بررسی حمله سرکوب DIO در مسیریابی اینترنت اشیاء

محمدحسن یزدانی[1]، بهرنگ برکتین*[2]

[1]گروه کامپیوتر، موسسه آموزش عالی جهاد دانشگاهی واحد صنعتی اصفهان

[2]دانشکده مهندسی کامپیوتر، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران

1 hasanyazdani74@gmail.com

2 behrang_barekatain@yahoo.com

چکیده–اینترنت اشیا مفهومی جدید در دنیای فناوری و ارتباطات است. به‌صورت خلاصه اینترنت اشیاء فناوری مدرنی است که در آن برای هر موجودی (انسان، حیوان یا اشیاء) قابلیت ارسال داده از طریق شبکه‌های ارتباطی، اعم از اینترنت یا اینترانت، فراهم می‌گردد. 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 فناوری باعث ایجاد چالش‌های امنیتی از قبیل حریم خصوصی، محرمانگی اطلاعات و اعتماد می‌گردد. شبکه‌های اینترنت اشیا در برابر انواع مختلف حملات آسیب‌پذیر هستند که حمله DIO یکی از مخرب‌ترین این حملات به شمار می‌آید. حمله‌ی سرکوب DIO، برخلاف دیگر حملات نیازی به سرقت کلیدهای رمزنگاری از گره‌های مشروع ندارد. این حمله، سرویس مسیریابی را به‌شدت تضعیف می‌کند. در این مقاله سعی می‌شود روی مفهوم اینترنت اشیا پرداخته و سپس مدل حمله DIO به‌صورت دقیق موردبررسی قرار می‌گیرد.

کلید واژه: پروتکل RPL، حمله DIO، اینترنت اشیا، نمودار DODAG، الگوریتم Trickle

1- مقدمه

اینترنت نه‌تنها توسط افراد، بلکه توسط دستگاه‌هایی هوشمند نیز مورداستفاده قرار می‌گیرد. دستگاه‌های هوشمند، دستگاه‌هایی هستند که قابلت محاسبه داشته و می‌توانند در کنار سایر فعالیت‌ها، اطلاعات را در شبکه منتشر کرده و دریافت کنند. به دلیل پیشرفت در فناوری و کاهش دستگاه‌های محاسباتی، دستگاه‌های هوشمند تبدیل به دستگاه‌های به‌صرفه‌تر و قابل‌دسترس‌تری در نزد عموم شده‌اند. مفهوم اینترنت اشیاء[1] بر اساس همین پیشرفت‌ها پدید آمده است. اینترنت اشیاء یک شبکهٔ مرکب و باز است که دستگاه‌های ناهمگون به نام اشیاء یا چیزهای هوشمند نظیر لوازم، کتاب‌ها و ماشین‌ها را گرد هم آورده و باهم ترکیب کرده است و سایر اشیاء معمولاً به محاسبات مربوط به کامپیوتر، حسگرها، تلفن‌های همراه و غیره تعلق ندارند. این دستگاه‌ها به دنبال به اشتراک‌گذاری اطلاعات، داده‌ها و منابع بوده و نسبت به شرایط و تغییرات محیطی عمل و عکس‌العمل نشان می‌دهند[1].

به دلیل افزایش دستگاه‌های هوشمند و سیار بودن و تحرک بعضی از این دستگاه‌ها،اینترنت اشیا در معرض آسیب‌پذیری‌های متعددی قرار می‌گیرد که ممکن است در یک زیر ساختارهای ارتباطی متغیر به وجود بیایند. اکثر دستگاه‌های اینترنت اشیا شامل ویژگی‌هایی نظیر منابع محاسباتی محدود (مانند انرژی پایین)پردازش ظرفیت محدود، ذخیره‌سازی، فقدان ارتباط در بین

[1] Internet of things

لینک‌ها و غیره می‌شوند. این محدودیت‌ها تبدیل به نقاط ضعف اینترنت اشیا در برابر حمالت مسیریابی می‌شود[2].

دانشمندان در سال ۲۰۱۲ پروتکل مسیریابی RPL [1]را به‌عنوان 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 آسیب‌پذیری‌های متعدی نیز برای آن ارائه‌شده است. امروزه برخی از این نگرانی‌ها همچنان باقی‌مانده و راه‌حلی برای آن‌ها ارائه نشده است. در این مقاله، ما حمله‌ی سرکوب DIO[2] که می‌تواند سرویس مسیریابی در RPL را به‌شدت تخریب کند، ارائه می‌دهیم. حمله‌ی سرکوب DIO، باعث ایجاد گره‌های قربانی برای سرکوب انتقال پیام‌های DIO (که پیام‌های RPL موردنیاز برای ساختن توپولوژی مسیریابی هستند) می‌شود. این امر منجر به تخریب کلی کیفیت مسیرها می‌شود که درنهایت می‌تواند به تکه‌تکه‌شدن شبکه بیانجامد. برخلاف سایر حملاتی که در مقالات و کتب به آن‌ها اشاره‌شده است، حمله‌ی سرکوب DIO، برای تولید پیام‌های RPL جعلی، به دشمن[3] نیاز ندارد. کافی است که او به‌صورت دوره‌ای، پیام‌هایی که قبلاً شنیده شدند را بازپخش کند؛ بنابراین این حمله می‌تواند بدون سرقت کلیدهای رمزنگاری از گره‌های مشروع، برقرار شود. حمله‌ی سرکوب DIO، از فن بازپخش (که یک فن حمله‌ی کلاسیک است) برای یک هدف کاملاً متفاوت استفاده می‌کند. از سوی دیگر، در حمله‌ی سرکوب DIO، برای این منظور مورداستفاده قرار می‌گیرد که قربانی را متقاعد کند که اطلاعات مسیریابی‌ای که در حال ارسال شدن است، چندین بار توسط گره‌های دیگر ارسال‌شده است. این حمله، سرویس مسیریابی را به‌شدت تضعیف می‌کند و هزینه‌ی انرژی آن به‌مراتب کمتر از یک حمله‌ی jamming است[3].

ادامه مقاله بدین‌صورت سازماندهی‌شده است: بخش دوم به معرفی پروتکل RPL و بخش سوم به تشریح نمودار DODAG و بخش چهارم به تشریح الگوریتم Trickle اختصاص داده‌شده است. در بخش پنجم به بررسی حملات در پروتکل RPL و در بخش ششم به بررسی اجمالی حمله DIO پرداخته‌شده است؛ و درنهایت نتیجه‌گیری مقاله در بخش هفتم ارائه‌شده است.

2- پروتکل RPL

با معرفی ایده اینترنت اشیا مهم‌ترین نگرانی بر سر راه گسترش این فناوری عدم سازگاری روش‌ها و یا پروتکل‌های رایج ارتباطی با آن به نظر می‌رسید. مهم‌ترین دلیل این ناسازگاری‌ها وجود ویژگی‌های خاص در اینترنت اشیاء ازجمله توان پردازشی، ذخیره‌سازی و منبع انرژی ضعیف[4] در دستگاه‌های این فنّاوری است.دانشمندان برای حل این مشکل به فکر تطبیق پروتکل‌های رایج ارتباطی با اینترنت اشیاء و یا ارائه پروتکل‌های جدید خاص این فناوری افتادند. در همین راستا در سال ۲۰۰۵ فناوری IEEE 802.15.4 که مخصوص لایه فیزیکی[5] و انتقال داده در شبکه‌های کم‌توان با نرخ بالا در گم‌شدن بسته‌ها است طراحی شد. دانشمندان این فنّاوری را برای لایه فیزیکی و انتقال داده پشته پروتکلی IPv6[6] اینترنت اشیاء نیز مناسب دیدند؛ اما در لایه شبکه، ویژگی‌های خاص در دستگاه‌های اینترنت اشیاء و علاوه بر آن مدل ترافیکی خاص (معمولاً از اشیا به سمت یک گره مشخص) دانشمندان را به سمت طراحی پروتکل‌های جدید و سازگار با این فناوری حرکت داد[3].

دانشمندان در سال ۲۰۱۲ پروتکل مسیریابیRPL را به‌عنوان گزینه سازگار با لایه شبکه در اینترنت اشیاء طراحی و ارائه نمودند. پس از ارائه این پروتکل و اهمیت امنیت در اینترنت اشیا، پژوهشگران بسیاری به بررسی امنیتی آن پرداخته و آسیب‌پذیری‌های متعدی نیز برای آن ارائه‌شده است.

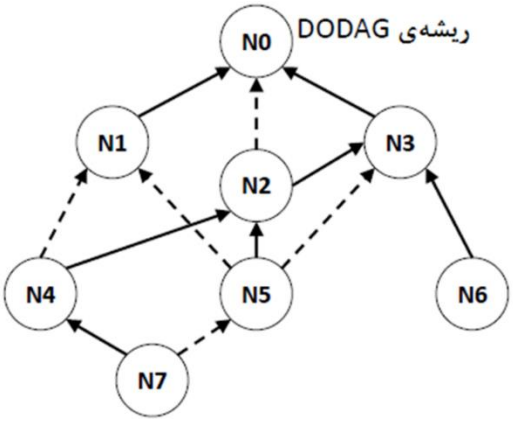
امروزه برخی از این نگرانی‌ها همچنان باقی‌مانده و راه‌حلی برای آن‌ها ارائه نشده ست[3].

[1] Routing Protocol for Low-Power and Lossy Networks
[2] DODAG information object
[3] Adversary
[4] Low-Power and Lossy Networks
[5] Physical layer
[6] Internet protocol version 6

6LoWPAN[1]پروتکل IPv6 است که برای ابزارهای کم‌توان و باقابلیت پردازش محدود طراحی‌شده است. این گروه چگونگی کپسوله کردن[2] و سازوکار فشرده‌سازی سرآمد آن را تعریف کرده است. به‌این‌ترتیب بسته‌های IPv6 می‌توانند روی شبکه‌های کم توان ومحدود ارسال یا دریافت شوند. برای، برآورده کردن این الزامات لایه انطباق 6LoWPANروش‌هایی مانند قطعه‌قطعه کردن بسته‌ها و فشرده‌سازی سربار را بکار می‌گیرد این لایه در فرستنده بسته را قطعه‌قطعه[3] می‌کند و در گیرنده مجدداً آن را سوار می‌کند[4].

3- نمودارDODAG

ساختار پایه در پروتکل RPL نمودار DODAG[4]است که کنترل‌کننده یا ریشه در مبدأ آن قرارگرفته است. در حالت پایدار هر مسیریاب شبکه حسگر بیسیم بر روی مسیر به سمت ریشه نمودار یک مجموعه از والدهای ثابت و یک والد برگزیده دارد. (شکل دو) هر مسیریاب که قسمتی از نمودار DODAGاست (والد خود را انتخاب کرده است) اقدام به ارسال پیام‌های کنترلی DIO می‌کند و رتبه‌ی خودش را درون نمودار مشخص می‌کند که نشان‌دهنده‌ی موقعیتش درون شبکه نسبت به ریشه است. به‌محض دریافت پیام‌های DIO یک گره مقدار رتبه‌ی خودش درون شبکه را محاسبه می‌کند که این رتبه باید از رتبه‌ی تمام والدهای خودش بزرگ‌تر باشد و بعدازآن با استفاده از تایمر قطره شروع به ارسال پیام‌های DIO می‌کند. درنتیجه تشکیل نمودار از ریشه شروع وبه تدریج کل شبکه را پوشش می دهد [4].



شکل ۲: مثال DODAG. پیکان‌های پیوسته، به والدین ارجح اشاره دارند، پیکان‌های خط‌چین به والدین دیگر در مجموعه والدین اشاره دارند[3].

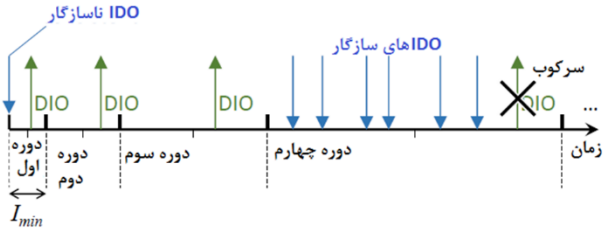
4- الگوریتم Trickle

انتشار DIO ها، توسط الگوریتم Trickle تنظیم می‌شود. این الگوریتم در ابتدا برای شایعات مؤدبانه[5] در شبکه‌های بی‌سیم، برای کاهش مصرف توان گره‌ها با به حداقل رساندن پیام‌های زائد و با سازگاری پویای نرخ انتقال، طراحی‌شده بود. به‌طور خاص، میزان انتشار DIO ها، با توجه به ثبات اطلاعات مسیریابی تنظیم می‌شود. اگر اطلاعات موجود در DIO از جانب همسایگان، با اطلاعات مسیریابی داخلی سازگار باشد، نرخ انتشار[6] کاهش می‌یابد. در غیر این صورت، اگر DIO های ناسازگار دریافت شوند، نرخ انتشار افزایش می‌یابد. RPL شرایطی را برای تعیین این‌که آیا یک DIO، سازگار است یا خیر، مشخص می‌کند. برای مثال، یک DIO که تغییری را در مجموعه والدین، والدین ارجح و فاصله تا ریشه، ایجاد نمی‌کند، باید سازگار در نظر گرفته شود[3].

الگوریتم Trickle، زمان را به دوره‌های با طول متغیر تقسیم می‌کند (شکل 2). گره، انتقال یک پیام DIO در یک‌زمان تصادفی t در نیمه‌ی دوم هر دوره را برنامه‌ریزی می‌کند. تا t، گره به پیام‌ها گوش می‌دهد و DIOهای سازگار را ردیابی می‌کند. در زمان t، پیام DIO برنامه‌ریزی‌شده، تنها در صورتی پخش می‌شود که تعداد DIOهای سازگار دریافت شده در دوره‌ی فعلی، کمتر از یک آستانه‌ی سرکوب (k) مشخص باشد. در غیر این صورت، انتقال

[1] IPv6 over Low-Power Wireless Personal Area Networks
[2] Encapsulation
[3] Segment
[4] Destination Oriented Directed Acyclic Graph
[5] Polite Gossiping
[6] Emission Rate

DIO سرکوب می‌شود که در دوره‌ی چهارم در مثال شکل 2 نشان داده‌شده است. در پایان دوره، اگر فقط DIOهای سازگار دریافت شده باشند، طول دوره بعدی دو برابر می‌شود تا زمانی که حداکثر طول Imax به دست آید. در هر زمان، اگر یک DIO ناسازگار دریافت شود، دوره‌ی فعلی متوقف می‌شود و الگوریتم دوباره از یک دوره‌ی حداقل طول Imin آغاز می‌شود. مکانیزم سرکوب DIO، یک بخش ضروری از الگوریتم Trickle است، زیرا مقیاس ترافیک DIO را به‌صورت لگاریتمی با تعداد گره‌ها می‌کند. غیرفعال کردن این مکانیزم توصیه نمی‌شود، زیرا می‌تواند منجر به تراکم شبکه‌ها شود[5] .



شکل 2. مثال الگوریتم Trickle با k=6. پیکان‌های رو به بالا، نشان‌دهنده‌ی DIO های ساطع‌شده هستند؛ پیکان‌های رو به پایین، نشان‌دهنده‌ی DIO های دریافت شده هستند؛ و ضربدر سیاه، نشان‌دهنده‌ی یک سرکوب DIO است.

5- بررسی حملات پروتکل RPL

دویر و همکاران [6]، تأثیر حمله کودال خاکستری را موردمطالعه قراردادند که در آن، یک گره مخرب، پیام‌هایی RPL را به شبکه تزریق می‌کند که حامل اطلاعات جعلی است و ترافیک را از گره‌های صادقِ اطراف جذب می‌کند. سپس گره مخرب می‌تواند مقدار زیادی از ترافیک را قطع کند و یا از بین ببرد. میزاد و همکاران [7]، تأثیر حمله‌ی DODAG Version که اثر مشابهی دارد را موردمطالعه قراردادند. شماره نسخه توسط ریشه برای کنترل فرآیند تعمیرDODAG استفاده می‌شود. هر پیام DIOشماره نسخه را به همراه دارد به‌طوری‌که در مواردی که نودهای دریافت‌کننده بخشی از یک نسخه DODAG قدیمی باشند، می‌توانند با شماره نسخه جدید به نمودار جدید بپیوندند. مقدار قدیمی‌تر نسخه تبلیغ‌شده در پیغام‌های DIO نشان می‌دهد که این گره به نسخه جدیدDODAG مهاجرت نکرده است. چنین گره‌ای نباید به‌عنوان والد ترجیح داده‌شده توسط سایر گره‌ها در نظر گرفته شود. درحالی‌که فرآیند بازسازی نمودار در حال انجام است، ممکن است بین دو نسخه از یک DODAG به‌طور موقت همکاری وجود داشته باشد. برای جلوگیری از حلقه، بسته‌های داده‌ها مجاز به انتقال از نسخه‌های قدیمی به یک نسخه جدید می‌باشند.

لی و همکاران [5]، تأثیر حمله‌ی رتبه‌بندی را بررسی کردند. ویژگی رتبه یک نقش حیاتی دارد که تقریباً مربوط به تمام عملیات‌های RPL است. سه فایده اصلی آن ایجاد توپولوژی بهینه، جلوگیری از تشکیل حلقه و مدیریت سربار کنترلی است. بااین‌حال، عیب این است که هرگونه حمله‌ای که با اهداف درجه رتبه انجام می‌شود نیز می‌تواند به تأثیرات چندگانه روی عملکرد RPLدست یابد.این پروتکل فرض می‌کند که تمام گره‌ها قابل‌اعتماد هستند و به دنبال قوانین پروتکل هستند بنابراین هیچ سازوکاری برای چک کردن رفتار گره وجود ندارد؛ بنابراین، پس‌ازاین که دفاع رمزنگاری را به خطر انداخت، یک مهاجم داخلی می‌تواند گره‌ها را کنترل کند تا عملکرد را با از بین بردن رتبه‌ها پایین بیاورد.

حملات DDoSبه معنای انکار توزیع‌شده سرویس است و این نوع از حمله سایبری به معنای به سازش یک سرویس برخط توسط درهم شکستن سرور از طریق منابع مختلف است. در حملات DDoSچند-وجهی، هکرها با چندین حملهDDoS ، به‌صورت هم‌زمان یا در زمان‌های مختلف به لایه‌های مختلف شبکه حمله می‌کنند. به گفته محققان شرکت آکامای، مقابله با حملات DDoSچند-وجهی نیازمند دفاع چند-وجهی است؛ زیرا برای هر حمله، یک دفاع جداگانه باید صورت پذیرد و با یک سامانه دفاعی نمی‌شود چند حمله را دفع کرد. معمولاً شرکت‌ها نیز به دلیل کمبود هزینه و نیرو، توانایی مقابله با این دست حملات را ندارند[9].

یکی دیگر از حملات پروتکل RPLحمله کرم چاله است. این حمله معمولاً توسط دو یا تعدادی بیشتر گره مخرب انجام می‌شود. دو گره مخرب درجاهای مختلف اقدام به ارسال و دریافت پیام مسیریابی به همدیگر از طریق کانال مجزا می‌کنند. در این روش، اگرچه دو گره مخرب دور از همدیگر قرارگرفته باشند، اما به نظر می‌رسند در محدوده ارتباطی یک گام همدیگر هستند؛ بنابراین، مسیر عبوری از طریق گره‌های مخرب به‌احتمال‌زیاد کوتاه‌تر از سایر مسیرها به نظر می‌رسد[12].

جدول ۱: بررسی بعضی از حملات مخرب در پروتکل RPL

ردیف	نام حمله	روش کار	خطرات
۱	sinkhole	یک گره مخرب، پیام‌های RPL ی را به شبکه تزریق می‌کند که حامل اطلاعات جعلی است و ترافیک را از گره‌های صادقِ اطراف جذب می‌کند	مهاجم می‌تواند مقدار زیادی از ترافیک را قطع یا از بین ببرد.
۲	DODAG Version	گره مخرب با تغییر نسخه نمودار مسیر حرکت اطلاعات را به‌طرف خود جذب می‌کند.	چنین دست‌کاری نه‌تنها باعث بازسازی غیرضروری نمودار می‌شود بلکه باعث ایجاد حلقه‌هایی در توپولوژی می‌شود.
۳	Rank	یک گره مخرب، در انتخاب گره‌های هاپ بعدی اشتباه می‌کند و یک‌فاصله‌ی اشتباه را به مسیر یاب مرزی اعلام می‌کند.	این حمله باعث ایجاد حلقه‌هایی بین گره و فرزندان خود می‌شود به‌طوری‌که شبکه ناپایدار می‌شود.
۴	DDoS	در این حمله لشکری از تجهیزات هک شده با ارسال درخواست‌های هم‌زمان به سرور قربانی آن را بمباران می‌کنند.	این حمله باعث کندی و یا توقف خدمات سرویس‌دهی می‌شود.
۵	Black Hole	مهاجم از پویایی پروتکل جهت شنود بسته‌های درخواست (PREQ) به نفع خود استفاده می کندو بعد مهاجم از یک بسته PREP جعل‌شده به‌عنوان پاسخ استفاده می‌کند که کوتاه‌ترین مسیر به سمت مقصد را نشان می‌دهد.	مهاجم یک اتصال بین گره مبدأ و خود برقرار می‌کند که سرنوشت تمام بسته‌ها موجود به دست مهاجم می‌افتد که می‌تواند اطلاعات را شنود یا دست‌کاری کند.
۶	Wormhole	دو گره مخرب درجاهای مختلف اقدام به ارسال و دریافت پیام مسیریابی به همدیگر از طریق کانال مجزا می‌کنند. در این روش، اگرچه دو گره مخرب دور از همدیگر قرارگرفته باشند، اما به نظر می‌رسند در محدوده ارتباطی یک گام همدیگر هستند؛ بنابراین، مسیر عبوری از طریق گره‌های مخرب به‌احتمال‌زیاد کوتاه‌تر از سایر مسیرها به نظر می‌رسد و مسیر حرکت اطلاعات از نود مهاجم می‌گذرد.	در این حمله گره مهاجم می‌تواند به‌آسانی اطلاعات مسیر را از گره مبدأ به گره مقصد را برباید.
۷	jamming	گره مخرب اقدام به ارسال بسته‌های سفارشی کرده وبِ موجب آن بقیه نودها از نقطه دسترسی قطع ارتباط می‌شود.	این حمله باعث می‌شود که امکان اتصال نودها به ریشه وجود نداشته باشد و موجب مختل شدن شبکه می‌شود.
۸	DAO	یک نود مخرب پیام‌ها DAO (که برای درخواست ارسال اطلاعات بروز رسانی را دارد) را که از گره‌های پایین‌تر ارسال‌شده است را می‌گیرد وبِ جای انتقال آن‌ها به ریشه بسته را دور می‌اندازد.	این حمله باعث می‌شود اطلاعات بروز رسانی به بعضی از گره‌ها نرسد و این گره‌ها موفق به اتصال به نمودار نشوند.
۹	DIO	یک گره مخرب یک پیام DIO معتبر را از شبکه می‌گیرد وبه صورت مکرر آن پیام را به دیگر گره‌ها ارسال می‌کند که باعث سرکوب پیام‌های DIO می‌شود و گره‌هایی که موردحمله واقع‌شده‌اند پیام‌های اصلی را دریافت نمی‌کنند.	سرکوب مداوم آن‌ها می‌تواند موجب شود که برخی از گره‌ها مخفی باقی بمانند و برخی از مسیرها، کشف‌نشده باقی بمانند. نتیجه، تخریب عمومی کیفیت مسیر یا در بدترین حالت، تکه‌تکه‌شان شبکه است.

6- حمله سرکوب DIO

RPL به‌منظور ایجاد و مدیریت مسیریابی اطلاعات در شبکه از سه نوع پیام کنترل استفاده می‌کند و این موارد عبارت‌اند از:

الف DODAG Object Information (DIO):
برای ایجاد و به‌روزرسانی توپولوژی شبکه استفاده می‌شود.

ب DODAG Object Adaptation (DAO):
برای اطلاعات پخش‌شده و اعلان‌ها مورداستفاده در به‌روزرسانی در مسیر شبکه استفاده می‌شود.

ج DODAG Information Solicitation(DIS):
(درخواست اطلاعات) زمانی استفاده می‌شود که یک گره جدید در هنگام انتظار برای پیوستن به شبکه اطلاعات مربوط به توپولوژی را جستجو کند[10].

هدف از حمله‌ی سرکوب DIO، متوقف کردن یا کُند کردن انتقال پیام‌های DIO در شبکه است. برای این منظور، سازوکار سرکوب DIOی الگوریتم Trickle مورد سوءاستفاده قرار می‌گیرد. در این حمله، دشمن، یک پیام DIO را به‌صورت مکرر ارسال می‌کند که توسط گره‌های گیرنده، سازگار تلقی می‌شود. اگر گره‌ها، DIO های سازگار کافی را دریافت کنند، انتقال DIOی خود را سرکوب می‌کنند. ازآنجایی‌که پیام‌های DIO برای کشف همسایه‌ها و توپولوژی شبکه مورداستفاده قرار می‌گیرند، سرکوب مداوم آن‌ها می‌تواند موجب شود که برخی از گره‌ها مخفی باقی بمانند و برخی از مسیرها، کشف‌نشده باقی بمانند. نتیجه، تخریب عمومی کیفیت مسیر یا در بدترین حالت، تکه‌تکه‌شان شبکه است. حمله‌ی سرکوب DIO که می‌تواند سرویس مسیریابی در RPL را به‌شدت تخریب کند [11].

در (پراسزو و هم کاران، ۲۰۱۷) یک‌راه حل برای جلوگیری از این حمله آورده شده است. این راه‌حل امکان‌پذیر کردن رمزگذاری لایه‌ی MAC به‌منظور ممانعت از شناسایی پیام‌های DIO و متمایز کردن آن‌ها از پیام‌های داده یا سایر انواع پیام‌های مسیریابی توسط دشمن است. متأسفانه، ممکن است این اقدام تقابلی، به‌تنهایی برای جلوگیری از حمله، کارآمد نباشد. درواقع، دشمن می‌تواند از برخی ویژگی‌های خاص برای شناسایی پیام‌های DIO استفاده کند. DIO ها به‌صورت فریم‌های چندپخشی[1] ارسال می‌شوند که از فرم‌های تک‌پخشی از هدر MAC که هرگز رمزگذاری نمی‌شوند، قابل متمایز شدن هستند. در میان فریم‌های چندپخشی، پیام‌های DIO را می‌توان از طریق اندازه‌ی بار مفید[2] آن‌ها شناسایی کرد. این به این دلیل امکان‌پذیر است که بسیاری از پروتکل‌های MAC گسترده از قبیل IEEE 802.15.4، از حالت عملیات رمزنگاری CCM استفاده می‌کنند که در هنگام رمزگذاری، اندازه‌ی بار مفید فریم را تغییر نمی‌دهند.حتی اگر دشمن، موفق به شناسایی پیام‌های DIO به‌طور مستقیم به‌وسیله‌ی اندازه‌ی آن‌ها نشود، می‌تواند اقدامات دیگری را انجام دهد. به‌عنوان‌مثال، می‌تواند یک پیام چندپخشی (DIS) را شناسایی و بازپخش کند که باعث می‌شود یک گره دریافت‌کننده‌ی قانونی، زمان‌سنج Trickle خود را ریست کند. پس از یک انتظار کوتاه‌تر از Imin، چنین گرهی یک DIO را ارسال خواهد کرد که می‌تواند توسط دشمن ضبط شود. شناسایی یک پیام DIS بر اساس اندازه‌ی آن، ساده‌تر از یک پیام DIO است، زیرا DIS کاملاً کوچک است و تنها می‌تواند یک گزینه با اندازه‌ی ثابت داشته باشد.

یکی دیگر از اقدامات متقابل احتمالی، سازوکار حفاظت از بازپخش است؛ که می‌تواند برای مقابله با حمله، مؤثر و کارآمد باشد، زیرابه گره‌های مشروع اجازه می‌دهد که پیام‌های بازپخش شده‌ی DIO را شناسایی کنند و از بین ببرند. اگرچه این سازوکارها می‌توانند توسط پلتفرم‌های جدید با توجه به CPU و حافظه مورداستفاده قرار گیرند، اما ازنظر پیام‌های کنترل اضافی، سربار قابل‌توجهی به همراه خواهد داشت. به‌عنوان‌مثال، استاندارد RPL، شامل یک سازوکار اختیاری حفاظت از بازپخش است [8].

که برای این‌که کاملاً ایمن باشد، به یک دست تکانی[3] چالش-پاسخ رمزنگاری برای ارزیابی تازگی اولین پیام دریافت شده از هر همسایه‌ی جدید نیاز دارد. چنین دست تکانی می‌تواند به‌وسیله‌ی پیام‌های بررسی سازگاری (CC) که قالب آن‌ها توسط استاندارد RPL مشخص‌شده است، اجرا شود. سپس، تازگی پیام‌ها پس از پیام اولی، توسط یک میدان

[1] Multicast

[2] Payload

[3] Handshake

شمارشگر افزایشی محافظت‌شده به‌وسیله‌ی یکپارچگی، تضمین می‌شود. دست تکانی چالش-پاسخ اولیه، سربار شبکه و درنتیجه مصرف انرژی را به‌طور قابل‌توجهی افزایش می‌دهد، اما تأخیر قابل‌توجهی را نیز در عملیات مسیریابی ایجاد می‌کند. چنین سرباری، تشکیل شبکه‌ی کلی را به تأخیر می‌اندازد و واکنش پروتکل مسیریابی به تغییرات توپولوژی را دشوار می‌سازد. بااین‌حال، در بسیاری از WSANها، ممکن است همگام‌سازی دقیق امن، امکان‌پذیر یا مقرون‌به‌صرفه نباشد[4].

7- نتیجه‌گیری

در این مقاله، ما حمله‌ی سرکوب DIO را بررسی کردیم. این حمله، گره‌های قربانی را وادار به سرکوب انتقال پیام‌های DIO می‌کند. این امر منجر به تخریب کلی کیفیت مسیر می‌شود که درنهایت می‌تواند به تکه‌تکه شدن شبکه منجر شود. برخلاف سایر حملات RPL که در مقالات و کتب به آن‌ها اشاره‌شده است، حمله‌ی سرکوب DIO، برای ایجاد پیام‌های RPL جعلی، به دشمن نیازی ندارد؛ بنابراین این حمله می‌تواند بدون سرقت کلیدهای رمزنگاری از گره‌های مشروع، برقرار شود. در تحقیق‌های به‌عمل‌آمده به‌غیراز مقاله (پراسزو وهم کاران، ۲۰۱۷) مقاله دیگری که به این حمله پرداخته باشد وجود ندارد. این دو راه‌کار از این حمله جلوگیری می‌کند ولی راهکار بهینه‌ای نیست در آینده ما قصد داریم به ارائه یک راهکار بهینه برای این حمله بپردازیم.

8- مراجع

[1]H.Azararjmand[1],M.H.MousatMahallahanReza[2],A.Pourbakhram[3] (2017)."Sink Attackb Model on the Internet of Things".International Conference on Recent Innovations in Electrical and Computer Engineering.

[2]L. Wallgren[1], S. Raza[2] and T. Voig[3]. "Routing attacks and countermeasures in the rplbased internet of things".International Journal of Distributed Sensor Networks, vol. 2013 2013.

[3]PericlePerazzo[1],Vallati,C2, Varano, D3, & Anastasi, G4. (11 August 2017). DIO Suppression Attack Against Routing in the Internet of Things. IEEE Communications Letters, 2524 - 2527.

[4]Picco, P[1], Istomin, T[2], & Kiraly, C[3]. (16 December 2016). RPL, the Routing Standard for the Internet of Things...OrIsIt.IEEE Communications Magazine, 16 - 22.

[5]Badis Djamaa[1], M. R[2]. (27 February 2015). Optimizing the Trickle Algorithm. IEEE Communications Letters, 819 - 822.

[6]Dvir, A[1]. Holczer, T[2]. & Buttyan, L[3]. (15 November 2011). VeRA - Version Number and Rank Authentication in RPL. IEEE Sensors J. vol. 13, no. 10, 3685–3692.

[7]Anthéa Mayzaud[1], A. S[2]. (2014). A Study of RPL DODAG Version Attacks. IFIP 8th Int. Conf. Auto. Infrastruct. Manage. Secur. (AIMS), 92-104.

[8]Tsvetko Tsvetkov[1] (2011).RPL: IPv6 Routing Protocol for Low Power and Lossy Networks. Internet Engineering Task Force (IETF),59-66.

[9]DA YIN[1], LIANMING ZHANG[2], AND KUN YANG[3](2018). A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework. IEEE Access,694-705.

[10]Y. Bin Zikria[1], M. K[2]. (December 2017). A survey on routing protocols supported by the Contiki Internet of things operating system. Future Generation Computer Systems, 1-20

[11] Le, A[1]. Loo, J[2]. Lasebae, A[3]. & Vinel, A[4]. (06 June 2013). The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks. IEEE Sensors Journal Volume: 13, Issue: 10, 3685 - 3692.

[12]Perazzo, P[1], Vallati, C[2], Varano, D[3], & Anastasi, G[4]. (2018). Implementation of a wormhole attack against a rpl network: Challenges and effects. European Dependable Computing Conference, 95-102.