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

بررسی امنیت پروتکل RPL در اینترنت اشیاء

مریم عیسوندی

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

چکیده

در اینترنت اشیاء ارتباط اشیاء با یکدیگر از طریق شبکه و به کمک مدارهای کم‌توان برقرار می‌شود و کاربردهای زیادی را در حوزه های مختلف از جمله مصرف انرژی، امنیت فیزیکی و هوشمندسازی شهرها فراهم می‌سازد. یکی از اولین مشکلات اینترنت اشیاء استفاده از دستگاه‌ها با توان پردازشی، ذخیره‌سازی و منبع انرژی ضعیف و همچنین مدل ترافیکی خاص در آن است. این امر موجب عدم سازگاری پروتکل‌های رایج مسیریابی در علم ارتباطات با آن می‌شود. به همین خاطر پروتکل مسیریابی RPL به‌منظور رفع نیازهای مسیریابی در اینترنت اشیاء ایجاد گشت. با افزایش بکارگیری اینترنت اشیا و واگذاری بسیاری از کارها در زندگی روزمره به اشیا، آسیب‌پذیری‌ها می‌توانند از فضای مجازی خارج و برجهان واقع تأثیر مخرب بگذارند. در برخی موارد این تأثیرات منفی حتی می‌تواند جبران‌ناپذیر نیز باشد نظیر قطع برق یک شهر. بنابراین با توجه به اهمیت بالای امنیت در اینترنت اشیاء پس از ایجاد پروتکل مسیریابیRPL پژوهشگران بسیاری شروع به بررسی آن ازنظر امنیت پرداختند. در این مقاله به تحلیل و بررسی امنیت پروتکل RPL و برخی از حملات مهم علیه آن پرداخته می‌شود.

واژه‌های کلیدی

اینترنت اشیاء، مسیریابی، پروتکل RPL، امنیت.

۱. مقدمه

در اینترنت اشیا، مدارهای الکترونیکی کوچک و کم‌توان امکان برقراری ارتباط میان اشیاء را فراهم می‌سازند. تاکنون کاربردهای فراوانی برای این فناوری معرفی شده است که از جمله آنها می‌توان به کنترل انرژی، امنیت فیزیکی و هوشمندسازی شهری اشاره کرد. یکی از مشکلات مهم اینترنت اشیاء در ابتدای پیداش، عدم سازگاری روش‌ها یا فناوری‌های ارتباطی مشهور با آن بود . در واقع ویژگی خاص دستگاه‌ها در این فناوری از جمله توان پردازشی و ارتباطی محدود امکان استفاده از فناوری‌های روز را در آن غیر ممکن می‌ساخت . علاوه بر این، برخی دیگر از ویژگیهای خاص این فناوری مانند نوع خاص ترافیک ارسالی(ترافیک به طور معمول 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 اشیاء بود. در همین راستا پروتکلی به نام RPL[1] مخصوص شبکه‌های کم‌توان و پر اتلاف توسط پژوهشگران طراحی شد [۴-۱]. RPL یک پروتکل مسیریابی بردار- فاصله[2] با رویکرد پیشگیرانه و براساس IPv6 می‌باشد که توسط انجمن IETF طراحی و در سند استاندارد RFC 6550 استاندارد شده است. همزمان با ارائه پروتکل RPL و به دلیل اهمیت فراوان امنیت اطلاعات در اینترنت اشیا، پژوهشگران بسیاری به بررسی حفره‌های امنیتی این پروتکل پرداخته و با گذشت زمان آسیب‌پذیری‌های متعددی در آن یافت شد. در ادامه پس از معرفی پروتکل RPL به معرفی به حملات امنیتی آن پرداخته شده است.

۲. پروتکل مسیریابی RPL

توپولوژی شبکه در پروتکل RPL به صورت یک گراف بدون دور جهت‌دار[3] بوده که شکل‌گیری آن به کمک پیام‌های کنترلی خاصی در قالب نسخه ششم ICMP صورت می‌گیرد[۶-۴]. این درخت DODAG[4] نام داشته و در فرآیند ایجاد آن ابتدا گره ریشه (گره‌ای که نسبت به سایر گره‌ها از نظر پردازشی قدرتمندتر بوده و مجری اصلی کاربردهای اینترنت اشیا در درخت DODAG است) به ارسال اطلاعات پیکربندی، در قالب یک پیام کنترلی تحت عنوان DIO[5] می‌پردازد. این پیام به صورت همه‌پخشی 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 به عنوان والد خود در DODAG انتخاب می‌کنند[۶-۴]. آنها پس از پیوستن به درخت، مدتی صبر کرده و سپس آخرین اطلاعات خود را به صورت همه-پخشی و در قالب پیام‌های DIO منتشر می‌کنند .به این ترتیب اطلاعات پیکربندی برای گره‌های بیشتری و از مسیرهای متعدد منتشر خواهد شد .گفتنی است که یک گره می‌تواند پیامهای DIO را از مسیرهای مختلف دریافت کند .در این شرایط گره مربوطه باید از بین گره‌های ارسال کننده DIO 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[۶-۴]:

- حلقه در درخت ایجاد نشود.
- ترافیک از نزدیکترین مسیر ممکن به ریشه برسد: این موضوع بر اساس یک مقدار مشخص به نام رتبه در پیام‌های DIO صورت می‌گیرد. این مقدار دارای رابطه مستقیم با فاصله گره از ریشه است .درواقع هر چه مقدار رتبه بیشتر باشد، گره ارسال کننده پیام DIO نیز از ریشه دورتر است. بر این اساس هر گره جهت انتخاب بهترین مسیر ممکن برای ارسال اطلاعات به ریشه باید از بین گره‌های ارسال کننده DIO گره‌ای با مقدار کمتر رتبه را انتخاب کند.

---

[1] Routing Protocol for Low Power and Lossy Networks

[2] Distance-Vector

[3] Directed Acyclic Graph (DAG)

[4] Destination Oriented Directed Acycle Graph-DODAG

[5] DODAG Information Object

در پروتکلRPL نوع دیگری از پیامهای کنترلی به نام DAO[6] نیز وجود دارد .طبق قوانینRPL، هر گره در درختDODAG 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[۶-۴].

مسیرهای رو به پایین در پروتکل RPL به دو صورت ذخیره می‌شوند[۶]:

۱. **ذخیره‌سازی به صورت توزیع شده**: در این حالت هر گره در درخت دارای جدول مسیریابی بوده و در این فرآیند مشارکت می‌کنند.

۲. **ذخیره‌سازی به صورت متمرکز** :در این حالت گره‌ها فاقد جدول مسیریابی بوده و تمام اطلاعات مورد نیاز باید به ریشه 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 RPL، پیامهای DIS[7] هستند .دستگاه‌های خواهان پیوستن به درختDODAG با ارسال این نوع پیام تقاضای ارسال اطلاعات مورد نیاز را می‌کنند .پیام‌های DIS باید به برگ‌های درخت ارسال شود[۶-۴].

۳. نگرانی‌های امنیتی در پروتکل RPL

در پروتکلRPL تا به امروز آسیب‌پذیری‌های امنیتی زیادی کشف شده که در ادامه به تشریح آنها می‌پردازیم.

۱،۳.حملات سیل‌آسا[8]

هدف از این حمله مصرف بیهوده منابع گره‌ها به نحوی است که موجب اختلال در عملکرد شبکه شود. این حمله به طور معمول در پروتکلRPL با ارسال بسیار زیاد پیام‌هایDIS به اطرافیان صورت می‌گیرد تا باعث شروع مجدد زمان‌سنج قطره‌چکان[9] شود[۳،۴،۷،۸] . در RPL ، شروع مجدد این زمان‌سنج منجر به ارسال پیغام‌های DIO و ایجاد سربار اضافه بر روی شبکه می‌شود.

۲،۳.حمله سرریز جدول مسیریابی

در این حمله مهاجم[10] سعی بر ایجاد مسیرهای ساختگی فراوان در جدول مسیریابی گره قربانی خواهد کرد. هدف از این کار اشغال فضای حافظه مربوط به جداول مسیریابی بوده به طوری که دیگر جایی برای ثبت مسیرهای جدید وجود نداشته باشد .در این شرایط عملکرد پروتکل RPL نه تنها برای آن گره بلکه به علت انتشار اطلاعات غلط با اختلال وسیعی روبه‌رو خواهد شد[۷].

۳،۳.حمله افزایش مقدار رتبه

در این حمله مهاجم با سوء استفاده از هزینه بالای بازیابی حلقه‌های مسیریابی در پروتکلRPL به افزایش ارادی مقدار رتبه خود می-پردازد. با این کار برخی گره‌ها به تغییر پدر ارجح پرداخته و برخی دیگر اقدام به این کار نمی‌کنند(کمینه زمانی برای به روز رسانی 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 پروتکلRPL شرکت نخواهد کرد[۷،۸].

۴،۳.حملات ناسازگاری درDODAG

در پروتکل RPL 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

---

[6] Destination Advertisement Object

[7] DODAG Information Solicitation

[8] Flooding

[9] Trickle

[10] Attacker

پروتکلRPL دارای یک سازوکار بازیابی بوده که پس از دریافت تعداد مشخصی از پیام‌های ناسازگاری فعال می‌شود .در این حالت نیز، زمان‌سنج قطره‌چکان شروع مجدد شده و پیغام DIO برای تعمیر درخت ارسال می‌شود. سربار این امر منجر به مصرف منابع برخی گره-ها 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[۳،۴،۷،۸].

۵،۳. حملات افزایش شماره نسخه

گره ریشه هنگام ایجاد درخت DODAG در پیام‌های DIO یک شماره نسخه نیز قرار داده و سپس آن را به صورت همه‌پخشی ارسال می‌کند. این شماره هنگام بازیابی ساختار درخت پروتکلRPL کاربرد دارد. درواقع گره ریشه با افزایش شماره نسخه در پیام‌های DIO وجود یک مشکل اساسی در درخت DODAG را به سایر گره‌ها خبر می‌دهد .در این شرایط گره‌های دریافت کننده پیامDIO باید اطلاعات قبلی خود را فراموش کرده و از ابتدا در فرآیند تشکیل درختDODAG 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[۷].

۶،۳.حمله کرم چاله

در این حمله گره مخرب ترافیک را با یک پیوند خارج از شبکه به قسمت دیگری از درختDODAG منتقل می‌کند. با این کار گره‌های بخش دوم نیاز به پردازش‌های به نسبت بالایی برای بررسی و مدیریت ترافیک ورودی داشته که ناشی از عدم تطابق با قوانینRPL است. بنابراین در شبکه سربار بیهوده ایجاد می‌شود[۳،۴،۷،۸].

۷،۳.حمله ناسازگاری DIO

در پروتکلRPL هنگام ذخیره‌سازی مسیرها به صورت توزیع شده نوعی ناسازگاری پیش‌بینی شده است .این ناسازگاری مربوط به شرایطی است که پیامی از طریق یک مسیر بی اعتبار(به عنوان مثال دارای زمان‌سنج پایان یافته)در گام بعدی(یکی از گره‌های فرزند در درختDODAG) مسیریابی شود .در این شرایط گره دوم یک پیام خطای مبنی بر عدم اعتبار مسیر به گره اولیه ارسال کرده و شرایط یاد شده را اطلاع می‌دهد .گره نخست نیز با دریافت این پیام باید مسیر دیگری را برای ارسال پیام خود انتخاب کند در حمله ناسازگاری DIO به طور دقیق از همین موضوع برای ایجاد اختلال در شبکه سوءاستفاده می‌شود .به عنوان، مثال گره مخرب با ارسال این نشانه برای تمام مسیرهای جدول خود در عمل دسترسی به گره‌های زیر درخت را غیرممکن می‌سازد[۷،۸].

۸،۳.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 [۷،۸].

۹،۳.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 DODAGبه دنبال دارد. فرآیندی که سربار فراوانی بر روی پروتکلRPL ایجاد می‌کند[۷،۸].

۱۰،۳.حملات سیاه‌چاله[11] و چاهک[12]

در این حملات گره مخرب در درخت DODAG به جای ارسال بسته‌های دریافتی شروع به حذف تمام(حمله سیاه‌چاله)یا بخشی از آنها (حمل iچاهک)بر اساس جدول مسیریابی می‌کند .به این ترتیب دسترسی به بخشی از گره‌های درختDODAG غیرممکن شده و یا با اختلال روبه‌رو می‌شود[۴،۷،۸].

۱۱،۳.حملات تکرار

---

[11] Blackhole

[12] Sinkhole

در این حملات گره مخرب پیام‌های کنترلی دریافتی را ضبط کرده و در زمانی دیگر دوباره به شبکه تزریق می‌کند . به علت عدم تمایز این پیام‌ها در پروتکلRPL شبکه متوجه این رفتار مخرب نشده و به صورت عادی رفتار می‌کند . بر این اساس توپولوژی درختDODAG می‌تواند به صورت غیرمجاز تغییر کند(به ویژه اگر موارد تکرار از نوع پیام‌های DIO باشند)[۷،۸].

۱۲،۳.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 محدوده بی‌سیم گره مخرب)در مکانی نزدیک به ریشه به نظر بیاید .هدف از این کار تغییر پدر ارجح برخی گره‌های درختDODAG بوده، به طوری که 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[۷،۸].

۱۳،۳.حملات جعل هویت

در این حملات گره مخرب به جعل شناسه فیزیکی سایر گره‌های درختDODAG از جمله گره ریشه می‌پردازد. هدف از این کار ایجاد برخی ناسازگاری‌ها درRPL از جمله ایجاد ترافیک جعلی با هدف مصرف منابع گره‌ها است[۳،۴،۷،۸].

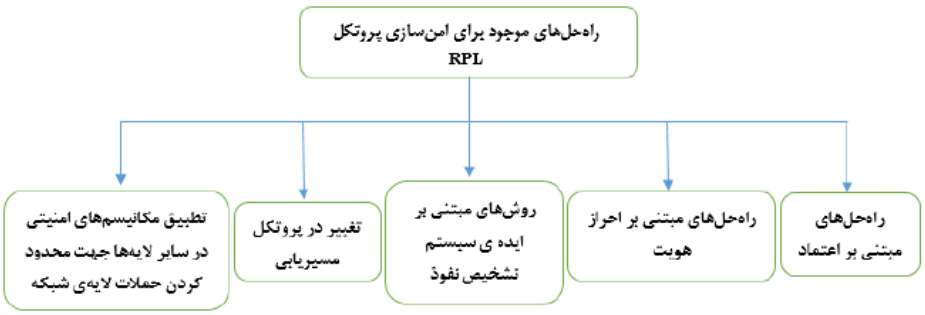
۱۴،۳.شنود و تحلیل ترافیک

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 به طور معمول چه موقع است؟
- کدام گره‌ها با هم بیشتر ارتباط برقرار می‌کنند؟

۴.راه‌حل های امنیتی موجود برای رفع حملات در RPL

به دلیل وجود نگرانی‌های امنیتی مختلف در پروتکل RPL ، پژوهشگران مختلف به ارائه راه‌حل‌های مختلف جهت ارتقای امنیت آن پرداخته‌اند. در شکل ۱ یک دسته‌بندی کلی از راه‌حل‌های موجود در این زمینه آورده شده است[۷-۱۱] .



شکل ۱. راه‌حل‌هاب امنیتی موجود برای پروتکلRPL

در ادامه به توصیف مختصر راهکارهای موجود می‌پردازیم.

۱،۴. راه‌حل‌های مبتنی بر اعتماد

در این راه‌حل‌ها از مفهوم اعتماد برای تشخیص رفتار مخربانه استفاده شده است. رفتار مخربانه می‌تواند بر اساس هدف پژوهش به صورت‌های متفاوتی در نظر گرفته شود؛ البته، رفتارهای خارج از قوانینRPL باعث کاهش پارامتر اعتماد خواهد شد .گذشت زمان هم یکی از متداول‌ترین رویکردها برای بازگشت اعتماد به مقدار اولیه است.

۲،۴. راه‌حل‌های مبتنی بر احراز هویت

در این روش‌ها، دسترسی غیرمجاز به منابع شبکه به کمک فرآیند احراز هویت محدود شده و یا به طور کامل از بین می‌رود.

۳،۴. روش‌های مبتنی بر ایده سیستم تشخیص نفوذ

روش‌های مبتنی بر ایده سیستم تشخیص نفوذ بر اساس تحلیل اطلاعات دریافتی از طرف گره‌های درخت به تشخیص رفتار مخربانه می-پردازند. در این راستا به طور معمول برخی تغییرات نیز در قوانین پروتکلRPL اعمال شده یا به آن افزوده می‌شود.

۴،۴.تغییر در پروتکل مسیریابی

بسیاری از پژوهشگران علت نگرانی‌های امنیتی پروتکلRPL را نوعی نقص در طراحی آن عنوان می‌کنند .آنها معتقدند که با اصلاح پروتکلRPL دیگر نیازی به رویکردهای امنیتی نبوده و می‌توان دست کم با بخش زیادی از این موارد مقابله کرد.

۵،۴.تطبیق مکانیسم‌های امنیتی در سایر لایه‌ها جهت محدود کردن حملات لایه شبکه

برخی دیگر از پژوهشگران حوزه امنیت اطلاعات و شبکه‌های رایانه‌ای ناسازگاری راهکارهای موجود و مشهور با پروتکلRPL را غیرممکن نمی‌دانند .به این ترتیب سعی بر تطبیق پروتکل‌های یادشده باRPL کرده تا بتوانند از مزایای آنها در رفع نگرانی‌های امنیتی این پروتکل نیز استفاده کنند.

۵. نتیجه

در این مقاله به بررسی چالش‌های امنیتی پروتکل RPL پرداخته شد. برای برخی از این حملات راهکارهایی پیشنهاد شده است و برخی از آنها همچنان هیچگونه راه‌حلی ندارند. این موارد می‌تواند زمینه پژوهش پژوهشگران باشد. علاوه بر این، راه‌حل‌های موجود نیز در کنار نقاط قوت خود دارای ضعف‌های قابل توجهی هستند که زمینه را برای پژوهش جهت ارائه یک راه‌حل بهینه و کارآمدتر فراهم می‌سازند. برخی پژوهشگران نیز معتقدند این پروتکل اشکالات بنیادی زیادی دارد و به دنبال ارائه یک پروتکل کارآمدتر هستند تا جایگزین این پروتکل شود.

منابع

[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 .
[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 .
[3]V. Adat and B. B. Gupta, “Security in Internetof Things: issues, challenges, taxonomy, and architecture”, Telecommunication Systems,Volume 67, Issue 3, pp 423–441, 2018.
[4] L. Wallgren, S. Raza and T. Voigt,"Routing Attacks and Countermeasures in the RPLBased Internet of Things", International Journal of Distributed Sensor Networks, Volume 2013.
[5]O. Iova, P. Picco, T. Istomin and C. Kiraly,"RPL: The Routing Standard for the Internet ofThings... Or Is It?," IEEE Communications Magazine, vol. 54, no. 12, pp. 16-22, December 2016.
[6]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.
[7]A. Mayzaud, R. Biddonel, and I. Chrisment, “A Taxonomy of Attacks in RPL-based Internet of Things” International Journal of Network Security, IJNS. 2016.
[8]A Raoof, A. Matrawy and C. h. Lung,“Routing Attacks and Mitigation Methods for RPL-Based Internet of Things” IEEE Communications Surveys & Tutorials, 2018.
[9]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.
[10]Mayzaud, A., Sheghal, A., Badonnel, A. and Chrisment, I. "Mitigation of Topological Inconsistency Attacks In RPl besed Low Power Lossy Networks."International Journal of Network Management, Volume 25, Issue 5,2015.
[11] 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.