# مروری بر حملات و راه‌حل‌های امنیتی پروتکل مسیریابی RPL

**محمد پیشدار[1*]، یونس سیفی[2] و مظفر بگ محمدی[3]**

[1]فارغ التحصیل کارشناسی ارشد فناوری اطلاعات، دانشگاه بوعلی سینا، همدان، ایران
mohamadpishdar@gmail.com

[2]استادیار گروه رایانه دانشگاه بوعلی سینا، همدان، ایران
yseifi@basu.ac.ir

[3]دانشیار گروه رایانه دانشگاه ایلام، ایلام، ایران
Mozafar@ilam.ac.ir

## چکیده

**پروتکل مسیریابی آر.پی.اِل[1] برای شبکه‌های کم‌توان (از منظر مصرف انرژی) و پر اتلاف (هنگام ارسال بسته‌ها)[2] طراحی شده است. شبکه‌هایی که به‌طورعمومی در آن‌ها از دستگاه‌هایی با توان پردازشی پایین و حافظهٔ کم‌حجم استفاده می‌شود. فناوری "اینترنت اشیا" یکی از کاربردهای رایج این شبکه‌ها است. در این فناوری ارتباط اشیا با یکدیگر از طریق شبکه و به‌کمک مدارهای کم‌توان برقرار می‌شود و کاربردهای زیادی را در حوزه‌های مختلفی از جمله مصرف انرژی، امنیت فیزیکی و هوشمندسازی شهرها فراهم می سازد. اینترنت اشیا با بسیاری از فناوری‌های مشابه به‌علت وجود اشیا و مدارهای الکترونیکی کم‌توان تمایز دارد. یکی از این موارد مربوط به موضوع امنیت اطلاعات آن می‌شود. ترکیب مدارهای الکترونیکی و اشیا در کنار پراکندگی دستگاه‌ها می‌توانند باعث ایجاد حملات سایبری مؤثرتری در محیط واقعی شود. بر این اساس، تأمین امنیت اطلاعات در این پروتکل و سایر بخش‌های اینترنت اشیا از اهمیت بالایی برخوردار است. در این مقاله، به مطالعه حملات سایبری موجود روی پروتکل مسیریابی آر.پی.اِل و همچنین راه‌حل‌های امنیتی مربوطه پرداخته شده است؛ سپس، این راه‌حل‌ها دسته‌بندی شده و نقاط ضعف و قوت آنها مورد بررسی قرار می‌گیرد. بخش انتهایی مقاله نیز به بررسی وضعیت فعلی امنیت اطلاعات در پروتکل آر.پی.اِل اختصاص دارد.**

**واژگان کلیدی: اینترنت اشیا، پروتکل مسیریابی آر.پی.اِل، امنیت در اینترنت اشیا، امنیت در پروتکل آر.پی.اِل**

## ۱- مقدمه

در فناوری اینترنت اشیا، مدارهای الکترونیکی کوچک و کم‌توان امکان برقراری ارتباط میان اشیا را فراهم می‌سازند. این ارتباطات از طریق یک سیستم قدرتمندتر به فضای اینترنت نیز قابل توسعه است. تاکنون کاربردهای فراوانی برای این فناوری معرفی شده است که از جمله آن ها می‌توان به کنترل انرژی، امنیت فیزیکی و هوشمندسازی شهری اشاره کرد. یکی از مشکلات مهم اینترنت اشیا در ابتدای پیداش، عدم سازگاری روش‌ها یا فناوری‌های ارتباطی مشهور با آن بود. درواقع ویژگی خاص دستگاه‌ها در این فناوری از جمله توان پردازشی و ارتباطی محدود امکان استفاده از فناوری‌های روز را در آن غیر ممکن می‌ساخت. علاوه‌براین، برخی دیگر از ویژگی‌های خاص این فناوری مانند نوع خاص ترافیک ارسالی (ترافیک به‌طورمعمول از حس‌گرها به یک گره در شبکه ارسال می‌شود) نیاز به طراحی پروتکل‌های جدید را الزامی می‌کرد. یکی از این نیازها، طراحی یک پروتکل جدید برای مسیریابی در اینترنت اشیا بود. در همین راستا پروتکلی به نام آر.پی.اِل مخصوص شبکه‌های کم‌توان (از منظر مصرف انرژی) و پر اتلاف (هنگام ارسال بسته‌ها) توسط پژوهش‌گران طراحی شد [۴,۳,۲,۱]. هم‌زمان با ارائهٔ پروتکل آر.پی.اِل و به‌دلیل اهمیت فراوان امنیت اطلاعات در اینترنت اشیا، پژوهش‌گران بسیاری به بررسی حفره‌های امنیتی این پروتکل پرداخته و با گذشت زمان آسیب‌پذیری‌های متعددی در آن یافت شد. در ادامه، پس

[1] Routing Protocol for Low Power and Lossy Networks
[2] Packet Forwarding

* نویسندهٔ عهده‌دار مکاتبات

از معرفی پروتکل آر.پی.اِل به نگرانی‌های امنیتی آن و راه‌حل‌های موجود پرداخته شده است [۴,۳,۲,۱].

گفتنی است که پژوهش‌گران دیگری نیز در مراجع [۷,۶,۵] به بررسی وضعیت امنیتی پروتکل آر.پی.اِل پرداخته‌اند که برای بهبود برخی نقاط ضعف موجود در پژوهش آن‌ها اقدام به ارائه این مقاله شد. از جملهٔ این ضعف‌ها می‌توان به معرفی مختصر نگرانی‌ها یا راه‌حل‌های امنیتی موجود، عدم پوشش بخش قابل توجهی از راه‌حل‌ها و همچنین نبود مقایسه و تحلیل راهکارها اشاره کرد.

## ۲- پروتکل مسیریابی آر.پی.اِل

توپولوژی شبکه در پروتکل آر.پی.اِل به‌صورت یک درخت بدون دور بوده که شکل‌گیری آن به کمک پیام‌های کنترلی خاصی در قالب نسخه ششم "پیام‌های کنترلی اینترنت[۱]" صورت می‌گیرد [۹,۸,۴]. این درخت "دو.دَگ"[۲] نام داشته و در فرآیند ایجاد آن ابتدا گرهٔ ریشه (گره‌ای که نسبت به سایر گره‌ها از نظر پردازشی قدرتمندتر بوده و مجری اصلی کاربردهای اینترنت اشیا در درخت دو.دَگ است) به ارسال اطلاعات پیکربندی، در قالب یک پیام کنترلی تحت عنوان دی.آی.او[۳] می‌پردازد. این پیام به‌صورت همه‌پخشی[۴] و در محدوده بی‌سیم گره ریشه ارسال خواهد شد. تمام گره‌های موجود در این محدوده با دریافت پیام یادشده ضمن پیوستن به درخت، ریشه را به‌عنوان والد خود در دو.دَگ انتخاب می‌کنند [۹,۸,۴]. آن‌ها پس از پیوستن به درخت، مدتی صبر کرده و سپس آخرین اطلاعات خود را به صورت همه‌پخشی[۴] و در قالب پیام‌های دی.آی.او منتشر می‌کنند. به این ترتیب اطلاعات پیکربندی برای گره‌های بیشتری و از مسیرهای متعدد منتشر خواهد شد. گفتنی است که یک گره می‌تواند پیام‌های دی.آی.او را از مسیرهای مختلف دریافت کند. در این شرایط گره مربوطه باید از بین گره‌های ارسال‌کنندهٔ دی.آی.او یک گره را برای ارسال ترافیک خود و زیردرخت مربوطه به ریشه انتخاب کند. به این گره "پدر ارجح" گفته شده و انتخاب آن بر اساس شرایط زیر صورت می‌گیرد [۹,۸,۴]:

- حلقه در درخت ایجاد نشود
- ترافیک از نزدیک‌ترین مسیر ممکن به ریشه برسد : این موضوع بر اساس یک مقدار مشخص به نام "رتبه[۵]" در پیام‌های دی.آی.او صورت می‌گیرد. این مقدار دارای رابطه مستقیم با فاصلهٔ گره از ریشه است. درواقع هر چه مقدار رتبه بیشتر باشد، گره ارسال‌کننده پیام دی.آی.او نیز از ریشه دورتر است. بر این اساس هر گره جهت انتخاب بهترین مسیر ممکن برای ارسال اطلاعات به ریشه باید از بین گره‌های ارسال‌کنندهٔ دی.آی.او گره‌ای با مقدار کمتر رتبه را انتخاب کند [۹,۸,۴].

در پروتکل آر.پی.اِل نوع دیگری از پیام‌های کنترلی به نام دی.آی.او[۶] نیز وجود دارد. طبق قوانین آر.پی.اِل، هر گره در درخت دو.دَگ از طریق این پیام اجداد خود (گره‌های موجود در مسیر ریشه) را از وضعیت مسیرهای رو به پایین (مسیرهای موجود در زیردرخت گره مربوطه) مطلع می‌سازد. این نوع مسیرها در گره‌ها ذخیره شده و فرآیند مسیریابی به‌کمک آن انجام می‌شود [۹,۸,۴]. مسیرهای رو به پایین در پروتکل آر.پی.اِل به دو صورت ذخیره می‌شوند [۹].

۱- **ذخیره‌سازی به‌صورت توزیع‌شده**: در این حالت هر گره در درخت دارای جدول مسیریابی بوده و در این فرآیند مشارکت می‌کنند.

۲- **ذخیره‌سازی به‌صورت متمرکز**: در این حالت گره‌ها فاقد جدول مسیریابی بوده و تمام اطلاعات مورد نیاز به ریشه به‌عنوان دانای کل ارسال شود. در این رویکرد گره ریشه با اطلاع از تمام مسیرهای موجود عمل مسیریابی را انجام می‌دهد.

آخرین نوع از پیام‌های کنترلی موجود در پروتکل آر.پی.اِل، پیام‌های دی.آی.اِس[۷] هستند. دستگاه‌های خواهان پیوستن به درخت دو.دَگ با ارسال این نوع پیام تقاضای ارسال اطلاعات مورد نیاز را می‌کنند. پیام‌های دی.آی.اِس باید به برگ‌های درخت ارسال شود [۹,۸,۴].

## ۳- نگرانی‌های امنیتی در آر.پی.اِل

در پروتکل آر.پی.اِل تا به امروز آسیب‌پذیری‌های امنیتی زیادی کشف شده که در ادامه به تشریح آن‌ها می‌پردازیم.

### ۳-۱- حملات سیل آسا [۸]

هدف از این حمله مصرف بیهوده منابع گره‌ها به‌نحوی است که موجب اختلال در عملکرد شبکه شود. این حمله به‌طورمعمول در پروتکل آر.پی.اِل با ارسال بسیار زیاد

[1] Internet Control Message Protocol (ICMP)
[2] Destination Oriented Directed Acycle Graph-DODAG
[3] DODAG Information Object
[4] Broadcast
[5] Rank
[6] Destination Advertisement Object
[7] Destination Advertisement Object
[8] Flooding




[ DOR: 20.1001.1.24763047.1399.9.1.2.5 ]

پیام‌های دی.آی.اِس به اطرافیان صورت می‌گیرد تا باعث شروع مجدد زمان‌سنج قطره‌چکان شود [۱۱,۱۰,۴,۳]. در آر.پی.اِل، شروع مجدد این زمان‌سنج منجر به ارسال پیغام‌های دی.آی.او و ایجاد سربار اضافه بر روی شبکه می‌شود.

## ۳-۲- حملات سرریز جداول مسیریابی

در این حمله مهاجم[1] سعی بر ایجاد مسیرهای ساختگی فراوان در جدول مسیریابی گره قربانی خواهد کرد. هدف از این کار اشغال فضای حافظهٔ مربوط به جداول مسیریابی بوده به‌طوری که دیگر جایی برای ثبت مسیرهای جدید وجود نداشته باشد. در این شرایط عملکرد پروتکل آر.پی.اِل نه‌تنها برای آن گره بلکه به‌علت انتشار اطلاعات غلط با اختلال وسیعی روبه‌رو خواهد شد [۱۰].

## ۳-۳- حمله افزایش مقدار رتبه

در این حمله مهاجم با سوءاستفاده از هزینه بالای بازیابی حلقه‌های مسیریابی در پروتکل آر.پی.اِل به افزایش ارادی مقدار رتبه خود می‌پردازد. با این کار برخی گره‌ها به تغییر پدر ارجح پرداخته و برخی دیگر اقدام به این کار نمی‌کنند (کمینه زمانی برای به‌روزرسانی شرایط درخت نیاز است). این امر می‌تواند به ایجاد حلقه در درخت ختم شود. مهاجم نیز برای تاثیر بیشتر حمله، در سازوکار مقابله با حلقه پروتکل آر.پی.اِل شرکت نخواهد کرد [۱۱,۱۰].

## ۳-۴- حملات ناسازگاری در دو.دَگ

در پروتکل آر.پی.اِل از پیام‌های کنترلی برای پیکربندی و مدیریت شبکه استفاده می‌گردد. این پیام‌ها شامل فیلدهای مشترکی بوده که یکی از آن‌ها جهت حرکت نام دارد. تنظیم مقدار ۱ در این فیلد به معنی حرکت پیام مربوطه به سمت پایین درخت و در جهت برگ‌ها است (برعکس این حالت نیز وجود دارد). بر این اساس اگر گره‌ای یک پیام کنترلی با جهت حرکت رو به پایین و مقدار رتبه (فیلدی در پیام‌های کنترلی) بیشتر نسبت به خود دریافت نماید (یا بالعکس) آنگاه می‌تواند وقوع یک ناسازگاری را تشخیص دهد. برای این شرایط پروتکل آر.پی.اِل دارای یک سازوکار بازیابی بوده که پس از دریافت تعداد مشخصی از پیام‌های ناسازگاری فعال می‌شود. در این حالت نیز، زمان‌سنج قطره‌چکان[2] شروع مجدد شده و پیغام دی.آی.او برای تعمیر درخت ارسال می‌شود. سربار این امر منجر به مصرف منابع برخی گره‌ها خواهد شد. به عبارت دیگر برخی لینک‌ها از دسترس خارج شده و هدایت ترافیک به یک نقطه خاص از درخت صورت می‌گیرد. امری که از پیامدهای آن می‌توان به افزایش مصرف انرژی و کندی پردازش‌ها اشاره کرد [۱۱,۱۰,۳].

## ۳-۵- حملات افزایش شماره نسخه

گره ریشه هنگام ایجاد درخت دو.دَگ در پیام‌های دی.آی.او یک شمارهٔ نسخه نیز قرار داده و سپس آن را به‌صورت همه‌پخشی ارسال می‌کند. این شماره هنگام بازیابی ساختار درخت پروتکل آر.پی.اِل کاربرد دارد. درواقع گره ریشه با افزایش شمارهٔ نسخه در پیام‌های دی.آی.او وجود یک مشکل اساسی در درخت دو.دَگ را به سایر گره‌ها خبر می‌دهد. در این شرایط گره‌های دریافت‌کننده پیام دی.آی.او باید اطلاعات قبلی خود را فراموش کرده و از ابتدا در فرآیند تشکیل درخت دو.دَگ شرکت کنند. در حمله "افزایش شماره نسخه" یک مهاجم با سوءاستفاده از این شماره و انتشار نسخه جعلی آن در درخت، سربار زیادی را (از نظر پردازشی و ارتباطی) به شبکه تحمیل می‌کند [۱۰].

## ۳-۶- حمله کرم‌چاله[3]

در این حمله گره مخرب ترافیک را با یک پیوند خارج از شبکه به قسمت دیگری از درخت دو.دَگ منتقل می‌کند. با این کار گره‌های بخش دوم نیاز به پردازش‌های به‌نسبه بالایی برای بررسی و مدیریت ترافیک ورودی داشته که ناشی از عدم تطابق با قوانین آر.پی.اِل است؛ بنابراین در شبکه سربار بیهوده ایجاد می‌شود [۱۱,۱۰,۴,۳].

## ۳-۷- حمله ناسازگاری‌دی.آی.او

در پروتکل آر.پی.اِل هنگام ذخیره‌سازی مسیرها به‌صورت توزیع‌شده نوعی ناسازگاری پیش‌بینی شده است. این ناسازگاری مربوط به شرایطی است که پیامی از طریق یک مسیر بی اعتبار (به‌عنوان مثال دارای زمان‌سنج پایان یافته) در گام بعدی (یکی از گره‌های فرزند در درخت دو.دَگ) مسیریابی شود. در این شرایط گره دوم یک پیام خطای مبنی بر عدم اعتبار مسیر به گره اولیه ارسال کرده و شرایط یادشده را اطلاع می‌دهد. گره نخست نیز با دریافت این پیام باید مسیر دیگری را برای ارسال پیام خود انتخاب کند. در حمله "ناسازگاری دی.آی.او"

[1] Attacker
[2] Trickle
[3] Wormhole


[ DOR: 20.1001.1.24763047.1399.9.1.2.5 ]

به‌طوردقیق از همین موضوع برای ایجاد اختلال در شبکه سوءاستفاده می‌شود. به‌عنوان، مثال گره مخرب با ارسال این نشانه برای تمام مسیرهای جدول خود درعمل دسترسی به گره‌های زیر درخت را غیرممکن می‌سازد [۱۱,۱۰].

### ۳-۸- حمله انتخاب بدترین والد

در این حمله گره مخرب در فهرست پدران خود به جای انتخاب گره بهینه، بدترین گره ممکن را جهت انتقال ترافیک به سمت ریشه انتخاب می‌کند. به این ترتیب تأخیر و سربار زیادی بر زیردرخت گره مخرب به دلیل افزایش هزینه ارتباط با ریشه تحمیل خواهد شد [۱۱,۱۰].

### ۳-۹- حملات جعل مسیر

در این حمله گره مخرب به ایجاد مسیرهای جعلی در گره‌های قربانی می‌پردازد. این امر ارسال پیام‌ها در مسیرهای اشتباه را در درخت دو.دَگ به‌دنبال دارد. فرآیندی که سربار فراوانی بر روی پروتکل آر.پی.اِل ایجاد می‌کند [۱۱,۱۰].

### ۳-۱۰- حملات سیاه‌چاله[1] و چاهک[2]

در این حملات گره مخرب در درخت دو.دَگ به جای ارسال بسته‌های دریافتی شروع به حذف تمام (حملهٔ سیاه‌چاله) یا بخشی از آن‌ها (حملهٔ چاهک) بر اساس جدول مسیریابی می‌کند. به این ترتیب دسترسی به بخشی از گره‌های درخت دو.دَگ غیرممکن شده و یا با اختلال روبه‌رو می‌شود [۴،۱۰و ۱۱].

### ۳-۱۱- حملات تکرار

در این حملات گره مخرب پیام‌های کنترلی دریافتی را ضبط کرده و در زمانی دیگر دوباره به شبکه تزریق می‌کند. به‌علت عدم تمایز این پیام‌ها در پروتکل آر.پی.اِل شبکه متوجه این رفتار مخرب نشده و به‌صورت عادی رفتار می‌کند. بر این اساس توپولوژی درخت دو.دَگ می‌تواند به‌صورت غیرمجاز تغییر کند (به‌ویژه اگر موارد تکرار از نوع پیام‌های دی.آی.او باشند) [۱۱,۱۰].

### ۳-۱۲- حمله کاهش مقدار رتبه

در این حمله گره مخرب با کاهش ارادی و ساختگی مقدار رتبه خود سعی دارد برای سایر گره‌ها (گره‌های موجود در محدودهٔ بی‌سیم گره مخرب) در مکانی نزدیک به ریشه به نظر بیاید. هدف از این کار تغییر پدر ارجح برخی گره‌های درخت دو.دَگ بوده، به‌طوری‌که ترافیک زیادی از گره مخرب عبور کند. در این شرایط مهاجم می‌تواند به اجرای حملات دیگری از جمله چاهک، سیاه‌چاله بر روی ترافیک دریافتی بپردازد [۱۰و۱۱].

### ۳-۱۳- حملات جعل هویت

در این حملات گره مخرب به جعل شناسه فیزیکی سایر گره‌های درخت دو.دَگ از جمله گره ریشه می‌پردازد. هدف از این کار ایجاد برخی ناسازگاری‌ها در آر.پی.اِل از جمله ایجاد ترافیک جعلی با هدف مصرف منابع گره‌ها است [۱۱,۱۰,۴,۳].

### ۳-۱۴- شنود و تحلیل ترافیک

گره مخرب در این حمله شروع به شنود و تحلیل ترافیک به صورت غیرمجاز می‌کند. حتی در صورت رمزنگاری اطلاعات نیز امکان تحلیل ترافیک وجود دارد. این تحلیل می‌تواند شامل پرسش‌هایی از جمله موارد زیر باشد [۷]:

- ارسال ترافیک از کدام گره‌ها به یکدیگر است؟
- زمان ارسال‌ها به‌طورمعمول چه موقع است؟
- کدام گره‌ها با هم بیشتر ارتباط برقرار می‌کنند؟

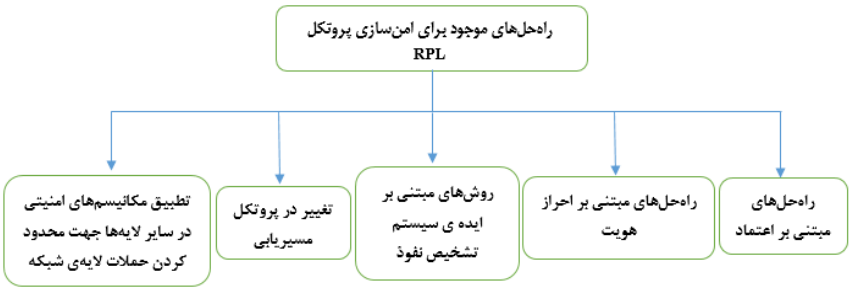
## ۴- راه‌حل‌های موجود برای امن‌سازی پروتکل آر.پی.اِل

به‌دلیل وجود نگرانی‌های امنیتی مختلف در پروتکل آر.پی.اِل، پژوهش‌گران به ارائه راه حل‌های مختلفی جهت ارتقای امنیت آن پرداخته‌اند. در شکل (۱) یک دسته‌بندی کلی از راه‌حل‌های موجود در این زمینه آورده شده است. در ادامه به معرفی هر دسته و راه‌حل‌های مربوطه پرداخته خواهد شد.

### ۴-۱- راه‌حل‌های مبتنی بر اعتماد

در این راه‌حل‌ها از مفهوم اعتماد برای تشخیص رفتار مخربانه استفاده شده است. رفتار مخربانه می‌تواند بر اساس هدف پژوهش به‌صورت‌های متفاوتی در نظر گرفته شود؛ البته، رفتارهای خارج از قوانین آر.پی.اِل باعث کاهش پارامتر اعتماد خواهد شد. گذشت زمان هم یکی از متداول‌ترین رویکردها برای بازگشت اعتماد به مقدار اولیه است. در ادامه راه‌حل‌های مبتنی بر اعتماد برای امن‌سازی پروتکل آر.پی.اِل آورده شده است.

[1] Blackhole
[2] Sinkhole




**(شکل-۱): راه‌حل‌های موجود برای امن‌سازی پروتکل آر.پی.اِل**

### ۱-۱-۴- روش سِک.تِراست[1]

اساس این روش میزان اعتماد گره‌ها نسبت به یکدیگر در رابطه با رعایت قوانین آر.پی.اِل هنگام ارسال بسته‌ها است. به‌عبارت دیگر، گره‌ای که میزان اعتماد پایینی به گره دیگری در درخت دارد، عملکرد آن را در ارسال بسته‌ها متناسب با قوانین آر.پی.اِل نمی‌داند. در واقع، اعتماد پایین نسبت به یک گره متناسب با وقوع یک رخداد غیرمعمول در ارسال بسته‌ها توسط آن گره است (پیام‌ها تنها در مسیرهای درخت دو.دَگ می‌توانند منتقل شوند). گفتنی است که این مشکل می‌تواند ناشی از برخی اتفاقات عادی شبکه‌های بی‌سیم مانند اتمام انرژی حس‌گرها و یا تداخل سیگنال‌ها (و نه از رفتار مخربانه) نیز باشد. برای رفع این تداخل سِک.تِراست قبل از اعلام رخداد حمله به بررسی اتمام باتری می‌پردازد [۱۲].

در روش سِک.تِراست علاوه‌بر ارسال نادرست بسته ها مشاهده هر کدام از رفتارهای فهرست زیر می‌تواند باعث کاهش بیشتر میزان اعتماد نسبت به یک گره شود [۱۲]:

- مشاهده هر گونه ناسازگاری در مقدار رتبه : مقدار رتبه باید با حرکت از ریشهٔ درخت به سمت برگ‌ها افزایش یابد.
- مشاهده ناسازگاری در موقعیت مکانی : یک گره مخرب ممکن است به جعل موقعیت و شناسه خود در درخت آر.پی.اِل دست بزند (این موضوع تحت عنوان حملاتی با عنوان سیبیل[2] شناخته می‌شود). این جعل نمی‌تواند موقعیت جغرافیایی گره مخرب را تغییر داده و بررسی موقعیت آن با توجه به اطلاعات موجود (هر گره می‌تواند موقعیت همسایگان و نشانی‌های آی.پی[3] آن‌ها را ذخیره کند) رفتار مخربانه را آشکار می‌کند.

در این روش اعتماد از ترکیب دو نوع مستقیم و غیر مستقیم به‌دست می‌آید. اعتماد مستقیم به معنی مشاهدات خود گره نسبت به همسایگان بلافصل خود (گره‌های والد و فرزند در درخت آر.پی.اِل) و اعتماد غیر مستقیم (اعتماد توصیه‌ای) از توصیه‌های سایر گره‌ها (گره هایی غیر از همسایگان) به دست خواهد آمد. کاهش مقدار اعتماد به یک حد مشخص منجر به تشخیص رفتار مخربانه خواهد شد. گفتنی است که اعتماد در این روش دارای نگاهی به گذشته بوده به این معنی که رفتار مخربانه حداقل تا مدتی در سیستم باقی مانده و فراموش نمی‌شود. در سِک.تِراست با گذر زمان و عدم مشاهدهٔ رفتار مخرب اعتماد به مقدار اولیه باز خواهد گشت [۱۲].

### ۲-۱-۴- روش تی.اِس.آر.اِف[4]

در سال ۲۰۱۳ روش بسیار مشابهی با سِک.تِراست در رابطه با شبکه‌های حس‌گر بی‌سیم تحت عنوان تی.اِس.آر.اِف توسط پژوهشگران ارائه شد [۱۳]. این روش به طور مستقیم برای پروتکل آر.پی.اِل طراحی نشده و با برخی تغییرات به آر.پی.اِل تعمیم پیدا کرده است. در این روش مفهوم اعتماد با توجه به ارسال صحیح پیام‌ها بر اساس جداول مسیریابی مشخص می‌شود. درواقع تطابق بیشتر با قواعد مسیریابی، اعتماد بیشتری را برای یک گره فراهم می‌سازد (و برعکس). تمام گره‌ها در تی.اِس.آر.اِف وظیفه نظارت و ارزیابی بر عملکرد همسایگان خود را بر عهده دارند که همین اطلاعات میزان اعتماد به آن‌ها را نیز مشخص می‌کند (اعتماد به‌صورت محلی و در هر گره مشخص می‌شود). در این روش نیز اعتماد به معنای عام از ترکیب دو نوع مستقیم و غیر مستقیم به دست می‌آید. بدیهی است که هنگام نزول میزان اعتماد نسبت به یک گره رفتار آن نیز به همان نسبت مخربانه در نظر گرفته می‌شود [۱۳].

[1] SecTrust
[2] Sybil
[3] Internet Protocol address
[4] Trust aware Secure Routing Framework in Wireless Sensor Network

## ۲-۴- راه‌حل‌های مبتنی بر احراز هویت[1]

در این روش‌ها، دسترسی غیرمجاز به منابع شبکه به‌کمک فرآیند احراز هویت محدود شده و یا به‌طور کامل از بین می‌رود. در ادامه به معرفی برخی از این روش‌ها خواهیم پرداخت.

### ۱-۲-۴- درخت مِرکِل[2]

این روش بر اساس یک رویکرد احراز هویت بوده که در آن هر گره اطلاعات شناسهٔ فرزندان خود را (در درخت دو.دَگ) به‌کمک یک تابع درهم‌سازی مشخص می‌کند. این اطلاعات در یک ساختار درختی با نام مِرکِل ثبت شده و به درخت دو.دَگ در آر.پی.اِل نظیر می‌گردد [۱۴]. درواقع اطلاعات هرگره در درخت مِرکِل حاصل درهم‌سازی اطلاعات فرزندان آن است.

با این ساختار گره‌ها می‌توانند اطلاعات شناسهٔ خود را به‌صورت یک‌طرفه درهم‌سازی کرده و به بررسی وجود آن در اطلاعات احراز هویت دریافتی (از طرف والد) بپردازند. در صورت عدم وجود اطلاعات یادشده، گره والد مخرب تشخیص داده خواهد شد. گفتنی است که این روش تنها در برابر حملاتی نظیر کرم‌چاله کارآمد است چرا که گره دوم در این حمله توسط فرزندان خود به‌درستی احراز هویت نخواهد شد [۱۳].

### ۲-۲-۴- روش وی.ای.آر.اِی[3]

اساس این روش زنجیرهٔ درهم‌سازی است. زنجیرهٔ درهم‌سازی روشی چند مرحله‌ای بوده که در هر قسمت آن یک فرآیند درهم‌سازی تا زمان برقراری یک شرط خاص تکرار می‌شود. به عبارت دیگر اطلاعات تولیدی در هر مرحله به‌عنوان حداقل یکی از ورودی‌های مرحله بعدی مورد استفاده قرار می‌گیرد. این روش می‌تواند با حملات "کاهش مقدار رتبه" و "تغییر شمارهٔ نسخه دو.دَگ" مقابله کند. برای این کار دو زنجیرهٔ درهم‌سازی مقدار رتبه و شمارهٔ نسخه پیام‌ها تعریف می‌شود. با فرض اینکه فهرست "$V_N,\ldots..V_0$" نشان‌دهنده زنجیر درهم‌سازی نسخه پیام‌ها از شماره صفر تا N (بزرگ‌ترین شماره در زنجیر درهم‌سازی) باشد آن‌گاه از طریق رابطهٔ (۱) می‌توان هر شماره از این فهرست را محاسبه کرد. در این رابطه h تابع درهم‌ساز، r عدد تصادفی و n بزرگ‌ترین شماره نسخه در زنجیر درهم‌سازی است [۱۵].

$$V_i = h^{n+1-i}(r) \qquad (۱)$$

در شماره نسخه i از این زنجیره مقادیر رتبه نیز با زنجیرهٔ درهم‌سازی دیگری به صورت $(R_{i,0},\ldots..,R_{i,l})$ نمایش داده می‌شود. مقدار $R_{i,l}$ در این فهرست (نشان‌دهنده مقدار رتبه یکم در شمارهٔ نسخه i می‌باشد) از طریق رابطهٔ (۲) قابل محاسبه است. در این رابطه $x_i$ عدد تصادفی است [۱۵].

$$R_{i,l} = h^{l+1}(x_i) \qquad (۲)$$

در این روش هنگام ایجاد درخت دو.دَگ، گره ریشه برخی اطلاعات اضافی را نیز منتشر می‌کند. با این اطلاعات گره‌های دریافت‌کننده (گره‌هایی که می‌توانند پیام‌های دریافتی را بازگشایی کند) به مقادیر $v_0$ (نخستین مقدار در رنجیر درهم‌سازی شماره نسخه‌ها) و $R_{l,1}$ (بزرگ‌ترین مقدار رتبه در زنجیره درهم‌ساز مربوط به شماره نسخه ۱) دسترسی پیدا می‌کنند (در ادامه، گره ریشه به انتشار مقادیر $V_i$ و $R_{I+1,l}$ نیز می‌پردازد). اطلاعاتی که به‌کمک آن امکان بررسی شمارهٔ نسخه‌ها برای گره‌های یادشده از طریق رابطهٔ (۳) فراهم می‌شود [۱۵].

$$h(V_i) = V_{i-1} \qquad (۳)$$

هر گره همچنین می‌تواند به بررسی مقدار رتبه مربوط به پدر خود در درخت دو.دَگ برای یک شمارهٔ نسخه خاص نیز بپردازد (با توجه به اطلاعات موجود در پیام‌ها). فرآیندی که به کمک آن جعل شمارهٔ نسخه دو.دَگ و تغییر مقدار رتبه با بررسی پیوستگی دو زنجیره معادلات (۱و۲) آشکار می‌شود [۱۵].

### ۳-۲-۴- روش تِرِیل[4]

مدتی پس از ارائه روش وی.ای.آر.اِی، محققان اقدام به بهبود آن در روشی تحت عنوان تِرِیل کردند. در این روش دو مشکل موجود در روش وی.ای.آر.اِی تحت عناوین "جعل هویت گره‌ها" و "قابلیت اجرای حملات تکرار" برطرف می‌شود [۱۶]. در این روش یک رمزنگاری زنجیروار به وی.ای.آر.اِی اضافه شده که به‌کمک آن می‌توان از جعل و ایجاد پیام‌های کنترلی ساختگی نیز جلوگیری کرد. درواقع، یک گره هنگام جعل هویت به فرآیند رمزنگاری نیاز داشته و در روش تِرِیل به‌کمک زنجیر رمزنگاری مذکور با این کار مقابله می‌شود. علاوه‌براین یک عدد تصادفی نیز به پیام‌های کنترلی اضافه شده تا با اجرای حملات تکرار مقابله کند [۱۶].

[1] Authentication
[2] Merkel
[3] Version Number and Rank Authntication in RPL
[4] Topology Authentication in RPL.

### ۴-۲-۴- روش بررسی مقدار رتبه

اساس این روش نیز زنجیرهٔ درهم‌سازی است. در این روش، گره ریشه به انتخاب یک عدد تصادفی و درهم‌سازی آن بر اساس یک تابع پیشفرض می‌پردازد. این مقدار در پیام دی.آی.او منتقل شده و هر گره با دریافت آن مجددا همان تابع درهم‌سازی را فراخوانی می‌کند؛ سپس، نتیجه مربوطه در قالب پیام‌های دی.آی.او منتشر شده و پس از گذشت زمان و هم‌گرایی درخت دو.دَگ، روابط (۴ و۵) برای هر گره شماره $N_i$ برقرار می‌گردد [۱۷].

$$P=\text{رتبه}^{\wedge}(N_i) \quad (۴)$$

$$\text{رتبه}^{\wedge}(N_i)=\text{رتبه}(N_i)-E_{path(i)} \quad (۵)$$

در این روابط، $\text{رتبه}^{\wedge}(N_i)$ به معنی تعداد درهم‌سازی‌های انجام شده بر روی مقدار $N_i$ بوده و مقدار $E_{path(i)}$ نیز نشان‌دهندهٔ تعداد گره‌های موجود در مسیر بین گره $N_i$ تا ریشه درخت است (در این روش فرض بر افزایش مقدار رتبه به‌صورت یک واحد در هر گام است).

گره ریشه پس از هم‌گرایی درخت دو.دَگ، شروع به ارسال مقدار $p_0$ (مقدار اولیهٔ زنجیر) به‌صورت همه‌پخشی می‌کند. با این کار هر گرهٔ موجود در درخت می‌تواند مقدار p را با توجه به $\text{رتبه}^{\wedge}(N_i)$ محاسبه نموده و با مقدار p دریافتی از پدر خود مقایسه نماید. فرآیندی که در آن برخی رفتارهای مخربانه تشخیص داده خواهند شد [۱۷]. به‌عنوان مثال، گره مخرب برای اجرای حملهٔ کاهش مقدار رتبه برای نزدیک‌ترشدن به ریشه (کاهش مقدار رتبه) باید از فراخوانی تابع درهم‌ساز سرباز زده و پیام مربوطه را بدون تغییر منتشر کند (دلیل این کار عدم دسترسی مهاجم به مقدار اولیه فرآیند درهم‌سازی در گره والد است). رفتاری که در مرحله دوم، پس از ارسال مقدار $p_0$ توسط ریشه تشخیص داده خواهد شد [۱۷].

## ۴-۳- روش‌های مبتنی بر ایدهٔ سیستم تشخیص نفوذ

روش‌های مبتنی بر ایدهٔ سیستم تشخیص نفوذ بر اساس تحلیل اطلاعات دریافتی از طرف گره‌های درخت به تشخیص رفتار مخربانه می‌پردازند. در این راستا به‌طورمعمول برخی تغییرات نیز در قوانین پروتکل آر.پی.اِل اعمال شده یا به آن افزوده می‌شود. در ادامه، یک پژوهش در این زمینه برای افزایش امنیت آر.پی.اِل معرفی شده است.

### ۴-۳-۱- روش اِس.وِل.تی.ای[1]

این روش یک سیستم تشخیص نفوذ برای اینترنت اشیاء بوده که از سه ماژول زیر تشکیل می‌شود. تمام این موارد به گره ریشه اضافه خواهند شد [۱۸].

- **6LowpanMapper**

این ماژول با ارسال یک پیام شروع به گره‌های درخت، از آن‌ها تقاضا می‌کند برخی اطلاعات را به‌صورت دوره‌ای برای این ماژول ارسال کنند. این اطلاعات شامل شماره گره، پدر ارجح، مقدار رتبه و فهرست همسایگان هستند. با ارسال دوره‌ای این موارد دید کاملی از درخت در ریشه شکل می‌گیرد.

- **ماژول تشخیص**

این ماژول بر اساس اطلاعات موجود در ماژول 6LowpanMapper به تشخیص ناسازگاری‌ها می‌پردازد. تفاوت بسیار زیاد مقدار رتبه در یک گره و همسایگان آن یکی از این ناسازگاری‌ها است. یکی دیگر از این موارد مربوط به زمانی است که تفاوت مقدار رتبه یک گره نسبت به پدرش از کمینه افزایش ممکن در یک گام کمتر باشد. در ماژول تشخیص اگر تعداد ناسازگاری‌های مربوط به یک گره بیش از آستانهٔ مشخصی باشد آن‌گاه آن گره مخرب در نظر گرفته شده و از درخت حذف خواهد شد (البته اِس.وِل.تی.ای یک‌بار به گره مربوطه قبل از حذف‌شدن فرصت مجدد می‌دهد). گفتنی است که در این ماژول ناسازگاری‌های دیگری از جمله تشخیص دسترس‌پذیری گره‌ها نیز بررسی می‌شود.

- **ماژول دیوارهٔ آتش**

در اِس.وِل.تی.ای یک ماژول دیواره‌ی آتش محدود جهت محافظت از گره‌های کم‌توان درخت دو.دَگ در برابر شبکه اینترنت وجود دارد [۱۸].

### ۴-۳-۲- تشخیص حمله کرم‌چاله با کمک ایده سامانهٔ تشخیص نفوذ

در این روش [۱۹]، هر گره دارای یک سری ماژول‌های خاص بوده که مسئولیت اندازه‌گیری قدرت سیگنال‌های دریافتی از طرف سایر گره‌های درخت دو.دَگ را دارد. این مقادیر پس از اندازه‌گیری به یک مقدار فاصله بر اساس رابطهٔ قدرت سیگنال و فاصله مکانی نظیر می‌شوند. درصورتی‌که دست‌کم یکی از این فاصله‌ها از بیشینه مقدار ممکن برای گره‌های همسایه (بر اساس قدرت سیگنال) بیشتر باشد، آن‌گاه حمله کرم‌چاله تشخیص داده خواهد شد (بیشینه قدرت سیگنال در اینترنت اشیا با توجه به

[1] SVELTE



[ DOR: 20.1001.1.24763047.1399.9.1.2.5 ]

ارتباطات بی‌سیم مقدار محدودی دارد). گره تشخیص دهنده سریعا مقدار شناسه، رتبه خود، پدر ارجح و فرزندان را برای گره ریشه در کنار قدرت سیگنال‌های دریافتی ارسال می‌کند. ریشه با دید کلی از درخت و با توجه به اطلاعات یادشده می‌تواند مکان فرستندهٔ سیگنال مخرب را نیز کشف کند.

در مرجع [۱۷] نیز روشی مشابه برای تشخیص حمله کرم‌چاله ارائه شده است. در این روش هر گره اطلاعات همسایگان خود را به‌صورت پیام دی.آی.او به گره ریشه خواهد فرستاد. گره ریشه با دریافت این اطلاعات به تعریف کاملی از توپولوژی درخت رسیده و این موضوع را به‌کمک پیام‌های تصدیق دی.آی.او (تصدیق دریافت پیام‌های دی.آی.او در پروتکل آر.پی.اِل) به گره‌های درخت منتقل می‌کند. این دستگاه‌ها به کمک اطلاعات دریافتی می‌توانند همسایگان واقعی خود را تشخیص داده و گره‌های مخرب در حمله کرم‌چاله را منزوی کنند [۲۰].

## ۴-۴- تغییر در پروتکل مسیریابی

بسیاری از پژوهش‌گران علت نگرانی‌های امنیتی پروتکل آر.پی.اِل را نوعی نقص در طراحی آن عنوان می‌کنند. آن‌ها معتقدند که با اصلاح پروتکل آر.پی.اِل دیگر نیازی به رویکردهای امنیتی نبوده و می‌توان دست‌کم با بخش زیادی از این موارد مقابله کرد. برخی از این بهبودها در ادامه آورده شده است.

### ۴-۴-۱- روش آستانه وفقی برای تشخیص ناسازگاری در آر.پی.اِل

این روش با برخی اصلاحات جزئی در فرآیند تعمیر پروتکل آر.پی.اِل سرعت واکنش به رفتار مخربانه را افزایش می‌دهد. درواقع پروتکل آر.پی.اِل هنگام رویارویی با برخی ناسازگاری‌ها به طور بهینه از خود واکنش نشان نداده که دلیل آن انتخاب نامناسب مقدار آستانه، برای شروع فرآیند تعمیر هنگام دریافت بسته‌های ناسازگار (در درخت دو.دَگ) است. در روش "آستانه وفقی" با تغییر پویای این مقدار بر اساس شرایط شبکه، واکنش به ناسازگاری‌ها تا حد بالایی بهبود پیدا می‌کند؛ بنابراین گره مخرب فرصت محدودتری را برای دست‌یابی به اهداف خود دارد [۲۱].

### ۴-۴-۲- روش ناکامی والدین [1]

در این روش عدم دریافت تعداد مشخصی از پیام‌های داده و کنترلی (از طرف گره‌های درخت دو.دَگ) در ریشه به معنای رخداد حمله چاهک تفسیر می‌شود (البته این فرآیند باید در یک بازهٔ زمانی محدود و مشخص اتفاق بیفتد). پس از تشخیص حمله مربوطه، گره ریشه اقدام به ارسال فهرستی از گره‌هایی که هیچ پیامی از آن‌ها دریافت نشده می‌کند. این فهرست در قالب پیام‌های دی.آی.او منتشر شده و گره‌های درخت را از نقطه احتمالی حمله در درخت با خبر می‌سازد. به این ترتیب هنگام تعمیر محلی درخت دو.دَگ امکان حذف گره مخرب وجود دارد [۱۷].

## ۴-۵- تطبیق مکانیسم‌های امنیتی در سایر لایه‌ها جهت محدود کردن حملات لایهٔ شبکه

برخی دیگر از پژوهشگران حوزهٔ امنیت اطلاعات و شبکه‌های رایانه‌ای ناسازگاری راه‌کارهای موجود و مشهور با پروتکل آر.پی.اِل را غیرممکن نمی‌دانند. به این ترتیب سعی بر تطبیق پروتکل‌های یادشده با آر.پی.اِل کرده تا بتوانند از مزایای آن‌ها در رفع نگرانی‌های امنیتی این پروتکل نیز استفاده کنند. در ادامه به معرفی یکی از این روش‌ها پرداخته شده است.

### ۴-۵-۱- پروتکل سی.او.اِی.پی[2] فشرده شده

در این روش سعی بر استفاده از سازوکار فشرده‌سازی پروتکل 6lowpan (پروتکلی برای تطبیق نسخهٔ ۶ پروتکل آی.پی با شبکه‌های کم‌توان دارای پهنای باند پایین) برای سازگاری رویکردهای معروف امنیتی از جمله دی.تی.اِل.اِس [3] با اینترنت اشیا شده است. امری که می‌تواند برخی حملات لایهٔ شبکه را نیز محدود سازد [۲۲]. از جملهٔ این موارد می‌توان به حملات تکرار و قطعه‌بندی بسته‌ها اشاره کرد.

گفتنی است که در سال‌های اخیر دانشمندان تلاش بسیار زیادی برای سازگاری سامانه‌های تشخیص نفوذ امروزی با اینترنت اشیا کرده‌اند. برای پوشش خلاء سخت‌افزاری موجود، فناوری‌های بسیاری از جمله رایانش مه، شبکه‌های نرم‌افزار محور برای ترکیب با اینترنت اشیا پیشنهاد شده است. نتایج این پژوهش‌ها تا کنون در مقابل حملات مربوط به پروتکل مسیریابی آر.پی.اِل مشخص نیست. همچنین قابلیت اجرایی و هزینهٔ این ترکیب در همه جا امکان‌پذیر به نظر نمی‌رسد [۲۵,۲۴,۲۳].

[1] Parent Fail-Over

[2] Constrained Application Protocol

[3] Datagram Transport Layer Security





[ DOR: 20.1001.1.24763047.1399.9.1.2.5 ]

(جدول-۱): خلاصه وضعیت امنیتی پروتکل آر.پی.اِل

| نام حمله | راه‌حل‌های موجود |
|---|---|
| سیل.آسا | ناموجود |
| سرریز جداول مسیریابی | ناموجود |
| افزایش مقدار رتبه | بررسی مقدار رتبه- سِک.تِراست- وی.ای.آر.ای- تِرِیل |
| ناسازگاری در دو.دَگ | ناموجود |
| افزایش شماره نسخه | وی.ای.آر.ای- تِرِیل |
| کرم‌چاله | مرکل,کرم‌چاله-سیستم تشخیص نفوذ |
| ناسازگاری‌دی.آی.او | آستانهٔ وفقی |
| انتخاب بدترین والد | ناموجود |
| جعل مسیر | ناموجود |
| حملات سیاه‌چاله و چاهک | سِک.تِراست- ناکامی والدین- اِس.وِل.تی.ای |
| حملات تکرار | سی.او.اِی.پی |
| کاهش مقدار رتبه | اِس.وِل.تی.ای- سِک.تِراست ,تِرِیل-بررسی مقدار رتبه |
| جعل هویت | سِک.تِراست-اِس.وِل.تی.ای |
| شنود و تحلیل ترافیک | رمزنگاری- سی.او.اِی.پی |

در جدول (۱) می‌توانیم تمام نگرانی‌های امنیتی و راه‌حل‌های ارائه‌شده برای پروتکل آر.پی.اِل تا به امروز را مشاهده کنیم. در جدول (۲) نیز نقاط قوت و ضعف راه‌حل‌های موجود بر اساس دسته‌بندی شکل (۱) آورده شده است. همان‌طور که مشاهده می‌شود این موارد بر اساس دسته‌بندی یادشده اشتراکات قابل توجهی دارند. به‌عنوان مثال بیش‌تر روش‌های بر اساس رویکرد احراز هویت (دارای بیشترین تعداد در جدول) به دقت بالایی در تشخیص رفتار مخرب رسیده‌اند که از ماهیت رویکرد یادشده سرچشمه می‌گیرد. البته گفتنی است که سربار پردازشی و واکنش به‌نسبه دیر به رفتار مخربانه نیز در این نوع راه‌حل‌ها به چشم می‌خورد.

## ۵- نتیجه‌گیری و پیشنهادها

با توجه به مطالب بررسی‌شده در این پژوهش بخش قابل توجهی از نگرانی‌های امنیتی پروتکل آر.پی.اِل تاکنون دارای دست‌کم یک راه‌حل بوده اما بسیاری از آن‌ها نیز هم‌چنان هیچ‌گونه راه‌حلی ندارند. مواردی که می‌توانند زمینه مطالعه پژوهش‌گران باشند. علاوه‌براین راه‌حل‌های موجود نیز در کنار نقاط قوت خود دارای ضعف‌های قابل توجهی نیز هستند که زمینه را برای پژوهش جهت ارائه یک راه‌حل بهینه و کارآمدتر فراهم می‌سازند. البته بخش عمده‌ای از این نقاط ضعف بر اساس اشتراکات راه‌حل‌های مربوط به هر دسته ناشی از اساس آن رویکرد است؛ لذا ارائه راه‌حل‌های جدید در قالب دسته‌های یادشده می‌تواند این ضعف‌ها را نیز شامل شود.

به‌طورکلی برای پژوهش در زمینه امن‌سازی پروتکل آر.پی.اِل با توجه به شرایط دستگاه‌های اینترنت اشیا بررسی رویکردهای جدید خارج از دسته‌بندی ارائه‌شده یا انتخاب دسته‌ای با نقاط ضعف کمتر پیشنهاد می‌شود.

(جدول -۲): بررسی نقاط قوت و ضعف راه‌حل‌های موجود

| ردیف | دسته | راه‌حل | نقاط قوت | نقاط ضعف |
|---|---|---|---|---|
| ۱ | مبتنی بر اعتماد | سِک.تراست | مقابله با طیف وسیعی از نگرانی‌ها- واکنش سریع به رفتار مخرب- وجود دید واحد نسبت به شبکه (مقابله با تعدد اطلاعات) | سربار ارتباطی و پردازشی بالا- امکان وجود اطلاعات متعدد در مورد یک گره در شبکه |
| ۲ | | تی.اِس.آر.اِف | | |
| ۳ | مبتنی بر احراز هویت | مرکل | سازگاری مناسب با آر.پی.اِل-واکنش سریع به رفتار مخرب | سربار پردازشی بالا-امکان خطا در تشخیص هنگام اجرای حمله کرم‌چاله با پیام‌های DAO -مقابله با تنها یک نگرانی امنیتی- عدم بررسی و آنالیز مناسب |
| ۴ | | وی.ای.آر.اِی | دقت بالا در تشخیص | واکنش نسبتا کند به رفتار مخربانه-سربار پردازشی- مقابله با تعداد بسیار کمی از نگرانی‌های امنیتی - عدم بررسی و آنالیز مناسب |
| ۵ | | تِرِیل | | واکنش نسبتا کند به رفتار مخربانه-سربار پردازشی- عدم بررسی و آنالیز مناسب |
| ۶ | | بررسی مقدار رتبه | | واکنش نسبتا کند به رفتار مخربانه-سربار پردازشی- مقابله با تعداد بسیار کمی از نگرانی‌های امنیتی - عدم بررسی و آنالیز مناسب |



[ DOR: 20.1001.1.24763047.1399.9.1.2.5 ]

| | | | | |
|---|---|---|---|---|
| ۷ | مبتنی بر ایده سیستم تشخیص نفوذ | اِس.وِل.تی.ای | بررسی و آنالیز روش در سطح بالا- وجود دید واحد نسبت به شبکه (مقابله با تعدد اطلاعات)- مقابله با طیف وسیعی از نگرانی‌ها | واکنش نسبتا کند به رفتار مخربانه-سربار پردازشی |
| ۸ | | تشخیص کرم‌چاله با سیستم تشخیص نفوذ | امکان تشخیص مکان دقیق گره مخرب در درخت-دقت مناسب در تشخیص حمله | سربار ارتباطی- مقابله با تعداد بسیار کمی از نگرانی‌های امنیتی – پیاده‌سازی دشوار |
| ۹ | تغییر در پروتکل مسیریابی | آستانه وفقی | پیاده‌سازی ساده-سربار ارتباطی و پردازشی کم | واکنش نسبتا کند به رفتار مخربانه-دقت نامناسب در تشخیص- مقابله با تعداد بسیار کمی از نگرانی‌های امنیتی |
| ۱۰ | | ناکامی والدین | | |
| ۱۱ | تطبیق سازوکارهای امنیتی مشهور با پروتکل آر.پی.اِل | سی.او.اِی.پی فشرده | مزایای استفاده از روش‌های مشهور از جمله نیاز به بررسی‌های امنیتی کمتر و پیاده‌سازی آسان‌تر | سربار پردازشی- مقابله با تعداد بسیار کمی از نگرانی‌های امنیتی- مشکلات پیاده‌سازی- امکان آسیب‌پذیری به علت فشرده‌سازی پروتکل‌های مشهور |

## ۶- مراجع


[1] M Ammar, G. Russello and B. Crispo, “Internet of Things: A survey on the security of IoT frameworks”, Journal of Information Security and Applications Volume 38, February 2018, Pages 8-27, 2018 , DOI=https://doi.org/10.1016/j.jisa.2017.11.002

[2] J. Granjial, E. Monteiro, and J. Silva,”Security for the Internet of Things: A survey of Existing Protocols and Open Research issues." IEEE Communications Surveys & Tutorials , Volume: 17, Issue: 3. 2015 , DOI=10.1109/COMST.2015.2388550

[3] V. Adat and B. B. Gupta, “Security in Internet of Things: issues, challenges, taxonomy, and architecture”, Telecommunication Systems Volume 67, Issue 3, pp 423–441, 2018, DOI= https://doi.org/10.1007/s11235-017-0345-9

[4] L. Wallgren, S. Raza and T. Voigt,"Routing Attacks and Countermeasures in the RPL-BasedInternet of Things", International Journal of Distributed Sensor NetworksVolume 2013, Article ID 794326, 2013, DOI=http://dx.doi.org/10.1155/2013/794326

[5] PO. Kamgueuab, E. Natafa and T. Djotio Ndieb, "Survey on RPL enhancements: A focus on topology, security and mobility", 2018, Computer Communications Journal, Volume 120, May 2018, Pages 10-21- DOI=https://doi.org/10.1016/j.comcom.2018.02.011

[6] S. Mangelkar, S. N. Dhage and A. V. Nimkar, "A comparative study on RPL attacks and security solutions," 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, 2017, pp. 1-6.

[7] A. Kamble, V. S. Malemath and D. Patil, "Security attacks and secure routing protocols in RPL-based Internet of Things: Survey," 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI), Pune, 2017, pp. 33-39.

[8] O. Iova, P. Picco, T. Istomin and C. Kiraly, "RPL: The Routing Standard for the Internet of Things... Or Is It?," in IEEE Communications Magazine, vol. 54, no. 12, pp. 16-22, December 2016, DOI= 10.1109/MCOM.2016.1600397CM

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

[10] A. Mayzaud, R. Biddonel, and I. Chrisment, “ A Taxonomy of Attacks in RPL-based Internet of Things” .International Journal of Network Security, IJNS. 2016, Link= https://hal.inria.fr/hal-01207859

[11] A Raoof, A. Matrawy and C. h. Lung, “Routing Attacks and Mitigation Methods for RPL-Based Internet of Things” IEEE Communications Surveys & Tutorials, 2018, DOI= 10.1109/COMST.2018.2885894

[12] D. Airehrour, J. Gutierrez, S.K. Ray, “SecTrust-RPL: A secure trust-aware RPL routing protocol for Internetof Things”, Future Generation Computer Systems 93 (2019) 860–876. 2019, DOI= https://doi.org/10.1016/j.future.2018.03.021

[13] J. Duan, D. Yong, and h. Zhu, "TSRF: A Trust Aware Secure Routing Framework in Wireless Sensor Network". Intenational Journal of Distributed Sensor Network: 15. 2014, DOI= 10.1155/2014/209436

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




[ DOR: 20.1001.1.24763047.1399.9.1.2.5 ]

Conference on Volume 25, Issue 5. 2013, DOI=https://doi.org/10.1002/sec.1023

[15] A. Dvir, T. Holczer, and L. Buttyan,"VeRA - Version Number and Rank Authentication in RPL". Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on. 2011, DOI=10.1109/MASS.2011.76

[16] M. Landsmann, M. Wahlisch and T. C. Schmidt, "Topology Authentication in RPL," 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Turin, 2013, pp. 73-74.

[17] K. Weekly and K. Pister, "Evaluating sinkhole defense techniques in RPL networks," 2012 20th IEEE International Conference on Network Protocols (ICNP), Austin, TX, 2012, pp. 1-6, DOI=10.1109/ICNP.2012.6459948

[18] S. Reza, L. Wallgren, and T. Voigt,"SVELTE: Real-time intrusion detection in the Internet of Things". Ad Hoc Networks Volume 11, Issue 8, November 2013, Pages 2661-267. 2013, DOI =https://doi.org/10.1016/j.adhoc.2013.04.014

[19] S. Deshmukh-Bhosaleab and S. Sonavanec, "A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things", Procedia ManufacturingVolume 32, 2019, Pages 840-847. 2019, DOI= https://doi.org/10.1016/j.promfg.2019.02.292

[20] V. Neerugatti and A. Rama Mohan Reddy, "Acknowledgement Based Technique for Detection of the Wormhole Attack in RPL Based Internet of Things Networks", Asian Journal of Computer Science and Technology Vol.8 No.S3, 2019, pp. 100-104, 2019

[21] 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

[22] S. Raza, H. Shafagh, K. Hewage, R. Hummen and T. Voigt, "Lithe: Lightweight Secure CoAP for the Internet of Things," in IEEE Sensors Journal, vol. 13, no. 10, pp. 3711-3720, Oct. 2013.

[23] D. Airehrour, J. Gutierrez, S.K. Ray, "A lightweight trust design for IoT Routing,in", IEEE 14th Intl Conf on Pervasive Intelligence and Computing, 2016,pp. 552–557.

[24] X. Anita, M. L. Manickam, and M. A. Bhagyaveni,"Two-Way Acknowledgment-Based Trust Framework forWireless Sensor Networks". International Journal of Distributed Sensor Networks: 15. 2014, DOI=10.1155/2013/952905. 2016

[25] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani,"New Trust Metric for the RPL Routing Protocol."2017 8th International Conference on Information and Communication Systems (ICICS). 2017 pp. 328-335, DOI=10.1109/IACS.2017.7921993

[26] D. Airehrour, J. Gutierrez, and S. Kumar Ray,"Secure routing for internet of things: A survey". Journal of Network and Computer Application: 14. 2016, DOI =https://doi.org/10.1016/j.jnca.2016.03.006

[27] Q. Jing, A. V. Vasilakos, J. Wan, J.,Lu, and D. Qiu, "Security of Internet of Things: Prespectives and challenges ". Wireless Networks , Volume 20, Issue 8, pp 2481–2501. 2016, DOI= 10.1007/s11276-014-0761-7

[28] P. O. Kamgueu, E. Nataf, T. D. Ndie, "Survey on RPL enhancements: A focus on topology, security and mobility", Computer CommunicationsVolume 120, May 2018, Pages 10-21

[29] T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, and M. Richardson, "A Security Threat Analysis for Routing Protocol for Low-power and Lossy Networks (RPLs)", 2015, RFC 7416, Internet Engineering Task Force.

[30] K. Iuchi, T. Matsunaga, K. Toyoda and I. Sasase, "Secure parent node selection scheme in route construction to exclude attacking nodes from RPL network," 2015 21st Asia-Pacific Conference on Communications (APCC), Kyoto, 2015, pp. 299-303.

[31] J. Hui and JP. Vasseur, "The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams", 2012, RFC 6553 (ProposedStandard), Internet Engineering Task Force

[32] A. Rehman, M. M. Khan, M. A. Lodhi and F. B. Hussain, "Rank attack using objective function in RPL for low power and lossy networks," 2016 International Conference on Industrial Informatics and Computer Systems (CIICS), Sharjah, 2016, pp. 1-5.

**محمد پیشدار** دانش‌آموخته رشتهٔ فناوری اطلاعات گرایش شبکه‌های رایانه‌ای از دانشگاه بوعلی سینا است. وی تا کنون دو مقالهٔ علمی را در نشریات بین‌المللی و داخلی در حوزه امنیت شبکه به چاپ رسانه است. ایشان دو کتاب در زمینهٔ امنیت اطلاعات را چاپ کرده و در حال حاضر کارشناس رایانش امن در مرکز آپای استان قزوین است.

**یونس سیفی** دوره کارشناسی خود در رشته مهندسی نرم‌افزار را در سال ۱۳۷۶در دانشگاه صنعتی شریف به پایان رسانید؛ سپس دوره کارشناسی ارشد مهندسی نرم‌افزار خود را در دانشگاه صنعتی امیرکبیر در سال ۱۳۸۰ خاتمه داد؛ و به‌عنوان عضو هیأت علمی در دانشگاه بوعلی سینا مشغول به تدریس و پژوهش شد. ایشان دکترای خود را در مهندسی فناوری اطلاعات گرایش امنیت شبکه در سال ۱۳۹۲ از دانشگاه صنعتی کوئینزلند استرالیا کسب کرد.

**مظفر بگ محمدی** دانشیار رشتهٔ رایانه و دانش‌آموختهٔ دانشگاه تهران است. ایشان تا کنون بیش از ۲۰ مقاله در نشریات بین المللی و داخلی در حوزه‌های مختلف شبکه و رایانه به چاپ رسانده و به‌علاوه، ایشان سه کتاب در زمینه‌های برنامه‌نویسی و شبکه‌های ر ایانه‌های ترجمه و چاپ کرده است. در حال حاضر، ایشان عضو هیأت علمی دانشگاه ایلام هستند.



[ DOR: 20.1001.1.24763047.1399.9.1.2.5 ]