دوفصلنامه محاسبات و سامانه های توزیع شده
سال چهارم، شماره اول، شماره پیاپی۷، صفحه ۲۵ تا ۳۸، سال ۱۴۰۰

بررسی حملات و راهکارهای امنیت اینترنت اشیاء(IOT)

فرانه زرافشان[۱]، رامین شیربندی[*۲]
[۱]عضوهیئت علمی دانشگاه آزاد اسلامی واحد آشتیان.
[۲]دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات دانشگاه آزاد اسلامی واحد آشتیان ایران.

چکیده

کلمه باظهورخانه های هوشمند شهرهای هوشمند و اشیاءهوشمند مفهوم اینترنت اشیاء(IOT)ظهور پیدا کرده است به عنوان حوزه ی که تاثیر پتانسیل و رشد غیر قابل باوری داشته وبا پیش بینی شرکت سیسکو تا سال۲۰۲۰ نزدیک به ۵۰ میلیارد دستگاه به هم متصل خواهند بودبا این حال اکثرا هک کردن این دستگاه های اینترنت کار ساده ی است و این دستگاه ها در معرض خطر هستند به طور معمول این دستگاه های اینترنت اشیاء توانایی های محاسباتی ذخیره سازی و ظرفیت شبکه ای محدودی دارند و بنابراین آنها نسبت به دیگردستگاه های انتهایی از قبیل گوشی های هوشمند تبلت ها یا کامپیوترهای بیشتر دربرابر حمله ها آسیب پذیرهستند مادراین مقاله به بررسی ومرور مسائل عمده امنیتی دراینترنت اشیاء میپردازیم مامسائل امنیتی اینترنت اشیاءرا به همراه حمله ها وتهدیدات وراهکارها نوآورانه مطرح میکنیم.

کلمات کلیدی: امنیتIOT، پروتکل هایIOT، امنیت شبکه.

Investigate IoT attacks and security measures

Faraneh Zarafshan[1], Ramin Shirbandi[*2].
[1]Faculty Member of Islamic Azad University ASHTIAN Branch.
[2]Master students of Information Technology Engineering, Islamic Azad University, ASHTIAN Branch.

Abstract

ASmart Cities Smart Cities and Smart Objects The concept of the Internet of Things (IoT) has emerged as an area of incredible potential growth and growth, with Cisco predicting that nearly 50 billion devices will be connected by 2020. Hacking these Internet devices is easy, and these devices are compromised. Typically, these IoT devices have limited storage computing capabilities and network capacity, so they are superior to other end devices such as smartphones. Tablets or computers are more vulnerable to attacks. The mother of this article examines and reviews the major security. issues on the Internet of Things.

Keywords:IoT security, IoT Protocols, Network Security.

تاریخچه مقاله:

تاریخ ارسال: ۱۴۰۰/۰۳/۲۱
تاریخ اصلاحات: ۱۴۰۰/۰۵/۰۵
تاریخ پذیرش: ۱۴۰۰/۰۶/۰۲
تاریخ انتشار: ۱۴۰۰/۰۶/۳۱

Keywords:

IoT security
IoT Protocols
Network Security

*ایمیل نویسنده مسئول:
raminshirbandi77@gmail.com

۱– مقدمه

اینترنت اشیاءIOTبه میلیاردهادستگاه فیزیکی درسراسرجهان گفته میشودکه درحال حاظربه اینترنت متصل هستندهمه این دستگاه هامیتوآنندااطلاعات راجمع آوری کرده وبه اشتراک بگذارند.حملات سایبری درشبکه های کامپیوتری اخیر۲۲درصدافزایش پیداکرده است.برخی ازبخش هامانندشهرهای هوشمندامورمالی وحمل نقل درموقعیت های حملات ازرتبه بندی بالاتری برخوردارهستندروزبه روزحملات پیچیده ترمیشوندودرجه ی آنهابالاترمی رود که موضوع نگران کننده ی است.حسگرهاوسائل هوشمندومحرک هابرای بکارگیری کاربردهای IOT استفاده میشوندطراحی اصلی IOT برسه لایه است لایه فیزیکی لایه شبکه ولایه کاربردی.دریک استفاده ی کاربردی IOT وسائل ناهمگن متفاوتی بهم وصل میشوندوباهم ارتباط برقرارمیکنند ازآنجایی که اغلب وسائل هوشمند ارزان قیمتی هستندبه حملات مختلف آسیب پذیرهستندهنگامی که کاربراطلاعات شخصی اش رادریک فضایی عمومی به اشتراک میگذاردوحریم خصوصی یک مسئله ی مهم است کاربرفقط درصورتی به استفاده ازبرنامه اعتمادخواهدکردکه مسائل امنیتی به درست موردتوجه قرارگیرد.چالش های اصلی درIOT امنیت وحریم خصوصی هستندبطوریکه زنجیره ی بلوکی شبیه یک شبکه ازکامپیوترهای گره است که درآن داده هابمدت طولانی مدت دریک مکان مرکزی ذخیره نمیشونداما‌بصورت یک دفترکل جهانی توزیع میشوندوبالاترین سطح رمزنگاری رااستفاده میکند.بارشدسریع دستگاه های هوشمندوشبکه های پرسرعت اینترنت اشیاء IOT به پذیرش اینترنت اشیاء به پذیرش عمومی ومحبوبیت گسترده ای به عنوآن استانداردهای اصلی برای شبکه های کم توآن و پراتلاف (LLNS) دسته یافت است.شبکه های LLNکه منابع محدودی دارنداینترنت اشیاءشبکه ارائه می دهند که درآن اشیاء یادستگاه های تعبیه شده دارای حسگرهایی هستندکه ازطریق یک شبکه خصوصی یاعمومی بهم متصل شده اند.دستگاه هادراینترنت اشیاءمی توآنندازراه دورکنترل شوندتاعملکردموردنظررا‌انجام دهند.

۲- اینترنت اشیا(IoT)

واژه IoT اولین بار توسط کوین اشتون در مرکز تشخیص خودکار MIT معرفی شد [۱]. او از اصطلاح IoT برای اشاره به اتصال اطلاعات RFID به اینترنت استفاده کرد. پس از معرفی ایده اینترنت اشیا توسط اشتون، مفهوم اشیا متصل به یکدیگر مورد توجه شرکت های فناوری اطلاعات و سازمان های دولتی قرار گرفت. اصطلاح IoT در در دوران جهان هوشمند به طور گسترده به کار می رود و تعاریف و مفاهیم بسیاری که مربوط به IoT هستند را می توان یافت. در [۲] نویسندگان؛ هوانگ و لی مفهوم IoT را به عنوان: " اینترنت مربوط به اطلاعات اشیا " توضیح می دهند. نویسندگان [۳] IoT را به صورت:
یک شبکه گسترده از اشیا به هم پیوسته با آدرس دهی منحصر به فرد، مبتنی بر پروتکل های ارتباطی استاندارد" تعریف می کنند. [۴] مفهوم IoT را به صورت گسترده تر به عنوان یک تکنولوژی معرفی می کند که اشیا فیزیکی را قادر می سازد تا با یکدیگر صحبت کنند، اطلاعات و دانش را با یکدیگر به اشتراک بگذارند، فکر کنند، درک کنند (ببینند، گوش کنند) و برای تصمیم گیری هماهنگ شوند.

۱-۲-عناصر تشکیل دهنده IoT:پنج عامل اصلی عناصر تشکیل دهنده IoT را در ادامه به اختصار توضیح می دهیم.
درک و شناسایی: حسگرها و عملگرها: با یک مثال خدمتتون عرض کنم اینکه به طور مثال یک AirCondition سنسوری که وجود دارد اطلاعات دما را از محیط سنس می کند و در صورت افزایش یا کاهش دما یک رفتاری را انجام می دهد.
شناسایی عنصری اساسی در اینترنت اشیا است که مطرح می شود. یک راه استفاده از کد های فراگیر (uCode) و یا کدهای الکترونیکی محصولات (EPC) برای شناسایی یک شی در اینترنت اشیا است. مدل بعدی سیستم یکپارچه نام منابع (URN) است که برای شناسایی و اجازه نامگذاری منحصر به فرد اشیا استفاده می شود، تا بتوان آن‌ها را در یک شبکه مورد بررسی قرار داد. یکی دیگر از گزینه هایی که در IoT در نظر گرفته شده است.
ارتباطات و زیرساخت WSN، 6LoWPAN، ZigBee، Z-Wave: علاوه بر تکنولوژی های LowWPAN۶، ZigBee، Z-Wave، فناوری های بیشتری مانند بلوتوث، BLE، Wi-Fi، فیبر نوری (Li-Fi)، LTE، سلولی (cellular)، نخ (رشته) (Thread)، ارتباط نزدیک میدان (NFC)، SigFox و LoRaWAN برای IoT وجود داردشبکه های حسگر بی سیم شامل یک یا چند ایستگاه پایه و تعدادی گره های حسگر می باشند. هر گره در WSN دارای بخش های مختلفی از جمله یک فرستنده-گیرنده رادیویی، آنتن، میکروکنترلر، مدار الکترونیکی و باتری است [۵]. به طور مثال یکی از چالش های موجود در IoT این است که بتوان دستگاه های کم هزینه را به شبکه متصل کرده و یک ارتباط امن و مطمئن برقرار نمود. LowWPAN۶ [۶] یکی از اجزای کلیدی برای دستیابی به این هدف است. که از

شبکه های بیسیم شخصی کم توان (LoWPAN) و IPv6 تشکیل شده است تا بتوان آن را در دستگاه های دارای منابع محدود و کم هزینه مورد استفاده قرار داد، زیرا اندازه بسته کوچکتر، و از رنج پهنای باند پایین تری استفاده می کند. ZigBee در شبکه های بی سیم کوتاه برد استفاده می شود چون از باتری استفاده می کند. معمولا در مواردی که برای دستیابی به مصرف انرژی پایین تر، پیچیدگی کم و سرعت داده کم مورد نیاز است استفاده می شود. در اکثر مواقع در حالت ذخیره انرژی قرار دارد و تنها زمانی فعال می‌شود که نیاز به انجام کاری دارد در نتیجه عمر باتری این دستگاه‌ها نسبتا ولانی است [۷]. Z-Wave همانند ZigBee، برای ارتباط بی‌سیم کوتاه برد بکار می‌رود، زیرا مزایایی از جمله هزینه کم و مصرف انرژی پایین دارد. این شبکه می تواند تا ۲۳۲ گره در شبکه داشته باشد که هر یک از آنها یک گره فرعی است و با استفاده از کنترل کننده، کنترل می شود.

محاسبه: انواع پلتفرم های سخت افزاری مانند Arduino، UDOO، FriendlyARM، Intel Galileo و Raspberry PI برای اجرای برنامه های IoT وجود دارند. علاوه بر پلتفرم های سخت‌افزاری، سیستم عامل نرم افزاری هم برای کارکردهای اینترنت اشیا مورد نیاز هستند. از جمله آنها می توان به Contiki، Tiny OS، LiteOS و RioT OS اشاره کرد. پلتفرم‌های ابری به اینترنت اشیا اجازه می‌دهند تا داده‌های ارسال‌شده توسط اشیا هوشمند را ذخیره کرده و آن را برای استخراج دانش با استفاده از مفاهیم کلان داده‌ها پردازش کنند.

خدمات: اینترنت اشیا خدمات مختلفی را برای شناسایی و دسترسی به اشیا، جمع‌آوری داده‌های خام از دنیای واقعی، استفاده از داده برای تصمیم‌گیری و سرویس های در دسترس ارائه می‌دهد.

معناشناسی: محققان معانی را به عنوان هسته اینترنت اشیا توصیف می کنند. معناشناسی به ارائه خدمات مورد نیاز مانند استخراج دانش، کشف منابع، کاربرد (استفاده از) منابع، تحلیل داده‌ها و تصمیم‌گیری کمک می‌کند. برای انجام این وظایف، از چارچوب توصیف منابع (RDF) و زبان هستی شناسی وب (آنتولوژی) (OWL) استفاده می شود.

معماری IoT: در(شکل۱) معماری پیشنهادی خان و همکاران نشان داده شده است که معماری های مختلف را به معماری پنج لایه کلی تبدیل کرده اند. در زیر جزئیات هر لایه به همراه ویژگی های آن بیان شده است.

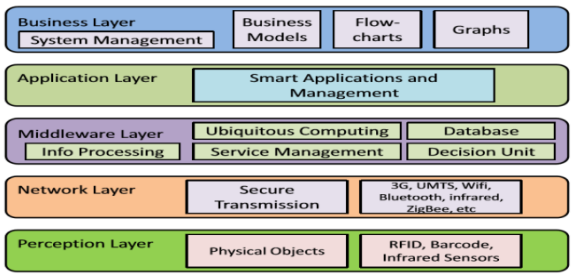
لایه درک: این لایه شامل اجسام و سنسورهای فیزیکی است. وظیفه اصلی این لایه، دریافت داده های فیزیکی توسط سنسورهای مختلف است و اطلاعات را پس از تبدیل به سیگنال های دیجیتال انتقال می دهد. فن آوری های مورد استفاده در این لایه شامل RFID، بارکد دو بعدی، GPS و غیره هستند.

لایه شبکه: همان لایه انتقال است که مسئولیت دریافت اطلاعات از لایه درک را بر عهده دارد. این لایه، داده های دریافت شده را از طریق شبکه های مختلفی که می توانند سیمی یا بی سیم باشند، به مرکز پردازش ارسال می کنند. فن آوری های مورد استفاده برای انتقال اطلاعات عبارتند از G۳، Wi-Fi، بلوتوث، ZigBee، مادون قرمز و غیره است. پروتکل هایی مانند IPv4 یا IPv6 نیز در این لایه برای آدرس‌دهی اشیا استفاده می شوند.

لایه میان افزار (Middleware): هدف اصلی این لایه ذخیره، تجزیه و تحلیل و پردازش داده ها و اطلاعات دریافت شده از لایه های پایین‌تر است. در این لایه از تکنولوژی هایی مانند پایگاه داده، پردازش هوشمند، محاسبات ابری و غیره برای ارائه خدمات استفاده می شود.

لایه اپلیکیشن (برنامه کاربردی): این لایه از داده های پردازش شده توسط میان افزار برای ارائه خدماتی مانند مدیریت لجستیک، خدمات مبتنی بر مکان و ایمنی استفاده می کند و نقش مهمی در پیاده سازی IoT در مقیاس گسترده دارد.

لایه کسب و کار: این لایه تمام برنامه ها را همراه با مدل های کسب و کار مدیریت می کند و همچنین مسئول تجزیه و تحلیل عمیق در مدل های مختلف کسب و کار و ایجاد جداول و نمودارها برای کمک به تصمیم گیری در کسب و کار است.



(شکل-۱): معماری ۵ لایه پیشنهادی خان و همکاران

همکاری سازمان‌های بین المللی برای تهیه استانداردها و پروتکل‌ها از سال ۲۰۰۳ سازمان‌هایی مانند کنسرسیوم وب گسترده جهانی (W3C)، کارگروه مهندسی اینترنت (IETF)، انجمن مهندسان برق و الکترونیک (IEEE) و موسسه استانداردهای ارتباطی اروپا (ETSI) برای تهیه استانداردها و پروتکل‌هایی IoT با هم همکاری نموده‌اند. این پروتکل ها را می توان به پروتکل های کاربردی، پروتکل های مسیریابی، پروتکل های لایه شبکه و پروتکل های لایه فیزیکی طبقه بندی کرد. جدول ۱ پروتکل های هر دسته را نشان می دهد [۸].

سه رکن اصلی پشته ارتباطات و استانداردهای اینترنت اشیا:پشته ارتباطی کم توان: اکثر اشیا در IoT توان خود را از باتری می گیرند، در نتیجه آن ها یک منبع محدودی از توان را در اختیار دارند. به این معنی که برقراری ارتباط با استفاده از یک پشته ارتباطی پرتوان دشوار است زیرا تغییر باتری میلیون ها اشیا به صورت روزانه، غیرقابل امکان و پر هزینه به نظر می رسد. از این رو پشته ارتباطات و استانداردهای IoT باید برای رفع این نیاز طراحی شود.

پشته ارتباطی با قابلیت اعتماد بالا: ارتباط انتها به انتهای قابل اعتماد یک عنصر بسیار مهم برای تمام پروتکل های شبکه است. در IoT، اصلی ترین چالش، دستیابی به بالاترین قابلیت اطمینان با استفاده از یک روش کارآمد است.

پشته ارتباطی اینترنتی فعال شده: ایده اولیه IoT این است که به اشیا اجازه صحبت، شنیدن و پاسخ دادن را بدهد، برای دستیابی به این هدف، به یک رسانه ارتباطی دو طرفه نیاز است. یکی از رسانه های موجود، اینترنت است که از IP(پروتکل اینترنت) برای برقراری ارتباط دو طرفه استفاده می کند. از آنجایی که استانداردها و پروتکل‌هایی که در اینترنت سنتی مورد استفاده قرار می‌گیرند برای بکارگیری در دستگاه‌های دارای منابع محدود امکان پذیر نیستند، برای IoT یک پشته ارتباطی فعال IP طراحی شده که نیاز دستگاه های دارای منابع محدود را برآورده می‌سازد.

(جدول- ۱): پروتکل های تهیه شده توسط سازمان های بین المللی برای اینترنت اشیا

Gategory	Protocols
Application Protocols	Constrained Application Protocol(coap)[23][24],message Qucue TransPort(MQTT)[25], Exrensible Messaging and Presencc Protocol(XMPP)[26][27], Advanced Message Queuing Protocol (AMQP)[28], Data .Distnbution Service(DDS)[29]
Routing Protocols	Routing Protocol for Low Power and Lossy Networks(RPL)[30]
Network Protocols	6LowPAN[31] IPv4 IPv6
Link/Device layer	IEEE802.15. Bluetooth Low-Energy(BLE) EPCglobal
Service Discovery Protocol	DNS Service Discovery (DNS-SD)[32] Multicast DNS (Mdns)[33]

۳ – دسته بندی امنیتی

از آنجایی که الگوی اینترنت اشیاء طیف گسترده‌ای از وسایل و تجهیزات، از تراشه‌های پردازشی نهفته‌ی کوچک گرفته تا سرورهای بزرگ انتهایی را در بر می‌گیرد، نیاز دارد تا مسائل امنیتی در سطوح مختلفی رسیدگی شوند. یک دسته‌بندی از مسائل امنیتی برای اینترنت اشیاء در شکل ۳ به همراه مراجع مربوط به هر مسئله ارائه شده است. ما تهدیدات امنیتی را با توجه به معماری استقرار اینترنت اشیاء به شرح زیر دسته‌بندی می‌کنیم

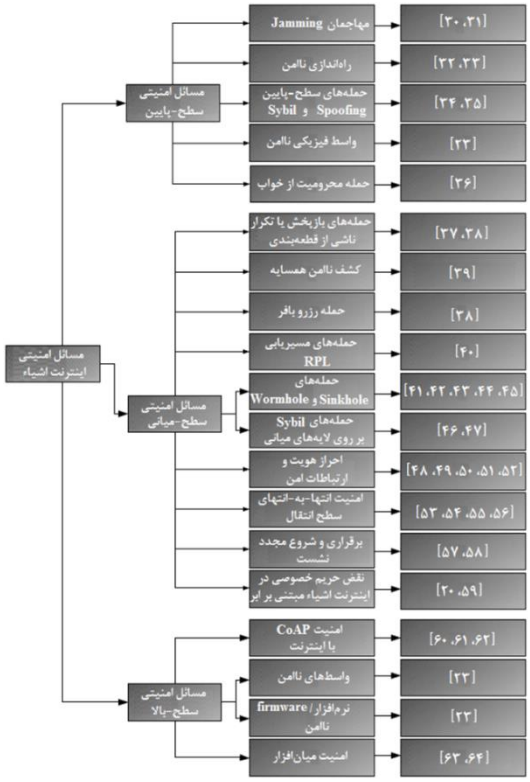
مسائل امنیتی سطح پایین
مسائل امنیتی سطح میانی
مسائل امنیتی سطح بالا

۳-۱ مسائل امنیتی سطح پایین: سطح اول امنیت مربوط به مسائل امنیتی در لایه‌های فیزیکی وپیوند داده در ارتباطات و همچنین سطح سخت‌افزار است.

مهاجمان حمله‌ی jamming: حمله‌های jamming بر روی دستگاه‌های بی‌سیم در اینترنت اشیاء سعی در از بین بردن شبکه‌ها دارند و این کار را با خراب کردن سیگنال‌های فرکانس رادیویی بدون دنبال کردن پروتکل خاصی انجام می‌دهند [۳۰ و ۳۱].

راه‌اندازی اولیه‌ی ناامن: یک روش امن برای راه‌اندازی و پیکربندی اینترنت اشیاء در لایه‌ی فیزیکی، عملکرد صحیح و مناسب کل سیستم را بدون نقض حریم خصوصی و اختلال سرویس‌های شبکه تضمین می‌کند [۳۲ و ۳۳]. ارتباطات لایه‌ی فیزیکی نیز باید امن شوند تا در دسترس گیرنده‌های غیرمجاز قرار نگیرند.

حمله‌های سطح-پایین Sybil و Spoofing:حمله‌های Sybil در یک شبکه‌ی بی‌سیم توسط گره‌های مخرب Sybil صورت می‌گیرند، گره‌هایی که از هویت‌های جعلی برای کاهش کاربردپذیری اینترنت اشیاء استفاده می‌کنند. در لایه‌ی فیزیکی، یک گره‌ی Sybil ممکن است از مقادیر تصادفی و جعل شده‌ی آدرس MAC برای جا زدن خود به عنوان یک دستگاه دیگر استفاده کند، در حالی که قصد تخریب و تخلیه‌ی منابع شبکه را دارد [۳۵ و ۳۴]. در نتیجه، گره‌های قانونی و مشروع در شبکه ممکن است نتوانند به منابع دسترسی داشته باشند.



(شکل-۳): دسته بندی مسائل امنیتی

واسط فیزیکی ناامن:. عوامل فیزیکی مختلف، تهدیدات جدی را برای عملکرد مناسب دستگاه‌های اینترنت اشیاء به وجود می‌آورند. در یک امنیت ضعیف فیزیکی، نرم‌افزار می‌تواند از طریق واسطهای فیزیکی مورد دسترسی قرار بگیرد، و ابزارهای آزمایش/دیباگ ممکن است برای به خطر انداختن گره‌های موجود در شبکه مورد سوءاستفاده قرار بگیرند[۲۳].

حمله‌ی محرومیت از خواب: دستگاه‌هایی با انرژی محدود در اینترنت اشیاء در برابر حمله‌های "محرومیت از خواب" آسیب‌پذیر هستند، این حمله‌ها باعث می‌شوند که گره‌های حسگر همیشه بیدار باشند [۳۶]. وقتی مقدار زیادی از وظایف در محیط LoWPAN۶ برای اجرا تنظیم می‌شوند، حمله‌های محرومیت از خواب منجر تخلیه‌ی باتری می‌شوند.

۲-۳ مسائل امنیتی سطح میانی: مسائل امنیتی سطح میانی به طور عمده مربوط به ارتباطات، مسیریابی و مدیریت نشست است و همانطور که در ادامه شرح داده شده‌اند، در لایه‌های شبکه و انتقال اینترنت اشیاء رخ می‌دهند.

حمله‌های بازپخش یا تکرار (تکثیر) به علت تکه تکه شدن:

تکه‌تکه شدن بسته‌های IPv6 در دستگاه‌های منطبق بر استاندارد IEEE 802.15.4 مورد نیاز است، زیرا این دستگاه‌ها با اندازه‌ی کوچک قاب کار می‌کنند. بازسازی قسمت‌های تکه‌ی بسته در لایه‌ی LoWPAN۶ ممکن است منجر به تخلیه‌ی منابع، سرریزی بافر و راه‌اندازی مجدد دستگاه شود [۳۷]. تکه‌های تکراری ارسال شده توسط گره‌های مخرب بر سرهم‌بندی مجدد بسته تاثیر می‌گذارد، بدین ترتیب مانع از پردازش دیگر بسته‌های قانونی و مجاز می‌شوند [۳۸].

کشف همسایه به صورت ناامن: معماری استقرار اینترنت اشیاء نیاز دارد که هر دستگاه در شبکه به صورت منحصربه‌فردی شناسایی شود. ارتباطات پیامی برای شناسایی باید به صورت امنی صورت گیرد تا تضمین شود که داده‌های ارسال شده به یک دستگاه در ارتباطات انتها-به-انتها در نهایت به مقصد مشخص شده می‌رسد. مرحله‌ی کشف همسایه که پیش از مرحله‌ی انتقال داده‌ها انجام می‌شود، شامل گام‌های مختلفی از جمله کشف مسیریاب و ترجمه‌ی آدرس است [۳۹]. استفاده از بسته‌های کشف همسایه بدون تایید و اعتبارسنجی مناسب ممکن است پیامدهای شدیدا سختی به همراه جلوگیری از سرویس (DoS) داشته باشد.

حمله‌ی رزرو بافر: از آنجایی که یک گره‌ی دریافت‌کننده باید فضای بافر را برای سرهم نمودن بسته‌های ورودی رزرو کند، از این رو یک مهاجم ممکن است از این مورد برای سرریزی فضای بافر با ارسال بسته‌های ناقص بهره ببرد [۳۸]. این حمله منجر به جلوگیری از سرویس (DoS) می‌شود، زیرا با پُر شدن فضای بافر توسط بسته‌های ناقص ارسال شده توسط مهاجم، دیگر فضایی برای تکه‌های بسته‌های دیگر (بسته‌های کاربردهای قانونی) نمی‌ماند و آنها دور ریخته می‌شوند.

حمله‌ی مسیریابی RPL: پروتکل مسیریابی IPv6 برای شبکه‌های کم-توان و با اتلاف (RPL) در برابر حمله‌های مختلف آسیب‌پذیر است، حمله‌هایی که از طریق گره‌های به خطر افتاده‌ی موجود در شبکه رخ می‌دهند [۴۰]. این حمله ممکن است منجر به تخلیه‌ی منابع و شنود شود.

حمله‌های sinkhole و wormhole: با حمله‌های sinkhole، گره‌ی مهاجم به درخواست‌های مسیریابی پاسخ می‌دهد، بنابراین باعث می‌شود تا مسیر بسته‌ها از گره‌ی مهاجم عبور کند و این امر می‌تواند بعدا برای اجرای فعالیت مخرب بر روی شبکه مورد استفاده قرار گیرد [۴۲ و ۴۱]. حمله‌ها بر روی شبکه ممکن است به علت تخریب عملیات LoWPAN۶ توسط حمله‌های wormhole باشد، در حمله‌ی wormhole یک تونل بین دو گره ایجاد می‌شود، به گونه‌ای که بسته‌های رسیده به یک گره

بلافاصله به گره‌ی دیگر می‌رسد [۴۵-۴۳]. این حمله‌ها پیامدهای شدیدی از جمله شنود، نقض حریم خصوصی و جلوگیری از سرویس (DoS) را در پی دارند.

حمله‌های Sybil بر روی لایه‌های میانی: همانند حمله‌های Sybil بر روی لایه‌های سطح پایین، گره‌های Sybil می‌توانند برای کاهش عملکرد شبکه و حتی نقض حریم خصوصی داده‌ها مورد استفاده قرار گیرند. ارتباطات انجام گرفته توسط گره‌های Sybil که از هویت‌های جعلی در یک شبکه استفاده می‌کنند، ممکن است منجر به هرزنگاری (spamming)، انتشار بدافزار یا راه‌اندازی حملات فیشینگ شود [۴۷ و ۴۶].

احراز هویت و ارتباطات امن: دستگاه‌ها و کاربران در اینترنت اشیاء باید از طریق سیستم‌های مدیریت کلید احراز هویت شوند. هر حفره‌ی حلقه‌ای (loophole) در امنیت لایه‌ی شبکه یا سربار زیاد ارتباطات امن ممکن است منجر به آسیب‌پذیری‌های زیادی در شبکه شود [۵۰-۴۸]. به عنوان مثال، با توجه به منابع محدود، سربار امنیت سطح انتقال دیتاگرام (DTLS) باید به حداقل برسد، و روش‌های رمزنگاری تضمین‌کننده‌ی ارتباطات امن داده‌ها باید با توجه به کارایی و کمبود دیگر منابع در نظر گرفته شوند [۵۲ و ۵۱].

امنیت انتها-به-انتهای سطح انتقال: امنیت انتها-به-انتهای سطح انتقال سعی دارد روش امنی را به گونه‌ای ارائه دهد که داده‌های ارسال شده توسط گره‌ی فرستنده، توسط گره‌ی مقصد مورد نظر به صورت قابل اعتمادی دریافت شود [۵۴ و ۵۳]. این امر به روش‌های احراز هویت جامعی نیاز دارد که ارتباط امن پیام را به صورت رمزنگاری شده و بدون نقض حریم خصوصی تضمین کند، و در عین حال با حداقل سربار کار کند [۵۶ و ۵۵].

برقراری و شروع مجدد نشست: ربودن نشست در لایه‌ی انتقال با پیام‌های جعلی می‌تواند منجر به جلوگیری از سرویس (DoS) شود [۵۸ و ۵۷]. یک گره‌ی مهاجم می‌تواند خود را به هویت گره‌ی قربانی در آورد تا به نشست بین دو گره ادامه دهد (یعنی گره‌ی مهاجم به جای گره‌ی قربانی، با جعل هویت وی، به ارتباط با طرف دیگر ارتباط ادامه دهد). گره‌های در حال ارتباط ممکن است با تغییر شماره ترتیب بسته‌ها، نیاز به ارسال مجدد پیام‌ها داشته باشند.

نقض حریم خصوصی بر روی اینترنت اشیاء مبتنی ابر:
حمله‌های مختلفی که ممکن است محرمانگی هویت و مکان را نقض کنند، ممکن است بر روی ابر یا در اینترنت اشیاء مبتنی بر شبکه‌های تحمل‌پذیر تاخیر رخ دهند [۵۹ و ۲۰]. به طور مشابه، یک فراهم‌کننده‌ی مخرب سرویس ابر که استقرار اینترنت اشیاء مبتنی بر آن است، می‌تواند به اطلاعات محرمانه‌ای که به یک مقصد خاص ارسال می‌شوند، دسترسی داشته باشد.

۳-۳. مسائل امنیتی سطح بالا- همانطور که در ادامه شرح داده شده است، مسائل امنیتی سطح بالا به طور عمده مربوط به برنامه‌های کاربردی در حال اجرا بر روی اینترنت اشیاء است.

امنیت CoAP با اینترنت: لایه‌ی سطح بالا، که شامل لایه‌ی برنامه‌ی کاربردی است، نیز در برابر حملات آسیب‌پذیر می‌باشد [۶۰-۶۲]. پروتکل برنامه‌ی کاربردی محدود شده (CoAP) در واقع یک پروتکل انتقال وب برای دستگاهی با منابع محدود است که از ملحقات DTLS با حالت‌های مختلف امنیتی استفاده می‌کند تا امنیت انتها-به-انتها را تامین نماید. پیام‌های CoAP فرمت خاصی را دنبال می‌کنند که در گزارش RFC-7252 29] تعریف شده است، که برای ارتباط باید رمزنگاری شود. به طور مشابه، چندپخشی پشتیبانی شده در CoAP نیاز به مدیریت مناسب کلید و روش‌های احراز هویت دارد.

واسطهای ناامن: برای دسترسی به سرویس‌های اینترنت اشیاء، واسطهایی که از طریق وب، تلفن همراه، و ابر مورد استفاده قرار می‌گیرند، در برابر حمله‌های مختلف آسیب‌پذیر هستند که ممکن است به شدت بر حریم خصوصی داده‌ها تاثیر بگذارد [۲۳].

نرم‌افزار/firmware ناامن: آسیب‌پذیری‌های متعددی در اینترنت اشیاء وجود دارند که از جمله‌ی آنها به مواردی اشاره نموده که توسط نرم‌فزار/firmware ایجاد می‌شوند [۲۳]. کدی که با زبان‌های از قبیل JSON، XML، SQLi و XSS نوشته شده است، باید به دقت مورد آزمایش قرار گیرد. به طور مشابه، بروزرسانی‌های نرم‌افزار/firmware نیز باید به صورت امن و مطمئنی انجام شود.

امنیت میان‌افزار: میان‌افزار اینترنت اشیاء که برای برقراری ارتباط میان موجودیت‌های ناهمگن در الگوی اینترنت اشیاء طراحی شده است، باید برای ارائه‌ی سرویس‌ها به اندازه‌ی کافی امن باشد. واسطها و محیط‌های مختلفی باید با استفاده از میان‌افزار ترکیب شوند تا ارتباطات امنی را ارائه دهند [۶۴ و ۶۳].

۴– راهکارهای امنیتی برای اینترنت اشیاء:

تهدیدات امنیتی در اینترنت اشیاء از آسیب‌پذیری‌های موجود در اجزای مختلف از قبیل برنامه‌های کاربردی/واسط‌ها، اجزای شبکه، نرم‌افزار، firmware، و دستگاه‌های فیزیکی بهره می‌برند که این موارد در سطوح مختلفی موجود هستند. کاربران در یک الگوی اینترنت اشیاء از طریق پروتکل ها با این اجزاء تعامل دارندکه ممکن است اقدامات امنیتی آنها درهم شکسته شود.

اقدامات متقابل برای تهدیدات امنیتی می‌پردازند تا به سطح خاصی از امنیت دست یابند. پروتکل‌های متنوعی که از استقرار اجزاء پشتیبانی می‌کنند، به پیچیدگی این اقدامات متقابل می‌افزایند. بررسی کلی شده است. یک تحلیل مقایسه‌ای از سطح-میانی شامل لایه انتقال، و سطح-بالایی به ترتیب در جدول‌های ۱ تا ۴ ارائه شده است. تحلیل مقایسه‌ای پارامترهای تهدیدها، پیامدهای آنها، لایه‌های متاثر (تحت تاثیر قرار گرفته)، سطوح مرتبط و راه‌حل‌های ممکن پیشنهاد شده در مقالات مرتبط را در نظر می‌گیرد.

(جدول-۱): طرحی از تهدیدات،پیامدها،راه حل های امنیتی، اینترنت اشیاء،سطح پایینی زیرلایه انتقال

شماره ترتیب	مسئله‌ی امنیتی	پیامدها	لایه‌های متاثر	سطوح اینترنت	راه‌حل‌های پیشنهادی	مراجع
۱	مهاجمان Jamming	اختلال و جلوگیری از سرویس	لایه‌ی فیزیکی	سطح-پایین	اندازه‌گیری قدرت سیگنال، محاسبه‌ی نرخ تحویل بسته،	[۲۹، ۳۱، ۳۰]
۲	حمله‌های Sybil و Spoofing	اختلال در شبکه، جلوگیری از سرویس	لایه‌ی فیزیکی	سطح-پایین	اندازه‌گیری قدرت سیگنال، و تخمین کانال	[۲۸-۲۷، ۳۵، ۳۴]
۳	راه‌اندازی و پیکربندی نالمن	نقض حریم خصوصی و جلوگیری از	لایه‌ی فیزیکی	سطح-پایین	تنظیم نرخ انتقال داده‌ها بین گره‌ها، و معرفی نویز	[۳۲، ۳۳، ۲۶]
۴	واسط فیزیکی نالمن	نقض حریم خصوصی، جلوگیری از	سخت‌افزار	سطح-پایین	اجتناب از دسترسی نرم‌افزار/	[۲۳]
۵	حملهی محرومیت از خواب	مصرف انرژی	لایه‌ی پیوند	سطح-پایین	سیستم تشخیص نفوذ مبتنی بر چند-لایه	[۳۶]
۶	فشرده‌سازی هدر و AES مبتنی بر نرم‌افزار، TPM، استفاده از RSA احراز هویت ترکیبی SHA1/AES، احراز هویت با استخراج‌کننده، رمزنگاری مقادیر نوع ارسال بار بسته با AH فشرده، ACAC، استفاده از رمزنگاری منتخب بیضوی، logهای توزیع	راه رفتن تصادفی بر روی گراف‌های اجتماعی، تحلیل رفتار کاربر، و نگهداری از لیست‌های کاربران مورد اعتماد/غیر قابل اعتماد	سطح-میانی	سطح-میانی	ارزیابی رتبه از طریق تابع زنجیره هش، مدیریت سطح اعتماد، تحلیل رفتار و ارتباطات گره‌ها، تشخیص ناهنجاری از طریق IDS، مدیریت کلید رمزنگاری، پیمایش گراف، و اندازه‌گیری قدرت سیگنال	[۴۱-۲۵، ۲۴-۹]
۷	احراز هویت و ارتباطات امن	حملههای Sybil	۴	سطح-میانی	نقض حریم خصوصی، Spamming، خطای بیزانتین، همه‌پخشی غیر قابل اعتماد	[۴۶، ۴۷، ۲۲-۹]

(جدول-۲): طرحی از تهدیدات،پیامدها و راه کار های منیتی اینترنت اشیاء سطح میانی

شماره ترتیب	مسئله‌ی امنیتی	پیامدها	لایه‌های متاثر	سطوح اینترنت اشیاء	راه‌حل‌های پیشنهادی	مراجع
۱	حمله‌های بازپخش یا تکرارناشی ازقطعه‌بندی	اختلال و جلوگیری از سرویس	لایه‌ی تطبیقی 6LoWPAN، و لایه‌ی شبکه	سطح-میانی	معرفی برچسب زمانی و گزینه‌های nonce برای محافظت در برابر حمله‌های بازپخش، و ارزیابی قطعه از طریق زنجیره‌های هش	[۳۷، ۳۸]
۲	کشف نالمن همسایه	IP Spoofing	لایه شبکه	سطح-میانی	احراز هویت با استفاده از رمزنگاری منحنی بیضوی (ECC) مبتنی بر امضاها	[۳۹]
۳	حمله رزرو بافر	مسدود کردن بافر مجدد	لایه‌ی تطبیقی 6LoWPAN، و لایه شبکه	سطح-میانی	رویکرد شکستن بافر موردنیاز برای انتقال کامل قطعه‌ها	[۳۸]
۴	حمله مسیریابی RPL	شنود، حمله مرد میانی	لایه شبکه IPv6	سطح-میانی	احراز هویت مبتنی بر امضا و هش کردن، و نظارت بر رفتار گره	[۴۰، ۵۷]
۵	حملههای Sinkhole و Wormhole	جلوگیری از سرویس	لایه شبکه	سطح-میانی	ارزیابی رتبه از طریق تابع زنجیره هش، مدیریت سطح اعتماد، تحلیل رفتار و ارتباطات گره‌ها تشخیص ناهنجاری از طریق IDS، مدیریت کلید رمزنگاری، پیمایش گراف، و اندازه‌گیری قدرت سیگنال	[۴۱-۲۵، ۲۴-۹]
۶	حملههای Sybil	نقض حریم خصوصی، Spamming، خطای بیزانتین، همه‌پخشی غیر قابل اعتماد	لایه‌ی شبکه	سطح-میانی	راه رفتن تصادفی بر روی گراف‌های اجتماعی، تحلیل رفتار کاربر، و نگهداری از لیست‌های کاربران مورد اعتماد/غیر قابل اعتماد	[۴۶، ۴۷، ۲۲-۹]
۷	لایه‌ی تطبیقی LoWPAN، لایه انتقال، لایه شبکه	فشرده‌سازی هدر و AES مبتنی بر نرم‌افزار، TPM، استفاده از RSA احراز هویت ترکیبی SHA1/AES، احراز هویت با استخراج‌کننده، رمزنگاری مقادیر نوع ارسال بار بسته با AH فشرده، ACAC، استفاده از رمزنگاری منحنی بیضوی، logهای توزیع	سطح-میانی	سطح-میانی	ارزیابی رتبه از طریق تابع زنجیره هش، مدیریت سطح اعتماد، تحلیل رفتار و ارتباطات گره‌ها تشخیص ناهنجاری از طریق IDS، مدیریت کلید رمزنگاری، پیمایش گراف، و اندازه‌گیری قدرت سیگنال	[۱۸، ۱۹، ۱۰، ۱۰، ۵۹، ۲۱، ۲۰]

(جدول-۳): طرحی از تهدیدات،پیامدها و راه کار های منیتی اینترنت اشیاء سطح میانی.

شماره ترتیب	مسئله‌ی امنیتی	پیامدها	لایه‌های متاثر	سطوح اینترنت اشیاء	راه‌حل‌های پیشنهادی	مراجع
۱	امنیت انتها-به- انتهای سطح انتقال	نقض حریم خصوصی	لایه ی انتقال، و لایه شبکه	سطح میانی	الگوریتم های مبتنی بر رمز DTLS ، IPSEC فشرده، فشرده سازی هدر DTLS. IKEV2 با استفاده از UDP فشرده ، و امنیت مبتنی بر AES/CCM با شناسایی و صدور مجوز دسترسی	[14-15,92,17,56-53]
۲	ایجاد و شروع مجدد نشست	جلوگیری از سرویس	لایه انتقال	سطح میانی	احراز هویت با کلید مخفی طولانی مدت ، و رمزنگاری مبتنی بر کلید متقارن	[58,14,57]

(جدول-۴): طرحی از تهدیدات، پیامدها، و راه‌حل‌های امنیتی اینترنت اشیاء در سطح بالایی.

شماره ترتیب	مسئله‌ی امنیتی	پیامدها	لایه‌های متاثر	سطوح اینترنت اشیاء	راه‌حل‌های پیشنهادی	مراجع
۱	امنیت CoAP با اینترنت	تنگنا در شبکه، جلوگیری از سرویس	لایه‌ی برنامه‌ی کاربردی، و لایه‌ی شبکه	سطح-بالا و سطح-میانی	نگاشت TLS/DTLS و HTTP/CoAP، پروکسی آینه (MP) و کشف منابع، تونل TLS/DTLS و فیلتر کردن پیام با استفاده از 6LBR	[۶۲-۶۰، ۱۳]
۲	واسطهای ثالث	نقض حریم خصوصی، جلوگیری از سرویس، اختلال در شبکه	لایه‌ی برنامه‌ی کاربردی	سطح-بالا	اجازه ندادن به کلمات عبور ضعیف، آزمایش کردن واسط در برابر آسیب‌پذیری‌های ابزارهای نرم‌افزاری (SQLi و XSS)، و استفاده از https به همراه دیواره‌ی آتش	[۲۳]
۳	نرم‌افزار/firmware ثالث	نقض حریم خصوصی، جلوگیری از سرویس، اختلال در شبکه	لایه برنامه کاربردی، لایه انتقال، لایه شبکه	سطح-بالا، میانی، و پایین	بروزرسانی‌های منظم و امن نرم‌افزار/firmware، استفاده از امضاهای فایل، و رمزنگاری با تایید	[۲۳]
۴	امنیت میان‌افزار	نقض حریم خصوصی پیشگیری از سرویس، اختلال در شبکه	لایه‌برنامه کاربردی، لایه انتقال، لایهی شبکه	سطح-بالا، میانی، و پایین	ارتباطات امن با استفاده از احراز هویت، سیاست‌های امنیت، مدیریت کلید میان دستگاه‌ها، دروازه‌ها و اجزای M2M، امنیت M2M لایه‌ی سرویس، میان‌افزار شفاف با استفاده از روش‌های احراز	[۶۳، ۱۰، ۶۴، ۱۱، ۱۲]

۵ – نتیجه گیری

امروزه دستگاه‌های اینترنت اشیاء ناامن بوده و قادر به دفاع از خود نیستند. علت این امر عمدتا به دلیل وجود منابع محدود در دستگاه‌های اینترنت اشیاء، استانداردهای نابالغ، و فقدان طراحی، توسعه، و پیاده‌سازی امن سخت‌افزاری و نرم‌افزاری است. همچنین تنوع منابع در اینترنت اشیاء مانع از تعریف یک روش کلی قوی برای امن نمودن لایه‌های اینترنت اشیاء شده است. ما در این مقاله به بررسی و مرور مسائل عمده‌ی امنیتی در اینترنت اشیاء پرداخته‌ایم. ما این مسائل را بسته به سطح بالا، سطح میانی، و سطح پایین لایه‌های اینترنت اشیاء دسته‌بندی نموده‌ایم. ما به طور خلاصه در مورد روش‌هایی بحث نموده‌ایم که در مقالات مختلف برای ارتقای امنیت اینترنت اشیاء در سطوح مختلف پیشنهاد شده‌اند. یک تحلیل پارامتری از حمله‌ها در اینترنت اشیاء و راه‌حل‌های احتمالی آنها نیز ارائه شده است. ما پیامدهای حمله‌ها را در نظر گرفته و آنها را به راه‌حل‌های ممکن ارائه شده در مقالات نگاشت نموده‌ایم. ما همچنین در این مورد بحث نموده‌ایم که بلاک‌چین چگونه می‌تواند به برخی از مهمترین مسائل امنیتی اینترنت اشیاء رسیدگی نموده و آنها را حل نماید. مقاله همچنین مسائل باز تحقیقاتی و چالش‌های آینده را مطرح و تعریف کرده است، مسائلی که نیاز به رسیدگی بیشتر توسط جوامع تحقیقاتی دارند تا راه‌حل‌های امنیتی قابل‌اطمینان، کارآمد، و مقیاس‌پذیر برای اینترنت اشیاء ارائه شود.

۶- مراجع

[1]"Auto-ID Labs," 2017. [Online]. Available: http://www.autoidlabs.org.

[2]Y. Huang and G. Li, "Descriptive Models for Internet of Things," in International Conference on Intelligent Control anf Information Processing, 2010, pp. 483–486.

[3]A. Bassi and G. Horn, "Internet of Things in 2020: A Roadmap for the Future," in European Commission: Information Society and Media, 2008.

[4]L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Networks, pp. 2787–2805, 2010.

[5]V. Potdar, A. Sharif, and E. Chang, "Wireless Sensor Networks," in International Conference on Advanced Information Networking and Applications Workshops, 2009, pp. 393–422.

[6] "Internet Engineering Task Force," 2007. [Online]. Available: https://tools.ietf.org/html/rfc4944.

[7]S. Farahani, ZigBee wireless networks and transceivers. 2011.

[8]B. Fouladi and S. Ghanoun, "Security Evaluation of the Z-Wave Wireless Protocol," Black hat USA, pp. 1–6, 2013.

[9] L. Alvisi, A. Clement, A. Epasto, S. Lattanzi, A. Panconesi, SoK: the evolution of sybil defense via social networks, in: Proceedings of the 2013 IEEE Symposium on Security and Privacy, SP '13, IEEE Computer Society, Washington, DC, USA, 2013, pp. 382–396. http://dx.doi.org/10.1109/SP.2013.33

[10]A. Gmez-Goiri, P. Ordua, J. Diego, D.L. de Ipiña, Otsopack: Lightweight semantic framework for interoperable ambient intelligence applications, Comput. Hum. Behav. 30 (Suppl. C) (2014) 460–467. http://dx.doi.org/10.1016/j.chb.
.۲۰۱۳/۰۶/۰۲۲

[11] OneM2M, Security solutions –OneM2M Technical Specification, 2017. URL http://onem2m.org/technical/latest-drafts.

[12]H.G.C. Ferreira, R.T. de Sousa, F.E.G. de Deus, E.D. Canedo, Proposal of a secure, deployable and transparent middleware for Internet of Things, in: 2014 9th Iberian Conference on Information Systems and Technologies, CISTI, 2014,pp.1–4. http://dx.doi.org/10.1109/CISTI.2014.6877069.

[13] S. Prez, J.A. Martnez, A.F. Skarmeta, M. Mateus, B. Almeida, P. Mal, ARMOUR: Large-scale experiments for IoT security trust, in: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), 2016, pp. 553–558. http://dx.doi.org/10.1109/WF-oT.2016.7845504.

Conference on Recent Advances in Internet of Things (RIoT), 2015, pp. 1–6. http://dx.doi.org/10.1109/RIOT.2015.7104906.

[22]D. Quercia, S. Hailes, Sybil attacks against mobile users: Friends and foes to the rescue, in: Proceedings of the 29th Conference on Information Communications, INFOCOM'10, IEEE Press, Piscataway, NJ, USA, 2010, pp. 336–340 URL http://dl.acm.org/citation.cfm?id=1833515.1833 58

[23]OWASP, Top IoT Vulnerabilities, 2016. URL https://www.owasp.org/index. php/Top_IoT_Vulnerabilities.

[24] S. Sharmila, G. Umamaheswari, Detection of sinkhole attack in wireless sensor networks using message digest algorithms, in: 2011 International Conference on Process Automation, Control and Computing, 2011, pp. 1–6

[25]A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen, M. Chai, The impact of rank attack on network topology of routing protocol for low-power and lossy networks, IEEE Sens. J. 13 (10) (2013) 3685–3692. http://dx.doi.org/10.1109/JSEN.2013. .۲۲۶۶۳۹۹

[26]Y.-C. Hu, A. Perrig, D.B. Johnson, Ariadne: A secure on-demand routing pro

[27]T. Pecorella, L. Brilli, L. Muchhi, The role of physical layer security in IoT: A novel perspective, Information 7 (3) (2016.(

[28]M. Demirbas, Y. Song, An RSSI-based scheme for sybil attack detection in wireless sensor networks, in: Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks, WOWMOM ,۰۶IEEE Computer Society, Washington, DC, USA, 2006, pp. 564–570. http

[29]L. Xiao, L. Greenstein, N. Mandayam, W. Trappe, Fingerprints in the ether: Using the

[14]R. Hummen, H. Wirtz, J.H. Ziegeldorf, J. Hiller, K. Wehrle, Tailoring end-to-end IP security protocols to the Internet of Things, in: 2013 21st IEEE International Conference on Network Protocols (ICNP), 2013, pp. 1–10. http://dx.doi.org/ /۱۰/۱۱۰۹ICNP.2013.6733571

[15] BUTLER-Consortium, BUTLER smartlife – uBiquitous, secUre inTernet-ofthings with Location and contExt-awaReness, 2014. URL http://cordis.europa. eu/docs/projects/cnect/1/287901/080/deliverable s/001-287901BUTLERD25.

[16] S. Raza, T. Chung, S. Duquennoy, D. Yazar, T. Voigt, U. Roedig, Securing Internet of Things with Lightweight IPsec, SICS, Lancaster University, UK

[17]S. Raza, S. Duquennoy, J. Hglund, U. Roedig, T. Voigt, Secure communication for the Internet of Things–a comparison of link-layer security and IPsec for ۶LoWPAN, Secur. Commun. Netw. 7 (12) (2014) 2654–2668. http://dx.doi

[18] T. Kothmayr, C. Schmitt, W. Hu, M. Brnig, G. Carle, 37th Annual IEEE Conference on Local Computer Networks - Workshops, 2012, pp. 956–963. http: //dx.doi.org/10.1109/LCNW.2012.642408

[19]X. Huang, Y. Xiang, E. Bertino, J. Zhou, L. Xu, Robust multi-factor authentication for fragile communications, IEEE Trans. Dependable Secure Comput. ۱۱ (۶) (۲۰۱۴) ۵۶۸–۵۸۱. http://dx.doi.org/10.1109/TDSC.2013.2297110 .

[20]I. Stojmenovic, S. Wen, X. Huang, H. Luan, An overview of fog computing and its security issues, Concurr. Comput. Pract. Exp. 28 (10) (2016) 2991–3005. http://dx.doi.org/10.1002/cpe.3485

[21] J.M. Bohli, A. Skarmeta, M.V. Moreno, D. Garca, P. Langendörfer, SMARTIE project: Secure IoT data management for smart cities, in: 2015 International

multiantenna wireless systems: An overview of signal processing approaches, IEEE Signal Process. Mag. 30 (5) (2013) 29–40.

[36] L. Xiao, L.J. Greenstein, N.B. Mandayam, W. Trappe, Channel-Based detection of sybil attacks in wireless networks, IEEE Transa. Inf. Forensics Secur. 4 (3(.۵۰۳–۴۹۲ (۲۰۰۹)

[37] Y. Chen, W. Trappe, R.P. Martin, Detecting and localizing wireless spoofing attacks, in: 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2017, pp. 193–202.

[38] T. Bhattasali, R. Chaki, A survey of recent intrusion detection systems for wireless sensor network, in: D.C. Wyld, M. Wozniak, N. Chaki, N. Meghanathan, D. Nagamalai (Eds.), Advances in Network Security and Applications: 4th International Conference, CNSA 2011, Chennai, India, July 15–17, 2011, Springer Berlin Heidelberg, Berlin, Heidelberg, 2011, pp. 268–280.

[39] H. Kim, Protection against packet fragmentation attacks at 6LoWPAN adaptation layer, in: 2008 International Conference on Convergence and Hybrid Information Technology, 2008, pp. 796–801. http://dx.doi.org/10.1109/ICHIT. .۲۰۰۸/۲۶۱

[40]R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, K. Wehrle, 6LoWPAN Fragmentation attacks and mitigation mechanisms, in: Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec '13, ACM, New York, NY, USA, 2013, pp. 55–66. http://dx.doi. org/10.1145/2462096.2462107.

[41]R. Riaz, K.-H. Kim, H.F. Ahmed, Security analysis survey and framework design for IP connected LoWPANs, in: 2009 International Symposium on Autonomous physical layer for wireless authentication, in: 2007 IEEE International Conference on Communications, 2007, pp. 4646–4651. http://dx.doi.org/10. /۱۱۰۹ICC.2007.767.

[30]M. Demirbas, Y. Song, An RSSI-based scheme for sybil attack detection in wireless sensor networks, in: Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks, WOWMOM ,۰۶'IEEE Computer Society, Washington, DC, USA, 2006, pp. 564–570. http: //dx.doi.org/10.1109/WOWMOM.2006.27

[31]W. Xu, T. Wood, W. Trappe, Y. Zhang, Channel surfing and spatial retreats: Defenses against wireless denial of service, in: Proceedings of the 3rd ACM Workshop on Wireless Security, WiSe '04, ACM, New York, NY, USA, 2004, pp. 80–89. http://dx.doi.org/10.1145/1023646.1023661

[32]W. Xu, W. Trappe, Y. Zhang, T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks, in: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc '05, ACM, New York, NY, USA, 2005, pp. 46–57. http://dx.doi.org/ .۱۰۶۲۶۸۹/۱۰۶۲۶۹۷/۱۰/۱۱۴۵

[33]G. Noubir, G. Lin, Low-power DoS attacks in data wireless LANs and countermeasures, SIGMOBILE Mob. Comput. Commun. Rev. 7 (3) (2003) 29–30.

[34] S.H. Chae, W. Choi, J.H. Lee, T.Q.S. Quek, Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone, Trans. Info. for. Sec. 9 (10) (2014) 1617–1628. http://dx.doi.org/10.1109/TIFS.2014.2341453.

[35] Y.-W.P. Hong, P.-C. Lan, C.-C.J. Kuo, Enhancing physical-layer secrecy in

[49]G. Wang, M. Mohanlal, C. Wilson, X. Wang, M. Metzger, H. Zheng, B.Y. Zhao, Social turing tests: Crowdsourcing sybil detection, in: Symposium on Network and Distributed System Security, NDSS, 2013.

[50]J. Granjal, E. Monteiro, J.S. Silva, Network-layer security for the Internet of Things using TinyOS and BLIP, Int. J. Commun. Syst. 27 (10) (2014) 1938–1963http://dx.doi.org/10.1002/dac.2444.

[51]S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, U. Roedig, Securing communication in 6LoWPAN with compressed IPsec, in: 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011, pp. 1–8. http://dx.doi.org/10.1109/DCOSS.2011.5982177.

[52] J. Granjal, E. Monteiro, J.S. Silva, Enabling network-layer security on IPv6 wireless sensor networks, in: 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, 2010, pp. 1–6. http://dx.doi.org/10.1109/GLOCOM.2010.5684293.

[53] P.N. Mahalle, B. Anggorojati, N.R. Prasad, R. Prasad, Identity authentication and capability based access control (iacac) for the internet of things, J. Cyber Secur. Mobility 1 (4) (2013) 309–348.

[54] D.U. Sinthan, M.-S. Balamurugan, Identity authentication and capability based access control (IACAC) for the Internet of Things, J. Cyber Secur. Mob. 1 (4) (2013) 309–348.

[55]M. Brachmann, O. Garcia-Morchon, M. Kirsche, Security for practical CoAP applications: Issues and solution approaches, in: 10th GI/ITG KuVS Fachgespraech Sensornetze (FGSN 2011), 2011.

[56] J. Granjal, E. Monteiro, J.S. Silva, End-to-end transport-layer security for Decentralized Systems, 2009, pp. 1–6. http://dx.doi.org/10.1109/ISADS.2009.5207373.

[42]A. Dvir, T. Holczer, L. Buttyan, VeRA - version number and rank authentication in RPL, in: 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, 2011, pp. 709–714. http://dx.doi.org/10.1109/MASS.2011.76.

K. Weekly, K. Pister, Evaluating sinkhole [43]defense techniques in RPL networks, in: Proceedings of the 2012 20th IEEE International Conference on Network Protocols (ICNP), ICNP '12, IEEE Computer Society, Washington, DC, USA, 2012, pp. 1–6. http://dx.doi.org/10.1109/ICNP.2012.6459948.

[44]F. Ahmed, Y.-B. Ko, Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks, Secur. Commun. Netw. 9 (18) (2016) 5143–5154SCN-16-0443.R1.

[45] A.A. Pirzada, C. McDonald, Circumventing sinkholes and wormholes in wireless sensor networks, in: International Workshop on Wireless Ad-Hoc Networks, 2005.

[46] W. Wang, J. Kong, B. Bhargava, M. Gerla, Visualisation of wormholes in underwater sensor networks: A distributed approach, Int. J. Secur. Netw. 3 (1(2008) 10–23.

[47]M. Wazid, A.K. Das, S. Kumari, M.K. Khan, Design of sinkhole node detection mechanism for hierarchical wireless sensor networks, Sec. Commun. Netw. 9 (17) (2016) 4596–4614. http://dx.doi.org/10.1002/sec.1652.

[48] K. Zhang, X. Liang, R. Lu, X. Shen, Sybil attacks and their defenses in the internet of things, IEEE Internet Things J. 1 (5) (2014) 372–383. http://dx.doi.org/10.1109/JIOT.2014.2344013

extending CoAP to support end-to-end message security for internet-integrated sensing applications, in: International Conference on Wired/Wireless Internet Communication, Springer Berlin Heidelberg, 2013, pp. 140–153.

[64] M. Sethi, J. Arkko, A. Kernen, End-to-end security for sleepy smart object networks, in: 37th Annual IEEE Conference on Local Computer Networks -Workshops, 2012, pp. 964–972. http://dx.doi.org/10.1109/LCNW.2012. .۶۴۲۴۰۸۹

[65]D. Conzon, T. Bolognesi, P. Brizzi, A. Lotito, R. Tomasi, M.A. Spirito, The VIRTUS middleware: An XMPP based architecture for secure IoT communications, in: 2012 21st International Conference on Computer Communications and Networks, ICCCN, 2012, pp. 1–6. http://dx.doi.org/10.1109/ICCCN.2012. .۶۲۸۹۳۰۹

[66]C.H. Liu, B. Yang, T. Liu, Efficient naming, addressing and profile services in Internet-of-Things sensory environments, Ad Hoc Netw. 18 (Suppl. C) (2014(.۱۰۱–۸۵
http://dx.doi.org/10.1016/j.adhoc.2013.02.008

internet-integrated sensing applications with mutual and delegated ecc public-key authentication, in: 2013 IFIP Networking Conference, 2013, pp. .۹–۱

[57]G. Peretti, V. Lakkundi, M. Zorzi, BlinkToSCoAP: An end-to-end security framework for the Internet of Things, in: 2015 7th International Conference on Communication Systems and Networks (COMSNETS), 2015, pp. 1–6. http: //dx.doi.org/10.1109/COMSNETS.2015.7098708 .

[58] S. Raza, T. Voigt, V. Jutvik, Lightweight IKEv2: a key management solution for both the compressed IPsec and the IEEE 802.15. 4 security, in: Proceedings of the IETF Workshop on Smart Object Security, vol. 23, 2012.

[59]N. Park, N. Kang, Mutual authentication scheme in secure internet of things technology for comfortable lifestyle, Sensors 6 (1) (2016) 20–20.

[60]M.H. Ibrahim, Octopus: An edge-fog mutual authentication scheme, Internat. J. Netw. Secur. 18 (6) (2016) 1089–1101 .

[61]M. Henze, B. Wolters, R. Matzutt, T. Zimmermann, K. Wehrle, Distributed configuration, authorization and management in the cloud-based internet of things, in: 2017 IEEE Trustcom/BigDataSE/ICESS, 2017, pp. 185–192. http: //dx.doi.org/10.1109/Trustcom/BigDataSE/ICES S.2017.236.

[62] M. Brachmann, S.L. Keoh, O.G. Morchon, S.S. Kumar, End-to-end transport security in the IP-based Internet of Things, in: 2012 21st International Conference on Computer Communications and Networks, ICCCN, 2012, pp. 1–5. http://dx.doi.org/10.1109/ICCCN.2012.6289292.

[63]J. Granjal, E. Monteiro, J.S. Silva, Application-layer security for the WoT:

*رامین شیربندی فارغ التحصیل رشته مهندسی فناوری اطلاعات ارشد دانشگاه آشتیان گرایش مدیریت سیستم های اطلاعاتی*ایمیل

Raminshirbandi77@gmail.com

*فرانه زرافشان فار التحصیل ممتاز مقاطع کارشناسی و کارشناسی ارشد به ترتیب در رشته های مهندسی کامپیوتر گرایش سخت افزار و مهندسی کامپیوتر گرایش معماری کامپیوتر از دانشگاه آزاد اسلامی اراک و فار التحصیل مقطع دکتری رشته مهندسی سیستم های کامپیوتری از دانشگاه UPM. ایشان در حال حاضر استادیار تمام وقت گروه مهندسی فناوری اطلاعات دانشگاه آزاد اسلامی واحد آشتیان و عضو هیأت مدیره شرکت دانش بنیان تحلیل پردازه ارقام هوشمند میباشد. وی استاد راهنما و مشاور بیش از ۴۰ پایان نامه مقطع کارشناسی ارشد و دکترا و استاد داور پایان نامه های ارشد در دانشگاههای مختلف بوده است. علاقه مندی های پژوهشی ایشان عبارتند از اینترنت اشیاء سیستم های توزیع شده و امنیت بحرانی، شبکههای موردی و بیسیم و امنیت شبکه.*Fzarfshan@gmail.com

روش ارجاع به مقاله : ف. زرافشان، ر. شیربندی، بررسی حملات و راهکارهای امنیت اینترنت اشیاء(IOT). دوفصلنامه محاسبات و سامانه های توزیع شده، سال چهارم، شماره اول، شماره پیاپی ۷، صفحه ۲۵ تا ۳۸، سال ۱۴۰۰.

How to cite: Faraneh Zarafshan, Ramin Shirbandi, Investigate IoT attacks and security measures, Journal of Distributed Computing and Systems(JDCS), Vol 4, Issue 1, Page 25-38, 2021.