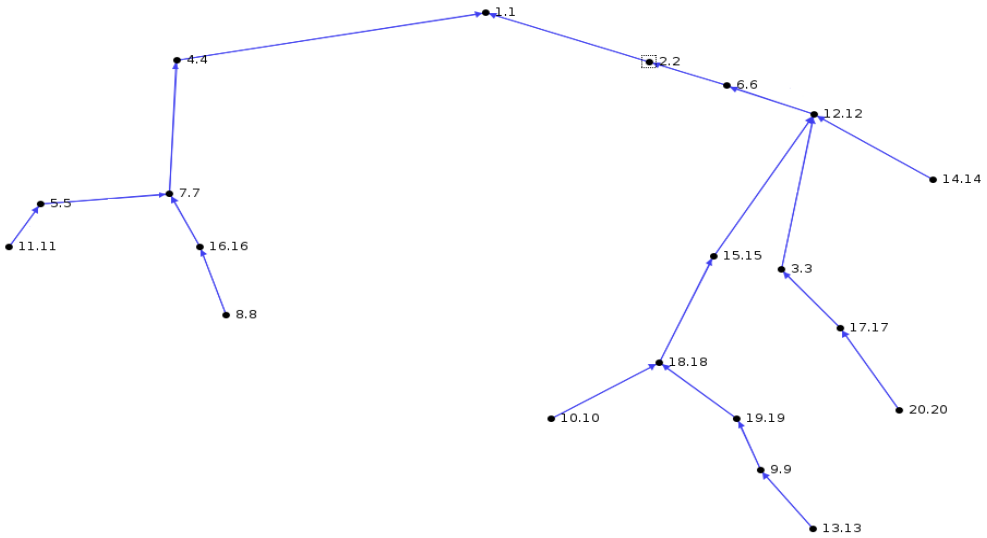
جدول ۱ : پارامترهای مورد استفاده در شبیه‌سازی

زمان شبیه‌سازی	۳۰ دقیقه
منطقه تحت پوشش	۱۵۰ * ۱۷۵ متر مربع
تعداد گره‌ها	۲۰ گره
بازه زمانی ارسال بسته	۱۰ ثانیه
اندازه بسته	۴۲ بایت
پروتکل مسیریابی	RPL
پروتکل لایه مک	۸۰۲,۱۵,۴

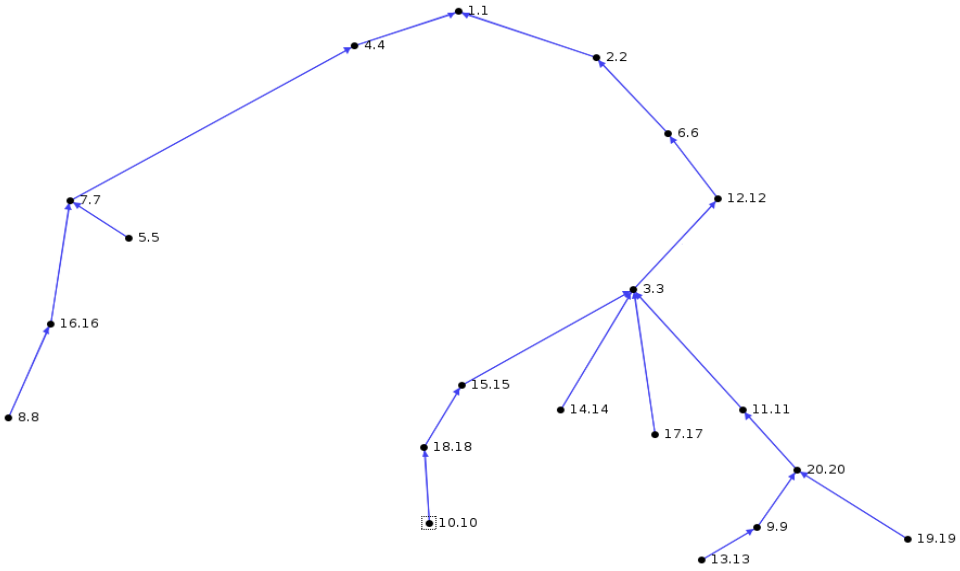


شکل ۲ : توپولوژی انتخابی

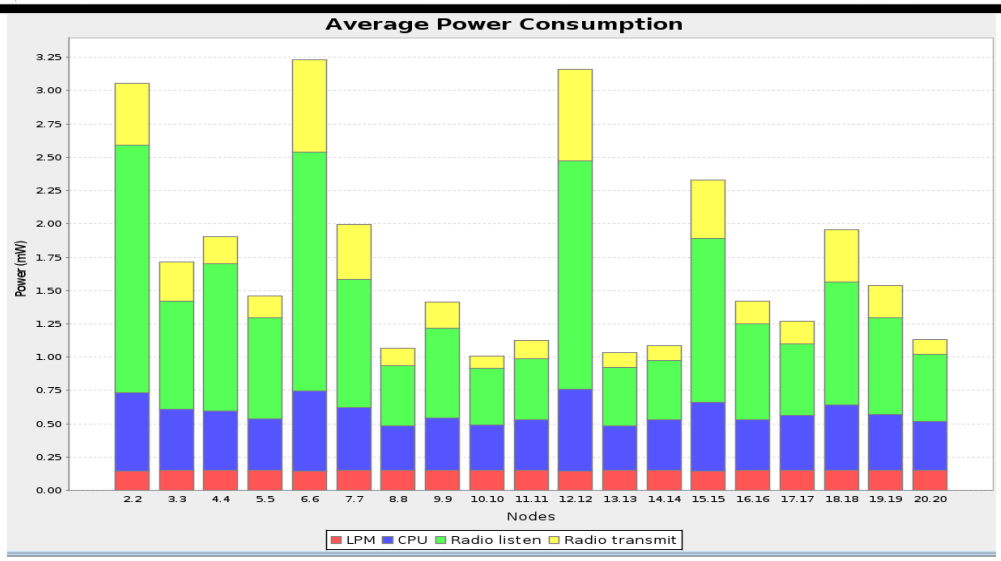
در شکل‌های شماره ۳ الی ۱۲ تاثیر حمله کاهش مقدار Rank بر پروتکل RPL و همچنین رفتار روش پیشنهادی در مقابل این حمله دیده می‌شود. با توجه به شکل شماره ۴ در اثر اجرای حمله کاهش مقدار Rank بسیاری از سنسورها در درخت با انتخاب گره مخرب به عنوان پدر مورد اشاره، ترافیک زیردرخت خود را از طریق این گره به سمت ریشه ارسال می‌نمایند.



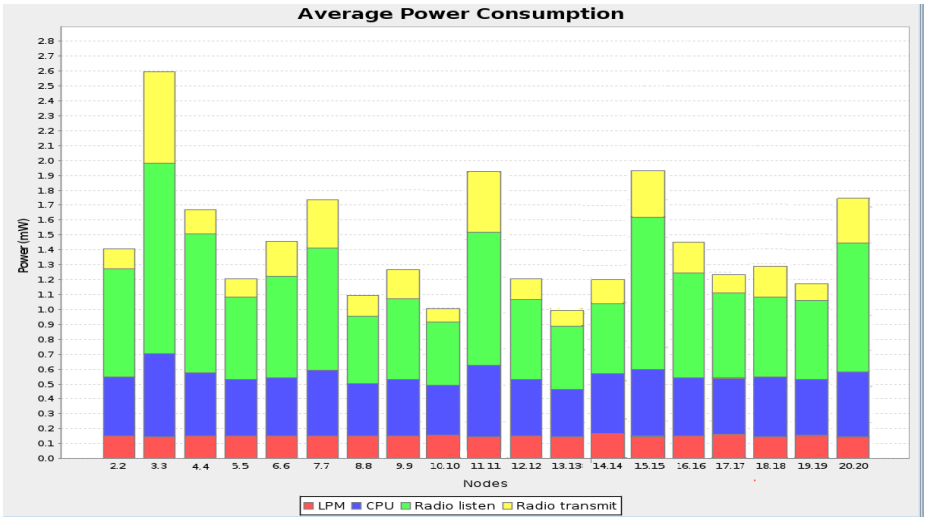
شکل ۳ : توپولوژی در RPL بدون رفتار مخربانه



شکل ۴ : توپولوژی حاصل از حمله کاهش مقدار RANK

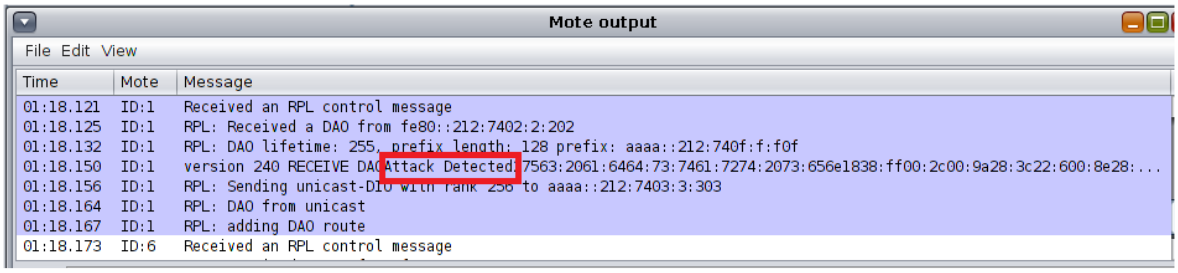


شکل ۵ : متوسط مصرف انرژی در RPL بدون رفتار مخربانه



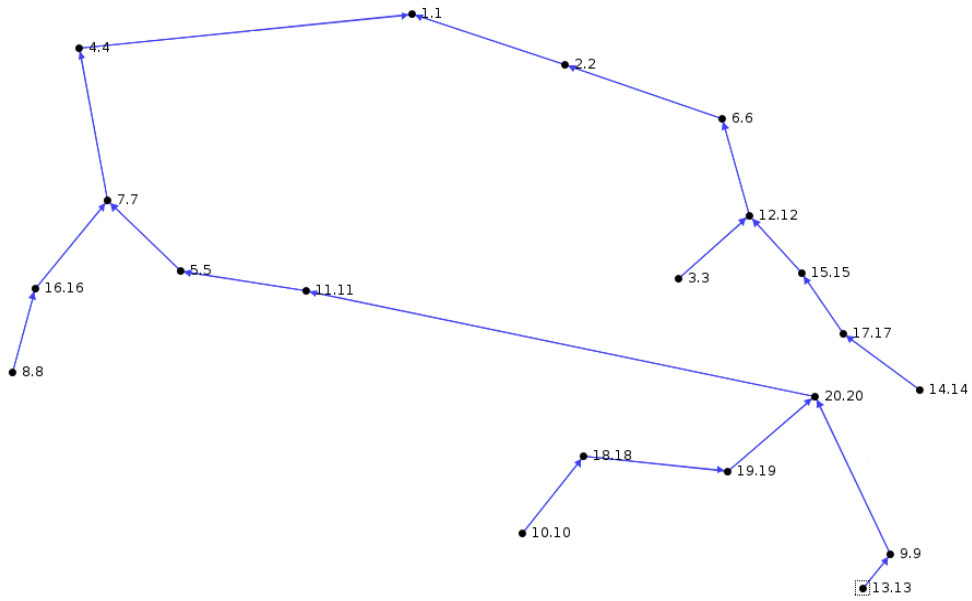
شکل ۶ : متوسط مصرف انرژی در حمله کاهش مقدار RANK

این امر در مصرف انرژی در برخی گره‌ها تاثیرگذار بوده است. این تاثیر در مصرف انرژی برخی گره‌ها به صورت افزایشی دیده می‌شود (مقایسه شکل شماره ۵ و شکل شماره ۶). عبور ترافیک بیشتر از گره‌های نامبرده به علت تغییر توپولوژی دلیل اصلی این امر است. افزایش ترافیک عبوری بر مصرف انرژی هر چهار عامل پردازش، حالت مصرف کم توان (در هنگام عدم وجود ارسال)، انتقال رادیویی و گوش دادن به رسانه مشترک در گره‌ها موثر بوده است. با توجه به شکل-های ۶ و ۷ مصرف انرژی از برگ‌ها به سمت ریشه افزایش می‌یابد. مکان‌هایی از توپولوژی شکل شماره ۲ همراه با ازدحام بیشتر سنسورها به دلیل دسترسی سخت‌تر به رسانه اشتراکی مصرف انرژی بیشتری را برای آنها به همراه دارند.

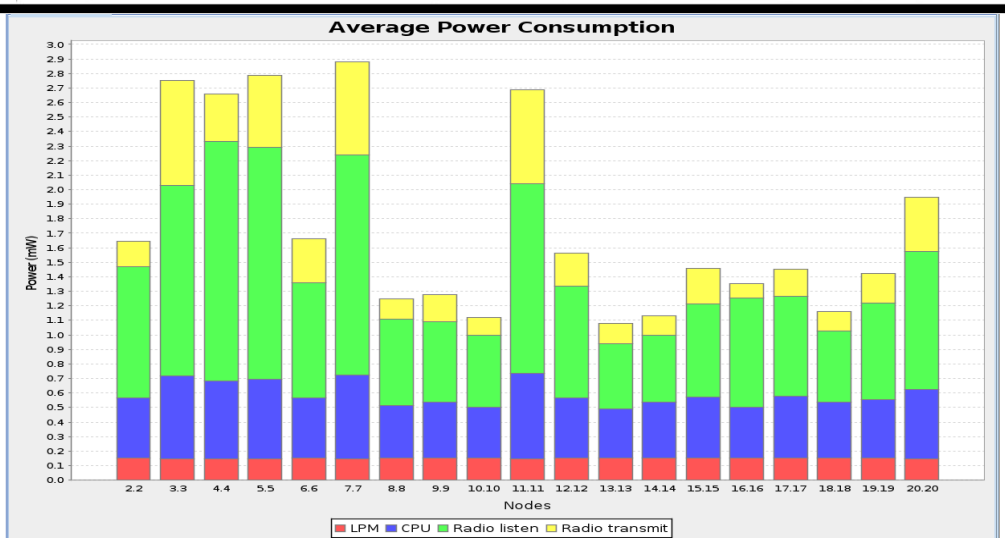


شکل ۷ : تشخیص حمله کاهش مقدار RANK در گره ریشه

همانطور که در شکل شماره ۷ مشاهده می‌گردد رفتار مخربانه پس از اجرای حمله مربوطه در گره ریشه تشخیص داده شده است. اجرای مکانیسم بازیابی پس از تشخیص حمله باعث دریافت آدرس گره مخرب به صورت لیست سیاه در گره‌های قربانی در حمله شده است. واکنش گره‌های قربانی به این امر تغییر پدر مورد اشاره خود از گره مخرب بوده است. این تغییر در شکل شماره ۸ دیده می‌شود.

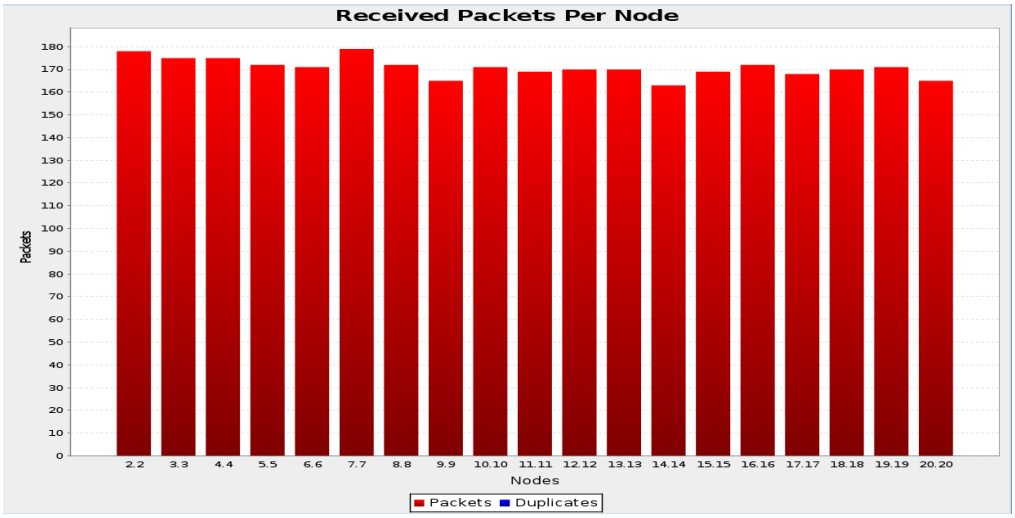


شکل ۸ : توپولوژی روش پیشنهادی-حمله کاهش مقدار RANK



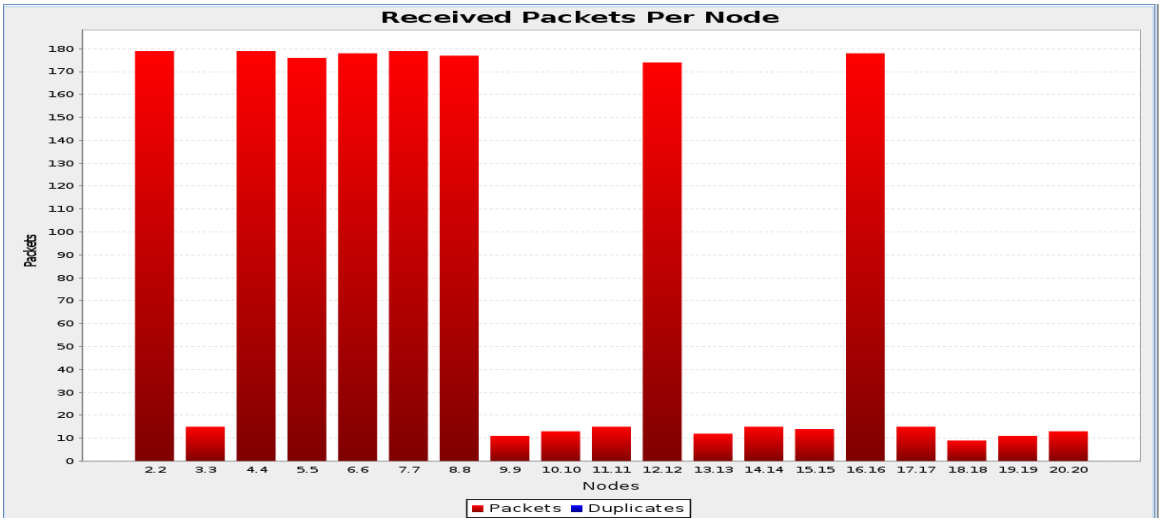
شکل ۹ : متوسط مصرف انرژی در روش پیشنهادی و حمله کاهش مقدار RANK

با توجه به شکل شماره ۹ مصرف انرژی مربوط به گره‌ها متناسب با عبور ترافیک از آنها مشابه حالت عادی است. این امر نشان‌دهنده بازگشت شبکه به شرایط عادی و عملکرد صحیح روش پیشنهادی در فرآیند تشخیص و مکانیسم بازیابی است.



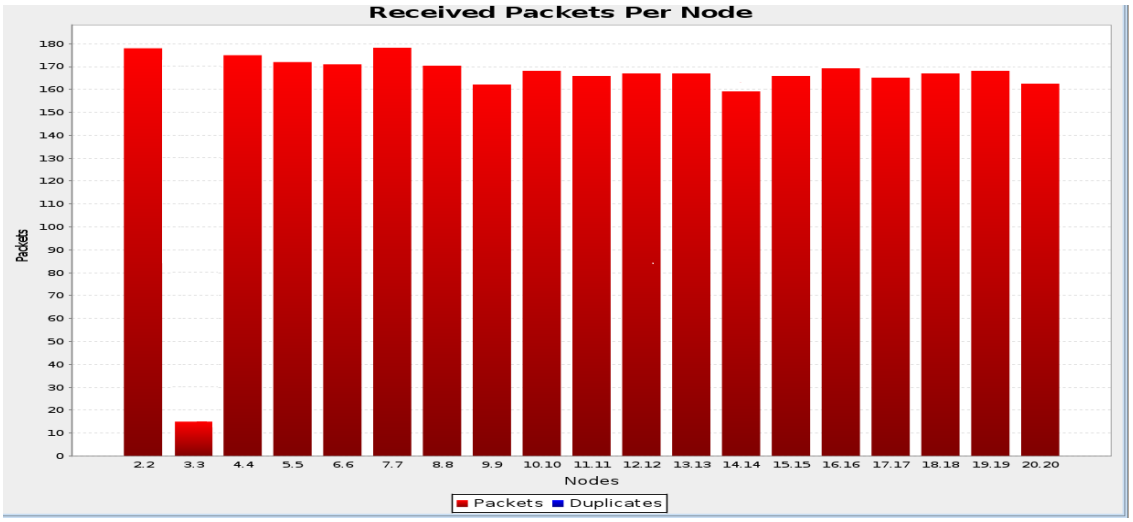
شکل ۱۰ : بسته‌های دریافت شده هر گره در RPL بدون رفتار مخربانه

همانطور که در شکل شماره ۱۰ 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.



شکل ۱۱ : بسته‌های دریافت شده هر گره در حمله کاهش مقدار RANK

قطع ارتباط گره‌های قربانی با ریشه در گره مخرب پس از اجرای حمله باعث کاهش شدید بسته‌های دریافت شده از آنها در ریشه شده است (شکل ۱۱).



شکل ۱۲ : بسته‌های دریافت شده هر گره در روش پیشنهادی-حمله کاهش مقدار RANK

پس از اجرای مکانیسم بازیابی و حذف گره قربانی ارسال بسته‌ها به سمت ریشه به طور مجدد به حالت عادی بازگشته است. همچنین با اجرای مکانیسم بازیابی ترافیک مربوط به گره مخرب توسط شبکه منتقل نگردیده است (شکل ۱۲).

۷-نتیجه‌گیری

در این پژوهش ضمن ارائه یک روش تشخیص و بازیابی حمله کاهش مقدار RANK مکانیسمی جهت بازیابی تغییرات ناشی از این حمله در درخت DODAG ارائه شد. سپس این مکانیسم در سیستم‌عامل Contiki و شبیه‌ساز Cooja مورد ارزیابی قرار گرفت. نتایج این ارزیابی (نمودارهای ۳ الی ۱۲) صحت عملکرد روش پیشنهادی را تایید می-نماید. از معایب این روش می‌توان به امکان ایجاد حملات جدید بر پایه این مکانیسم در پروتکل RPL و وجود احتمال رخداد حمله کاهش مقدار Rank با وجود این مکانیسم در حالات خاص (بر اساس شرایط شبکه) اشاره نمود.

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

مراجع

1. 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.
2. 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.
3. Airehrour, D. Gutierrez, J. and Kumar Ray, S. (2016). "Secure routing for internet of things: A survey." Journal of Network and Computer Application: 14.
4. Le, A. Lee, J. Lasebade, A. Vinel, A. Chen, Y and Chai, M (2013). "The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks." IEEE SENSORS JOURNA
5. 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
6. Diaz, A. and Sanchez, P. (2016).”Simulation of Attacks for Security in Wireless Sensor Network”, Sensors (Basel).18
7. Granjial, J. Monteiro, E. and Silva, J. (2015) “Security for the Internet of Things: A survey Of Existing Protocols and Open Research issues”,
8. Mayzaud, A. Biddonel, R. and Chrisment, I. (2016).” A Taxonomy of Attacks in RPL-based Internet of Things”, International Journal of Network Security, IJNS, 2016
9. RFC 2373 (2003) “Internet Protocol Version 6 (IPv6) Addressing Architecture”
10. RFC 6550 (2012) “IPV6 Routing Protocol For Low Power and Lossy Network”
11. RFC 6206 (2011) “The Trickle Algorithm”
12. Contiki Os Tutotials
13. 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

14. 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
15. Idris Khan, F. Shon, T. Lee, T. and Kim, K. (2013).” Wormhole Attack Prevention Mechanism for RPL Based LLN Network”, Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on
16. 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
17. Weekly, K. and Pister P. (2012), “Evaluating sinkhole defense techniques in RPL networks”, Network Protocols (ICNP), 2012 20th IEEE International Conference on